Lecture Notes in Electrical Engineering 358

Marco Baldi
Stefano Tomasin
Editors

Physical and Data-Link Security Techniques for Future Communication Systems

Springer

Lecture Notes in Electrical Engineering

Volume 358

About this Series

"Lecture Notes in Electrical Engineering (LNEE)" is a book series which reports the latest research and developments in Electrical Engineering, namely:

- Communication, Networks, and Information Theory
- Computer Engineering
- Signal, Image, Speech and Information Processing
- Circuits and Systems
- Bioengineering

LNEE publishes authored monographs and contributed volumes which present cutting edge research information as well as new perspectives on classical fields, while maintaining Springer's high standards of academic excellence. Also considered for publication are lecture materials, proceedings, and other related materials of exceptionally high quality and interest. The subject matter should be original and timely, reporting the latest research and developments in all areas of electrical engineering.

The audience for the books in LNEE consists of advanced level students, researchers, and industry professionals working at the forefront of their fields. Much like Springer's other Lecture Notes series, LNEE will be distributed through Springer's print and electronic publishing channels.

More information about this series at http://www.springer.com/series/7818

Marco Baldi · Stefano Tomasin
Editors

Physical and Data-Link Security Techniques for Future Communication Systems

Springer

Editors

Marco Baldi
Department of Information Engineering
Università Politecnica delle Marche
Ancona
Italy

Stefano Tomasin
Department of Information Engineering
University of Padova
Padova
Italy

ISSN 1876-1100 ISSN 1876-1119 (electronic)
Lecture Notes in Electrical Engineering
ISBN 978-3-319-23608-7 ISBN 978-3-319-23609-4 (eBook)
DOI 10.1007/978-3-319-23609-4

Library of Congress Control Number: 2015948725

Springer Cham Heidelberg New York Dordrecht London

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made.

Printed on acid-free paper

Springer International Publishing AG Switzerland is part of Springer Science+Business Media
(www.springer.com)

Preface

In recent years, communication and data security is becoming of paramount importance, and some significant academic and industrial research efforts are being directed in this area.

Besides classical approaches to security, new paradigms are taking root, with immense potential in a number of scenarios. Among them, physical layer security is one of the most fascinating, though partly unexplored research areas. The first impulse to this approach has been given in the seventies with Wyner's study on the wiretap channel, and since then this field knew an exponential growth. The chance to exploit the random and unique character of the transmission channel to achieve security and authentication is very attractive, and may pave the way to new and more user-oriented security solutions.

However, physical layer security is still not sufficiently mature to provide practical solutions to be included in current communication systems and standards, therefore some effort is still needed in this direction. On the other hand, classical solutions rely on computational security techniques, like cryptography, and work at the data-link layer, assuming perfect transmission at the physical layer. This is a known limit of classical security techniques, especially when they are used over the wireless channel, which always represents a great security challenge, due to its intrinsic broadcast nature. In several occasions, the use of classical security solutions over the wireless channel has resulted in overlooked security threats and vulnerabilities, thus demonstrating the need for a more comprehensive security design, starting at the physical layer. Despite this, the integration of physical and data-link layer security techniques is still in initial stages. Other channels, as the powerline communication channel, pose similar problems as the wireless transmissions, as well as many privacy concerns for the applications usually running on this medium.

The *enhancing communication security by cross-layer physical and data-link techniques* (ESCAPADE) research project supported by the Italian Ministry of Education aims at providing a contribution in the direction to fill the gap, by studying innovative and practical physical and data-link layer security techniques, as well as their integration. The Workshop on Communications Security (WCS 2014) was organized in the framework of the project to foster discussion among researchers working in both these fields, with the aim to address important open problems in the relevant areas and exchange new ideas concerning the links between them.

This book originates from the workshop, and collects extended versions of the works presented on that occasion, together with some relevant invited contributions, addressing some of the most important problems in the two fields of physical and data-link layer security techniques. We believe that this can provide a useful collection of reference material to those interested in these areas, thus fostering the adoption of mixed physical and data-link layer security solutions.

The first part of the book is devoted to physical layer security, with an invited tutorial on advances in this area, starting from a general view and then focusing on some specific scenarios and practical techniques. Among them, we find the use of fading channels and practical codes to achieve security, which are two important solutions in this area, addressed in detail in the next two chapters. Then, two important variants of the basic physical layer security setting are considered, that is, transmission over broadcast channels with confidential messages and extraction of secret keys from the wireless channel. The implementation of these techniques in practical scenarios is then addressed by two chapters on key extraction in ultra wideband transmissions and power line communication networks. The security features of two special settings are then studied. In fact, the next two chapters focus on security in compressed sensing—where the aim is to reduce the sampled size of signals—and fuzzy vaults—which aim at providing secure authentication based on biometric features. The latter chapter opens the second part of the book, which is devoted to computational security techniques, with contributions concerning cryptosystems, like the Naccache-Stern and AES schemes, and their cryptanalysis. The last two chapters of the book provide an insight into the implementation of security and authentication techniques in practice, which is an important target to achieve by any newly introduced security solution.

The editors wish to gratefully acknowledge Franco Chiaraluce and Nicola Laurenti for their precious help throughout the ESCAPADE project, and Nicola Maturo and Giacomo Ricciutelli for their tireless support concerning the organization of WCS 2014.

We also want to thank Matthieu Bloch, Arsenia Chorti, David Elkouss, Frederic Gabry, Ingmar Land, Ayoub Otmani, Edoardo Persichetti, Francesco Renna, Davide Schipani, and Aydin Sezgin for having reviewed the chapters and helped to improve the book quality.

Ancona, Paris
June 2015

Marco Baldi
Stefano Tomasin

Acknowledgments

This book was supported in part by the MIUR project “ESCAPADE” (Grant RBFR105NLC) under the “FIRB—Futuro in Ricerca 2010” funding program.

Contents

Chapter 1
Physical Layer Security: A Paradigm Shift in Data Confidentiality

Arsenia Chorti, Camilla Hollanti, Jean-Claude Belfiore and Harold Vincent Poor

Abstract Physical layer security (PLS) draws on information theory to characterize the fundamental ability of the wireless physical layer to ensure data confidentiality. In the PLS framework it has been established that it is possible to simultaneously achieve reliability in transmitting messages to an intended destination and perfect secrecy of those messages with respect to an eavesdropper by using appropriate encoding schemes that exploit the noise and fading effects of wireless communication channels. Today, after more than 15 years of research in the area, PLS has the potential to provide novel security solutions that can be integrated into future generations of mobile communication systems. This chapter presents a tutorial on advances in this area. The treatment begins with a review of the fundamental PLS concepts and their corresponding historical background. Subsequently it reviews some of the most significant advances in coding theory and system design that offer a concrete platform for the realization of the promise of this approach in data confidentiality.

A. Chorti (✉)
School of Computer Science and Electronic Engineering, University of Essex,
Wivenhoe Park, Colchester CO4 3SQ, UK
e-mail: achorti@essex.ac.uk

C. Hollanti
Department of Mathematics and Systems Analysis, Aalto University
School of Science, 00076 Aalto, Finland
e-mail: camilla.hollanti@aalto.fi

J.-C. Belfiore
Department of Communications and Electronics, Telecom ParisTech,
46, Rue Barrault, 75634 Paris Cedex 13, France
e-mail: jean-claude.belfiore@telecom-paristech.fr

H.V. Poor
Department of Electrical Engineering, EQUAD, Princeton University,
19 Olden Street, Princeton, NJ 08544, USA
e-mail: poor@princeton.edu

M. Baldi and S. Tomasin (eds.), *Physical and Data-Link Security Techniques for Future Communication Systems*, Lecture Notes in Electrical Engineering 358, DOI 10.1007/978-3-319-23609-4_1

1.1 Introduction

1.1.1 Historical Background

In the design of any communication system two fundamental requirements are taken into consideration: (i) reliability in the exchange of information between a source node (in our context, commonly referred to as *Alice*) and an intended destination (*Bob*), and (ii) security in terms of data confidentiality and message integrity with respect to an adversary (*Eve*). These two aspects in the design of any actual communication system have traditionally been addressed separately. This divide is reflected in a decisive difference in the setup of the elementary models proposed first by Claude Shannon for the investigation of the two issues, depicted in Figs. 1.1 and 1.2.

In terms of reliability, a noisy transmission channel was assumed to connect Alice and Bob. On the other hand, for the study of security a noiseless medium linking Alice, Bob and Eve was considered. Using this latter model, Shannon proved in [32] that in the noiseless scenario *perfect secrecy* (unconditional security) in a symmetric key encryption system can be achieved only when the entropy of the security key is at least equal to that of the message; i.e., one needs to use a “one-time-pad” to achieve perfect secrecy in this setting. As a consequence of this pessimistic result, the conclusion that perfect secrecy is not attainable in realistic communication systems

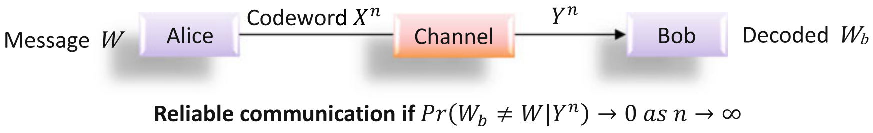

Message W
Alice
Codeword X^n
Channel
Y^n
Bob
Decoded W_b
Reliable communication if $Pr(W_b \neq W|Y^n) \to 0$ as $n \to \infty$

Fig. 1.1 Reliability model

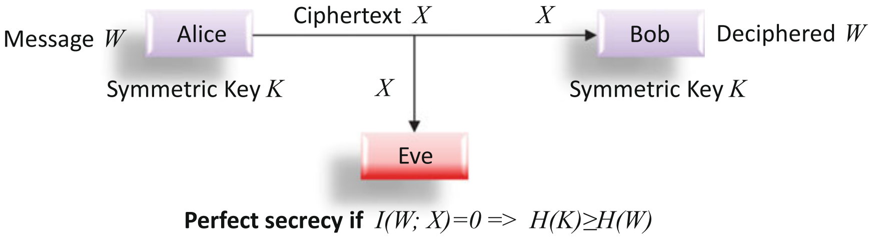


Fig. 1.2 Data confidentiality model

was drawn and alternative approaches to security were sought based on computational complexity properties.

Nowadays, practical cryptographic approaches are built to alternatively achieve *semantic security*, i.e., to withstand polynomial time chosen plaintext and chosen ciphertext attacks [11]. State of the art authenticated encryption schemes that guarantee data confidentiality and integrity have been built around the assumption that the underlying symmetric key block ciphers are semantically secure; however, no formal proof exists to-date for the most advanced block ciphers, including the AES-128, AES-196 and AES-256. Notably, for symmetric key authenticated encryption schemes to work the existence of a "shared" source of entropy that can be accessed by both Alice and Bob and that is inaccessible to Eve is still required, and, the entropy of this source should be sufficient to support a computational complexity proof in the semantic security setting. In protocols in which the keys are only used once this source of randomness is necessary for the continuous update of the symmetric keys. On the other hand, if the keys are used multiple times this source of randomness is used to update complementary parameters, e.g., initialization vectors (IVs), nonces or salts of the particular enciphering schemes used.

On the other hand, in public key authenticated encryption schemes no pre-shared secret is assumed and the security of such schemes relies on the (unproven) intractability of certain "hard" algebraic problems typically involving the use of large prime numbers and elliptic curves. Furthermore, from a practical point of view, the computational resources required by such protocols are significant; this is a serious limiting factor in power limited or mobile applications. As a result, novel approaches for securing next generation mobile systems are needed.

1.1.2 Physical Layer Security

Recently, a fundamentally different approach to security has emerged from the area of information theory under the generic term *physical layer security* (PLS). PLS encompasses all *keyless* security technologies that can ensure perfect secrecy by exploiting a source of entropy typically considered a foe rather than a friend: the noise and the interference in real communication media. PLS was pioneered by Wyner and was founded on the observation that Shannon's noiseless model in [32] is unnecessarily restrictive. In fact, in *all* realistic communication settings the observations of Bob and Eve are *different* realizations of a joint probability distribution (the output of the transmission channel).

Wyner [35] investigated the so called *wiretap channel model* in which Eve's channel is a degraded version of the main channel between Alice and Bob, depicted in Fig. 1.3. He proved that in this setting Alice and Bob can exchange information reliably (with asymptotically zero error rates) and with perfect secrecy (with asymptotically zero rate of information leakage) with the use of a suitable pair of *encoder/decoder* functions. The rate at which information can be transmitted secretly from the source to its intended destination was termed an achievable secrecy rate, and the maximal achievable secrecy rate was termed the channel's *secrecy capacity* (SC).

Maurer [22] and Ahlswede and Csiszár [1] investigated the potential use of noisy channels for secret key distillation and introduced the concept of secret key capacity (SKC), in analogy to the SC. Key generation at the physical layer has been extensively discussed as it offers unique opportunities to generate symmetric secret keys without the overhead of public key encryption. In this context, there exist two different approaches: the channel-type model approach and the source-type model approach. According to the former, a random sequence is transmitted over the channel and observed by Alice and Bob. In the latter Alice and Bob observe a common source of randomness, e.g., their channel gains in a reciprocal transmission medium setting (for example in slow fading channels).

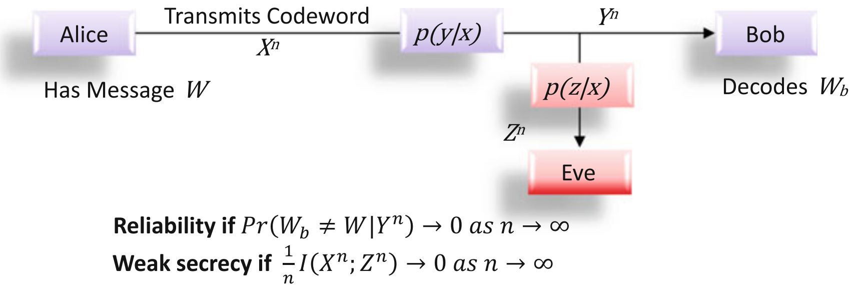

Alice
Transmits Codeword
X^n
$p(y/x)$
Y^n
Bob
Has Message W
$p(z/x)$
Decodes W_b
Z^n
Eve
Reliability if $Pr(W_b \neq W|Y^n) \rightarrow 0 \; as \; n \rightarrow \infty$
Weak secrecy if $\frac{1}{n} I(X^n; Z^n) \rightarrow 0 \; as \; n \rightarrow \infty$

Fig. 1.3 Wyner's model

To exploit either approach in order to distil a shared secret key, Bennet et al. [3] proposed a concrete three-step approach:

1. Advantage distillation: Alice and Bob identify from a set of correlated observations the ones over which they have an "advantage" with respect to Eve.
2. Information reconciliation: These observations are then further processed to "reconcile" discrepancies in order to obtain a mutual shared secret.
3. Privacy amplification: The shared secret is hashed with a universal hash function in order to remove redundancy and produce a uniformly distributed key sequence without leaking information to Eve.

In the following sections we will briefly review the SC of the most important classes of channels and the design of the respective state-of-the-art encoders for secrecy. Subsequently, we will discuss in detail the feasibility of PLS technologies and outline open research issues and future directions of study. This review will be concluded with an overview of the key points regarding PLS technologies.

1.2 Secrecy Capacity of Important Classes of Channels

Following Wyner's contribution, the SC of the scalar Gaussian wiretap channel was analyzed in [16]. It was shown that in this class of channels the SC, denoted by C_s, is given simply as the difference of the capacities of the main link, denoted by C_m, and of Eve's link, denoted by C_e, i.e.,

$$C_s = (C_m - C_e)^+ \tag{1.1}$$

with $(\cdot)^+ = \max(\cdot, 0)$. In [6], Wyner's approach was generalized to the transmission of confidential messages over broadcast channels, depicted in Fig. 1.4.

The broadcast channel with confidential messages (BCC) [6] investigates the scenario in which Alice wishes to broadcast a common message to both Bob and Eve and a confidential message only to Bob. The channel is modeled through a joint probability distribution function for Bob's and Eve's observations, conditioned on the channel input (broadcast by Alice). It was shown in [6] that the SC is the maximum of the difference of the mutual information of the link between Alice and Bob and

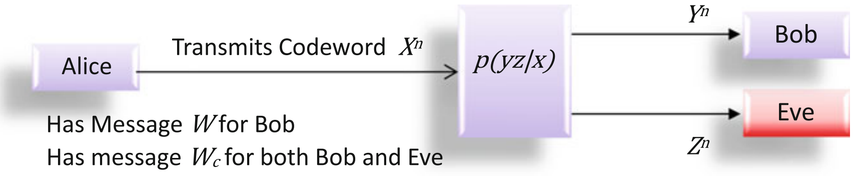


Fig. 1.4 Criszár and Körner's model

of the mutual information in the link between Alice and Eve, expressed as follows when the rate of the common message is set to zero:

$$C_s = \max_{\substack{p_{UX}(u,x) \\ U \to X \to YZ}} I(U;Y) - I(U;Z), \tag{1.2}$$

where U denotes the output of the source,[1] X the input of the channel, Y the observation at the intended destination and Z the observation of the eavesdropper, while the maximization is over all possible joint input distributions $p_{UX}(u,x)$ and $U \to X \to YZ$ form a Markov chain.

As a result, in contrast to the Gaussian wiretap channel, depending on the joint distribution of Bob's and Eve's observations, it can be possible to have a non-zero SC even in the non-degraded case, i.e., even when Eve has a better channel than Bob on average. Such an example is the BCC fading channel, see [18] for more details. For the fading BCC where the confidential message for one receiver must be perfectly secret from the other, it was demonstrated that the secrecy capacity is non-zero even when on average Eve's channel is better than Bob's channel. This can be achieved if the transmitted encoded symbols are multiplexed over the time slots during which Bob's channel fading gain is larger than Eve's fading gain. The key to achieving the SC of the fading channel is optimal power allocation; see [9] for the ergodic fading channel and [18] for the the parallel Gaussian BCC. Finally, a positive SC can be achieved with only statistical channel state information of the eavesdropper's channel, by multiplexing the codewords across all fading realizations [5].

The SC of the multiple-input multiple-output (MIMO) channel allowing an arbitrary number of antennas at the transmitter, legitimate receiver, and eavesdropper was derived in [24], after a considerable amount of previous work that had provided partial proofs or bounds in some limited cases. Since the broadcast channel is not degraded, a new proof technique involving a study of a Sato-like outer bound via the solution of a certain algebraic Riccati equation was introduced. The SC turned out to be the expected one—the results indeed revealed the difference of the mutual information to the legitimate receiver and that to the eavesdropper maximized over the input distribution, similarly to the previous cases. The MIMO SC was independently proved in various other works using different techniques, see [12, 13] among many others. The concept was later extended to the case of three messages (one common and two confidential messages) and to the imperfect secrecy setting by Ekrem and Ulukus [8] and Liu et al. [20], as well as to the delayed channel state information (CSI) feedback case by Yang et al. [37].

In the MIMO multi-receiver case with an external eavesdropper, the SC was derived in [8], and a variant of dirty-paper coding with Gaussian signals was shown to be capacity-achieving. An interesting feature was that the previous converse proof

[1] The channel prefixing random variable U accounts for randomness introduced in the encoding process.

techniques turned out to be insufficient, and thus a new proof technique involving the Fisher information matrix and the generalized De Bruijn identity was adopted.

Furthermore, the multiple-access channel (MAC) with one or two confidential messages was studied in [17] in the binary and Gaussian cases. Inner and outer bounds on the capacity-equivocation region were obtained, where the equivocation (or, conditional entropy) characterizes the level of secrecy maintained at the eavesdropper. In the case of a degraded MAC, the region was explicitly characterized.

Regarding relay networks, the first study of the SC of the relay channel with confidential messages has appeared in [26] while further analyses followed [10, 27]; these contributions established that the SC of one-way relay channels is zero, unless the source-destination channel is better than the source relay channel. In essence, relay topologies of practical interest in which the link to the relay is better than the direct link were shown to be inherently insecure. Due to this limiting result, subsequent work focused primarily on cooperative relay channels with trustworthy relays [2].

1.3 Code Design for Secrecy

Theoretical limits on the SC of wiretap channels have been extensively studied for a broad set of scenarios. On the other hand, the richness of results for the characterization of capacity-equivocation regions is in sharp contrast with the limited amount of actual wiretap code designs, an area in which little is yet known. Theoretical approaches suggest that such code designs should possess a nested code structure and (probably) exploit stochastic encoding. The term “double-binning” encoders was introduced to describe such nested structures with an “outer encoder” essentially generating public codewords that act as cosets to secret codewords generated from an “inner encoder”. Nevertheless, designing explicit SC achieving codes based on this principle is a challenging task as it requires a fine understanding and analysis of a code’s algebraic structure. As a first step to facilitate such designs, Ozarow and Wyner proposed the so-called wiretap II codes [28] adhering to the scenario in which the channel to Bob is a noiseless binary channel, while Eve experiences erasures.

As noted previously, Wyner proved that both robustness to transmission errors and a prescribed degree of data confidentiality can simultaneously be attained by channel coding without any secret key. Wyner replaced Shannon’s perfect secrecy with the weak secrecy condition, namely the asymptotic rate of leaked information between the transmit message and the channel output at Eve’s side should vanish as the code length tends to infinity. Unfortunately, it is still possible for a scheme satisfying weak secrecy to exhibit some security flaws, e.g., the total amount of leaked information may go to infinity, and now it is widely accepted that a physical-layer security scheme should be secure in the sense of Csiszár’s strong secrecy, i.e., the total information leakage should vanish when the code length tends to infinity.

In this framework, recently Mahdavifar and Vardy [21] have proposed polar wiretap codes for symmetric binary input channels and demonstrated that they can be SC achieving for long lengths. Alternatively, the most exploited approach to the design of practical codes so far has been to use low density parity check (LDPC) codes [34], both for binary erasure and symmetric channels and for Gaussian channels with binary inputs.

An important recent development concerns the case of the Gaussian wiretap channel with a power constraint which has been addressed by using lattice codes [19]. This channel model is key in further developments since coding schemes for it include both modulation and coding. Importantly, strong secrecy for any message was proven in this situation in [19]. The proposed coding scheme uses two nested lattices, a fine and a coarse one. A point in the fine lattice is the sum of a coarse lattice point and a point of minimal energy which is in the fine lattice, but not in the coarse lattice. This latter point is similar to the remainder of a Euclidean division.

The proposed coding scheme works as follows:

- A sequence of pseudorandom bits labels the points of the coarse lattice.
- The data labels the pseudo remainder.

If the lattice scheme is correctly designed, then the legitimate receiver, Bob, can reliably decode the fine lattice while Eve has no information concerning the data. A lattice scheme which is good for the wiretap channel is designed in the following manner:

- The fine lattice is good for coding.
- The coarse lattice is good for secrecy, which means that its "flatness factor" [19] vanishes when the code length goes to infinity.

Figure 1.5 shows Eve's likelihood when the noise variance is small and large. When it is large, then Eve cannot distinguish the points of the fine lattice (almost identically distributed). When the flatness factor is small, then points are almost undistinguishable for Eve. The flatness factor is closely related to the theta series of the coarse lattice, which was first studied by Oggier et al. [25].

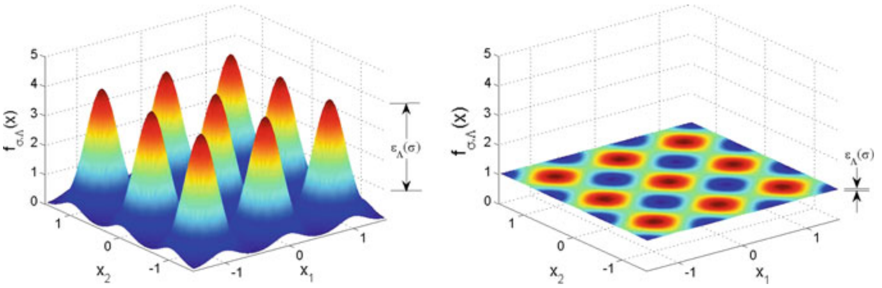


Fig. 1.5 Eve's likelihood when using a two-dimensional lattice. The flatness factor measures the span

1.4 Privacy Amplification Techniques

As explained in Sect. 1.3, the SC and the SKC are asymptotic metrics—achieved as the length of the respective encoders becomes arbitrarily long. These metrics are defined according to a "weak secrecy" requirement so that the *rate of information leakage* to Eve should be arbitrarily small. As noted previously, the adequacy of this secrecy definition has been questioned on the grounds that the absolute amount of information that can be observed by the adversary is not bounded and in general can be non-negligible.

In this context, Maurer and Bennet et al. [3, 22] and other related work [23] have proven that the use of *privacy amplification techniques* can effectively transform a weakly secure channel to a strongly secure channel, in which the adversary can at most observe a negligible absolute amount of information. Favorably, it was demonstrated that the definitions of the SC and of the SKC can be strengthened *without any penalty in terms of achievable rates*. Interestingly, strong secrecy can be obtained from weak secrecy "for free" through the use of a public feedback channel, in essence extending the one-way communication models to two-way communication models.

The core idea behind these techniques is the use of appropriate feedback messages chosen to provide enough *side information* to Bob's secrecy decoder to completely resolve any residual ambiguity, while at the same time leaking only a negligible absolute amount of information to Eve.

–*Toy example*: Let us assume the following scenario of a two phase secret key distillation process. First, Alice broadcasts a random bit sequence. For the sake of simplicity, let us assume that Bob and Eve obtain *independent* noisy observations of this sequence and respective "soft" bit sequences at the outputs of their decoders. In the second phase of the key distillation Bob broadcasts the positions of his most "reliably decodable" bits (bits he decoded with probability arbitrarily close to unity). Assuming that there is sufficient noise in the channel and the sequences are long enough, the probability that Eve has reliably decoded the exact same subsequence as Bob becomes negligible. Finally, Alice and Bob distill their common keys by using a universal hash function to compress the mutually established subsequence. As a result of the use of an *information reconciliation phase* and of a *privacy amplification phase* Alice and Bob have thus distilled a secret key while the absolute amount of information leaked to Eve is kept arbitrarily small.

In the key distillation example discussed above the adversarial channel need not be degraded with respect to (w.r.t.) the main channel; it suffices that it is not almost noiseless, i.e., that Eve cannot reliably decode the whole sequence. In analogy, the use of feedback to ensure secrecy can be further generalized to enable the broadcasting of secret messages in non-degraded channels.

–*Toy example*: let us assume the case in which Alice wishes to transmit a secret message d to Bob while the links between Alice, Bob and Eve are scalar Gaussian channels and the main link is noisier than the eavesdropping link. Under these

Table 1.1 Privacy amplification in non-degraded Gaussian channel

First phase	
Bob transmits	Local random symbol x
Alice receives	$x + n, n \sim \mathcal{N}(0, \sigma_m^2)$
Eve receives	$x + w, w \sim \mathcal{N}(0, \sigma_e^2), \sigma_e^2 \leq \sigma_m^2$
Second phase	
Alice transmits	Encoded symbol $f(d + x + n)$
Bob's optimal decoder	Cancels out x and retrieves d from $f(d + n)$
Eve's optimal decoder	Retrieves d from $f(d + n - w)$ (degraded channel w.r.t. Bob)

assumptions, the SC of the one-way Gaussian channel between Alice and Bob is zero. However, this negative setting can be reversed by allowing for two-way communication between Alice and Bob as described in Table 1.1.

1.5 Applications of PLS Technologies and Extensions to Systems with Active Attacks

In the absence of a feedback channel and under the assumption that only the statistics of the adversarial channel are known, the question of feasibility of PLS technologies can be reduced to whether the intended destination has a measurable statistical advantage w.r.t. to the adversary. There exist important realistic scenarios in which such opportunities can be substantiated, as described in the following.

1.5.1 Massive MIMO and Small Cell Systems

Fifth generation ($5G$) technologies with hundreds of antennas at the base stations can be promising candidates for the use of PLS technologies. In massive MIMO systems [7] there can exist channel degrees of freedom (DoF) that are unobservable by the adversary. As an example, based on the transmitter gain pattern the signal-to-interference-plus-noise-ratio (SINR) is not necessarily higher in receivers in the proximity of the base station. The possibility of designing adaptive beamforming strategies accounting for the generation of highly secure regions of a guaranteed minimum SC arises. In parallel, millimeter wave, wireless optical systems and in general small cell networks are prominent candidates for the use of PLS techniques due to the sharp decline in signal quality outside a short range radius around the transmitter.

1.5.2 Multiple Access and Multi-user Cooperative Networks

In multiple access systems the employment of interference alignment techniques has been demonstrated to offer concrete opportunities for employment of PLS technologies, e.g. see Koyluoglu et al. [14]. Using interference alignment along with secrecy precoding, it has been proven that in a generic K user Gaussian interference channel $\frac{K-2}{2K}$ secure DoF can be achieved by each user in the ergodic setting when only the statistics of the adversarial channel are available. Furthermore, in cooperative networks with K legitimate users and E eavesdroppers the probability that the SC is below a target rate, denoted by P_{out}, has been shown to exhibit an abrupt phase transition characteristic as shown in Fig. 1.6 [5]. As a result, in large multi-user networks, the feasibility of PLS can be incorporated into the network architecture design.

1.5.3 Interference Assisted PLS Technologies

In non-degraded one-way wiretap channels the use of helping interferers (HIs) has been extensively investigated in the literature, e.g. [33]. In the generic HI framework a transmitter sends a confidential message to its intended receiver in the presence of a passive eavesdropper whose reception is jammed with the help of an independent interferer. The achievable secrecy rate and several computable outer bounds on the SC of the wiretap channel with an HI were evaluated in [33] for both discrete memoryless and Gaussian channels.

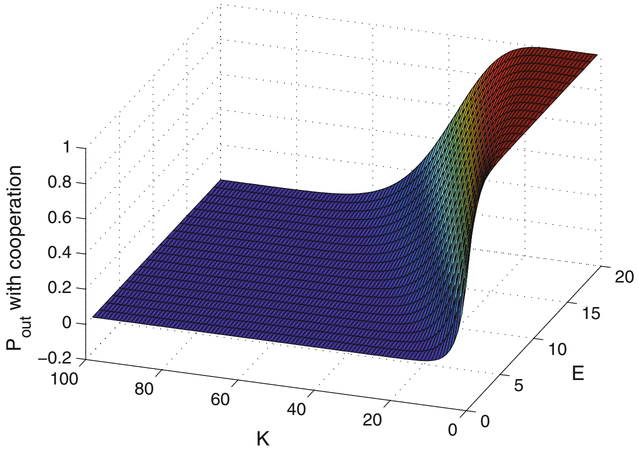


Fig. 1.6 Probability of secrecy outage for a target rate 1bps/Hz as a function of the diversity order K of Bob and E of Eve [5]

1.5.4 OFDM Systems

Orthogonal frequency division multiplexing (OFDM) is a ubiquitous signaling technique for current mobile, WiFi and other systems. Thus, in the application of PLS, consideration of OFDM systems is an important element. This problem was addressed by Renna et al. [29, 30] by considering the physical layer of an OFDM transmitter/receiver pair in the presence of an eavesdropper that might either use an OFDM structure or choose a more complex receiver architecture. The analysis was made possible by modeling the system as a particular instance of a high dimensional MIMO wiretap channel. The problem of determining the SC was formulated as a maximization problem under a trace constraint, and simple expressions were given for its high signal-to-noise (SNR) limit.

1.5.5 Backscatter Systems

Backscatter wireless communication lies at the heart of many practical low-cost, low-power, distributed passive sensing systems. The inherent cost restrictions coupled with the modest computational and storage capabilities of passive sensors, such as radio frequency identification (RFID) tags, render the adoption of classical security techniques challenging; which motivates the introduction of PLS approaches in this setting. This problem has been studied in [31], where, first, the secrecy rate of a basic single-reader, single tag RFID model was studied. Then, the unique features of the backscatter channel were exploited to maximize this secrecy rate.

1.5.6 Use of PLS Technologies Against Active Eavesdroppers

PLS techniques have been investigated for their potential use against various types of active attacks [36]. Lai et al. [15] proposed a straightforward application of PLS for authentication purposes. The use of double-binning secrecy encoders was studied with the outer bin containing a public message and the inner bin a secret key to be used for authentication purposes. Furthermore, in [4] impersonation type of attacks were considered, with the active eavesdropper using false feedback to mislead the transmitter w.r.t. the achievable secrecy rate. Interestingly it was shown that in the high SNR regime the SC of such broadcasting systems is in essence unaffected by these type of attacks.

1.6 Open Research Issues and Future Directions in PLS

During the last 15 years considerable research effort has concentrated on the area of information theoretic security. Today, the fundamental limits of secure communications over noisy channels have been established in the form of the respective capacity equivocation regions as discussed in Sect. 1.2. Furthermore, practical coding schemes that achieve the SC of certain channels have already come to light as discussed in Sect. 1.3. Despite significant results in the above-mentioned areas, a lot remains to be done before PLS technologies can be incorporated into practical engineering designs and their full potential for secure transmissions over noisy channels is achieved.

The first and foremost challenge in this direction is the design of explicit low complexity secrecy code constructions; unsurprisingly, similarly to the baseline scenario without secrecy constraints, this has proved to be a challenging task. In spite of existing results for certain specific models such as the discrete memoryless channel, much remains to be done. The most promising designs of secrecy encoders so far are based on polar codes and lattice codes; however, these schemes require large block lengths and therefore are only practical for delay unconstrained applications, e.g., e-mail exchange. Unfortunately, they cannot be employed in delay constrained applications such as multimedia streaming or in networks with computationally limited devices such as wireless sensors. Secrecy encoder designs at short and medium block-lengths is the single foremost important open issue that needs to be investigated in the PLS framework.

Furthermore, several topics related to jointly authenticated and confidential transmissions remain unchartered areas of research. The exploitation of shared randomness techniques to establish a common source of randomness that is provably inaccessible to attackers could in principle form the basis of such schemes. In the same framework, the design of cross-layer security protocols is still in its infancy. Such designs could have the potential to exploit the unique properties of PLS techniques in demanding wireless scenarios such as ad hoc and device-to-device networks in which centralized key management schemes are not attainable and computational and power resources are constrained. Furthermore, the joint employment of PLS and encryption has only been considered from the viewpoint of independently using the respective approaches at different layers of the OSI protocol; no joint consideration of crypto-PLS designs yet exists. To this end, the systematic study of PLS in the active eavesdropping setting would be necessary, extending existing active attacker threat models to account for noisy communication channels.

1.7 Conclusions

Today, despite the indisputable success of established cryptographic approaches, recent advances in communications, networking and computing technologies require a paradigm shift in information security. In fact, the decentralized, relayed, virtualized or even un-managed (device-to-device), and heterogeneous nature of modern networks (e.g., 5G) renders the generation, management, and storage of secret keys particularly challenging under current security protocols. Additionally, the recent advances in the area of quantum computing have elicited the urgency of investigating alternative approaches to information security that do not rely on assumptions regarding the computational complexity of the associated problems.

Including the physical layer of communication systems in the security design has the potential to lead to this necessary paradigm shift. Several information-theoretic results suggest that the imperfections inherently present in a communication medium (fading, thermal noise, interference) may be harnessed to conceal information from potential eavesdroppers by coding at the physical-layer itself. In essence, the noise present in the communication channel can be exploited to achieve secrecy similar to one-time-pad encryption. After more than a decade of intense research in the area of PLS the fundamental limits of secure communications over noisy channels are now better understood and practical coding schemes that achieve the promise of information-theoretic results have come to light. Thus there is sufficient momentum and underlying science for PLS techniques to be considered for incorporation into practical engineering systems.

Acknowledgments The financial support from the Academy of Finland (grants #276031, #282938, #283262) and Magnus Ehrnrooth Foundation is gratefully acknowledged. Part of this work was carried out under the European Science Foundation's COST Action IC1104. This work was also supported by the U.S. National Science Foundation Grant CMMI-1435778.

References

1. Ahlswede R, Csiszàr I (1993) Common randomness in information theory and cryptography-part I: secret sharing. IEEE Trans Inf Theory 39(4):1121–1132
2. Bassily R, Ekrem E, He X, Tekin E, Xie J, Bloch MR, Ulukus S, Yener A (2013) Cooperative security at the physical layer: a summary of recent advances. IEEE Signal Process Mag 30(5):16–28
3. Bennett CH, Brassard G, Crépeau C, Maurer UM (1995) Generalized privacy amplification. IEEE Trans Inf Theory 50(2):394–400
4. Chorti A, Perlaza SM, Han Z, Poor V (2013) On the resilience of wireless multiuser networks to passive and active eavesdroppers. IEEE J Sel Areas Commun 31(9):1850–1863
5. Chorti A, Papadaki KP, Poor HV (2015) Optimal power allocation in block fading channels with confidential messages. IEEE Trans Wirel Commun (to appear)
6. Csiszár I, Körner J (1978) Broadcast channels with confidential messages. IEEE Trans Inf Theory 24(3):339–348
7. Dean T, Goldsmith A (2013) Physical-layer cryptography through massive MIMO. arXiv:1310.1861 [cs.IT], submitted to IEEE Transactions on Information Theory
8. Ekrem E, Ulukus S (2011) The secrecy capacity of the Gaussian MIMO multi-receiver wiretap channel. IEEE Trans Inf Theory 57(4):2083–2114
9. Gopala P, Lai L, El-Gamal H (2008) On the secrecy capacity of fading channels. IEEE Trans Inf Theory 54(10):4687–4698
10. He X, Yener A (2010) Cooperation with an untrusted relay: a secrecy perspective. IEEE Trans Inf Theory 56(8):3807–3827

11. Katz J, Lindell Y (2007) Introduction to modern cryptography. CRC Press Inc., Boca Raton
12. Khisti A, Wornell GW (2010) Secure transmission with multiple antennas-part I: the MISOME wiretap channel. IEEE Trans Inf Theory 56(7):3088–3104
13. Khisti A, Wornell GW (2010) Secure transmission with multiple antennas-part II: the MIMOME wiretap channel. IEEE Trans Inf Theory 56(11):5515–5532
14. Koyluoglu O, El Gamal H, Lai L, Poor HV (2011) Interference alignment for secrecy. IEEE Trans Inf Theory 57(6):3323–3332
15. Lai L, El Gamal H, Poor HV (2009) Authentication over noisy channels. IEEE Trans Inf Theory 55(2):906–916
16. Leung-Yan-Cheong SK, Hellman ME (1978) The Gaussian wire-tap channel. IEEE Trans Inf Theory 24(4):451–456
17. Liang Y, Poor HV (2008) Multiple-access channels with confidential messages. IEEE Trans Inf Theory 54(3):976–1002
18. Liang Y, Poor HV, Shamai S (2008) Secure communication over fading channels. IEEE Trans Inf Theory 54(6):2470–2492
19. Ling C, Luzzi L, Belfiore J-C, Stehle D (2014) Semantically secure lattice codes for the Gaussian wiretap channel. IEEE Trans Inf Theory 60(10):6399–6416
20. Liu R, Liu T, Poor HV, Shamai S (2013) New results on multiple-input multiple-output broadcast channels with confidential messages. IEEE Trans Inf Theory 59(3):1346–1359
21. Mahdavifar H, Vardy A (2011) Achieving the secrecy capacity of wiretap channels using polar codes. IEEE Trans Inf Theory 57(10):6428–6442
22. Maurer UM (1993) Secret key agreement by public discussion from common information. IEEE Trans Inf Theory 39(3):733–742
23. Maurer UM, Renner R, Wolf S (2007) Unbreakable keys from random noise, Security with Noisy Data. Springer, New York, pp 21–44
24. Oggier F, Hassibi B (2011) The secrecy capacity of the MIMO wiretap channel. IEEE Trans Inf Theory 57(8):4961–4972
25. Oggier F, Solé P, Belfiore J-C (2011) Lattice codes for the wiretap Gaussian channel: construction and analysis. arXiv:1103.4086v3 [cs.IT]
26. Oohama Y (2001) Coding for relay channels with confidential messages. In: Proceedings of the information theory workshop (ITW) (Cairns, Australia), pp 87–89
27. Oohama Y (2007) Capacity theorems for relay channels with confidential messages. In: IEEE International Symposium on Information Theory—ISIT 2007 (Nice, France), pp 926–930
28. Ozarow L, Wyner A (1985) Wire-tap channel II. Advances in Cryptology, Lecture Notes in Computer Science vol. 209. Springer, New York, pp 33–50
29. Renna F, Laurenti N, Poor HV (2012) Physical layer secrecy for OFDM transmissions over fading channels. IEEE Trans Inf Forensics Secur 7(4):1354–1367
30. Renna F, Laurenti N, Tomasin S, Baldi M, Maturo N, Bianchi M, Chiaraluce F, Bloch M (2013) Low-power secret-key agreement over OFDM, CoRR abs/1302.4767
31. Saad W, Zhou X, Han Z, Poor HV (2014) On the physical layer security of backscatter wireless systems. IEEE Trans Wirel Commun 13(6):3442–3451
32. Shannon C (1949) Communication theory of secrecy systems. Bell Syst Tech J 28:656–715
33. Tang X, Liu R, Spasojevic P, Poor HV (2011) Interference assisted secret communication. IEEE Trans Inf Theory 57(5):3153–3167
34. Thangaraj A, Dihidar S, Calderbank A, McLaughlin S, Merolla J-M (2007) Applications of LDPC codes to the wiretap channel. IEEE Trans Inf Theory 53(8):2933–2945
35. Wyner AD (1975) The wire-tap channel. Bell Syst Tech J 54(8):1355–1387
36. Xiangyun Z, Maham B, Hjorungnes A (2012) Pilot contamination for active eavesdropping. IEEE Trans Wirel Commun 11(3):903–907
37. Yang S, Kobayashi M, Piantanida P, Shamai S (2013) Secrecy degrees of freedom of MIMO broadcast channels with delayed CSIT. IEEE Trans Inf Theory 59(9):5244–5256

Chapter 2
Secure Communication in Wiretap Channels with Partial and Statistical CSI at the Transmitter

Eduard Jorswieck, Pin-Hsun Lin, Sabrina Engelmann and Anne Wolf

Abstract One major challenge in physical layer security for confidential communication is the lack of channel state information at the transmitter about the channel to the passive eavesdropper. Depending on the attacker and channel assumptions, the statistical or deterministic channel uncertainty model is applied. The chapter reviews recent results for both uncertainty models and compares different signaling and pre-coding schemes and their achievable average and outage secrecy rates in fast and slow-fading wiretap channels. In addition to wiretap coding, artificial noise and non-Gaussian layered signaling are necessary to guarantee non-zero secrecy rates in scenarios where Gaussian wiretap codebooks do not work.

2.1 Introduction and Model

Information theoretic security can provide unconditional perfect secrecy on the physical layer [3, 12]. In general, the legitimate link needs some advantage over the attacker, which is a passive eavesdropper in this chapter. Thus we focus on data confidentiality. In a wireless communication setup, one major challenge for knowing and exploiting the advantage provided by the fading channel is channel uncertainty. One way to tackle the problem of channel uncertainty is to incorporate this into the information theoretic description of the channel. This leads to uncertain channel states

E. Jorswieck (✉) · P.-H. Lin · S. Engelmann · A. Wolf
TU Dresden, Communications Theory, Dresden, Germany
e-mail: Eduard.Jorswieck@tu-dresden.de

P.-H. Lin
e-mail: Pin-Hsun.Lin@tu-dresden.de

S. Engelmann
e-mail: Sabrina.Engelmann@tu-dresden.de

A. Wolf
e-mail: Anne.Wolf@tu-dresden.de

M. Baldi and S. Tomasin (eds.), *Physical and Data-Link Security Techniques for Future Communication Systems*, Lecture Notes in Electrical Engineering 358, DOI 10.1007/978-3-319-23609-4_2

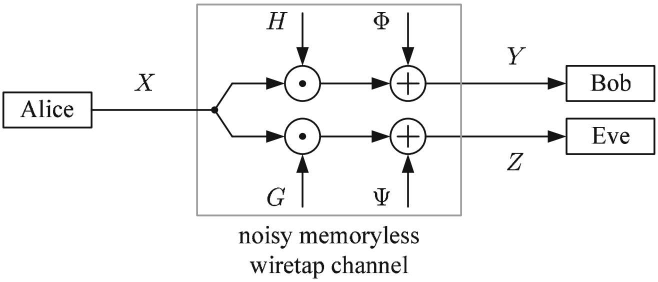


Fig. 2.1 General wiretap channel model

and thereby to the (CWC) and (AVWC) models described in [19]. In this chapter, we focus on slow and fast fading wiretap channels with deterministic and statistical (CSI) at the transmitter.

2.1.1 Signal Model

Let us consider the general wiretap channel model in Fig. 2.1. The received signal at Bob and Eve is given by

$$Y = \sqrt{H}X + \Phi, \qquad Z = \sqrt{G}X + \Psi \tag{2.1}$$

where the (AWGN) Φ and Ψ and the transmitted signal X are statistically independent at the two receivers, and we have a usual power constraint at the transmitter $E[X^2] \leq P$ with perfect CSI at the receivers. The transmit (SNR) is denoted by $\rho = \frac{P}{\sigma^2}$ with noise variance σ^2.

2.1.2 Channel Model and CSI

In general, the fading channel can be fast or slow fading [23]. In addition, the uncertainty about the channel state can be modeled deterministically by a region of uncertainty or statistically according to some error distribution. Depending on the fading channel model, the right performance metric needs to be chosen. We distinguish the following three different channel models and CSI scenarios.

1. Slow fading channel with deterministic uncertainty: The channel G to the eavesdropper stems from a set of possible realizations Γ and the legitimate link needs to be prepared for the worst (compound channel approach).
2. Slow fading channel with statistical uncertainty: The channel is quasi-static block fading and it keeps (approximately) constant during the transmission of one codeword. With statistical CSI the right performance measure is the outage probability.

3. Fast fading channel with statistical uncertainty: In fast fading, the channels change from channel use to channel use. With statistical CSI, the average rate is the right performance metric.

2.1.3 Reliability and Confidentiality Model

The wiretap channel as described above is characterized by its input alphabet $\mathscr{X}$, the output alphabets $\mathscr{Y}$, $\mathscr{Z}$ and the channel distribution $p(Y, Z|X)$. A $(2^{nR_s}, n)$-code consists of a message set $\mathscr{W}$, a stochastic encoder and a decoding function. The average decoding error probability for equi-probable messages is $P_e^{(n)} = \frac{1}{M}\sum_{w=1}^{M} \mathsf{Pr}\left(\hat{w} \neq w|x^{(n)}\text{sent}\right)$, where $x^{(n)}$ is the channel input vector with length n. A secrecy rate R_s is achievable if for any $\varepsilon_0 > 0$ there is a (M, n)-code such that $M \geq 2^{nR_s}$ and $P_e^{(n)} \leq \varepsilon_0$ and (weak secrecy criterion) [4]

$$nR_s - H(W|z^{(n)}) \leq n\varepsilon_0. \tag{2.2}$$

In the case with CSI at the transmitter, the secrecy capacity is given by

$$\max_{p(X|U)p(U)} I(U; Y|H) - I(U; Z|G) \tag{2.3}$$

with the following special result for the non-degraded Gaussian (SISO) wiretap channels with perfect CSI at the transmitter [10].

$$\max_{p(x|h,g)} [I(X; Y, H) - I(X; Z, H, G)]^+.$$

This expression is evaluated in [4] for the Gaussian SISO wiretap channel and in [9] for the Gaussian (MIMO) wiretap channel.

2.2 Statistical Uncertainty in Fast Fading

In fast-fading wiretap channels only few secrecy capacity results are known in some specific cases such as the legitimate and eavesdropper channels are (iid) with the same distribution except the variances [15, 16], for block fading [7], and for the case without CSI anywhere [17].

The order of the legitimate and the eavesdropper channel are of fundamental interest when it comes to the computation of the secrecy rate. Therefore, let us repeat the definitions of physical and stochastic degradedness.

Definition 2.1 The wiretap channel is **physically degraded** if the transition distribution function satisfies $P_{YZ|X}(y,z|x) = P_{Y|X}(y|x)P_{Z|Y}(z|y)$, i.e., if X, Y, Z form a Markov chain $X - Y - Z$.

The wiretap channel is **stochastically degraded** if its conditional marginal distributions are the same as those of a physically degraded wiretap channel, i.e., there exists $\tilde{P}_{Z|Y}$ such that $P(z|x) = \sum_Y P_{Y|X}(y|x)\tilde{P}_{Z|Y}(Z|Y)$.

Definition 2.2 Denote the set of **feasible set** as
$\mathscr{S}_{\mathscr{D}^+} = \{(H,G) :$ H and G form a degraded wiretap channel with positive secrecy capacity$\}$.

However, the fading channels H and G are usually characterized in terms of the following statistical orders [21].

Definition 2.3 For given random variables X and Y the **usual stochastic order** (st), the **convex order** (cx), the **concave order** (cv), the **increasing convex order** (icx), the **increasing concave order** (icv), and the **Laplace transform order** (Lt) are respectively defined as

$$\begin{aligned}
X \le_{st} Y \quad &\text{if} \quad \mathbb{E}[f(X)] \le \mathbb{E}[f(Y)] \quad \text{for all increasing } f \\
X \le_{cx(cv)} Y \quad &\text{if} \quad \mathbb{E}[f(X)] \le \mathbb{E}[f(Y)] \quad \text{for all convex (concave) } f \\
X \le_{icx(icv)} Y \quad &\text{if} \quad \mathbb{E}[f(X)] \le \mathbb{E}[f(Y)] \quad \text{for all increasing convex (concave) } f \\
X \le_{Lt} Y \quad &\text{if} \quad \mathbb{E}[\exp(-sX)] \le \mathbb{E}[\exp(-sY)] \quad \text{for all } s > 0. \qquad (2.4)
\end{aligned}$$

Definition 2.4 Define the following sets $\mathscr{S}_{st} = \{(H_r, H_e) : H_r \ge_{st} H_e\}$, $\mathscr{S}_{cx} = \{(H_r, H_e) : H_r \ge_{cx} H_e\}$, and $\mathscr{S}_{icx} = \{(H_r, H_e) : H_r \ge_{icx} H_e\}$.

The following results explain the relationship between the information theoretic inspired degradedness and the stochastic orders. The order relations in (2.4) operate on the (CCDF) denoted by $\bar{F}_{\cdot}(x)$ for the channel. The proofs can be found in [14].

Theorem 2.1 *Assume there is only statistical CSI of H and G at the transmitter. If the stochastic order between H and G is in the feasible set, the ergodic secrecy capacity with statistical CSI at the transmitter is*

$$C_S = \frac{1}{2}\left(\mathbb{E}_H[\log(1+\rho H)] - \mathbb{E}_G[\log(1+\rho G)]\right). \qquad (2.5)$$

The proof in [14] is based on Sato upper bound and the observation that the linear MMSE estimator of Y from Z is optimal for Gaussian input distribution. Note that similar proofs for full CSIT cases can be found in [5, 9]. The difference here is that only statistical CSIT of both channels are available.

Lemma 2.1 *If H is stochastically larger than G, then it is a degraded wiretap channel.*

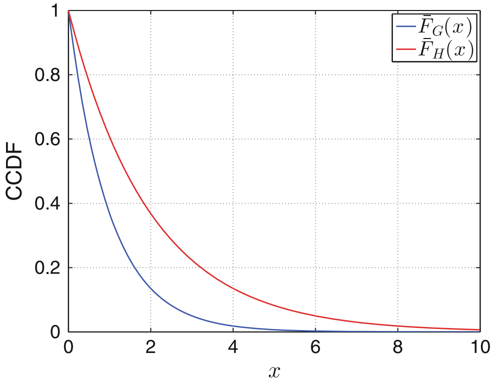


Fig. 2.2 Assume the magnitudes of the main and eavesdropper channels are two independent Rayleigh random variables with variances $\sigma_H^2 > \sigma_G^2$ with CCDF shown *right* $\bar{F}_H(x) > \bar{F}_G(x)$ and secrecy capacity in (2.5)

The idea of the proof is based on an artificial construction of a virtual joint distribution of the channel output Y and Z which has the same marginal distribution and thereby the same secrecy capacity. This virtual joint distribution is created by

$$\bar{F}_{\bar{H},\bar{G}}(h, g) = \min\{\bar{F}_H(h), \bar{F}_G(g)\}.$$

Then, it can be shown that this joint distribution leads to a degraded channel.

In Fig. 2.2, there is one example where the main channel is stochastically larger than the eavesdropper channel.

In Fig. 2.3, there is another example where the two channels, the main channel as well as the eavesdropper channel do not fulfil the stochastic order relation. Therefore, we cannot conclude that the channels are degraded and the secrecy capacity result from (2.5) may not hold.

This leads immediately to the question, whether the characterization using the stochastic order is complete in the sense that it is an equivalent condition for degradedness. The following result shows that this is not the case.

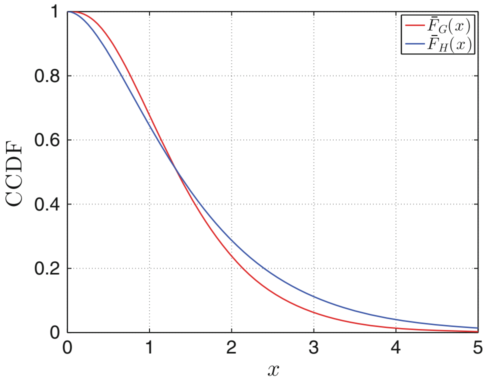


Fig. 2.3 Assume the magnitudes of the main and eavesdropper channels are two independent Nakagami-m random variables with shape parameters $(m, w) = (2, 1.25)$ for H and $(3, 2)$ for G. Then, they are not in the feasible set and the secrecy capacity is unknown

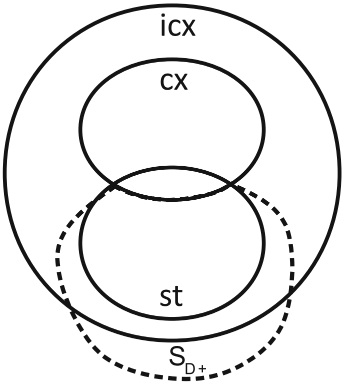


Fig. 2.4 The relation between different stochastic orders and the set of degraded channels with positive secrecy capacity which is encircled by the *dashed line*

Lemma 2.2 *The usual stochastic order $H \geq_{st} G$ is sufficient but not necessary to generate an equivalent degraded wiretap channel.*

The proof is based on a counter example of a channel pair which is not stochastically ordered but still results in a degraded channel.

Having this negative result, it seems reasonable to check the other orders for their relevance to express degradedness. The increasing convex order does not provide a clear characterization.

Lemma 2.3 *The increasing convex order is not sufficient to guarantee $(H, G) \in \mathscr{S}_{\mathscr{D}^+}$, i.e., $\mathscr{S}_{\mathscr{D}^+} \cap \mathscr{S}_{icx} \neq \emptyset$ and $\mathscr{S}_{\mathscr{D}^+} \not\supseteq \mathscr{S}_{icx}$. $(H, G) \in \mathscr{S}_{\mathscr{D}^+}$ does not necessarily imply $H \geq_{icx} G$, i.e., $\mathscr{S}_{icx} \not\supseteq \mathscr{S}_{\mathscr{D}^+}$.*

The proofs of these two results is based on another example of a quite general setup in which the CCDFs of H and G have an arbitrary number of intersection points resulting in $H \not\geq_{icx} G$ with degradedness and positive secrecy capacity.

As another order, the increasing convex order allows to express a condition for which the channels are not degraded.

Lemma 2.4 *If $(H, G) \in \mathscr{S}_{\mathscr{D}^+}$, then $H \not\geq_{cx} G$. If $H \geq_{cx} G$, then $(H, G) \notin \mathscr{S}_{\mathscr{D}^+}$. That is, $\mathscr{S}_{\mathscr{D}^+} \cap \mathscr{S}_{cx} = \emptyset$.*

The proof is based on a similar construction as for the increasing convex order above.

In Fig. 2.4, the results above are illustrated. The set corresponding to the increasing convex order contains both the set of convex and stochastic order. The intersection of the set of the convex and stochastic order are exactly those channels which are degraded and have zero secrecy capacity.[1] Furthermore the set $\mathscr{S}_{\mathscr{D}^+}$ has parts outside the set of the increasing convex order. Finally, the set corresponding to the convex order is outside the set $\mathscr{S}_{\mathscr{D}^+}$.

[1] The Venn diagram in the conference version [13] is not correct in the sense that the set of cx should not be included in $\mathscr{S}_{\mathscr{D}^+}$.

Another question regarding the non-degraded case arises: can we do better with non-Gaussian codebooks? The answer is positive and the following layered scheme is motivated by the deterministic model [1]. In the deterministic model, we assume Alice transmits q-bit and the number of bits successfully transmitted through the fading main and Eve's channels are modelled by iid random sequences N_r-bit and N_e-bit. Assume each bit is transmitted in a single layer. We also assume that there is full CSI of the main channel at Bob and both the main and Eve's channels at Eve known causally. By adapting the scheme in [24] from the broadcast channel to the wiretap case, we have the following result. Here, the CCDF for the discrete random variables are denoted by $\bar{F}_{N_\cdot}(n)$.

Theorem 2.2 *The secrecy capacity of the binary erasure wiretap channel is*

$$C_S = \sum_{n \in \mathscr{I}} \bar{F}_{N_r}(n) - \bar{F}_{N_e}(n), \tag{2.6}$$

with $\mathscr{I} = \{n | \bar{F}_{N_r}(n) > \bar{F}_{N_e}(n)\}$.

The proof has two parts: For achievability, each message in each layer is iid Bernoulli with $p = 1/2$. The auxiliary random U is set to X and only those layers with positive secrecy rates are activated. For the upper bound (converse), another virtual joint distribution with same marginals is created taking the maximum of the individual CCDFs, called *channel enhancement*. This results in a degraded channel for which the secrecy capacity is known. Fortunately, both upper and lower bounds match.

The next step is to bring the conceptual idea to the Gaussian channel setup. First, this result has two implications for the Gaussian wiretap channel. On the one hand, it leads directly to the following (genie-aided) upper bound:

Theorem 2.3 *With* $\rho = 1$, *the capacity upper bound of the fading Gaussian wiretap channel with statistical CSIT is*

$$C_S^{UB} = \frac{1}{2} \int_{H \in \mathscr{I}} [\log(1+h) f_H(h) - \log(1+h) f_G(h)] dh, \tag{2.7}$$

with $\mathscr{I} = \{h | \bar{F}_H(h) > \bar{F}_G(h)\}$.

The proof is based on the channel enhancement for which Gaussian input is known to be optimal.

On the other hand, it also leads to the following achievable scheme: The binary expansion model is given by

$$Y = \sum_{n=1}^{\infty} \sqrt{3H} X_n 2^{-n} + \Phi \tag{2.8}$$

where X_n is the n-th digit of X and Bernoulli distributed with $p = 1/2$. Thus X is uniformly distributed in $[-1, 1]$.

Theorem 2.4 *The achievable ergodic secrecy rate is* $\sum_{n\in\{k:R_k>0\}} R_n$ *where the ergodic secrecy rate of the layer n is given by*

$$R_n = \left(\mathbb{E}_H[h(X+\Phi) - h(V_n^{(h)})] - \mathbb{E}_G[h(X+\Psi) - h(V_n^{(h)})]\right)^+ \tag{2.9}$$

where $V_n^{(h)}$ *follows the (PDF)*

$$f_{V_n^{(h)}}(\nu) = \sum_{k=1}^{2^{n-1}} \left(\bar{F}_G^{(h)}(\nu - 1 + 2^{-(n-2)}k + 2^{-n}) - \bar{F}_G^{(h)}(\nu - 1 + 2^{-(n-2)}k + 3\cdot 2^{-n})\right),$$

$\bar{F}_G^{(h)}$ *is the CCDF of Gaussian distribution with zero mean and variance* $1/(3h)$.

The proof is based on a calculation of the mutual information expressions for the main and the eavesdropper channel for each layer exploiting the properties of the binary expansion model in (2.8).

The are several observations from Theorem 2.4: It seems from the expression of the rate of layer n that we can also select the layer which contribute with positive secrecy rates like in the case with perfect CSIT. This is not true since the transmitter does not know the exact channel realization for the statistical CSIT setup. Furthermore, there are cases in which Gaussian signalling outperform the achievable rate in Theorem 2.4. The reason is that the layered scheme has a uniform input distribution and does suffer from a shaping loss.

Note that the discrete signalling, e.g., (QAM) used in [11] is a special case of the proposed layered scheme in the complex field. For example if we set $n = 2$ then we obtain 4-PAM as $\mathscr{X} = \{-3/4, -1/4, 1/4, 3/4\}$. This scheme suggests a simple parallel encoding and modulation of the layers.

In Table 2.1, we report several examples of different Nakagami-*m* fading channels with parameters (m, w) and the achievable secrecy rates with Gaussian signalling as the state of the art. For simplicity, the considered number of layers in the proposed scheme is up to 3. Therefore, the numerically computed achievable secrecy rates are a lower bound of the proposed ergodic secrecy rates.

The results in Table 2.1 show that under Nakagami-*m* channels, the proposed achievable scheme inspired by layered signalling outperforms Gaussian signalling in several cases. In some cases (second row), it can improve the connectivity of confidential data transmission.

2.3 Statistical Uncertainty in Slow Fading

In the slow-fading scenario, we consider a MISO link between the legitimate as well as between transmitter and eavesdropper nodes. The signal model from (2.1) is refined accordingly

$$Y = h^H wX + \Phi \qquad \text{and} \qquad Z = g^H wX + \Psi, \tag{2.10}$$

with MISO channel vectors h and g and beamforming vector w. The instantaneous achievable secrecy rate is given by

$$R_S = \left[\log\left(1 + \rho|h^H w|^2\right) - \log\left(1 + \rho|g^H w|^2\right)\right]^+ \tag{2.11}$$

with optimal beamforming vector under perfect CSI given by the generalized eigenvector which belongs to the generalized maximum eigenvalue $\nu_{\max}(I + \rho hh^H, I + \rho gg^H)$ [20]. If only statistical CSI is available at the transmitter, outages will occur depending on the realization of the random fading channels. We model the CSI at the transmitter by $g = \sqrt{\kappa}d + \sqrt{1-\kappa}\tilde{g}$ where d is the known or estimated component of the channel and $\tilde{g}$ is unknown and random according to an iid Gaussian distribution. By κ the quality of the CSI is modeled.

In literature three outage events are distinguished: the overall secrecy outage event [2] $E_1 = \{R_S < R_S^{\varepsilon}\}$, the union of secrecy outage events [8] $E_2 = \{\log_2(1 + \rho|h^H w|^2) < R_S^{\varepsilon})\} \cup \{1/nH(W|Z) < R_S^{\varepsilon} - \epsilon_0\}$ or the two secrecy outage events [26] $E_3 = \{\log_2(1 + \rho|g^H w|^2) > R_T - R_S^{\varepsilon}\}$ and $E_4 = \{\log_2(1 + \rho|h^H w|^2) < R_T\}$. Within this chapter, we use the overall secrecy outage event E_1.

Since the transmitter does not know the channel to the eavesdropper perfectly, it might be useful to apply (AN) to the transmit strategy [18]. The programming problem without (AN) is formulated as follows:

$$\min_{\|w\|^2 \le 1} \Pr\left(\log_2 \frac{1 + \rho|h^H w|^2}{1 + \rho|g^H w|^2} < R_S^{\varepsilon}\right), \tag{2.12}$$

The programming problem with AN in the null-space of the main channel reads:

$$\min_{\|w\|^2 \le \varphi, \mathrm{tr} WW^H = (1-\varphi), h^H W = 0} \Pr\left(\log_2 \frac{1 + \rho|h^H w|^2}{1 + \frac{\rho|g^H w|^2}{1 + \rho\|g^H W\|^2}} < R_S^{\varepsilon}\right). \tag{2.13}$$

Table 2.1 Comparison of ergodic secrecy rates between Gaussian and layered signalling for different fading channel distributions

(m, w) of H	(m, w) of G	Gaussian rate[a]	Layered[a]
(10, 1)	(1, 1.2)	0.0057	0.0318
(10, 1)	(1, 1.4)	0	0.0131
(1, 1)	(0.2, 1)	0.1247	0.1292

[a] in bits per channel use

The solution to (2.12) requires the following special beamforming vectors $w_{MRT} = h/\|h\|$, $w_{ZF} = \prod_d^\perp h/\| \prod_d^\perp h\|$ and $w_{ZF}^\perp = \prod_d h/\| \prod_d h\||$. The proof of the results can be found in [6].

Theorem 2.5 *Let* $\tau \in [0, 1]$. *Then the optimal beamforming vector* w *solving (2.12) is given by* $w(\tau) = \sqrt{\tau} w_{ZF}^\perp + \sqrt{1-\tau} w_{ZF}$. *The secrecy outage probability* ε *can be expressed with the Marcum Q-function of the first order* Q_1 *as*

$$\varepsilon = Q_1 \left(\sqrt{\frac{2\kappa\tau}{1-\kappa}} \|d\|, \sqrt{\frac{2 - 2^{R_S^\varepsilon + 1} + 2\rho |h^H w(\tau)|^2}{2^{R_S^\varepsilon} \rho (1-\kappa)}} \right). \tag{2.14}$$

The proof of this result relies on the intuition that Alice has basically only two goals: at first, to maximize the received signal power at Bob to have better reliability. Second, to minimize the received signal power at Eve to have better confidentiality. The first goal corresponds to the direction of the known component h. The second goal corresponds to the direction of the known component for the statistical channel g. It can be shown that a linear combination of both directions is sufficient.

The solution from Theorem 2.5 is illustrated in Fig. 2.5. It can be observed that the quality of the CSI has a large impact on the achievable outage probability.

The optimal transmit strategy for the case with AN is parametrized by three parameters, the beamforming weight τ, the power splitting parameter φ and the power weight to the known channel and the null space component ξ.

Theorem 2.6 *The optimal solution to (2.13) is given by the parameters* $\tau \in [0, 1]$, $\varphi \in [0, 1]$ *and* $\xi \in [0, 1]$ *with achievable instantaneous secrecy rates*

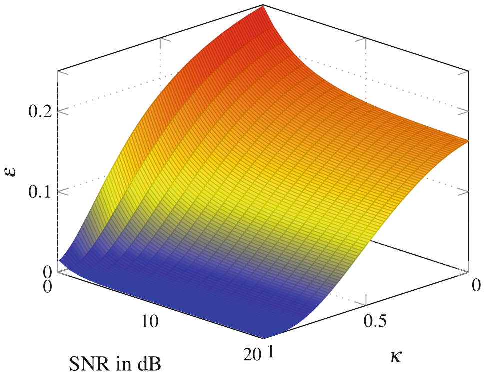


Fig. 2.5 Secrecy outage probability ε for MISO with 4 transmit antennas, uncertainty model with fixed angle of 65° between h and d, which is given by $\arccos \frac{|h^d|}{\|h\|\|d\|}$ for a fixed target secrecy rate $R_S^\varepsilon = 0.8$ bits per channel use

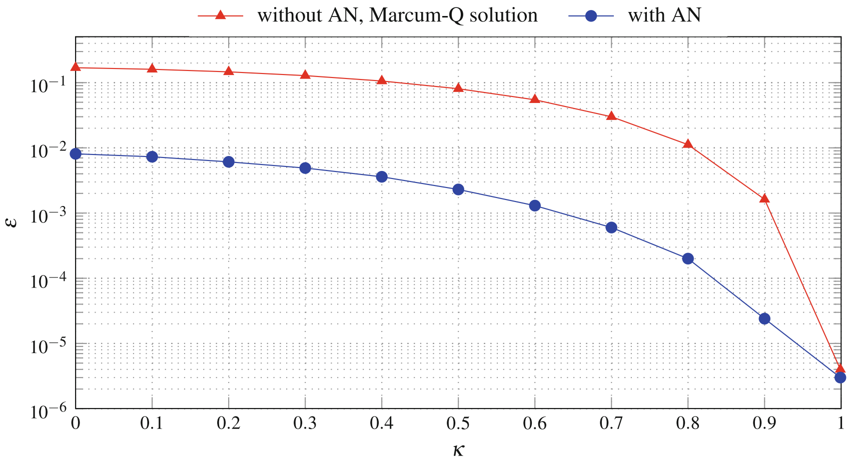


Fig. 2.6 Secrecy outage probability ε, derived by Theorem 2.6 for target secrecy rate $R_S^\varepsilon = 0.8$ bits per channel use and SNR of 10 dB for the same angle of 65° as in Fig. 2.5

$$R_S = \Bigg[\log_2(1 + \rho\varphi|h^H w(\tau)|^2) - \log_2 \left(1 + \frac{\rho\varphi|g^H w(\tau)|^2}{1 + \rho(1-\varphi)\left(\xi |g^H \frac{\prod_h^\perp d}{\|\prod_h^\perp d\|}|^2 + \frac{1-\xi}{n_T-2} \sum_{k=1}^{n_T-2} |g^H u_k|^2 \right)} \right) \Bigg]^+ \tag{2.15}$$

with u_k spanning an orthonormal basis to the span of h and d.

The proof of this result has two main parts. In the first part, it is shown that the same linear combination of directions as for the case without AN is optimal here, too. In the second part, it is shown that it is optimal to distribute the remaining power for the AN component in the null space of the two known channels h and d.

The solution in Theorem 2.6 and the gain by using AN is illustrated in Fig. 2.6.

The results for the statistical uncertainty of the eavesdropper channel show that in slow fading channels, the secrecy outage probability can be significantly minimized by using AN. Furthermore, by smart beamforming, depending on the quality of the CSI, the secrecy outage probability can be further reduced.

2.4 Deterministic Uncertainty

For the deterministic uncertainty scenario, we consider a MIMO link between all three nodes. The signal model is modified accordingly and channels H and G are matrices. For simplicity, we assume that all nodes have the same number of antennas n. To model the lack of CSI at the transmitter about the channel G, we assume that it is only known that G belongs to some uncertainty set, i.e.,

$$G \in \mathscr{G} = \{G \in \mathbb{C}^{n,n} \,|\, \mathrm{tr}(G^H G) \leq g\}. \tag{2.16}$$

The constraint in (2.16) corresponds to the sum channel gain from the transmitter to the eavesdropper. If the legitimate nodes know the minimum distance of the attacker to the transmitter, they can compute a corresponding suitable g. The transmit covariance matrix Q is power constrained by the set $\mathscr{Q} = \{Q \succeq 0 \,|\, \mathrm{tr}(Q) \leq P\}$.

The resulting achievable secrecy rate under worst case G is given by

$$R_S^+ = \max_{Q \in \mathscr{Q}} \min_{G \in \mathscr{G}} \Big[\log\det(I + \rho Q H^H H) - \log\det(I + \rho Q G^H G)\Big]^+. \tag{2.17}$$

Fortunately, the following characterization of the max-min solution to (2.17) simplifies the problem [25]. The eigenvalues of $H^H H$ and $G^H G$ are denoted by $\alpha_1, \dots, \alpha_n$ and $\beta_1, \dots, \beta_n$, respectively. The eigenvalues of the transmit covariance matrix Q are identified by $\lambda_1, \dots, \lambda_n$.

Theorem 2.7 *The following vector programming problem is equivalent to problem (2.17), i.e., the optimal eigenvectors of Q and $G^H G$ diagonalize $H^H H$:*

$$\max_{\lambda \in \mathscr{L}} \min_{\beta \in \mathscr{B}} \left[\sum_{k=1}^{n} \log_2(1 + \rho\lambda_k\alpha_k) - \log_2(1 + \rho\lambda_k\beta_k)\right]^+ \tag{2.18}$$

with $\mathscr{L} = \{\lambda \in \mathbb{R}^n \,|\, \lambda_1, \dots, \lambda_n \geq 0$ and $\sum_{k=1}^n \lambda_k \leq P\}$ and $\mathscr{B} = \{\beta \in \mathbb{R}^n \,|\, \beta_1, \dots, \beta_n \geq 0$ and $\sum_{k=1}^n \beta_k \leq g\}$. This problem can be further reformulated into

$$\max_{\lambda \in \mathscr{L}} \min_{\beta \in \mathscr{B}} \sum_{k=1}^{n} [\log_2(1 + \rho\lambda_k\alpha_k) - \log_2(1 + \rho\lambda_k\beta_k)]^+. \tag{2.19}$$

This characterization is obtained if the structure of the vector problem above is exploited by using a set of n parallel encoders instead of a joint encoder, which allows an individual encoding of the information for the resulting n parallel channels.

Furthermore, the optimal solution to the minimization problem in (2.19) with respect to β for fixed λ is given by

$$\beta_k^* = \left[\frac{1}{\mu} - \frac{1}{\rho\lambda_k}\right]_0^{\alpha_k}, \tag{2.20}$$

with $\mu > 0$ *such that* $\sum_{k=1}^{n} \beta_k = g$.

The proof of the theorem comprises two parts, which correspond to the derivation of the optimal transmit directions of $G^H G$ and Q for a given channel matrix H using Hadamard's inequality, which provides a bound on the determinant of a positive (semi-)definite matrix.

Note that $\mathscr{L}$ and $\mathscr{B}$ are compact convex sets. Furthermore, the objective function in (2.19) is continuous and (quasi-)concave on $\mathscr{L}$ for all $\beta \in \mathscr{B}$ and also continuous and (quasi-)convex on $\mathscr{B}$ for all $\lambda \in \mathscr{L}$. By the minimax theorem in [22], the saddle-point property holds and min and max can be swapped in (2.19).

Since there is no closed-form solution for the outer maximization problem, upper and lower bounds on the secrecy rate expressions are derived by taking a proper super- and sub-set of the set $\mathscr{B}$.

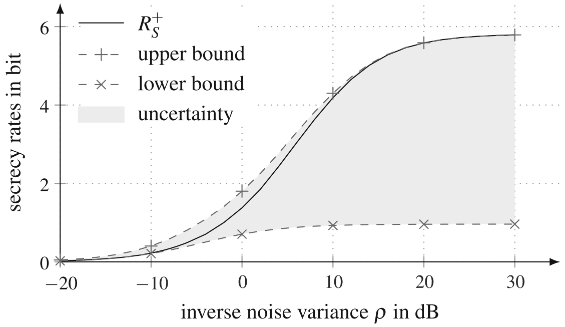


Fig. 2.7 Worst-case secrecy rates with upper and lower bounds for four antennas at all nodes, $P = 1$, $g = 2$ and channel realization $\alpha = [3.9, 1.5, 1.0, 0.6]$

In Fig. 2.7, the numerically optimized worst-case secrecy rate is shown together with some lower and upper bounds for which a closed form solution exist. It can be observed that the secrecy rate saturates for high SNR because the unknown negative term in (2.19) will not vanish. Furthermore, there is a large gap between lower and upper bound which increases with SNR. As future research, we envision to tighten these bounds. However, even without perfect CSI of the eavesdropper link, a certain secrecy rate can be achieved.

2.5 Conclusions

Uncertainty is one major challenge in physical layer security for confidential communication. Based on channel and CSI models, we have developed different coding/precoding schemes and have derived achievable secrecy expressions.

The important conclusion for confidential wireless system design is to carefully model the channel statistics (e.g. fast or slow fading) as well as the available CSI at the legitimate transmitter about the eavesdropper link. Based on these models, the correct objective function and constraints are derived.

In general, it holds that the more CSI, and the better the adaptivity and flexibility at the legitimate transmitter, the higher the achievable secrecy rates.

We have excluded multi-user networks with confidential messages, helper or friendly jamming nodes, public feedback, practical code design and many other issues. Some of these scenarios are partially addressed in the literature and some still contain open research problems.

References

1. Avestimehr A, Diggavi S, Tse D (2011) Wireless network information flow: a deterministic approach. IEEE Trans Inf Theory 57(4):1872–1905. doi:10.1109/TIT.2011.2110110
2. Barros J, Rodrigues M (2006) Secrecy capacity of wireless channels. In: IEEE International symposium on information theory, pp 356–360. doi:10.1109/ISIT.2006.261613
3. Bloch M, Barros J (2011) Physical-layer security: from information theory to security engineering. Cambridge University Press, Cambridge
4. Csiszár I, Körner J (1978) Broadcast channels with confidential messages. IEEE Trans Inf Theory 24:339–348
5. Ekrem E, Ulukus S (2009) Ergodic secrecy capacity region of the fading broadcast channel. In: IEEE international conference on communications. ICC '09, pp 1–5. doi:10.1109/ICC.2009.5199000
6. Gerbracht S, Scheunert C, Jorswieck E (2012) Secrecy outage in MISO systems wih partial channel information. IEEE Trans Inf Forensics Secur 7(2):704–716
7. Gopala PK, Lai L, Gamal HE (2008) On the secrecy capacity of fading channels. IEEE Trans Inf Theory 54(10):4687–4698. doi:10.1109/TIT.2008.928990
8. Gungor O, Tan J, Koksal C, El-Gamal H, Shroff N (2013) Secrecy outage capacity of fading channels. IEEE Trans Inf Theory 59(9):5379–5397. doi:10.1109/TIT.2013.2265691
9. Khisti A, Wornell GW (2010) Secure transmission with multiple antennas—part II: the mimome wiretap channel. IEEE Trans Inf Theory 56(11):5515–5532. doi:10.1109/TIT.2010.2068852
10. Leung-Yan-Cheong S, Hellman M (1978) The Gaussian wire-tap channel. IEEE Trans Inf Theory 24(4):451–456. doi:10.1109/TIT.1978.1055917
11. Li Z, Yates R, Trappe W (2010) Achieving secret communication for fast Rayleigh fading channels. IEEE Trans Wirel Commun 9(9):2792–2799. doi:10.1109/TWC.2010.080210.090948
12. Poor HV, Shamai (Shitz) S (2009) Information theoretic security. Found Trends Commun Inf Theory 5(4–5):355–580
13. Lin PH, Jorswieck E (2014) On the fading gaussian wiretap channel with statistical channel state information at transmitter. In: 2014 IEEE conference on communications and network security (CNS), pp 121–126. doi:10.1109/CNS.2014.6997476
14. Lin PH, Jorswieck EA (subm. Dec. 2014) On the fast fading Gaussian wiretap channel with statistical channel state information at transmitter. IEEE Trans Inf Forensics Secur
15. Lin S, Lin CL (2014) On secrecy capacity of fast fading MIMOME wiretap channels with statistical CSIT. IEEE Trans Wirel Commun 13(6):3293–3306. doi:10.1109/TWC.2014.041714.11654
16. Lin SC, Lin PH (2013) On secrecy capacity of fast fading multiple-input wiretap channels with statistical CSIT. IEEE Trans Inf Forensics Secur 8(2):414–419. doi:10.1109/TIFS.2012.2233735

17. Mukherjee P, Ulukus S (2013) Fading wiretap channel with no csi anywhere. In: 2013 IEEE international symposium on information theory proceedings (ISIT), pp 1347–1351. doi:10.1109/ISIT.2013.6620446
18. Negi R, Goel S (2005) Secret communication using artificial noise. In: Proceedings of the IEEE vehicular technology conference (VTC), vol 3, pp 1906–1910. doi:10.1109/VETECF.2005.1558439
19. Schaefer RF, Boche H, Poor HV (2015) Secure communication under channel uncertainty and adversial attacks. In: Proceedings of IEEE submitted
20. Shafiee S, Ulukus S (2007) Achievable rates in Gaussian MISO channels with secrecy constraints. In: IEEE international symposium on information theory, ISIT 2007, pp 2466–2470. doi:10.1109/ISIT.2007.4557589
21. Shaked M, Shanthikumar JG (2007) Stochastic orders. Springer, Berlin
22. Sion M (1958) On general minimax theorems. Pac J Math 8(1):171–176
23. Tse D, Viswanath P (2005) Fundamentals of wireless communication. Cambridge University Press
24. Tse D, Yates R (2012) Fading broadcast channels with state information at the receivers. IEEE Trans Inf Theory 58(6):3453–3471. doi:10.1109/TIT.2012.2191471
25. Wolf A, Jorswieck EA (2010) Maximization of worst-case secrecy rates in MIMO wiretap channels. In: Proceedings of asilomar conference on signals, systems and computers
26. Yuksel M, Erkip E (2011) Diversity-multiplexing tradeoff for the multiple-antenna wire-tap channel. IEEE Trans Wirel Commun 10(3):762–771. doi:10.1109/TWC.2011.010411.090943

Chapter 3
MIMOME Gaussian Channels with GMM Signals in High-SNR Regime: Fundamental Limits and Tradeoffs

Francesco Renna, Nicola Laurenti and Stefano Tomasin

Abstract Achievable secrecy rates over a multiple-input multiple-output multiple-eavesdropper (MIMOME) wiretap channel are considered, when the legitimate users have perfect knowledge only of the legitimate channel state and the eavesdropper channel is drawn from a (possibly unknown) continuous probability density. Legitimate users are assumed to deploy more antennas than the eavesdropper. A signaling transmission based on K-class Gaussian mixture model (GMM) distributions is proposed, which can be considered as an artificial-noise augmented signal, where the noise statistics are data-dependent. The proposed scheme is shown to achieve the secrecy capacity, $\log K$, in the high signal-to-noise ratio (SNR) regime. Moreover, the tradeoff between secrecy and reliability at finite SNR is explored via the characterization of an upper bound to the error probability at the legitimate receiver, an upper bound to the mutual information leakage to the eavesdropper and via numerical simulations.

3.1 Introduction

Wireless channels are inherently susceptible to eavesdropping due to their broadcast nature. In response to such issues, the application of information theoretic secrecy principles to widely used communication systems has represented a rising research topic, in an effort to extend security to the lowest layers. Seminal works from the 70s have established the secrecy capacity of a wiretap channel, that is the maximum rate

F. Renna (✉)
University College London, London, UK
e-mail: f.renna@ucl.ac.uk

N. Laurenti · S. Tomasin
University of Padua, Padua, Italy
e-mail: nil@dei.unipd.it

S. Tomasin
e-mail: tomasin@dei.unipd.it

M. Baldi and S. Tomasin (eds.), *Physical and Data-Link Security Techniques for Future Communication Systems*, Lecture Notes in Electrical Engineering 358, DOI 10.1007/978-3-319-23609-4_3

at which agent Alice can transmit a secret message to agent Bob while not revealing any information to an eavesdropper agent Eve. Their focus was centered first on the analysis of discrete memoryless and Gaussian channels [12, 22]. Since then, a number of different scenarios have been investigated, including the broadcast channel with confidential messages (BCC) case where multiple receivers require a common message and possibly a different secret message each [3], the case of secret message transmission over parallel channels [1, 13], fading channels [20] and the multiple-input multiple-output multiple-eavesdropper (MIMOME) case [10, 15, 19], even particularized to OFDM transmission [18]. In this chapter we focus on the MIMOME channel which finds many important applications in wireless communication systems where the transmitter and the receivers are equipped with multiple antennas.

In particular, we consider the case in which both Alice and Bob have perfect knowledge of the channel state information (CSI) of their legitimate channel, whereas they do not know the channel to Eve, which is assumed to be drawn from a continuous probability density. A similar scenario was considered in [8], where the eavesdropper channel is not known to the legitimate terminals, even statistically and Alice and Bob were assumed to deploy more antennas than Eve. The same framework was generalized in [7] to the BCC case with an adversarial eavesdropper whose channel is unknown to the other three terminals. In both works, achievable secrecy rates were obtained by using wiretap coding schemes. However, explicit coding constructions to achieve such rates were not provided. In [4] the uncertainty in the CSI of both channels by Alice and Bob is modeled by bounding channel estimate errors inside a given ellipsoid, and the worst-case secrecy rate under such constraints is derived in the low-SNR regime.

We present an explicit construction of wiretap codebooks and we evaluate the corresponding achievable secrecy rates. In particular, we consider the scenario in which the transmitted symbols are randomly generated from a continuous set, the secret message determining only the statistics of the random symbol through a map that is known to all agents. A similar approach has been proposed in [17], where a multiplicative Gaussian wiretap channel is considered. In that case the transmitted codeword is obtained by multiplying a binary message vector with entries in $\{0, 1\}$ by a diagonal random matrix with independent zero-mean unit-variance Gaussian entries. The message vector is assumed to be sparse (i.e., with many zeros). Assuming that Eve has fewer observations than Bob through a known and fixed channel matrix, it is shown that secret transmission is possible and lower and upper bounds to the secrecy capacity are derived, when Alice has knowledge of both channels. With a similar precoding technique, [14] guarantees perfect secrecy by assuming complete ignorance by Eve about the state of the legitimate channel.

In this chapter, differently from [17], we do not restrict the transmitted message to be taken from a binary sparse distribution but we allow denser discrete signaling. As a result, the transmitted signal is a Gaussian mixture model (GMM) multivariate vector. The considered scheme can be thought also as a generalization of an artificial-noise transmission scheme, where noise statistics are data-dependent. We carry out our analysis in the finite-dimension regime, that is, we assume the number of antennas at Alice, Bob and Eve to be finite. Moreover, we assume that the antennas at both Alice and Bob outnumber those at Eve, and leverage such advantage to provide secrecy for the legitimate terminals. We then focus on the low-noise (or equivalently, high-SNR) regime, characterizing the achievable rate of this scheme in the absence of noise, where secrecy is provided by the different channels between the agents. We tailor the statistics of the message vector to maximize the secrecy rate. The main results provided in this chapter are the following:

1. we devise a system for information-theoretic secrecy at the physical layer where the transmitted signal is generated from one of K different Gaussian distributions with indices $\{1, \ldots, K\}$ and the informative message is the chosen distribution index;
2. we prove that in the high-SNR limit, the maximum secrecy rate that can be achieved by such a system equals the unconstrained capacity, $\log K$, even when Alice only has statistical knowledge of the channel to Eve;
3. we provide a constructive way to design GMM inputs that achieve the maximum secrecy rate in the high-SNR limit;
4. for finite SNR values, we characterize the trade-off between reliable decoding at the legitimate receiver and mutual information leakage to the eavesdropper.

Throughout this chapter, vectors (respectively, matrices), both deterministic and random, are denoted by boldface lowercase (respectively, uppercase) Latin or Greek letters, while log denotes the base 2 logarithm. The symbols $\det(\cdot)$ and $\mathrm{pdet}(\cdot)$ denote the determinant and the pseudo-determinant, respectively, of a square matrix. $\mathbb{P}[A]$ represents the probability of the event A, whereas $\mathbb{E}[\cdot]$ denotes the expectation operator and $\mathbb{I}(\cdot;\cdot)$ is the mutual information between two random variables. We also use the symbol $[x]^+ = \max\{x, 0\}$. $\mathrm{null}(\boldsymbol{A})$ and $\mathrm{rank}(\boldsymbol{A})$ denote the null space and rank of $\boldsymbol{A}$, respectively. $\mathscr{R}(\boldsymbol{A})$ denotes the linear space generated by the columns of $\boldsymbol{A}$.

3.2 System Model

We consider a wireless MIMOME transmission scenario, as depicted in Fig. 3.1, in which agent Alice (A) aims at transmitting to agent Bob (B) a secret message u which must be kept secret to a third agent Eve (E). Alice is equipped with m_a antennas, while Bob and Eve have m_b and m_e antennas respectively, with $m_e < m_b < m_a$. Between each couple of antennas an AWGN flat static channel is available, whose gain does not change for the duration of the entire transmission. At time t, Alice transmits a column vector $\boldsymbol{x}$ of m_a real symbols on her antennas.[1] The MIMOME channel is modeled by matrices $\boldsymbol{H} \in \mathbb{R}^{m_b \times m_a}$ and $\boldsymbol{G} \in \mathbb{R}^{m_e \times m_a}$, the signal vectors

[1] Extension to complex-valued transmission is left for future study.

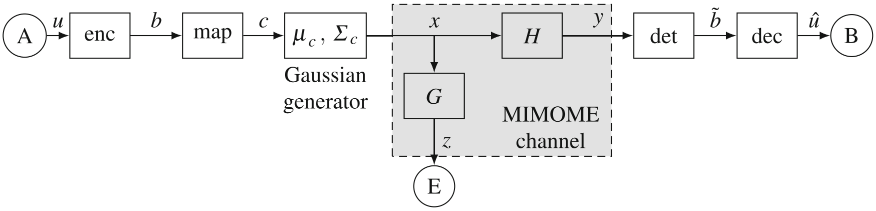


Fig. 3.1 System model. The confidential message u is encoded into the information bearing index c

received by Bob and Eve have dimension m_b and m_e, respectively, and they can be written as

$$\begin{aligned} \boldsymbol{y} &= \boldsymbol{Hx} + \boldsymbol{w}_b \\ \boldsymbol{z} &= \boldsymbol{Gx} + \boldsymbol{w}_e, \end{aligned} \tag{3.1}$$

where $\boldsymbol{w}_b, \boldsymbol{w}_e \sim \mathcal{N}(\boldsymbol{0}, \boldsymbol{I}\sigma^2)$ represent AWGN noise. We assume that Alice and Bob know $\boldsymbol{H}$, whereas they do not know $\boldsymbol{G}$, which is assumed to be drawn from a continuous probabilty density function (pdf), which is also unknown to the legitimate users. On the contrary, Eve is assumed to have perfect knowledge of both channel matrices.

We consider an average power constraint on the transmitted signal, i.e.,

$$\mathbb{E}[\boldsymbol{x}^T\boldsymbol{x}] \leq P. \tag{3.2}$$

3.2.1 Transmission Technique

We assume that Alice and Bob agree before transmission on a set of K column vectors of size m_a, $\boldsymbol{\mu}_k, k = 1, \ldots, K$, and K $m_a \times m_a$ positive semidefinite matrices $\boldsymbol{\Sigma}_k, k = 1, \ldots, K$. These vectors and matrices are assumed to be also known to Eve. At each transmission Alice encodes by an error correcting code the message u of B_u bits into the bit sequence b of B_b bits (block enc in Fig. 3.1). The code rate of the error correcting code is therefore B_u/B_b. Then a mapper follows, which maps $\log K$ bits into the symbol $c \in \{1, \ldots, K\}$ (block map in Fig. 3.1). However, c is not directly transmitted on the channel, as in a regular non-secure transmission scheme. In fact, in order to provide secrecy we consider a *non deterministic* modulator, where in order to transmit symbol c, the corresponding transmitted vector $\boldsymbol{x}$ is randomly taken from the multivariate normal distribution $\mathcal{N}(\boldsymbol{\mu}_c, \boldsymbol{\Sigma}_c)$ (block Gaussian generator in Fig. 3.1), whose mean and variance are uniquely determined by c. The randomness employed by the modulation will be leveraged to prevent Eve from decoding the secret message. In other words, the message will determine the mean and covariance of the random Gaussian vector that will be transmitted on the channel.

In particular, let p_k be the probability that message $k = 1, \ldots, K$ is transmitted. Then the input signal $\boldsymbol{x} \in \mathbb{R}^{m_a}$ has a GMM distribution with pdf

$$f_{\boldsymbol{x}}(\boldsymbol{a}) = \sum_{k=1}^{K} p_k \nu(\boldsymbol{a}; \boldsymbol{\mu}_k, \boldsymbol{\Sigma}_k), \tag{3.3}$$

where

$$\nu(\boldsymbol{a}; \boldsymbol{\mu}_k, \boldsymbol{\Sigma}_k) = \frac{\exp\left(-\frac{1}{2}(\boldsymbol{a} - \boldsymbol{\mu}_k)^T \boldsymbol{\Sigma}_k^{-1} (\boldsymbol{a} - \boldsymbol{\mu}_k)\right)}{\sqrt{(2\pi)^n \det \boldsymbol{\Sigma}_k}} \tag{3.4}$$

is the pdf of a multivariate normal distribution. In other terms, the input signals are drawn with probability p_k from the Gaussian distribution $\mathcal{N}(\boldsymbol{\mu}_k, \boldsymbol{\Sigma}_k)$.

Also, the power constraint can be rewritten now as

$$\mathbb{E}[\boldsymbol{x}^T \boldsymbol{x}] = \sum_{k=1}^{K} p_k \operatorname{tr}(\boldsymbol{\Sigma}_k + \boldsymbol{\mu}_k \boldsymbol{\mu}_k^T) \leq P. \tag{3.5}$$

Note that when $\boldsymbol{\Sigma}_c = \boldsymbol{\Sigma}$ for $c = 1, \ldots, K$, i.e., all symbols have the same correlation matrix, we obtain an artificial noise transmission system, where the information is conveyed by vectors $\boldsymbol{\mu}_c$, $c = 1, \ldots, K$, and the Gaussian component of the transmitted signal is the artificial noise. Instead, when $\boldsymbol{\Sigma}_c$ are different for each c, we obtain a system where the artificial noise is data-dependent, therefore also the correlation actually carries information on the data. The performance of this non-trivial generalization of the artificial noise system is here investigated.

3.2.2 Receiver Architecture

The receiver aims at reconstructing the data bit sequence from the received vector signal $\boldsymbol{y}$. This is achieved by a detection block that classifies the received signal in order to obtain the probability that symbol c was used to generate the transmitted Gaussian vector (block det in Fig. 3.1). Then a (soft) version $\tilde{b}$ of the bits b is passed to the error correction decoder to obtain $\hat{u}$ (block dec in Fig. 3.1). The description of this receiver is out of the scope of this chapter, where we aim at characterizing the performance of the systems in terms of maximum achievable rates in the high SNR regime. As a relevant example, consider the case in which the covariance matrices of the received (noise-free) symbols $\boldsymbol{H}\boldsymbol{\Sigma}_c\boldsymbol{H}^T$ have all distinct null spaces. Then, in the absence of noise, Bob can take a decision on the transmitted symbol by projecting $\boldsymbol{y}$ into all possible K null spaces of $\boldsymbol{H}\boldsymbol{\Sigma}_c\boldsymbol{H}^T$, with $c = 1, 2, \ldots, K$ and choose the value c^* for which the projection gives the projected mean value $\boldsymbol{N}_c\boldsymbol{\mu}_c$, where the rows of $\boldsymbol{N}_c$ form an orthogonal basis of $\operatorname{null}(\boldsymbol{H}\boldsymbol{\Sigma}_c\boldsymbol{H}^T)$.

3.3 Achievable Rate in the Low-Noise Regime

In this section, we characterize the secrecy rates that are achievable in the MIMOME scenario described in Sect. 3.2. We consider the secrecy rate R_s achieved in the low-noise regime, i.e., in the limit $\sigma^2 \to 0$. We will also describe explicitly how to design input sources that achieve the maximum of the achievable secrecy rates in the low-noise regime, i.e., the low-noise secrecy capacity.

In the following we show that the achievable rate in the low-noise regime is $\log K$ bit/symbol. This result will be provided by Theorem 3.1 that will show that there exist correlation matrices $\boldsymbol{\Sigma}_c$ and means $\boldsymbol{\mu}_c$ that at the same time provides an asymptotic zero error probability for Bob, while leaking no information on c to Eve. Before showing this result we consider the following lemma, that outlines a construction of input covariance matrices that will be used to prove the achievability of secrecy capacity.

Lemma 3.1 *Let* $\boldsymbol{H} \in \mathbb{R}^{m_b \times m_a}$ *be given such that* $\operatorname{rank}(\boldsymbol{H}) = m_b < m_a$ *and let* $s < m_b$*. Let* $\boldsymbol{U} \in \mathbb{R}^{m_a \times m_b}$ *a matrix whose columns form an orthonormal basis for* $\operatorname{null}(\boldsymbol{H})^\perp$*. Let*

- *define* $\boldsymbol{W}_\epsilon \in \mathbb{R}^{m_b \times m_b}$ *a matrix such that all bottom left minors of* $\boldsymbol{W}_\epsilon^k$ *are non-zero for* $k = 1, \dots, K$ *and for a sequence of* ϵ *converging to zero, and such that* $\lim_{\epsilon \to 0} \boldsymbol{W}_\epsilon = \boldsymbol{I}$*,*
- $\boldsymbol{I}_{m_b \times s}$ *is the matrix consisting in the first* s *columns of the identity matrix* $\boldsymbol{I}_{m_b}$*,*
- *define matrix*

$$\boldsymbol{V}_{\epsilon,k} = \boldsymbol{W}_\epsilon^k \boldsymbol{I}_{m_b \times s}, \tag{3.6}$$

- *define*

$$\boldsymbol{\Sigma}_k(\epsilon) = \boldsymbol{U}\boldsymbol{V}_{\epsilon,k}\boldsymbol{V}_{\epsilon,k}^T\boldsymbol{U}^T. \tag{3.7}$$

Then, $\forall \epsilon > 0$ *there exists a set of positive semidefinite matrices* $\{\boldsymbol{\Sigma}_k(\epsilon)\}_{k=1,\dots,K}$ *with rank* $\operatorname{rank}(\boldsymbol{\Sigma}_k(\epsilon)) = s$*,* $\forall k$*, that jointly satisfy the following:*

1. $r_k \triangleq \operatorname{rank}(\boldsymbol{H}\boldsymbol{\Sigma}_k(\epsilon)\boldsymbol{H}^T) = s$*,* $\forall k$
2. $r_{k\ell} \triangleq \operatorname{rank}(\boldsymbol{H}(\boldsymbol{\Sigma}_k(\epsilon) + \boldsymbol{\Sigma}_\ell(\epsilon))\boldsymbol{H}^T) = \min\{m_b, 2s\}$*,* $\forall k, \ell$
3. *there exists a unique* $\boldsymbol{\Sigma}(0)$*, such that* $\lim_{\epsilon \to 0} \boldsymbol{\Sigma}_k(\epsilon) = \boldsymbol{\Sigma}(0)$*,* $\forall k$*.*

Proof See the appendix.

Example 3.1 Let $\bar{\boldsymbol{I}}_{m_b}$ denote the reverse identity matrix

$$\bar{\boldsymbol{I}}_{m_b} = \begin{bmatrix} 0 \cdots & 0 & 1 \\ \vdots & \iddots & \iddots & 0 \\ 0 & \iddots & \iddots & \vdots \\ 1 & 0 & \cdots & 0 \end{bmatrix}. \tag{3.8}$$

Matrix $\boldsymbol{W}_\epsilon = \boldsymbol{I}_{m_b} + \epsilon\bar{\boldsymbol{I}}_{m_b}$ satisfies conditions of Lemma 3.1. In fact, we can note that, in this case, it holds

$$\boldsymbol{W}_\epsilon^k = \frac{1}{2}\left[(1+\epsilon)^k + (1-\epsilon)^k\right]\boldsymbol{I}_{m_b} + \frac{1}{2}\left[(1+\epsilon)^k - (1-\epsilon)^k\right]\bar{\boldsymbol{I}}_{m_b}, \tag{3.9}$$

and, therefore, conditions in Lemma 3.1 hold if $\epsilon > 0$ and $\epsilon \neq 1$. A further example is obtained by expressing $\boldsymbol{W}_\epsilon$ in terms of the Cayley transform [6] of an anti-symmetric matrix:

$$\boldsymbol{W}_\epsilon = (\boldsymbol{I} - \epsilon(\boldsymbol{A} - \boldsymbol{A}^T))(\boldsymbol{I} + \epsilon(\boldsymbol{A} - \boldsymbol{A}^T))^{-1} \tag{3.10}$$

where $\boldsymbol{A}$ is a random matrix drawn from a continuous pdf. In particular, in this case we note that $\boldsymbol{W}_\epsilon$ is unitary and the probability that any sub matrix of $\boldsymbol{W}_\epsilon^k$ is not full rank is zero.

We are now ready to show the result on the secrecy capacity of the proposed scheme.

Theorem 3.1 *Consider the MIMOME system described in (3.1) with $m_e < m_b < m_a$ antennas, GMM transmission and discrete input $c \in \{1, \ldots, K\}$. Assume that Alice has perfect knowledge of the channel towards Bob, $\boldsymbol{H}$, and that $\boldsymbol{G}$ is assumed be drawn from a continuous density on $\mathbb{R}^{m_e \times m_a}$. Then there exist GMM input parameters $\{p_k\}$, $\{\boldsymbol{\mu}_k\}$ and $\{\boldsymbol{\Sigma}_k(\epsilon)\}$ such that*

$$\lim_{\epsilon\to 0}\lim_{\sigma^2\to 0} \mathbb{I}(\boldsymbol{y}; c) = \log K \tag{3.11}$$

and for all $\eta > 0$

$$\lim_{\epsilon\to 0} \mathbb{P}\left[\mathbb{I}(\boldsymbol{z}, c) \geq \eta\right] = 0. \tag{3.12}$$

Then, in the low-noise regime, the secrecy rate

$$\sup_{\epsilon} \lim_{\sigma^2\to 0} R_s(\epsilon) = \log K, \tag{3.13}$$

is achievable with probability 1 and it coincides with the secrecy capacity, which is achieved by choosing $p_k = 1/K$ and $\boldsymbol{\mu}_k = \boldsymbol{0}$, for $k = 1, \ldots, K$, and $\boldsymbol{\Sigma}_k(\epsilon)$ as in Lemma 3.1.

Proof See the appendix.

It is relevant to observe that the signaling scheme determined by the input covariance matrices in Lemma 3.1 guarantees that, asymptotically, $\mathbb{I}(\boldsymbol{z}; c) \to 0$ for any realization of the eavesdropper channel matrix $\boldsymbol{G}$, with probability 1. This result has been shown to hold in the low-noise limit $\sigma^2 \to 0$, thus implying that, for all values $\sigma^2 > 0$, the mutual information to Eve still asymptotically approaches zero, since adding noise decreases the quality of communication. Therefore the proposed scheme provides secrecy even without the knowledge of the eavesdropper channel and, most notably, without requiring the use of wiretap codes. In fact, simple error correcting coding can be used and secrecy is obtained directly by leveraging the fact that the mutual information at the eavesdropper can be reduced asymptotically to zero by tuning the parameter ϵ. Moreover, in the low-noise regime, such scheme achieves the secrecy capacity $\log K$.

From Theorem 3.1 we also observe that when the scheme is designed in order to maximize the secrecy rate, a solution significantly different from the artificial noise scheme is obtained. Indeed, the same mean $\boldsymbol{\mu}_c$ is used for all symbols, which are instead distinguished by the covariance matrices $\boldsymbol{\Sigma}_c$.

3.4 Asymptotic Behavior

We now explore how the low-noise limit described in the previous section is approached when $\sigma^2 > 0$. In particular, we aim at deriving design criteria useful for a noisy scenario by analyzing the impact of non-zero mean classes on the information leakage and by deriving low-noise expansion for the error portability at the legitimate receiver and the mutual information at the eavesdropper.

3.4.1 Design of Input Mean Values $\boldsymbol{\mu}_k$

We start by considering the choice of the input mean values $\boldsymbol{\mu}_k$. As already shown in the proof of Theorem 3.1, also when choosing $\boldsymbol{\mu}_k = \mathbf{0}$, for $k = 1, \ldots, K$ it is possible to guarantee that the (uncoded) symbol error probability associated to the maximum a posteriori (MAP) decoder at Bob approaches zero when $\sigma^2 \to 0$.

On the other hand, the following lemma considers the effect of input means onto the information leakage to Eve. More specifically, we consider here an upper bound to $\mathbb{I}(z; c) = h(z) - h(z|c)$, where $h(\cdot)$ denotes the differential entropy. Conditioned on $c = k$, the random vector z follows the Gaussian distribution with mean $\boldsymbol{G}\boldsymbol{\mu}_k$ and covariance $\boldsymbol{G}\boldsymbol{\Sigma}_k(\epsilon)\boldsymbol{G}^T + \boldsymbol{I}\sigma^2$ and we can write the conditional differential entropy of z given c as

$$h(z|c) = \sum_{k=1}^{K} \frac{1}{2K} \log\left[(2\pi e)^{m_e} \det\left(\boldsymbol{G}\boldsymbol{\Sigma}_k\boldsymbol{G}^T + \boldsymbol{I}\sigma^2\right)\right]. \tag{3.14}$$

Moreover, we can consider the upper bound to the differential entropy of z given by the differential entropy of a multivariate normal distribution with the same mean vector and covariance matrix, that is by writing [2]

$$h(\boldsymbol{z}) \leq h_G(\boldsymbol{z}) = \frac{1}{2}\log\left[(2\pi e)^{m_e}\det\left(\boldsymbol{\Sigma}_z(\epsilon)\right)\right], \tag{3.15}$$

which leads to the upper bound to the information leakage to Eve

$$\bar{\mathbb{I}}(\boldsymbol{z}; c) = h_G(\boldsymbol{z}) - h(\boldsymbol{z}|c) \tag{3.16}$$

$$= \frac{1}{2}\log\left[(2\pi e)^{m_e}\det\left(\boldsymbol{\Sigma}_z(\epsilon)\right)\right]$$
$$- \sum_{k=1}^{K}\frac{1}{2K}\log\left[(2\pi e)^{m_e}\det\left(\boldsymbol{G}\boldsymbol{\Sigma}_k(\epsilon)\boldsymbol{G}^T + \boldsymbol{I}\sigma^2\right)\right]. \tag{3.17}$$

Note that, in general, when $\boldsymbol{\mu}_k \neq \boldsymbol{0}$, the mean and covariance of the eavesdropper observation $\boldsymbol{z}$ are given by

$$\boldsymbol{\mu}_[\boldsymbol{z}] = \mathbb{E}\boldsymbol{z} = \sum_{k=1}^{K} p_k \boldsymbol{G}\boldsymbol{\mu}_k$$
$$\boldsymbol{\Sigma}_z = \mathbb{E}(\boldsymbol{z} - \boldsymbol{\mu}_z)(\boldsymbol{z} - \boldsymbol{\mu}_z)^T$$
$$= \sum_{k=1}^{K} p_k \boldsymbol{G}\left(\boldsymbol{\Sigma}_k + \boldsymbol{\mu}_k\boldsymbol{\mu}_k^T\right)\boldsymbol{G}^T$$
$$- \sum_{k,\ell=1}^{K} p_k p_\ell \boldsymbol{G}(\boldsymbol{\mu}_k\boldsymbol{\mu}_\ell^T)\boldsymbol{G}^T + \boldsymbol{I}\sigma^2. \tag{3.18}$$

The following lemma states that using zero-mean classes minimizes the upper bound to the information leakage in (3.17).

Lemma 3.2 *Given the positive semidefinite matrix* $\boldsymbol{\Sigma}_z$ *in (3.18), it holds*

$$\log\det(\boldsymbol{\Sigma}_z) \geq \log\det\left(\sum_{k=1}^{K} p_k \boldsymbol{G}\boldsymbol{\Sigma}_k\boldsymbol{G}^T + \boldsymbol{I}\sigma^2\right). \tag{3.19}$$

Proof Consider the difference matrix

$$\boldsymbol{\Delta} = \boldsymbol{\Sigma}_z - \left(\sum_{k=1}^{K} p_k \boldsymbol{G}\boldsymbol{\Sigma}_k\boldsymbol{G}^T + \boldsymbol{I}\sigma^2\right)$$
$$= \sum_{k=1}^{K} p_k \boldsymbol{G}\boldsymbol{\mu}_k(\boldsymbol{G}\boldsymbol{\mu}_k)^T - \sum_{k=1}^{K} p_k \boldsymbol{G}\boldsymbol{\mu}_k \sum_{\ell=1}^{K} p_\ell \boldsymbol{\mu}_\ell^T \boldsymbol{G}^T. \tag{3.20}$$

Note that $\boldsymbol{\Delta}$ is the covariance matrix of a discrete random vector taking values in the alphabet $\{\boldsymbol{G}\boldsymbol{\mu}_1, \dots, \boldsymbol{G}\boldsymbol{\mu}_K\}$ with probability mass function (pmf) $\{p_1, \dots, p_K\}$, and thus, it is positive semidefinite. Then, by leveraging Weyl's Theorem (see Corollary 4.3.3 in [9]), we can conclude that the ordered eigenvalues of $\boldsymbol{\Sigma}_z$ are all greater or equal than the corresponding ordered eigenvalues of the matrix on the left hand side of (3.19), thus proving the inequality.

3.4.2 Error Probability

In the following, we analyze the behavior of the (uncoded) symbol error probability at Bob by assuming $p_k = 1/K$ and $\boldsymbol{\mu}_k = \boldsymbol{0}$, for $k = 1, \dots, K$, and $\boldsymbol{\Sigma}_k(\epsilon)$ as in Lemma 3.1.

We consider first the case $K = 2$. In this case, the symbol error probability associated to a MAP decoder can be written as

$$\mathbb{P}[\hat{c} \neq c] = \int_{-\infty}^{+\infty} \min\{p_1 \cdot p(\boldsymbol{y}|c = 1), p_2 \cdot p(\boldsymbol{y}|c = 2)\} d\boldsymbol{y}, \tag{3.21}$$

where $p(\boldsymbol{y}|c = 1)$ and $p(\boldsymbol{y}|c = 2)$ represent the conditional pdf of the legitimate receiver input when the transmitted symbol is equal to 1 or 2, respectively. Note that these conditional pdfs are zero-mean, Gaussian, with covariance matrices $\boldsymbol{H}\boldsymbol{\Sigma}_1(\epsilon)\boldsymbol{H}^T + \sigma^2\boldsymbol{I}$ and $\boldsymbol{H}\boldsymbol{\Sigma}_2(\epsilon)\boldsymbol{H}^T + \sigma^2\boldsymbol{I}$, respectively. Then, on noting that

$$\min\{a, b\} \leq \sqrt{ab}, \quad a, b \geq 0, \tag{3.22}$$

we can express the Bhattacharyya upper bound of $\mathbb{P}[\hat{c} \neq c]$ as [5]

$$P_{\text{err}} = \sqrt{p_1 p_2} \int_{-\infty}^{+\infty} \sqrt{p(\boldsymbol{y}|c = 1)p(\boldsymbol{y}|c = 2)} d\boldsymbol{y} = \frac{1}{2} e^{-B_{12}}, \tag{3.23}$$

where

$$B_{k\ell} = \frac{1}{2} \log \frac{\frac{1}{2}\det\left(\boldsymbol{H}\left(\boldsymbol{\Sigma}_k(\epsilon) + \boldsymbol{\Sigma}_\ell(\epsilon)\right)\boldsymbol{H}^T + 2\sigma^2\boldsymbol{I}\right)}{\sqrt{\det\left(\boldsymbol{H}\boldsymbol{\Sigma}_k(\epsilon)\boldsymbol{H}^T + \sigma^2\boldsymbol{I}\right)\det\left(\boldsymbol{H}\boldsymbol{\Sigma}_\ell(\epsilon)\boldsymbol{H}^T + \sigma^2\boldsymbol{I}\right)}}.$$

For $K > 2$, on applying the union bound, we obtain an upper bound to the error probability $\mathbb{P}[\hat{c} \neq c]$ as

$$P_{\text{err}} = \frac{1}{K} \sum_{k=1}^{K} \sum_{\ell \neq k} e^{-B_{k\ell}}. \tag{3.24}$$

In the high-SNR regime, the upper bound can be expanded as [16]

$$P_{\mathrm{err}} = \left(\frac{g_c}{\sigma^2}\right)^{-d} + o\left(\left(\frac{1}{\sigma^2}\right)^{-d}\right). \tag{3.25}$$

The diversity-order d determines the slope of the upper bound to the error probability (in a logarithmic scale), and it is given by

$$d = \min_{k\neq\ell} d(k,\ell) = \min_{k\neq\ell} \frac{1}{4}(2r_{k\ell} - r_k - r_\ell), \tag{3.26}$$

where

$$r_k = \mathrm{rank}(\boldsymbol{H}\boldsymbol{\Sigma}_k(\epsilon)\boldsymbol{H}^T) \tag{3.27}$$
$$r_{k\ell} = \mathrm{rank}(\boldsymbol{H}(\boldsymbol{\Sigma}_k(\epsilon) + \boldsymbol{\Sigma}_\ell(\epsilon))\boldsymbol{H}^T). \tag{3.28}$$

On the other hand, the coding gain g_c represents the power offset of the upper bound to the error probability (in a logarithmic scale) and it is given by

$$g_c = \left[\sum_{(k,\ell)\in\mathscr{S}_d} \frac{1}{K} 2^{r_{k\ell}} \left[\frac{v_{k\ell}}{\sqrt{v_k v_\ell}}\right]^{-\frac{1}{2}}\right]^{-\frac{1}{d}}, \tag{3.29}$$

where $\mathscr{S}_d$ is the set of pairs of indexes corresponding to pairs of classes with minimum diversity-order, that is, $\mathscr{S}_d = \{(k,\ell) : k \neq \ell, d(k,\ell) = d\}$, and

$$v_k = \mathrm{pdet}(\boldsymbol{H}\boldsymbol{\Sigma}_k(\epsilon)\boldsymbol{H}^T) \tag{3.30}$$
$$v_{k\ell} = \mathrm{pdet}(\boldsymbol{H}(\boldsymbol{\Sigma}_k(\epsilon) + \boldsymbol{\Sigma}_\ell(\epsilon))\boldsymbol{H}^T). \tag{3.31}$$

Then, on leveraging the results in Lemma 3.1, we can characterize the diversity-order achieved by the GMM inputs described in Theorem 3.1, as it is straightforward to verify that

$$d = \begin{cases} 0 & , \text{ if } m_b \leq s \\ (m_b - s)/2 & , \text{ if } s < m_b < 2s \\ s/2 & , \text{ if } m_b \geq 2s \end{cases}. \tag{3.32}$$

Therefore, we can conclude that the diversity order does not depend on ϵ and it is just a function of s and the number of antennas at Bob. On the other hand, the coding gain depends on ϵ.

Figure 3.2 shows an example of the upper bound (dashed lines) and true symbol error probability (solid lines) to Bob for a given value of $\boldsymbol{H}$. In the high-SNR regime, the upper bound is characterized by the diversity-order d and the coding gain g_c.

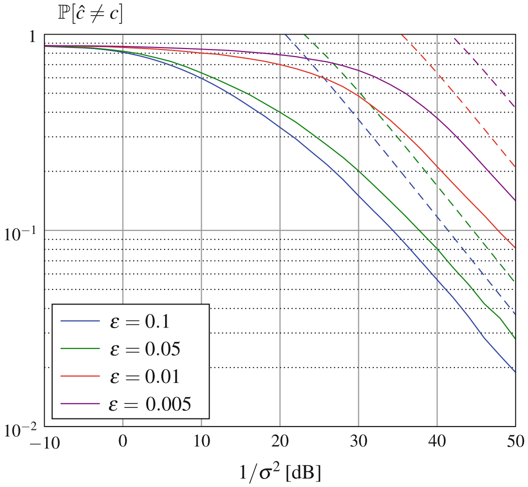


Fig. 3.2 Example of the upper bound (*dashed lines*) and true symbol error probability (*solid lines*) to Bob for a given value of $\boldsymbol{H}$. In the high-SNR regime, the upper bound is characterized by the diversity-order d and the coding gain g_c

3.4.3 Information Leakage to Eve

For a given value of $\boldsymbol{G}$, we can also provide a high-SNR, first-order expansion of the upper bound to the mutual information leakage to Eve $I(\sigma^2) = \bar{\mathbb{I}}(\boldsymbol{z}; c)$ in (3.17).[2] We assume $p_k = 1/K$ and $\boldsymbol{\mu}_k = \mathbf{0}$, for $k = 1, \ldots, K$, and $\boldsymbol{\Sigma}_k(\epsilon)$ as in Lemma 3.1 and we can write

$$I(\sigma^2) = I(0) + I'(0) \cdot \sigma^2 + o(\sigma^2), \tag{3.33}$$

where

$$I(0) = \frac{1}{2} \log\det\left(\sum_{k=1}^{K} \frac{1}{K} \boldsymbol{G}\boldsymbol{\Sigma}_k(\epsilon)\boldsymbol{G}^T\right) - \sum_{k=1}^{K} \frac{1}{2K} \log\det\left(\boldsymbol{G}\boldsymbol{\Sigma}_k(\epsilon)\boldsymbol{G}^T\right) \tag{3.34}$$

and

$$I'(0) = \frac{1}{2\ln 2}\left[\operatorname{tr}\left(\left(\sum_{k=1}^{K} p_k \boldsymbol{G}\boldsymbol{\Sigma}_k\boldsymbol{G}^T\right)^{-1}\right) - \sum_{k=1}^{k} p_k \operatorname{tr}\left(\left(\boldsymbol{G}\boldsymbol{\Sigma}_k\boldsymbol{G}^T\right)^{-1}\right)\right]. \tag{3.35}$$

Figure 3.3 shows an example of the high-SNR expansion of the mutual information leakage to Eve for a given value of $\boldsymbol{G}$. Actual value (solid lines) and first-order expansion (dashed lines).

[2] The following expansion is valid for all possible values of the channel matrix $\boldsymbol{G}$ except for a set with null measure.

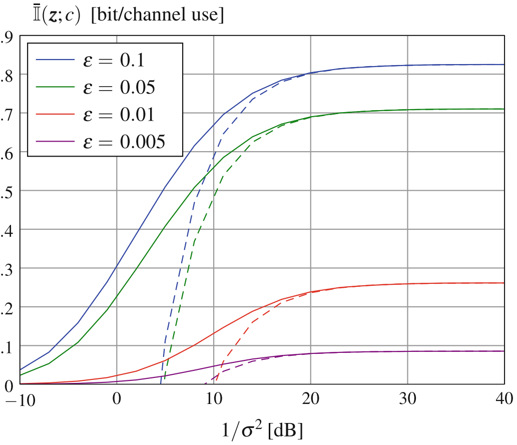


Fig. 3.3 Example of the high-SNR expansion of the mutual information leakage to Eve for a given value of $\boldsymbol{G}$. Actual value (*solid lines*) and first-order expansion (*dashed lines*)

3.5 Numerical Results

In the previous sections, we have described a transmission strategy which achieves a secrecy rate equal to log K in the low-noise regime without the need of wiretap coding. In this section, we focus on finite SNR values, assessing the *equivocation rate* [21]

$$R_e = \left[\mathbb{I}(\boldsymbol{y}; c) - \mathbb{I}(\boldsymbol{z}; c)\right]^+ . \tag{3.36}$$

We consider an error correcting code with rate $R_c = \mathbb{I}(\boldsymbol{y}; c)$ and recall that, when the equivocation rate R_e is equal to the transmission rate R_c, then we have perfect secrecy [22]. We set $m_a = 10$, $m_b = 6$ and $m_e = 4$, respectively.

Figure 3.4 shows the cumulative distribution function (CDF) of the equivocation rates obtained when the legitimate channel matrix $\boldsymbol{H}$ contains the first m_b rows of an m_a-dimensional discrete cosine transform (DCT) matrix, whereas the eavesdropper channel matrices are randomly generated with i.i.d. zero-mean, unit-variance, Gaussian entries. The SNR is equal to 35 dB, the numbers of classes of the transmitted signals are $K = 2$ and $K = 8$, and $\epsilon = 0.01$ and $\epsilon = 0.005$. We also report the value of the secrecy rate R_H that is achieved by the wiretap coding scheme described in [8]. We can notice that, when $K = 2$, our scheme provides a much lower equivocation rate than the secrecy rate of [8]. Moreover, on increasing the number of transmitted classes to $K = 8$, higher equivocation rates are achieved than the secrecy rate of [8], at the expense of a higher information leakage towards Eve.

We then consider the case in which also $\boldsymbol{H}$ is generated at random with i.i.d., zero-mean, unit-variance Gaussian entries. Alice is assumed to know the current realization of the legitimate channel coefficients, and she could arguably optimize the values of K and ϵ to maximize the equivocation rate under a given constraint on the probability that the leakage to the eavesdropper overcomes a given threshold. Nevertheless, we assess approximately the performance of the system by considering

Fig. 3.4 CDF of the equivocation rates R_e with fixed $\boldsymbol{H}$. SNR = 35 dB, $\epsilon = 0.01, 0.005$. $m_a = 10$, $m_b = 6$ and $m_e = 4$, $K = 2, 8$. The *dashed vertical lines* represent the transmission rates R_c

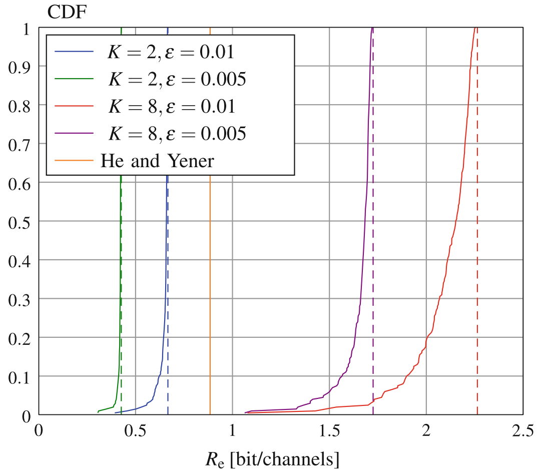
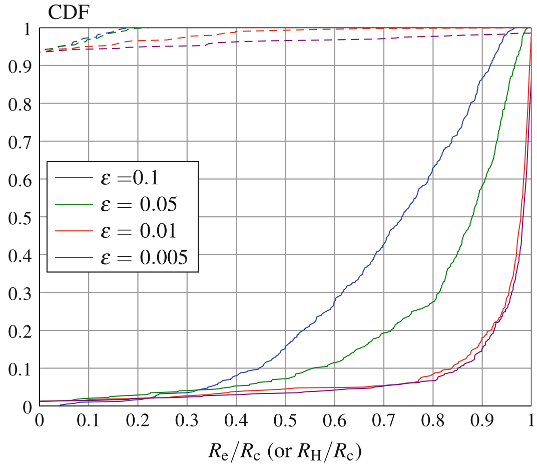


Fig. 3.5 CDF of the rate R_e/R_c (*solid lines*) and of the ratio R_H/R_c (*dashed lines*). SNR = 25 dB. $m_a = 10$, $m_b = 6$ and $m_e = 4$, $K = 2$ and $\epsilon = 0.1, 0.05, 0.01, 0.005$



the case in which $K = 2$, SNR = 25 dB, and by choosing $\epsilon = 0.1, 0.05, 0.01, 0.005$. Figure 3.5 shows the CDF of R_e/R_c, i.e., the secure fraction of the transmitted rate. For comparison, we also report the CDF of R_H/R_c, where R_c is still the code rate of our scheme. We observe that, by taking $\epsilon \leq 0.01$, only 20 % of the channel realizations correspond to information leakages to Eve that are larger than the 10 % of the transmitted rate. Moreover, for such values of ϵ, the transmission rate guaranteed by our scheme is higher than the secrecy rate of [8] for the large majority of channel realizations.

3.6 Conclusions

In this work, we have studied secrecy rates achieved over a MIMOME channel when transmitted signals are drawn from a K-classes GMM distribution and when the secret message is encoded into the index representing the chosen Gaussian distribution among the K classes. We have considered the case in which the transmitter and the legitimate receiver have perfect knowledge of the legitimate channel, whereas they do not know the eavesdropper channel, which is drawn from a (possibly unknown) continuous probability density. On the other hand, we have assumed that the legitimate user can deploy more antennas than Eve.

We have shown that, in the high-SNR regime, the secrecy capacity associated to this scenario is equal to the capacity without secrecy constraints, i.e., $\log K$. We have also provided a constructive description of a class of GMM distributions that achieve the secrecy capacity in the high-SNR regime by nulling the mutual information to Eve.

The reliability and secrecy performance of the system when the noise power σ^2 is strictly greater than zero have also been considered. In particular, we have provided a high-SNR expansion of an upper bound to the uncoded symbol error probability at Bob associated to the capacity achieving inputs. Moreover, we have provided a high-SNR expansion of an upper bound to the corresponding mutual information leakage to Eve. Such expansions can offer the means to properly design the tradeoff between secrecy and reliability in implementation scenarios where the effect of noise cannot be neglected. Finally, the tradeoff between reliable decoding and information leakage to the eavesdropper is also explored via numerical simulations for the case of coded transmissions.

Appendix

Proof of Lemma 3.1

It is clear from (3.7) and (3.6) that $\operatorname{rank}(\boldsymbol{\Sigma}_k(\epsilon)) = s, \forall k, \epsilon$. Then, since $\mathscr{R}(\boldsymbol{\Sigma}_k(\epsilon)) \subset \mathscr{R}(\boldsymbol{U})$ and $\mathscr{R}(\boldsymbol{U}) \perp \operatorname{null}(\boldsymbol{H})$, then $\operatorname{rank}(\boldsymbol{H}\boldsymbol{\Sigma}_k(\epsilon)\boldsymbol{H}^{\mathrm{T}}) = \operatorname{rank}(\boldsymbol{\Sigma}_k(\epsilon))$ and condition (1) follows.

In order to prove condition (2), observe that

$$r_{k\ell} = \operatorname{rank}(\boldsymbol{H}(\boldsymbol{\Sigma}_k(\epsilon) + \boldsymbol{\Sigma}_\ell(\epsilon))\boldsymbol{H}^{\mathrm{T}}) = \operatorname{rank}(\boldsymbol{V}_{\epsilon,k}\boldsymbol{V}_{\epsilon,k}^{\mathrm{T}} + \boldsymbol{V}_{\epsilon,\ell}\boldsymbol{V}_{\epsilon,\ell}^{\mathrm{T}}) \quad (3.37)$$

as $\mathscr{R}(\boldsymbol{\Sigma}_k(\epsilon)) \perp \operatorname{null}(\boldsymbol{H})$. Moreover,

$$\mathrm{rank}(\boldsymbol{V}_{\epsilon,k}\boldsymbol{V}_{\epsilon,k}^{\mathrm{T}}+\boldsymbol{V}_{\epsilon,\ell}\boldsymbol{V}_{\epsilon,\ell}^{\mathrm{T}}) = m_b-\nu(\boldsymbol{V}_{\epsilon,k}\boldsymbol{V}_{\epsilon,k}^{\mathrm{T}}+\boldsymbol{V}_{\epsilon,\ell}\boldsymbol{V}_{\epsilon,\ell}^{\mathrm{T}}) \tag{3.38}$$

$$= m_b-\dim\left[\mathrm{null}(\boldsymbol{V}_{\epsilon,k}\boldsymbol{V}_{\epsilon,k}^{\mathrm{T}})\cap\mathrm{null}(\boldsymbol{V}_{\epsilon,\ell}\boldsymbol{V}_{\epsilon,\ell}^{\mathrm{T}})\right] \tag{3.39}$$

$$= m_b-\dim\left[\mathrm{null}(\boldsymbol{V}_{\epsilon,k}^{\mathrm{T}})\cap\mathrm{null}(\boldsymbol{V}_{\epsilon,\ell}^{\mathrm{T}})\right] \tag{3.40}$$

$$= m_b-\dim\mathrm{null}\left(\begin{bmatrix}\boldsymbol{V}_{\epsilon,k}^{\mathrm{T}}\\ \boldsymbol{V}_{\epsilon,\ell}^{\mathrm{T}}\end{bmatrix}\right) \tag{3.41}$$

$$= m_b-\nu([\boldsymbol{V}_{\epsilon,k}\ \boldsymbol{V}_{\epsilon,\ell}]^{\mathrm{T}}) \tag{3.42}$$

$$= \mathrm{rank}([\boldsymbol{V}_{\epsilon,k}\ \boldsymbol{V}_{\epsilon,\ell}]) \tag{3.43}$$

$$= \mathrm{rank}\left([\boldsymbol{I}_{m_{\mathrm{b}}\times s}\ \boldsymbol{W}_{\epsilon}^{\ell-k}\boldsymbol{I}_{m_{\mathrm{b}}\times s}]\right). \tag{3.44}$$

Then, by leveraging the previous assumption on the bottom left minors of $\boldsymbol{W}_{\epsilon}^{k}$, we have that the bottom left $(m_{\mathrm{b}}-s)\times s$ sub matrix of $\boldsymbol{W}_{\epsilon}^{\ell-k}$ is full rank, and therefore condition 2) holds.

Finally, condition 3) follows from the fact that $\lim\limits_{\epsilon\to 0}\boldsymbol{W}_{\epsilon}=\boldsymbol{I}_{m_{\mathrm{b}}}$, and we have

$$\boldsymbol{\Sigma}(0)=\boldsymbol{U}\begin{bmatrix}\boldsymbol{I}_s & \boldsymbol{0}\\ \boldsymbol{0} & \boldsymbol{0}\end{bmatrix}\boldsymbol{U}^{\mathrm{T}}. \tag{3.45}$$

Proof of Theorem 3.1

The converse part of the proof is trivial, and it is based on the fact that the secrecy capacity is always lower or equal than the capacity without secrecy constraints, that implies

$$C_s\le\max_{c}\mathbb{I}(\boldsymbol{y};c)\le\mathbb{H}(c)\le\log K, \tag{3.46}$$

where $\mathbb{H}(c)$ is the entropy of c and the upper bound in the right hand side is achieved when $p_k=1/K$, for $k=1,\dots,K$.

In order to provide the achievability part of the proof, we consider the achievable secrecy rates that are obtained by imposing $u=c$ and we consider separately reliability and secrecy. In this case, the error correcting code is not used and $\hat{u}$ is the hard decision taken on $\tilde{b}$. We assume that the transmitter adopts a signaling scheme with $p_k=1/K$ and $\boldsymbol{\mu}_k=\boldsymbol{0}$, for $k=1,\dots,K$. Moreover, given $\epsilon>0$, the input covariance matrices are obtained from the construction described in Lemma 3.1 where s is chosen such that $m_{\mathrm{e}}\le s<m_{\mathrm{b}}$. From the lemma we conclude that for any two distinct values $c_1\neq c_2$, $1\le c_1,c_2\le K$, the null spaces of the covariance matrices $\boldsymbol{H}\boldsymbol{\Sigma}_{c_1}\boldsymbol{H}^T$ and $\boldsymbol{H}\boldsymbol{\Sigma}_{c_2}\boldsymbol{H}^T$ are distinct. Let us consider a decoder that computes

$$\alpha_c=||\boldsymbol{N}_c\boldsymbol{y}||, \tag{3.47}$$

where $\boldsymbol{N}_c$ is a matrix containing a basis of the null space generated by $\boldsymbol{H}\boldsymbol{\Sigma}_c\boldsymbol{H}^T$, and then chooses

$$\hat{c} = \text{argmin}_c \alpha_c. \tag{3.48}$$

In the absence of noise this decoder achieves zero error probability since the null spaces of $\boldsymbol{\Sigma}_c$ are all distinct and therefore

$$\lim_{\sigma^2 \to 0} \mathbb{P}[\hat{c} \neq c] = 0. \tag{3.49}$$

More in general, the Bhattacharyya upper bound to the error probability associated to a MAP decoder at Bob, P_{err} in (3.24), can be shown to approach zero in the high-SNR regime, i.e., following the steps of [16] we again conclude that (3.49) holds. Then, by leveraging Fano's inequality [2], we can state that

$$\lim_{\sigma^2 \to 0} \mathbb{H}(c|\boldsymbol{y}) = 0, \tag{3.50}$$

where $\mathbb{H}(\cdot|\cdot)$ denotes the conditional entropy, and, therefore,

$$\lim_{\sigma^2 \to 0} \mathbb{I}(\boldsymbol{y}; c) = \mathbb{H}(c) = \log K. \tag{3.51}$$

Consider now the information leaked to the eavesdropper

$$\mathbb{I}(\boldsymbol{z}; c) = h(\boldsymbol{z}) - h(\boldsymbol{z}|c). \tag{3.52}$$

First note that even if c is known at the eavesdropper, the transmitted signal $\boldsymbol{x}$ is not completely known to Eve, since it is randomly generated from the Gaussian distribution $\mathcal{N}(\boldsymbol{\mu}_c, \boldsymbol{\Sigma}_c)$. Conditioned on $c = k$, the random vector $\boldsymbol{z}$ follows the Gaussian distribution with mean $\boldsymbol{G}\boldsymbol{\mu}_k = \boldsymbol{0}$ and covariance $\boldsymbol{G}\boldsymbol{\Sigma}_k(\epsilon)\boldsymbol{G}^{\text{T}} + \boldsymbol{I}\sigma^2$ and we can write the conditional differential entropy of $\boldsymbol{z}$ given c as

$$h(\boldsymbol{z}|c) = \sum_{k=1}^{K} \frac{1}{2K} \log\left[(2\pi e)^{m_{\text{e}}} \det\left(\boldsymbol{G}\boldsymbol{\Sigma}_k\boldsymbol{G}^{\text{T}} + \boldsymbol{I}\sigma^2\right)\right]. \tag{3.53}$$

Note in particular that since $\boldsymbol{x}|c$ is still a random vector, $h(\boldsymbol{z}|c) \neq h(\boldsymbol{w})$.

Then, note that the eavesdropper observation $\boldsymbol{z}$ follows the GMM distribution

$$f_z(\boldsymbol{b}) = \sum_{k=1}^{K} \frac{1}{K} \nu(\boldsymbol{b}; \boldsymbol{0}, \boldsymbol{G}\boldsymbol{\Sigma}_k\boldsymbol{G}^{\text{T}} + \boldsymbol{I}\sigma^2), \tag{3.54}$$

and we can consider the upper bound to the information leakage to Eve that is obtained by upper bounding the differential entropy of $\boldsymbol{z}$ by that of a multivariate normal distribution with the same mean vector and covariance matrix,

$$\boldsymbol{\mu}_z = \mathbf{0} \tag{3.55}$$

$$\boldsymbol{\Sigma}_z(\epsilon) = \frac{1}{K}\sum_{k=1}^{K}\boldsymbol{\Sigma}_k(\epsilon) + \boldsymbol{I}\sigma^2, \tag{3.56}$$

respectively, that is by writing [2]

$$h(z) \le h_G\,(z) = \frac{1}{2}\log\left[(2\pi e)^{m_\mathrm{e}}\det\left(\boldsymbol{\Sigma}_z(\epsilon)\right)\right]. \tag{3.57}$$

Such upper bound is given by

$$\begin{aligned}\bar{\mathbb{I}}(\epsilon, \boldsymbol{G}) &= h_G(z) - h(z|c) & (3.58)\\ &= \frac{1}{2}\log\left[(2\pi e)^{m_\mathrm{e}}\det\left(\sum_{k=1}^{K}\frac{1}{K}\boldsymbol{\Sigma}_k(\epsilon) + \boldsymbol{I}\sigma^2\right)\right] & (3.59)\\ &- \sum_{k=1}^{K}\frac{1}{2K}\log\left[(2\pi e)^{m_\mathrm{e}}\det\left(\boldsymbol{G}\boldsymbol{\Sigma}_k(\epsilon)\boldsymbol{G}^\mathrm{T} + \boldsymbol{I}\sigma^2\right)\right].\end{aligned}$$

Observe that such value is random, as it is a function of the random matrix $\boldsymbol{G}$, moreover, it is also a function of the parameter ϵ, which determines the expression of the input covariance matrices. Then, we consider a further upper bound to the information leakage to Eve, which is obtained by considering a noiseless channel to the eavesdropper, i.e., by imposing $\sigma^2 = 0$. On recalling that $\boldsymbol{G}$ is drawn from a continuous density, we can show that, for all $\eta > 0$, it holds

$$\lim_{\epsilon\to 0}\mathbb{P}\left[\bar{\mathbb{I}}(\epsilon, \boldsymbol{G}) \ge \eta\right] = 0. \tag{3.60}$$

In particular, the Markov's inequality provides

$$\mathbb{P}[\bar{\mathbb{I}}(\epsilon, \boldsymbol{G}) \ge \eta] \le \frac{\mathbb{E}[\bar{\mathbb{I}}(\epsilon, \boldsymbol{G})]}{\eta}. \tag{3.61}$$

Moreover, when $\sigma^2 = 0$, we have

$$\bar{\mathbb{I}}(\epsilon, \boldsymbol{G}) = \frac{1}{2}\log\det\left(\sum_{k=1}^{K}\frac{1}{K}\boldsymbol{G}\boldsymbol{\Sigma}_k(\epsilon)\boldsymbol{G}^\mathrm{T}\right) - \sum_{k=1}^{K}\frac{1}{2K}\log\det\left(\boldsymbol{G}\boldsymbol{\Sigma}_k(\epsilon)\boldsymbol{G}^\mathrm{T}\right) \tag{3.62}$$

except for a set of values $\boldsymbol{G}$ that has a null measure. Hence,

$$\lim_{\epsilon\to 0}\mathbb{E}[\bar{\mathbb{I}}(\epsilon,\boldsymbol{G})] = \tag{3.63}$$

$$\lim_{\epsilon\to 0}\mathbb{E}\left[\frac{1}{2}\log\det\left(\sum_{k=1}^{K}\frac{1}{K}\boldsymbol{G}\boldsymbol{\Sigma}_k(\epsilon)\boldsymbol{G}^{\mathrm{T}}\right)-\sum_{k=1}^{K}\frac{1}{2K}\log\det\left(\boldsymbol{G}\boldsymbol{\Sigma}_k(\epsilon)\boldsymbol{G}^{\mathrm{T}}\right)\right]= \tag{3.64}$$

$$\lim_{\epsilon\to 0}\mathbb{E}\left[\frac{1}{2}\log\det\left(\sum_{k=1}^{K}\frac{1}{K}\boldsymbol{G}\boldsymbol{\Sigma}_k(\epsilon)\boldsymbol{G}^{\mathrm{T}}\right)\right]-\mathbb{E}\left[\sum_{k=1}^{K}\frac{1}{2K}\log\det\left(\boldsymbol{G}\boldsymbol{\Sigma}_k(\epsilon)\boldsymbol{G}^{\mathrm{T}}\right)\right] \tag{3.65}$$

where the matrices $\boldsymbol{G}\boldsymbol{\Sigma}_k(\epsilon)\boldsymbol{G}^{\mathrm{T}}$ are non-singular since $m_{\mathrm{e}} \leq s$. It is therefore possible to evaluate the limit as $\epsilon \to 0$ inside the expectation operator. In fact, we note that the expectations in (3.65) can be expressed in closed form [11]. Then, by leveraging condition 3) in Lemma 3.1, we also have that, for $\epsilon \to 0$, all $\boldsymbol{\Sigma}_k(\epsilon)$ converge to the same matrix, thus leading to

$$\lim_{\epsilon\to 0}\mathbb{E}[\bar{\mathbb{I}}(\epsilon,\boldsymbol{G})] = 0 \tag{3.66}$$

Note that the result (3.60) holds for all input covariance matrices verifying condition 3) in Lemma 3.1. Therefore, the same inputs that guarantee the reliability condition (3.51) also guarantee the absence of information leakage to Eve.

Lastly, from (3.60), recalling that $\bar{\mathbb{I}}(\epsilon,\boldsymbol{G})$ is an upper bound of $\mathbb{I}(z;c)$, we obtain (3.12).

References

1. Baldi M, Chiaraluce F, Laurenti N, Tomasin S, Renna F (2014) Secrecy transmission on parallel channels: theoretical limits and performance of practical codes. IEEE Trans Inf Forensics Secur 9(11):1765–1779
2. Cover TM, Thomas JA (1991) Elements of information theory. Wiley, New York
3. Csiszár I, Körner J (1978) Broadcast channels with confidential messages. IEEE Trans Inf Theory 24(3):339–348
4. Cumanan K, Ding Z, Sharif B, Tian GY, Leung KK (2014) Secrecy rate optimizations for a MIMO secrecy channel with a multiple-antenna eavesdropper. IEEE Trans Veh Technol 63(4):1678–1690
5. Duda RO, Hart PE, Stork DG (2000) Pattern classification, 2nd edn. Wiley-Interscience, New York
6. Golub GH, Loan CFV (1996) Matrix computations. Johns Hopkins University Press, Baltimore
7. He X, Yener A (2014) MIMO wiretap channels with unknown and varying eavesdropper channel states. IEEE Trans Inf Theory 60(11):6844–6869
8. He X, Khisti A, Yener A (2014) MIMO broadcast channel with an unknown eavesdropper: secrecy degrees of freedom. IEEE Trans Commun 62(1):246–255
9. Horn R, Johnson C (1985) Matrix analysis. Cambridge University Press, Cambridge
10. Khisti A, Wornell GW (2010) Secure transmission with multiple antennas-part II: the MIMOME wiretap channel. IEEE Trans Inf Theory 56(11):5515–5532

11. Kiessling M, Speidel J (2004) Exact ergodic capacity of MIMO channels in correlated Rayleigh fading environments. In: Proceedings of IEEE International Zurich Seminar on Communication, Zurich, Switzerland
12. Leung-Yan-Cheong S, Hellman ME (1978) The Gaussian wire-tap channel. IEEE Trans Inf Theory 24(4):451–456
13. Li Z, Yates R, Trappe W (2006) Secrecy capacity of independent parallel channels. In: Allerton conference in communication, control, and computing, Monticello, IL
14. Lin CH, Tsai SH, Lin YP (2014) Secure transmission using MIMO precoding. IEEE Trans Inf Forensics Secur 9(5):801–813
15. Liu T, Shamai S (2009) A note on the secrecy capacity of the multiple-antenna wiretap channel. IEEE Trans Inf Theory 55(6):2547–2553
16. Reboredo H, Renna F, Calderbank R, Rodrigues MRD (2013) Compressive classification. In: Proceedings of IEEE international symposium on information theory (ISIT), Istanbul, Turkey
17. Reeves G, Goela N, Milosavljevic N, Gastpar M (2011) A compressed sensing wire-tap channel. CoRR abs/1105.2621
18. Renna F, Laurenti N, Poor H (2012) Physical-layer secrecy for OFDM transmissions over fading channels. IEEE Trans Inf Forensics Secur 7(4):1354–1367
19. Tomasin S (2013) Resource allocation for secret transmissions over MIMOME fading channels. In: IEEE global conference on communication (GLOBECOM), Workshop on Trusted Communications with Physical Layer Security, Atlanta
20. Tomasin S, Laurenti N (2014) Secret message transmission by HARQ with multiple encoding. In: Proceedings of IEEE international conference on communication (ICC), Sydney, Australia
21. Wong CW, Wong T, Shea J (2011) Secret-sharing LDPC codes for the BPSK-constrained Gaussian wiretap channel. IEEE Trans Inf Forensics Secur 6(3):551–564
22. Wyner A (1975) The wiretap channel. Bell Syst Tech J 54(8):1355–1387

Chapter 4
Performance Analysis of Transmission over AWGN Wiretap Channels with Practical Codes

Marco Baldi, Franco Chiaraluce, Nicola Maturo and Stefano Tomasin

Abstract The wiretap coding problem has been addressed since a long time from an information theoretic standpoint. This has permitted to find the ultimate achievable limits under the hypothesis of random coding, which however is far from practice. Some families of practical codes have also been already considered in this scenario, but their achievable secrecy has mostly been assessed in asymptotic conditions (i.e., under the hypothesis of infinite codeword length) and using discrete channel models. In this chapter, we analyze the performance of practical codes over the Gaussian wiretap channel by using suitable metrics which take into account the codeword length and even the specific code structure. This way, we are able to assess the performance of real codes in the finite code length regime, and compare it with the ultimate achievable limits. We focus on low-density parity-check codes as they are among the most viable candidates for the use in this setting.

4.1 Introduction

The wiretap channel model [25] is the first and main reference model for physical layer secure transmissions, and it is well known that perfect secrecy can be achieved over the wiretap channel under the hypothesis of ideal random coding [14, 25].

M. Baldi (✉) · F. Chiaraluce · N. Maturo
Università Politecnica delle Marche, Ancona, Italy
e-mail: m.baldi@univpm.it

F. Chiaraluce
e-mail: f.chiaraluce@univpm.it

N. Maturo
e-mail: n.maturo@univpm.it

S. Tomasin
University of Padua, Padua, Italy
e-mail: tomasin@dei.unipd.it

M. Baldi and S. Tomasin (eds.), *Physical and Data-Link Security Techniques for Future Communication Systems*, Lecture Notes in Electrical Engineering 358, DOI 10.1007/978-3-319-23609-4_4

However, apart from the theoretical model, the need to implement real transmissions with practical codes may force them to be far from perfect secrecy, and such a risk needs to be quantified.

4.1.1 Previous Works

Some families of practical codes, like low-density parity-check (LDPC) codes and polar codes, have been shown to be able to achieve the wiretap channel secrecy capacity in the asymptotic regime (i.e., with infinite codeword length) [13, 17, 22]. However, despite this provides a very important new insight into the design of practical codes for the wiretap channel, it is not easy to predict how far from the secrecy capacity the secret throughput will be when the codeword length is reduced to some (finite) practical value. Moreover, many previous works consider discrete channel models (like the binary erasure channel (BEC) or the binary symmetric channel (BSC) models) for both the main and wiretapper's channels. However, the most interesting applications of physical layer security techniques are recognized to be in wireless communications, therefore a continuous channel model (like the additive white Gaussian noise (AWGN) channel model, with or without fading) is best suited for describing the physical layer. On the other hand, it is not realistic to suppose that an eavesdropper of a wireless link is forced to discard the soft information coming from the channel, and to use hard detection.

More in detail, an interesting family of two edge type LDPC codes has been proposed in [1, 18, 19] for the use in wiretap coding schemes exploiting Wyner's coset encoding technique. These codes are shown to achieve weak secrecy in asymptotic conditions (i.e., at infinite code lengths) over wiretap channels modeled as BECs. In addition, in [19] some results for finite length codes are provided, but still only over BECs. The weak secrecy criterion used in these works requires that the mutual information between the secret message and the eavesdropper's observation goes to zero rate-wise, rather than in absolute terms, as needed by the strong secrecy criterion. More recently, the same setting of a wiretapper BEC and a coset encoding technique has been considered in the proposal of a scheme able to achieve strong secrecy rather than weak secrecy [21], by exploiting large-girth LDPC codes. However, this result only holds in the asymptotic regime, i.e., for infinite length codes. Another scheme which has been proven to achieve perfect secrecy is based on polar codes [9]. However, also in this case such a target is achieved for discrete channels and infinite length codes, while no result is provided for finite length codes. Indeed, all evidence up to now suggests that perfect secrecy (interpreted as zero information leakage about the secret message in absolute terms, rather than rate-wise) may not be achievable by using short length codes, or in general finite length codes.

Another recent trend which is important to mention concerns some attempts to study the problems of physical layer security and wiretap coding in more general terms, and also exploring their links with computational security and cryptography. The work [7] studies the general problem of finding efficiently invertible extractors, which involves wiretap protocols. However, also in this case, the focus is on asymptotic security notions used to search for asymptotic optimal wiretap protocols over discrete, memoryless, and symmetric channels. In [5], the security notions classically used for transmissions over the wiretap channel are reviewed, and their links with the more robust notion of semantic security used in cryptography are explored. The authors also propose a new coding scheme characterized by polynomial-time decoding and achieving the secrecy capacity for the case of BSCs. Such a scheme can be extended to other discrete memoryless channels, but continuous channels (like the AWGN channel) are not taken into account. One of the very few works on coding for Gaussian wiretap channels is [16], where the authors address the problem of practical code design and propose a secure nested code structure. The authors derive the achievable rate-equivocation region based on the threshold behavior of good code sequences, that is, by considering the performance of code ensembles in the asymptotic regime, without taking into account finite length codes.

4.1.2 Error Rate Used as a Secrecy Metric

The bit error rate (BER) and codeword error rate (CER) are very common metrics for assessing the transmission reliability in practical terms, since they are quite easy to estimate for any fixed coding and modulation scheme, even through numerical simulations. An approach to use these metrics also for security has been proposed in [12], where the condition of being subjected to a BER close to 0.5 was imposed to the eavesdropper in order to achieve security. Then, the differential evolution technique was used to design optimized LDPC codes with the aim of achieving the desired BER performance for both the authorized receiver and the eavesdropper. The quality ratio between their two channels, defined as the *security gap*, was also used as a metric, which should be kept as small as possible. A similar approach has been followed in [2].

When used for assessing reliability, the error rate-based metrics can be easily related to other, information theoretic metrics, like the conditional entropy (for which we can exploit Fano's inequality). The same is instead not straightforward when we aim at measuring security. A bridge between information theoretic and error rate-based security metrics can be found in [24], where the authors propose a secret key sharing scheme for the wiretap channel. The same approach, based on the eavesdropper's equivocation rate on the secret message, has also been used to study coded transmissions over the Gaussian wiretap channel [23] and parallel channels [3], in the finite code length regime. The work [23] considers punctured LDPC codes, while in [3] the focus is on more classical coding schemes (like Bose-Chaudhuri-Hocquenghem (BCH) codes).

4.1.3 Our Contribution

In this chapter, we address the problem of measuring the reliability and secrecy performance from an information theoretic standpoint in the finite codeword length regime. For this purpose, as in the mentioned previous works, we exploit the link between the equivocation rate and the error rate in order to explore the capacity-equivocation regions of the codes we consider. Using the equivocation rate as a security metric also allows us to compare the performance achieved in the finite codeword length regime with that achievable in the asymptotic regime. We also focus on LDPC codes as a prominent solution for wiretap coding, but, differently from [23], we consider non-punctured LDPC coded transmissions, which are more common in practice with respect to punctured transmissions. We aim at finding good codes both in terms of reliability and security through a very simple code optimization approach. With respect to existing literature, the main contributions of this chapter are as follows.

- We consider continuous wiretap channels (no restriction on the use of soft information by Eve) and finite length codes.
- We take into account the specific code structure (no code ensembles).
- We relate the wiretapper's equivocation rate to the error rate, thus providing an information theoretic secrecy metric which is, at the same time, relevant to the specific code and comparable with the ultimate achievable limits.

The organization of the chapter is as follows. In Sect. 4.2, we define the channel model and the metrics we use throughout the chapter. In Sect. 4.3, we use these metrics to assess the ultimate performance achievable in asymptotic conditions. In Sect. 4.4, we show how the same metrics can be applied to the finite codeword length regime, and in Sect. 4.5 we draw some conclusions.

4.2 Channel Model and Metrics

In the Gaussian wiretap channel model, Alice transmits a k_s-bit secret message M by encoding it into an n-bit codeword X, through a binary linear block code $\mathscr{C}$. The choice of the transmitted codeword X not only depends on the secret message bits, but also on k_r random bits which are used to implement a form of nested coding [10]. The code $\mathscr{C}$ has information length $k = k_s + k_r$ and codeword length n. Its rate is $R_c = k/n$. The secret message rate is $R_s = k_s/n$. Both the authorized receiver (Bob) and an eavesdropper (Eve) receive Alice transmission, and they have full knowledge of the code $\mathscr{C}$. Bob's and Eve's channels are impaired with AWGN, and their received vectors are noted by Y and Z, respectively. In order to achieve successful transmission of M, we must achieve the following targets:

1. *reliability target*: the secret message M must be reliably decoded by Bob (i.e., with a sufficiently small error rate),
2. *security target*: Eve must be unable to gather any (or almost any) information about M.

From both the security and reliability standpoints, we aim at finding suitable metrics to be used for measuring performance in the finite code length regime, and comparing it with that achievable in asymptotic conditions.

4.2.1 Reliability Metrics

Concerning the reliability target, the following metrics can be used:

- In asymptotic conditions (infinite length codes), without any constraints on the choice of the code, the ultimate performance limit is represented by the channel capacity, which coincides with the highest code rate that can be used to achieve error-free transmission. We consider a continuous binary-input channel with AWGN and signal-to-noise ratio (SNR) per bit $\frac{E_b}{N_0}$, having capacity:

$$C\left(\frac{E_b}{N_0}\right) = 1 - \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} \mathrm{e}^{-\frac{\left(y-\sqrt{E_b/N_0}\right)^2}{2}} \log_2\left(1 + \mathrm{e}^{-2y\sqrt{E_b/N_0}}\right) dy. \quad (4.1)$$

- In asymptotic conditions (infinite length codes), but with the constraint to use LDPC coded transmissions, the density evolution technique [8, 20] can be used to compute a decoding threshold, in terms of SNR, above which transmission can occur without errors.
- In the finite code length regime, the performance of practical LDPC codes can be assessed through Montecarlo simulations, and the SNR needed to achieve a sufficiently low decoding error probability can be estimated.

4.2.2 Security Metrics

Concerning the security target, the concepts of *strong secrecy* and *weak secrecy* are classically used for wiretap coding schemes [6, 15]. The definitions of strong and weak secrecy are in the asymptotic regime. In fact, we say that we have strong secrecy when the amount of information leaked about M through observing Z vanishes as n goes to infinity, i.e., $\lim_{n\to\infty} \mathrm{I}(M; Z) = 0$, where $\mathrm{I}(x; y)$ denotes the mutual information between x and y. Similarly, we have weak secrecy when the rate of information leaked about M through observing Z vanishes as n goes to infinity, i.e., $\lim_{n\to\infty} \mathrm{I}(M; Z)/n = 0$. Despite this, we can use notions similar to strong and weak secrecy also in the finite code length regime. In fact, both of them are based on the information leakage about the secret message, measured in terms of the mutual information between the secret message and the wiretapper's observation. The difference is that for weak secrecy the information leakage is measured rate-wise, while for strong secrecy it is measured in absolute terms. Therefore, we could measure these quantities in the finite code length regime as well.[1] Another, similar way of measuring the information leakage about the secret message is by using the wiretapper's equivocation on the secret message, as done in Wyner's original work [25]. According to [25], perfect secrecy is achieved when the wiretapper's equivocation rate on the secret message equals the entropy of the data source. In this case, we use again a rate-wise measure of the information leakage, which is weaker than the notion of strong secrecy. However, as outlined in Sect. 4.1, all evidence up to now suggests that strong secrecy may not be achievable with finite length codes. Based on these premises, in the following we use the wiretapper's equivocation rate as a secrecy measure. We make this choice since it allows to relate the secrecy metrics with the error rate, as we will show next, which is an important feature to take into account the specific code structure in the performance assessment.

By denoting as $\mathrm{H}(\cdot)$ the entropy function, the wiretapper's equivocation rate is simply defined as $R_e = \frac{1}{n}\mathrm{H}(M|Z)$. Since we suppose to deal with independent and identically distributed secret messages, the source entropy rate is equal to R_s, and perfect secrecy is achieved when the equivocation rate R_e equals the secret message rate R_s:

$$\widetilde{R_e} = R_e/R_s = 1. \tag{4.2}$$

We denote $\widetilde{R_e}$ as the *fractional equivocation rate*. Obviously, the ultimate limit achievable by the equivocation rate is represented by the secrecy capacity $C_s = [C_B - C_E]^+$, where C_B and C_E are Bob's and Eve's channel capacities, respectively. It is well known that the wiretapper's equivocation rate on the secret message can also be expressed as [6, 15]:

$$R_e = \frac{1}{n}\left[\mathrm{H}(X) - \mathrm{I}(X;Z) + \mathrm{H}(M|Z,X) - \mathrm{H}(X|M,Z)\right], \tag{4.3}$$

where $\mathrm{H}(X|M,Z)$ is the entropy of X conditioned on receiving Z and knowing the secret message M.

4.2.3 Fictitious Receiver

In order to estimate $\mathrm{H}(X|M,Z)$, we can suppose the existence of a fictitious receiver which is in the same position as Eve's, but, differently from Eve, he knows the secret message M. We name this other subject Frank, and include it in our communication

[1] Obviously, in the finite length regime Bob's error probability cannot be vanishing. Therefore, in order to apply these metrics in such a regime, the reliability target must be converted into requiring that Bob achieves some sufficiently small error probability.

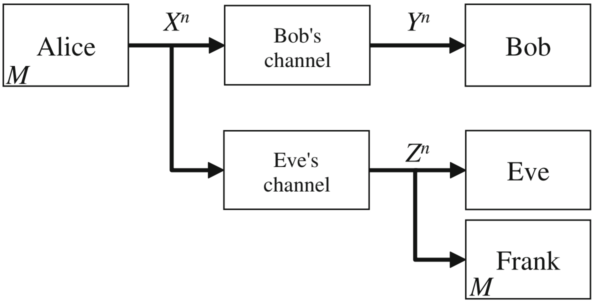


Fig. 4.1 Wiretap channel model with fictitious receiver

model, which is depicted in Fig. 4.1. The letter M inside Alice's and Frank's boxes points out that the message M is known to both Alice and Frank. Frank receives from the channel the same vector Z received by Eve and then tries to perform decoding for recovering the k_r random bits, which represent the only source of uncertainty for him in order to retrieve X.

In (4.3), we have $\mathrm{I}(X; Z) \le nC_E$, $\mathrm{H}(X) = k$ and $\mathrm{H}(M|Z, X) \le \mathrm{H}(M|X) = 0$. Concerning the term $\mathrm{H}(X|M, Z)$, by Fano inequality we have $\mathrm{H}(X|M, Z) \le 1 + k_r\eta$, where η is the decoding error probability (or CER) experienced by Frank. Based on these considerations, we can find a lower bound on the wiretapper's equivocation rate on the secret message as [23]:

$$\begin{aligned} R_e &\ge \frac{1}{n}\left[k - nC_E - k_r\eta - 1\right] = \\ &= R_c - C_E - (R_c - R_s)\eta - \frac{1}{n} = R_e^*. \end{aligned} \tag{4.4}$$

This way, we find a secrecy metric which takes into account the code length, and therefore it is suitable to assess performance also in the finite code length regime, which is of interest for practical codes. Furthermore, this metric depends on Frank's CER, which can be easily estimated, for practical codes, through numerical simulations. Looking at (4.4), one could think that an optimal solution is to impose that Eve and Frank have a very low SNR. In this case, we have $\eta \approx 1$ and $C_E \approx 0$. Under these hypotheses, and by considering sufficiently long codes to make the term $\frac{1}{n}$ negligible, we would have $R_e^* \approx R_s$. Unfortunately, this apparently optimal solution is not viable for the following reasons:

- Fixing a small value of η as Frank's performance target is beneficial for security. In fact, if Frank's error rate on the sole random bits is small, this means that Eve's equivocation will be concentrated on the secret message bits, which is what we want to achieve.
- Allowing a not-too-degraded channel for the eavesdropper is also beneficial, since this means that security can be guaranteed even when Eve is not far from Bob. This is an important aspect which is also caught by the analysis based on the security gap.

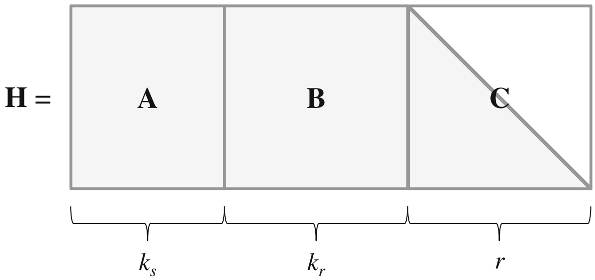


Fig. 4.2 Parity-check matrix of the considered codes

Based on these considerations, we want to achieve a value of R_e^* as high as possible, without renouncing to impose a small value of η. This requires to optimize Frank's performance as well, in such a way that he is able to achieve good decoding performance (i.e., small η) with small SNR, which means having a small capacity C_E of (Frank's and) Eve's channel.

Let us consider LDPC coding and let us suppose (without loss of generality) that encoding is systematic. Let the transmitted codeword be $\mathbf{c} = [M|R|P]$, where M is the k_s-bit secret message, R is the k_r-bit random message and P is the r-bit redundancy vector added by the encoder. In real world secure transmissions, systematic encoding shall be avoided, especially if source coding is not perfect (as always occurs in practice). For this purpose, the use of an information bit scrambler is advisable [2]. Nevertheless, in our analysis, which is aimed at estimating the performance achievable, the hypothesis of systematic coding can be maintained, since it helps simplifying the analysis. Under this hypothesis, we can describe the code $\mathscr{C}$ through a lower triangular parity-check matrix $\mathbf{H}$. More precisely, we can divide the matrix $\mathbf{H}$ into three blocks as shown in Fig. 4.2. These three blocks, named $\mathbf{A}$, $\mathbf{B}$ and $\mathbf{C}$ in the figure, have size $r \times k_s$, $r \times k_r$ and $r \times r$ bits, respectively. $\mathbf{C}$ is a lower triangular matrix, which is a sufficient condition to perform systematic encoding.

Bob, who does not know in advance either the secret or the random message, must use the whole matrix $\mathbf{H}$ to perform decoding. Eve is in the same condition, although she receives the signal through a different channel. Frank, instead, can take advantage of the perfect knowledge of M, and only needs to recover the random message R. Therefore, he can precompute $\mathbf{A} \cdot M^T = \mathbf{s}$, were ^{T} denotes transposition. Then, he can use the following reduced parity-check system to look for the vector $[R|P]$ having syndrome $\mathbf{s}$:

$$[\mathbf{B}|\mathbf{C}] \cdot [R|P]^T = \mathbf{H}' \cdot \mathbf{c}'^T = \mathbf{s}. \tag{4.5}$$

Obviously, decoding for a vector having an all-zero syndrome (as usual) or a different syndrome is equivalent, due to the code linearity. Hence, Frank can perform decoding through the reduced LDPC code defined by $\mathbf{H}' = [\mathbf{B}|\mathbf{C}]$, which has rate $R_F = k_r/(k_r + r)$. The code rate for Bob and Eve instead coincides with the overall code rate, i.e., $R_c = k/n$. Through simple arithmetic, we find

$$R_F = \frac{R_c - R_s}{1 - R_s}. \tag{4.6}$$

From (4.6) we have $\frac{R_F}{R_c} = \frac{1-\frac{R_s}{R_c}}{1-R_s}$ and, since $R_c < 1$, we have $\frac{R_F}{R_c} < 1$. Therefore, Frank's advantage of knowing the secret message M translates into his ability to work with a lower code rate with respect to Bob and Eve, i.e., with an increased error correction capability.

4.3 Asymptotic Performance

A first important benchmark is represented by the performance achievable in optimal conditions, which represents the ultimate bound we will aim at approaching when working with practical, finite length codes.

4.3.1 Ideal Codes

Let us first consider the hypothesis of working with optimal codes, i.e., codes able to reach the channel capacity. Under this hypothesis, R_c coincides with Bob's channel capacity C_B, while R_F coincides with Frank's channel capacity C_F. Moreover, since Eve and Frank experience the same channel, Eve's channel capacity is $C_E = C_F = R_F$. Therefore, the secrecy capacity can be written as $C_s = R_c - R_F$. Then, replacing R_F with the r.h.s. of (4.6), we obtain the following expression for the fractional secrecy capacity, which provides the ultimate bound on $\widetilde{R_e}$:

$$\widetilde{C_s} = \frac{C_s}{R_s} = \frac{1 - R_c}{1 - R_s}. \tag{4.7}$$

We have chosen some values of the code rate R_c of the type $1/x$ or $x/(x+1)$, with x integer, ranging between 1/5 and 4/5. For all of them, we have computed $\widetilde{C_s}$ as a function of R_s, and the results are reported in Fig. 4.3. From the figure we observe that $\widetilde{C_s}$ is a monotonically increasing function of R_s, as expected from (4.7), and it reaches 1 when the secret message rate reaches its maximum, i.e., $R_s = R_c$. Apparently, this brings us to the conclusion that we should fix $R_s = R_c$ in order to maximize $\widetilde{C_s}$ and achieve optimal performance from the secrecy standpoint. This would mean to renounce transmitting randomness to confuse the eavesdropper. However, moving on the curves of Fig. 4.3 (i.e., fixing R_c) means also varying the SNR of Eve: in particular, from (4.6) we can obtain the value of R_F associated with a couple R_s and R_c. Since we are considering rates coincident with capacities, the value of R_F corresponds to a capacity of the Eve's channel and therefore to a specific SNR value,

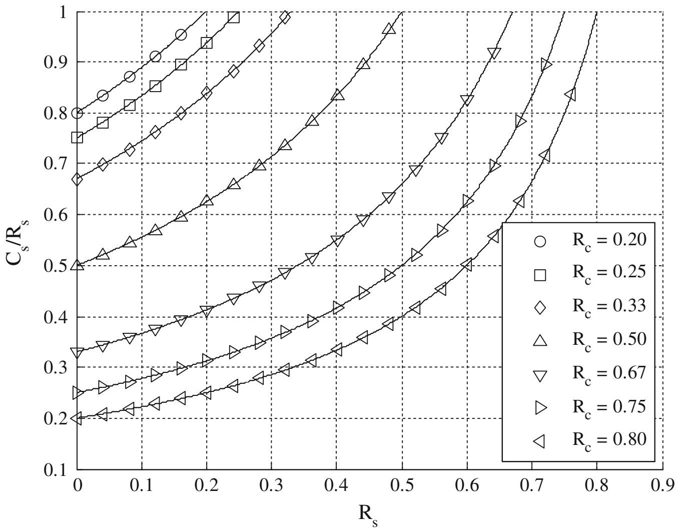


Fig. 4.3 $\widetilde{C_s}$ versus secret message rate (R_s) for some values of the code rate (R_c), under the hypothesis of ideal (capacity achieving) coding

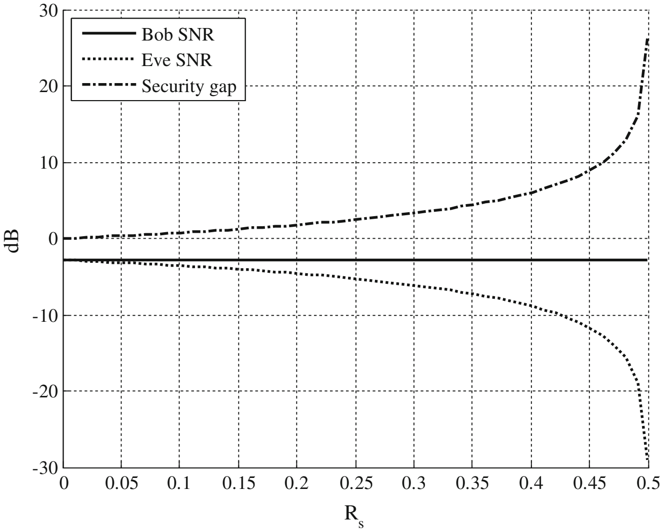


Fig. 4.4 Bob's and Eve's channels SNR and their ratio (security gap) versus secret message rate (R_s) for $R_c = 0.5$, under the hypothesis of ideal (capacity achieving) coding

through the binary input additive white Gaussian noise (BIAWGN) channel capacity (4.1). As $R_s \rightarrow R_c$ we have that Eve's SNR tends to zero (as R_F tends to zero, too). This trend is shown in Fig. 4.4, where we fix $R_c = 0.5$ and plot the Bob's and Eve's channels SNR under the hypothesis of ideal coding, for varying R_s. In the figure we also report the value of the security gap. As expected, while the SNR of Bob's channel is fixed (as the code rate), when R_s approaches R_c the SNR of Eve's channel converges to zero and the security gap diverges. Therefore, in order to have non-zero Eve's SNR and a finite security gap we must consider $R_s < R_c$, and this requires the use of randomness. However, the choice of a value of R_s not too small compared to R_c is obliged in order to achieve high values of $\widetilde{C_s}$.

4.3.2 Infinite Length LDPC Codes

Another valuable assessment in the asymptotic regime can be done by taking into account the specific LDPC code structure. In fact, any LDPC code can be represented through a Tanner graph, that is a bipartite graph having two groups of nodes, variable and check nodes, corresponding to the codeword bits and the parity-check equations, respectively. An edge exists between the jth variable node and the ith check node if and only if the (i, j)th element of $\mathbf{H}$ is 1. The number of edges connected to a node is called the degree of that node. The code Tanner graph can hence be described through the following two polynomials, which define the variable and check node degree distributions:

$$\lambda(x) = \sum_{i=2}^{d_v} \lambda_i x^{i-1}, \qquad \rho(x) = \sum_{j=2}^{d_c} \rho_j x^{j-1}. \tag{4.8}$$

In (4.8), d_v and d_c are the maximum variable and check node degrees, respectively, and the coefficient λ_i $\left(\rho_j\right)$ is the fraction of edges connected to the variable (check) nodes with degree i (j). For this reason, we say that these two polynomials describe the degree distributions from the edge perspective. Alternatively, $\lambda(x)$ can be converted into the polynomial $\nu(x) = \sum_{i=1}^{d_v} \nu_i x^i$, which describes the same distribution from the node perspective. The coefficients ν_i and λ_i are related as follows:

$$\begin{aligned} \nu_i &= \frac{\lambda_i / i}{\sum_{j=1}^{d_v} \lambda_j / j}, \\ \lambda_i &= \frac{\nu_i \cdot i}{\sum_{j=1}^{d_v} \nu_j \cdot j}. \end{aligned} \tag{4.9}$$

The same procedure can be applied to the polynomial $\rho(x)$ to obtain another polynomial, $c(x)$, which represents the same distribution from the node perspective. The code rate can be computed starting from $\lambda(x)$ and $\rho(x)$ as:

$$R_c = 1 - \frac{\sum_{i=2}^{d_v} \rho_i / i}{\sum_{j=2}^{d_c} \lambda_j / j}. \tag{4.10}$$

Efficient, low complexity LDPC code decoding algorithms are based on the belief propagation principle, which exploits an iterated exchange between the nodes of the code Tanner graph of soft messages concerning the reliability of each received bit. Therefore, the Tanner graph node degree distributions determine the performance of an LDPC code under belief propagation decoding. The density evolution technique [20] allows to estimate the performance achievable in the asymptotic regime (i.e., under the hypothesis of infinite length codes with Tanner graphs free of closed loops), under belief propagation decoding, by an LDPC code described through its degree distribution pair $(\lambda(x), \rho(x))$. In short, the method consists of computing the statistics of the decoder messages and their evolution during the iterations of the decoding algorithm, in such a way as to estimate the probability that decoding converges to an error-free codeword. Using a Gaussian approximation for the probability distributions of the decoder messages has been shown as a good solution to reduce the computational complexity without losing accuracy [8]. Through density evolution, a channel quality threshold can be found, above which the code is expected to converge to error-free estimations in asymptotic conditions. When we deal with AWGN channels, as in our case, such threshold is expressed in terms of an SNR value. Density evolution can also be used to optimize the code degree distributions, that is, to find degree distribution pairs able to achieve minimum values of the channel threshold.

Differently from classical transmission problems, in the considered setting we have a code chosen by Alice which is used by three receivers: Bob, Eve and Frank. In particular, Bob and Eve use the same code, defined by $\mathbf{H}$, while Frank uses the code defined by $\mathbf{H}'$, according to (4.5). Since we want both Bob and Frank to achieve good performance, we need to optimize both $\mathbf{H}$ and $\mathbf{H}'$. These two codes have different rate, and the second parity-check matrix is somehow contained in the first one. This is quite a new and challenging code optimization problem, which can be faced through a density evolution-based joint optimization of the two codes, as done in [4]. In this chapter, instead, for the sake of simplicity we follow a greedy approach, that is, we first optimize the smallest code, defined by $\mathbf{H}'$, and then, having fixed its degree distributions, we optimize the largest code, defined by $\mathbf{H}$, in an incremental way. In the next section we provide an example of optimization and compare the asymptotic performance with that achievable in the finite code length regime.

4.4 Finite Length Performance

Based on the analysis developed in the previous sections, we can estimate the reliability and security performance achievable by some finite length LDPC codes, and compare it with that achievable in asymptotic conditions.

For this purpose, we first choose the code rate R_c and the secret message rate R_s. Given their values, we need to find an optimized degree distribution pair for both Bob's and Frank's codes. This must be done by taking into account that Frank's code parity-check matrix is contained in Bob's code parity-check matrix, according to Fig. 4.2. Then, the value n of Bob's code length is fixed, and Frank's code length follows as $n' = (1 - R_s)n$. Given the two codes length and rate, as well as their optimized degree distributions, we can design their parity-check matrices through the Progressive Edge Growth (PEG) algorithm [11].

The performance achieved by these two codes can then be assessed through numerical simulations. In particular, we can fix two target values for Bob's and Frank's CER (ζ and η, respectively), and estimate the limit SNR, in terms of $\frac{E_b}{N_0}$, which is needed on the two channels in order to achieve the target CERs.

Let us consider, as an example, the following choice of the code parameters:

- $R_c = 0.5$
- $R_s = 0.4$
- $R_F = 0.16667$
- $n = 10{,}000$ or $n = 50{,}000$

In order to find good distribution pairs for both Bob and Frank, we use the greedy approach described in the previous section, with some heuristics in order to ensure that both distributions have good asymptotic thresholds but are also practically feasible through the PEG algorithm (in the sense that it succeeds in allocating all the edges without introducing short closed loops in the associated Tanner graphs). For the latter purpose, we also aim at keeping the average variable node degree in Frank's distribution below 4, since we have verified that this allows to achieve practical codes with better performance than by using higher average degrees. This way, for Frank's code we have obtained the following degree distributions (from the node perspective):

$$\begin{cases} v(x) = 0.1268x^6 + 0.186x^3 + 0.6872x^2, \\ c(x) = 0.2382x^4 + 0.7682x^3, \end{cases} \tag{4.11}$$

which correspond to a density evolution threshold equal to $\frac{E_b}{N_0} = -0.32\,\text{dB}$. Bob's degree distribution has been obtained starting from Frank's distribution and adding only degree-3 variable nodes, which has resulted to be a simple and efficient solution. This way, for Bob we obtain the following degree distributions (from the node perspective):

$$\begin{cases} v(x) = 0.07608x^6 + 0.5116x^3 + 0.41232x^2, \\ c(x) = 0.63184x^6 + 0.36816x^5, \end{cases} \tag{4.12}$$

corresponding to a density evolution threshold equal to $\frac{E_b}{N_0} = 1.1\,\text{dB}$.

Starting from these distributions, and using the PEG algorithm, we design Frank's and Bob's code parity-check matrices with ($n = 10{,}000, n' = 6{,}000$) and ($n = 50{,}000, n' = 30{,}000$). Through Montecarlo simulations of transmission over the AWGN channel with binary phase shift keying (BPSK), we estimate the value of $\frac{E_b}{N_0}$ which is needed to reach $\zeta = \eta = 10^{-2}$ when these codes are used. These $\frac{E_b}{N_0}$ values allow us to assess the performance in terms of reliability and security both in asymptotic and in finite code length conditions.

Table 4.1 Performance ($\frac{E_b}{N_0}$ in dB and $\widetilde{C_s}$ or $\widetilde{R_e^*}$ in bit/s/Hz) achieved in ideal, asymptotic and finite length conditions by Frank and Bob in the considered setting ($R_c = 0.5$, $R_s = 0.4$, $R_F = 0.16667$, $\zeta = \eta = 10^{-2}$)

Condition	Frank's $\frac{E_b}{N_0}$	Bob's $\frac{E_b}{N_0}$	$\widetilde{C_s}$ or $\widetilde{R_e^*}$
Ideal	−1.07	0.19	$\widetilde{C_s} = 0.83$
$n \to \infty$	−0.32	0.85	$\widetilde{R_e^*} = 0.77$
$n = 50{,}000$	0.4	1.05	$\widetilde{R_e^*} = 0.69$
$n = 10{,}000$	0.8	1.3	$\widetilde{R_e^*} = 0.65$

The results obtained are reported in Table 4.1, where we provide the estimated $\frac{E_b}{N_0}$ values for Bob and Frank. The corresponding values of SNR per codeword bit can be simply obtained by multiplying them by R_c and R_F, respectively. We remind that the SNR per codeword bit of Frank's and Eve's channels is the same by definition. In the table we first consider the ideal condition, that is, when both Frank's and Bob's codes are ideal and achieve capacity. For this case, besides the $\frac{E_b}{N_0}$ values, we provide the value of $\widetilde{C_s}$, computed according to (4.7). The other rows of the table instead consider LDPC codes: first in asymptotic conditions (based on density evolution), and then in the finite code length regime. For these cases, besides the $\frac{E_b}{N_0}$ values, we provide the value of $\widetilde{R_e^*} = R_e^*/R_s$, where R_e^* is computed according to (4.4).

From these results we observe that the considered code parameters do not allow to achieve perfect secrecy, as expected, since all the values in the last column of the table are below one. On the other hand, under the hypothesis of infinite length LDPC codes, a fractional equivocation rate ≥ 0.77 is reached, which is not far from the fractional secrecy capacity limit (0.83) corresponding to the case of ideal coding. Using finite length LDPC codes yields some further losses, as expected. However, if we use codes with length $n = 50{,}000$ bits, for the considered parameters we achieve a fractional equivocation rate ≥ 0.69, which means that about 70 % or more of the secret message bits are actually secret from an information theoretic standpoint. This is a useful measure, which tells us that we have a *practical coding loss* of about 30 % on the uncertainty (and hence the security level) of each transmitted message.

4.5 Conclusion

We have addressed the problem of assessing the reliability and security performance of practical coded transmissions over the AWGN wiretap channel. Differently from most previous analyses, which work in the asymptotic (i.e., infinite code length) regime, we have focused on the finite code length regime, and also taken into account the specific code structure. For this purpose, we have resorted to an information theoretic measure of secrecy which advocates Wyner's definition of perfect secrecy, and is also applicable in the finite code length regime.

This has permitted us to estimate the performance achievable by practical, finite length LDPC coded transmissions and to compare it with the ultimate limits achievable in ideal and asymptotic conditions. This tool has permitted us to show that practical coded transmissions incur in a practical coding loss which prevents them from achieving the ultimate performance limits.

Acknowledgments This work was supported in part by the MIUR project "ESCAPADE" (Grant RBFR105NLC) under the "FIRB—Futuro in Ricerca 2010" funding program.

References

1. Andersson M, Rathi V, Thobaben R, Kliewer J, Skoglund M (2010) Equivocation of Eve using two edge type LDPC codes for the binary erasure wiretap channel. In: Proceedings of the 44th Asilomar conference on signals, systems and computers, Pacific Grove, California, pp 2045–2049
2. Baldi M, Bianchi M, Chiaraluce F (2012) Coding with scrambling, concatenation, and HARQ for the AWGN wire-tap channel: a security gap analysis. IEEE Trans Inf Forensics Secur 7(3):883–894
3. Baldi M, Chiaraluce F, Laurenti N, Tomasin S, Renna F (2014) Secrecy transmission on parallel channels: theoretical limits and performance of practical codes. IEEE Trans Inf Forensics Secur 9(11):1765–1779
4. Baldi M, Ricciutelli G, Maturo N, Chiaraluce F (2015) Performance assessment and design of finite length LDPC codes for the Gaussian wiretap channel. In: Proceedings of IEEE ICC 2015—workshop on wireless physical layer security, London, United Kingdom, pp 446–451
5. Bellare M, Tessaro S, Vardy A (2012) Semantic security for the wiretap channel. In: Safavi-Naini R, Canetti R (eds) Advances in cryptology—CRYPTO 2012, vol 7417, Lecture Notes in Computer Science, Springer, Berlin, pp 294–311
6. Bloch M, Barros J (2011) Physical-layer security: from information theory to security engineering, 1st edn. Cambridge University Press, Cambridge
7. Cheraghchi M, Didier F, Shokrollahi A (2012) Invertible extractors and wiretap protocols. IEEE Trans Inf Theory 58(2):1254–1274
8. Chung SY, Richardson TJ, Urbanke RL (2001) Analysis of sum-product decoding of low-density parity-check codes using a Gaussian approximation. IEEE Trans Inf Theory 47(2):657–670
9. Şaşoğlu E, Vardy A (2013) A new polar coding scheme for strong security on wiretap channels. In: Proceedings of IEEE international symposium on information theory, Istanbul, Turkey, pp 1117–1121
10. Harrison WK, Almeida J, Bloch MR, McLaughlin SW, Barros J (2013) Coding for secrecy. IEEE Signal Process Mag 30(5):41–50
11. Hu XY, Eleftheriou E, Arnold DM (2001) Progressiveedge-growth Tanner graphs. In: Proceedings of IEEE global telecommunication conference (GLOBECOM'01), San Antonio, Texas, pp 995–1001
12. Klinc D, Ha J, McLaughlin S, Barros J, Kwak BJ (2011) LDPC codes for the Gaussian wiretap channel. IEEE Trans Inf Forensics Secur 6(3):532–540
13. Koyluoglu OO, El Gamal H (2010) Polar coding for secure transmission and key agreement. In: Proceedings of IEEE international symposium on personal, indoor, and mobile radio communications (PIMRC 2010), Istanbul, Turkey, pp 2698–2073
14. Leung-Yan-Cheong S, Hellman M (1978) The Gaussian wire-tap channel. IEEE Trans Inf Theory 24(4):451–456

15. Liang Y, Poor HV, Shamai (Shitz) S (2008) Information theoretic security. Found Trends Commun Inf Theory **5**(4–5):355–580
16. Liu R, Liang Y, Poor HV, Spasojević P (2007) Secure nested codes for type II wiretap channels. In: Proceedings of IEEE information theory workshop, Lake Tahoe, California, pp 337–342
17. Mahdavifar H, Vardy A (2010) Achieving the secrecy capacity of wiretap channels using polar codes. In: Proceedings of IEEE international symposium on information theory, Austin, Texas, pp 913–917
18. Rathi V, Andersson M, Thobaben R, Kliewer J, Skoglund M (2009) Two edge type LDPC codes for the wiretap channel. In: Proceedings of 43rd Asilomar conference on signals, systems and computers, Pacific Grove, California, pp 834–838
19. Rathi V, Urbanke R, Andersson M, Skoglund M (2011) Rate-equivocation optimal spatially coupled LDPC codes for the BEC wiretap channel. In: Proceedings of IEEE international symposium on information theory, St. Petersburg, Russia, pp 2393–2397
20. Richardson TJ, Urbanke RL (2001) The capacity of low-density parity-check codes under message-passing decoding. IEEE Trans Inf Theory 47(2):599–618
21. Subramanian A, Thangaraj A, Bloch M, McLaughlin SW (2011) Strong secrecy on the binary erasure wiretap channel using large-girth LDPC codes. IEEE Trans Inf Forensics Secur 6(3):585–594
22. Thangaraj A, Dihidar S, Calderbank A, McLaughlin S, Merolla JM (2007) Applications of LDPC codes to the wiretap channel. IEEE Trans Inf Theory 53(8):2933–2945
23. Wong CW, Wong TF, Shea JM (2011) LDPC code design for the BPSK-constrained Gaussian wiretap channel. In: Proceedings of IEEE global telecommunication conference (GLOBECOM'11), Houston, Texas, pp 898–902
24. Wong CW, Wong TF, Shea JM (2011) Secret-sharing LDPC codes for the BPSK-constrained Gaussian wiretap channel. IEEE Trans Inf Forensics Secur 6(3):551–564
25. Wyner AD (1975) The wire-tap channel. Bell Syst Tech J 54(8):1355–1387

Chapter 5
Broadcast Channels with Confidential Messages: Channel Uncertainty, Robustness, and Continuity

Rafael F. Schaefer, Andrea Grigorescu, Holger Boche and H. Vincent Poor

Abstract The *broadcast channel with confidential messages (BCC)* models the communication scenario in which a transmitter sends simultaneously common and confidential information to two receivers. The common information must be received by both receivers while the confidential information is designated for one receiver only and must be secured against the other one. The performance of this system is usually characterized by its secrecy capacity region determining the maximum transmission rates. In this chapter, the issue of whether this secrecy capacity region depends *continuously* on the system parameters or not is examined. In particular, this is done for *compound channels*, in which the users know only that the true channel realization is constant for the whole duration of transmission and this comes from a pre-specified uncertainty set. The secrecy capacity region of the compound BCC is shown to be robust in the sense that it is a continuous function of the uncertainty set. This means that small variations in the uncertainty set result in small variations in secrecy capacity.

R.F. Schaefer (✉) · H.V. Poor
Department of Electrical Engineering, Princeton University, Princeton, NJ 08544, USA
e-mail: rafaelfs@princeton.edu

H.V. Poor
e-mail: poor@princeton.edu

A. Grigorescu · H. Boche
Lehrstuhl für Theoretische Informationstechnik, Technische Universität München,
80333 Munchen, Germany
e-mail: andrea.grigorescu@tum.de

H. Boche
e-mail: boche@tum.de

M. Baldi and S. Tomasin (eds.), *Physical and Data-Link Security Techniques for Future Communication Systems*, Lecture Notes in Electrical Engineering 358, DOI 10.1007/978-3-319-23609-4_5

5.1 Introduction

Error correction and data encryption are usually strictly separated in current communication systems. While error correction is typically realized at the physical layer transforming the unreliable communication channel into a reliable bit-pipe, data encryption is done on top of that with the help of cryptographic principles. A drawback of this approach is its reliance on the assumption of insufficient computational capabilities of non-legitimate receivers.

Nowadays, *information theoretic approaches to security* are intensively discussed to complement such cryptographic techniques. By taking the properties of the noisy communication channel into account, information theoretic approaches establish reliable communication and data confidentiality jointly at the physical layer. Information theoretic security was initiated by Shannon [36] and continued by Wyner, who introduced the now-popular wiretap channel in [39]. Subsequently, this was generalized to the broadcast channel with confidential messages (BCC) by Csiszár and Körner [14]. This area of research provides a promising approach to achieve unconditional security and to embed secure communication into wireless networks. It is not surprising that it has drawn considerable attention recently; see for example [7, 22, 27, 28, 32, 40] and references therein. Accordingly, it has also been identified by operators and national agencies as a key technique for future secure communication systems [16, 18, 21].

Wireless communication systems are inherently vulnerable to eavesdropping due to the open nature of the wireless medium. Indeed, transmitted signals are received by intended users but are easily eavesdropped upon by non-legitimate receivers. These observations make the above discussed studies particularly crucial for wireless systems. However, many of the previous works lack in practical relevance as they usually assume perfect knowledge of all channels (including those to potential eavesdroppers). But practical systems will always be limited in channel state information (CSI) due to the nature of the wireless medium and estimation/feedback inaccuracy. Moreover, malevolent eavesdroppers will not share any channel information with the legitimate users making eavesdropping even harder. Accordingly, limited CSI must be assumed to ensure reliability and confidentiality.

In this chapter, the concept of *compound channels* [5, 38] is considered, which makes a first step in the direction of more realistic CSI assumptions. In this model, the actual channel realization is assumed to be unknown. The users know only that the true channel realization belongs to a known uncertainty set and that this realization remains constant for the entire duration of transmission. Secure communication over compound wiretap channels has been studied in [4, 17, 23, 26, 34, 35]. Despite all these efforts, a general single-letter characterization of the secrecy capacity remains unknown (if it exists at all). Such a description has been found only for certain special cases such as degraded channels or certain MIMO channels.

In this chapter, the *compound broadcast channel with confidential messages (BCC)* is considered. In this communication problem, a transmitter aims to send a common message to two receivers and, at the same time, a confidential message to only one of them keeping the other receiver in the dark. This channel provides a useful model for studying wireless networks involving both multicast and unicast messages, such as subscription content-delivery systems. First studies can be found in [24, 33] and, similarly to the compound wiretap channel, a general single-letter characterization of the secrecy capacity region remains unknown. Only a multi-letter description has been established so far.

The following analysis is motivated by the observation that the performance of a communication system should depend *continuously* on its system parameters. In the context of compound BCCs, this means that small variations in the uncertainty set should only lead to small variations in the secrecy capacity; i.e., that the system will be *robust* to the uncertainty. Since otherwise, if small changes would lead to dramatic losses in performance, the approach at hand will most likely not be used. Surprisingly, the question of continuity of capacities is rarely discussed. Some work for the compound wiretap channel and arbitrarily varying wiretap channel can be found in [10, 11].

The aim of this work is to extend these concepts and ideas to the compound BCC. For this purpose, the compound BCC is introduced in Sect. 5.2 and a distance concept to measure how "close" two compound BCCs are in Sect. 5.3. The main contribution of this work is then that the secrecy capacity region of the compound BCC is continuous in the uncertainty set. This shows that small variations in the uncertainty set only lead to small variations in the secrecy capacity. Finally, a concluding discussion is given in Sect. 5.4. Parts of this work have been presented before in [20].

Notation

Discrete random variables are denoted by capital letters and their realizations and ranges by lower case and script letters, respectively; all information quantities and logarithms are taken to the base 2; $\mathbb{N}$ and $\mathbb{R}_+$ denote the sets of non-negative integers and non-negative real numbers; $(0, 1)$ and $[0, 1]$ denote open and closed intervals between 0 and 1; $H(\cdot)$, $H_2(\cdot)$, $I(\cdot;\cdot)$ are the entropy, binary entropy, and mutual information, respectively; $X - Y - Z$ denotes a Markov chain of random variables X, Y, and Z in this order; the set of all probability distributions is denoted by $\mathscr{P}(\cdot)$; $\overline{\text{conv}}(\cdot)$ denotes the convex hull closure; $\|\nu - \mu\| =: \sum_{a\in\mathscr{A}} |\nu(a) - \mu(a)|$ is the total variation distance of measures μ and ν on $\mathscr{A}$; lhs =: rhs means the value of the right hand side (rhs) is assigned to the left hand side (lhs); lhs := rhs is defined accordingly.

5.2 Compound Broadcast Channels with Confidential Messages

In this section we introduce the *compound broadcast channel with confidential messages (BCC)* in which the actual channel realization is unknown to the transmitter and both receivers. They know only that this realization remains constant during the entire duration of transmission and belongs to a known uncertainty set.

5.2.1 Compound Broadcast Channels

Let $\mathscr{X}$, $\mathscr{Y}$, and $\mathscr{Z}$ be finite input and output alphabets of the transmitter and both receivers respectively. Let $\mathscr{S}$ be a finite state set. For each channel state $s \in \mathscr{S}$, input and output sequences $x^n \in \mathscr{X}^n$, $y^n \in \mathscr{Y}^n$, and $z^n \in \mathscr{Z}^n$ of length n, the discrete memoryless broadcast channel is given by $P^n_{YZ|X,s}(y^n, z^n|x^n) =: \prod_{i=1}^n P_{YZ|X,s}(y_i, z_i|x_i)$. Since there is no cooperation allowed between receiver 1 and 2, it suffices to consider the marginal channels only which are denoted by $W_s^n(y^n|x^n) =: \prod_{i=1}^n W_s(y_i|x_i)$ and $V_s^n(z^n|x^n) =: \prod_{i=1}^n V_s(z_i|x_i)$ respectively.

This allows us to define the marginal compound channels to both receivers by the families of channels for all $s \in \mathscr{S}$ as

$$\mathscr{W} =: \big\{W_s : s \in \mathscr{S}\big\} \quad \text{and} \quad \mathscr{V} =: \big\{V_s : s \in \mathscr{S}\big\}.$$

Definition 5.1 The discrete memoryless *compound broadcast channel* $\mathfrak{W}$ is given by the families of pairs of compound channels with common input as

$$\mathfrak{W} =: \big\{\mathscr{W}, \mathscr{V}\big\} = \big\{(W_s, V_s) : W_s \in \mathscr{W}, V_s \in \mathscr{V}\big\}.$$

Remark 5.1 In what follows we will call $\mathfrak{W}$ also the uncertainty set of the compound BCC. In [10, Sect. II-B] it is discussed why it is reasonable to specify the uncertainty set by the set of channel matrices $(\mathscr{W}, \mathscr{V})$ and not by the state set $\mathscr{S}$ itself. Indeed, two compound channels can be “close” in their set of channel matrices although their state sets may differ considerably.

5.2.2 Codes for Compound BCCs

In the communication problem at hand, the transmitter sends over the compound BCC simultaneously a common message M_0 to both receivers and a confidential message M_1 to receiver 1, which must be kept secret from receiver 2. The corresponding compound BCC is depicted in Fig. 5.1.

We consider a block code of arbitrary but fixed length n. Let $\mathscr{M}_0 =: \{1, \dots, M_{0,n}\}$ be the set of common messages and $\mathscr{M}_1 =: \{1, \dots, M_{1,n}\}$ the set of confidential messages. We frequently make use of the abbreviation $\mathscr{M} =: \mathscr{M}_0 \times \mathscr{M}_1$.

Definition 5.2 An $(n, M_{0,n}, M_{1,n})$-*code* for the compound BCC consists of a stochastic encoder at the transmitter

$$E\colon \mathscr{M}_0 \times \mathscr{M}_1 \to \mathscr{P}(\mathscr{X}^n), \tag{5.1}$$

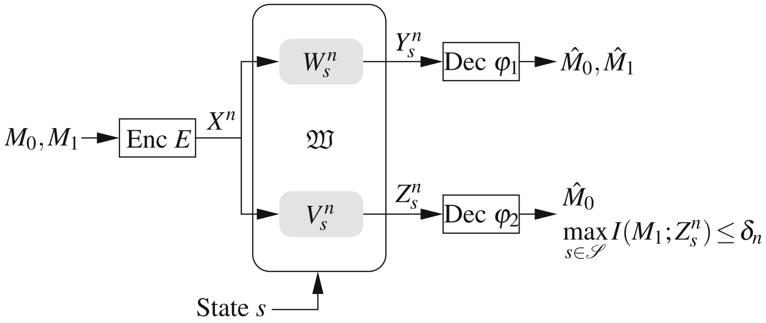


Fig. 5.1 Compound broadcast channel with confidential messages. The transmitter encodes messages M_0 and M_1 into a codeword $X^n = E(M_0, M_1)$ and transmits it over the compound BCC to the receivers, which have to decode their intended messages $(\hat{M}_0, \hat{M}_1) = \varphi_1(Y_s^n)$ and $\hat{M}_0 = \varphi_2(Z_s^n)$ for any channel realization $s \in \mathcal{S}$. At the same time, the second receiver has to be kept ignorant of M_1 in the sense that $\max_{s\in\mathcal{S}} I(M_1; Z_s^n) \leq \delta_n$

i.e., a stochastic matrix, and decoders at receivers 1 and 2

$$\varphi_1 \colon \mathcal{Y}^n \to \mathcal{M}_0 \times \mathcal{M}_1 \tag{5.2a}$$

$$\varphi_2 \colon \mathcal{Z}^n \to \mathcal{M}_0. \tag{5.2b}$$

Remark 5.2 Note that since the actual channel realization is unknown to the transmitter and both receivers, the encoder (5.1) and decoders (5.2) must not depend on the state $s \in \mathcal{S}$ (and therewith not the particular (W_s, V_s)), i.e., they must be universal with respect to the state set $\mathcal{S}$ (and uncertainty set $\mathfrak{W}$).

When the transmitter has sent the message pair $m = (m_0, m_1) \in \mathcal{M}$ and the receivers have received $y^n \in \mathcal{Y}^n$ and $z^n \in \mathcal{Z}^n$, their decoders are in error if $\varphi_1(y^n) \neq (m_0, m_1)$ or $\varphi_2(z^n) \neq m_0$. Then for an $(n, M_{0,n}, M_{1,n})$-code of Definition 5.2, the average probabilities of decoding error for receivers 1 and 2 and channel realization $s \in \mathcal{S}$ are

$$\bar{e}_{1,n}(s) := \frac{1}{|\mathcal{M}|} \sum_{m\in\mathcal{M}} \sum_{x^n\in\mathcal{X}^n} \sum_{y^n:\varphi_1(y^n)\neq(m_0,m_1)} W_s^n(y^n|x^n) E(x^n|m_0, m_1)$$

$$\bar{e}_{2,n}(s) := \frac{1}{|\mathcal{M}|} \sum_{m\in\mathcal{M}} \sum_{x^n\in\mathcal{X}^n} \sum_{z^n:\varphi_2(z^n)\neq m_0} V_s^n(z^n|x^n) E(x^n|m_0, m_1).$$

Since reliable communication is required for all $s \in \mathcal{S}$, we consider the maximum average error probabilities, i.e. $\bar{e}_{1,n} = \max_{s\in\mathcal{S}} \bar{e}_{1,n}(s)$ and $\bar{e}_{2,n} = \max_{s\in\mathcal{S}} \bar{e}_{2,n}(s)$.

The confidential message M_1 has to be kept secret from receiver 2 for all channel realizations $s \in \mathcal{S}$. Therefore, we require $\max_{s\in\mathcal{S}} I(M_1; Z_s^n) \leq \delta_n$ for some $\delta_n > 0$ with M_1 the random variable uniformly distributed over the set $\mathcal{M}_1$ and $Z_s^n = (Z_{s,1}, Z_{s,2}, \ldots, Z_{s,n})$ the output at receiver 2 for the channel realization $s \in \mathcal{S}$.

This criterion is known as *strong secrecy* [13, 29] and the intuition is to control the total amount of information leaked to the non-legitimate receiver. This leads to the following definition.

Definition 5.3 A rate pair $(R_0, R_1) \in \mathbb{R}_+^2$ is said to be *achievable* for the compound BCC if for any $\tau > 0$ there is an $n(\tau) \in \mathbb{N}$ and a sequence of $(n, M_{0,n}, M_{1,n})$-codes such that for all $n \geq n(\tau)$ we have $\frac{1}{n} \log M_{0,n} \geq R_0 - \tau, \frac{1}{n} \log M_{1,n} \geq R_1 - \tau$,

$$\max_{s \in \mathscr{S}} \left\{ \bar{e}_{1,n}(s), \bar{e}_{2,n}(s) \right\} \leq \lambda_n,$$

and

$$\max_{s \in \mathscr{S}} I(M_1; Z_s^n) \leq \delta_n \tag{5.3}$$

with $\lambda_n, \delta_n \to 0$ as $n \to \infty$.

The closure of the set of all achievable rate pairs (R_0, R_1) is the *secrecy capacity region* $\mathscr{C}_S(\mathfrak{W})$ of the compound BCC $\mathfrak{W}$.

Remark 5.3 One might argue that the secrecy criterion (5.3) should reflect the fact that the common message M_0 is available at receiver 2 as side information. In [33] it has been shown that incorporating this type of side information does not change the secrecy capacity. Accordingly, (5.3) can be generalized to $\max_{s \in \mathscr{S}} I(M_1; Z_s^n | M_0) \leq \delta_n$ (or equivalently to $\max_{s \in \mathscr{S}} I(M_1; M_0, Z_s^n) \leq \delta_n$ if M_0 and M_1 are independent) at no cost.

5.2.3 Capacity Results

The discrete memoryless compound BCC has been studied in [19, 33]. In [33] an achievable secrecy rate region and a multi-letter outer bound have been established. Based on this, [19] presents a precise multi-letter characterization of the corresponding secrecy capacity region.

Proposition 5.1 ([33, Theorem 2]) *An achievable secrecy rate region for the compound BCC $\mathfrak{W}$ is given by the set of all rate pairs $(R_0, R_1) \in \mathbb{R}_+^2$ that satisfy*

$$\begin{aligned} R_0 &\leq \min_{s \in \mathscr{S}} \min \left\{ I(U; Y_s), I(U; Z_s) \right\} \\ R_1 &\leq \min_{s \in \mathscr{S}} I(V; Y_s | U) - \max_{s \in \mathscr{S}} I(V; Z_s | U) \end{aligned}$$

for random variables $U - V - X - (Y_s, Z_s)$ forming a Markov chain with Y_s and Z_s the random variables associated with the outputs of the channels W_s and V_s.

Furthermore, the generalized secrecy criterion (cf. Remark 5.3) goes exponentially fast to zero and the decoding error of the confidential message M_1 at the non-legitimate receiver 2 goes exponentially fast to one.

A single-letter expression for the secrecy capacity region is still unknown (if it exists at all). However, a multi-letter outer bound has been established in [33, Theorem 3] which yields a multi-letter description of $\mathscr{C}_S(\mathfrak{W})$ of the compound BCC $\mathfrak{W}$ in [19]. For this purpose, let $n \in \mathbb{N}$ be arbitrary but fixed and we define the rate region $\mathscr{R}_n(\mathfrak{W}, U, V, X^n)$ as the set of all rate pairs $(R_0, R_1) \in \mathbb{R}_+^2$ that satisfy

$$R_0 \leq \frac{1}{n} \inf_{s \in \mathscr{S}} \min\big\{I(U; Y_s^n), I(U; Z_s^n)\big\} \tag{5.4a}$$

$$R_1 \leq \frac{1}{n}\big(\inf_{s \in \mathscr{S}} I(V; Y_s^n|U) - \sup_{s \in \mathscr{S}} I(V; Z_s^n|U)\big) \tag{5.4b}$$

for random variables satisfying the Markov chain relationship $U - V - X^n - (Y_s^n, Z_s^n)$. Then, we define the region

$$\overline{\mathscr{R}}_n(\mathfrak{W}) = \bigcup_{U - V - X^n} \mathscr{R}_n(\mathfrak{W}, U, V, X^n),$$

i.e., $\overline{\mathscr{R}}_n(\mathfrak{W})$ is the union of the regions $\mathscr{R}_n(\mathfrak{W}, U, V, X^n)$ over all random variables satisfying the Markov chain relationship $U - V - X^n$.

Theorem 5.1 ([19]) *The secrecy capacity region $\mathscr{C}_S(\mathfrak{W})$ of the compound BCC $\mathfrak{W}$ is the convex hull closure of the union of the regions $\overline{\mathscr{R}}_n(\mathfrak{W})$ over all $n \in \mathbb{N}$, i.e.,*

$$\mathscr{C}_S(\mathfrak{W}) = \overline{\text{conv}}\big(\bigcup_{n \in \mathbb{N}} \overline{\mathscr{R}}_n(\mathfrak{W})\big). \tag{5.5}$$

Remark 5.4 The union of the rate regions $\bigcup_{n \in \mathbb{N}} \overline{\mathscr{R}}_n(\mathfrak{W})$ may itself not be convex, which necessitates the convex hull in (5.5). Note that all rate pairs in the convex hull can be achieved by time sharing between rate pairs in $\overline{\mathscr{R}}_n(\mathfrak{W})$.

5.3 Continuity of the Compound Secrecy Capacity Region

In this section we analyze the secrecy capacity region $\mathscr{C}_S(\mathfrak{W})$ of the compound BCC $\mathfrak{W}$. The main result will be that $\mathscr{C}_S(\mathfrak{W})$ depends in a *continuous* way on the uncertainty set $\mathfrak{W}$. To do so, we need a suitable concept to measure the distance between two compound BCCs. This is introduced first.

5.3.1 Distance Between Compound BCCs

Let (W, V) and $(\widetilde{W}, \widetilde{V})$ be two broadcast channels with finite input and output alphabets $\mathscr{X}$, $\mathscr{Y}$, and $\mathscr{Z}$. We define the distance between the two marginal channels (to receivers 1 and 2 respectively) based on the total variation distance[1] as

$$d(W, \widetilde{W}) =: \max_{x\in\mathscr{X}} \sum_{y\in\mathscr{Y}} \big|W(y|x) - \widetilde{W}(y|x)\big|$$
$$d(V, \widetilde{V}) =: \max_{x\in\mathscr{X}} \sum_{z\in\mathscr{Z}} \big|V(z|x) - \widetilde{V}(z|x)\big|$$

and the distance between two BCs as

$$d\big((W, V), (\widetilde{W}, \widetilde{V})\big) =: \max\big\{d(W, \widetilde{W}), d(V, \widetilde{V})\big\}.$$

To extend this concept to compound BCs, let $\mathfrak{W}_1 = \{(W_{s_1}, V_{s_1}) : s_1 \in \mathscr{S}_1\}$ and $\mathfrak{W}_2 = \{(W_{s_2}, V_{s_2}) : s_2 \in \mathscr{S}_2\}$ be two finite compound BCs with marginal compound channels $\mathscr{W}_i = \{W_{s_i} : s_i \in \mathscr{S}_i\}$ and $\mathscr{V}_i = \{V_{s_i} : s_i \in \mathscr{S}_i\}$ for $i \in \{1, 2\}$. We define the distance between two marginal compound channels to receiver 1 as

$$d_1(\mathscr{W}_1, \mathscr{W}_2) = \max_{s_2\in\mathscr{S}_2} \min_{s_1\in\mathscr{S}_1} d(W_{s_1}, W_{s_2})$$
$$d_2(\mathscr{W}_1, \mathscr{W}_2) = \max_{s_1\in\mathscr{S}_1} \min_{s_2\in\mathscr{S}_2} d(W_{s_1}, W_{s_2})$$

and to receiver 2 as

$$d_1(\mathscr{V}_1, \mathscr{V}_2) = \max_{s_2\in\mathscr{S}_2} \min_{s_1\in\mathscr{S}_1} d(V_{s_1}, V_{s_2})$$
$$d_2(\mathscr{V}_1, \mathscr{V}_2) = \max_{s_1\in\mathscr{S}_1} \min_{s_2\in\mathscr{S}_2} d(V_{s_1}, V_{s_2}).$$

Definition 5.4 Let $\mathfrak{W}_1$ and $\mathfrak{W}_2$ be two compound BCs. The distance $D(\mathfrak{W}_1, \mathfrak{W}_2)$ between $\mathfrak{W}_1$ and $\mathfrak{W}_2$ is then defined as

$$D(\mathfrak{W}_1, \mathfrak{W}_2) = \max\big\{d_1(\mathscr{W}_1, \mathscr{W}_2), d_2(\mathscr{W}_1, \mathscr{W}_2), d_1(\mathscr{V}_1, \mathscr{V}_2), d_2(\mathscr{V}_1, \mathscr{V}_2)\big\}.$$

This concept is suitable to characterize how "close" two compound BCs are. In addition, it can also be used to quantify how well one compound BC approximates another one.

Finally, to compare different rate regions, we define a distance between two sets as follows.

[1] Note that the distance can also be defined based on another norm. This follows from the fact that the output alphabets $\mathscr{Y}$ and $\mathscr{Z}$ are finite. A norm other than the total variation distance would only result in slightly different constants.

Definition 5.5 Let $\mathscr{R}_1$, and $\mathscr{R}_2$ be two non-empty compact subsets of the metric space $(\mathbb{R}_+^2, d)$ with $d(x^2, y^2) = \sum_{i=1}^{2} |x_i - y_i|$ for all $x^2 = (x_1, x_2)$ and $y^2 = (y_1, y_2)$. We define the distance between two sets as

$$D_R(\mathscr{R}_1, \mathscr{R}_2) = \max\big\{\max_{r_1 \in \mathscr{R}_1} \min_{r_2 \in \mathscr{R}_2} d(r_1, r_2), \max_{r_2 \in \mathscr{R}_2} \min_{r_1 \in \mathscr{R}_2} d(r_1, r_2)\big\}.$$

5.3.2 *Continuity of the Secrecy Capacity Region*

Now we are in the position to study the behavior of the secrecy capacity of the compound BCC. In particular, we are interested in the question of what happens if there are variations in the uncertainty set. Obviously, one is interested in a *continuous* behavior of the secrecy capacity. Since small changes in the uncertainty set should only lead to small changes in the corresponding secrecy capacity region.

For the following analysis, we need some technical results stated in the following. Similar results appeared first in the area of quantum information theory [2, 25] and have recently been extended to the compound wiretap channel in [10, 11].

The following lemma is also stated in [10, 11].

Lemma 5.1 *Let $\mathscr{X}$ and $\mathscr{Y}$ be finite alphabets and $\varepsilon \in (0, 1)$ be arbitrary. Further, let (X, Y) and $(\tilde{X}, \tilde{Y})$ be random variables according to joint probability distributions $P_{XY}, P_{\tilde{X}\tilde{Y}} \in \mathscr{P}(\mathscr{X} \times \mathscr{Y})$ with $\|P_{XY} - P_{\tilde{X}\tilde{Y}}\| \leq \varepsilon$. It holds that*

$$\big|H(Y|X) - H(\tilde{Y}|\tilde{X})\big| \leq \delta_1(\varepsilon, |\mathscr{Y}|) \tag{5.6}$$

with $\delta_1(\varepsilon, |\mathscr{Y}|) =: 2\varepsilon \log |\mathscr{Y}| + 2H_2(\varepsilon)$.

Proof The proof follows the idea of [2] for quantum sources. We obtain sharper constants by considering classical probability distributions only in this work. For completeness, the details can be found in the appendix. □

Lemma 5.2 *Let $\mathscr{X}$ and $\mathscr{Y}$ be finite alphabets and $W, \widetilde{W} : \mathscr{X} \to \mathscr{P}(\mathscr{Y})$ be arbitrary channels with*

$$d(W, \widetilde{W}) \leq \varepsilon$$

for some $\varepsilon > 0$. For an arbitrary $n \in \mathbb{N}$, let $\mathscr{U}$ and $\mathscr{V}$ be two finite sets, $P_U \in \mathscr{P}(\mathscr{U})$ the uniform distribution of U, $P_{V|U} : \mathscr{U} \to \mathscr{P}(\mathscr{V})$ the conditional distribution of V given U and $E(x^n|v)$, $x^n \in \mathscr{X}^n$ conditioned on $v \in \mathscr{V}$, an arbitrary stochastic encoder. We consider the probability distributions

$$P_{UVY^n}(u, v, y^n) = \sum_{x^n \in \mathscr{X}^n} W^n(y^n|x^n) E(x^n|v) P_{V|U}(v|u) P_U(u)$$

$$P_{UV\tilde{Y}^n}(u, v, y^n) = \sum_{x^n \in \mathscr{X}^n} \widetilde{W}^n(y^n|x^n) E(x^n|v) P_{V|U}(v|u) P_U(u).$$

Then it holds that

$$\left|I(V;Y^n|U)-I(V;\tilde{Y}^n|U)\right|\leq n\delta_2(\varepsilon,|\mathscr{Y}|) \tag{5.7}$$

with $\delta_2(\varepsilon,|\mathscr{Y}|)=:4\varepsilon\log|\mathscr{Y}|+4H_2(\varepsilon)$.

Proof The proof is an adaptation of the proof in [10, 11] for the compound wiretap channel (which itself goes back to a proof idea in [25] for quantum capacities). The details can be found in the appendix. □

Remark 5.5 Note that the right-hand side of (5.6) and (5.7) depend only on the size of the output alphabet $\mathscr{Y}$, but they are independent of the size of the auxiliary alphabets $\mathscr{U}$ and $\mathscr{V}$, the conditional distribution $P_{V|U}$, and the chosen stochastic encoder E.

The previous lemma shows that whenever two channels are close, certain conditional mutual information terms are close as well. We use this observation to prove the following result which states that two similar compound BCCs have similar corresponding secrecy rate regions, cf. (5.4).

Lemma 5.3 *Let* $\varepsilon\in(0,1)$ *and* $n\in\mathbb{N}$ *be fixed. Further, let* $\mathfrak{W}_1$ *and* $\mathfrak{W}_2$ *be two compound BCCs and* U, V, *and* X^n *be random variables satisfying the Markov chain relationship* $U-V-X^n$. *If*

$$D(\mathfrak{W}_1,\mathfrak{W}_2)\leq\varepsilon$$

then it holds that

$$D_R(\mathscr{R}_n(\mathfrak{W}_1,U,V,X^n),\mathscr{R}_n(\mathfrak{W}_2,U,V,X^n))\leq\delta(\varepsilon,|\mathscr{Y}|,|\mathscr{Z}|)$$

with $\delta(\varepsilon,|\mathscr{Y}|,|\mathscr{Z}|)=\delta'(\varepsilon,|\mathscr{Y}|,|\mathscr{Z}|)+\delta''(\varepsilon,|\mathscr{Y}|,|\mathscr{Z}|)$, $\delta'(\varepsilon,|\mathscr{Y}|,|\mathscr{Z}|)=:4H_2(\varepsilon)+4\varepsilon\max\{\log|\mathscr{Y}|,\log|\mathscr{Z}|\}$, *and* $\delta''(\varepsilon,|\mathscr{Y}|,|\mathscr{Z}|)=:4\varepsilon\log|\mathscr{Y}||\mathscr{Z}|+8H_2(\varepsilon)$.

Proof For any particular choice of U, V, and X^n, the rate regions $\mathscr{R}_n(\mathfrak{W}_1,U,V,X^n)$ and $\mathscr{R}_n(\mathfrak{W}_2,U,V,X^n)$ are

$$\mathscr{R}_n(\mathfrak{W}_1,U,V,X^n)=\left\{\begin{array}{l} R_{0,\mathscr{S}_1}\leq\frac{1}{n}\inf_{s_1\in\mathscr{S}_1}\min\{I(U;Y_{s_1}^n),I(U;Z_{s_1}^n)\} \\ R_{1,\mathscr{S}_1}\leq\frac{1}{n}\inf_{s_1\in\mathscr{S}_1}I(V;Y_{s_1}^n|U)-\frac{1}{n}\sup_{s_1\in\mathscr{S}_1}I(V;Z_{s_1}^n|U)\end{array}\right\}$$

and

$$\mathscr{R}_n(\mathfrak{W}_2,U,V,X^n)=\left\{\begin{array}{l} R_{0,\mathscr{S}_2}\leq\frac{1}{n}\inf_{s_2\in\mathscr{S}_2}\min\{I(U;Y_{s_2}^n),I(U;Z_{s_2}^n)\} \\ R_{1,\mathscr{S}_2}\leq\frac{1}{n}\inf_{s_2\in\mathscr{S}_2}I(V;Y_{s_2}^n|U)-\frac{1}{n}\sup_{s_2\in\mathscr{S}_2}I(V;Z_{s_2}^n|U)\end{array}\right\},$$

i.e., they are rectangles described by the rates $(R_{0,\mathscr{S}_1},R_{1,\mathscr{S}_1})$ and $(R_{0,\mathscr{S}_2},R_{1,\mathscr{S}_2})$ satisfying (5.4a) and (5.4b) respectively.

Note that both regions are rectangles sharing the corner point (0, 0). Therefore, the longest distance between these two sets is given by the maximum corner points $(A_{0_{\mathscr{S}_1}}, A_{1_{\mathscr{S}_1}})$ and $(A_{0_{\mathscr{S}_2}}, A_{1_{\mathscr{S}_2}})$, where

$$A_{0_{\mathscr{S}_i}} = \max_{(R_{0,\mathscr{S}_i}, R_{1,\mathscr{S}_i}) \in \mathscr{R}_n(\mathfrak{W}_i, U, V, X^n)} R_{0,\mathscr{S}_i}$$

denotes the maximum common rate and

$$A_{1_{\mathscr{S}_i}} = \max_{(R_{0,\mathscr{S}_i}, R_{1,\mathscr{S}_i}) \in \mathscr{R}_n(\mathfrak{W}_i, U, V, X^n)} R_{1,\mathscr{S}_i}$$

the maximum confidential rate of region $\mathscr{R}_n(\mathfrak{W}_i, U, V, X^n)$, $i = 1, 2$. With this observation, the distance $D_R(\mathscr{R}_n(\mathfrak{W}_1, U, V, X^n), \mathscr{R}_n(\mathfrak{W}_2, U, V, X^n))$, cf. Definition 5.5, is

$$D_R(\mathscr{R}_n(\mathfrak{W}_1, U, V, X^n), \mathscr{R}_n(\mathfrak{W}_2, U, V, X^n)) = |A_{0_{\mathscr{S}_1}} - A_{0_{\mathscr{S}_2}}| + |A_{1_{\mathscr{S}_1}} - A_{1_{\mathscr{S}_2}}|. \tag{5.8}$$

Thus, it remains to evaluate both terms on the right hand side of (5.8), i.e., the difference between the maximum common rates $|A_{0_{\mathscr{S}_1}} - A_{0_{\mathscr{S}_2}}|$ and the difference between the maximum confidential rates $|A_{1_{\mathscr{S}_1}} - A_{1_{\mathscr{S}_2}}|$.

Common Message Rate

From (5.4a) we see that there are four cases that may occur:

1. $A_{0_{\mathscr{S}_1}} = \frac{1}{n} \inf_{s_1 \in \mathscr{S}_1} I(U; Y_{s_1}^n)$ and $A_{0_{\mathscr{S}_2}} = \frac{1}{n} \inf_{s_2 \in \mathscr{S}_2} I(U; Y_{s_2}^n)$
2. $A_{0_{\mathscr{S}_1}} = \frac{1}{n} \inf_{s_1 \in \mathscr{S}_1} I(U; Z_{s_1}^n)$ and $A_{0_{\mathscr{S}_2}} = \frac{1}{n} \inf_{s_2 \in \mathscr{S}_2} I(U; Z_{s_2}^n)$
3. $A_{0_{\mathscr{S}_1}} = \frac{1}{n} \inf_{s_1 \in \mathscr{S}_1} I(U; Y_{s_1}^n)$ and $A_{0_{\mathscr{S}_2}} = \frac{1}{n} \inf_{s_2 \in \mathscr{S}_2} I(U; Z_{s_2}^n)$
4. $A_{0_{\mathscr{S}_1}} = \frac{1}{n} \inf_{s_1 \in \mathscr{S}_1} I(U; Z_{s_1}^n)$ and $A_{0_{\mathscr{S}_2}} = \frac{1}{n} \inf_{s_2 \in \mathscr{S}_2} I(U; Y_{s_2}^n)$.

In the following we treat these cases individually. For the first case, we have

$$\left|A_{0_{\mathscr{S}_1}} - A_{0_{\mathscr{S}_2}}\right| = \left|\frac{1}{n} \inf_{s_1 \in \mathscr{S}_1} I(U; Y_{s_1}^n) - \frac{1}{n} \inf_{s_2 \in \mathscr{S}_2} I(U; Y_{s_2}^n)\right|. \tag{5.9}$$

Let $\eta > 0$ be arbitrary. There exists an $\hat{s}_1 = \hat{s}_1(\eta)$ such that

$$\inf_{s_1 \in \mathscr{S}_1} I(U; Y_{s_1}^n) \geq I(U; Y_{\hat{s}_1}^n) - \eta. \tag{5.10}$$

Since $D(\mathfrak{W}_1, \mathfrak{W}_2) < \varepsilon$, there is an $\hat{s}_2 = \hat{s}_2(\hat{s}_1)$ such that

$$d(W_{\hat{s}_1}, W_{\hat{s}_2}) < \varepsilon. \tag{5.11}$$

We can now apply Lemma 5.2 (with U in (5.7) of Lemma 5.2 being constant and U in (5.9) taking the role of V in (5.7) of Lemma 5.2). By (5.11), we then have

$$\Big|I(U;Y_{\hat{s}_1}^n)-I(U;Y_{\hat{s}_2}^n)\Big|\leq n\delta_2(\varepsilon,|\mathscr{Y}|). \tag{5.12}$$

Combining (5.10) and (5.12) we obtain

$$\begin{aligned}\inf_{s_1\in\mathscr{S}_1} I(U;Y_{s_1}^n) &\geq I(U;Y_{\hat{s}_2}^n)-n\delta_2(\varepsilon,|\mathscr{Y}|)-\eta\\ &\geq \inf_{s_2\in\mathscr{S}_2} I(U;Y_{s_2}^n)-n\delta_2(\varepsilon,|\mathscr{Y}|)-\eta.\end{aligned}$$

Since this inequality holds for all $\eta>0$, we obtain

$$\inf_{s_1\in\mathscr{S}_1} I(U;Y_{s_1}^n) > \inf_{s_2\in\mathscr{S}_2} I(U;Y_{s_2}^n)-n\delta_2(\varepsilon,|\mathscr{Y}|).$$

By changing the roles of $\mathscr{S}_1$ and $\mathscr{S}_2$ in the previous derivation, we also get $\inf_{s_2\in\mathscr{S}_2} I(U;Y_{s_2}^n) > \inf_{s_1\in\mathscr{S}_1} I(U;Y_{s_1}^n)-n\delta_2(\varepsilon,|\mathscr{Y}|)$ so that

$$\Big|\inf_{s_1\in\mathscr{S}_1} I(U;Y_{s_1}^n)-\inf_{s_2\in\mathscr{S}_2} I(U;Y_{s_2}^n)\Big|\leq n\delta_2(\varepsilon,|\mathscr{Y}|).$$

Using the same line of argument as for the first case above, we accordingly have for the second case

$$\Big|\inf_{s_1\in\mathscr{S}_1} I(U;Z_{s_1}^n)-\inf_{s_2\in\mathscr{S}_2} I(U;Z_{s_2}^n)\Big|\leq n\delta_2(\varepsilon,|\mathscr{Z}|).$$

In the third and fourth case, one maximum common rate depends on Y and the other on Z. For the third case, we have

$$\begin{aligned}B_{0_{\mathscr{S}_1}} &= \frac{1}{n}\inf_{s_1\in\mathscr{S}_1} I(U;Z_{s_1}^n)\geq\frac{1}{n}\inf_{s_1\in\mathscr{S}_1} I(U;Y_{s_1}^n)=A_{0_{\mathscr{S}_1}}\\ B_{0_{\mathscr{S}_2}} &= \frac{1}{n}\inf_{s_2\in\mathscr{S}_2} I(U;Y_{s_2}^n)\geq\frac{1}{n}\inf_{s_2\in\mathscr{S}_2} I(U;Z_{s_2}^n)=A_{0_{\mathscr{S}_2}}.\end{aligned}$$

This necessitates further case studies and we have six possibilities to relate the two previous inequalities:

1. $B_{0_{\mathscr{S}_1}}\geq A_{0_{\mathscr{S}_1}}\geq B_{0_{\mathscr{S}_2}}\geq A_{0_{\mathscr{S}_2}}$ and Lemma 5.2 implies

$$|A_{0_{\mathscr{S}_1}}-A_{0_{\mathscr{S}_2}}|\leq|B_{0_{\mathscr{S}_1}}-A_{0_{\mathscr{S}_2}}|\leq\delta_2(\varepsilon,|\mathscr{Z}|)$$

2. $B_{0_{\mathscr{S}_1}}\geq B_{0_{\mathscr{S}_2}}\geq A_{0_{\mathscr{S}_1}}\geq A_{0_{\mathscr{S}_2}}$ implying

$$|A_{0_{\mathscr{S}_1}} - A_{0_{\mathscr{S}_2}}| \le |B_{0_{\mathscr{S}_1}} - A_{0_{\mathscr{S}_2}}| \le \delta_2(\varepsilon, |\mathscr{Z}|)$$

3. $B_{0_{\mathscr{S}_1}} \ge B_{0_{\mathscr{S}_2}} \ge A_{0_{\mathscr{S}_2}} \ge A_{0_{\mathscr{S}_1}}$ implying

$$|A_{0_{\mathscr{S}_1}} - A_{0_{\mathscr{S}_2}}| \le |A_{0_{\mathscr{S}_1}} - B_{0_{\mathscr{S}_2}}| \le \delta_2(\varepsilon, |\mathscr{Y}|)$$

4. $B_{0_{\mathscr{S}_2}} \ge A_{0_{\mathscr{S}_2}} \ge B_{0_{\mathscr{S}_1}} \ge A_{0_{\mathscr{S}_1}}$ implying

$$|A_{0_{\mathscr{S}_1}} - A_{0_{\mathscr{S}_2}}| \le |A_{0_{\mathscr{S}_1}} - B_{0_{\mathscr{S}_2}}| \le \delta_2(\varepsilon, |\mathscr{Y}|)$$

5. $B_{0_{\mathscr{S}_2}} \ge B_{0_{\mathscr{S}_1}} \ge A_{0_{\mathscr{S}_2}} \ge A_{0_{\mathscr{S}_1}}$ implying

$$|A_{0_{\mathscr{S}_1}} - A_{0_{\mathscr{S}_2}}| \le |A_{0_{\mathscr{S}_1}} - B_{0_{\mathscr{S}_2}}| \le \delta_2(\varepsilon, |\mathscr{Y}|)$$

6. $B_{0_{\mathscr{S}_2}} \ge B_{0_{\mathscr{S}_1}} \ge A_{0_{\mathscr{S}_1}} \ge A_{0_{\mathscr{S}_2}}$ implying

$$|A_{0_{\mathscr{S}_1}} - A_{0_{\mathscr{S}_2}}| \le |A_{0_{\mathscr{S}_2}} - B_{0_{\mathscr{S}_1}}| \le \delta_2(\varepsilon, |\mathscr{Z}|).$$

We can use the same line of argument for the fourth case to bound the distance between the two maximum achievable common rates. As a conclusion, it then holds for all cases that

$$\begin{aligned}|A_{0_{\mathscr{S}_1}} - A_{0_{\mathscr{S}_2}}| &\le \max\{\delta_2(\varepsilon, |\mathscr{Y}|), \delta_2(\varepsilon, |\mathscr{Y}|)\}\\ &= 4H_2(\varepsilon) + 4\varepsilon \max\{\log|\mathscr{Y}|, \log|\mathscr{Z}|\}. \end{aligned} \tag{5.13}$$

Confidential Message Rate

It remains to evaluate the confidential message rate. Using the same line of argument as in the first case for the common message rate, we get

$$\begin{aligned}|A_{1_{\mathscr{S}_1}} - A_{1_{\mathscr{S}_2}}| &= \Big|\frac{1}{n}\inf_{s_1\in\mathscr{S}_1} I(V;Y_{s_1}^n|U) - \frac{1}{n}\sup_{s_1\in\mathscr{S}_1} I(V;Z_{s_1}^n|U)\\ &\qquad - \frac{1}{n}\inf_{s_2\in\mathscr{S}_2} I(V;Y_{s_2}^n|U) + \frac{1}{n}\sup_{s_2\in\mathscr{S}_2} I(V;Z_{s_2}^n|U)\Big|\\ &\le \frac{1}{n}\Big|\inf_{s_1\in\mathscr{S}_1} I(V;Y_{s_1}^n|U) - \inf_{s_2\in\mathscr{S}_2} I(V;Y_{s_2}^n|U)\Big|\\ &\qquad + \frac{1}{n}\Big|\inf_{s_2\in\mathscr{S}_2} I(V;Z_{s_2}^n|U) - \inf_{s_1\in\mathscr{S}_1} I(V;Z_{s_1}^n|U)\Big|\\ &\le \delta_2(\varepsilon, |\mathscr{Y}|) + \delta_2(\varepsilon, |\mathscr{Z}|)\\ &\le 4\varepsilon\log|\mathscr{Y}||\mathscr{Z}| + 8H_2(\varepsilon). \end{aligned} \tag{5.14}$$

Putting (5.13) and (5.14) together yields the desired result proving the lemma. □

Now we are in a position to state and prove the main result of this work. The following theorem shows that whenever two compound BCCs are close, their corresponding secrecy capacity regions are close as well.

Theorem 5.2 *Let* $\varepsilon \in (0, 1)$*. Let* $\mathfrak{W}_1$ *and* $\mathfrak{W}_2$ *be two compound BCCs. If*

$$D(\mathfrak{W}_1, \mathfrak{W}_2) \leq \varepsilon, \tag{5.15}$$

then it holds that

$$D_R(\mathscr{C}_S(\mathfrak{W}_1), \mathscr{C}_S(\mathfrak{W}_2)) \leq \delta(\varepsilon, |\mathscr{Y}|, |\mathscr{Z}|).$$

Proof For any choice of random variables U, V, and X^n satisfying the Markov chain relationship $U - V - X^n$, we define the sets $\mathscr{D}_1, \mathscr{B}_1 \subset \mathbb{R}_+^2$ as

$$\mathscr{D}_1 = \bigcup_{n\in\mathbb{N}} \bigcup_{U-V-X^n} \mathscr{R}_n(\mathfrak{W}_1, U, V, X^n)$$
$$\mathscr{B}_1 = \mathscr{C}_S(\mathfrak{W}_1) \backslash \bigcup_{n\in\mathbb{N}} \bigcup_{U-V-X^n} \mathscr{R}_n(\mathfrak{W}_1, U, V, X^n)$$

so that $\mathscr{D}_1 \cup \mathscr{B}_1 = \mathscr{C}_S(\mathfrak{W}_1)$. Now, let $(R_{0_{\mathscr{S}_1}}, R_{1_{\mathscr{S}_1}}) \in \mathscr{D}_1$. Then there exists an $n \in \mathbb{N}$ and random variables $\hat{U}$, $\hat{V}$, and $\hat{X^n}$ satisfying the Markov chain relationship $\hat{U} - \hat{V} - \hat{X^n}$ such that $(R_{0_{\mathscr{S}_1}}, R_{1_{\mathscr{S}_1}}) \in \mathscr{R}_n(\mathfrak{W}_1, \hat{U}, \hat{V}, \hat{X^n})$. From Lemma 5.3 and (5.15) it then follows that

$$D_R(\mathscr{R}_n(\mathfrak{W}_1, \hat{U}, \hat{V}, \hat{X^n}), \mathscr{R}_n(\mathfrak{W}_2, \hat{U}, \hat{V}, \hat{X^n})) \leq \delta(\varepsilon, |\mathscr{Y}|, |\mathscr{Z}|).$$

This means that there exists a rate pair

$$(R_{0_{\mathscr{S}_2}}(R_{0_{\mathscr{S}_1}}), R_{1_{\mathscr{S}_2}}(R_{1_{\mathscr{S}_1}})) \in \mathscr{R}_n(\mathfrak{W}_2, \hat{U}, \hat{V}, \hat{X^n})$$

such that

$$|R_{0_{\mathscr{S}_1}} - R_{0_{\mathscr{S}_2}}| + |R_{1_{\mathscr{S}_1}} - R_{1_{\mathscr{S}_2}}| \leq \delta(\varepsilon, |\mathscr{Y}|, |\mathscr{Z}|).$$

Now, for any rate pair $(\hat{R}_{0_{\mathscr{S}_1}}, \hat{R}_{1_{\mathscr{S}_1}}) \in \mathscr{B}_1$, there exist two rate pairs

$$(\dot{R}_{0_{\mathscr{S}_1}}, \dot{R}_{1_{\mathscr{S}_1}}), (\tilde{R}_{0_{\mathscr{S}_1}}, \tilde{R}_{1_{\mathscr{S}_1}}) \in \mathscr{D}_1$$

such that

$$\hat{R}_{0_{\mathscr{S}_1}} = \lambda \dot{R}_{0_{\mathscr{S}_1}} + (1-\lambda)\tilde{R}_{0_{\mathscr{S}_1}}$$
$$\hat{R}_{1_{\mathscr{S}_1}} = \lambda \dot{R}_{1_{\mathscr{S}_1}} + (1-\lambda)\tilde{R}_{1_{\mathscr{S}_1}}$$

for some $\lambda \in (0, 1)$. Now, for each $(\dot{R}_{0_{\mathscr{S}_1}}, \dot{R}_{1_{\mathscr{S}_1}})$ and $(\tilde{R}_{0_{\mathscr{S}_1}}, \tilde{R}_{1_{\mathscr{S}_1}})$ there exist random variables $\dot{U}$, $\dot{V}$, $\dot{X}^n$ $\tilde{U}$, $\tilde{V}$, and $\tilde{X^n}$ satisfying the Markov chain relations $\dot{U} - \dot{V} - \dot{X}^n$ and $\tilde{U} - \tilde{V} - \tilde{X^n}$ such that $(\dot{R}_{0_{\mathscr{S}_1}}, \dot{R}_{1_{\mathscr{S}_1}}) \in \mathscr{R}_n(\mathfrak{W}_1, \dot{U}, \dot{V}, \dot{X}^n)$ and $(\tilde{R}_{0_{\mathscr{S}_1}}, \tilde{R}_{1_{\mathscr{S}_1}}) \in \mathscr{R}_n(\mathfrak{W}_1, \tilde{U}, \tilde{V}, \tilde{X}^n)$. Then from Lemma 5.3 and (5.15) we have that there exist rate pairs $(\dot{R}_{0_{\mathscr{S}_2}}(\dot{R}_{0_{\mathscr{S}_1}}), \dot{R}_{1_{\mathscr{S}_2}}(\dot{R}_{1_{\mathscr{S}_1}})) \in \mathscr{R}_n(\mathfrak{W}_2, \dot{U}, \dot{V}, \dot{X}^n)$ and $(\tilde{R}_{0_{\mathscr{S}_2}}(\tilde{R}_{0_{\mathscr{S}_1}}), \tilde{R}_{1_{\mathscr{S}_2}}(\tilde{R}_{1_{\mathscr{S}_1}})) \in \mathscr{R}_n(\mathfrak{W}_2, \tilde{U}, \tilde{V}, \tilde{X}^n)$ such that

$$\begin{aligned}
|\dot{R}_{0_{\mathscr{S}_1}} - \dot{R}_{0_{\mathscr{S}_2}}| + |\dot{R}_{1_{\mathscr{S}_1}} - \dot{R}_{1_{\mathscr{S}_2}}| &\leq \delta(\varepsilon, |\mathscr{Y}|, |\mathscr{Z}|)\\
|\tilde{R}_{0_{\mathscr{S}_1}} - \tilde{R}_{0_{\mathscr{S}_2}}| + |\tilde{R}_{1_{\mathscr{S}_1}} - \tilde{R}_{1_{\mathscr{S}_2}}| &\leq \delta(\varepsilon, |\mathscr{Y}|, |\mathscr{Z}|).
\end{aligned}$$

This means there is a rate pair $(\hat{R}_{0_{\mathscr{S}_2}}, \hat{R}_{1_{\mathscr{S}_2}}) \in \mathscr{C}_S(\mathfrak{W}_2)$ with

$$\begin{aligned}
\hat{R}_{0_{\mathscr{S}_2}} &= \lambda \dot{R}_{0_{\mathscr{S}_2}} + (1-\lambda)\tilde{R}_{0_{\mathscr{S}_2}}\\
\hat{R}_{1_{\mathscr{S}_2}} &= \lambda \dot{R}_{1_{\mathscr{S}_2}} + (1-\lambda)\tilde{R}_{1_{\mathscr{S}_2}}.
\end{aligned}$$

In addition, we have

$$\begin{aligned}
|\hat{R}_{0_{\mathscr{S}_1}} - \hat{R}_{0_{\mathscr{S}_2}}| &= |\lambda \dot{R}_{0_{\mathscr{S}_2}} + (1-\lambda)\tilde{R}_{0_{\mathscr{S}_2}} - \lambda \dot{R}_{0_{\mathscr{S}_1}} + (1-\lambda)\tilde{R}_{0_{\mathscr{S}_1}}|\\
&\leq \lambda|\dot{R}_{0_{\mathscr{S}_1}} - \dot{R}_{0_{\mathscr{S}_2}}| + (1-\lambda)|\tilde{R}_{0_{\mathscr{S}_1}} - \tilde{R}_{0_{\mathscr{S}_2}}|\\
&\leq \delta'(\varepsilon, |\mathscr{Y}|, |\mathscr{Z}|) \qquad (5.16)
\end{aligned}$$

and similarly

$$|\hat{R}_{1_{\mathscr{S}_1}} - \hat{R}_{1_{\mathscr{S}_2}}| \leq \delta''(\varepsilon, |\mathscr{Y}|, |\mathscr{Z}|). \qquad (5.17)$$

Now (5.16) and (5.17) results in

$$|\hat{R}_{0_{\mathscr{S}_1}} - \hat{R}_{0_{\mathscr{S}_2}}| + |\hat{R}_{1_{\mathscr{S}_1}} - \hat{R}_{1_{\mathscr{S}_2}}| \leq \delta(\varepsilon, |\mathscr{Y}|, |\mathscr{Z}|).$$

Thus, we can conclude that for every rate pair $(R_{0_{\mathscr{S}_1}}, R_{1_{\mathscr{S}_1}}) \in \mathscr{C}_S(\mathfrak{W}_1)$ we can find a rate pair $(R_{0_{\mathscr{S}_2}}(R_{0_{\mathscr{S}_1}}), R_{1_{\mathscr{S}_2}}(R_{1_{\mathscr{S}_1}})) \in \mathscr{C}_S(\mathfrak{W}_2)$ such that

$$|R_{0_{\mathscr{S}_1}} - R_{0_{\mathscr{S}_2}}| + |R_{1_{\mathscr{S}_1}} - R_{1_{\mathscr{S}_2}}| \leq \delta(\varepsilon, |\mathscr{Y}|, |\mathscr{Z}|). \qquad (5.18)$$

Similarly, we can use the same line of argument to show the other direction: for every rate pair $(R_{0_{\mathscr{S}_2}}, R_{1_{\mathscr{S}_2}}) \in \mathscr{C}_S(\mathfrak{W}_2)$ there is a rate pair $(R_{0_{\mathscr{S}_1}}(R_{0_{\mathscr{S}_2}}), R_{1_{\mathscr{S}_1}}(R_{1_{\mathscr{S}_2}})) \in \mathscr{C}_S(\mathfrak{W}_1)$ such that (5.18) holds. This completes the proof. □

5.4 Discussion

This work was motivated by the question as to whether the secrecy capacity region of the compound BCC depends continuously on the uncertainty set or not. We have shown that the compound BCC model is robust, i.e., small changes in the uncertainty set lead only to small changes in the secrecy capacity region. The continuous behavior of the secrecy capacity is a necessary condition for the existence of codes that are robust against small variations in the uncertainty set, since otherwise, a discontinuous behavior of the secrecy capacity would immediately rule out the existence of robust codes. For future work, a detailed analysis of such robust codes is the next step for making this concept interesting for practical applications.

For compound channels the true channel realization is unknown. However, a crucial assumption is that it remains constant for the entire duration of transmission. Weakening this assumption leads to the concept of *arbitrarily varying channels (AVCs)* [1, 6, 15], in which the channel realization is allowed to vary in an unknown and arbitrary manner from channel use to channel use. The corresponding *arbitrarily varying wiretap channel (AVWC)* has been studied in [3, 8–12, 30, 31, 37] and interesting phenomena appear. In contrast to the compound wiretap channel, it now matters whether traditional deterministic/unassisted codes with pre-specified encoder and decoder are used, or more sophisticated codes, where the choice of encoder and decoder is coordinated based on coordination resources such as common randomness available to all users. There are situations in which the traditional approach leads to zero capacity, while the coordinated approach yields a positive capacity. Moreover, the unassisted secrecy capacity of the AVWC turns out to be discontinuous in the uncertainty set [10, 11], while common randomness allows recovering of the continuous dependence of the secrecy capacity on the uncertainty set [31, 37]. As a first step, in [19, 20] it has been demonstrated that the unassisted secrecy capacity region of the arbitrarily varying BCC depends on the uncertainty set in a discontinuous way. But it is an interesting and open question to find a complete characterization of this behavior (as in [31, 37] for the AVWC).

Acknowledgments This work of R. F. Schaefer was supported by the German Research Foundation (DFG) under Grant WY 151/2-1. This work of A. Grigorescu was supported by the German Research Foundation (DF) under Grant BO 1734/20-1. This work of H. Boche was supported by the German Ministry of Education and Research (BMBF) under Grants 01BQ1050 and 16KIS0118. This work of H. V. Poor was supported by the U.S. National Science Foundation under Grant CMMI-1435778.

Appendix

The following proofs of Lemmas 5.1 and 5.2 are adaptations of [2] and [25] where similar results were proved in the context of quantum information theory. However, we obtain bounds with better constants by restricting the analysis to classical probability distributions only.

Proof of Lemma 5.1

The proof of this lemma can also be found in [10, 11] and is given here for completeness. It follows [2] where a similar result is presented in the context of quantum information. However, we are able to get a better constant by using the fact that $H(Y|X) \geq 0$ for all $P_{XY} \in \mathscr{P}(\mathscr{X} \times \mathscr{Y})$. This is in contrast to the quantum version in [2].

Let $P_{XY}, P_{\tilde{X}\tilde{Y}} \in \mathscr{P}(\mathscr{X} \times \mathscr{Y})$ be joint probability distributions with $\|P_{XY} - P_{\tilde{X}\tilde{Y}}\| \leq \varepsilon$. We assume that

$$\sum_{x\in\mathscr{X}} \sum_{y\in\mathscr{Y}} \big|P_{XY}(x,y) - P_{\tilde{X}\tilde{Y}}(x,y)\big| = \varepsilon \tag{5.19}$$

is satisfied with equality since otherwise ε in (5.19) could be replaced with a smaller $\tilde{\varepsilon} < \varepsilon$ accordingly.

We define the function

$$f(x,y) =: \big|P_{XY}(x,y) - P_{\tilde{X}\tilde{Y}}(x,y)\big| \tag{5.20}$$

and set

$$p^*(x,y) = (1-\varepsilon)P_{XY}(x,y) + f(x,y)$$

for all $(x,y) \in \mathscr{X} \times \mathscr{Y}$ so that $p^* \in \mathscr{P}(\mathscr{X}, \mathscr{Y})$ is a joint probability distribution on $\mathscr{X} \times \mathscr{Y}$.

Further, we set

$$\hat{p}(x,y) = \frac{1}{\varepsilon} f(x,y), \tag{5.21a}$$

and

$$\hat{q}(x,y) = \frac{1}{\varepsilon}\big((1-\varepsilon)\big[P_{XY}(x,y) - P_{\tilde{X}\tilde{Y}}(x,y)\big] + f(x,y)\big). \tag{5.21b}$$

Next we check that $\hat{p}$ and $\hat{q}$ are well defined such that they are indeed probability distributions. $\hat{p}(x,y) \geq 0$ for all $(x,y) \in \mathscr{X} \times \mathscr{Y}$ is obviously true. It remains to verify that $\hat{q}(x,y) \geq 0$ for all $(x,y) \in \mathscr{X} \times \mathscr{Y}$ is also satisfied.

If $P_{XY}(x,y) \leq P_{\tilde{X}\tilde{Y}}(x,y)$, then

$$\begin{aligned} -f(x,y) &\leq P_{XY}(x,y) - P_{\tilde{X}\tilde{Y}}(x,y) \\ &\leq (1-\varepsilon)\big(P_{XY}(x,y) - P_{\tilde{X}\tilde{Y}}(x,y)\big) \\ &\leq 0 \end{aligned}$$

so that $\hat{q}(x, y) \geq 0$. On the other hand, if $P_{XY}(x, y) > P_{\tilde{X}\tilde{Y}}(x, y)$, then

$$\begin{aligned} 0 &< (1-\varepsilon)\big(P_{XY}(x, y) - P_{\tilde{X}\tilde{Y}}(x, y)\big) \\ &\leq P_{XY}(x, y) - P_{\tilde{X}\tilde{Y}}(x, y) \\ &\leq f(x, y) \end{aligned}$$

so that $\hat{q}(x, y) \geq 0$ also in this case. From the definition of $\hat{p}$ and $\hat{q}$ in (5.21) and (5.19)–(5.20) it can further easily be verified that

$$\sum_{x\in\mathscr{X}} \sum_{y\in\mathscr{Y}} \hat{p}(x, y) = \sum_{x\in\mathscr{X}} \sum_{y\in\mathscr{Y}} \hat{q}(x, y) = 1$$

which shows that $\hat{p} \in \mathscr{P}(\mathscr{X} \times \mathscr{Y})$ and $\hat{q} \in \mathscr{P}(\mathscr{X} \times \mathscr{Y})$ are joint probability distributions.

With this we can rewrite p^* as

$$\begin{aligned} p^*(x, y) &= (1-\varepsilon)P_{XY}(x, y) + \varepsilon\hat{p}(x, y) &\quad (5.22a) \\ &= (1-\varepsilon)P_{\tilde{X}\tilde{Y}}(x, y) + \varepsilon\hat{q}(x, y) &\quad (5.22b) \end{aligned}$$

for all $(x, y) \in \mathscr{X} \times \mathscr{Y}$. Next, we show that (5.22a) implies

$$\big|H(Y|X) - H(Y^*|X^*)\big| \leq \varepsilon \log|\mathscr{Y}| + H_2(\varepsilon). \tag{5.23}$$

To do so, we use the fact that the conditional entropy is concave, i.e.,

$$H(Y^*|X^*) \geq (1-\varepsilon)H(Y|X) + \varepsilon H(\hat{Y}|\hat{X}).$$

With this, we have

$$\begin{aligned} H(Y|X) - H(Y^*|X^*) &\leq H(Y|X) - (1-\varepsilon)H(Y|X) - \varepsilon H(\hat{Y}|\hat{X}) \\ &= \varepsilon\big(H(Y|X) - H(\hat{Y}|\hat{X})\big) \\ &\leq \varepsilon H(Y|X) \\ &\leq \varepsilon \log|\mathscr{Y}|. &\quad (5.24) \end{aligned}$$

Using the concavity of the entropy

$$H(X^*) \geq (1-\varepsilon)H(X) + \varepsilon H(\hat{X})$$

and the upper bound on the joint entropy

$$H(X^*, Y^*) \leq (1-\varepsilon)H(X, Y) + \varepsilon H(\hat{X}, \hat{Y}) + H_2(\varepsilon),$$

we get

$$\begin{aligned} H(Y^*|X^*) &= H(X^*, Y^*) - H(X^*) \\ &\le (1-\varepsilon)H(Y|X) + \varepsilon H(Y^*|X^*) + H_2(\varepsilon) \end{aligned}$$

and further

$$\begin{aligned} H(Y|X) - H(Y^*|X^*) &\ge -\varepsilon\big(H(Y^*|X^*) - H(Y|X)\big) - H_2(\varepsilon) \\ &\ge -\varepsilon H(Y^*|X^*) - H_2(\varepsilon) \\ &\ge -\varepsilon \log|\mathscr{Y}| - H_2(\varepsilon). \end{aligned} \tag{5.25}$$

Now, (5.24) and (5.25) yield

$$\big|H(Y|X) - H(Y^*|X^*)\big| \le \varepsilon \log|\mathscr{Y}| + H_2(\varepsilon)$$

which shows (5.23). (By the same arguments, one can show that (5.22b) implies $|H(\tilde{Y}|\tilde{X}) - H(Y^*|X^*)| \le \varepsilon \log|\mathscr{Y}| + H_2(\varepsilon)$.)

Finally, this yields

$$\begin{aligned} &\big|H(Y|X) - H(\tilde{Y}|\tilde{X})\big| \\ &\quad= \big|H(Y|X) - H(Y^*|X^*) + \big(H(Y^*|X^*) - H(\tilde{Y}|\tilde{X})\big)\big| \\ &\quad\le \big|H(Y|X) - H(Y^*|X^*)\big| + \big|H(\tilde{Y}|\tilde{X}) - H(Y^*|X^*)\big| \\ &\quad\le 2\varepsilon \log|\mathscr{Y}| + 2H_2(\varepsilon) \end{aligned}$$

which is (5.6), proving the lemma. □

Proof of Lemma 5.2

The proof presented in the following is based on [10, Lemma 2]. Let $0 \le k \le n$ be arbitrary. We define

$$P_{UVY_1^k\tilde{Y}_{k+1}^n}(u, v, y_1^k, y_{k+1}^n) =: \sum_{x^n \in \mathscr{X}^n} \prod_{l=1}^{k} W(y_l|x_l) \prod_{l=k+1}^{n} \widetilde{W}(y_l|x_l) E(x^n|v) P_{V|U}(v|u) P_U(u).$$

So we have

$$I(V; Y^n|U) - I(V; \tilde{Y}^n|U) = \sum_{k=0}^{n-1} \Big(I(V; Y_1^{k+1}\tilde{Y}_{k+2}^n|U) - I(V; Y_1^k\tilde{Y}_{k+1}^n|U)\Big).$$

For all $0 \leq k \leq n-1$ it holds that

$$\begin{aligned}
&I(V;Y_1^{k+1}\tilde{Y}_{k+2}^n|U) - I(V;Y_1^k\tilde{Y}_{k+1}^n|U)\\
&\quad= I(V;Y_1^k|U) + I(V;Y_{k+1}\tilde{Y}_{k+2}^n|Y_1^kU) - I(V;Y_1^k|U) - I(V;\tilde{Y}_{k+1}^n|Y_1^kU)\\
&\quad= I(V;Y_{k+1}\tilde{Y}_{k+2}^n|Y_1^kU) - I(V;\tilde{Y}_{k+1}^n|Y_1^kU)\\
&\quad= I(V;\tilde{Y}_{k+2}^n|Y_1^kU) + I(V;Y_{k+1}|\tilde{Y}_{k+2}^nY_1^kU)\\
&\qquad\quad - I(V;\tilde{Y}_{k+2}^n|Y_1^kU) - I(V;\tilde{Y}_{k+1}|\tilde{Y}_{k+2}^nY_1^kU)\\
&\quad= I(V;Y_{k+1}|\tilde{Y}_{k+2}^nY_1^kU) - I(V;\tilde{Y}_{k+1}|\tilde{Y}_{k+2}^nY_1^kU)\\
&\quad= H(Y_{k+1}|\tilde{Y}_{k+2}^nY_1^kU) - H(\tilde{Y}_{k+1}|\tilde{Y}_{k+2}^nY_1^kU)\\
&\qquad\quad - H(VY_{k+1}|\tilde{Y}_{k+2}^nY_1^kU) + H(V\tilde{Y}_{k+1}|\tilde{Y}_{k+2}^nY_1^kU).
\end{aligned}\tag{5.26}$$

We want to analyze the right-hand side of (5.26). For $0 \leq k \leq n-1$, it holds that

$$\begin{aligned}
&\|P_{UVY_1^{k+1}\tilde{Y}_{k+2}^n} - P_{UVY_1^k\tilde{Y}_{k+1}^n}\|\\
&\quad= \sum_{v\in\mathscr{V}}\sum_{u\in\mathscr{U}}\sum_{y^n\in\mathscr{Y}^n}\Big|P_{UVY_1^{k+1}\tilde{Y}_{k+2}^n}(u,v,y_1^{k+1}y_{k+2}^n) - P_{UVY_1^k\tilde{Y}_{k+1}^n}(u,v,y_1^ky_{k+1}^n)\Big|\\
&\quad= \sum_{v\in\mathscr{V}}\sum_{u\in\mathscr{U}}\sum_{y^n\in\mathscr{Y}^n}\Big|\sum_{x^n\in\mathscr{X}^n}\Big(\prod_{l=1}^{k+1}W(y_l|x_l)\prod_{l=k+2}^{n}\widetilde{W}(y_l|x_l)\\
&\qquad\quad - \prod_{l=1}^{k+1}W(y_l|x_l)\prod_{l=k+2}^{n}\widetilde{W}(y_l|x_l)\Big)E(x^n|v)P_{V|U}(v|u)P_U(u)\Big|\\
&\quad= \sum_{v\in\mathscr{V}}\sum_{u\in\mathscr{U}}\sum_{y^n\in\mathscr{Y}^n}\Big|\sum_{x^n\in\mathscr{X}^n}\prod_{l=1}^{k}W(y_l|x_l)\prod_{l=k+2}^{n}\widetilde{W}(y_l|x_l)\Big(W(y_{k+1}|x_{k+1})\\
&\qquad\quad - \widetilde{W}(y_{k+1}|x_{k+1})\Big)E(x^n|v)P_{V|U}(v|u)P_U(u)\Big|\\
&\quad\leq \sum_{v\in\mathscr{V}}\sum_{u\in\mathscr{U}}\sum_{y^n\in\mathscr{Y}^n}\sum_{x^n\in\mathscr{X}^n}\prod_{l=1}^{k}W(y_l|x_l)\prod_{l=k+2}^{n}\widetilde{W}(y_l|x_l)\Big|W(y_{k+1}|x_{k+1})\\
&\qquad\quad - \widetilde{W}(y_{k+1}|x_{k+1})\Big|E(x^n|v)P_{V|U}(v|u)P_U(u)\\
&\quad= \sum_{v\in\mathscr{V}}\sum_{u\in\mathscr{U}}\sum_{x^n\in\mathscr{X}^n}\Big(\sum_{y^n\in\mathscr{Y}^n}\prod_{l=1}^{k}W(y_l|x_l)\prod_{l=k+2}^{n}\widetilde{W}(y_l|x_l)\Big|W(y_{k+1}|x_{k+1})\\
&\qquad\quad - \widetilde{W}(y_{k+1}|x_{k+1})\Big|\Big)E(x^n|v)P_{V|U}(v|u)P_U(u)
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{u\in\mathscr{U}} \sum_{x^n\in\mathscr{X}^n} \sum_{y_{k+1}\in\mathscr{Y}} \Big| W(y_{k+1}|x_{k+1}) \\
&\qquad\qquad - \widetilde{W}(y_{k+1}|x_{k+1})\Big| E(x^n|v)P_{V|U}(v|u)P_U(u) \\
&< \varepsilon \sum_{v\in\mathscr{V}} \sum_{u\in\mathscr{U}} \sum_{x^n\in\mathscr{X}^n} E(x^n|v)P_{V|U}(v|u)P_U(u) = \varepsilon.
\end{aligned}
$$

This shows that the total variation between the joint probability distribution $P_{UVY^k\tilde{Y}^n_{k+1}}$ and $P_{UVY^{k+1}\tilde{Y}^n_{k+2}}$ is smaller than ε. Then by Lemma 5.1 it holds that

$$
\Big| H(Y_{k+1}|\tilde{Y}^n_{k+2}Y_1^kU) - H(\tilde{Y}_{k+1}|\tilde{Y}^n_{k+2}Y_1^kU)\Big| < 2\varepsilon\log|\mathscr{Y}| + 2H_2(\varepsilon) \tag{5.27}
$$

and

$$
\begin{aligned}
&\Big| H(VY_{k+1}|\tilde{Y}^n_{k+2}Y_1^kU) - H(V\tilde{Y}_{k+1}|\tilde{Y}^n_{k+2}Y_1^kU)\Big| \\
&\quad = \Big| H(V|\tilde{Y}^n_{k+2}Y_1^kU) + H(Y_{k+1}|V\tilde{Y}^n_{k+2}Y_1^kU) \\
&\qquad\qquad - H(V|\tilde{Y}^n_{k+2}Y_1^kU) - H(\tilde{Y}_{k+1}|V\tilde{Y}^n_{k+2}Y_1^kU)\Big| \\
&\quad = \Big| H(Y_{k+1}|V\tilde{Y}^n_{k+2}Y_1^kU) - H(\tilde{Y}_{k+1}|V\tilde{Y}^n_{k+2}Y_1^kU)\Big| \\
&\quad < 2\varepsilon\log|\mathscr{Y}| + 2H_2(\varepsilon).
\end{aligned} \tag{5.28}
$$

Inserting (5.27) and (5.28) into (5.26) we obtain

$$
\Big| I(V;Y_1^{k+1}\tilde{Y}^n_{k+2}|U) - I(V;Y_1^k\tilde{Y}^n_{k+1}|U)\Big| \le 4\varepsilon\log|\mathscr{Y}| + 4H_2(\varepsilon) := \delta_2(\varepsilon,|\mathscr{Y}|). \tag{5.29}
$$

This gives in particular the following upper bound for the difference between $I(V;Y^n|U)$ and $I(V;\tilde{Y}^n|U)$:

$$
\begin{aligned}
\Big| I(V;Y^n|U) - I(V;\tilde{Y}^n|U)\Big| &\le \sum_{k=0}^{n-1} \Big| I(V;Y_1^{k+1}\tilde{Y}^n_{k+2}|U) - I(V;Y_1^k\tilde{Y}^n_{k+1}|U)\Big| \\
&\le n\delta_2(\varepsilon,|\mathscr{Y}|)
\end{aligned}
$$

proving the lemma. □

References

1. Ahlswede R (1978) Elimination of correlation in random codes for arbitrarily varying channels. Z Wahrscheinlichkeitstheorie verw Gebiete 44:159–175
2. Alicki R, Fannes M (2004) Continuity of quantum conditional information. J Phys A: Math Gen 37(5):L55–L57
3. Bjelaković I, Boche H, Sommerfeld J (2013) Capacity results for arbitrarily varying wiretap channels. Information theory, combinatorics, and search theory. Springer, Berlin, pp 123–144
4. Bjelaković I, Boche H, Sommerfeld J (2013) Secrecy results for compound wiretap channels. Prob Inf Trans 49(1):73–98
5. Blackwell D, Breiman L, Thomasian AJ (1959) The capacity of a class of channels. Ann Math Stat 30(4):1229–1241
6. Blackwell D, Breiman L, Thomasian AJ (1960) The capacities of certain channel classes under random coding. Ann Math Stat 31(3):558–567
7. Bloch M, Barros J (2011) Physical-layer security: from information theory to security engineering. Cambridge University Press, Cambridge
8. Boche H, Schaefer RF (2013) Capacity results and super-activation for wiretap channels with active wiretappers. IEEE Trans Inf Forensics Secur 8(9):1482–1496
9. Boche H, Schaefer RF (2014) Arbitrarily varying wiretap channels with finite coordination resources. In Proceedings of IEEE international conference on communication workshops, Sydney, Australia, pp 746–751
10. Boche H, Schaefer RF, Poor HV (2014) On the continuity of the secrecy capacity of compound and arbitrarily varying wiretap channels. IEEE Trans Inf Forensics Secur. http://arxiv.org/abs/1409.4752
11. Boche H, Schaefer RF, Poor HV (2015) On the continuity of the secrecy capacity of wiretap channels under channel uncertainty. In: Proceedings of IEEE international conference on communication, London, UK, June 2015
12. Boche H, Schaefer RF, Poor HV (2014) On arbitrarily varying wiretap channels for different classes of secrecy measures. In: Proceedings of IEEE international symposium on information theory, Honolulu, pp 2376–2380
13. Csiszár I (1996) Almost independence and secrecy capacity. Probl Pered Inf 32(1):48–57
14. Csiszár I, Körner J (1978) Broadcast channels with confidential messages. IEEE Trans inf theory 24(3):339–348
15. Csiszár I, Narayan P (1988) The capacity of the arbitrarily varying channel revisited: positivity, constraints. IEEE Trans Inf Theory 34(2):181–193
16. Deutsche Telekom AG Laboratories (2010) Next generation mobile networks: (r)evolution in mobile communications. Technology Radar Edition III/2010, Feature Paper
17. Ekrem E, Ulukus S (2010) On Gaussian MIMO compound wiretap channels. In: Proceedings of the conference on information sciences and systems, Baltimore, pp 1–6
18. Fettweis G, Boche H, Wiegand T et al (2014) The tactile internet. Technical report, ITU-T Technology Watch reports. http://www.itu.int/oth/T2301000023/en
19. Grigorescu A (2015) Robust biometric authentication and secure message transmission. Master's thesis, Technische Universität München, Munich, Germany
20. Grigorescu A, Boche H, Schaefer RF, Poor HV (2015) Capacity region continuity of the compound broadcast channel with confidential messages. In: Proceedings of IEEE conference on information theory workshop, Jerusalem, Israel
21. Helmbrecht U, Plaga R (2008) New challenges for IT-security research in ICT. In: World federation of scientists international seminars on planetary emergencies, Erice, Italy, pp 1–6
22. Jorswieck EA, Wolf A, Gerbracht S (2010) Secrecy on the physical layer in wireless networks. Trends in Telecommunications Technologies, pp 413–435
23. Khisti A (2011) Interference alignment for the multiantenna compound wiretap channel. IEEE Trans Inf Theory 57(5):2976–2993

24. Kobayashi M, Liang Y, Shamai (Shitz) S, Debbah M (2009) On the compound MIMO broadcast channels with confidential messages. In: Proceedings of IEEE international symposium on information theory, Seoul, Korea, pp 1283–1287
25. Leung D, Smith G (2009) Continuity of quantum channel capacities. Commun Math Phys 292(1):201–215
26. Liang Y, Kramer G, Poor HV, Shamai (Shitz) S (2009) Compound wiretap channels. EURASIP J Wireless Commun 142374:1–13
27. Liang Y, Poor HV, Shamai (Shitz) S (2009) Information theoretic security. Found Trends Commun Inf Theory 5(4–5):355–580
28. Liu R, Trappe W (eds) (2010) Securing wireless communications at the physical layer. Springer, Berlin
29. Maurer UM, Wolf S (2000) Information-theoretic key agreement: from weak to strong secrecy for free. In: EUROCRYPT 2000. Lecture Notes in Computer Science, vol 1807, Springer, Berlin, pp 351–368
30. MolavianJazi E, Bloch M, Laneman JN (2009) Arbitrary jamming can preclude secure communication. In: Proceedings of the 47th annual Allerton conference on communication, control, computing, Monticello, IL, pp 1069–1075
31. Nötzel J, Wiese M, Boche H (2015) The arbitrarily varying wiretapchannel—secret randomness, stability and super-activation. IEEE Trans Inf Theory. http://arxiv.org/abs/1501.07439
32. Schaefer RF, Boche H (2014a) Physical layer service integration in wireless networks—signal processing challenges. IEEE Signal Process Mag 31(3):147–156
33. Schaefer RF, Boche H (2014b) Robust broadcasting of common and confidential messages over compound channels: strong secrecy and decoding performance. IEEE Trans Inf Forensics Secur 9(10):1720–1732
34. Schaefer RF, Loyka S (2013) The secrecy capacity of a compound MIMO gaussian channel. In: Proceedings of IEEE conference information theory workshop, Seville, Spain, pp 104–108
35. Schaefer RF, Loyka S (2014) The compound secrecy capacity of a class of non-degraded MIMO gaussian channels. In: Proceedings of the 52nd annual allerton conference on communication, control, and computing, Monticello, pp. 1004–1010
36. Shannon CE (1949) Communication theory of secrecy systems. Bell Syst Tech J 28(4):656–715
37. Wiese M, Nötzel J, Boche H (2014) The arbitrarily varying wiretap channel-deterministic and correlated random coding capacities under the strong secrecy criterion. IEEE Trans Inf Theory. http://arxiv.org/abs/1410.8078
38. Wolfowitz J (1960) Simultaneous channels. Arch Rational Mech Anal 4(4):371–386
39. Wyner AD (1975) The wire-tap channel. Bell Syst Tech J 54:1355–1387
40. Zhou X, Song L, Zhang Y (eds) (2013) Physical layer security in wireless communications. CRC Press, Boca Raton

Chapter 6
End-to-End Key Establishment with Physical Layer Key Generation and Specific Attacker Models

Stefan Pfennig, Elke Franz, Sabrina Engelmann and Anne Wolf

Abstract Physical layer key generation got much attention during the last time. However, the need of a common physical channel implies that only point-to-point keys can be generated. In this chapter, we investigate approaches how these point-to-point keys can be used for a secure establishment of end-to-end keys between two users who can only communicate over a multi-hop network. We start with a review of physical layer key generation taking different attacker models into account. Subsequently, we introduce general approaches for the end-to-end key establishment in the presence of various attackers who differ in their behavior and their area of control. We discuss four different path selection algorithms for the key establishment and evaluate their performance by means of simulations. The results show that the end-to-end key establishment can be protected by means of physical layer keys with a reasonable effort if suitable path selection is applied.

6.1 Introduction

Cryptography is a fundamental technique for securing digital communication, particularly, for ensuring confidentiality, integrity, and accountability of transmitted messages. Of course, cryptographic systems cannot perform their function without establishing the required keys. We have to consider that the security of the key establishment crucially influences the security of the cryptosystem. Within this chapter, we focus on the use of symmetric cryptography since it requires less computational

S. Pfennig (✉) · E. Franz · S. Engelmann · A. Wolf
Technische Universität Dresden, 01062 Dresden, Germany
e-mail: stefan.pfennig@tu-dresden.de

E. Franz
e-mail: elke.franz@tu-dresden.de

S. Engelmann
e-mail: sabrina.engelmann@tu-dresden.de

A. Wolf
e-mail: anne.wolf@tu-dresden.de

M. Baldi and S. Tomasin (eds.), *Physical and Data-Link Security Techniques for Future Communication Systems*, Lecture Notes in Electrical Engineering 358, DOI 10.1007/978-3-319-23609-4_6

effort than asymmetric cryptography and, therefore, provides better performance. However, a drawback of symmetric cryptography is the fact that we need a prior secure exchange of the secret key between the communication partners. In general, existing protocols require that the communication partners already possess a secret that can be used to derive a new cryptographic key, or that a trusted party is involved in the key exchange [3].

In [10] it was shown, that symmetric point-to-point keys can be generated on the physical layer. For instance, the key may be generated from random characteristics of the wireless channel, which are only available to the communication partners.

The goal of this chapter is to present approaches how such physical layer point-to-point keys can be used for a secure exchange of end-to-end keys between two users who can only communicate over a (multi-hop) network. We consider different attacker models which are mainly characterized by the role and the behavior of the attacker.

In Sect. 6.2, we present the system model and specify the attacker models that are studied within this chapter. Section 6.3 gives an overview of the fundamentals of physical layer key generation and demonstrates how point-to-point keys can be generated between two nodes. In Sect. 6.4, we discuss protocols that allow the establishment of secret end-to-end keys under consideration of the specified attacker models. Section 6.5 concludes and gives an outlook.

6.2 System Assumptions and Attacker Models

6.2.1 System Model

We consider a scenario where two users, a sender $\mathscr{S}$ and a receiver $\mathscr{R}$, wish to establish a secret key for securing their communication by means of symmetric cryptography. We assume that there is no direct link between them. Thus, they have to communicate with each other over multiple hops. We assume that a wireless network is used to forward this communication. The nodes (or relays) in this network are called forwarders. In the most general case, these forwarders may be arbitrarily distributed and connected. Within this chapter, we assume that we have a multi-hop network with $m \cdot \ell$ forwarding nodes that are positioned in ℓ different groups (see Fig. 6.1). Each group $\mathscr{F}_i$ with $i \in \{1, 2, \ldots, \ell\}$ consists of m nodes $\mathscr{F}_{1,i}, \mathscr{F}_{2,i}, \ldots, \mathscr{F}_{m,i}$. The nodes of group $\mathscr{F}_i$ have only links to the nodes of the neighboring groups $\mathscr{F}_{i-1}$ and $\mathscr{F}_{i+1}$, but they can communicate with all nodes of these groups directly. The sender $\mathscr{S}$ and the receiver $\mathscr{R}$ are only connected to the nodes of the groups $\mathscr{F}_1$ and $\mathscr{F}_\ell$, respectively. Hence, they have to transmit their messages over $\ell + 1$ hops.

This system model is motivated by the high-performance low-energy computing platform HAEC that is currently under design [5]. The HAEC architecture contains a number of boards with 3-D stacked processor chips that are optically interconnected. Nodes of neighboring boards are fully linked using wireless links. Since we only

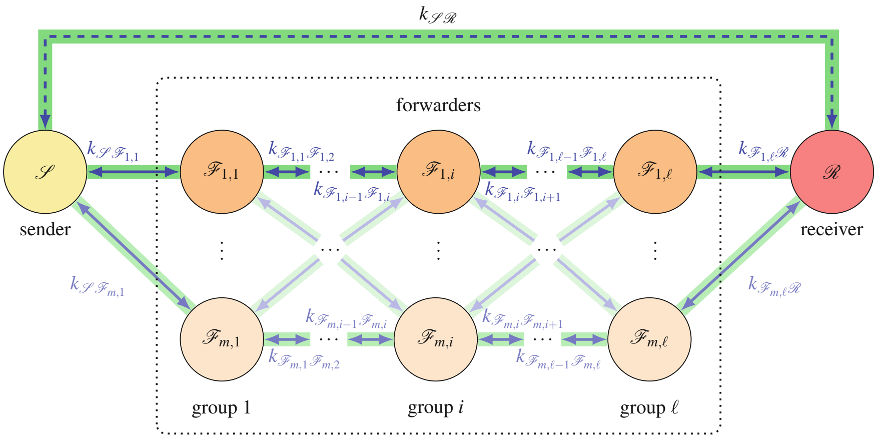

$k_{\mathscr{S}\mathscr{R}}$
forwarders
$k_{\mathscr{S}\mathscr{F}_{1,1}}$
$\mathscr{S}$
sender
$\mathscr{F}_{1,1}$
$k_{\mathscr{F}_{1,1}\mathscr{F}_{1,2}}$
$k_{\mathscr{F}_{1,i-1}\mathscr{F}_{1,i}}$
$\mathscr{F}_{1,i}$
$k_{\mathscr{F}_{1,\ell-1}\mathscr{F}_{1,\ell}}$
$k_{\mathscr{F}_{1,i}\mathscr{F}_{1,i+1}}$
$\mathscr{F}_{1,\ell}$
$k_{\mathscr{F}_{1,\ell}\mathscr{R}}$
$\mathscr{R}$
receiver
$k_{\mathscr{S}\mathscr{F}_{m,1}}$
$k_{\mathscr{F}_{m,\ell}\mathscr{R}}$
$\mathscr{F}_{m,1}$
$k_{\mathscr{F}_{m,i-1}\mathscr{F}_{m,i}}$
$k_{\mathscr{F}_{m,1}\mathscr{F}_{m,2}}$
$\mathscr{F}_{m,i}$
$k_{\mathscr{F}_{m,i}\mathscr{F}_{m,i+1}}$
$k_{\mathscr{F}_{m,\ell-1}\mathscr{F}_{m,\ell}}$
$\mathscr{F}_{m,\ell}$
group 1
group i
group ℓ

Fig. 6.1 System model

consider wireless communication in the scope of this chapter, we refer to the inter-board connections only. The groups in our system model represent the nodes of one board, the links between the groups correspond to the wireless connections between neighboring boards.

We assume that point-to-point keys are generated by means of the physical layer between nodes of adjacent groups. These point-to-point keys are denoted by $k_{\mathscr{S},\mathscr{F}_{j,1}}$, $k_{\mathscr{F}_{j,i},\mathscr{F}_{j',i+1}}$ and $k_{\mathscr{F}_{j,\ell},\mathscr{R}}$ with $j, j' \in \{1, 2, \ldots, m\}$ and $i \in \{1, 2, \ldots, \ell - 1\}$ as illustrated in Fig. 6.1. The communication for the establishment of the end-to-end key $k_{\mathscr{S}\mathscr{R}}$ between the sender $\mathscr{S}$ and the receiver $\mathscr{R}$ is protected by means of the physical layer point-to-point keys.

6.2.2 *Attacker Models*

In order to assess the security of the key exchange, possible attacks need to be considered. As a first step, we have to define the attacker models. Generally, we assume that sender and receiver are trustworthy. Likewise, we assume that two adjacent nodes who want to generate a physical layer point-to-point key are trustworthy with respect to this key exchange. However, they are not necessarily trustworthy for the end-to-end key exchange, i.e., they might be interested in learning the exchanged end-to-end key or disturbing a successful key exchange. In the context of our investigations, we particularly consider the following aspects to describe the attacker:

6.2.2.1 Behavior

A *passive* attacker only eavesdrops the communication, while an *active* attacker is able to jam or to interrupt the communication, hence, modify or even delete transmitted messages.

6.2.2.2 Area of Control

This aspect describes *how many links or forwarding nodes* can be controlled by an attacker. Instead of one attacker who controls more than one link or node we can equivalently assume multiple attackers who cooperate to increase their area of control. Since both scenarios result in the same situation from the perspective of the honest users, we will use the first point of view in the following.

6.2.2.3 Role

Generally, we distinguish whether the attacker is an *insider* or an *outsider* with regard to the communication that is necessary for the key exchange.

A more detailed description of the possible roles of an attacker can only be done with respect to the layer that is discussed. At the physical layer, an insider is part of the communication network. More exactly, the insider has direct links to the legitimated nodes $\mathscr{A}$ and $\mathscr{B}$ who wish to generate a physical layer point-to-point key. We assume that $\mathscr{A}$ and $\mathscr{B}$ have already communicated with this node in former time slots. Hence, they may have knowledge about their channels to such an attacker. In contrast, an outsider is an external entity that does not belong to the communication network. Consequently, the legitimated nodes do not have reliable knowledge about their channels to such an attacker. Thus, we will distinguish between network nodes and external entities at the physical layer.

At upper layers, we do not consider physical channels, thus, we work with another distinction between insiders and outsiders. An insider participates in the communication that is necessary for the key exchange. Since sender and receiver are trustworthy by definition, an insider can only be a forwarder on the path between sender and receiver. All other attackers are outsiders to this communication. This covers both external entities and network nodes who do not participate as forwarders in this communication. As discussed in Sect. 6.4, the protection against both types of outsiders is the same. Within this chapter, we do not consider active insiders at upper layers.

6.3 Physical Layer Key Generation

6.3.1 Fundamentals of Physical Layer Key Generation

In this section, we give an overview of the fundamentals of physical layer key generation before we discuss in the following sections which approaches can be used for the scenario and the different attacker models specified in Sect. 6.2.

Key generation on the physical layer is widely discussed in literature nowadays (see [2, Chap. 4] and [8, Chap. 9] for an overview). Mainly, there are two different approaches that need to be distinguished: the source-type model and the channel-type model. For both models, the main idea is the same: Two users, $\mathscr{A}$ and $\mathscr{B}$, want to generate a common secret key by means of the physical layer. For that purpose, they use a certain advantage they have over an eavesdropper $\mathscr{E}$, i.e., a passive attacker. For the source-type model, such an advantage is that $\mathscr{A}$ and $\mathscr{B}$ can observe correlated sequences from a common source of randomness, whereas $\mathscr{E}$ has either no access to this source or can only observe another sequence, which differs from the realizations obtained by $\mathscr{A}$ and $\mathscr{B}$. For the channel-type model, the advantage of $\mathscr{A}$ and $\mathscr{B}$ over $\mathscr{E}$ is the current realization of their communication channel, which cannot be observed by an eavesdropper that is located at another position. Exploiting their particular advantage over the eavesdropper, $\mathscr{A}$ and $\mathscr{B}$ want to agree on a common key. Ideally, they can communicate over an authenticated and noiseless public channel with unlimited bandwidth in order to exchange some information for the key agreement. The communication strategy has to guarantee that the key is kept secret from $\mathscr{E}$ who has perfect access to this public channel. Finally, both generate an individual key based on the information that is then available to them. The requirements for a secret key agreement are formulated as follows [8, Chap. 9] and [2, Chap. 4]:

1. The keys that are generated by $\mathscr{A}$ and $\mathscr{B}$ have to be equal with high probability.
2. The generated keys have to be independent of the public communication and the further observations of the eavesdropper.
3. The generated keys have to be approximately uniformly distributed over the key alphabet.

Here, it is assumed that all involved parties are allowed to know the applied codebook as well as the public communication strategy in principle. The rate of the secret key generation can be measured. A secret key rate is called achievable if there exists a public communication strategy such that the requirements above are fulfilled. The secret key capacity C_k is the maximum achievable secret key rate. For a formal definition of the secret key rate and capacity, we refer to [1] or the references above.

6.3.1.1 Source-Type Model

In the source-type model (see Fig. 6.2), two legitimated nodes, $\mathscr{A}$ and $\mathscr{B}$, observe correlated sequences X^n and Y^n of length n from a common source of randomness. These sequences are used to generate a shared key between both parties. In general, the eavesdropper $\mathscr{E}$ also has access to this source of randomness and observes a sequence Z^n of length n, which is correlated with the sequences of $\mathscr{A}$ and $\mathscr{B}$. The source, which is modeled as a discrete memoryless source [1, 10] or a memoryless Gaussian source [2, Sect. 5.1.3], is an i.i.d. source with the joint probability mass/density function p_{XYZ}.

The secret key capacity C_k of the source-type model is upper- and lower-bounded by [2, Chap. 4]:

$$I(X;Y) - \min\{I(X;Z), I(Y;Z)\} \leq C_k \leq \min\{I(X;Y), I(X;Y|Z)\},$$

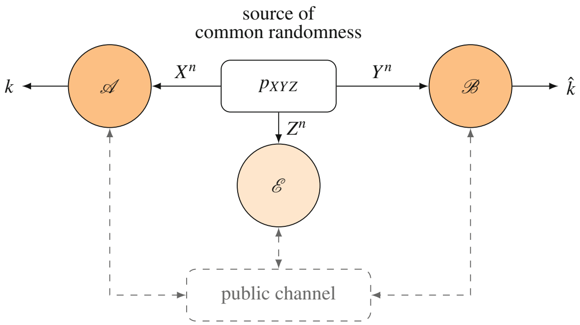


Fig. 6.2 Source-type model for key generation

where $I(X; Y)$ and $I(X; Y|Z)$ are the mutual information between the random variables X and Y and the conditional mutual information between X and Y given Z. For some special cases, closed form expressions of the secret key capacity are known. These are the cases if (X, Y) are independent of Z and if X, Y and Z form a Markov chain in the order $X \to Y \to Z$ or $Y \to X \to Z$. A typical application of the source-type model is the key generation from the channel characteristics. For instance, the channel state of the reciprocal wireless channel between $\mathscr{A}$ and $\mathscr{B}$ can be used as source of common randomness. The eavesdropper $\mathscr{E}$ has no (or only very limited) access to the channel state information of this channel. The nodes $\mathscr{A}$ and $\mathscr{B}$ send pilot signals, which enable the partner to estimate the current channel state. These estimates are then used to generate the common secret key.

6.3.1.2 Channel-Type Model

In the channel-type model (see Fig. 6.3), one legitimated node ($\mathscr{A}$) generates a random sequence and transmits it over the wireless channel to the other legitimated node ($\mathscr{B}$). This random sequence is used to generate the common key between $\mathscr{A}$ and $\mathscr{B}$. In general, there exists also a channel between $\mathscr{A}$ and the eavesdropper $\mathscr{E}$.

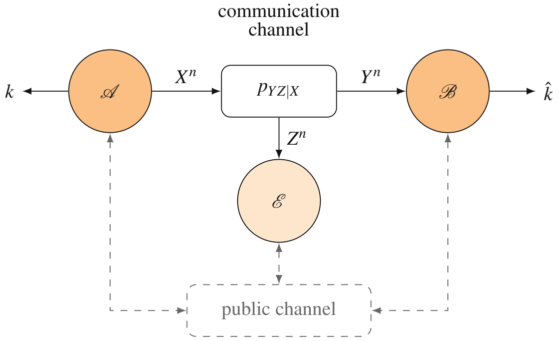


Fig. 6.3 Channel-type model for key generation

Consequently, $\mathscr{E}$ gets a correlated observation of the random sequence. The bounds on the secret key capacity C_k of the channel-type model are very similar to the ones of the source-type model. The only difference is that the node $\mathscr{A}$ has an additional degree of freedom to choose the probability mass/density[1] function p_X that maximizes the mutual information expressions [2, Chap. 4]:

$$\max\left\{\max_{p_X}\left[I(X;Y)-I(X;Z)\right], \max_{p_X}\left[I(X;Y)-I(Y;Z)\right]\right\} \\ \leq C_k \leq \max_{p_X}\min\left\{I(X;Y), I(X;Y|Z)\right\}.$$

For special cases, closed form expressions of the secret key capacity can be derived analogously to the source-type model.

6.3.1.3 Sequential Key Distillation

For both models, an appropriate coding scheme and a key agreement protocol for the public authenticated noiseless channel are necessary in order to get a key that is only known by the nodes $\mathscr{A}$ and $\mathscr{B}$. The steps of such a key agreement protocol are presented in the following using the example of the source-type model.

- *Advantage Distillation:* The nodes $\mathscr{A}$ and $\mathscr{B}$ try to find observations where they have an advantage over the node $\mathscr{E}$ and discard all other observations.
- *Information Reconciliation:* The nodes $\mathscr{A}$ and $\mathscr{B}$ process their observations in order to correct errors and match their observations.
- *Privacy Amplification:* The nodes $\mathscr{A}$ and $\mathscr{B}$ agree on a hash function in order to generate a common key.

These steps, which follow the randomness sharing process we presented above, do not provide further options for a possible attacker, since all information in these steps is locally processed at nodes $\mathscr{A}$ and $\mathscr{B}$ or exchanged over the public channel. Thus, the key agreement protocol is not within the focus of this chapter. More details on the single steps of the protocol can be found in [2, Chap. 4].

6.3.2 Key Generation in Presence of Passive Attackers

Now, we consider the generation of point-to-point keys between nodes of neighboring groups. Thus, we can draw our attention to an adapted system model (see Fig. 6.4), which can be derived from the original system model in Sect. 6.2. We regard two nodes ($\mathscr{A}$ and $\mathscr{B}$ in Fig. 6.4) that can directly communicate with each other over a wireless link and want to generate a common secret key in the presence of one

[1] For the case with continuous channel alphabets, we have to further add a constraint on the second order moment of the channel input X, see [14].

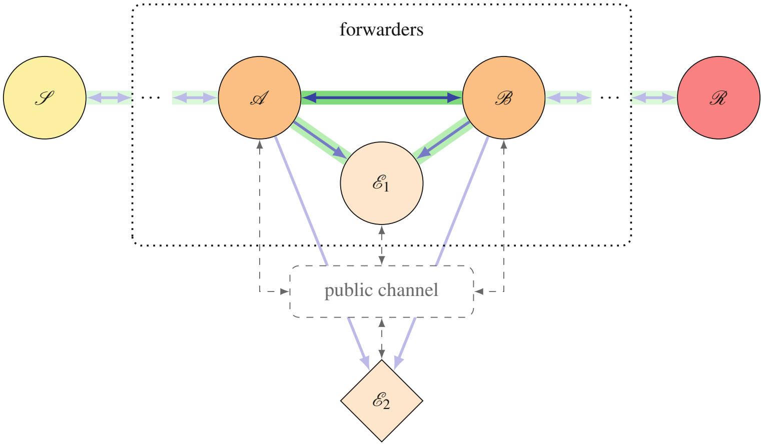


Fig. 6.4 System model for the key generation on the physical layer

or more passive attackers. A passive attacker is an eavesdropper, who is interested in the secret key that is generated between the nodes $\mathscr{A}$ and $\mathscr{B}$. In the context of physical layer key generation, we have to distinguish between eavesdroppers who are part of the communication network (like $\mathscr{E}_1$ in Fig. 6.4) and external entities (like $\mathscr{E}_2$ in Fig. 6.4), who are completely alien to the legitimated nodes.

6.3.2.1 Eavesdropping Network Nodes

Due to the fact that the eavesdropper is part of the communication network, we can assume that the nodes $\mathscr{A}$ and $\mathscr{B}$ also communicate with the eavesdropping node $\mathscr{E}_1$ in other time slots. Therefore, it is reasonable that the nodes $\mathscr{A}$ and $\mathscr{B}$ know their particular channels to the eavesdropper and the corresponding channel statistics. In this case, either the key generation according to the source-type or the key generation according to the channel-type model can be used. Which one is preferable, strongly depends on the channel characteristics. The channel-type model is better controllable by the legitimated nodes, as the probability distribution of the random sequence can be chosen. It is mainly suitable for slowly varying or static channels, where the channel state remains (nearly) constant for a comparatively long time, since the achievable secret key rate is mainly determined by the randomness of the transmitted sequence. In contrast, the secret key rate that is achievable according to the source-type model depends on the random process of the source of common randomness, which might be quite inefficient, e.g., if we do not have a channel characteristic that changes often enough.

In order to ensure that the generated key is kept secret from all possibly eavesdropping network nodes, it is necessary to consider a kind of worst-case scenario. This can be achieved by modeling a compound channel that comprises all network nodes of the neighboring groups as possible eavesdroppers. In this case, we always have to take into account the best possible eavesdropper for each key generation process. A detailed analysis of the compound wiretap channel was carried out in [7] in the context of secrecy rate optimization. For the channel-type model with a Gaussian multi-antenna channel, worst-case approaches can be found in [12, 13], where the set of possible eavesdropper channels was defined by an upper bound on the sum of all channel gains and a channel estimation error that is bounded by a certain norm constraint, respectively.

6.3.2.2 Eavesdropping External Entities

In this case, the eavesdropper is not part of the communication network and consequently it is not reasonable that the nodes $\mathscr{A}$ and $\mathscr{B}$ have any knowledge about their channels to the eavesdropper $\mathscr{E}_2$. Nevertheless, we can make some assumptions on the quality of such an eavesdropper channel, e.g., depending on the possible positions, where an external eavesdropper can be, the propagation conditions etc. Hence, the key generation according to the channel-type model, where the key is extracted from the transmitted sequence, should only be used in combination with an appropriate worst-case analysis. But protecting the key against the best possible eavesdropper will definitely reduce the achievable key rate. In this case, it seems to be more suitable to choose the source-type model in order to generate secret keys. Here, we can assume that we have no or only very weak correlation between the main channel from $\mathscr{A}$ to $\mathscr{B}$ (and vice versa) and the possible eavesdropping channels to $\mathscr{E}_2$. Nevertheless, the reciprocity of the wireless channel between the nodes $\mathscr{A}$ and $\mathscr{B}$ is a necessary condition if we use the state of the fading channel as source of common randomness. In order to achieve high secret key rates, the variation of the channel must be sufficiently large. For instance, a fast fading channel, which varies relatively fast compared to the transmission time of a codeword, could be a good source for secret key generation. Multi-path scattering and non-line of sight channels are also quite helpful in this situation. The secret-key generation from a source-type model was for instance studied in [4, 6, 11], where pilot-based channel estimation procedures were used for secret key agreement in multi-antenna scenarios with correlated channels. The impact of the spatial channel correlation on the achievable secret-key rate was analyzed and optimal precoding schemes were derived.

6.3.2.3 Cooperating Eavesdroppers

Multiple cooperating eavesdroppers can be interpreted as one “more powerful” eavesdropper with an accordingly adapted channel characteristic. Thus, the achievable secret key rates might decrease, but the system principally works as shown above.

6.3.3 Key Generation in Presence of Active Attackers

Active attackers may jam the key generation process on the physical layer. Permanent jamming, which could be treated as an additional noise, only reduces the channel quality, which would consequently decrease the achievable secret key rates for both models presented above. A time varying jamming is more challenging for the key generation, since it may affect the channel estimation phase. If the key is generated according to the source-type model, there is the risk that the channel reciprocity is no longer given. In this case, the key bits that would be generated from these differently estimated channel states would probably not be the same at the nodes $\mathscr{A}$ and $\mathscr{B}$, but this problem should be detected and solved by the key agreement protocol afterwards, however at the expense of the achievable rate. If the key is generated according to the channel-type model, time varying jamming could make the key generation process vulnerable, since a wrong channel estimation at node $\mathscr{A}$ could lead to a wrong coding and resource allocation strategy. If one of the nodes $\mathscr{A}$ and $\mathscr{B}$ detects such jamming behavior, it could be a good choice to pause the key generation process for a certain time.

6.4 Protocols for End-to-End Key Exchange

6.4.1 End-to-End Key Exchange in Presence of Passive Outsiders

For the following discussion, we assume that all network nodes successfully established physical layer point-to-point keys. We start with a rather weak attacker. We assume that the attacker is an external entity that is only able to eavesdrop the communication between two nodes. Thus, the sender $\mathscr{S}$ can generate the end-to-end key $k_{\mathscr{S}\mathscr{R}}$ and transmit it hop by hop to the receiver $\mathscr{R}$ using an arbitrarily chosen path, e.g., from $\mathscr{S}$ over the nodes $\mathscr{F}_{1,i}$ with $i \in \{1, 2, \ldots, \ell\}$ to $\mathscr{R}$. To prevent the attacker from gaining any information, each link is encrypted using the physical layer point-to-point keys (in this example, $k_{\mathscr{S},\mathscr{F}_{1,1}}, k_{\mathscr{F}_{1,1},\mathscr{F}_{1,2}}, \ldots, k_{\mathscr{F}_{1,\ell},\mathscr{R}}$). Additionally, the point-to-point encryption ensures that the key is kept secret from all other network nodes, which are also passive outsiders in this scenario.

6.4.2 Key Exchange in Presence of Active Outsiders

First, we again consider only external entities as potential passive attackers. In contrast to the scenario above, we now assume that the external entity is additionally able to jam or modify the communication. Since all network nodes are assumed to be trustworthy again, the idea for the end-to-end key establishment is similar to the one we presented in Sect. 6.4.1. The difference is that each point-to-point communication is also authenticated by means of the available point-to-point keys. Additionally, the receiver should acknowledge the receipt of a valid key. This acknowledgment must be also authenticated and relayed by the forwarders to the sender. This allows the sender to switch to another (if possible link-disjoint) path and to retry the key exchange on this path, if the acknowledgment does not arrive within a certain time. Under the assumption that there exists at least one path between the sender and the receiver which cannot be jammed by the attacker, the sender can exchange the key with the receiver after a finite amount of time. Of course, we cannot assure availability of the system if all links between two adjacent groups of forwarders are jammed.

Again, the protection method additionally works against all other network nodes, which are then (passive or active) outsiders, too. Since the point-to-point keys are used for the authentication, even such an outsider cannot unnoticeably modify the transmitted key $k_{\mathscr{S}\mathscr{R}}$ because he cannot compute a corresponding message authentication code for the modified key.

6.4.3 *Key Exchange in Presence of Passive Insiders*

Since each network node knows his point-to-point keys, a forwarder who is involved in the key exchange can learn the end-to-end key $k_{\mathscr{S}\mathscr{R}}$ and decrypt the subsequent communication. It is not possible to prevent the success of such an insider attack by using just a single path without asymmetric cryptography. Thus, we need at least one additional node-disjoint path. In principle, we could use one path for key transmission and the other one for communication. Alternatively, the sender can use both paths for the transmission of two different keys $k_{\mathscr{S}\mathscr{R}_1}$ and $k_{\mathscr{S}\mathscr{R}_2}$. After the transmission, sender and receiver locally compute $k_{\mathscr{S}\mathscr{R}} = k_{\mathscr{S}\mathscr{R}_1} \oplus k_{\mathscr{S}\mathscr{R}_2}$, where $\oplus$ denotes the binary XOR. This solution provides the advantage that both paths can be used afterwards for the encrypted communication.

Another option is to exchange keys of half the required length and concatenate them later to save transmission overhead [9]. However, parts of the key may reveal some plaintext information or, at least, the search space for a brute-force key attack shrinks. Thus, we recommend the XOR method, since an attacker cannot gain any information from knowing all keys except one.

6.4.3.1 Passive Attacker with a Larger Area of Control

In this scenario, we assume a passive attacker who controls at most a network nodes. Thus, we need at least $a + 1$ keys and different paths for key distribution such that $k_{\mathscr{S}\mathscr{R}} = \bigoplus_{j=1}^{a+1} k_{\mathscr{S}\mathscr{R}_j}$ contains at least one key $k_{\mathscr{S}\mathscr{R}_j}$ that is unknown to the attacker. To fulfill this condition, there must be at most $m - 1$ attackers in each group $\mathscr{F}_i$ with

$i \in \{1, 2, \ldots, \ell\}$. This implies that there is at least one trustworthy node per group $\mathscr{F}_i$ and if we use all possible combinations of links between the nodes, there will be at least one $k_{\mathscr{S}\mathscr{R}_j}$ that is confidential.

In our system model (Fig. 6.1) with $m \cdot \ell$ forwarders, there exist m^ℓ different paths, i.e., potential partial keys. Thus, even for small values of m and ℓ, it will be really expensive to use all paths, for larger values it will be even impossible.

In the next section, we investigate how many paths are really necessary to achieve a certain level of security against an attacker that controls a certain amount of nodes. Additionally, we look on principles for choosing the paths to further reduce the necessary number of paths.

6.4.4 Evaluation

In order to derive formulas for the number of required paths, we assume that the nodes which are controlled by an attacker are equally distributed on the groups. Furthermore, this assumption makes it more likely that at least one node per group is trustworthy, which is a necessary condition for establishing a secret key.

For c randomly chosen paths, we can calculate the probability p for choosing at least one trustworthy path:

$$p = 1 - \left(1 - \left(1 - \frac{a}{m \cdot \ell}\right)^\ell\right)^c. \tag{6.1}$$

Since $\left(1 - \frac{a}{m \cdot \ell}\right)^\ell$ is the probability for a path to be trustworthy, we can calculate the number c of randomly chosen paths we need on average to get at least one trustworthy path:

$$c = \frac{1}{\left(1 - \frac{a}{m \cdot \ell}\right)^\ell}. \tag{6.2}$$

However, "on average" means that in a certain number of cases this number does not suffice to get a trustworthy path. Therefore, we can introduce a value ε that determines the chance for an attacker to be successful, i.e., to control at least one node in each of the c randomly chosen paths. If we set ε accordingly to our demands, we can calculate the number c_ε of necessary paths:

$$c_\varepsilon = \frac{\log(\varepsilon)}{\log\left(1 - \left(1 - \frac{a}{m \cdot \ell}\right)^\ell\right)}. \tag{6.3}$$

6.4.4.1 Advanced Path Selection

All equations in the previous section hold under the assumption of randomly chosen paths. The question is whether we can do better. As starting point, we assume that there is only one group of forwarders, i.e., $\ell = 1$. Hence, we can simplify (6.1) to $p = 1 - \left(\frac{a}{m}\right)^c$. If we use each path only once, the equation changes to $p = 1 - \frac{\binom{m-a}{c}}{\binom{m}{c}}$. Hence, the probability increases for all $c > 1$.

Generalizing that for arbitrary values of ℓ, we can think of 4 different methods for choosing a path. These methods are called Rand, Once, Smart, and Once Smart. They are explained in the following and illustrated in Fig. 6.5.

Rand: We simply select random paths without memorizing them for next choices. Thus, there is no need for memory (Fig. 6.5a).

Once: We select a random path but ensure that we use each whole path only once. Thus, we need to memorize all chosen paths (Fig. 6.5b).

Smart: This method works in rounds. Within one round, each forwarder can be used only once. Since each group of forwarders consists of m nodes, we can choose m paths that are (node- and link-) disjoint within one round. When all nodes are selected, a new round starts. We just need to memorize the forwarders selected within one round, which results in a reasonable memory consumption (Fig. 6.5c).

Once Smart (OS): As the name suggests, Once Smart is a combination of Once and Smart. Basically, we use the Smart scheme but in addition, we also memorize all paths chosen in former rounds. Thus, we do not reuse a path and choose disjoint paths as often as possible. However, this results in the highest memory requirements (Fig. 6.5d).

6.4.4.2 Results

As mentioned above, (6.1)–(6.3) only hold for random path selection. In order to assess the suggested improved path selection algorithms, they were simulated for a network with $m = 4$ and $\ell = 2$. For each algorithm and each possible number of attackers $a \in \{1, 2, \ldots, (m-1) \cdot \ell\}$, the simulation was run 1000 times to determine the average numbers c and the numbers c_ε that are necessary to select at least one trustworthy path with a probability of 99 %, i.e., $\varepsilon = 0.01$. To verify the results, the averaged numbers were compared to the estimated values computed by means of (6.2) and (6.3).

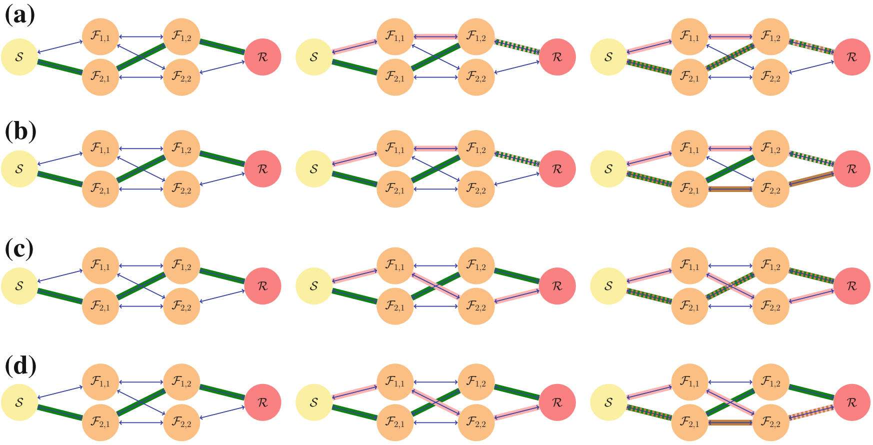


Fig. 6.5 Example of choosing 3 paths consecutively with the 4 different path selection algorithms for a small network with $m = \ell = 2$. **a** Rand: Due to the random selection, parts and whole paths could be reused. **b** Once: Whole paths could be used only once, but parts of a path could be reused. **c** Smart: Neither parts nor whole paths could be reused within one round (m paths per round). However, paths could be selected again in the next round. **d** Once Smart: There are only (path- and node-)disjoint paths within one round (like Smart). Additionally, whole paths could not be reused in later rounds

Figure 6.6 confirms that the averaged numbers for Rand correspond to the estimated numbers (Est). It also shows that Once requires fewer paths than Smart for a higher number of attackers a. For a smaller number of attackers, the opposite holds. The reason for this relation is that we need more paths with a growing number of attackers. The more paths are chosen, the more likely they are used again. Since Once prevents that whole paths can be selected again, it performs better if repetitions are likely. For a lower number of attackers, fewer paths are needed and, therefore, repetitions are less likely. Hence, Once performs similar to Rand. Smart delivers disjoint paths per round. This is beneficial for a lower value of a, since we do not use an attacked node twice. However, the benefit diminishes with increasing a and we get a behavior like Rand, since we use paths more often. As expected, OS combines the benefits of both suboptimal algorithms Once and Smart. Thus, OS performs best for each value of a.

The absolute number of paths grows with an increasing number of attackers a in a given topology. Hence, we normalized the average number of paths required by each algorithm (c_{Alg}) by dividing these values by the number of paths required by Rand (c_{Rand}) in order to visualize the performance gains of the path selection algorithms. Figure 6.7a represents the normalized values $\tilde{c}_{\mathsf{Alg}} = \frac{c_{\mathsf{Alg}}}{c_{\mathsf{Rand}}}$. Corresponding results for $m = 9$, $\ell = 3$ and $m = 16$, $\ell = 4$ are shown in Fig. 6.7b, c, respectively. All the three plots confirm the characteristic that has already been seen in Fig. 6.6b. Smart performs best in case of a medium number of attackers (best results at approx-

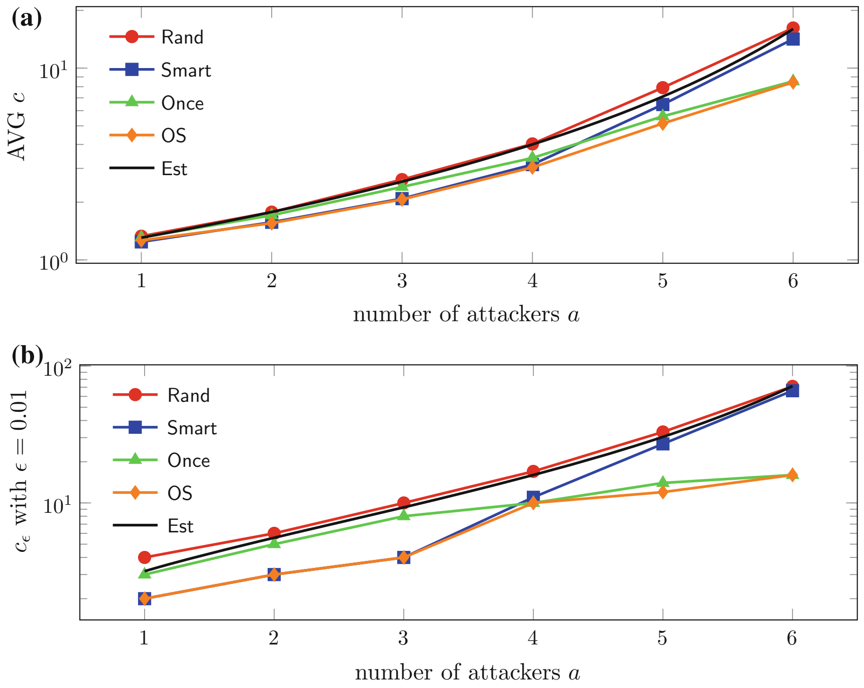


Fig. 6.6 Numbers c and c_ε of necessary paths for choosing at least one trustful path using different path selection algorithms. **a** Average number c of necessary paths for $m = 4$ and $\ell = 2$. **b** Number of necessary paths c_ε with $\varepsilon = 0.01$ for $m = 4$ and $\ell = 2$

imately $a = \frac{m \cdot \ell}{2}$), while Once works best in case of many attackers (best results at $a = (m-1) \cdot \ell$). The performance of OS corresponds to the minimum of Once and Smart. However, the advantages of the three path selection algorithms over Rand diminish with larger networks.

To get an impression of the overall gain of each path selection algorithm, the normalized values $\tilde{c}$ and $\tilde{c}_\varepsilon$ were averaged over all $a \in \{1, 2, \ldots, (m-1) \cdot \ell\}$. Table 6.1 shows the averaged values for networks of different sizes. The values confirm that the benefits of improved selection algorithms diminish with increasing network size.

Table 6.2 illustrates the absolute number of paths for some exemplary values of m, ℓ, and a. Especially for larger topologies, the need for different paths is moderate. For a network with $m = 16$, $\ell = 4$ and half of the nodes being malicious, less than a thousandth of all available paths (64 of 65536) was necessary to get at least one trustworthy path with a probability of at least 99 % in our simulations. Since there exist 16 node- and link-disjoint paths in such a topology where a key establishment is possible in parallel, we expect to need only 4 rounds to establish a secure key.

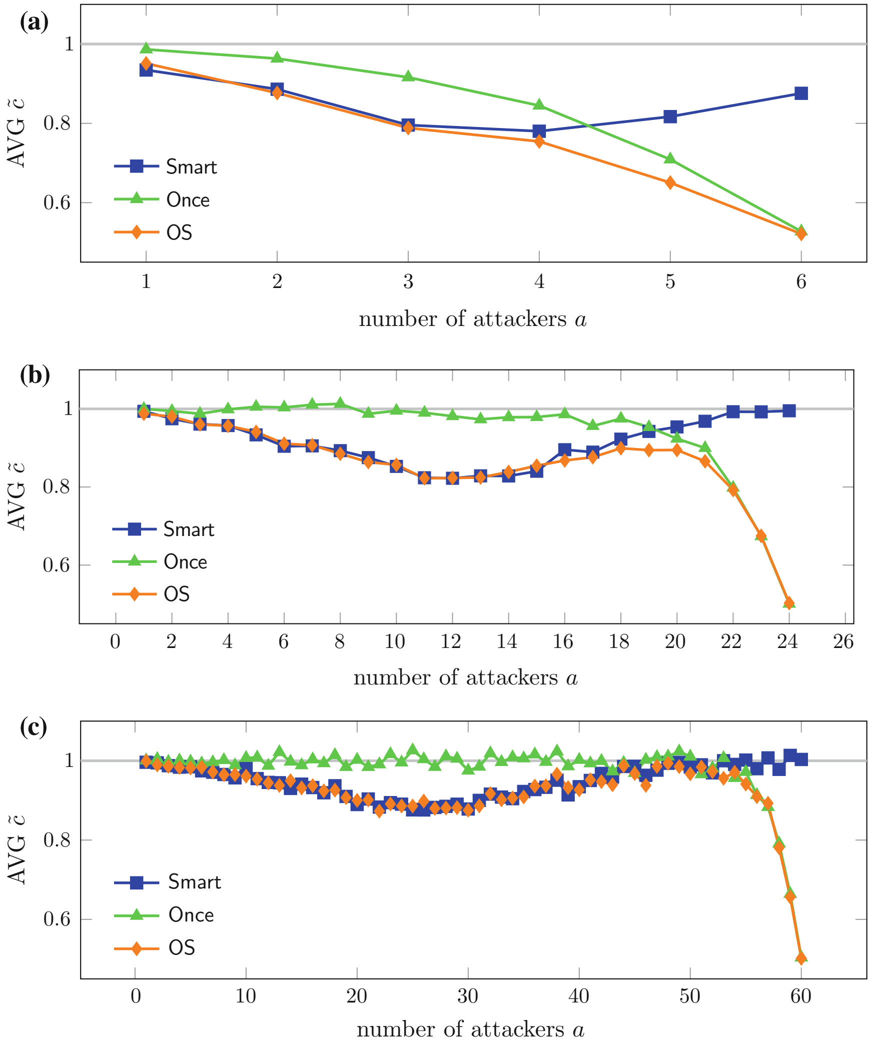


Fig. 6.7 Relative average number $\tilde{c}$ of necessary paths needed for choosing at least one trustful path for a different number of attackers a and for different topologies. **a** Normalized average $\tilde{c}$ for $m = 4$ and $\ell = 2$. **b** Normalized average $\tilde{c}$ for $m = 9$ and $\ell = 3$. **c** Normalized average $\tilde{c}$ for $m = 16$ and $\ell = 4$

Table 6.1 Averaged normalized costs for different path selection algorithms in comparison to Rand

m	ℓ	AVG $\tilde{c}$ Smart	AVG $\tilde{c}$ Once	AVG $\tilde{c}$ OS	$\tilde{c}_{\varepsilon=0.01}$ Smart	$\tilde{c}_{\varepsilon=0.01}$ Once	$\tilde{c}_{\varepsilon=0.01}$ OS
4	2	0.84820	0.82454	0.75701	0.63247	0.60353	0.42954
9	3	0.91442	0.94021	0.86166	0.82958	0.88953	0.73169
16	4	0.94782	0.97756	0.92330	0.89012	0.96256	0.84156

Lower values mean less effort and a performance gain

Table 6.2 Absolute values for Rand and OS for different topologies

m	ℓ	a	AVG c Rand	AVG c OS	$c_{\varepsilon=0.01}$ Rand	$c_{\varepsilon=0.01}$ OS	# of paths
4	2	3	2.623	2.068	10	4	16
9	3	6	2.143	1.952	8	6	729
9	3	13	7.415	6.112	33	25	729
9	3	20	60.373	54.016	279	226	729
16	4	16	3.151	2.953	13	10	65536
16	4	32	15.663	14.364	71	64	65536
16	4	48	254.645	253.032	1227	1192	65536

m, ℓ and exemplary number a of attackers

6.5 Conclusion

We have shown that a point-to-point physical layer key generation is possible in the presence of passive and active attackers, although the achievable secret key rate significantly depends on the given scenario. These point-to-point keys can be used to ensure confidentiality and integrity of an end-to-end key exchange if we just consider outside attackers. In the case of passive insiders, we need to transmit partial keys on different paths to establish a confidential end-to-end key. If there is at least one trustworthy path and this path is used for transmission of a partial key, the combined end-to-end key is kept secret from the attacker. However, using all available paths to ensure confidentiality is either highly costly even for smaller networks or impossible for larger networks due to the exponential growth of paths with larger networks. Hence, we evaluated a reasonable number of paths and how to select them best for different networks of forwarders. We have shown that with a good path selection we can significantly reduce the number of necessary paths to find a trustworthy one and therewith establish a confidential end-to-end key with a certain probability $1 - \varepsilon$ that can be set accordingly.

However, this evaluation is just a first step on the feasibility of end-to-end keys established by means of physical layer point-to-point keys. For continuation, we need to look on the performance of the physical layer key exchange to compare the effort of the proposed scheme to common key exchange protocols. Furthermore, it is also necessary to consider active insiders. One possible direction is to investigate the use of majority schemes.

Acknowledgments This work is supported in part by the German Research Foundation (DFG) in the Collaborative Research Center 912 “Highly Adaptive Energy-Efficient Computing” and by the Federal Ministry of Education and Research of the Federal Republic of Germany (Förderkennzeichen 16 KIS 0009, Prophylaxe). The authors alone are responsible for the content of the chapter.

References

1. Ahlswede R, Csiszár I (1993) Common randomness in information theory and cryptography—part I: secret sharing. IEEE Trans Inf Theory 39(4):1121–1132
2. Bloch M, Barros J (2011) Physical-layer security: from information theory to security engineering. Cambridge University Press, Cambridge
3. Boyd C, Mathuria A (2003) Protocols for authentication and key establishment. Springer, Berlin
4. Engelmann S, Wolf A, Jorswieck EA (2014) Precoding for secret key generation in multiple antenna channels with statistical channel state information. In: Proceedings of the IEEE international conference on acoustics, speech, and signal processing (ICASSP), Florence, Italy
5. Fettweis G, Nagel W, Lehner W (2012) Pathways to servers of the future. In: Design, automation and test in europe conference exhibition (DATE), pp 1161-1166
6. Jorswieck EA, Wolf A, Engelmann S (2013) Secret key generation from reciprocal spatially correlated MIMO channels. In: Proceedings of the 56th IEEE global communications conference (GLOBECOM), Atlanta, USA, invited
7. Liang Y, Kramer G, Poor HV, Shamai (Shitz) S (2009) Compound wiretap channels. EURASIP J Wirel Commun Netw
8. Liang Y, Poor HV, Shamai (Shitz) S (2009) Information theoretic security. Found Trends Commun Inf Theory **5**(4-5):355–580
9. Ling H, Znati T (2007) End-to-end pairwise key establishment using node disjoint secure paths in wireless sensor networks. IJSN 2(1/2):109–121
10. Maurer UM (1993) Secret key agreement by public discussion from common information. IEEE Trans Inf Theory 39(3):733–742
11. Tomasin S, Jorswieck EA (2014) Pilot-based secret key agreement for reciprocal correlated MIMOME block fading channels. In: Proceedings of the 57th IEEE global communications conference (GLOBECOM), Austin, USA
12. Vía J (2014) Robust secret key capacity for the MIMO induced source model. In: Proceedings of the IEEE international conference on acoustics, speech and signal processing (ICASSP), Florence, Italy
13. Wolf A, Jorswieck EA (2011) Maximization of worst-case secret key rates in MIMO systems with eavesdropper. In: Proceedings of the 54th IEEE global communications conference (GLOBECOM), Houston, USA
14. Wong TF, Bloch MR, Shea JM (2009) Secret sharing over fast-fading MIMO wiretap channels. EURASIP J Wirel Commun Netw

Chapter 7
Experimental Results on Secret-Key Extraction from Unsynchronized UWB Channel Observations

Gianni Pasolini, Enrico Paolini, Davide Dardari and Marco Chiani

Abstract Wireless channel reciprocity can be exploited by two users willing to achieve confidential communications over a public channel as a common source of randomness for the generation of a secret key. In this chapter, the important issue of signal synchronization between the two users is discussed and a simple and practical solution is proposed to overcome this problem. The proposed scheme is tested with a real measurements campaign aimed at extracting secret-keys from the physical parameters of ultrawide bandwidth channels in an indoor scenario. The proposed solution is proved to be effective, as shown in the numerical results that provide an insight on the rate of agreement between the keys separately generated by the two users.

7.1 Introduction

Over the last few years, the importance of wireless communications in everyday life has dramatically increased owing to the widespread diffusion of smart devices, such as tablets and smartphones, enabling ubiquitous communications and a broad range of services and applications. The issue of privacy in wireless networks is becoming, therefore, more and more relevant, especially for security-critical services such as electronic payments and eHealth [24].

G. Pasolini (✉) · E. Paolini · D. Dardari · M. Chiani
Department of Electrical, Electronic, and Information Engineering,
"G. Marconi" University of Bologna, Bologna, Italy
e-mail: gianni.pasolini@unibo.it

E. Paolini
e-mail: e.paolini@unibo.it

D. Dardari
e-mail: davide.dardari@unibo.it

M. Chiani
e-mail: marco.chiani@unibo.it

M. Baldi and S. Tomasin (eds.), *Physical and Data-Link Security Techniques for Future Communication Systems*, Lecture Notes in Electrical Engineering 358, DOI 10.1007/978-3-319-23609-4_7

Unfortunately, the intrinsic broadcast nature of the propagation medium makes wireless communications highly susceptible to eavesdropping. The adoption of reliable and effective cryptographic techniques is thus mandatory to protect transmitted data from being disclosed to unintended parties.

Currently used ciphers exploit the computational hardness of recovering the message from the ciphertext without knowing the key (*computational security*) [5]. The confidentiality of data relies on symmetric or asymmetric ciphering: in the former the sender and the recipient share a common key that is used to perform both encryption and decryption, whereas in the latter the sender encrypts data with one key (public key) and the recipient uses a different key (private key) for the decryption.

It is well know that symmetric ciphering suffers from the fundamental problem of key distribution, whereas asymmetric ciphering is computationally intensive, especially for low complexity devices subject to severe energy constraints (as expected in Internet of Things applications) [9]. Moreover, it is based on the unproven assumption that certain one-way functions are hard to invert [5]. Therefore, asymmetric ciphering techniques may potentially be compromised if computational power increases dramatically or efficient methods for solving the underlying mathematical problems are discovered [2].

Recently, *information-theoretic security* has been proposed to complement or replace classic cryptographic techniques, with the purpose to increase the security of wireless communications or to reduce the implementation complexity. It does not require a preliminary key exchange and it is stronger than computational security because no assumptions on the eavesdropper's computational power is needed and perfect secrecy can be theoretically achieved (*unconditional security*) [11].

The basis of information-theoretic security dates back to Shannon, who provided an example of perfect cipher, namely one-time pad, in which the message is concealed by adding (modulo 2) a random secret-key of the same length. Shannon defined a cipher system to be perfect if the mutual information between the message M and the ciphertext C is zero, i.e., $I(M; C) = 0$, by assuming that the eavesdropper has a perfect copy of C. He then proved that perfect secrecy is achievable only when the entropy of the random secret key K is larger than or equal to that of M (i.e., when the size of the key is at least as large as the size of the message) [6].

The pessimistic Shannon's assumption of perfect availability of C at the eavesdropper was successively relaxed by Wyner [26] with the introduction of the *wire-tap channel* model, in which the eavesdropper has only a degraded version of C. Starting from this model he showed that (virtually) perfect secrecy can still be reached without sharing a secret-key, provided that the legitimate parties have some "advantage" with respect to the eavesdropper. Specifically, the secrecy capacity, defined as the largest achievable secret communication rate, of the wire-tap channel is different from zero (i.e., the secret communication is possible) only if the channel from the sender to the legitimate receiver is "stronger" than the channel from the sender to the eavesdropper. A problem with advantage-based methods is that some knowledge about the eavesdropper channel quality is required [10] and the advantage (channel state) is often not under control of the legitimate parties [1, 20].

Another approach is to use a common source of information between intended parties, partially unknown to the eavesdropper, and exploit it to generate a common secret key K to use for message ciphering over a public channel [21]. Maurer [16] showed that, as opposed to the wire-tap channel, the sender and the receiver can still agree on a secret key even when the channel secrecy capacity is equal to zero, provided they have access to a common source. He proved that key agreement can be reached through an iterative exchange of messages over a public channel fully accessible to the eavesdropper. The secret keys so generated may then be used either in one-time pad cipher schemes, or as secret keys for existing symmetric-key encryption systems.

As firstly proposed in [8], radio propagation characteristics may also be used as common source of information for secret key agreement. Owing to the channel reciprocity, in fact, this information represents a common source of randomness exploitable by both ends of a communication link to separately generate a common encryption key. Any eavesdropper, located in a different position with respect to the legitimate users, will not observe the same channel and therefore will hardly be able to guess the same key [17].

Several solutions have been proposed that aim at generating secret-keys observing some channel-dependent characteristic. A channel metric commonly adopted for the key generation is, for instance, received signal strength (RSS), because it is usually provided by wireless devices [18]. Other suggested key generation strategies exploit:

- the magnitude or phase information of narrowband channels [22];
- the frequency diversity of wideband communications (e.g., orthogonal frequency division multiplexing (OFDM) [7] or ultrawide bandwidth (UWB) communications [13, 15, 25]);
- the spatial diversity of multiple-input multiple-output (MIMO) systems [17].

Besides the available physical layer, the choice of the metric depends also on its sensitivity to possible imperfect reciprocity issues caused by implementation aspects. The different front-ends (amplifiers, filters, etc.) of the legitimate users' devices may have a detrimental impact on the correlation of the channels. Similarly, accurate time synchronization between the legitimate users is a critical issue potentially able to dramatically reduce the correlation between their observations.

In this chapter we focus on the UWB technology that, owing to its fine time resolution (in the order of nanoseconds), can provide accurate and information-rich measurements of the channel response to some stimulus and can be favorably employed for secret-key extraction [25]. Throughout the chapter, we highlight a main issue in exploiting the UWB technology not addressed in previous works on the subject, represented by the critical *time synchronization* of the legitimate users' observations. Even in the case of a perfect channel reciprocity, in fact, the waveforms acquired by the two legitimate users are likely to be misaligned in the time domain. This issue, arising when performing experimental activities using real devices, is usually neglected by key generation algorithms proposed by the literature in the field. In order to exploit the channel reciprocity, however, any actual implementation of key generation algorithm must adopt effective countermeasures to overcome this issue. In this chapter an original solution is presented that makes the key generation algorithm insensitive to time misalignments. Its effectiveness is evaluated with a measurements campaign in an indoor scenario, with the purpose to highlight the impact of system parameters on the key generation process and its robustness to attacks. Since our main purpose is to present the new approach, its feasibility is tested using standard techniques to extract the secret-key from the received waveforms. A fine tuning of the involved parameters or the implementation of more sophisticated *ad-hoc* techniques are out of the scope of this chapter.

7.2 Problem Statement

Alice and Bob are legitimate users willing to establish a secure wireless connection in the presence of a passive eavesdropper,[1] denoted in the following by Eve. Thanks to the wireless channel reciprocity, the channel between Alice and Bob represents a common source of randomness that can be jointly exploited by the two legitimate users to separately generate a common secret-key. The eavesdropper, being in a different position with respect to Bob and Alice, observes a different channel and is thus prevented, in principle, from generating the same key. The key is then used to encrypt and decrypt Alice and Bob's communications over a public channel.

A typical sequential key generation algorithm consists of the following steps [3]:

- *Randomness sharing* (or *channel probing*), which corresponds to the observation by both Alice and Bob of some channel feature (e.g., impulse response, magnitude, phase rotation, RSS, frequency selectivity);
- *Advantage distillation*, an optional step aimed at "distilling" observations for which Alice and Bob have an advantage on Eve;
- *Information reconciliation*, that is devoted to correct the keys mismatch due to noise, interference, asymmetric equipments, etc. This step is usually preceded or jointly implemented with a quantization phase of the observed metric. Key agreement can be reached through public discussions over a channel fully accessible by the eavesdropper (the public channel);
- *Privacy amplification*, a deterministic independent processing of the common bit sequences in order to generate a secure secret-key. Hash functions can be conveniently used, for instance, to increase the key security, as they are designed to generate significantly different outputs even with similar inputs. Therefore, even slight mismatches of Eve's key with respect to the legitimate key produce, after the hash function processing, significant discrepancies.

With respect to the above outlined key generation procedure, this chapter addresses steps 1 (*Randomness sharing*) and 3 (*Information reconciliation*), which are discussed in the following.

[1] Throughout the chapter we assume that the eavesdropper does not take any action apart from trying to listen Alice and Bob' transmissions without being detected.

7.3 Frequency Domain Randomness Sharing

The randomness sharing step is aimed at generating correlated observations of some channel-dependent feature to be used by Alice and Bob as a common source of randomness for the key generation. To exploit channel reciprocity for shared secret-key generation, the legitimate users send alternatively to each other a known probing signal $p(t)$ having center frequency f_0 and bandwidth W. Denote by $r_{xy}(t)$ the signal received by node $y \in \{\text{Alice, Bob, Eve}\}\backslash\{x\}$ corresponding to the probing signal sent by node $x \in \{\text{Bob, Alice}\}$, given by

$$r_{xy}(t) = s_{xy}(t - \tau_{xy}) + n_y(t), \tag{7.1}$$

where $s_{xy}(t)$ is the response to $p(t)$ of the channel between nodes x and y, τ_{xy} the communication delay between nodes x and y, and $n_y(t)$ the AWGN.

When channel reciprocity holds, we have $s_{\text{Alice Bob}}(t) \approx s_{\text{Bob Alice}}(t)$, whereas in general Eve, due to her different position, is expected to experience a channel response significantly different from that seen by Alice and Bob.

The secret-key generation algorithm task consists of observing $r_{xy}(t)$ in a proper time interval with duration T_{ob} and of deriving a sequence of bits according to some specific method. We assume the observation interval includes the whole channel response[2] and, as worst case, that also Eve is aware of the algorithm adopted by Alice and Bob as well as of $p(t)$.

As pointed out in the introduction, existing key generation algorithms based on channel reciprocity work in the time-domain and tacitly assume a perfect time synchronization among Alice and Bob [13]. A time mismatch, even in the order of $100 - 200$ ps, might prevent time-domain based algorithms to work properly. Unfortunately, in practical UWB systems synchronization algorithms can hardly reach a precision below 1 ns, making most of the proposed time-domain based schemes not applicable in general [4].

To overcome this issue, we propose an alternative algorithm whose performance is independent of the timing mismatch, thus not requiring a tight synchronization among nodes. Denote by $r(t) = s(t - \tau) + n(t)$ the signal received by the generic node (Alice, Bob or Eve). Without loss of generality the noise component can be expressed as $n(t) = \tilde{n}(t - \tau)$ by preserving the same statistical characteristics due to the stationarity of the random process. Consider the Fourier transform $R(f)$ of $r(t)$ calculated in the observation interval T_{ob}. It can be expressed as

$$R(f) = S(f)\, e^{-j2\pi f\tau} + \tilde{N}(f)\, e^{-j2\pi f\tau}\,, \tag{7.2}$$

[2] This requires a mild synchronization among Alice and Bob which does not pose any challenging issue from a practical viewpoint.

where $S(f)$ and $\tilde{N}(f)$ are the Fourier transforms of $s(t)$ and $\tilde{n}(t)$, respectively, taken in the same observation interval T_{ob}. Next, introduce the filtering function

$$\Pi(f) = \begin{cases} 1 & \text{if } f \in \left[f_0 - \frac{W}{2}, f_0 + \frac{W}{2}\right] \\ 0 & \text{otherwise.} \end{cases}$$

It is immediate to show that the signal defined as

$$Z(f) = |R(f)|\Pi(f) = \left|S(f) + \tilde{N}(f)\right| \Pi(f) \tag{7.3}$$

does not depend on τ. By sampling $Z(f)$ in K frequencies f_k uniformly distributed in the interval $[f_0 - W/2, f_0 + W/2]$ we can construct a sequence $z_k = Z(f_k)$, for $k = 1, 2, \ldots, K$, of samples that can be used successively as source of randomness to generate the secret-key, regardless synchronization mismatches.

Operatively, the above technique may be implemented at each receiver by sampling the waveform received over the observation window T_{ob}, performing the fast Fourier transform (FFT) of the obtained samples and taking the amplitude of each frequency-domain sample. The price to pay for the transformation (7.3) is the loss of half of the overall available information exploitable from the channel response.[3] This will lead to a potential reduction of the generated secret-key length.

7.4 Information Reconciliation

At the end of the *randomness sharing* step, both Alice and Bob have derived their own set of frequency domain samples $z_k = Z(f_k)$, for $k = 1, 2, \ldots, K$.

In our experimental setup both Alice and Bob skip the optional *advantage distillation* phase and start the *information reconciliation* procedure, according to the following steps:

- The set of frequency domain samples is passed through a uniform quantization procedure. Each node, either Alice or Bob, adapts its quantizer dynamic range to make it coincident with the dynamic range of derived amplitude-spectrum. This means that, in the frequent case where the amplitude-spectra derived by Alice and Bob have different dynamic ranges, the quantization steps they adopt are different. This solution allows to cope with possible (very likely) differences between Alice and Bob's front-end gains (amplifier gains, connector attenuations, etc.).
- In order to reduce the mismatch between the quantized amplitude-spectra derived by Alice and Bob, censored regions are possibly introduced around the quantization thresholds. Both Alice and Bob discard those frequency-domain samples of their respective quantized amplitude-spectra that fall within the censored regions and

[3] This is due to the fact that, using this technique, we cannot exploit the information content associated with the channel response phase spectrum.

communicate to the counterpart the indexes of discarded values. The effect of this step is twofold: on the one side it increases the key agreement probability between Alice and Bob, removing possible ambiguities. On the other side, it reduces the amount of information available for the key generation, which results in shorter secret-keys.

- The quantized amplitude-spectra, deprived of censored values (if any), are Grey-coded by each node in order to minimize the amount of wrong bits in case of quantization mismatch between Alice and Bob. This step, performed by both Alice and Bob, produces two sequences of bits that constitute the raw keys to be reconciliated through an exchange of messages over the public channel.
- The public phase of the adopted reconciliation technique is the one suggested in [25] for the linear block coding case. More specifically, the technique is based on an (n, k) linear block code $\mathscr{C}$ that is known to both legitimate users (and to the eavesdropper) and on its standard array. The standard array of $\mathscr{C}$ is a table having 2^{n-k} rows and 2^k columns, each entry of which is one of the 2^n possible binary words of length n. Letting H be a parity-check matrix of $\mathscr{C}$, each row of the standard array is associated with a specific syndrome, in that all 2^k length-n binary words in the row generate the same syndrome when multiplied by the transpose of H. All words in the same row form a coset and the first word in the row is dubbed the coset leader. The cosets are indexed from 0 to $2^{n-k} - 1$ while the elements in a coset are indexed from 0 to $2^k - 1$. The first row of the standard array contains all 2^k codewords, in an ascending Hamming weight order (so that its coset leader is the all-0 codeword). The coset leader of any other row is a binary length-n pattern of minimum Hamming weight, yielding the syndrome associated with that coset, while each other word in the coset is the bit-wise sum of the coset leader with the corresponding codeword in the first row.

  The reconciliation technique works as follows. Both legitimate users perform a segmentation of their raw keys into fragments of length n bits each. One of the two legitimate users, say Alice, transmits to the other, say Bob, the index of the coset to which the fragment belongs and takes note, without transmitting, of the correspondent column index. The coset indexes are transmitted on a public channel accessible to Eve. For each received coset index, Bob identifies, in the standard array of $\mathscr{C}$, the column index of the length-n word in the coset that is at minimum Hamming distance from the corresponding fragment in his raw key. Both Alice and Bob replace their length-n fragments with the length-k column indexes so generated. A key of $t\,k$ bits, for some integer $t > 1$, is thus obtained from a raw key of $t\,n$ bits.

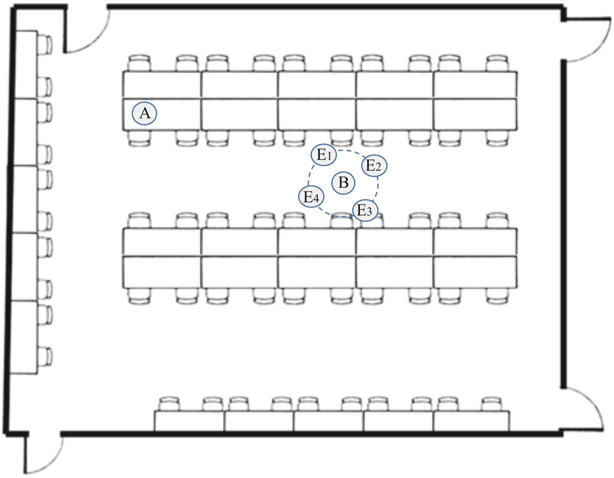


Fig. 7.1 Indoor scenario where the waveforms acquisition experiments were carried out. Alice and Bob were in fixed positions; four different Eve's locations were considered for each Bob-Eve distance

7.5 Numerical Results

7.5.1 Randomness Sharing: Experimental setup

In order to implement the *randomness sharing* step using impulse radio UWB signals, we performed a measurements campaign in the hardware laboratory of our Department, an indoor scenario composed of walls, furniture, and instrumentation.

Time Domain PulsOn 410 nodes [23] were employed to impersonate Alice, Bob, and Eve. Each of these radio devices owns a Broadspec planar elliptical dipole antenna and its equivalent isotropically radiated power (EIRP) is equal to -12.8 dBm. The generated UWB signal has a frequency band centered at 4.2 GHz. Channel probing was performed by transmitting UWB waveforms with a time duration in the order of 2 ns. To increase the signal-to-noise ratio (SNR), an integration factor $N_s = 1024$ has been used. The amplitude of the acquisition window was $T_{\rm ob} = 21$ ns, allowing to capture multipath components due to the cluttered environment. Finally, the sampling time was set to 61.03 ps.

A floor plan of the environment where measurements were acquired is shown in Fig. 7.1, in which the positions of Alice, Bob, and Eve are also illustrated. As it can be seen, Alice and Bob nodes were kept in a fixed position for all measurements, 4.5 m far apart, while different positions of Eve were considered. The node impersonating Eve was positioned, in particular, at a distance $d_{\rm Eve}$ of 20, 30, and 40 cm from Bob.[4]

[4] It has been shown via extensive measurement campaigns that indoor UWB channels become independent for antenna displacements larger than about 15 cm [19].

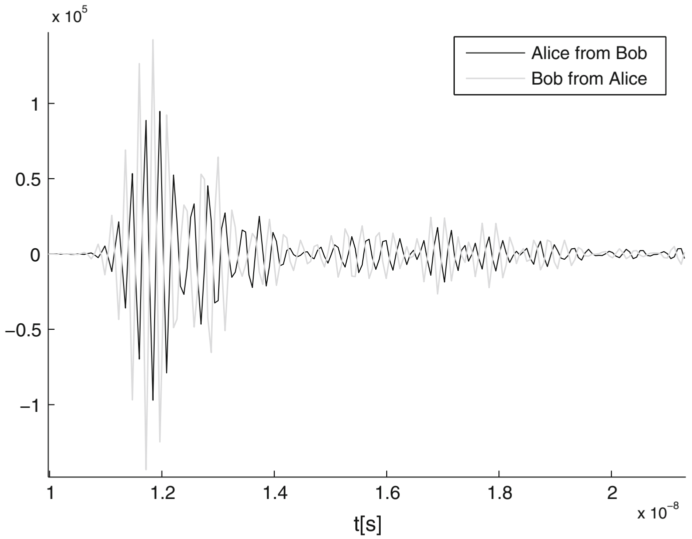


Fig. 7.2 Examples of UWB waveforms acquired by Alice and Bob over some time window having the same amplitude for both users. The two waveforms are approximately equal to each other apart from a shift in the time domain (synchronization error) and from a scaling factor (this latter due to different front-end characteristics)

For each distance d_{Eve}, four Eve's positions were considered, with angular separation of 90° one to the other in the circle of radius d_{Eve} centered at Bob.

Under channel reciprocity conditions, the signals received by Alice and Bob are approximately equal, apart from a possible misalignment τ in the time domain and a scale factor due to front-end differences. An illustrative example is reported in Fig. 7.2, that shows two UWB waveforms collected by Alice and Bob during our measurements. In Fig. 7.3 the corresponding amplitude spectra are shown along with the spectrum derived by Eve, positioned at 20 cm from Bob, starting from the signal received from Alice. As it can be observed, apart from a scale factor due to front-end asymmetries, Alice and Bob's spectra show a good agreement, that confirms the effectiveness of the method proposed in Sect. 7.3. The spectrum derived by Eve, instead, shows significant differences with respect to the previous ones. In general, the correlation between the spectra derived by Eve and those derived by Alice and Bob depends on the propagation scenario and the position of Eve with respect to the legitimate users [12–14].

7.5.2 Measured Performance

By means of the previously described experimental setup, we finally derived the secret-keys generated by Alice, Bob and Eve on the basis of the actual UWB signals

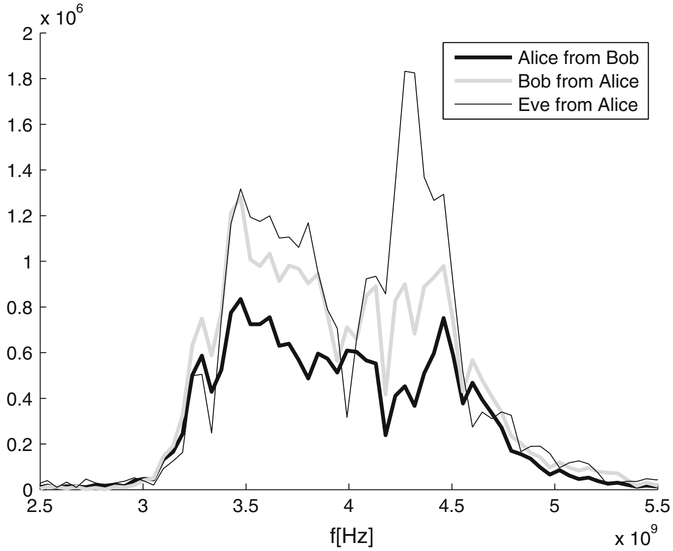


Fig. 7.3 Example of amplitude spectra at Alice, Bob and Eve, with Eve at 20 cm from Bob. Eve's spectrum has bee derived starting from the signal received from Alice

they observed in the indoor scenario depicted in Fig. 7.1. All of them were collected and the performance of the proposed key generation algorithm was investigated in terms of:

- *Agreement rate* between Alice and Bob's secret keys, defined as the ratio between the number of Alice and Bob's keys that exhibited a perfect matching and the total number of generated keys;
- *Eve success rate*, defined as the ratio between the number of Eve's keys that perfectly matched the key on which Alice and Bob agreed and the total number of generated keys;
- *Key length*, i.e., the length of the secret-keys on which Alice and Bob reached an agreement.

These performance metrics have been investigated under different conditions in terms of:

- Eve's distance from Bob. For each distance $d_{\mathrm{Eve}} \in \{20, 30, 40\,\mathrm{cm}\}$, the *randomness sharing* and *information reconciliation* steps were executed 2000 times for each of the four positions of Eve around Bob. It follows that 8000 secret-keys were generated for each d_{Eve}.
- Number n_{bits} of bits used to quantize the received signal's amplitude-spectrum. Numerical results have been derived, in particular, considering $n_{bits} = 2$ and $n_{bits} = 3$, with $2^{n_{bits}}$ representing the corresponding number of quantization intervals.

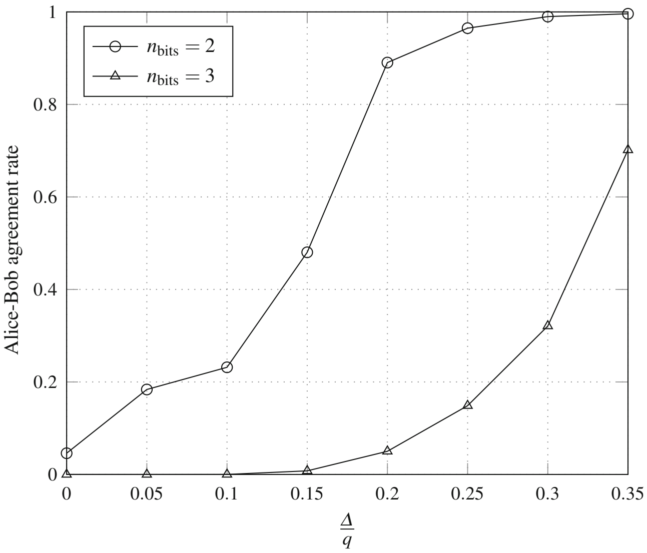


Fig. 7.4 Alice and Bob agreement rate for $d_{\text{Eve}} = 20\,\text{cm}$

- The amplitude Δ of censored regions. In the following, all performance metrics are investigated as a function of $\frac{\Delta}{q}$, with $q = \frac{\max\{Z(f)\}}{2^{n_{bits}}}$ denoting the amplitude of the quantization interval. Please note that, owing to possible differences of Alice and Bob's front-ends, the amplitude-spectra separately derived by the legitimate users could have different dynamic ranges, as shown in Fig. 7.3. It follows that, in general, Alice and Bob operate with different values of q.

The key agreement rate between Alice and Bob is investigated in Fig. 7.4 as a function of both $\frac{\Delta}{q}$ and n_{bits}, in the case $d_{\text{Eve}} = 20\,\text{cm}$. As expected, this performance metric improves for increasing values of $\frac{\Delta}{q}$, regardless the value of n_{bit}: removing the samples of the amplitude-spectrum that fall near the quantization boundaries reduces, in fact, the key mismatch events. The comparison between the two curves shows, moreover, that the choice of n_{bit} has a significant impact on the experienced agreement rate: a remarkable performance degradation is observed, in fact, simply passing from $n_{bit} = 2$ to $n_{bit} = 3$. Please notice, however, that the choice of n_{bit} impacts also on the secret-key length, hence, in order to get a complete picture of the key generation performance from Alice and Bob's perspective, this performance metric deserves a specific investigation.

Figure 7.5 shows, on this regard, the mean value of the key length and the correspondent standard deviation as a function of $\frac{\Delta}{q}$ in both cases of $n_{bit} = 2$ and $n_{bit} = 3$, with $d_{\text{Eve}} = 20\,\text{cm}$. Please recall that mean values and standard deviations were derived considering only those keys for which Alice and Bob experienced an

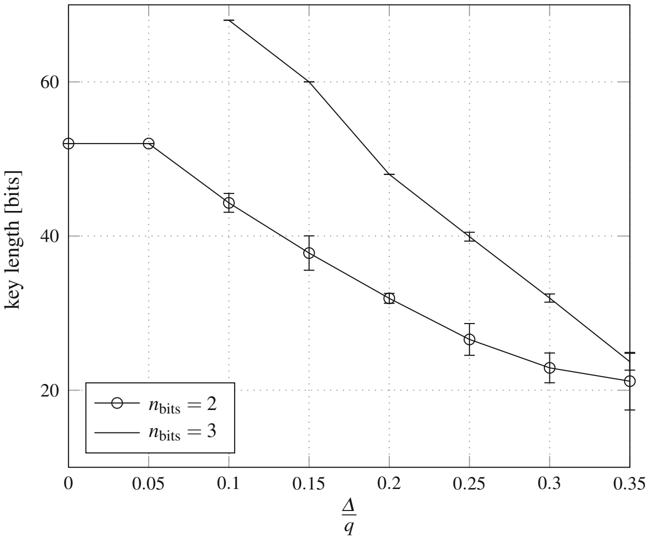


Fig. 7.5 Mean key length and related standard deviation for $d_{\text{Eve}} = 20\,\text{cm}$

agreement. As far as the impact of $\frac{\Delta}{q}$ is concerned, it is straightforward to understand that for increasing values of $\frac{\Delta}{q}$ the number of samples of the amplitude-spectrum that are discarded increases as well, which results in shorter secret-keys. Figure 7.5 also shows that larger values of n_{bits}, although more critical in terms of agreement rate, lead to less dispersed and larger (hence more secure) key lengths.

The key security issue is investigated, in particular, in Fig. 7.6, that shows the role played by d_{Eve} and $\frac{\Delta}{q}$ on Eve's success rate in the case $n_{bit} = 2$. The increasing trends of the curves for increasing values of $\frac{\Delta}{q}$ is not surprising: also Eve benefits, in fact, from the removal of the ambiguous samples of the signal amplitude-spectrum.

The impact of d_{Eve} on Eve's success rate is, instead, less intuitive. In the scenario we considered it appears, in fact, that the threat posed by Eve increases as her distance from Bob gets larger. Observe, however, that although the cross-correlation between the channels experienced by Eve and the legitime users' channel asymptotically tends to zero as d_{Eve} increases, it is also true that the way such cross-correlation approaches to zero could not be monotonically decreasing. It follows that, locally, increasing values of d_{Eve} could correspond to increasing values of the channels' cross-correlation, and therefore to higher Eve's success rates. Let us stress, however, that as long as $\frac{\Delta}{q} \leq 0.25$, the presence of Eve does not significantly undermine the secrecy of Alice and Bob's communications, even for the very short d_{Eve} distances here considered. Please notice that for $n_{bit} = 2$, values of $\frac{\Delta}{q}$ in the range 0.2–0.25 provide both an agreement rate larger than 90 % and an Eve's success rate close to zero.

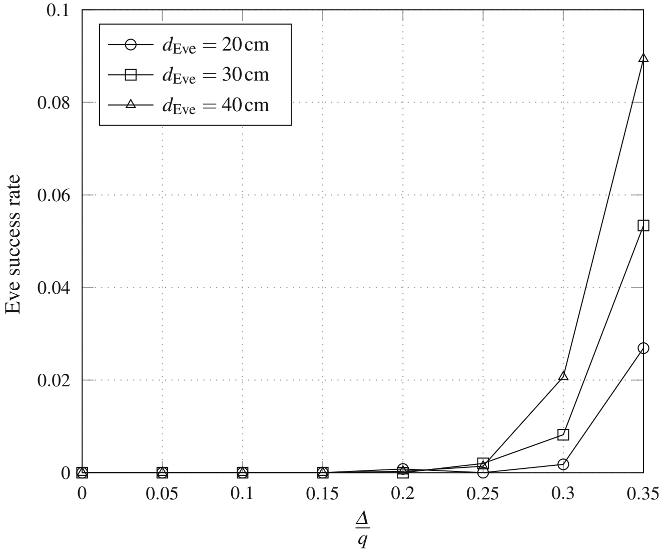


Fig. 7.6 Eve's success rate as a function of $\frac{\Delta}{q}$ and d_{Eve}, $n_{bits} = 2$

7.6 Conclusions

In this chapter we addressed secret-key generation on the basis of correlated channel observations carried out by two legitimate users willing to encrypt their communications over a public channel. We proposed, in particular, an original strategy to cope with the issue of time synchronization, which is particularly critical when UWB signals are used to probe the channel. The results of the experimental activity we carried out to validate our solution were presented, showing both its effectiveness and its sensitivity to relevant parameters that affect its performance.

Acknowledgments We wish to thank Nicoló Decarli for setting up the experimental testbed.

References

1. Ahlswede R, Csiszar I (1993) Common randomness in information theory and cryptography. I. Secret sharing. IEEE Trans Inf Theory 39(4):1121–1132
2. Bernstein DJ, Buchmann J (2009) Post-quantum cryptography. Springer, Berlin
3. Bloch M, Barros J (2011) Physical-layer security. Information theory to security engineering. Cambridge University Press, Cambridge
4. Dardari D, Conti A, Ferner U, Giorgetti A, Win M (2009) Ranging with ultrawide bandwidth signals in multipath environments. In: Proceedings of the IEEE **97**(2):404–426
5. Diffie W, Hellman M (1976) New directions in cryptography. IEEE Trans. Inf. Theory 22(6):644–654

6. El Gamal A, Kim YH (2011) Network information theory. Cambridge University Press, Cambridge
7. El Hajj Shehadeh Y, Alfandi O, Hogrefe D (2012) Towards robust key extraction from multipath wireless channels. J Commun Netw
8. Hershey J, Hassan A, Yarlagadda R (1995) Unconventional cryptographic keying variable management. IEEE Trans Commun 43(1):3–6
9. Iera A, Floerkemeier C, Mitsugi J, Morabito G (2010) The internet of things (guest editorial). IEEE Wirel Commun 17(6):8–9
10. Li J, Petropulu A (2011) On ergodic secrecy rate for Gaussian MISO wiretap channels. IEEE Trans Wirel Commun 10(4):1176–1187
11. Liang Y, Poor HV, Shamai (Shitz) S (2008) Information theoretic security. Found Trends Commun Inf Theory **5**(4–5):355–580. http://dx.doi.org/10.1561/0100000036
12. Madiseh M, McGuire M, Neville S, Shirazi A (2008) Secret key extraction in ultra wideband channels for unsynchronized radios. In: Proceedings of the 6th annual communication networks and services research conference (CNSR) 2008, pp 88–95
13. Madiseh M, He S, McGuire M, Neville S, Dong X (2009) Verification of secret key generation from UWB channel observations. In: IEEE international conference on communications (ICC) 2009, pp 1–5
14. Madiseh M, Neville S, McGuire M (2010) Time correlation analysis of secret key generation via UWB channels. In: IEEE global telecommunications conference (GLOBECOM) 2010, pp 1–6
15. Marino F, Paolini E, Chiani M (2014) Secret key extraction from a UWB channel: analysis in a real environment. In: IEEE international conference on ultra-wideband (ICUWB) 2014, pp 80–85
16. Maurer U (1993) Secret key agreement by public discussion from common information. IEEE Trans Inf Theory 39(3):733–742
17. Pasolini G, Dardari D (2015) Secret information of wireless multi-dimensional gaussian channels. IEEE Trans Wirel Commun 14(6):3429–3442
18. Patwari N, Croft J, Jana S, Kasera S (2010) High-rate uncorrelated bit extraction for shared secret key generation from channel measurements. IEEE Trans Mobile Comput 9(1):17–30
19. Prettie C, Cheung D, Rusch L, Ho M (2002) Spatial correlation of UWB signals in a home environment. In: IEEE conference on ultra wideband systems and technologies, 2002. Digest of Papers, pp 65–69
20. Rabbachin A, Conti A, Win M (2015) Wireless network intrinsic secrecy. IEEE/ACM Trans Netw 23(1):56–69
21. Ren K, Su H, Wang Q (2011) Secret key generation exploiting channel characteristics in wireless communications. IEEE Wirel Commun 18(4):6–12
22. Severi S, Abreu G, Pasolini G, Dardari D (2014) A secret key exchange scheme for near field communication. In: IEEE wireless communications and networking conference (WCNC) 2014, pp 428–433
23. Time Domain Corporation (2008) System analysis module user's manual—PulsON 220TM UWB Radio
24. Weber RH (2010) Internet of things new security and privacy challenges. Comput Law Secur Rev 26(1):23–30
25. Wilson R, Tse D, Scholtz R (2007) Channel identification: secret sharing using reciprocity in ultrawideband channels. In: IEEE international conference on ultra-wideband (ICUWB) 2007, pp 270–275
26. Wyner AD (1975) The wire-tap channel. Bell Syst Tech J **54**(8):1334–1387. http://ci.nii.ac.jp/naid/80013288768/en/

Chapter 8
Physical Layer Security in Power Line Communication Networks

Alberto Pittolo and Andrea M. Tonello

Abstract This chapter digs into the secrecy provided and guaranteed at the physical layer, named physical layer security (PLS), over power line communication (PLC) channels for in-home networks. The PLC scenario peculiarities are briefly discussed in terms of channel characteristics and noise features. The effects of the channel properties on the performance are evaluated, in terms of the achievable secrecy rate, starting from the single-input single-output (SISO) scheme with additive white Gaussian noise. The results are also compared to the more common wireless scenario, namely a scenario where the channels are independent and experience Rayleigh fading as a consequence of rich scattering. Furthermore, the performance improvement attainable with the use of multiple-input multiple-output (MIMO) transmission is discussed. The effect of increasing the transmission band 2–30 to 2–86 MHz and the effect of colored spatially correlated noise is also investigated. Moreover, a non uniform power allocation strategy, provided by the application of an alternating optimization (AO) approach is evaluated. A comparison with the channel capacity, achieved without secrecy constraints, is also performed. The experimental results are provided relying on measured noise and channel responses.

8.1 Introduction

In recent years we have witnessed a fast and worldwide increase of data connectivity demand. This is due to the widespread use of social media services and multimedia content access. In order to satisfy this continuously growing amount of data transfer needs, new wireless and wireline technologies and standards have been developed.

A. Pittolo
University of Udine, Via Delle Scienze 206, 33100 Udine, Italy
e-mail: alberto.pittolo@uniud.it

A.M. Tonello (✉)
Alpen-Adria-Universität, Universitätsstraße 65-67,
9020 Klagenfurt am Wörthersee, Austria
e-mail: andrea.tonello@aau.at

M. Baldi and S. Tomasin (eds.), *Physical and Data-Link Security Techniques for Future Communication Systems*, Lecture Notes in Electrical Engineering 358, DOI 10.1007/978-3-319-23609-4_8

Among the no-new-wires technologies, power line communication (PLC) has gained momentum due to its ability to offer high data rates exploiting the existing power delivery infrastructure. Broadband PLC operates in the band 2–30 MHz, e.g., the HomePlug AV (HPAV) compliant modems [7]. The latest HomePlug AV2 (HPAV2) [24] devices use orthogonal frequency division multiplexing (OFDM), together with multiple-input multiple-output (MIMO) transmission over multiple wires, and an extended band of 2–86 MHz. They can reach data rate in excess of 500 Mbit/s.

However, it is important not only to offer high data rates but also to grant security, especially in a multiuser network context where confidential communications and transactions are exchanged. Although cryptographic mechanisms are generally used, physical layer security can strengthen security by implementing strategies at the physical layer. As the wireless communication medium, the PLC scenario is intrinsically broadcast. Hence, the communication channel is shared among the users in the network so that a transmitted signal can reach each node belonging to the network.

There are essentially two ways to think and provide secrecy in a communication system. At the high levels of the ISO/OSI stack, named complexity-based security, and at the physical layer (the lowest of the ISO/OSI stack levels), known as physical layer security (PLS) [19] or information-theoretic security. The main differences are summarized below.

Complexity-based It is the most common and deployed approach. It includes all the methods and the cryptographic techniques such as the data encryption standard (DES) or the RSA. This cryptographic approach assumes the adversary to have limitations on the computational power and/or available resources. Thus, the computational resources required to extract and decrypt the original message (the plaintext) from the encrypted one (the ciphertext) render it practically infeasible for the adversary in a reasonable time.

Information-theoretic This approach was formulated by Shannon [18] and it is widely accepted as the strictest notion of security. Indeed, in this case, the adversary has unlimited resources, nevertheless no information has to be released. This concept underlies the formulation of the PLS, which exploits the physical medium time, frequency and spatial diversity in order to complement and enhance the security provided by other layers.

Although PLS has been deeply investigated and analyzed for the wireless scenario, little effort has been spent for the PLC case. A preliminary discussion about PLS on PLC has been made by the authors in [15]. Then, the study has been extended in [17] considering the effects of the PLC channel, as well as analyzing the multi-user case. Subsequently, a study about PLS over MIMO PLC channels, in the 2–28 MHz frequency range and with additive white Gaussian noise (AWGN), has been carried out in [25].

In order to perform an analysis of PLS in PLC, it is important to firstly understand the properties of the PLC network and the channel properties. As it will be clear in the following description, the PLC context significantly differs from the wireless context.

8.1.1 Properties of the PLC Channel and Network

Even though wireless and PLC communication scenarios have some similarities, such as the broadcast nature, they significantly differ in channel statistics and properties, background noise and achievable performance. For example, the highly uncorrelated channel assumption, which usually holds in wireless networks, is no longer valid for PLC networks. This is, since wireless networks are essentially based on a star-style structure, while PLC ones deploy a tree topology, with multiple branches departing from the same node, see Fig. 8.1. In this configuration, the links to the end nodes share part of the wires up to a particular node, named pinhole or keyhole, where branches depart. This network topology leads to what is known as keyhole effect [1, 3], which typically affects PLC scenarios. The keyhole effect in cooperative multi-hop PLCs has been recently studied in [11]. As later clarified, this phenomenon causes spatial correlation among the channels and limits the performance.

Another prominent characteristic is the frequency correlation between the subchannels of a multi-carrier transmission scheme, mainly due to cross-talks and coupling effects. Furthermore, the PLC channels are affected by fading which exhibits different statistics from the wireless channels. Indeed, while wireless fading has a well-known Rayleigh amplitude distribution [20], the PLC scenario shows lognormal fading statistics [6, 21], as demonstrated in the following.

A final key feature that should be taken into account is the type of background noise. Unlike the wireless case, the PLC scenario is subject to colored Gaussian noise

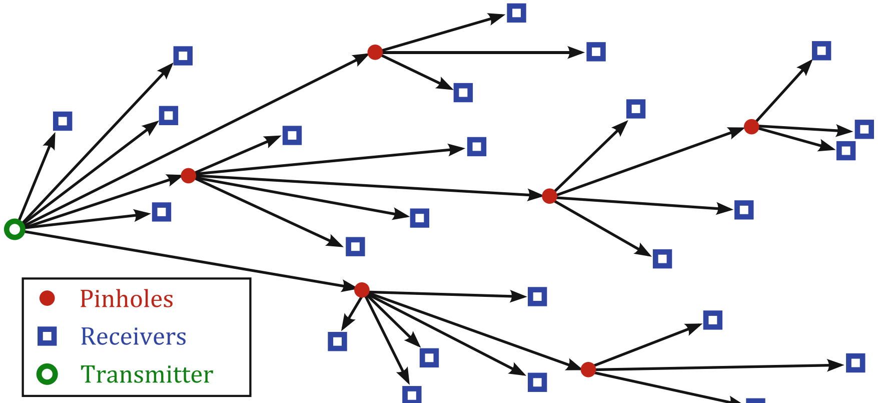


Fig. 8.1 Tree structured scheme of a typical PLC network topology

with an exponential decreasing profile, as discussed in [22]. Consequently, all these channel and noise properties affect the performance achievable on PLC networks with respect to the wireless case, typically affected by uncorrelated Rayleigh fading under AWGN.

8.1.2 Main Contributions

In the following, a brief description of the power line channel is provided, discussing its features and main properties, as well as the achievable performance in terms of maximum secrecy rate. To simplify the presentation first, a simpler single-input single-output (SISO) scenario in the 2–28 MHz frequency range and under AWGN, is considered. The specifications comply with the HPAV standard [7]. In this configuration set up, the effects of the PLC channel properties on the secrecy rate are evaluated and discussed, comparing the main results with a typical wireless case. In particular, independent and Rayleigh fading channels are assumed, as typically happens for rich scattering urban mobile channels.

Then, the multiple-input multiple-output (MIMO) transmission scenario is considered. The power allocation problem is assessed by applying an alternating optimization algorithm. The MIMO transmission considered exploits not only the differential transmission modes over three wires, but also an additional receiving mode, named common mode (CM). The analysis relies on real channel and noise measurements and fulfills the HPAV2 standard specifications [24]. These assumptions allow to provide results of practical relevance.

8.2 PLC Wiretap Channel

The communication channel configuration where a transmitter Alice wishes to send a secret or confidential message x to an intended receiver Bob, so that no information can be inferred by an eavesdropper Eve, is known as wiretap channel, see Fig. 8.2. Eve represents the adversary which tries to detect and disclose the message x having an arbitrarily high amount of available computational resources, as the information-theoretic secrecy foresees. The quantities h_A, h_B and h_E correspond to the channel state information (CSI) between Alice, Bob, and Eve, respectively; the two latter join

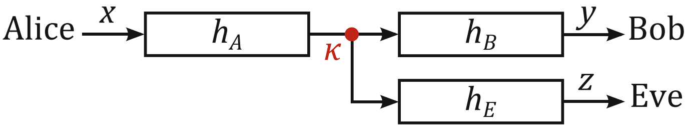


Fig. 8.2 Overall wiretap channel scheme

at the same point, the keyhole κ, while, y and z are the received signals at Bob and Eve, respectively. Note that for the MIMO scheme discussed in Sect. 8.4 the CSIs h_A, h_B and h_E are described by matrices, while the signals x, y and z become vectors.

The wiretap channel was firstly analyzed and introduced by Wyner in [23], where the secrecy rate was firstly found for a simple degraded wiretap channel. In this communication scenario, the channel to Bob (h_B) is considered less noisy than Eve's who receives a degraded, or noisier, version with respect to Bob. This assumption simplifies the analysis, enabling the derivation of the secrecy limits.

A more general broadcast scenario was considered by Csiszár and Körner [4]. The studied generic broadcast channel represents the case in which the channel from Alice (h_A) is assumed as ideal and the channels to Bob (h_B) and Eve (h_E) are statistically independent. This configuration is suitable to represent star-stile networks, such as rich scattering wireless scenarios.

The model depicted in Fig. 8.2 offers a sufficiently general setup by including a keyhole channel structure and can model other communication configurations with the proper assumptions. The branch node κ represents the keyhole, or pinhole from which the links to Bob and Eve depart. Thus, the transmitted signal needs to cross the keyhole and travel an identical section, represented by h_A, before reaching the intended receiver and the eavesdropper. This introduces spatial correlation and a rank-deficiency of the communication channel, limiting the achievable secrecy rate performance [1, 3, 11]. The keyhole channel scheme in Fig. 8.2 resembles a tree-style network, which is the typical underlying structure of PLC networks.

8.2.1 Secrecy Capacity

The secrecy capacity of the system in Fig. 8.2 represents the amount of information (e.g. bit/s) that can be reliably transmitted to the receiver. This means that the average decoding error probability approaches zero at the intended receiver, while the uncertainty at the eavesdropper, usually expressed by the equivocation rate, equals the secrecy rate. This way, no information is released to the eavesdropper, which cannot decode the messages from Alice at any positive rate lower than the secrecy capacity. For further details the reader is referred to [9]. In the following, a SISO scheme is considered, but all the results can be extended to the MIMO communication scenario. The secrecy capacity, namely the maximum achievable secrecy rate, is defined as [13]

$$C_S = \max_{f_X \in \mathscr{F}} [I(X;Y) - I(X;Z)]^+, \tag{8.1}$$

where f_X and $\mathscr{F}$ represent the probability density function (pdf) of the channel input X and the set of all the possible pdfs for X, respectively. Instead, $I(X;Y)$ and $I(X;Z)$ stand for the mutual information among X, Y and X, Z, respectively. Note that $[q]^+ = \max(q, 0)$. The mutual information terms $I(\cdot)$ are convex in f_X, this allows the formulation of a lower bound R_S for the secrecy capacity in (8.1), given by [9]

$$C_S \geq \left[\max_{f_X \in \mathscr{F}} [I(X;Y)] - \max_{f_X \in \mathscr{F}} [I(X;Z)] \right]^+ = R_S. \tag{8.2}$$

Since it is known how to maximize the mutual information terms, the lower bound in (8.2) is typically used for the calculation of the achievable secrecy rate.

As discussed in the following, the PLS turns out to be an optimization problem aiming at maximizing the information rate among the intended users, while keeping the eavesdropper completely ignorant about the message and unable to distill any information. As mentioned in Sect. 8.1, the PLS exploits all the available channel features in order to grant and enhance the secrecy of the system. In this regard, it is essential to investigate and study the main PLC channel features.

8.2.2 Channel Properties

In order to assess the effect of the PLC channel properties on the performance, the statistical behavior of the channel is herein discussed. As mentioned in Sect. 8.1.1, the PLC networks, due to their underlying structure and to the physical medium, exhibit different phenomena with respect to the wireless scenario. In the following, the main features are individually analyzed relying on channel measurements carried out in three home sites [21]. The 2–86 MHz frequency range is considered.

8.2.2.1 Statistics

One of the most important properties to assess is the channel gain ($|h|^2$) statistics. Toward this end, the statistical analysis of the measurements is made relying on the likelihood function, defined as [14]

$$\Lambda(\vartheta) = \prod_{X \in \mathscr{X}} p(X|\vartheta), \tag{8.3}$$

where $X \in \mathscr{X}$ represents the set of measured samples, while $p(\cdot)$ and ϑ are the probability density function (pdf) and the parameters, obtained by the estimation, of the fitting distribution. The higher the value provided by the likelihood function, the better the tested distribution fits the measured data.

The test is performed on the measured channel gains for all the main and well known distributions, such as: exponential, gamma, log-normal, normal, Rayleigh, Weibull and log-logistic. For each distribution, the parameters that provide the best fit are found. The value obtained by each pdf is depicted in Fig. 8.3, which shows the logarithmic version of (8.3) as a function of frequency.

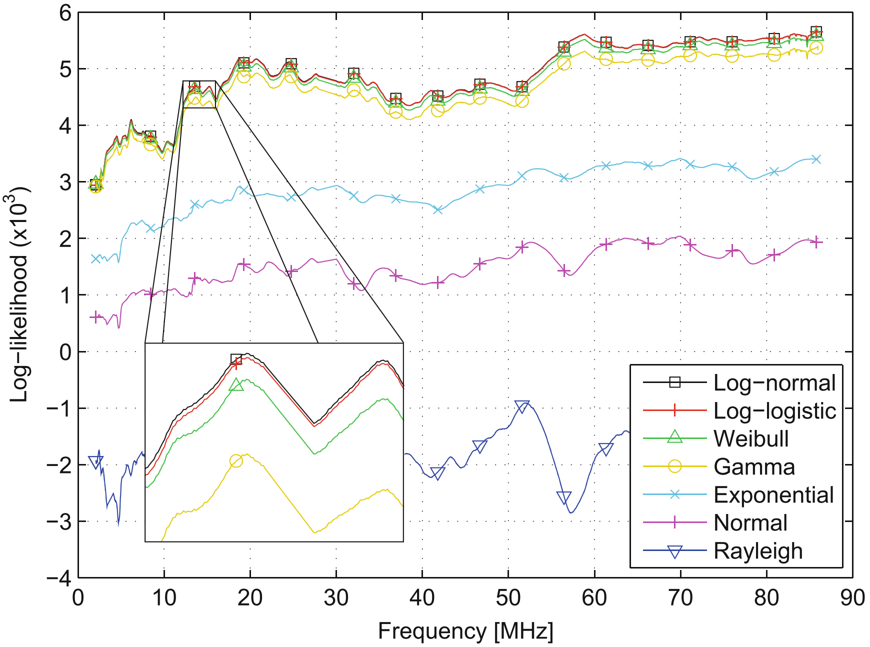


Fig. 8.3 Best log-likelihood value of the measured channel gains for each tested distribution $\mathscr{X}$

It is noted that the highest score is obtained by the log-normal distribution, along the entire frequency range. This means that, in this case, the measured PLC channel gains are log-normally distributed with good approximation [21]. However, also other statistical distributions, such as log-logistic, Weibull and gamma, obtain similar scores. This is due to the pdf shape of all these distributions, which is very similar, with the main difference limited to the tails. Since the network structure, the loads, and the reflections and propagation effects can be different in different scenarios, log-normality does not strictly apply in all contexts. However, it is noticeable that the PLC channels do not exhibit Rayleigh fading, contrariwise to what happens in the wireless case [20].

8.2.2.2 Frequency Correlation

Since broadband PLC is considered, multi-carrier modulation (OFDM) is adopted at the physical layer. This is the modulation scheme used by the HPAV and HPAV2 standards. In OFDM the broadband channel is partitioned in a number of parallel sub-channels whose responses can be correlated. The degree of this correlation is evaluated in terms of normalized covariance matrix between the sub-channel responses, defined as

$$R_{hh}(i,j) = \frac{C_{hh}(i,j)}{\sqrt{C_{hh}(i,i)C_{hh}(j,j)}}. \tag{8.4}$$

The normalized covariance matrix $\mathbf{R_{hh}}$ contains the pairwise covariance coefficient between each pair of sub-channels, identified by the indices i and j. $\mathbf{C_{hh}}$ is the covariance matrix whose elements are defined as

$$C_{hh}(i,j) = E[(h(i)-\mu_i)(h(j)-\mu_j)], \tag{8.5}$$

where the operator $E[\cdot]$ denotes the expectation, $h(i)$, $h(j)$ the i-th and j-th sub-channel gains and μ_i, μ_j their mean ($\mu = E[h]$), respectively. The expectation is performed on the channel measurements.

The normalized covariance is evaluated on the logarithmic, or dB, version of the channels gains, which is normally distributed. Thus, it becomes easier to generate and simulate correlated log-normal random channels, starting from independent normally distributed realizations. Figure 8.4 depicts the normalized covariance matrix between the measured sub-channels in dB scale. It can be noted as certain sub-channels are more related to some others, where the colors become darker, as happens for

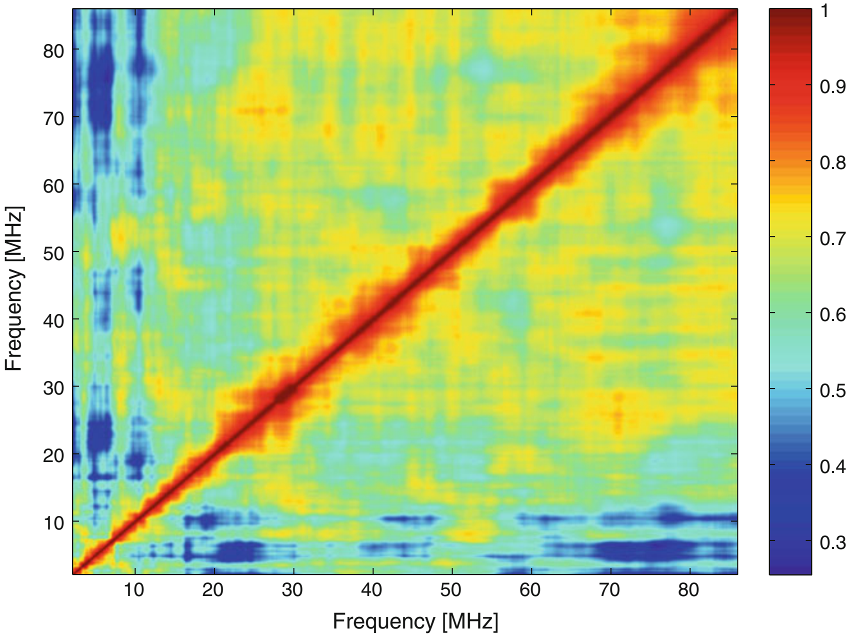


Fig. 8.4 Normalized covariance matrix for the measured channel gains in dB scale

the sub-channels in the upper right corner, which identifies high frequencies. This phenomenon is due to the crosstalk among the wires and to the coupling effects, which become prominent at higher frequencies.

8.2.2.3 Spatial Correlation

The spatial correlation represents the correlation coefficient, or degree of correlation, among the main channel and the wiretapper channel. With reference to Fig. 8.2, the main channel, denoted by h_M, refers to the communication link among Alice and Bob. Thus, it is given by the product of the two channels in cascade, as $h_M = h_A h_B$. The wiretap channel, denoted by h_W, instead, refers to the communication link between Alice and Eve, given by $h_W = h_A h_E$.

Since the transmitting and receiving plugs are known, the measurements are carefully divided among the main and the wiretapper channel so that the corresponding channels share the same transmitting plug. Therefore, the communication scheme resembles that depicted in Fig. 8.2.

The correlation coefficient ρ among the main and the wiretapper channel, in dB scale, is depicted in Fig. 8.5 as a function of frequency. As can be seen, the value is quite high over the entire frequency range, with some peaks and minimums confined

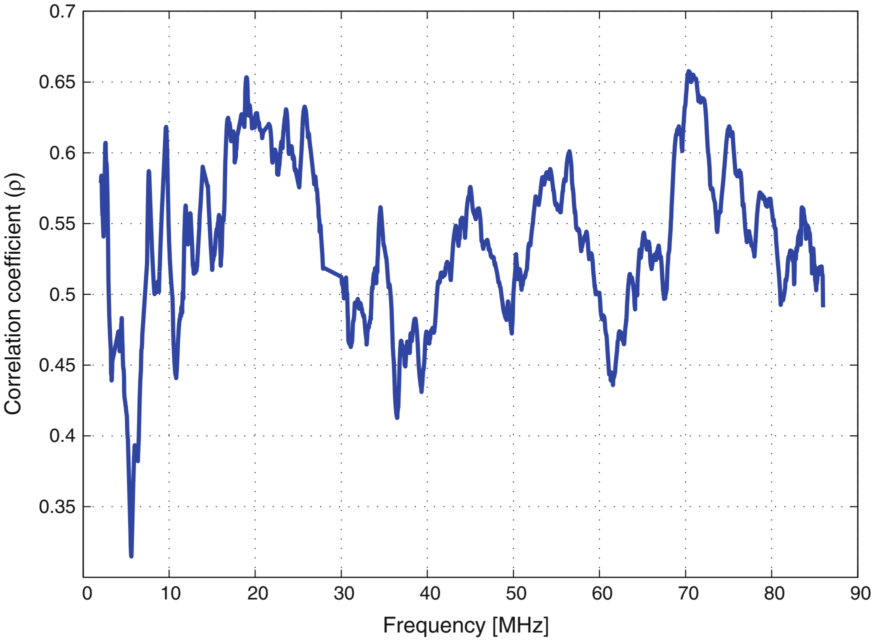


Fig. 8.5 Spatial correlation coefficient between the main and the wiretapper channels in dB scale

at certain carriers (frequencies). The spatial correlation herein shown is mainly due to the keyhole effect caused by the underlying network structure.

8.2.3 Noise Properties

As mentioned in Sect. 8.1.1, not only the channel properties affect the PLC performance. Also the background noise must be taken into account. Contrariwise the wireless case, affected by white Gaussian noise, PLC networks are subject to colored Gaussian background noise. Depending on the PLC context, different noise floors and profiles have been documented [22]. A typical noise power spectral density (PSD) profile is depicted in Fig. 8.6.

The displayed PSDs refers to the noise measured at the star-style receiving modes for the MIMO scheme described in Sect. 8.4.1. As can be noted, the common mode experiences a higher PSD with respect to the other three modes. The effects on the channel performance of these colored noise PSD profiles, together with the spatial correlation between the modes, are discussed in Sect. 8.4. In the following, the effects of the PLC channel properties on the achievable secrecy rate are evaluated for the simpler SISO scheme under AWGN.

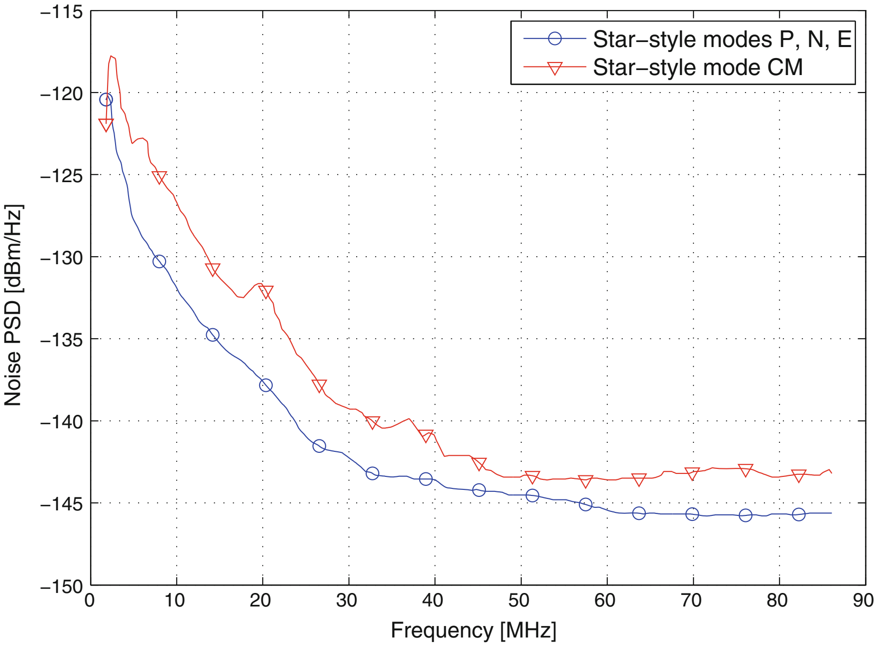


Fig. 8.6 Typical background noise at the star-style receiving modes in a MIMO PLC network

8.3 SISO Scheme Under AWGN

As described in Sect. 8.2.2, PLC networks are subject to a variety of physical phenomena. In order to asses how these phenomena affect the PLS performance, different types of random channels are generated through a numerical model. In particular, the impact of the channel statistics, the frequency and spatial correlation, as well as the keyhole effect, is evaluated generating random channels responses with the appropriate statistics. Furthermore, this approach allows the PLC and the wireless scenario comparison, relying on channel responses with different distributions. To facilitate the comprehension, the SISO channel is considered first. Moreover, to fairly compare wireless and PLC scenarios, the same background AWGN noise is assumed.

8.3.1 Optimization Problem Formulation

As discussed in Sect. 8.1, the evaluation of the secrecy capacity for the model depicted in Fig. 8.2 involves solving an optimization problem. Assuming OFDM transmission with N carriers or sub-channels, the received signals by Bob and by Eve, at the c-th carrier, can be written as

$$y_c = h_{M,c} x_c + n_{B,c}, \tag{8.6}$$

$$z_c = h_{W,c} x_c + n_{E,c}, \tag{8.7}$$

respectively, where, the transmitted signal on carrier c is x_c. Moreover, $h_{M,c}$ and $h_{W,c}$ are the main and the wiretapper channels, while $n_{B,c}$ and $n_{E,c}$ represent the effect of the additive Gaussian noise, with zero mean and variance σ_n^2. The transmitted signal and the noise are assumed to be statistically independent from each other and for each sub-channel c. Moreover, as usually happens, the power at the transmitter is limited by a total power constraint $\sum_{c=1}^{N} |x_c|^2 \leq P_T$, where P_T is the total available power. Finally, perfect channel state information (CSI) is assumed at the transmitter side. Thus, Bob and Eve know their own channel, while Alice has access to both channel gains to Bob and Eve. This case resembles the situation in which Eve is not an adversary, but simply an unintended user of the same network.

The secrecy rate of the system model discussed in Sect. 8.2 can be computed according to (8.2) [13], as

$$R_S(\mathbf{P_x}) = \sum_{c=1}^{N} \left[\log_2 \left(1 + \frac{\alpha_c P_{x,c}}{\sigma_n^2} \right) - \log_2 \left(1 + \frac{\beta_c P_{x,c}}{\sigma_n^2} \right) \right]^+ , \tag{8.8}$$

where $P_{x,c}$ is the transmitting power on the c-th sub-channel, whereas $\alpha_c = |h_{M,c}|^2$ and $\beta_c = |h_{W,c}|^2$ are the channel gains of the main and the wiretapper channels, respectively. The power allocated on each sub-channel is organized in a vector $\mathbf{P_x} =$

$[P_{x,1}, \ldots, P_{x,N}]$, which corresponds to the transmitter power allocation strategy for a given channel realization. Note that the secrecy rate in (8.8) is upper bounded by $\sum_{c=1}^{N} \left[\log_2(\alpha_c/\beta_c)\right]^+$ for arbitrarily large power $\mathbf{P_x}$ and can turn out to be small if the channel does not provide enough diversity.

The secrecy rate optimization problem for the multi-carrier system aims at maximizing the quantity in (8.8), under a total power constraint, and it is formulated as

$$\max_{\mathbf{P_x}} \left[R_S(\mathbf{P_x})\right] \text{ subject to } \sum_{c=1}^{N} P_{x,c} \leq P_T \text{ and } P_{x,c} \geq 0. \tag{8.9}$$

To perform a fair analysis, the total power P_T equals the sum of the HPAV PSD constraint over the used sub-channels. Although, as seen, this is a non-convex optimization problem, it has been shown in [8] that the optimal power allocation strategy is to not allocate power on the sub-channels in which Eve has a higher gain than Bob, i.e. when $\alpha_c \leq \beta_c$. Consequently, the resulting problem becomes convex and can be easily solved through the Karush-Kuhn-Tucker (KKT) conditions [2]. For a more complete and general treatment the reader is referred to [9, 17].

8.3.2 Effects of Channel Characteristics on Performance

The typical PLC channel properties, discussed in Sect. 8.2.2, are herein evaluated in terms of achievable secrecy rates. Hence, the first step is to compute the statistical parameters and the degree of frequency and spatial correlation, starting from real channel measurements. The evaluation is performed relying on 1300 in-home channel measurements in the 2–28 MHz frequency range, carried out in different house sites, as specified in [21]. The specifications comply with the HPAV standard [7].

For the secrecy rate computation, a signal-to-noise ratio (SNR) of 80 dB has been assumed, without taking into account the channel attenuation. This SNR value is typical in PLC networks since, usually, the PSD at the transmitter is constrained at −50 dBm/Hz, while the noise PSD floor equals −130 dBm/Hz. The secrecy rate achieved over the channel measurements is compared to that of the numerically simulated channel realizations, generated taking into account different channel effects as follows. For further details the reader is referred to [17].

1. *Independent channels*: the main and the wiretapper channels are independently generated with a log-normal distribution.
2. *Keyhole effect*: three independent log-normal channel realizations are generated for the Alice's, Bob's and Eve's channels (h_A, h_B and h_E, respectively), see Fig. 8.2. The parameters are imposed so that the mean and the variance of the main and wiretapper channels turn out to be equivalent to those of the channel measurements. This is made possible exploiting the properties of the product of log-normal variables.

3. *Spatial correlation*: in this case, the main and wiretapper channels are generated, with a log-normal distribution, according to the measured correlation coefficient discussed in Sect. 8.2.2.3. The frequency correlation is not considered.
4. *Frequency correlation*: the log-normally generated channels exhibit the same frequency correlation of the measured channels, analyzed in Sect. 8.2.2.2, but are spatially uncorrelated.
5. *Keyhole effect and frequency correlation*: the same procedure in 2 is applied to frequency correlated channels. Thus, the frequency correlation and keyhole effect are jointly considered.
6. *Spatial and frequency correlation*: the generated channel realizations are affected by both frequency correlation and spatial correlation, between the main and the wiretapper channels, as usually happens in real PLC networks.

The secrecy rate, for all the above listed channel realizations, has been computed solving (8.9), as in [17]. The secrecy rate complementary cumulative distribution function (CCDF) is depicted in Fig. 8.7. It can be seen as the CCDF for the measured channels completely differs from that of the independent channels in both trend and average secrecy rate, summarized in Table 8.1. Also when considering the spatial correlation or the keyhole effect the trend does not change, although there is an average secrecy rate reduction. When the frequency correlation is introduced, the

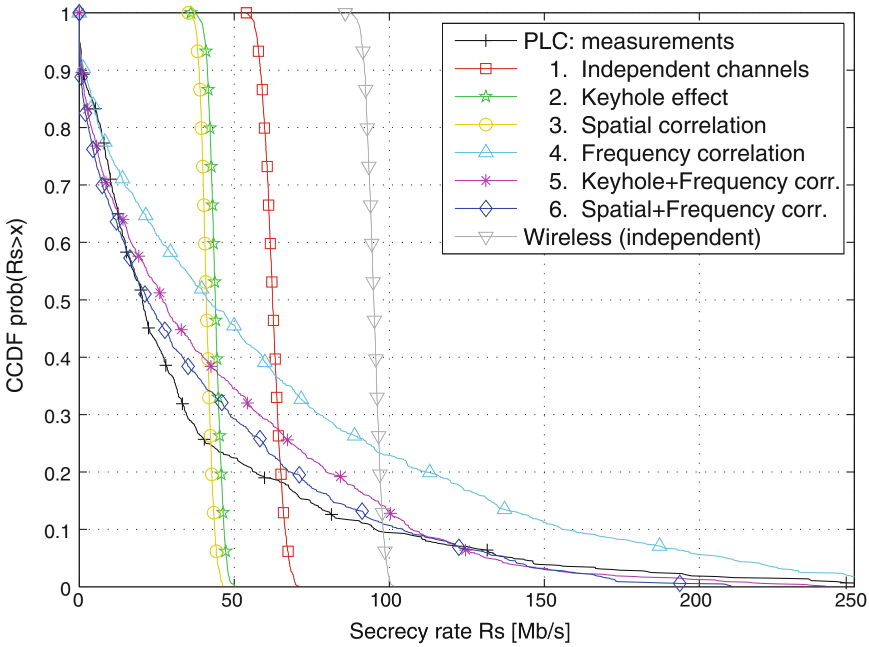


Fig. 8.7 Secrecy rate CCDF comparison among measurements and simulated realizations with different phenomena. The secrecy rate for wireless independent channels is also depicted

Table 8.1 Average secrecy rate for different simulated PLC channel phenomena

Scenario	Channel type	Average secrecy rate (Mb/s)
Wireless	Independent	95
PLC	Independent	62.5
PLC	Keyhole effect	44
PLC	Spatial correlation	41.1
PLC	Frequency correlation	62.9
PLC	Keyhole + frequency correlation	43.7
PLC	Spatial + frequency correlation	38.9
PLC	Measurements	37.4

CCDF trend improves. Moreover, it closely approaches the measured one when also the keyhole effect or the spatial correlation are taken into account. The agreement can also be noted looking at the average secrecy rates summarized in Table 8.1. This analysis demonstrates that the channel statistics, together with the frequency and spatial correlation, constrain and limit the PLC channel performance. As a final remark, the results in Fig. 8.7 validate the implemented numerical model for the channel generation.

8.3.2.1 Wireless Versus PLC

It is interesting to compare the secrecy rate attainable in wireless channels characterized by statistically independent Rayleigh fading and in PLC channels that exhibit correlated log-normal fading. As above specified, in order to perform a fair comparison, an equal SNR of 80 dB (without considering the channel attenuation) is assumed for both scenarios. The secrecy rate CCDF is reported in Fig. 8.7 where it is shown that the wireless case outperforms the PLC one. The difference is noticeable also in terms of average secrecy rate, displayed in Table 8.1.

8.4 MIMO Scheme Under Colored and Correlated Noise

The limits on the secrecy rate, due to the PLC channel characteristics, can be mitigated exploiting the spatial domain end extending the used bandwidth. The performance improvements provided by the MIMO transmission scheme with an additional receiving mode, namely the common mode (CM), the bandwidth extension up to 86 MHz and a novel alternating optimization (AO) approach are herein assessed. It has already been proved in [25] that MIMO transmission can increase PLS performances on PLC. However, the work considers numerically generated channels with two transmitting and receiving modes in the 2–28 MHz frequency band, under AWGN. In this section,

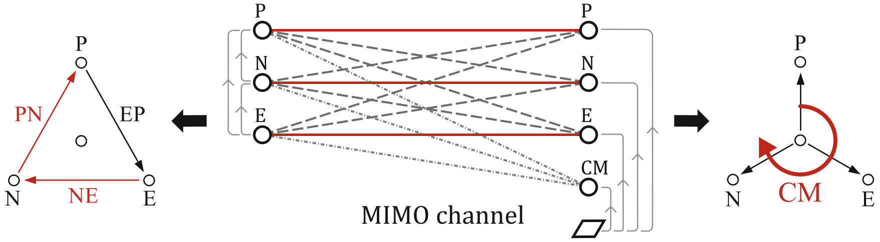


Fig. 8.8 MIMO Δ-style transmitting and star-style receiving modes according to STF-410

the analysis is further extended relying on real channel and noise PSD measurements. As specified by the HPAV2 [24], the 2–86 MHz bandwidth is considered, and the maximum number of possible transmitting and receiving modes are exploited, as described in the following. These assumptions provide actual performance results that can be viewed as a target for future devices development.

8.4.1 MIMO Structure

In today's houses, power supply networks usually consist of three different wires, namely the phase (P), the neutral (N) and the protective earth (E). Hence, due to Kirchhoff's laws, only two Δ-style modes can be exploited at the same time. Where Δ mode means to inject the differential signals between pair of wires, see Fig. 8.8 for details. Instead, at the receiver side, the signals can be observed between one conductor and a reference plane, referred to star-style mode. Beyond the three available star-style modes, one additional mode, given by the coupling between the wires and the physical earth, can be exploited, namely the common mode (CM) [5]. The CM is given by the current that flows in the three conductors, which has the same intensity and direction. Thus, a 2×4 MIMO transmission scheme can be implemented between the transmitter and the receiver side.

8.4.2 Alternating Optimization Algorithm

The secrecy rate maximization belongs to the family of non-convex optimization problems, which are non-trivial and not easily solvable. This is because the secrecy capacity is obtained by the maximization of the difference of two convex terms, as shown in (8.1). The optimization becomes even more difficult when considering MIMO wiretap channels, with one or multiple eavesdroppers. Anyway, to provide a solution, an alternating optimization (AO) approach has been proposed in [12]. The secrecy capacity optimization problem has been reformulated with an equivalent expression which can be brought back to two convex optimization problems, alternatively solved, as briefly described in the following.

For each used sub-channel, the secrecy rate maximization in (8.9) can be reformulated for the MIMO transmission scheme as follows

$$C_S = \max_{\mathbf{X}} \left[\log_2 |\mathbf{I} + \mathbf{H_M}^H \mathbf{X}\mathbf{H_M}| - \log_2 |\mathbf{I} + \mathbf{H_W}^H \mathbf{X}\mathbf{H_W}|\right], \qquad (8.10)$$
$$\text{subject to } \mathrm{Tr}(\mathbf{X}) \leq P_c,\ \mathbf{X} \succeq 0,$$

where $\mathbf{X}$ is the covariance matrix of the transmitted signal x, while $\mathbf{H_M}$ and $\mathbf{H_W}$ represent the main and wiretapper MIMO channel matrices, respectively. Furthermore, P_c is the PSD constraint on the c-carrier and $\mathbf{X} \succeq 0$ means that $\mathbf{X}$ must be positive semidefinite. The identity matrix is represented as $\mathbf{I}$. The optimization problem in (8.10) is properly reformulated exploiting the following lemma [10].

Lemma 8.1 *Let* $\mathbf{E} \in \mathbb{C}$ *be any* $N \times N$ *positive definite matrix* ($\mathbf{E} \succ 0$)*. Consider the function* $f(\mathbf{S}) = -\mathrm{Tr}(\mathbf{S}\mathbf{E}) + \log_2 |\mathbf{S}| + \mathbf{N}$*, then*

$$\log_2 |\mathbf{E}^{-1}| = \max_{\mathbf{S} \succeq 0} f(\mathbf{S}), \qquad (8.11)$$

and the optimal solution to the right-hand side of (8.11) is $\mathbf{S}^* = \mathbf{E}^{-1}$.

Hence, applying Lemma 8.1 via setting $\mathbf{E} = \mathbf{I} + \mathbf{H_W}^H \mathbf{X}\mathbf{H_W}$, the problem in (8.10) can be reformulated as

$$\max_{\mathbf{X},\mathbf{S}} \left[\log_2 |\mathbf{I} + \mathbf{H_M}^H \mathbf{X}\mathbf{H_M}| - \mathrm{Tr}\left(\mathbf{S}(\mathbf{I} + \mathbf{H_W}^H \mathbf{X}\mathbf{H_W})\right) + \log_2 |\mathbf{S}|\right], \qquad (8.12)$$
$$\text{subject to } \mathrm{Tr}(\mathbf{X}) \leq P_c,\ \mathbf{X} \succeq 0,\ \mathbf{S} \succeq 0,$$

where $\mathbf{S}$ denotes a Hermitian positive semidefinite matrix. For simplicity the constant $\mathbf{N}$ has been dropped. The problem in (8.12) is still non-convex with respect to (w.r.t.) both $\mathbf{X}$ and $\mathbf{S}$. However, it can be verified that the problem is convex w.r.t. either $\mathbf{X}$ or $\mathbf{S}$, fixing the other decision variable. This property motivated the use of an AO approach. Defining $\mathbf{X}^n$, $\mathbf{S}^n$ the solutions for the n-th iteration, the following two optimization problems are alternatively solved

$$\mathbf{S}^n = \arg\max_{\mathbf{S} \succeq \mathbf{0}} \left[\log_2 |\mathbf{S}| - \mathrm{Tr}\left(\mathbf{S}(\mathbf{I} + \mathbf{H_W}^H \mathbf{X}^{n-1}\mathbf{H_W})\right)\right], \qquad (8.13)$$
$$\mathbf{W}^n = \arg\max_{\mathbf{W}} \left[\log_2 |\mathbf{I} + \mathbf{H_M}^H \mathbf{X}\mathbf{H_M}| - \mathrm{Tr}(\mathbf{H_W}^H \mathbf{S}^n \mathbf{H_W}\mathbf{X})\right], \qquad (8.14)$$
$$\text{subject to } \mathrm{Tr}(\mathbf{X}) \leq P_c,\ \mathbf{X} \succeq 0.$$

As mentioned, both the problems (8.13) and (8.14) are convex, and can be alternatively solved, as done by the AO algorithm. The solution is guaranteed to converge at a KKT point. For further details the reader is referred to [12].

The solution reported in [12] assumes AWGN. Herein, it is extended to the more complicated colored and correlated Gaussian noise scenario. A non-uniform power allocation solution is found. The results rely on real channel and noise assumptions.

8.4.3 Results for the MIMO Scenario

The focus is on the MIMO wiretap channel. The transmitter exploits the two Δ-style transmitting modes, while both Bob and Eve use all the four star-style receiving modes, as discussed in Sect. 8.4.1. The performance is evaluated exploiting 353 MIMO channel measurements, carried out through an experimental measurement campaign across Europe and collected by the ETSI special task force 410 (STF-410) [5]. The considered frequency range is 2–86 MHz, and the PSD constraint at the transmitter is −50 dBm/Hz in the 2–30 MHz, while −80 dBm/Hz in the 30–86 MHz, according to the latest HPAV2 standard [24]. Moreover an AWGN and a colored and correlated Gaussian background noise are considered. For the colored noise the exponential profile is taken from the STF-410 noise PSD measurements, while the spatial correlation is implemented between the modes as discussed in [16]. The white noise, instead, has been generated so that it exhibits a total power equivalent to the colored one in the considered bandwidth. The channels are equally divided and assigned to the intended receiver and to eavesdropper, respectively.

Under the above system specifications, the secrecy rate achieved over the 2 × 4 MIMO wiretap channel is evaluated and depicted in Fig. 8.9. As a term of comparison, two different noise models are taken into account, white and independent in Fig. 8.9a, and colored and correlated in Fig. 8.9b. Furthermore, the performance

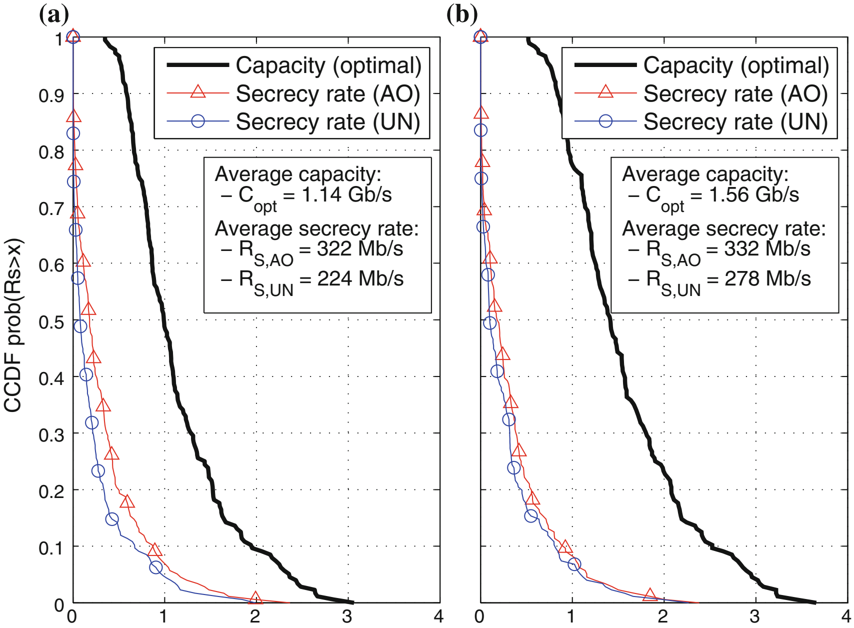


Fig. 8.9 Secrecy rate CCDF for uniform and AO approach power allocation under AWGN (**a**) or colored and correlated (**b**) Gaussian background noise. The channel capacity is also depicted

achieved with the allocation strategy provided by the AO algorithm is compared to that achieved under uniform power allocation (identified by the subscripts AO and UN, respectively).

The comparison is made in terms of secrecy rate CCDF. It can be noted as the AO algorithm translates into a performance improvement for both considered background noise models. This is even more evident looking at the average secrecy rate displayed in the boxes. In practice, an increase of about 30 and 20 % has been noticed for the AWGN and the colored and correlated noise, respectively. When considering colored and correlated noise the performance increases further. This happens since the noise correlation makes easier its cancellation at the receiver side. As a further term of comparison, the channel capacity, achieved without any secrecy constraint, is also computed and depicted in Fig. 8.9. It can be noted as its average value is almost four times higher than the average secrecy rate. This consideration gives the idea on the cost in granting and providing secrecy and confidentiality, in terms of PLS performance.

8.4.3.1 Overall Comparison

A comparison between the SISO and MIMO scenarios is reported in this section. The average secrecy rate, averaged over the channel realizations, of the two transmission schemes for different frequency ranges and background noise models, is summarized in Table 8.2. As a term of comparison, both the SISO database (DB), discussed in Sect. 8.3.2 (identified by 'our DB'), and the ETSI measurements, described in Sect. 8.4.3, are considered. Moreover, various power allocation strategies are assumed.

The results show that when considering the 2–28 MHz frequency range and the keyhole effect, with the same transmitting plug for the main and the wiretapper channels, the average secrecy rate for the SISO scheme is not very high. This, even though the optimization problem is subject to a total power constraint, as detailed in Sect. 8.3.1. However, the SISO channel performance for the house sites (our DB) almost doubles when considering the entire database, irrespectively of the transmitting plug. Indeed, with this choice, the channels used in the simulation are more

Table 8.2 Average secrecy rate comparison for different transmission schemes, frequency ranges, power allocation strategies and background noise

Transmission scheme	Frequency range (MHz)	Background noise	Power allocation	Measurements database	Secrecy rate (Mbit/s)
SISO	2–28	AWGN	Optimal	Our DB (same Tx)	37.4
SISO	2–28	AWGN	Uniform	Our DB (all)	52.8
SISO	2–28	AWGN	Uniform	ETSI (all)	62.9
MIMO	2–28	AWGN	Uniform	ETSI (all)	90.4
MIMO	2–86	Measured	AO	ETSI (all)	332

Two distinct databases are considered

uncorrelated. For comparison purposes, in this case a uniform power constraint, equal to the HPAV PSD limit, is considered. However, this assumption does not significantly affect the achievable performance, as detailed in [17].

Now, the ETSI measurements are considered under the same uniform power constraint and AWGN. Focusing on the reduced 2–28 MHz frequency range and converting the 2×4 Δ-style to star-style MIMO scheme into a Δ-style to Δ-style SISO channel, it can be seen as the average secrecy rate is only slightly higher compared to that achieved on the whole DB of the other measurement campaign. Thus, the two different scenarios can be compared. If the spatial dimension is exploited through MIMO transmission, the performance increases further. Moreover, the bandwidth extension up to 86 MHz, the real background noise assumption, together with the AO algorithm, provide a drastic increase in the achievable secrecy rate.

It can be concluded that the keyhole effect significantly limits the achievable secrecy rate. However, the performance improves through MIMO transmission, bandwidth extension, real noise assumption and non uniform power allocation.

8.5 Final Remarks

It has been shown that PLS over PLC is possible, although constrained and limited by the channel properties and the network characteristics. The results show that PLC channels exhibit log-normal fading, with frequency correlation, due to coupling and cross-talk, and spatial correlation, mainly caused by the underlying network structure. The typical tree-structured PLC network topology gives rise to what is known as keyhole effect, which causes spatial correlation and rank deficiency. As showed, these effects, together with the channel statistics, limit the PLS performance. Furthermore, the comparison among wireless (characterized by Rayleigh fading) and PLC scenarios (characterized by correlated log-normal fading) shows that the former outperforms the latter in terms of secrecy rate, under the same SNR assumption. However, the performance can be improved through the exploitation of the spatial dimension, via the use of MIMO transmission, extending the transmission band 2–28 to 2–86 MHz, and exploiting the power allocation provided by the AO algorithm. The performance improves further when colored and spatially correlated background noise is considered. The results have been obtained with measured channels and noise PSD. Therefore, they have practical value and provide an indication of the achievable level of secrecy if physical layer mechanisms are considered.

References

1. Almers P, Tufvesson F, Molisch AF (2006) Keyhole effect in MIMO wireless channels: measurements and theory. IEEE Trans Wirel Commun 5(12):3596–3604
2. Boyd S, Vandenberghe L (2004) Convex optimization. Cambridge University Press, Cambridge. http://www.stanford.edu/boyd/cvxbook/bvcvxbook.pdf

3. Chizhik D, Foschini GJ, Gans MJ, Valenzuela RA (2002) Keyholes, correlations, and capacities of multielement transmit and receive antennas. IEEE Trans Wirel Commun 1(2):361–368 April
4. Csiszár I, Körner J (1978) Broadcast channels with confidential messages. IEEE Trans Inf Theory 24(3):339–348
5. ETSI TR 101 562–1 V 1.3.1 (2012) "PowerLine Telecommunications (PLT); MIMO PLT; Part 1: Measurement Methods of MIMO PLT," European Telecommunication Standardization Institute, Technical Report
6. Galli S (2011) A novel approach to the statistical modeling of wireline channels. IEEE Trans Commun 59(5):1332–1345 May
7. HomePlug AV System Specifications, HomePlug Powerline Alliance, Version 1.0.09 (2007)
8. Jorswieck EA, Wolf A (2008) Resource allocation for the wire-tap multi-carrier broadcast channel. In: Proceedings of International Conference on Telecommunication (ICT), 2008, pp 1–6
9. Jorswieck EA, Wolf A, Gerbracht S (2010) Secrecy on the physical layer in wireless networks. Trends in telecommunications technologies. InTech, pp 413–435
10. Jose J, Prasad N, Khojastepour M, Rangarajan S (2011) On robust weighted-sum rate maximization in MIMO interference networks. In: Proceedings of IEEE international conference on communication (ICC), 2011, pp 1–6
11. Lampe L, Vinck AJH (2012) Cooperative multihop power line communications. In: Proceedings of the 16th IEEE International Symposium on Power Line Communication and Its Application (ISPLC), Vancouver, 27–30 March 2012, pp 1–6
12. Li Q, Hong M, Wai H-T, Liu Y-F, Ma W-K, Luo Z-Q (2013) Transmit solutions for MIMO wiretap channels using alternating optimization. IEEE J Sel Areas Commun 31(9): 1714–1727
13. Li Z, Yates R, Trappe W (2010) Secrecy capacity of independent parallel channels. In: Liu R, Trappe W (eds) Securing wireless communications at the physical layer. Springer, New York, pp 1–18
14. Myung IJ (2003) Tutorial on maximum likelihood estimation. J Math Psychol 47(1): 90–100 Feb
15. Pittolo A, Tonello AM (2013) Physical layer security in PLC networks: achievable secrecy rate and channel effects. In: Proceedings of the 17th IEEE international symposium on power line communication and its application (ISPLC), Johannesburg, South Africa, 24–27 March 2013, pp 273–278
16. Pittolo A, Tonello AM, Versolatto F (2014) Performance of MIMO PLC in measured channels affected by correlated noise. In: Proceedings of the 18th IEEE international symposium on power line communication and its application (ISPLC), March 2014, pp 261–265
17. Pittolo A, Tonello AM (2014) Physical layer security in power line communication networks: an emerging scenario, other than wireless. IET Communication 8(8), 1239–1247. 22 May 2014
18. Shannon CE (1949) Communication theory of secrecy systems. Bell Syst Tech J 28(4): 656–715 oct
19. Shiu Y-S, Chang SY, Wu H-C, Huang SC-H, Chen H-H (2011) Physical layer security in wireless networks: a tutorial. IEEE Wirel Commun 18(2):66–74
20. Stüber G (2001) Principles of mobile communication. Kluwer Academic, Boston. http://books.google.it/books?id=65fF83bja0C
21. Tonello AM, Versolatto F, Pittolo A (2014) In-home power line communication channel: statistical characterization. IEEE Trans Commun 62(6):2096–2106 Jun
22. Tonello AM, Pittolo A, Girotto M (2014) Power line communications: understanding the channel for physical layer evolution based on filter bank modulation. IEICE Trans Commun **E97-B**(8): 1494–1503, 1 August 2014
23. Wyner AD (1975) The wire-tap channel. Bell Syst Tech J 54(8):1355–1387
24. Yonge L, Abad J, Afkhamie K, Guerrieri L, Katar S, Lioe H, Pagani P, Riva R, Schneider D, Schwager A (2013) An overview of the HomePlug AV2 Technology. J Electron Comput Eng
25. Zhuang Y, Lampe L (2014) Physical layer security in MIMO power line communication networks. In: Proceedings of 18th IEEE international symposium on power line communication and its application (ISPLC), Glasgow, Scotland, 30 March–2 Apr 2014, pp 272–277

Chapter 9
Security Aspects of Compressed Sensing

Tiziano Bianchi and Enrico Magli

Abstract In this chapter, we will consider the security achievable by the compressed sensing (CS) framework under different constructions of the sensing matrix. CS can provide a form of data confidentiality when the signals are sensed by a random matrix composed of i.i.d. Gaussian variables. However, alternative constructions, based either on different distribution or on circulant matrices, which have similar CS recovery performance as Gaussian random matrices and admit faster implementations, are more suitable for practical CS systems. Compared to Gaussian matrices, which leak only the energy of the sensed signal, we show that generic matrices leak also some information about the structure of the sensed signal. In order to characterize this information leakage, we propose an operational definition of security linked to the difficulty of distinguishing equal energy signals and we propose practical attacks to test this definition. The results provide interesting insights on the security of generic sensing matrices, showing that a properly randomized partial circulant matrix can provide a weak encryption layer irrespective of the signal sparsity and the sensing domain.

9.1 Introduction

Compressed sensing (CS) has recently been proposed as an efficient framework for acquiring sparse signals represented by few nonzero coefficients in a suitable basis [8]. CS relies on the fact that linear measurements of a sparse signal enable signal recovery with high probability when the measurements satisfy certain incoherence properties with respect to the signal basis. Interestingly, measurements acquired using linear projections generated according to a random sensing matrix have such properties [3]. The low complexity acquisition and reduced energy consumption

T. Bianchi (✉) · E. Magli
Politecnico di Torino, Corso Duca Degli Abruzzi 24, 10129 Torino, Italy
e-mail: tiziano.bianchi@polito.it

E. Magli
e-mail: enrico.magli@polito.it

M. Baldi and S. Tomasin (eds.), *Physical and Data-Link Security Techniques for Future Communication Systems*, Lecture Notes in Electrical Engineering 358, DOI 10.1007/978-3-319-23609-4_9

offered by CS can be beneficial to several applications, as shown by recent works on spectrum sensing [9], wireless sensor networks [11], network anomaly detection [15]. Hence, assessing whether the randomness in the acquisition process implicitly provides some kind of confidentiality is an important open problem.

In the literature, the security of CS has been analyzed following two main paradigms. A first approach is to argue that CS provides computational secrecy if viewed as a cryptosystem, since looking for the correct sensing matrix over the key space is a computationally intractable problem [16, 17]. However, this approach does not provide any formal security proof regarding CS. The second approach is to consider the security of random linear measurements according to an information theoretic framework [19]. As correctly pointed out in [17], CS does not provide information theoretic secrecy, since the mutual information between the measurements and the sensed signal is always greater than zero. However, it is possible to prove that CS measurements asymptotically reveal only the energy of the signal [2] and that normalizing the measurements can provide a perfectly secure channel in the case of Gaussian sensing matrices [1].

The results in the previous works are based on the central limit theorem and the properties of the Gaussian distribution and are valid when the elements of the sensing matrix are i.i.d. random variables. Moreover, they consider a scenario in which the sensing matrix is continually updated, implementing a sort of one time pad. Such requirements are usually too demanding for practical CS systems. Using fully random matrices requires either storing or generating on the fly a great amount of random values. Moreover, the generation of Gaussian distributed values may be difficult in low complexity systems.

The above problems can be solved in practice by resorting to structured matrices [7, 12] and generating the sensing matrix according to simpler distributions, like the Bernoulli one. However, even if such constructions guarantee similar recovery properties as fully random matrices made of Gaussian i.i.d. values, their security properties are still not fully understood. In this chapter, we will analyze the security of practical sensing matrices according to an alternative security definition based on the performance of a detector which tries to distinguish different signals from their measurements. We will also provide useful bounds to characterize the security of CS according to this definition and validate such bounds in simple scenarios through simulations.

9.2 Background

9.2.1 Compressed Sensing

A signal $x \in \mathbb{R}^n$ is called k-sparse if there exists a basis Φ such that $x = \Phi\vartheta$ and ϑ has at most k nonzero entries, i.e., $||\vartheta||_0 \leq k$. According to the compressed sensing framework, a k-sparse signal can be exactly recovered from $m < n$ linear measurements

$$y = Ax \tag{9.1}$$

by solving a non-convex minimization problem [4, 8].

In practice, if the entries of A are i.i.d. variables from a sub-Gaussian distribution, then exact recovery of k-sparse signals can be achieved with very high probability by solving the convex minimization problem

$$\hat{\vartheta} = \arg\min_{\vartheta} ||\vartheta||_1, \quad \text{subject to } A\Phi\vartheta = y \tag{9.2}$$

as long as $m = O(k \log(n/k))$ [3].

9.2.2 Security Definitions

Let us call the set of possible plaintexts $\mathscr{P}$, the set of cipher texts $\mathscr{C}$ and a key K. A private key cryptosystem is a pair of functions $e_K : \mathscr{P} \to \mathscr{C}, d_K : \mathscr{C} \to \mathscr{P}$ such that, given a plain text $p \in \mathscr{P}$, and a ciphertext $c \in \mathscr{C}$, we have that $d_K(e_K(p)) = p$ and that it is unfeasible, without knowing the key K, to determine p such that $e_K(p) = c$.

A cryptosystem is said to be perfectly secure [19] if the posterior probability of the ciphertext given the plaintext p is independent of p, i.e., if

$$\mathbb{P}(c|p) = \mathbb{P}(c). \tag{9.3}$$

Given a perfectly secure cryptosystem, an attack cannot be more successful than guessing the plaintext at random.

Following the approach in [1], we define a CS-based cryptosystem where the signal x is the plain text p, the sensing matrix A is the secret key K and the measurement vector y is the cipher text c. The encryption function e_A is the matrix multiplication between the sensing matrix A and the signal x; the decryption is achieved by solving the problem in (9.2). We assume that each sensing matrix is used only once (one-time sensing matrix (OTS) scenario), and that different sensing matrices are statistically independent. Under this scenario, we can assume that the adversary has only knowledge of the measurements y (ciphertext-only attack (COA) scenario), since the knowledge of plaintext/ciphertext pairs (x, y) does not reveal anything about the unknown plaintexts. CS-based cryptosystems cannot achieve in general perfect secrecy [1, 17]. However, weaker security notions may apply, as we will show in the next sections.

9.3 Security of the Measurements

In this section, we summarize the main results regarding the security of CS measurements. In the first subsection, we review the security of fully random sensing matrices, i.e., when the matrix entries are i.i.d. random variables. In the second subsection, we address the security of partial circulant random sensing matrices, which have an important role in the deployment of practical CS systems.

9.3.1 Fully Random Matrices

Let us consider the OTS cryptosystem defined by $y = Ax$. Let us denote with $I(x, y)$ the mutual information between x and y [5], and define $\mathscr{E}_x = ||x||_2^2$. We have the following important result [1]:

Theorem 9.1 *If $[A]_{i,j}$ are i.i.d. zero-mean Gaussian variables, then the OTS cryptosystem satisfies $I(x; y) = I(\mathscr{E}_x; y)$.*

The above result says that an OTS cryptosystem using an i.i.d. Gaussian sensing matrix does not reveal anything more about x than its energy and what can be inferred by knowing its energy. It is worth noting that this is true irrespective of the sparsity degree of x, that is, x does not necessarily have to be sparse. In the following, we will denote such a cryptosystem as Gaussian-OTS (G-OTS) cryptosystem.

The special properties of Gaussian sensing matrices can be exploited to obtain a perfectly "secured" version of the G-OTS cryptosystem. Let us modify the G-OTS cryptosystem so that only normalized measurements are transmitted, i.e., using as ciphertext the vector

$$u_y = \begin{cases} y/\sqrt{\mathscr{E}_y} & \mathscr{E}_y > 0 \\ U & \mathscr{E}_y = 0 \end{cases} \tag{9.4}$$

where U is a random vector uniformly distributed on a unit radius m-sphere. We denote it as SG-OTS.

Theorem 9.2 *The SG-OTS cryptosystem is perfectly secure, i.e., $\mathbb{P}(u_y|x) = \mathbb{P}(u_y)$.*

Proof It is easy to verify that for a Gaussian A the vector y is spherically distributed, i.e., u_y is uniformly distributed on the unit radius m-sphere irrespective of x. □

9.3.2 Circulant Matrices

Due to the complexity of performing the product Ax when A is a fully random matrix, some authors have suggested to use partial circulant matrices generated from a row of i.i.d. variables [12, 18, 21]. Such matrices have the following form

$$A = \begin{bmatrix} a_1 & a_2 & a_3 & \dots & a_n \\ a_n & a_1 & a_2 & \dots & a_{n-1} \\ \vdots & & & & \vdots \\ a_{n-m+2} & a_{n-m+3} & a_{n-m+4} & \dots & a_{n-m+1} \end{bmatrix} \tag{9.5}$$

where the first row $a^T = [a_1, a_2, \dots, a_n]$ is a vector of i.i.d. variables from a Gaussian or sub-Gaussian (e.g., Bernoulli) distribution. Partial circulant matrices have similar recovery performance as fully random matrices [21]. Moreover, they can be diagonalized using a discrete Fourier transform (DFT) as

$$A = PW^H \Lambda W \tag{9.6}$$

where W is the unitary DFT matrix, Λ is a diagonal matrix whose nonzero elements are the DFT of the sequence $[a_1, a_n, a_{n-1}, \dots, a_2]$, i.e., the first column of the $n \times n$ fully circulant matrix generated from a^T, and P is a $m \times n$ matrix that selects the first m entries of a vector of n elements. Thanks to the above decomposition, the product Ax can be efficiently implemented using a fast Fourier transform (FFT). Moreover, the cost of transmitting or generating the sensing matrix is also sensibly reduced, since only n random values are required.

In order to generalize the concept of partial circulant matrix, in the following we will consider sensing matrices that can be expressed as

$$A = PW^H \Lambda WR. \tag{9.7}$$

In the above notation, we assume that P select a generic subset of m indexes [21], whereas R is a generic scrambling matrix. The above construction is somewhat similar to the structurally random matrices proposed in [7].

Let us consider the OTS cryptosystem defined by $y = Ax$, where A can be expressed as in (9.7) and the matrices P and R are public. We will denote such a cryptosystem as OTS-circulant (OTS-C). Let us define C_v as the circular autocorrelation matrix of vector v, that is, $[C_v]_{ij} = \sum_{r=1}^{n} v_r v_{r+i-j \mod n}$, for $i, j = 1, \dots, n$, where $[A]_{ij}$ denotes the element in the ith row and jth column of matrix A. It is easy to verify that C_v is a Toeplitz matrix and that its diagonal elements are equal to $\mathcal{E}_v = v^T v$. We have the following result:

Theorem 9.3 *If a_i, $i = 1, \dots, n$, are i.i.d. zero-mean Gaussian variables, then the OTS-C cryptosystem satisfies $\mathbb{P}(y|x) = \mathbb{P}(y|PC_{Rx}P^T)$.*

Proof Let us consider the probability distribution function $\mathbb{P}(y|x)$ for a given x. Since a_i are Gaussian, we have that $\mathbb{P}(y|x)$ is a multivariate Gaussian distribution with mean $\mu_{y|x}$ and covariance matrix $C_{y|x}$. It is immediate to find $\mu_{y|x} = E[y|x] = E[A]x = 0$, whereas we have

$$\begin{aligned} C_{y|x} &= E[Axx^T A^T] = E[PW^H \Lambda (WRx)(WRx)^H \Lambda^H WP^T] \\ &= nPW^H \text{diag}\{WRx\} E[(W^H a)(W^H a)^H] \\ &\quad \times \text{diag}\{WRx\}^H WP^T \\ &= nPW^H \text{diag}\{WRx\} W^H E[aa^T] W \text{diag}\{WRx\}^H WP^T \\ &= n\sigma_A^2 PW^H \text{diag}\{WRx\} \text{diag}\{WRx\}^H WP^T = \sigma_A^2 PC_{Rx} P^T \end{aligned} \tag{9.8}$$

where diag$\{v\}$ denotes a diagonal matrix defined by vector v, we use $\Lambda = \sqrt{n} \cdot \text{diag}\{W^H a\}$ and the fact that diag$\{u\}v = \text{diag}\{v\}u$, and we assume that a_i have variance σ_A^2. It follows that y depends on x only through the autocorrelation $PC_{Rx}P^T$, i.e., $\mathbb{P}(y|x) = \mathbb{P}(y|PC_{Rx}P^T)$. □

The above result says that an OTS-C cryptosystem using i.i.d. Gaussian variables reveals only some elements of the circular autocorrelation matrix of Rx, according to the particular selection matrix P. It is worth noting that this is true irrespective of the sparsity degree of x, that is, x does not necessarily have to be sparse.

In the following, we will consider three variants of the OTS-C cryptosystem:

1. Gaussian-OTS-C (G-OTS-C) cryptosystem, where P is fixed and public and R is the identity matrix, implying $\mathbb{P}(y|x) = \mathbb{P}(y|PC_x P^T)$;
2. Gaussian-OTS-singly randomized circulant (G-OTS-R1), where the selection matrix P is randomly drawn, with uniform distribution, over all the possible choices of m indexes out of n and kept secret whereas R is the identity matrix. In this case, it is easy to derive

$$\mathbb{P}(y|x) = \frac{1}{N_P} \sum_{r=1}^{N_P} \mathcal{N}(0, \sigma_A^2 P_r C_x P_r^T)$$

   where P_r denotes the rth possible selection matrix, $N_P = n!/(n-m)!$, and $\mathcal{N}(\mu, C)$ denotes a multivariate Gaussian distribution with mean μ and covariance matrix C.
3. Gaussian-OTS-doubly randomized circulant (G-OTS-R2), where P is chosen as above and R is a diagonal matrix introducing a random sign flip on the elements of x, i.e., its diagonal elements are i.i.d. Rademacher variables. In this case, we obtain

$$\mathbb{P}(y|x) = \frac{1}{N_P} \frac{1}{N_R} \sum_{r=1}^{N_P} \sum_{s=1}^{N_R} \mathcal{N}(0, \sigma_A^2 P_r C_{R_s x} P_r^T)$$

   where R_s denotes the sth possible sign randomization matrix and $N_R = 2^n$.

9.4 Security Metrics

Measurements taken with a non-Gaussian or a circulant sensing matrix in general are not distributed according to a spherically symmetric distribution. As a result, this kind of sensing matrices provide a weaker security than Gaussian sensing matrices, since their information leakage is not limited to the energy of x [1]. In order to characterize this additional leakage, we introduce a security metric based on the problem of distinguishing whether the measurements y comes from one of two known signals x_1 and x_2. This security definition is inspired to indistinguishability definitions commonly used in cryptography [10]. Let us consider a signal x that belongs to a two-element set $\{x_1, x_2\}$; a detector is a function that given the measurements y outputs one of two possible signals x_1, x_2. Formally, this can be defined as $\mathscr{D} : \mathbb{R}^m \rightarrow \{x_1, x_2\}$. Given a certain detector, we define the probability of detection with respect to signal x_i as $P_{d,i} = \Pr\{\mathscr{D}(y) = x_i | x = x_i\}$ and the respective probability of false alarm as $P_{f,i} = \Pr\{\mathscr{D}(y) = x_i | x \neq x_i\}$. It is immediate to verify $P_{d,2} = 1 - P_{f,1}$ and $P_{f,2} = 1 - P_{d,1}$, so that $P_{d,1} - P_{f,1} = P_{d,2} - P_{f,2} \triangleq P_d - P_f$.

Definition 1 A cryptosystem is ϑ-indistinguishable with respect to two signals x_1 and x_2 if for every possible detector $\mathscr{D}(y)$ we have

$$P_d - P_f \leq \vartheta. \tag{9.9}$$

According to the above definition, lower values of ϑ correspond to higher security, with $\vartheta = 0$ being equivalent to perfect secrecy.

Given an OTS cryptosystem defined by a sensing matrix A with a certain distribution, we can link the ϑ-indistinguishability of the cryptosystem to $\mathbb{P}(y|x_1)$ and $\mathbb{P}(y|x_2)$. Let us define the total variation (TV) distance between the probability distributions $\mathbb{P}_A(a)$ and $\mathbb{P}_B(b)$ as $\delta(\mathbb{P}_A(a), \mathbb{P}_B(b)) = \frac{1}{2} \int |\mathbb{P}_A(t) - \mathbb{P}_B(t)| dt$. Let us also denote in short $\delta(\mathbb{P}(y|x_1), \mathbb{P}(y|x_2)) = \delta(\mathbb{P}_1, \mathbb{P}_2)$. We have the following:

Theorem 9.4 *An OTS cryptosystem is at least $\delta(\mathbb{P}_1, \mathbb{P}_2)$-indistinguishable with respect to two signals x_1 and x_2.*

Proof The sum of error probabilities in a statistical hypothesis test can be lower bounded as [14]

$$\begin{aligned}\Pr\{\mathscr{D}(y) = x_2 | x_1\} + \Pr\{\mathscr{D}(y) = x_1 | x_2\} &= 1 - P_d + P_f \\ &\geq 1 - \delta(\mathbb{P}(y|x_1), \mathbb{P}(y|x_2))\end{aligned} \tag{9.10}$$

from which it is immediate to derive $P_d - P_f \leq \delta(\mathbb{P}_1, \mathbb{P}_2)$. □

In general, it is difficult to find a closed form expression for the TV distance in the case of arbitrary distributions and/or structured matrices. However, a useful upper bound on the TV distance can be evaluated thanks to the Pinsker's inequality, which states $\delta(\mathbb{P}_1, \mathbb{P}_2) \leq \sqrt{D(\mathbb{P}_1||\mathbb{P}_2)/2}$, where $D(\mathbb{P}_1||\mathbb{P}_2)$ denotes the Kullback-Leibler (KL) divergence between the distributions $\mathbb{P}_1$ and $\mathbb{P}_2$.[1]

9.4.1 Bounds for Fully Random Matrices

Under the assumption that the elements of y are i.i.d., it is possible to find an upper bound for $P_d - P_f$ by numerically evaluating the KL divergence between $\mathbb{P}([y]_i|x_1)$ and $\mathbb{P}([y]_i|x_2)$, where $[y]_i$ denotes the ith element of vector y. Namely, we can estimate

$$P_d - P_f \leq \vartheta_{\mathrm{KL}}(x_1, x_2) \triangleq \sqrt{\frac{m}{2} D(\mathbb{P}([y]_i|x_1)||\mathbb{P}([y]_i|x_2))} \tag{9.11}$$

where KL divergences can be computed numerically. In order to compute numerical approximations of the probability density functions $\mathbb{P}([y]_i|x_1)$ and $\mathbb{P}([y]_i|x_2)$, we can consider the characteristic function of the random variable $a = [A]_{ij}$, defined as $\varphi_a(t) = E[e^{jta}]$. It is well known that the pdf of a random variable a can be obtained as $\mathbb{P}(a) = \frac{1}{2\pi}\int_{-\infty}^{\infty} \varphi_a(t)e^{-jta}dt$, i.e., that the characteristic function and the corresponding pdf form a Fourier transform pair. We have that the characteristic function of $[y]_i$ given a generic signal x can be computed as

$$\varphi_{[y]_i|x}(t) = \prod_{j=1}^{n} \varphi_a([x]_j t) \tag{9.12}$$

where $\varphi_a(t)$ is the characteristic function of a generic element of the sensing matrix A. Hence, given x_1 and x_2, we can use (9.12) to evaluate the characteristic functions $\varphi_{[y]_i|x_1}$ and $\varphi_{[y]_i|x_2}$, find the corresponding $\mathbb{P}([y]_i|x_1)$ and $\mathbb{P}([y]_i|x_2)$ through a Fourier transform.

9.4.2 Bounds for Circulant Matrices

In the case of circulant sensing matrices composed by Gaussian random variables, it is possible to exploit the fact that the KL divergence of two multivariate Gaussian distributions has a nice closed form. Given any two different signals x_1 and x_2, we have the following result:

[1] Actually, since KL divergence is not symmetric, a stricter bound is given as $\delta(\mathbb{P}_1, \mathbb{P}_2) \leq \sqrt{\min\left(D(\mathbb{P}_1||\mathbb{P}_2), D(\mathbb{P}_2||\mathbb{P}_2)\right)/2}$. In the following sections, for the sake of conciseness, we will always consider a single KL divergence. However, experimental results are based on the stricter bound.

Theorem 9.5 *A G-OTS-C cryptosystem is at least $\vartheta_C(x_1, x_2)$-indistinguishable w.r.t. x_1, x_2, where*

$$\vartheta_C(x_1, x_2) = \frac{1}{2}\sqrt{\log\frac{|C_2|}{|C_1|} + \mathrm{Tr}(C_2^{-1}C_1) - m} \tag{9.13}$$

and $C_h = PC_{x_h}P^T$, for $h = 1, 2$.

Proof Thanks to Proposition 9.3, we have that $\mathbb{P}(y|x_h) = \mathcal{N}(0, \sigma_A^2 C_h)$. Hence, the Kullback-Leibler (KL) divergence between $\mathbb{P}(y|x_1)$ and $\mathbb{P}(y|x_2)$ can be expressed as [6]

$$D(\mathbb{P}_1||\mathbb{P}_2) = \frac{1}{2}\left[\log\frac{|C_2|}{|C_1|} + \mathrm{Tr}(C_2^{-1}C_1) - m\right]. \tag{9.14}$$

The result then follows from Pinsker's inequality. □

Theorem 9.6 *A G-OTS-R1 cryptosystem is at least $\vartheta_{R1}(x_1, x_2)$-indistinguishable w.r.t. x_1, x_2, where*

$$\vartheta_{R1}(x_1, x_2) = \sqrt{\frac{1}{4N_P^2}\sum_{r1=1}^{N_P}\sum_{r2=1}^{N_P}\left[\log\frac{|C_{2,r2}|}{|C_{1,r1}|} + \mathrm{Tr}(C_{2,r2}^{-1}C_{1,r1})\right] - \frac{m}{4}} \tag{9.15}$$

and $C_{h,r} = P_r C_{x_h} P_r^T$, for $h = 1, 2$. A G-OTS-R2 cryptosystem is at least $\vartheta_{R2}(x_1, x_2)$-indistinguishable w.r.t. x_1, x_2, where

$$\vartheta_{R2}(x_1, x_2) = \sqrt{\frac{1}{4N_P^2N_R^2}\sum_{r1=1}^{N_P}\sum_{r2=1}^{N_P}\sum_{s1=1}^{N_R}\sum_{s2=1}^{N_R}\left[\log\frac{|C_{2,r2,s2}|}{|C_{1,r1,s1}|} + \mathrm{Tr}(C_{2,r2,s2}^{-1}C_{1,r1,s1})\right] - \frac{m}{4}} \tag{9.16}$$

and $C_{h,r,s} = P_r C_{R_s x_h} P_r^T$, for $h = 1, 2$.

Proof For G-OTS-R1 and G-OTS-R2, we have that $\mathbb{P}(y|x_h)$ can be expressed as a mixture of Gaussian distributions. The KL divergence between two mixture distributions $\mathbb{P}_i = \sum_r w_{h,r}\mathbb{P}_{h,r}$, $h = 1, 2$, can be upper bounded using the following convexity bound [13]

$$D(\mathbb{P}_1||\mathbb{P}_2) \le \sum_{r1,r2} w_{1,r1}w_{2,r2}D(\mathbb{P}_{1,r1}||\mathbb{P}_{2,r2}). \tag{9.17}$$

Hence, the result can be easily obtained by considering that $w_{1,r} = w_{2,r} = \frac{1}{N_P}$, for G-OTS-R1, or $w_{1,r} = w_{2,r} = \frac{1}{N_P N_R}$, for G-OTS-R2, and then applying Pinsker's inequality to the upper bound on the KL divergence. □

For relatively large values of n and m, the exact computation of the bounds in (9.15) and (9.16) can become prohibitively expensive. A possible approach is to estimate the bound using Monte Carlo integration. Alternatively, following the suggestion in [13], we can approximate the KL divergence between the two mixture distributions using the KL divergence of two multivariate Gaussian distributions having the same mean and covariance matrix. For the G-OTS-R1 cryptosystem, the covariance matrix of the involved mixture distributions has a very peculiar form, since

$$[C_h]_{ij} = \sum_{r=1}^{N_P} \frac{1}{N_P}[C_{h,r}]_{ij} = \begin{cases} \sigma_A^2 \mathscr{E}_{x_h} & i = j \\ \sigma_A^2 \sum_{s \neq t} x_{h,s} x_{h,t} & i \neq j \end{cases} \tag{9.18}$$

for $h = 1, 2$. The above covariance matrix can be expressed in a compact form as $C_h = \alpha_h I_m + \beta_h \mathbb{1}\mathbb{1}^T$, where we define $\alpha_h = \frac{\sigma_A^2}{n-1}(n\mathscr{E}_{x_h} - (\mathbb{1}^T x_h)^2)$ and $\beta_h = \frac{\sigma_A^2}{n-1}((\mathbb{1}^T x_h)^2 - \mathscr{E}_{x_h})$. According to the above representation, the KL divergence between $\mathbb{P}(y|x_1)$ and $\mathbb{P}(y|x_2)$ can be approximated as

$$\begin{aligned} D(\mathbb{P}_1||\mathbb{P}_2) \approx& \frac{1}{2}\left[\log\frac{\alpha_2^{m-1}(\alpha_2 + m\beta_2)}{\alpha_1^{m-1}(\alpha_1 + m\beta_1)} + \frac{m\alpha_2(\alpha_1 + \beta_1) + m(m-1)\alpha_1\beta_2}{\alpha_2(\alpha_2 + m\beta_2)} - m\right] \\ \triangleq& \tilde{D}(x_1, x_2). \end{aligned} \tag{9.19}$$

Thanks to the above equation, an approximate security metric can be defined as

$$\vartheta'_{R1}(x_1, x_2) = \sqrt{\frac{\tilde{D}(x_1, x_2)}{2}}.$$

However, since (9.19) is not an upper bound on KL divergence, $\vartheta'_{R1}(x_1, x_2)$ does not provide a strict security bound for the G-OTS-R1 cryptosystem.

Unfortunately, the above approach cannot be used to provide a meaningful bound for the G-OTS-R2 cryptosystem, since in this case we have

$$C_h = \sum_{r=1}^{N_P}\sum_{s=1}^{N_R} \frac{1}{N_P N_R} C_{h,r,s} = \mathscr{E}_{x_h} I_m,$$

meaning that for equal-energy signals the approximated KL divergence is zero. Nevertheless, by using the convexity bound approach, an approximate security metric for the G-OTS-R2 cryptosystem can be obtained as

$$\vartheta'_{R2}(x_1, x_2) = \sqrt{\frac{1}{2N_R^2}\sum_{s1=1}^{N_R}\sum_{s2=1}^{N_R} \tilde{D}(R_{s1}x_1, R_{s2}x_2)}.$$

Again, the exact computation of the above metric may become too expensive for large values of n. In those cases, we can resort to Monte Carlo integration.

9.4.3 Bounds for Normalized Measurements

The normalization strategy described in Sect. 9.3 does not provide a perfectly secure channel in the case of arbitrary sensing matrices. However, we can provide an upper bound on the security of normalized measurements by using the above bounds that holds for equal energy signals. Let us define $u_{x_h} = x_h/\sqrt{\mathscr{E}_{x_h}}$ and $u_{y_h} = y_h/\sqrt{\mathscr{E}_{y_h}}$, where $y_h = Ax_h$, $h = 1, 2$. Then we have the following

Theorem 9.7 *The upper bounds given in* (9.13)*,* (9.15)*, and* (9.16) *computed for equal-energy signals* u_{x_1}, u_{x_2} *holds also in the case of normalized measurements of generic signals* x_1, x_2*.*

Proof Let us define $y_i' = Au_{x_i}$. It is easy to verify that $u_{y_i'} = y_i'/\sqrt{\mathscr{E}_{y_i'}} = u_{y_i}$. Then, we have the following inequalities involving the KL divergence

$$\begin{aligned} D(y_1'||y_2') &= D(\mathbb{P}(u_{y_1}, \mathscr{E}_{y_1'})||\mathbb{P}(u_{y_2}, \mathscr{E}_{y_2'})) \\ &= D(u_{y_1}||u_{y_2}) + D(\mathbb{P}(\mathscr{E}_{y_1'}|u_{y_1})||\mathbb{P}(\mathscr{E}_{y_1'}|u_{y_1})) \\ &\geq D(u_{y_1}||u_{y_2}) \end{aligned} \tag{9.20}$$

where we exploited the chain rule for KL divergence [5] and the fact that KL divergence is always nonnegative. Hence, the proof follows from the following chain of inequalities

$$\delta(\mathbb{P}(u_{y_1}), \mathbb{P}(u_{y_2})) \leq \sqrt{\frac{1}{2}D(u_{y_1}||u_{y_2})} \leq \sqrt{\frac{1}{2}D(y_1'||y_2')} \tag{9.21}$$

where it is easy to verify that the right hand side of (9.21) evaluates to the upper bound on the distinguishability of equal energy signals. □

9.5 Attacks to CS Cryptosystems

The bounds introduced in the previous Section hold for any possible attack under the COA scenario. However, it is interesting to evaluate the performance of practical attacks with respect to those bounds. We consider an hypothetical scenario in which an OTS cryptosystem is used to sense two distinct signals x_1 and x_2 having equal energy. Without loss of generality, we can assume that $\mathscr{E}_{x_1} = \mathscr{E}_{x_2} = 1$. The aim of the attacker is to guess whether the measurements conceal the signal x_1 or the signal x_2. This is a classical detection problem, where the aim is to distinguish whether the measurements y come from the probability distribution $\mathbb{P}(y|x_1)$ or from the probability distribution $\mathbb{P}(y|x_2)$.

Let us consider a detector $\mathscr{D}$. The Neyman-Pearson (NP) lemma states that for $P_f = \alpha$, the probability of detection is maximized by letting $\mathscr{D}(y) = x_1$ whenever

$$\Lambda(y) = \frac{\mathbb{P}(y|x_1)}{\mathbb{P}(y|x_2)} \geq \tau \tag{9.22}$$

where τ satisfies $\Pr\{\Lambda(y) \geq \tau | x_2\} = P_f$.

When the sensing matrix is made up of i.i.d. elements, it turns out that the elements of y are i.i.d. as well. This permits to rewrite the optimal NP test as

$$\Lambda'(y) = \sum_{i=1}^{m} (\log(\mathbb{P}([y]_i|x_1)) - \log(\mathbb{P}([y]_i|x_2))) \geq \tau'. \tag{9.23}$$

Moreover, since each element of y is given by the sum of independent variables, the distributions $\mathbb{P}([y]_i|x_1)$ and $\mathbb{P}([y]_i|x_2)$ can be numerically computed as detailed in Sect. 9.4.

In the case of the G-OTS-C cryptosystem, the optimal NP test can be easily obtained as

$$\Lambda_C(y) = y^T (C_2^{-1} - C_1^{-1}) y \geq \tau'. \tag{9.24}$$

In the case of the G-OTS-R1 cryptosystem, the optimal NP test would be obtained as the ratio of two mixture distributions. Since the computation of the NP test is not practical in this case, we consider a simpler test obtained by approximating the two mixture distributions using two multivariate Gaussian distributions with the same mean and covariance matrix. By using the expressions of the covariance matrices found in Sect. 9.3, the test can be expressed as

$$\Lambda_R(y) = \left(\frac{1}{\alpha_2} - \frac{1}{\alpha_1}\right) y^T y - \left(\frac{\beta_2}{\alpha_2(\alpha_2 + m\beta_2)} - \frac{\beta_1}{\alpha_1(\alpha_1 + m\beta_1)}\right) (\mathbb{1}^T y)^2 \geq \tau''. \tag{9.25}$$

It is worth noting that the above test is not able to distinguish equal-energy signals sensed with the G-OTS-R2 cryptosystem, since equal energy signals yields measurements with the same covariance matrix.

9.6 Simulation Results

In this section, we evaluate the distinguishability of equal-energy signals in different scenarios. In each experiment, for the numerical evaluation of ϑ_{KL} and the NP test (9.23), the involved pdfs have been sampled on 10000 equispaced bins between -8

and 8, whereas ϑ_{R1}, ϑ_{R2}, and ϑ'_{R2} have been estimated via a Monte Carlo integration using 10^5 random samples.

9.6.1 Upper Bound Validation

The first experiment has been carried out with the aim of assessing the different upper bounds on the distinguishability of unit energy signals: thanks to Theorem 9.7, similar results also apply to arbitrary signals if we consider normalized measurements. In the case of fully random matrices, the signals have been defined as $[x_1]_i = 1/\sqrt{n}$ and $[x_2]_i = Z(\alpha)e^{-\alpha(i-1)}$, for $i = 1, \ldots, n$, where $Z(\alpha)$ is a suitable normalizing constant such that $\mathscr{E}_{x_2} = 1$. In Fig. 9.1 we show the numerically evaluated upper bound ϑ_{KL} when the entries of A are i.i.d. uniform variables with unit variance (uniform sensing matrix), for $n = 1000$ and different combinations of α and m parameters. In the same plots, we also show the maximum value of $P_d - P_f$ achieved by the optimal NP test (9.23), evaluated over 10^6 independent realizations. As can be seen, the performance of the detection attack is predicted quite well by the numerical upper bound.

In the case of G-OTS cryptosystems based on circulant matrices, the signals have been defined as $x_1 = [1, 0, \ldots, 0]$ and $[x_2]_i = Z(\alpha)e^{-4\alpha(i-1)}$, for $i = 1, \ldots, n$, where $Z(\alpha)$ is a suitable normalizing constant such that $\mathscr{E}_{x_2} = 1$. For the G-OTS-C cryptosystem, we consider the matrix P that selects the first m rows of the $n \times n$ circulant matrix $W^H \Lambda W$: an advantage of this construction is that the resulting sensing matrix enables several processing tasks directly on the measurements [20]. In Fig. 9.2, we compared the theoretical upper bounds ϑ_C, ϑ_{R1}, and ϑ_{R2} with the performance obtained by the optimal test Λ_C and the suboptimal test Λ_R, respectively, for $n = 100$ and different combinations of α and m parameters. The approximated

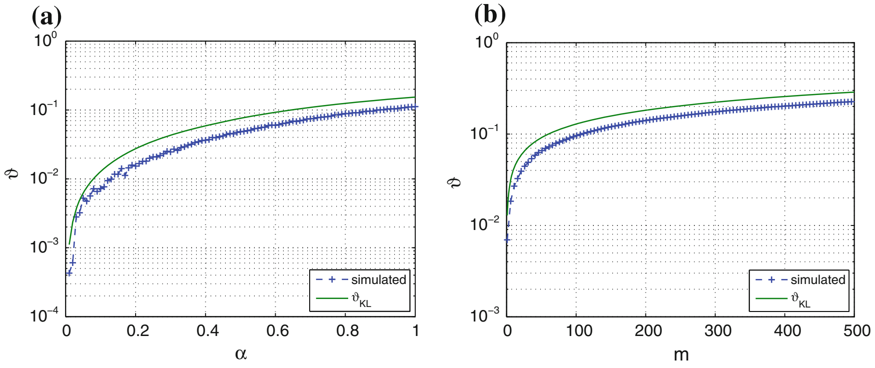


Fig. 9.1 Distinguishability of unit energy vectors using a uniform sensing matrix: **a** $m = 1$, $n = 1000$; **b** $\alpha = 0.1$, $n = 1000$

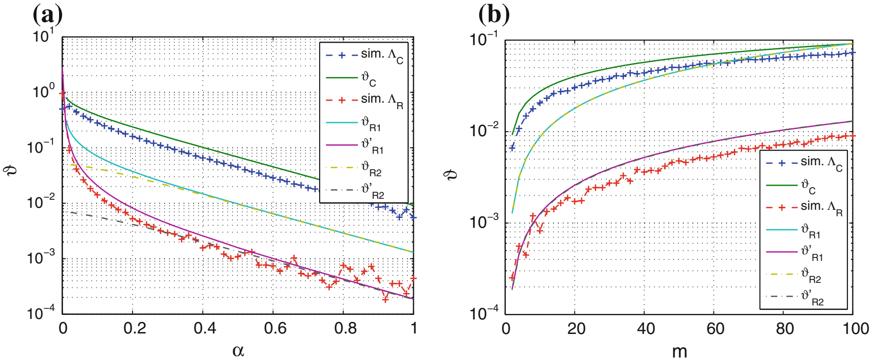


Fig. 9.2 Distinguishability of unit energy vectors using circulant matrices: **a** $m = 2$, $n = 100$; **b** $\alpha = 1$, $n = 100$

bounds ϑ'_{R1}, and ϑ'_{R2} are shown as well. The performance of the detection attack Λ_C is predicted quite well by the theoretical upper bound ϑ_C, whereas the upper bounds ϑ_{R1} and ϑ_{R2} appear quite loose. Interestingly, the approximation ϑ'_{R1} is quite close to the simulated performance of the detection attack Λ_R, especially for higher values of ϑ.

9.6.2 Expected Security

In the second experiment, we computed the numerical upper bounds and the approximated bounds for different realizations of equal-energy signals x_1 and x_2 and different scenarios. Namely, we considered 1000 pairs ϑ_1, ϑ_2 of independent vectors with k nonzero entries uniformly distributed on a unit norm n-sphere, where the respective k-sparse signals were obtained by multiplying those vectors by a unitary matrix Φ. The first scenario considered as Φ the identity matrix, i.e., the signals were sparse in the sensing domain. The second scenario considered as Φ the discrete cosine transform (DCT) matrix. It can be noticed that for equal energy signals a sensing matrix with Gaussian i.i.d. entries achieves perfect secrecy [1], i.e., $\vartheta = 0$. Hence, the proposed experiment permits to immediately evaluate the security loss incurred when using more structured sensing matrices.

In both scenarios we computed ϑ_{KL} for $m = 1$, since for $m > 1$ ϑ_{KL} can be easily obtained by multiplying the distinguishability calculated previously by a factor $\sqrt{m}$, whereas ϑ_C, ϑ'_{R1}, and ϑ'_{R2} were computed for $m = 2$.

In Fig. 9.3a, we show the 0.95 percentile of ϑ_{KL} when $n = 1000$ and k varies in the interval [1, 500]. As expected, if the signals are sparse in the sensing domain the distinguishability decreases when k increases, whereas if the signal are sparse in a different domain the distinguishability is almost constant with respect to k. In Fig. 9.3b, we show the 0.95 percentile of ϑ_{KL} when $k = 10$ and n varies in the

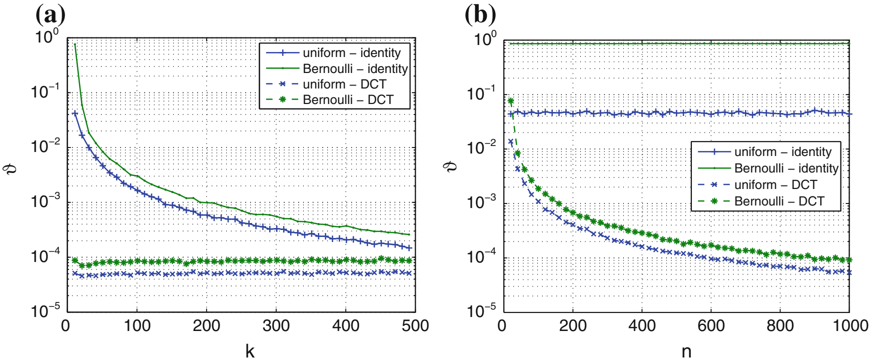


Fig. 9.3 Distinguishability of k-sparse unit energy signals when using different fully random sensing matrix: **a** $n = 1000$; **b** $k = 10$

interval [20, 1000]. As expected, the distinguishability of signals that are sparse in the DCT domain decreases when n increases, whereas if the signals are sparse in the sensing domain the distinguishability does not depend on n.

In Fig. 9.4a, we show the 0.95 percentile of ϑ_C, ϑ'_{R1}, and ϑ'_{R2} when $n = 1000$ and k varies in the interval [1, 500]. The results show that for the two considered classes of sparse signals the security of G-OTS-C and G-OTS-R1 has a similar behavior: the security of both cryptosystems is independent of k when the signal is sparse in the sensing domain, whereas there is a strong dependence on the signal sparsity when the signal is sparse in the DCT domain, since sparser signals are more difficult to conceal. An intuitive explanation is that a very sparse signal in the DCT domain is heavily correlated in the sensing domain and a circulant matrix leaks a lot of information on this correlation. For G-OTS-R2, the security is independent of both k and the sparsity domain, indicating that the prerandomization improves the confidentiality of measurements.

In Fig. 9.4b, we show the 0.95 percentile of ϑ_C, ϑ'_{R1}, and ϑ'_{R2} when $k = 10$ and n varies in the interval [20, 1000]. The security of the G-OTS-C cryptosystem increases for large values of n when the signal is sparse in the sensing domain, whereas it decreases for large values of n when the signal is sparse in the DCT domain. This can be explained by the fact that a signal having a fixed sparsity in the DCT domain becomes extremely correlated when n increases. In the case of the G-OTS-R1 cryptosystem, the security is independent of n when the signal is sparse in the DCT domain, whereas it significantly increases for large values of n when the signal is sparse in the sensing domain. In the case of the G-OTS-R2 cryptosystem, the security always increases for large values of n, showing that this second acquisition strategy guarantees the same level of confidentiality irrespective of the sparsity domain.

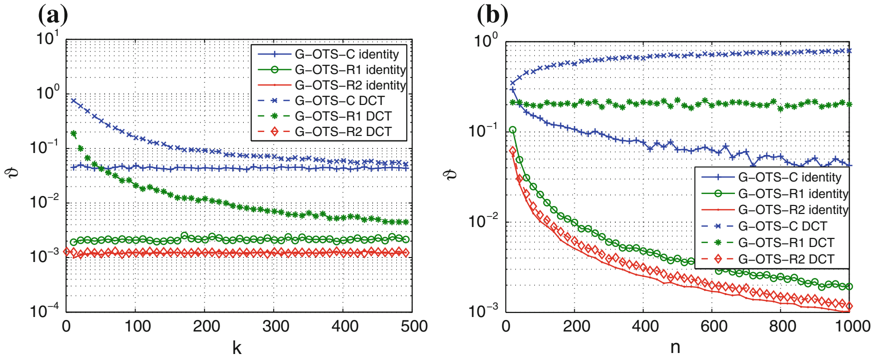


Fig. 9.4 Distinguishability of k-sparse unit energy signals when using different random circulant sensing matrices: **a** $n = 1000$; **b** $k = 10$

9.7 Conclusions

In this chapter, we have analyzed the security of CS measurements when the sensing matrix is either a fully random non-Gaussian matrix or a partial circulant random matrix. Unlike the case of fully random Gaussian matrices, which reveal only the energy of the sensed signal, we find that more general constructions also reveal some partial information on the structure of the signal. This fact implies that normalizing the measurements cannot achieve a perfectly secure channel for this kind of matrices. In order to measure this loss of security, we introduce an operational definition of security based on the problem of distinguishing different signals and we provide useful bounds for evaluating the security of various types of sensing matrices according to this definition.

The above definition has been applied considering two classes of sparse signals. The results indicate that non-Gaussian sensing matrices can provide a certain level of confidentiality when signals are sparse in a DFT-like domain, however they are not able to conceal signals that are very sparse in the sensing domain. For what concerns circulant sensing matrices, the results indicate that partial circulant matrices obtained by taking the first rows of a circulant matrix, which are interesting in practical settings since they enable processing directly on the measurements, provide a very poor encryption layer. The security of circulant sensing matrices can be improved by using a proper randomization. If the sensing matrix is obtained by choosing the rows at random, this construction provides a weak encryption layer if the signals are sparse in the sensing domain, but is not very secure if the signal is sparse in a DFT-like domain. If, in addition, the signs of the signal samples are randomly scrambled before acquisition, this second construction is shown to provide a weak encryption layer irrespective of the sparsity of the signal and the sparsity domain. It is worth noting that the above randomized constructions, even if they do not permit direct processing of the measurements, still retain the computational advantages of standard circulant matrices.

Acknowledgments The research leading to these results has received funding from the European Research Council under the European Community's Seventh Framework Programme (FP7/2007-2013) / ERC Grant agreement no. 279848.

References

1. Bianchi T, Bioglio V, Magli E (2014) On the security of random linear measurements. In: 2014 IEEE International conference on acoustics, speech and signal processing (ICASSP'14), pp 3992–3996, doi:10.1109/ICASSP.2014.6854351
2. Cambareri V, Haboba J, Pareschi F, Rovatti H, Setti G, Wong KW (2013) A two-class information concealing system based on compressed sensing. In: ISCAS'13, pp 1356–1359, doi:10.1109/ISCAS.2013.6572106
3. Candes E, Tao T (2006) Near-optimal signal recovery from random projections: universal encoding strategies? IEEE Trans Inf Theory 52(12):5406–5425. doi:10.1109/TIT.2006.885507
4. Candes E, Romberg J, Tao T (2006) Robust uncertainty principles: exact signal reconstruction from highly incomplete frequency information. IEEE Trans Inf Theory 52(2):489–509. doi:10.1109/TIT.2005.862083
5. Cover TM, Thomas JA (2006) Elements of Information Theory. Wiley-Interscience, Hoboken
6. Do M (2003) Fast approximation of Kullback-Leibler distance for dependence trees and hidden Markov models. IEEE Signal Process Lett 10(4):115–118. doi:10.1109/LSP.2003.809034
7. Do T, Gan L, Nguyen N, Tran T (2012) Fast and efficient compressive sensing using structurally random matrices. IEEE Trans Signal Process 60(1):139–154. doi:10.1109/TSP.2011.2170977
8. Donoho D (2006) Compressed sensing. IEEE Trans Inf Theory 52(4):1289–1306. doi:10.1109/TIT.2006.871582
9. Fanzi Z, Li C, Tian Z (2011) Distributed compressive spectrum sensing in cooperative multihop cognitive networks. IEEE J Sel Topics Signal Process 5(1):37–48. doi:10.1109/JSTSP.2010.2055037
10. Goldwasser S, Micali S (1984) Probabilistic encryption. J Comput Syst Sci 28(2):270–299. doi:10.1016/0022-0000(84)90070-9
11. Haupt J, Bajwa W, Rabbat M, Nowak R (2008) Compressed sensing for networked data. IEEE Signal Process Mag 25(2):92–101. doi:10.1109/MSP.2007.914732
12. Haupt J, Bajwa W, Raz G, Nowak R (2010) Toeplitz compressed sensing matrices with applications to sparse channel estimation. IEEE Trans Inf Theory 56(11):5862–5875
13. Hershey J, Olsen P (2007) Approximating the Kullback Leibler divergence between Gaussian mixture models. In: ICASSP'07, vol 4, pp IV-317–IV-320, doi:10.1109/ICASSP.2007.366913
14. Lehmann EL, Romano JP (2005) Testing Statistical Hypotheses, 3rd edn. Springer, New York
15. Mardani M, Mateos G, Giannakis G (2013) Dynamic anomalography: tracking network anomalies via sparsity and low rank. IEEE J Sel Topics Signal Process 7(1):50–66. doi:10.1109/JSTSP.2012.2233193
16. Orsdemir A, Altun H, Sharma G, Bocko M (2008) On the security and robustness of encryption via compressed sensing. In: IEEE Military communications conference, 2008 (MILCOM 2008), pp 1–7, doi:10.1109/MILCOM.2008.4753187
17. Rachlin Y, Baron D (2008) The secrecy of compressed sensing measurements. In: IEEE 2008 46th Annual allerton conference on communication, control, and computing, pp 813–817, doi:10.1109/ALLERTON.2008.4797641
18. Rauhut H (2009) Circulant and toeplitz matrices in compressed sensing. In: SPARS'09—Signal processing with adaptive sparse structured representations

19. Shannon CE (1949) Communication theory of secrecy systems. Bell Syst Tech J 28:656–715
20. Valsesia D, Magli E (2014) Compressive signal processing with circulant sensing matrices. In: IEEE ICASSP'14, pp 1015–1019, doi:10.1109/ICASSP.2014.6853750
21. Yin W, Morgan S, Yang J, Zhang Y (2010) Practical compressive sensing with Toeplitz and circulant matrices. In: Proceeding of SPIE, vol 7744, pp 77,440K–77,440K–10, doi:10.1117/12.863527

Chapter 10
Subspace Fuzzy Vault

Kyle Marshall, Davide Schipani, Anna-Lena Trautmann and Joachim Rosenthal

Abstract Fuzzy vault is a scheme providing secure authentication based on fuzzy matching of sets. A major application is the use of biometric features for authentication, whereby unencrypted storage of these features is not an option because of security concerns. While there is still ongoing research around the practical implementation of such schemes, we propose and analyze here an alternative construction based on subspace codes. This offers some advantages in terms of security, as an eventual discovery of the key does not provide an obvious access to the features. Crucial for an efficient implementation are the computational complexity and the choice of good code parameters. The parameters depend on the particular application, e.g. the biometric feature to be stored and the rate one wants to allow for false acceptance. The developed theory is closely linked to constructions of subspace codes studied in the area of random network coding.

K. Marshall (✉) · D. Schipani · J. Rosenthal
Institute of Mathematics, University of Zurich, Zurich, Switzerland
e-mail: kyle.marshall@math.uzh.ch

D. Schipani
e-mail: davide.schipani@math.uzh.ch

J. Rosenthal
e-mail: joachim.rosenthal@math.uzh.ch

A.-L. Trautmann
Department of Electrical and Electronic Engineering,
University of Melbourne, Melbourne, Australia

A.-L. Trautmann
Department of Electrical and Computer Systems Engineering,
Monash University, Melbourne, Australia
e-mail: anna-lena.trautmann@unimelb.edu.au

M. Baldi and S. Tomasin (eds.), *Physical and Data-Link Security Techniques for Future Communication Systems*, Lecture Notes in Electrical Engineering 358, DOI 10.1007/978-3-319-23609-4_10

10.1 Introduction

Fuzzy vault is the term used by Juels and Sudan in [7] to describe a cryptographic primitive, in which a key κ is hidden by a set of features A in such a way, that any witness B, which is close enough to A under the set difference metric, can decommit κ. Fuzzy vault is related to the fuzzy commitment scheme of Juels and Wattenberg [8], which gives a solution for noisy hashing of data for the Hamming distance. This and a dual version of it, the fuzzy syndrome hashing scheme, were considered by the authors in [1, 4, 17].

The motivation for fuzzy vault is related to the growing interest in using fuzzy authentication systems, i.e. systems that do not require an exact match, but rather a partial one, between two sets. Instances include the use of biometric features for authentication, personal entropy systems to allow password recovery by answering a set of questions with a level of accuracy above a certain threshold, privacy-protected matching to allow find a match between two parties without disclosing the features in public.

In early biometric authentication systems, comparison of a biometric was done against an image stored locally on the machine, rather than in some hashed form. For security purposes however, passwords are normally stored in hashed form. Moreover, since biometric data is irreplaceable in the sense that once compromised it cannot be changed, storing the data in un-hashed form can pose a significant security risk [3]. Biometric data is inherently noisy, however, so direct hashing of a user's features would prevent the authentic user from accessing the system, as no error tolerance in the matching would be allowed. Using error correcting techniques, the fuzzy vault is a scheme that can recover a secret key hidden by features even in the presence of noise. Recent advancements have been made in the pre-alignment of biometrics (cf. [11] and references therein), specifically fingerprints, allowing for comparative methods without storage of the image itself. These advancements make fuzzy vault a promising and feasible cryptographic solution for noisy data.

Recently, much work has been done in the area of error correcting codes in projective space. These codes turn out to be appropriate for error correction in random network coding [9], and are referred to as error correcting random network codes, projective space codes, or subspace codes. The aim of this chapter is to show that the construction of the fuzzy vault in [7] can be extended and adapted to work for subspace codes in an analogous way with advantages and limitations. Namely, we present a construction for a fuzzy vault based on constant dimension subspace codes, a class of error correcting codes in projective n-space over a finite field $\mathbb{F}_q$. For illustration, an example will be provided by using spread codes, a particular class of subspace codes.

The rest of the chapter is organized as follows: Sect. 10.2 provides preliminaries, terminology and refreshes the original fuzzy vault scheme. Section 10.3 presents the new scheme based on subspace codes. Section 10.4 relates to security and examples and lastly Sects. 10.5 and 10.6 give further considerations and concluding final remarks.

10.2 Preliminaries

Denote by $\mathbb{F}_q$ the finite field with q elements, where q is a prime power. The *set difference metric* d_Δ is defined as

$$d_\Delta(A, B) := |(A\backslash B) \cup (B\backslash A)|, \quad A, B \subseteq \mathbb{F}_q$$

and the *Hamming metric* d_H is defined as

$$d_H(u, v) := |\{i \mid u_i \neq v_i\}|, \quad u = (u_1, \dots, u_n), v = (v_1, \dots, v_n) \in \mathbb{F}_q^n.$$

Let $g_1, \dots, g_n \in \mathbb{F}_q^*$ be distinct elements. A k-dimensional *Reed-Solomon code* $\mathscr{C} \subseteq \mathbb{F}_q^n$ can be defined as

$$\mathscr{C} = \{(f(g_1), \dots, f(g_n)) \mid f(x) \in \mathbb{F}_q[x], \deg(f) < k\}.$$

It has minimum Hamming distance $d_{\min,H}(\mathscr{C}) = n-k+1$ and cardinality $|\mathscr{C}| = q^k$ [12].

A *constant dimension (subspace) code* is a subset of the Grassmannian $\mathscr{G}_q(k, n)$, the set of all k-dimensional subspaces of $\mathbb{F}_q^n$. The subspace distance defines a metric on $\mathscr{G}_q(k, n)$, given by

$$d_S(U, V) := \dim(U + V) - \dim(U \cap V), \quad U, V \in \mathscr{G}_q(k, n)$$

for $U, V \in \mathscr{G}_q(k, n)$ [9]. While finding good subspace codes is still an open research problem, there are many candidates now, including the Reed-Solomon-like and spread code constructions [9, 13]. An explicit construction of a spread code can be found in [13], and it is this construction we use as the definition of a spread code: Let $p(x) \in \mathbb{F}_q[x]$ be an irreducible monic polynomial of degree k and $P \in \mathbb{F}_q^{k\times k}$ be its companion matrix. Let $n = ks$ for $s \in \mathbb{N}$. Then,

$$\mathscr{S} = \{\text{rowsp}(A_1 \mid \cdots \mid A_s) \mid A_i \in \mathbb{F}_q[P], (A_1 \mid \cdots \mid A_s) \neq (0 \mid \cdots \mid 0)\}$$

is called a (k, n)-*spread code*, where rowsp(A) is the row space of a matrix A. From the definition, one can see that the minimum subspace distance of a spread code is $d_{\min,S}(\mathscr{S}) = 2k$ and that the cardinality is $|\mathscr{S}| = \frac{q^n-1}{q^k-1}$.

For practical purposes we need a unique representation of subspaces, and we will choose their matrix representation in reduced row echelon form (i.e. the matrix in reduced row echelon form whose row space is the respective subspace) as such.

We will now briefly revisit the fuzzy vault scheme [7]. We will refer to the following description (cf. also [6]), although we are aware of different interpretations of the scheme throughout the literature, especially in terms of the decoding algorithms and parameters [16]. Since this scheme is based on polynomial evaluation, it will henceforth be called the *polynomial fuzzy vault* (PFV) scheme.

Let $\kappa = (k_0, k_1, ..., k_{\ell-1}) \in \mathbb{F}_q^\ell$ be the secret key and $\kappa(x) = k_0 + k_1x + ...k_{\ell-1}x^{\ell-1} \in \mathbb{F}_q[x]$ the corresponding key polynomial. Let $A \subset \mathbb{F}_q \backslash \{0\}$ be the set of genuine features with $|A| = t > \ell$. Furthermore, let $\lambda : \mathbb{F}_q \to \mathbb{F}_q$ be a random map such that $\lambda(x) \neq \kappa(x)$ for all $x \in B$. Choose $r > t$ and select a set $B \subset \mathbb{F}_q \backslash A$ such that $|B| = r - t$. Construct the sets

$$\begin{aligned} \mathscr{P}_{auth} &= \{(x, \kappa(x)) \mid x \in A\}, \\ \mathscr{P}_{chaff} &= \{(x, \lambda(x)) \mid x \in B\}, \\ \mathscr{V} &= \mathcal{P}_{auth} \cup \mathscr{P}_{chaff}. \end{aligned}$$

We will call $\mathscr{P}_{auth}$ the set of *authentic points*, $\mathscr{P}_{chaff}$ the set of *chaff points* and $\mathscr{V}$ the set of *vault points*.

The remaining parts of the fuzzy vault are a code and a corresponding error correcting decoding algorithm. The code is the ℓ-dimensional Reed-Solomon code $\mathscr{C} \subseteq \mathbb{F}_q^t$,

$$\mathscr{C} = \{(f(g_1), \dots, f(g_t)) \mid f(x) \in \mathbb{F}_q[x], \deg(f) < \ell\},$$

whose defining distinct evaluation points $g_1, \dots, g_t$ are the points in A, i.e. the genuine features. The key polynomial $\kappa(x)$ gives rise to a codeword of $\mathscr{C}$. If a witness attempts to gain access to the key, the witness submits a set of features $W \subset \mathbb{F}_q$. Let $Z \subseteq \mathscr{V}$ be the set of vault points (x, y) with $x \in W$. As the error correction capability of $\mathscr{C}$ is $\lfloor (t - \ell)/2 \rfloor$, the witness needs $|Z \cap \mathscr{P}_{auth}| \geq t - \lfloor (t - \ell)/2 \rfloor = \lceil (t + \ell)/2 \rceil$ to recover $\kappa(x)$ with the decoding algorithm.

To simplify the setting and have a more workable model, assume that $|W| = t$ and that $B = \mathbb{F}_q \backslash A$. Then $|Z| = t$ and we can rewrite $d_\Delta(A, W) = 2t - 2|A \cap W| = 2t - 2|Z \cap \mathscr{P}_{auth}|)$. Thus the witness gains access to the key if

$$d_\Delta(A, W) \leq 2t - (t + \ell) \iff d_\Delta(A, W) \leq d_{min,H}(\mathscr{C}) - 1.$$

It was shown in [15] that certain reasonable parameters for the PFV scheme cause the system to be susceptible to a brute force attack. Choi et al. in [2] speed up the attack by using a fast polynomial reconstruction algorithm. These attacks may indicate that additional security measures should be taken to prevent the loss of a user's features. A different type of security analysis is provided in [6].

10.3 A Fuzzy Vault Scheme Utilizing Subspace Codes

We will now explain our new variant of the fuzzy vault scheme, and call this particular implementation the *subspace fuzzy vault* (SFV) scheme. Unlike the PFV scheme in which the key is given by the coefficients of a polynomial, the key $\hat{\kappa}$ in this scheme is a subspace with a disguised generator matrix κ (not in reduced row echelon form).

Definition 10.1 Let $k \leq n, \mathscr{C} \subset \mathscr{G}_q(k,n)$ a constant dimension subspace code, and $\hat{\kappa} \in \mathscr{C}$ a secret subspace. Choose some $\kappa \in \mathbb{F}_q^{k \times n}$ such that $\mathrm{rowsp}(\kappa) = \hat{\kappa}$. We will hide the key by a set of linearly independent features $A \subset \mathbb{F}_q^k$ with $|A| = k$ and a set $B = \mathbb{F}_q^k \backslash A$. Let $\lambda(x) : \mathbb{F}_q^k \rightarrow \mathbb{F}_q^n$ be a random map such that $\lambda(x) \notin \mathrm{rowsp}(\check{})$ for all $x \in B$. Define the sets

$$\begin{aligned} \mathscr{P}_{auth} &= \{(x, x\kappa) \mid x \in A\}, \\ \mathscr{P}_{chaff} &= \{(x, \lambda(x)) \mid x \in B\}, \\ \mathscr{V} &= \mathscr{P}_{auth} \cup \mathscr{P}_{chaff}. \end{aligned}$$

$\mathscr{P}_{auth}$ is called the set of *authentic points*, $\mathscr{P}_{chaff}$ is called the set of *chaff points*, and $\mathscr{V}$ the set of *vault points*.

In order for a witness to decommit $\hat{\kappa}$, a set $W \subset \mathbb{F}_q^k$ is submitted and the second coordinates of the elements in the vault whose first coordinates correspond to W are used to generate a subspace W'. This subspace is then decoded to yield a codeword $U \in \mathscr{C}$. We assume that W consists of at most k linearly independent features.

For a set $S \subset \mathbb{F}_q^k$, we will denote by $\langle S \rangle_\kappa$ the subspace spanned by the elements $\{s\kappa \mid s \in S\}$. We will also assume $\dim(W') = |W|$, although this may not happen, introducing some probability of error, as we mention below. The assumption is justified by estimating its probability using counting formulas like that in the following Lemma 10.1, whilst supposing n big enough and the second coordinates of the chaff points being randomly chosen within their domain.

Theorem 10.1 *In the setting of Definition 10.1, the vault recovers the key $\hat{\kappa}$ if and only if*

$$d_\Delta(A, W) \leq \frac{1}{2}(d_{\min,S}(\mathscr{C}) - 1).$$

Proof We can express $W' = (W' \cap \hat{\kappa}) \oplus E$ for some subspace $E \subset \mathbb{F}_q^n$. As shown in [9], we can uniquely recover $\hat{\kappa}$ from W' if and only if $d_S(W', \hat{\kappa}) \leq \frac{1}{2}(d_{\min,S}(\mathscr{C}) - 1)$.

Using properties of the rank and linear algebra identities, we get

$$\begin{aligned} d_\Delta(A, W) &= |W \backslash A| + |A \backslash W| \\ &= \dim(\langle W \backslash A \rangle_\kappa) + \dim(\langle A \backslash W \rangle_\kappa) \\ &= \dim(\langle W \backslash A \rangle_\kappa) + k - \dim(\langle A \cap W \rangle_\kappa) \\ &= \dim(E) + k - \dim(\hat{\kappa} \cap W') \\ &= d_S(W', \hat{\kappa}). \end{aligned}$$

Indeed, as $|W| \leq k$, $|A| = k$, and W and A are sets of linearly independent features, Sylvester's rank inequality implies $|W \backslash A| \leq \dim(\langle W \backslash A \rangle_\kappa)$, while the inequality in the other direction is obvious, therefore $|W \backslash A| = \dim(\langle W \backslash A \rangle_\kappa)$; similarly we have $|A \backslash W| = \dim(\langle A \backslash W \rangle_\kappa)$ and $|A \cap W| = \dim(\langle A \cap W \rangle_\kappa)$. Also $\dim(\hat{\kappa} \cap W') =$

$|A \cap W|$, as the second coordinates of $W \backslash A$ generate a subspace which does not intersect $\hat{\kappa}$ by definition of $\mathscr{P}_{chaff}$ and given that $B = \mathbb{F}_q^k \backslash A$.

Overall, it follows that $d_\Delta(A, W) = d_S(W', \hat{\kappa})$, and therefore we can uniquely decode W' to $\hat{\kappa}$ as soon as the set difference between A and W is at most $\frac{1}{2}(d_{\min,S}(\mathscr{C}) - 1)$. □

10.3.1 Variants of the Scheme

In order to loosen the constraints on the choice of parameters, other settings and scheme variants can be considered, although some probability of error may be introduced.

For example, we can allow $|A| = |W| = t \geq k$, with the features thought as randomly chosen in the ambient space rather than linearly independent. Other looser assumptions include also B being a proper subset of $\mathbb{F}_q^k \backslash A$.

In these cases, one needs to compare $\dim(\hat{\kappa} \cap W')$ with $|A \cap W|$ and $\dim(\hat{\kappa} + W')$ with $|A \cup W|$. For example $\dim(\hat{\kappa} \cap W')$ is no bigger than k while $|A \cap W|$ would be no bigger than t; $|A \cup W|$ counts elements of A which do not contribute to the dimension of $\hat{\kappa}$; $\dim(W')$ may not be equal to $|W|$ and the looser assumption on B may reduce the dimension of W' even more, introducing further variability.

Depending on the assumptions and parameters, one can expect to have bounds of the form:

$$d_\Delta(A, W) - \delta_1 \leq d_S(W', \hat{\kappa}) \leq d_\Delta(A, W) + \delta_2,$$

for some $\delta_1, \delta_2 \in \mathbb{N}$. Depending on the given threshold for $d_\Delta(A, W)$, one can estimate the probability of falsely accepting or falsely rejecting the witness.

To be more precise, with the above mentioned looser assumptions, we get $\dim(\hat{\kappa}) = k = |A| - (t - k)$, $\dim(W') \leq |W|$ and $\dim(\hat{\kappa} \cap W') \leq |A \cap W|$. If y is an upper bound on the difference between $|A \cap W|$ and the maximum number of linearly independent elements within $A \cap W$ (i.e. $y = 0$ for the hypothesis of Theorem 10.1), we have on one side

$$\begin{aligned} d_S(W', \hat{\kappa}) &= \dim(\hat{\kappa}) + \dim(W') - 2\dim(\hat{\kappa} \cap W') \\ &\leq |A| - (t - k) + |W| - 2(|A \cap W| - y) \\ &= d_\Delta(A, W) - (t - k) + 2y. \end{aligned}$$

On the other side, if z is an upper bound for $|W| - \dim(W')$, we get

$$\begin{aligned} d_S(W', \hat{\kappa}) &= \dim(\hat{\kappa}) + \dim(W') - 2\dim(\hat{\kappa} \cap W') \\ &\geq |A| - (t - k) + |W| - z - 2(|A \cap W|) \\ &= d_\Delta(A, W) - (t - k) - z. \end{aligned}$$

Note that z depends on the assumptions on the size of B and on the choice of chaff points and the parameter n, as discussed in the first part of Sect. 10.3. I.e. z can be neglected if n is big enough, B is the complement to A, and the chaff points are randomly chosen. Similar bounds can also be obtained for $t < k$.

Incidentally, these inequalities provide an alternative proof to Theorem 10.1.

10.4 Security and Examples

Notice that we can use n as a degree of freedom to enlarge the size of the key space.

We know the following fact from [10]:

Lemma 10.1 *Let $k \leq \delta \leq n$. The number of $\delta \times n$ matrices over $\mathbb{F}_q$ with rank k is given by*

$$N_q(k, \delta, n) = \frac{\left(\prod_{i=0}^{k-1} q^n - q^i\right)\left(\prod_{i=0}^{k-1} q^\delta - q^i\right)}{\prod_{i=0}^{k-1} q^k - q^i}. \tag{10.1}$$

With $\delta = \kappa$ we can see that we can play on n to make this number grow as we please, in order to make it hard searching for the right set of k linearly independent features.

Moreover, the complexity of such a brute force attack should be combined with the difficulty of determining the rank of an arbitrary $k \times n$ matrix over $\mathbb{F}_q$. The naive approach, using Gaussian algorithm, requires at most $n(k^2 - k)$ field operations, and in case the field is $\mathbb{F}_2$ at most $n(k^2 - k)/2$. There exist fast algorithms for determining the rank of a matrix but these are only asymptotically better and are often much worse for small values of k and n.

10.4.1 Other Attacks

When $|A| = t > k$, not only may some difficulty in decoding arise, but if t is much bigger than k, other types of brute force attacks may be devised. In the following a strategy is described which tries to find a set in $\mathbb{F}_q^n$ containing k linearly independent vectors that are meant to reveal the authentic features.

Assume now to have t authentic points and $r - t$ chaff points, with the set of features $\{x_1, ..., x_t\}$ being a set of random elements of $\mathbb{F}_q^k$. We can assume that the second coordinates of the authentic set $\{x_1\kappa, ..., x_t\kappa\}$ contain a set of k linearly independent vectors in $\mathbb{F}_q^n$. Indeed, given Lemma 10.1, we can compute the probability that $x_1\kappa, ..., x_t\kappa$ contains a set of k linearly independent vectors as

$$\frac{N_q(k, k, t)}{q^{kt}},$$

that is the probability that $(x_1, ..., x_t)^T$ is a rank k matrix. For common vault parameters, and especially for larger t, this value is close to 1, so as to justify our assumptions.

Now, the expected number of subsets of size δ out of $r > \delta$ random points in $\mathbb{F}_q^n$ that span a k-dimensional space can be estimated as

$$\alpha_q(k, \delta, n) = \frac{\binom{r}{\delta} N_q(k, \delta, n)}{q^{\delta n}}. \tag{10.2}$$

Ideally, an attacker would want to find a $\delta_0 \leq |A| = t$ so that $\alpha_q(k, \delta_0, n) < 1$ in order to have a high probability of recovering the key in the event that the δ_0 points span a space of dimension k. On the other side, to counter this type of attack, one tries to keep k very close to t and r big enough, so that α_q does not get small.

We will approximate the complexity of a brute force attack following this approach. The attack is similar in approach to that proposed in [7] and depends on finding a suitable δ_0, so that the probability of δ_0 random vectors in $\mathbb{F}_q^n$ spanning a subspace of dimension k is small.

It is noted in [15] that the average number of attempts for a user to guess δ points in the authentic set is $\binom{r}{\delta}/\binom{t}{\delta} < 1.1(r/t)^\delta$ for $r > t > 5$. Given that it takes $n(\delta^2 - \delta)/2$ operations to row reduce a $\delta \times n$ binary matrix, we obtain the following upper bound for the expected time to recover the key.

Lemma 10.2 *In the above settings, let δ_0 be so that $\alpha_2(k, \delta_0, n) < 1$ from Eq.* (10.2). *On average, an attacker can recover the secret key in $C \cdot (r/t)^{\delta_0}$ operations, where $C < 0.55 \cdot n(\delta_0^2 - \delta_0)$.*

10.4.2 Example Using Spread Codes

As an example of how to construct a vault using subspace codes, we will use spread codes, as defined in Sect. 10.2.

Spread codes are somewhat restrictive in that the minimum distance is completely determined by k, unlike other subspace codes where one can trade off the distance with other parameters. Nevertheless we illustrate the construction using spread codes because of their simplicity.

Example 10.1 Let us assume that the features belong to $\mathbb{F}_2^{16}$, so that $k = 16$. In this case, we can recover the key if and only if the set difference is at most 15. We are free to choose n as long as it is a positive integer multiple of k. For example we can choose $n = 96$ so that we have roughly 2^{80} keys.

Note that an $(n, k)_q$ spread code can be decoded in $\mathscr{O}((n-k)k^5)$ field operations over $\mathbb{F}_q$, as shown in [5]. For more information on spread codes and other decoding algorithms, the reader is referred to [5, 13, 14].

10.5 Further Considerations

One of the disadvantages of using a biometric for security is that once an attacker knows a user's features, the user can never use a biometric scheme based on those features again.In the PFV finding the key is essentially equivalent to finding the features, as they are immediately retrievable as the first coordinates of the points in the authentic set, i.e. by testing whether these correspond to evaluations of the key polynomial. In the SFV, instead, an attacker who is capable of obtaining $\hat{\kappa}$, has no big advantage in recovering $x_1, ..., x_t$ from $x_1\kappa, ..., x_t\kappa$, not knowing which particular κ was used to generate the second coordinates of the authentic points. Ideally, to make the system even more resilient, the user should have the features obscured, for instance one might want to store in the vault a hash of the features, instead of the features themselves, as

$$\begin{aligned}\mathscr{P}_{auth} &= \{(h(x), x\kappa) \mid x \in A\}\\ \mathscr{P}_{chaff} &= \{(h(x), \lambda(x)) \mid x \in B\},\end{aligned}$$

for a suitable hash function h. There is also another important reason to use hashes as above in the system. In fact, suppose that an attacker finds an element in the unhashed version of the vault whose first coordinate is a linear combination of other first coordinates of other elements in the vault. Then he can check whether its second coordinate is also a linear combination (with the same coefficients) of the corresponding second coordinates of the other elements. If this happens he can argue that the element belongs to $\mathscr{P}_{auth}$. Clearly also this attack can be prevented by taking t close to k, besides using an hash function to hide the first coordinates.

10.6 Conclusions

We have proposed a new authentication scheme based on noisy data like biometric features. The idea has similarities with the fuzzy vault scheme and works in the set difference metric, but it exploits the new setting of subspace codes. We have presented a main theorem with two alternative proofs that shows under which distance conditions authentication succeeds with respect to the code parameters. We have also showed the possibility of considering a few variants based on slightly different assumptions and how the main theorem can be generalized. This can allow more flexibility for the choice of parameters and for future applications. The security of the scheme has been analyzed, whereby brute force attacks require bigger computational costs compared with traditional schemes. This however comes with a price, that is the computational complexity of state of the art decoding schemes for subspace codes is also rather high. There are also a few other nice features of the new scheme, for example its resilience to exposing the features even if the key were compromised.

Future research includes enhancing the scheme or devising alternative schemes based on subspace codes that would enable more efficient and flexible parameter profiles or decoding scenarios. Also considering examples with families of codes other than spread codes may help suggest future steps towards an actual deployment in practice.

Acknowledgments Kyle Marshall and Joachim Rosenthal were supported by Swiss National Science Foundation Grant no. 149716. Anna-Lena Trautmann was supported by Swiss National Science Foundation Fellowship no. 147304. The authors would like to thank Marco Bianchi and Natalia Silberstein for fruitful discussions regarding this work.

References

1. Baldi M, Bianchi M, Chiaraluce F, Rosenthal J, Schipani D (2011) On fuzzy syndrome hashing with LDPC coding. In: Proceeding of 4th international sympoisum applied sciences in biomedical and communication technologies (ISABEL), pp 1–5
2. Choi WY, Lee S, Moon D, Chung Y, Moon KY (2008) A fast algorithm for polynomial reconstruction of fuzzy fingerprint vault. IEICE Electron Express 5(18):725–731
3. Clancy C (2003) Secure smartcard-based fingerprint authentication. In: ACM Workshop on biometrics: methods and applications, pp 45–52
4. Fontein F, Marshall K, Rosenthal J, Schipani D, Trautmann AL (2012) On burst error correction and storage security of noisy data. In: Proceeding 20th international symposium mathematical theory of networks and systems (MTNS)
5. Gorla E, Manganiello F, Rosenthal J (2012) An algebraic approach for decoding spread codes. Adv Math Commun (AMC) 6(4):443–466
6. Hartloff J, Bileschi M, Tulyakov S, Dobler J, Rudra A, Govindaraju V (2013) Security analysis for fingerprint fuzzy vaults. In: SPIE defense, security and sensing
7. Juels A, Sudan M (2006) A fuzzy vault scheme. Des Codes Crypt 38(2):237–257
8. Juels A, Wattenberg M (1999) A fuzzy commitment scheme. In: Proceeding 6th ACM conference on computer and communications security, CCS '99, pp 28–36
9. Koetter R, Kschichang F (2007) Coding for errors and erasures in random network coding. In Proceeding of IEEE international symposium, information theory
10. Laksov D, Thorup A (1994) Counting matrices with coordinates in finite fields and of fixed rank. Mathematica Scandinavica 74:19–33
11. Li P, Yang X, Cao K, Tao X, Wang R, Tian J (2010) An alignment-free fingerprint cryptosystem based on fuzzy vault scheme. J Netw Comput Appl 33(3):207–220
12. MacWilliams FJ, Sloane N (1977) The Theory of Error-Correcting Codes. North Holland, Amsterdam
13. Manganiello F, Gorla E, Rosenthal J (2008) Spread codes and spread decoding in network coding. In: Proceeding of IEEE international symposium information theory, pp 881–885
14. Manganiello F, Trautmann A-L (2014) Spread decoding in extension fields. Finite Fields Appl 25:94–105
15. Mihailescu P, Munk A, Tams B (2009) The fuzzy vault for fingerprints is vulnerable to brute force attack. In: Proceeding of BIOSIG, pp 43–54
16. Poon HT, Miri A (2012) On efficient decoding for the fuzzy vault scheme. In: IEEE 11th International conference information science signal processing and their application, pp 454–459
17. Schipani D, Rosenthal J (2010) Coding solutions for the secure biometric storage problem. In: Information theory workshop (ITW), 2010 IEEE, Dublin, Ireland, pp 1–4

Chapter 11
An Information Rate Improvement for a Polynomial Variant of the Naccache-Stern Knapsack Cryptosystem

Giacomo Micheli, Joachim Rosenthal and Reto Schnyder

Abstract We adapt an information rate improvement by Chevallier-Naccache-Stern for the Naccache-Stern knapsack cryptosystem, called the prime packing strategy, to the polynomial version of the protocol.

11.1 Introduction

In 1997 Naccache and Stern [4] proposed a new public key cryptosystem known as the *Naccache-Stern Knapsack cryptosystem*, or *NSK* for short. This system was based on modular arithmetic in the integers and had a number theoretic flavor. However, NSK suffers from a low information rate: The ratio of message to ciphertext size is less than 10 % for many practical parameters. More recently in 2008, Chevallier-Mames, Naccache and Stern [2] presented several alterations to the protocol that improve the information rate at the cost of a larger public key size.

More than a decade after the NSK protocol was invented, Micheli and Schiavina presented a generalized monoid based version of the NSK Protocol [3], as well as an instance based on polynomials over finite fields. This variant suffers from the same low information rate. In this chapter, we apply the improvements of [2] to this polynomial based variant.

G. Micheli (✉) · J. Rosenthal · R. Schnyder
Institute of Mathematics, University of Zurich,
Winterthurerstrasse 190, 8057 Zurich, Switzerland
e-mail: giacomo.micheli@math.uzh.ch

J. Rosenthal
e-mail: rosenthal@math.uzh.ch

R. Schnyder
e-mail: reto.schnyder@math.uzh.ch

M. Baldi and S. Tomasin (eds.), *Physical and Data-Link Security Techniques for Future Communication Systems*, Lecture Notes in Electrical Engineering 358, DOI 10.1007/978-3-319-23609-4_11

11.2 Recalling the NSK Protocol

We recall here the NSK protocol and its generalization. They are both based on the following problem:

Problem 11.1 Let L be a positive integer, M be a monoid and $c, v_1, \dots, v_L$ elements of M. Find (if one exists) a vector $m = (m_1, \dots m_L) \in \{0, 1\}^L$ for which

$$c = \prod_{i=1}^{L} v_i^{m_i}.$$

In what follows, we show some instances of the problem above and the cryptographic protocol arising from them. Let $\mathbb{F}_q$ be the finite field of order q.

Problem 11.2 Fix a positive integer L, the monoid $M = (\mathbb{F}_q[x], \cdot)$, irreducible polynomials $p_1, \dots, p_L \in M$ and

$$c = \prod_{i=1}^{L} p_i^{m_i}.$$

for some $(m_1, \dots m_L) \in \{0, 1\}^L$. Find the vector m.

It is immediate that Problem 11.2 can be easily solved by reducing c modulo p_i for each i: we have in fact $m_i = 1$ if and only if $c \equiv 0 \mod p_i$.

Problem 11.3 Let g be an irreducible polynomial of degree N, L a positive integer and $M = (\mathbb{F}_q[x]/(g(x)), \cdot) \cong (\mathbb{F}_{q^N}, \cdot)$. Let $v_1, \dots, v_L \in M$ and

$$c = \prod_{i=1}^{L} v_i^{m_i}.$$

for some $(m_1, \dots m_L) \in \{0, 1\}^L$. Find the vector m.

The generic instance of Problem 11.3 is now difficult compared to Problem 11.2. This gap is exploited in [3]. In what follows we recall their protocol, which we will refer to as the *polynomial NSK* or *pNSK* for short.

Alice sets up the system as follows:

- Alice chooses a finite field $\mathbb{F}_q$, L irreducible polynomials $p_i \in \mathbb{F}_q[x]$, an irreducible polynomial g for which $\sum_{i=1}^{L} \deg p_i < \deg g$ and a pair of integers (e, s) for which $es \equiv 1 \mod q^N - 1$.
- The private key is $(p_1, \dots, p_L, s)$.
- The public key is $(v_1, \dots, v_L, \mathbb{F}_q[x]/(g(x)))$, where $v_i = p_i^e$.

The encryption of a message $m \in \{0, 1\}^L$ is performed as

$$m \mapsto \prod_i v_i^{m_i} = c \in \mathbb{F}_q[x]/(g(x)).$$

Alice can then decrypt by computing $c^s \in \mathbb{F}_q[x]/(g(x))$ and reducing the result modulo p_i for each i, since $c^s \mod g(x)$ (together with its factorization in terms of the p_i) suitably lifts to $\mathbb{F}_q[x]$ using the property $\sum_{i=1}^{L} \deg p_i < \deg g$.

The original NSK is obtained by replacing $\mathbb{F}_q[x]$ by $\mathbb{Z}$ and irreducible polynomials by prime numbers.

11.3 Prime Packing

In what follows our goal is to show that a direct adaptation of the NSK packing presented in [2] is also possible in the case of the polynomial variant. We pack the irreducible polynomials up to degree d as follows: Let $b, t \in \mathbb{N}$ be positive integers for which $bt \leq \overline{\pi}(d)$, where $\overline{\pi}(d)$ is the number of irreducible polynomials up to degree d. Partition the first (according to any ordering respecting the degree) bt polynomials in t sets $\{S_i\}$ each of size b satisfying that for all $i, j \in \{1, \dots, t\}$, if $f \in S_i$ and $h \in S_j$ we have

$$i \leq j \Rightarrow \deg(f) \leq \deg(h).$$

More informally, we pack the polynomials up to degree d into t packs, each of them containing the b polynomials of the lowest possible degree. Let us denote by $p_{j,i}$ the ith polynomial living in the jth box S_j, again ordered by degree. In particular, we have $\deg p_{j,i} \leq \deg p_{j,b}$ for all i and j. The protocol will then be modified as follows. The space of messages becomes $\{1, \dots, b\}^t$, we require now only $\sum_{j=1}^{t} \deg p_{j,b} < \deg g = N$. Again, let $es \equiv 1 \mod q^N - 1$.

The public key is set up as $\left(\{v_{j,i}\}_{i,j}, \mathbb{F}_q[x]/(g(x))\right)$, where again $v_{j,i} = p_{j,i}^e$. The secret key is analogously $\left(\{p_{j,i}\}_{i,j}, s\right)$. The encryption of a message $m = (m_1, \dots, m_t) \in \{1, \dots, b\}^t$ is performed as

$$m \mapsto \prod_{j=1}^{t} v_{j,m_j} = c \in \mathbb{F}_q[x]/(g(x)).$$

Alice can then decrypt by computing $c^s \in \mathbb{F}_q[x]/(g(x))$ and reducing the result modulo $p_{j,i}$ for each i, j, as before.

It is now easy to compute the information rate and public key size: The information rate is $\frac{t \log b}{N \log q}$, and the public key has size $btN \log q$.

Table 11.1 Information rate and public key size of prime packing for $q = 6287$, deg $g = 131$ and various box sizes

b	t	Information rate (%)	Public key size (kbit)
pNSK	130	7.9	215
5	130	18.3	1074
10	130	26.1	2149
30	130	38.6	6447
50	127	43.4	10496
70	109	40.4	12612

11.3.1 Example Parameters

As an example, consider the medium prime case $q = 6287$. We compare the information rate and public key size of our scheme in the case deg $g = 131$ for various values of the box size b in Table 11.1. Computations were done using Sage [6]. The first row corresponds to the original pNSK (which is not quite the same as setting $b = 1$). Note that for small box sizes b, we always get $t = 130$ boxes. This is because it is possible to use only degree 1 polynomials for the $p_{j,i}$. As b becomes larger, this is no longer possible, and the information rate suffers.

Evidently, the information rate can be greatly improved at the cost of a much larger public key size. This cost can be somewhat reduced by applying the "powers of primes" technique of [2], and we will do so in Sect. 11.4.

11.3.2 Asymptotic Information Rate

As in [2], we can obtain linear bandwidth by setting the number of packs equal to their size. Indeed, we show that if we set $n := b = t$, then the information rate of pNSK using prime packing is asymptotically equal to $\frac{1}{2}$.

To analyze the information rate, we first need to find the degree of the nth irreducible polynomial p_n, according to any order respecting the degree. In [3, Sect. 3.2.2], it was shown that the number of irreducible polynomials in $\mathbb{F}_q[x]$ of degree at most d is asymptotically equal to $\frac{q}{q-1}\frac{q^d}{d}$. Hence, the polynomials with a given degree d should be numbered roughly between $\frac{q}{q-1}\frac{q^{d-1}}{d-1}$ and $\frac{q}{q-1}\frac{q^d}{d}$. Thus, if the polynomial p_n has degree d_n, we have

$$\frac{q}{q-1}\frac{q^{d_n-1}}{d_n-1} \lesssim n \lesssim \frac{q}{q-1}\frac{q^{d_n}}{d_n},$$

where $a_n \lesssim b_n$ means that $\limsup_{n\to\infty} a_n/b_n \leq 1$. Taking logarithms gives

$$(d_n - 1) - \log_q(d_n - 1) \lesssim \log_q n - \log_q \frac{q-1}{q} \lesssim d_n - \log_q d_n,$$

which asymptotically is the same as

$$d_n - 1 \lesssim \log_q n \lesssim d_n.$$

We hence see that $d_n = \deg p_n \sim \log_q n$.

Now we can approximate the degree of g:

$$\begin{aligned} N = \deg g &= 1 + \sum_{i=1}^{n} \deg p_{in} \\ &\sim \sum_{i=1}^{n} \log_q(in) \sim \sum_{i=1}^{n} \log_q(n^2) \sim 2n \log_q n. \end{aligned}$$

For the first $\sim$, note that the indices of p_{in} in the sum are all at least n, and so only the asymptotic behavior of $\deg p_{in}$ is relevant. Finally, we get for the information rate

$$\frac{t \log_2 b}{N \log_2 q} \sim \frac{n \log_2 n}{2n \log_q n \log_2 q} = \frac{n \log_2 n}{2n \log_2 n} = \frac{1}{2}.$$

11.4 Powers of Primes

In [2, Sect. 4], prime packing was applied to a variant of NSK using a base larger than 2 in order to further improve information rate and reduce public key size. This method can also be applied to the polynomial NSK variant.

As in Sect. 11.3, we again choose a degree d and integers b and t satisfying $bt \leq \overline{\pi}(d)$, and we partition the first bt irreducible polynomials into t sets S_i of size b. We further choose an integer parameter $\ell \geq 1$. We again denote by $p_{j,i}$ the ith polynomial in the jth box, ordered by degree. As before, we need an irreducible polynomial $g \in \mathbb{F}_q[x]$ of large degree as our modulus, but this time, we require that $\sum_{j=1}^{t} \ell \deg p_{j,b} < \deg g = N$. Again, we choose integers e and s with $es \equiv 1 \mod q^N - 1$ and set $v_{j,i} = p_{j,i}^e$. The public key is $\big(\{v_{j,i}\}_{i,j}, \ell, \mathbb{F}_q[x]/(g(x))\big)$ and the private key is $\big(\{p_{j,i}\}_{i,j}, s\big)$.

For each box S_i, we now have more options available for encryption than simply choosing one element of S_i: we can choose up to ℓ elements, allowing repetitions, and multiply those. Each of these possibilities corresponds to a b-tuple in $T = \{(k_1, \dots, k_b) \in \mathbb{N}^b \mid k_1 + \cdots + k_b \leq \ell\}$. As shown in [2, Appendix A], there are $\binom{b+\ell}{\ell} = B$ such tuples, and there is a bijection $\varphi\colon \{1, \dots, B\} \to T$ that can be computed efficiently [5]. Hence, we use the message space $\{1, \dots, B\}^t$, and we encrypt a message $m = (m_1, \dots, m_t)$ as

$$m \mapsto \prod_{j=1}^{t} \prod_{i=1}^{b} v_{j,i}^{k_{j,i}} = c \in \mathbb{F}_q[x]/(g(x)),$$

where $\varphi(m_j) = (k_{j,1}, \dots, k_{j,b}) \in T$.

Decryption is again done by lifting and factoring c^s and inverting φ.

We can again give a formula for information rate and public key size. The information rate is $\frac{t \log B}{N \log q}$, and the public key still has size $btN \log q$.

11.4.1 Toy Example

We present a small example to clarify the "powers of primes" method. Let $q = 2$, and we consider a system with $t = 2$ packs of $b = 3$ irreducible polynomials each. Let furthermore $\ell = 2$. The first six irreducible polynomials are

$$\begin{aligned} p_{1,1} &= x & p_{2,1} &= x^3 + x + 1 \\ p_{1,2} &= x + 1 & p_{2,2} &= x^3 + x^2 + 1 \\ p_{1,3} &= x^2 + x + 1 & p_{2,3} &= x^4 + x^3 + 1. \end{aligned}$$

We need $\ell \deg p_{1,3} + \ell \deg p_{2,3} = 12 < \deg g = N$, so we choose

$$g = x^{13} + x^4 + x^3 + x + 1.$$

We randomly choose secret exponents $e = 6020$ and $s = 6380 \equiv e^{-1} \mod 2^{13} - 1$. The public elements are now given by $v_{j,i} \equiv p_{j,i}^e \mod g$:

$$\begin{aligned} v_{1,1} &= x^{11} + x^{10} + x^9 + x^8 + x^6 + x^5 & v_{2,1} &= x^8 + x^7 + x^6 + x^5 + x^4 + 1 \\ v_{1,2} &= x^{11} + x^{10} + x^9 + x^8 + x^6 + x & v_{2,2} &= x^{12} + x^{11} + x^6 + x^5 + x^3 \\ v_{1,3} &= x^{12} + x^{11} + x^{10} + x^9 + x^5 + x^3 + x^2 + 1 & v_{2,3} &= x^{12} + x^{11} + x^{10} + x^6 + x^5 + x^2. \end{aligned}$$

Note that $B = \binom{3+2}{2} = 10$, so we can represent a message in base 10. We choose the following encoding from integers 0 to 9 to 3-tuples (k_1, k_2, k_3) satisfying $k_1 + k_2 + k_3 \le 2$.

$$\begin{array}{lllll} 0 \mapsto (0,0,0) & 1 \mapsto (1,0,0) & 2 \mapsto (2,0,0) & 3 \mapsto (0,1,0) & 4 \mapsto (1,1,0) \\ 5 \mapsto (0,2,0) & 6 \mapsto (0,0,1) & 7 \mapsto (1,0,1) & 8 \mapsto (0,1,1) & 9 \mapsto (0,0,2). \end{array}$$

Table 11.2 Information rate and public key size of the "powers of primes" variant for $q = 6287$, $\deg g = 131$ and various box sizes and bases

b	ℓ	t	Information rate (%)	Public key size (kbit)
1	1	130	7.9	215
2	2	65	10.1	215
10	10	13	13.8	215
30	1	130	39.0	6447
42	2	65	38.9	4513
310	26	5	38.8	2562
83	26	5	25.1	686

To encrypt the message $m = 94$, we hence compute

$$v_{1,1}^{0} v_{1,2}^{0} v_{1,3}^{2} \cdot v_{2,1}^{1} v_{2,2}^{1} v_{2,3}^{0} \equiv x^{12} + x^{9} + x^{8} + x^{3} + x^{2} + 1 = c \mod g.$$

To decrypt, raise the ciphertext to s and factor:

$$\begin{aligned} m^{s} &\equiv x^{10} + x^{9} + x^{6} + x^{5} + x^{4} + x + 1 \mod g \\ &= (x^{2} + x + 1)^{2} \cdot (x^{3} + x + 1) \cdot (x^{3} + x^{2} + 1) \\ &= p_{1,1}^{0} p_{1,2}^{0} p_{1,3}^{2} \cdot p_{2,1}^{1} p_{2,2}^{1} p_{2,3}^{0}, \end{aligned}$$

from which the message is recovered.

11.4.2 Example Parameters

We again consider the case $q = 6287$ and compare the information rate and public key size of the "powers of primes" variant in the case $\deg g = 131$ for different values for b and ℓ in Table 11.2. The first row corresponds to the original pNSK, which is obtained by setting $b = 1$ and $\ell = 1$.

As we can see, the "powers of primes" method allows, to an extent, for larger information rates at the same key size, or for smaller keys for a given information rate.

11.5 Security

As for the original Naccache-Stern cryptosystem, we do not know of a security proof for the pNSK, with or without our information rate improvements. However, we can recall a few considerations regarding the security of NSK from [2, 4], which also apply to our variant.

First of all, note that our system is broken if one can solve a discrete logarithm problem $p^s_{j,i} = v_{j,i}$, as this directly reveals the secret key. Although the $p_{j,i}$ don't have to be released publicly, they must have low degree and can thus be guessed easily. Hence, it is important to choose parameters in such a way that the field $\mathbb{F}_q[x]/(g(x))$ is large enough to withstand a DLP attack. Compared to the original NSK, we have to be even more careful due to recent quasipolynomial attacks on small characteristic [1].

As remarked in [4], a birthday-search attack on the message is possible on all NSK variants. In our case, this happens by dividing the packs S_j into two sets T_1 and T_2 of similar size and searching for a collision in an appropriate way. For example, in the "powers of primes" situation, one could look for exponents $k_{j,i}$ such that

$$\prod_{j\in T_1}\prod_{i=1}^{b} v_{j,i}^{k_{j,i}} = c\cdot \prod_{j\in T_2}\prod_{i=1}^{b} v_{j,i}^{-k_{j,i}}.$$

To prevent this, the size of the message space should be chosen to be at least twice the desired security level.

Furthermore, since $2 \mid q^d - 1$ for odd q, it is possible to find the parity of the number of factors $v_{j,i}$ in a ciphertext c that are quadratic nonresidues in $\mathbb{F}_q[x]/(g(x))$ by simply checking whether c itself is a quadratic residue. This is only a small information leakage, but nonetheless it should be avoided by encoding messages in such a way that this parity is always the same. A similar attack can be applied for other small factors of $q^d - 1$, so it should be chosen to have few such factors.

Acknowledgments The authors were supported by Swiss National Science Foundation grant number 149716 and *Armasuisse*

References

1. Barbulescu R, Gaudry P, Joux A, Thomé E (2014) A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic. In: Advances in Cryptology-Eurocrypt 2014. Springer, pp 1–16
2. Chevallier-Mames B, Naccache D, Stern J (2008) Linear bandwidth naccache-stern encryption. In: Security and Cryptography for Networks. Springer, pp 327–339
3. Micheli G, Schiavina M (2014) A general construction for monoid-based knapsack protocols. Adv Math Commun 8(3)
4. Naccache D, Stern J (1997) A new public-key cryptosystem. In: Advances in Cryptology, EUROCRYPT. pp 27–36
5. Stanton D, White D (1986) Constructive combinatorics. Springer, New York
6. Stein W, et al. (2014) Sage mathematics software (version 6.1.1). The Sage Development Team, http://www.sagemath.org

Chapter 12
Implementation and Improvement of the Partial Sum Attack on 6-Round AES

Francesco Aldà, Riccardo Aragona, Lorenzo Nicolodi and Massimiliano Sala

Abstract The Partial Sum Attack is one of the most powerful attacks, independent of the key schedule, developed in the last 15 years against reduced-round versions of AES. In this chapter, we introduce a slight improvement to the basic attack which lowers the number of chosen plaintexts needed to successfully mount it. Our version of the attack on 6-round AES can be carried out completely in practice, as we demonstrate providing a full implementation. We also detail the structure of our implementation, showing the performances we achieve.

12.1 Introduction

The research on the cryptanalysis of block ciphers partly deals with studying and proposing attacks on their reduced-round versions. Results on reduced versions are very interesting, since they help to better understand the behavior of a cipher, pointing out weaknesses in its structure which can eventually lead to attacks on the full version or characterize the security margin of the cipher.

In 2000, Ferguson et al. [5] introduced one of the most effective attacks, independent of the key schedule, developed in the last 15 years against reduced-round

F. Aldà (✉)
Horst Görtz Institute for IT Security and Faculty of Mathematics,
Ruhr-Universität Bochum, Universitätsstraße 150, 44801 Bochum, Germany
e-mail: francesco.alda@rub.de

R. Aragona · M. Sala
Department of Mathematics, University of Trento, Via Sommarive 14,
38123 Povo, Trento, TN, Italy
e-mail: riccardo.aragona@unitn.it

M. Sala
e-mail: maxsalacodes@gmail.com

L. Nicolodi
Independent Researcher, Lavis, TN, Italy
e-mail: lo@hidden-bits.com

M. Baldi and S. Tomasin (eds.), *Physical and Data-Link Security Techniques for Future Communication Systems*, Lecture Notes in Electrical Engineering 358, DOI 10.1007/978-3-319-23609-4_12

versions of the Advanced Encryption Standard [3, 4], the *Partial Sum Attack*. Specifically, they developed attacks against AES reduced to 6, 7 and 8 rounds. The attack on 6-round is particularly powerful and its complexity is in the range which is referred to as practicable in the literature. It improves a previous attack which was first described in [3]. The latter is based on *integral cryptanalysis*, a general technique which is applicable to a large class of SPN block ciphers. This technique was originally designed by Lars Knudsen in the paper presenting the block cipher Square [2], as a specific attack against its byte-oriented structure. This is the reason why this class of attacks is commonly known as *Square Attack*. Since AES inherits many properties from Square, this attack can be easily extended to reduced-round versions of the Advanced Encryption Standard.

In this chapter, we introduce a slight theoretical improvement to the Partial Sum Attack on 6-round AES which lowers the number of chosen plaintexts needed to successfully mount it, and we describe the structure of our full implementation. After examining the literature which was developed after the publication of [5], we are not aware of any effective implementation of this attack. Therefore, we strongly believe that our implementation is the very first and, mostly, we show that it is completely practicable. Moreover, we believe that our effort allows a deeper understanding of the attack workflow and can point out some other weaknesses neither discovered nor exploited so far.

We would like to underline that a remark similar to the observation which our improvement is based on can be found in [12], although we achieved this result independently. Nevertheless, we believe that our analysis is more careful and detailed. In fact, the hypotheses which lead to this theoretical result are inherently strong, since they require the reduced-round cipher to "behave" like a random permutation. However, the attack we are dealing with strongly exploits the fact that AES can be easily distinguished from a random permutation. Therefore, it was not clear *a priori* whether these properties, or a good approximation of them, were actually satisfied in a real scenario. Thanks to our implementation which exploits the aforementioned improvement, we investigated these assumptions and explored how well the theoretical model describes an actual execution of the attack. In particular, the experimental results show that the number of false positives obtained closely matches that which was expected from the theoretical analysis. For a detailed explanation, we refer to Sect. 12.3.2.

The rest of the chapter is organized as follows: in Sect. 12.2, we briefly introduce the Square Attack and its extensions and we subsequently describe the Partial Sum Attack in detail. In Sect. 12.3, we present our main results. First, we explain our slight theoretical improvement, pointing out the issues that its implementation involves. We then detail our implementation and provide the results of our computations. In particular, we achieved to recover a full 6-round key in less than 12 days with 25 cores.

12.2 Preliminaries

We recall that the encryption process of AES-128, -192 and -256 consists of an initial key addition followed by the application of 10, 12 and 14 round transformations, respectively. The initial key addition and every round transformation take as input an intermediate result, called the *state*, and a round key which is derived from the cipher key through the key schedule. The state is always treated as a 4×4 matrix whose coefficients belong to $\mathbb{F}_{2^8}$. The output of any round is another state. The round transformation is a sequence of four processing steps: *SubBytes*, *ShiftRows*, *MixColumns* and *AddRoundKey*. The *SubBytes* (*SB*) step is the only non-linear transformation of the cipher. It is an invertible byte substitution that operates independently on each byte of the state, according to an S-box. The S-box, which is henceforth indicated as γ, consists of the multiplicative patched inversion over $\mathbb{F}_{2^8}$, followed by an invertible affine transformation. The *ShiftRows* (*SR*) step is a byte transposition that cyclically shifts the rows of the state over different offsets. Specifically, let $s_{i,j}$ and $s'_{i,j}$ be the state bytes in position (i, j) before and after the *ShiftRows* transformation, respectively. Then $s'_{i,j} = s_{i,(j+i) \bmod 4}$ for $i, j \in \{0, 1, 2, 3\}$. The *MixColumns* (*MC*) step is a linear transformation which operates on the state column-by-column, treating each column as a polynomial over $\mathbb{F}_{2^8}[x]$. This polynomial is then multiplied modulo $x^4 + 1$ with the fixed polynomial $m(x) = (\alpha + 1)x^3 + x^2 + x + \alpha$, where $\alpha \in \mathbb{F}_{2^8}$ is such that $\alpha^8 = \alpha^4 + \alpha^3 + \alpha + 1$. Finally, in the *AddRoundKey* (*ARK*) transformation, the state is bitwise XORed with the corresponding round key. By *SubBytes*$^{-1}$, *ShiftRows*$^{-1}$, *MixColumns*$^{-1}$ and *AddRoundKey*$^{-1}$, we denote the inverses of the aforementioned steps. The final round differs from the others since the *MixColumns* step is removed. For further details on the structure of AES, we refer to [3, 4].

In the following sections, we first give an overview on the Square Attack on 4-round AES and we briefly introduce its extensions. We then describe the Partial Sum Attack in detail.

12.2.1 Square Attack

The Square Attack is a chosen plaintext attack, which is independent of the specific choices of the S-box of the *SubBytes* function, the multiplication polynomial of the *MixColumns* transformation and the key schedule. For the sake of clarity, however, we will often refer to the specific parameters used in AES.

In order to explain how this attack can be performed, we first introduce the following definition.

Definition 12.1 A Δ-set is a set of 256 AES states that differ in one of the state bytes (called *active* byte) and are equal in the other state bytes (called *passive* bytes). In other words, if U is a Δ-set, for every $x, y \in U$ we have

$$\begin{cases} x_{i,j} \neq y_{i,j} & \text{if } (i,j) \text{ is active} \\ x_{i,j} = y_{i,j} & \text{if } (i,j) \text{ is passive} \end{cases}$$

where $i, j \in \{0, 1, 2, 3\}$.

As it is explained in [4], the Square Attack on 4-round AES is heavily based on the following property.

Proposition 12.1 *Let $b_{i,j}^{(l)}$ be the byte in position (i, j), $i, j \in \{0, 1, 2, 3\}$, of the lth state of a Δ-set after three rounds. Then*

$$\sum_{l=1}^{256} b_{i,j}^{(l)} = 0. \tag{12.1}$$

In other words, the states at the end of the third round are *balanced*, i.e. all bytes at the input of the fourth round sum to zero. Note that the initial key addition is implicitly assumed and not counted in the number of rounds.

Let us consider a 4-round reduced AES, in which the fourth round is a final round, i.e. it does not include *MixColumns*. This implies that every byte of the ciphertext only depends on one byte of the input of the fourth round. The Square Attack on 4-round AES can then be mounted as follows. For any lth state of a Δ-set, $1 \leq l \leq 256$, let $c_{i,j}^{(l)}$, where $i, j \in \{0, 1, 2, 3\}$, be the ciphertext byte in position (i, j). Let $k_{i,j}^{(4)}$ be a guess for the byte in position (i, j) of the 4th round key (which is the last key used). For any (i, j), if the value of $k_{i,j}^{(4)}$ is correct, the following equation holds:

$$\sum_{l=1}^{256} \gamma^{-1}\left(c_{i,j}^{(l)} + k_{i,j}^{(4)}\right) = \sum_{l=1}^{256} b_{i,(j+i) \bmod 4}^{(l)} = 0, \tag{12.2}$$

where $b_{i,j}^{(l)}$ is the byte in position (i, j) of the lth state of a Δ-set after the application of three rounds, and γ^{-1} is the S-box of *SubBytes*$^{-1}$.

If Eq. (12.2) does not hold, the assumed value for the key byte must be wrong. This check is expected to eliminate all wrong key bytes, except for one value that could satisfy (12.2) by chance. To be more precise, the following result holds.

Proposition 12.2 *If $(X^{(l)})_{1 \leq l \leq 256}$ is a sequence of independent uniformly distributed random variables with values in $\mathbb{F}_{2^8}$, then the probability*

$$\mathbb{P}\left[\sum_{l=1}^{256} X^{(l)} = 0\right] = 2^{-8}.$$

Proof Let X and Y be two discrete independent random variables, with density functions $f_1(x)$ and $f_2(x)$ respectively. The convolution $f_3(x) = [f_1 * f_2](x) = \sum_y f_1(y) f_2(x - y)$ is the density function of the random variable $Z = X + Y$. Since X

Table 12.1 Estimated probability to obtain a zero sum for a random set of plaintexts and for a Δ-set at the end of the 3rd round

Random set	Δ-set
0.003904	0.007794

Number of trials: $2 \cdot 10^4$

and Y take values in $\mathbb{F}_{2^8}$, their sum Z takes values in $\mathbb{F}_{2^8}$ too. Therefore, the density function of Z is an uniformly distributed random variable, since it is the circular convolution of two independent uniformly distributed random variables. This result can be easily extended to the sum of an arbitrary number of random variables. □

Before proceeding with the analysis of the attack, we would like to stress that the hypotheses of Proposition 12.2 are inherently strong. In particular, the bytes of the state at the end of the 3rd round are assumed to be independent and uniformly distributed. Although these are natural assumptions for modeling the attack, it is not clear a priori whether they hold even in practice. We thus performed some tests which aimed to estimate the probability to obtain a zero sum for a random set of 256 plaintexts and for a Δ-set at the end of the 3rd round. The values reported in Table 12.1 were obtained by averaging the estimates we collected using $2 \cdot 10^4$ random sets and $2 \cdot 10^4$ different Δ-sets, encrypted through an equal number of random keys, respectively.

As Table 12.1 shows, the tests we performed give evidence that Proposition 12.2 well describes the behavior of the cipher even at the end of the 3rd round. As expected, for a random set of 256 plaintexts there exists (on average) only one value which satisfies Eq. (12.2) by chance. In the case of a Δ-set, the estimate is roughly $1/128$, since both the correct key byte and another random value satisfy (12.2).

Since checking Eq. (12.2) for a single Δ-set is expected to leave only 1 over 256 of the wrong key assumptions as a possible candidate, the 4th round key can be found with a sufficiently large confidence using two different Δ-sets. Henceforth, this crosscheck will be referred to as *verification step*.

All in all, two Δ-sets have to be used, and all 16 bytes of the 4th round key need to be recovered. Therefore, the working factor consists of 2^9 encryptions and $2^9 \cdot 2^4 = 2^{13}$ evaluations of Eq. (12.2).

In [4], Daemen et al. describe how this attack can be extended adding one round at the end or one round at the beginning. Combining the basic attack on 4 rounds with both extensions yields the Square Attack on 6-round AES. We can sketch this attack as follows. For the extension by one round at the end, the attacker has to perform a partial decryption of two rounds instead of only one, implying that four more bytes of the final round key need to be guessed. The idea for the extension by one round at the beginning consists of choosing a set of 256 plaintexts which, at the end of the first round, results in a Δ-set with a single active byte. This requires to guess four bytes of the initial round key $k^{(0)}$. We refer to [4] for further details on these two extensions. In both cases, we need to guess five key bytes instead of one. By combining these two methods, nine bytes need to be guessed.

12.2.2 Partial Sum Attack

Without considering the verification steps, the Square Attack on 6-round AES requires the storage of 2^{32} chosen plaintexts and the corresponding ciphertexts. Moreover, $(2^8)^9 = 2^{72}$ steps are needed for guessing nine key bytes, when it is applied to only recover 4 bytes of the 6th round key. Therefore, it is completely out of reach for current computing resources.

The Partial Sum Attack [5] significantly improves the Square Attack on 6-round AES. Ferguson et al. introduced two main ideas. First, instead of guessing four bytes of the initial round key $k^{(0)}$, one can use 2^{32} plaintexts such that one column of the states at the input of *MixColumns* of the first round ranges over all possible values of $(\mathbb{F}_{2^8})^4$ and all other bytes are constant. Throughout the rest of the chapter, we denote by $\bar{\Delta}$-set such a group of 2^{32} plaintexts. For any value of the initial round key, the corresponding ciphertexts consist of 2^{24} groups of 2^8 encryptions that vary in a single active byte at the end of the first round. In fact, imposing a particular linear combination which ranges over all possible values of $\mathbb{F}_{2^8}$ and three other linear combinations which are constant for all 256 states, we can uniquely determine a set of plaintexts which results in a Δ-set with a single active byte at the end of the first round. In particular, one has 2^{24} ways to choose the values for these three linear combinations.

Therefore, all an attacker has to do is guess four bytes of the 6th round key and one byte of the 5th round key, perform a partial decryption to a single state byte at the end of the 4th round, sum this value over all 2^{32} encryptions, and check whether the result is zero. Compared to the Square Attack on 6 rounds, the attacker needs to guess 40 bits instead of 72.

The further idea behind the improvement introduced by Ferguson et al. consists in organizing the partial decryption on *partial sums*. In order to properly understand what *partial sums* are and how one can use them, we introduce the following notation, where the pair (i, j) is used to denote the state entry (with $i, j \in \{0, 1, 2, 3\}$), and the index l (with $1 \leq l \leq 2^{32}$) denotes the lth element of a $\bar{\Delta}$-set:

$b_{i,j}^{(l)}$ is a byte at the end of the 4th round;

$a_{i,j}^{(l)}$ is a byte of the state at the 5th round before the application of *MixColumns*;

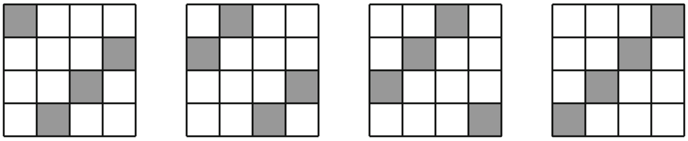
$a_s^{(l)}$ is the sth column of the lth state at the 5th round before the application of *MixColumns*. Thus $a_j^{(l)} = \left(a_{0,j}^{(l)}, a_{1,j}^{(l)}, a_{2,j}^{(l)}, a_{3,j}^{(l)}\right)^\top$;

$c_{i,j}^{(l)}$ is a byte at the end of the 6th round, which we refer to as the ciphertext byte;

$k^{(h)}$ is the hth round key and $\bar{k}^{(h)} = \mathit{MixColumns}^{-1}(k^{(h)})$;

$\bar{k}_{i,j}^{(h)}$ is a byte of $\bar{k}^{(h)}$.

It is easy to show that, in order to compute the partial decryption to a state byte at the end of the 4th round, we need to consider four bytes in each ciphertext and guess the corresponding bytes of the 6th round key, according to one of the configurations shown in Fig. 12.1. Observe that each configuration has exactly one byte per state row and one byte per state column.



1 st set config. 2nd set config. 3rd set config. 4th set config.

Fig. 12.1 The set of 4 bytes of the 6th round key (resp. ciphertexts) for the Partial Sum Attack on 6-round AES

In the following computations, with abuse of notation, we denote by *MixColumns*$^{-1}$ and *SubBytes*$^{-1}$ the inverse of *MixColumns* and *SubBytes* applied to a single column of the state. The relations between the $a^{(l)}$'s, the $c^{(l)}$'s and the $k^{(h)}$'s are easily established:

$$a_j^{(l)} = \begin{bmatrix} a_{0,j}^{(l)} \\ a_{1,j}^{(l)} \\ a_{2,j}^{(l)} \\ a_{3,j}^{(l)} \end{bmatrix} = \mathit{MixColumns}^{-1}\left(\mathit{SubBytes}^{-1}\begin{pmatrix} c_{0,j}^{(l)} + k_{0,j}^{(6)} \\ c_{1,(j-1) \bmod 4}^{(l)} + k_{1,(j-1) \bmod 4}^{(6)} \\ c_{2,(j-2) \bmod 4}^{(l)} + k_{2,(j-2) \bmod 4}^{(6)} \\ c_{3,(j-3) \bmod 4}^{(l)} + k_{3,(j-3) \bmod 4}^{(6)} \end{pmatrix}\right),$$

where $j \in \{0, 1, 2, 3\}$. When j is understood, we will remove it; for example we denote

$$\xi^{(l)} = \begin{bmatrix} \xi_0^{(l)} \\ \xi_1^{(l)} \\ \xi_2^{(l)} \\ \xi_3^{(l)} \end{bmatrix} := \mathit{SubBytes}^{-1}\begin{pmatrix} c_{0,j}^{(l)} + k_{0,j}^{(6)} \\ c_{1,(j-1) \bmod 4}^{(l)} + k_{1,(j-1) \bmod 4}^{(6)} \\ c_{2,(j-2) \bmod 4}^{(l)} + k_{2,(j-2) \bmod 4}^{(6)} \\ c_{3,(j-3) \bmod 4}^{(l)} + k_{3,(j-3) \bmod 4}^{(6)} \end{pmatrix},$$

for $1 \leq l \leq 2^{32}$. Let N be the byte matrix of *MixColumns*$^{-1}$. Working out the product, we have

$$a_j^{(l)} = \begin{bmatrix} N_0 \cdot \xi_0^{(l)} + N_1 \cdot \xi_1^{(l)} + N_2 \cdot \xi_2^{(l)} + N_3 \cdot \xi_3^{(l)} \\ N_3 \cdot \xi_0^{(l)} + N_0 \cdot \xi_1^{(l)} + N_1 \cdot \xi_2^{(l)} + N_2 \cdot \xi_3^{(l)} \\ N_2 \cdot \xi_0^{(l)} + N_3 \cdot \xi_1^{(l)} + N_0 \cdot \xi_2^{(l)} + N_1 \cdot \xi_3^{(l)} \\ N_1 \cdot \xi_0^{(l)} + N_2 \cdot \xi_1^{(l)} + N_3 \cdot \xi_2^{(l)} + N_0 \cdot \xi_3^{(l)} \end{bmatrix},$$

where, in the specific case of AES (see Sect. 12.2),

$$\begin{aligned} N_0 &= \alpha^3 + \alpha^2 + \alpha \\ N_1 &= \alpha^3 + \alpha + 1 \\ N_2 &= \alpha^3 + \alpha^2 + 1 \\ N_3 &= \alpha^3 + 1. \end{aligned}$$

Thus we can compute a state byte at the end of the 4th round as follows:

$$b^{(l)}_{i,(j+i) \bmod 4} = \gamma^{-1}\left(a^{(l)}_{i,j} + \bar{k}^{(5)}_{i,j}\right), \tag{12.3}$$

where $i \in \{0, 1, 2, 3\}$ and γ^{-1} is the S-box of *SubBytes*$^{-1}$, as usual. Observe that in (12.3) γ^{-1} is applied to $a^{(l)}_{i,j} + \bar{k}^{(5)}_{i,j}$ rather than to $a^{(l)}_{i,j} + k^{(5)}_{i,j}$. The latter would be wrong, since $k^{(5)}_{i,j}$ is added *after* the application of *MixColumns*.

In order to identify a possible right guess, we have to check if $\sum_{l=1}^{2^{32}} b^{(l)}_{i,(j+i) \bmod 4} = 0$. This sum can be expressed as

$$\sum_{l=1}^{2^{32}} \gamma^{-1}\left(N_{-i} \cdot \xi^{(l)}_0 + N_{1-i} \cdot \xi^{(l)}_1 + N_{2-i} \cdot \xi^{(l)}_2 + N_{3-i} \cdot \xi^{(l)}_3 + \bar{k}^{(5)}_{i,j}\right), \tag{12.4}$$

where the indices $-i$, $1-i$, $2-i$, $3-i$ are all meant to be reduced modulo 4, giving a remainder in $\{0, 1, 2, 3\}$.

If we trivially execute this summation, given 2^{32} ciphertexts and 2^{40} possible key guesses, we have to sum 2^{72} different values, which does not significantly improve the basic Square Attack. As it is pointed out in [5], Expression (12.4) can be organized in a more efficient manner. Once the row i is fixed, for each $t \in \{0, 1, 2, 3\}$, it is possible to associate a partial sum $x^{(l)}_t$ to each set $\{\xi^{(l)}_0, \dots, \xi^{(l)}_t\}$, defined as follows:

$$x^{(l)}_t := \sum_{z=0}^{t} N_{z-i} \cdot \xi^{(l)}_z.$$

In particular,

$$x^{(l)}_2 = x^{(l)}_1 + N_{2-i}\xi^{(l)}_2 \text{ and } x^{(l)}_3 = x^{(l)}_2 + N_{3-i}\xi^{(l)}_3.$$

In order to simplify the notation, let $(c^{(l)}_0, c^{(l)}_1, c^{(l)}_2, c^{(l)}_3)$ be the 4-tuple formed by the lth ciphertext's bytes, extracted according to one of the configurations described above. Guessing the key values and using the partial sums, we can define the following maps

$$(c^{(l)}_0, c^{(l)}_1, c^{(l)}_2, c^{(l)}_3) \longmapsto (x^{(l)}_1, c^{(l)}_2, c^{(l)}_3) \longmapsto (x^{(l)}_2, c^{(l)}_3) \longmapsto x^{(l)}_3.$$

Using a similar notation, let (k_0, k_1, k_2, k_3) be four values for the 6th round key, which we want to guess, arranged in the same configuration chosen for the ciphertexts, and let k_4 be a guess for the 5th round key byte $\bar{k}^{(5)}_{i,j}$. The Partial Sum Attack is organized as follows.

- We start with the list of 2^{32} 4-tuples $(c_0^{(l)}, c_1^{(l)}, c_2^{(l)}, c_3^{(l)})$. Guessing k_0 and k_1, we can compute each triple $(x_1^{(l)}, c_2^{(l)}, c_3^{(l)})$.
- We then guess k_2, and compute each pair $(x_2^{(l)}, c_3^{(l)})$.
- Similarly, we guess k_3, and compute each value of $x_3^{(l)}$.
- Finally, guessing the value of k_4, we can compute Expression (12.4) and check whether the result is zero.

12.2.3 Complexity

In the first phase one guesses 2 bytes and processes 2^{32} ciphertexts bytes. For each choice of k_0 and k_1, one more byte has to be guessed, but only 2^{24} triples have to be processed. In the third phase, k_3 has to be guessed but one has only to process 2^{16} pairs. This holds similarly for the other two phases. Summing up all the contributions, we obtain that 2^{50} operations are required for a single $\bar{\Delta}$-set of 2^{32} elements.

12.3 Implementation and Improvement

The results described in this work started from Aldà's Master's thesis [1], where he developed a C++ code of the Partial Sum Attack and introduced (independently of [12]) the improvement specified in Sect. 12.3.2.

12.3.1 High-Level Scheme of the Implementation

To the best of our knowledge, this is the very first implementation of the Partial Sum Attack on 6-round AES. In this section, we explain the main ideas and principles we used in our implementation. We refer to Sect. 12.3.3 for further technical details on our implementation.

As it is displayed in Fig. 12.2, the steps involved in the attack are very simple. At the beginning of the attack, a $\bar{\Delta}$-set with 2^{32} elements has to be encrypted. In this way, we can obtain and store the 4-tuples $(c_0^{(l)}, c_1^{(l)}, c_2^{(l)}, c_3^{(l)})$, formed by the lth ciphertext's bytes, extracted according to one of the configurations described in Sect. 12.2.2. Extending the idea introduced in [5], it is sufficient to count how often each 4-tuple appears during the computation. As there are only 2^{32} possible 4-tuples, we do not have to store all $(c_0^{(l)}, c_1^{(l)}, c_2^{(l)}, c_3^{(l)})$ values. Since Expression (12.4) has to be computed in a field of characteristic 2, it suffices to count modulo 2. In fact, only the summands which appear an odd number of times give a non-zero contribution. Hence, a single bit suffices for each count and it is possible to store our list of 4-tuples

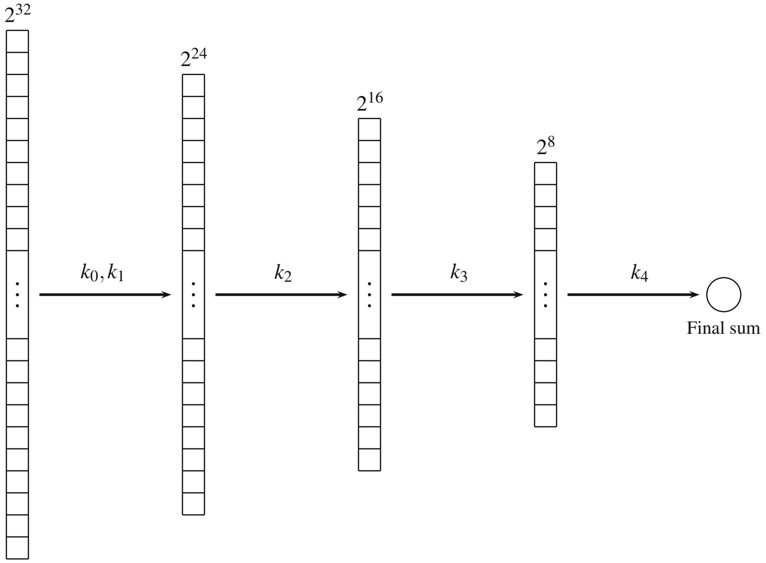


Fig. 12.2 The workflow of the Partial Sum Attack

in a 2^{32}-bit vector. Therefore, the space requirement for 2^{32} counters is just 2^{32} bits, which correspond to 0.5GB.

We then start a loop over 2^{16} possible values of k_0, k_1. For each pair (k_0, k_1), we compute the partial sums $x_1^{(l)}$ and store the triples $(x_1^{(l)}, c_2^{(l)}, c_3^{(l)})$. Using the same rationale, it suffices to count the parity of times each triple occurs. Again, we store all parities in a 2^{24}-bit vector. Moreover, we observe that, using an appropriate sorting, it suffices to compute the value $x_1^{(l)}$ every 2^{16} elements: in fact, this value only depends on $c_0^{(l)}, c_1^{(l)}, k_0$ and k_1. Thus, if $1 \leq l, h \leq 2^{32}$, we have

$$\begin{cases} c_0^{(l)} = c_0^{(h)} \\ c_1^{(l)} = c_1^{(h)} \end{cases} \Longrightarrow x_1^{(l)} = x_1^{(h)}.$$

This observation significantly reduces the number of computations involved in this step, allowing entire blocks of bits to be updated at the price of very few calculations (see Sect. 12.3.3 for further details).

The same ideas can be similarly applied to the second step. For each value k_2, one computes the partial sums $x_2^{(l)}$, counts the parity of times each pair $(x_2^{(l)}, c_3^{(l)})$ occurs and stores it in a 2^{16}-bit vector. As before, it suffices to compute the value $x_2^{(l)}$ every 2^8 elements: in fact, this value only depends on $x_1^{(l)}, c_2^{(l)}$ and k_2.

In the third step, for each value k_3, we compute the partial sums $x_3^{(l)}$, count how many times each $x_3^{(l)}$ occurs and store its parity in a 2^8-bit vector. Unlike the previous steps, this must be done scanning every entry of the 2^{16}-bit vector, since both $x_2^{(l)}$ and $c_3^{(l)}$ must be used in the computation of $x_3^{(l)}$. Finally, looping over the value k_4, it is possible to compute the final sum and check whether the result is zero.

As it was explained for the Square Attack, checking this sum for a single $\bar{\Delta}$-set is expected to eliminate 255 of the wrong key assumptions $(k_0, k_1, k_2, k_3, k_4)$. It is therefore necessary to verify their correctness using different $\bar{\Delta}$-sets (*verification steps*). At each positive verification, the key space is reduced by a factor 2^{-8}. Apparently, this implies that 6 different $\bar{\Delta}$-sets (or more) are needed to find the correct 5-tuple $(k_0, k_1, k_2, k_3, k_4)$ with overwhelming probability. This result can be improved, as it is explained in the following section.

12.3.2 Improvement

As it was already underlined, when it was published, the Partial Sum Attack represented one of the best cryptanalytic results on reduced-round versions of the Advanced Encryption Standard. After its publication, many other researchers worked on the integral cryptanalysis of Rijndael (and its specification AES), finding new extensions or improvements for this class of attacks (see for example [7, 9, 12]). Our approach started from performing a full implementation of the attack as it is described in Sect. 12.3.1, trying to understand where some other potentialities could be exploited.

In the original paper [5], it is claimed that at least 6 sets of 2^{32} plaintexts, which form a $\bar{\Delta}$-set, are necessary in order to find the correct 5-tuple $(k_0, k_1, k_2, k_3, k_4)$. However, we observed that only two $\bar{\Delta}$-sets suffices to determine the correct 4-tuple (k_0, k_1, k_2, k_3) with high probability. In fact, fixing one configuration according to which the ciphertexts bytes $(c_0^{(l)}, c_1^{(l)}, c_2^{(l)}, c_3^{(l)})$ are extracted, one can compute the sum in four different state bytes at the end of the 4th round (we can choose $i \in \{0, 1, 2, 3\}$ in Eq. (12.3)). We provide a visual example in Fig. 12.3.

If we consider each sum as independent and make use of Proposition 12.2, using only two $\bar{\Delta}$-sets, the probability that for a 4-tuple (k_0, k_1, k_2, k_3) there exists for each row a value k_4 which gives a zero sum for both $\bar{\Delta}$-sets is $(1/256)^8$. Note that the bytes of the 5th round key, which produce zero sums, may be different for each row, but, as for (k_0, k_1, k_2, k_3), their correctness should follow by the crosschecking between the two $\bar{\Delta}$-sets. Therefore, checking the value of the sum on four rows at the end of the 4th round is expected to determine, with sufficiently high confidence, the correct 4-tuple (k_0, k_1, k_2, k_3). More specifically, only one false positive (k_0, k_1, k_2, k_3) is expected to survive to all verification steps.

The hypothesis which this result is mainly based on consists of considering the sums on four rows as independent. As pointed out in Sect. 12.2.1, there is no certainty that this assumption holds perfectly in practice. Intuitively, even though the bytes involved in the sums belong to the same state and their correlation is hence nonzero, the diffusion and confusion introduced by the round transformations should make

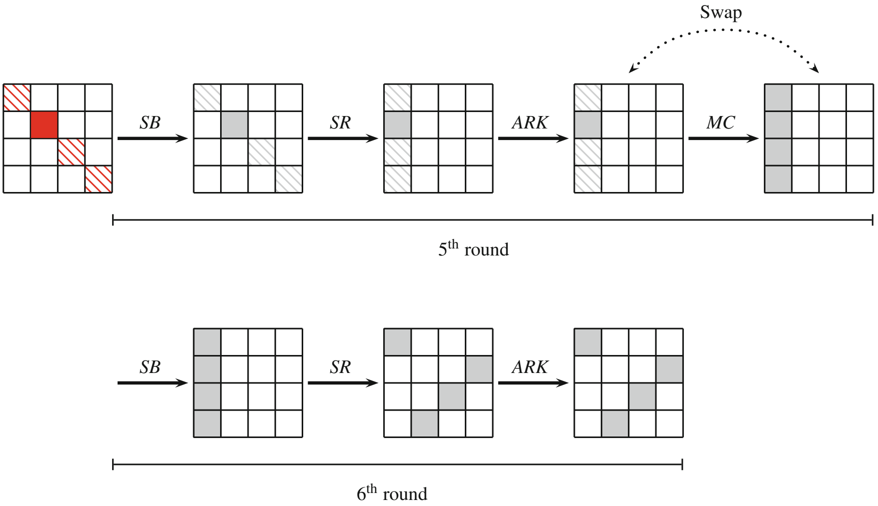


Fig. 12.3 The state bytes at the end of the 4th round (in the *top-left matrix*) which can be computed for a configuration according to which the ciphertexts bytes $(c_0^{(l)}, c_1^{(l)}, c_2^{(l)}, c_3^{(l)})$, for $1 \leq l \leq 2^{32}$, are extracted

it negligible after few rounds. The experimental results we performed using our implementation (which exploits the aforementioned improvement) show that using only two $\bar{\Delta}$-sets and computing the sum on four rows do not eliminate all wrong guesses, as we expected. In particular, besides the correct 4-tuple, we obtained on average one false positive, independently of the configuration chosen. Although more tests are needed in order to provide a better estimate, our results already indicate that the probability of false positive closely matches the expected one. Moreover, we believe that future analyses in this direction could point out further properties of the cipher, which may lead to other improvements of the attack.

All in all, we observed that the number of chosen plaintexts which are necessary in order to mount the attack (with high confidence) can be reduced from 6 $\bar{\Delta}$-sets of 2^{32} elements to only 2. In order to lower the probability of false positives (but still enhancing the basic attack described in [5]), we also performed some attacks using 3 $\bar{\Delta}$-sets, checking the sum on four rows at the end of the 4th round. As expected, in this setting we did not observe any false positive.

Although we reached this conclusion independently, we would like to point out that a remark similar to our observation can be found in [12]. As already observed, we believe that our analysis is more careful and detailed, since we supported the applicability of the hypotheses which this result is based on by means of experimental analyses on AES. Specifically, we provided a full implementation which strongly exploits the aforementioned improvement, and the results we obtained running the attack showed that the number of false positives closely matches the one which was expected from the theoretical analysis.

Among other speed-ups we introduced, this improvement allowed us to achieve optimal performances, showing the complete practicability of the attack, as it will be presented in the following section.

12.3.3 Implementation's Details

First of all, we ported Aldà's code [1] to C, to reduce the overhead of C++ abstractions, which are useful but not essential for this kind of application. During this phase, we decided to map every Boolean vector's element to a bit inside an `unsigned char`'s array. On one hand, this process forced us to create some ancillary functions to toggle and mask bits as necessary but, on the other hand, it had the side effect of accelerating some functions where shifting and masking were required, because we did it byte by byte, instead of bit by bit. Moreover, it allowed us to save space and time while writing and reading the encrypted arrays to and from the disk, storing every 2^{32} array in a 512 MB file and saving time while testing the attack. After completing the porting and introducing the new memory management concepts, we started focusing on how the memory management operations could be accelerated and we ended up managing every group of 8 `unsigned char` array elements as an `unsigned long long int` array, where possible. This allowed us to deal with the allocated memory as a set of 64 bit blocks, reducing the time needed to complete, for example, some `XOR` operations between these arrays. The resulting implementation was satisfactory.

We also decided to allow the parallelization of the attack on multiple core systems and, for this purpose, we needed to exchange information between each process. We chose `OpenMPI` [6, 8] because we appreciated its documentation and the maturity of the open source project supporting it. Porting the code from a linear to a parallel paradigm presented no real difficulties because the attack is mainly composed by loops, repeated for values from 0 to 255, so we decided to execute the 5 most inner loops on each worker (a worker is a parallel process running the attack), assigning to each of them a range of values of k_0 to go through in the outer of these 5 loops. Moreover, we shared the encrypted vectors, using `NFSv4`, on every system running the attack and using the same share storage to save the guessed partial keys and to check the status of the attack from each worker.

Our code works as follows. The master process coordinating the attack distributes the values to each worker using the `Round-Robin algorithm` [11] and then waits for replies from each of them. After finishing the attack with one of the assigned values, every worker reports the result to the master, if successful. If the attack with that value was not successful, the worker checks the shared storage looking if the current partial key has been guessed and, if so, it stops the attack, otherwise it starts the attack with the next assigned value.

To retrieve the whole 16-byte key, the attack has to be run 4 times, according to the four configurations shown in Fig. 12.1. The master writes 4 files that contain the

Table 12.2 Experimental results obtained running our implementation of the Partial Sum Attack on 6-round AES

Number of $\bar{\Delta}$-sets	Average time (days)	Memory (GB)
2	12.1	1.028
3	11.5	1.542

The keys were chosen according to the example vectors provided in [10]

partial keys guessed, and it also writes the whole key in another file when the attack is completed for every configuration.

The final outcome of this effort was interesting in terms of memory and time used. The attacks have been launched on 6 desktop PC, with 4 cores (Intel Pentium CPU G640 @2.80 GHz) and 8 GB of RAM each, using 25 processes. The first process coordinated the attacks, while the remaining 24 workers actually performed the attacks. The results we obtained are summarized in Table 12.2.

From these experimental results, we can note that the attacks which use 3 $\bar{\Delta}$-sets are generally slightly faster, though they obviously require more memory to be performed. This is not too surprising, since using only 2 $\bar{\Delta}$-sets triggers more verification steps on different rows (as observed in Sect. 12.3.2, there are more wrong key candidates which give a zero sum on a fixed row), which are time consuming operations in our current implementation.

Based on the results of Table 12.2, we estimate that, on average, the 128-bit 6th round key can be retrieved in 25.8 h using 256 workers.

The source code of our implementation of the Partial Sum Attack is available on `http://tdsoc.org`.

Acknowledgments Most of the results shown in this work were developed in the first author's Master's thesis and he would like to thank the other authors, especially his supervisor (the last author). For interesting discussions, the authors would like to thank Anna Rimoldi.

References

1. Aldà F (2013) The Partial Sum Attack on 6-round reduced AES: implementation and improvement. Master's thesis (laurea magistrale), University of Trento, Department of Mathematics
2. Daemen J, Knudsen L, Rijmen V (1997) The block cipher SQUARE. Fast software encryption. Springer, Heidelberg, pp 149–165
3. Daemen J, Rijmen V (1998) AES proposal: Rijndael. In: First advanced encryption standard (AES) conference
4. Daemen J, Rijmen V (2002) The design of Rijndael. In: AES—the advanced encryption standard. Information security and cryptography. Springer, Berlin
5. Ferguson N, Kelsey J, Lucks S, Schneier B, Stay M, Wagner D, Whiting D (2001) Improved cryptanalysis of Rijndael. In: Fast software encryption. Springer, Berlin, pp 213–230
6. Gabriel E, Fagg GE, Bosilca G, Angskun T, Dongarra JJ, Squyres JM, Sahay V, Kambadur P, Barrett B, Lumsdaine A, Castain RH, Daniel DJ, Graham RL, Woodall TS (2004) Open MPI: goals, concept, and design of a next generation MPI implementation. LNCS, vol 3241. Springer, Heidelberg, pp 97–104

7. Galice S, Minier M (2008) Improving integral attacks gainst Rijndael-256 up to 9 rounds. In: Progress in cryptology—AFRICACRYPT 2008. Springer, Heidelberg, pp 1–15
8. Graham RL, Woodall TS, Squyres JM (2006) Open MPI: a flexible high performance MPI. LNCS, vol 3911. Springer, Heidelberg, pp 228–239
9. Li YJ, Wu WL (2011) Improved integral attacks on Rijndael. J Inf Sci Eng 27(6):2031–2045
10. Pub NF (2001) 197: advanced encryption standard (AES), vol 197, pp 441–0311
11. Silberschatz A, Galvin PB, Gagne G (2008) Operating system concepts. Wiley, New York
12. Tunstall M (2012) Improved "partial sums"-based square attack on AES. In: International conference on security and cryptography—SECRYPT 2012. INSTICC Press, pp 25–34

Chapter 13
A Real Life Project in Cryptography: Assessment of RSA Keys

Riccardo Aragona, Francesco Gozzini and Massimiliano Sala

Abstract We describe a project carried out by CryptoLabTN. In this project we provide a rigorous analysis of the RSA cryptographic keys employed in the Certification Authority (CA) to certify the keys exchange during some financial transactions. In particular, we consider the asymptotically fastest known factorization algorithm, that is, the General Number Field Sieve (GNFS). We estimate the computational effort required by an attacker to break the certification keys. Our estimate differs from a direct application of the asymptotic estimates,because in a real-life attack several factors have to be vetted.

13.1 Introduction

In order to guarantee secrecy of the data exchange during some financial transactions, the Certification Authority (CA) has the role to issue PKI (Public Key Infrastructure) certificates used for authentications and keys exchange between the terminals. The security of each transaction is enforced through the following procedure:

- generation of RSA keys and request of PKI certificate;
- mutual authentication between the terminals;
- initialization of the channel; and
- keys exchange.

We provide a mathematical evaluation of the optimal length of the RSA keys employed in such CA. The choices about the length of a cryptographic key are

R. Aragona (✉) · F. Gozzini · M. Sala
Department of Mathematics, University of Trento,
via Sommarive 14, 38123 Povo (Trento), Italy
e-mail: riccardo.aragona@unitn.it

F. Gozzini
e-mail: gozzini89@gmail.com

M. Sala
e-mail: maxsalacodes@gmail.com

M. Baldi and S. Tomasin (eds.), *Physical and Data-Link Security Techniques for Future Communication Systems*, Lecture Notes in Electrical Engineering 358, DOI 10.1007/978-3-319-23609-4_13

based on a risk analysis of the possible breaking of the corresponding cryptographic system. The risk is assessed in terms of the total amount of the assets protected by a specific security level. The impact analysis is carried out by modeling a real-world attacker, to provide insights about optimal lengths of RSA moduli for the CA.

We assume that the private key of each actor is sufficiently protected; it follows that the attack scenario is the *public key factorization*. Therefore we conduct an analysis of the best factorization algorithm known in literature, the *General Number Field Sieve (GNFS)* [12].

Starting from an analysis of the runtime of published attacks based on the GNFS, we estimate the computational effort employed by an attacker. Such effort depends on the computing power of attacker. So we estimate

- hardware purchasing power of the attacker in Sect. 13.3.2
- future development of standard microprocessor performances in Sect. 13.3.3
- future development of cryptanalytic capabilities of the attacker in Sect. 13.3.4

Using these parameters we construct an *attacker model*. We notice that the estimates found during our work, using the developed model, are significantly less than those coming from a direct application of classical asymptotic estimates, although obviously the two coincide at infinity.

13.2 RSA Security and Factorization of a Composite Number

The security of the RSA cryptosystem [15] is based on

- computational hardness of the problem of factoring large numbers;
- computational hardness of recovering the plaintext from the ciphertext without knowing the private key.

In [4] Boneh and Venkatesan showed that the factorization can be much more difficult than inverting the RSA encryption function. However, nowadays, apart from special situations, we are not able to invert the RSA encryption function without knowing the factorization of the RSA modulus.

The common idea of the best known attacks on RSA is to factorize the modulus N writing it as difference of squares modulo N: in other words, given a composite integer N, find $x, y \in \mathbb{Z}$ such that

$$x^2 \equiv y^2 \mod N \quad \text{with} \quad x \not\equiv \pm y \mod N.$$

It follows that $\gcd(x - y, N)$ and $\gcd(x + y, N)$ are non-trivial factors of N with probability greater or equal to $\frac{1}{2}$.

The most efficient factoring algorithm based on this idea is the *General Number Field Sieve*.

13.2.1 General Number Field Sieve

The *General Number Field Sieve (GNFS)* is an improvement to the classical *Quadratic Sieve (QS)* [11]. When using QS to factor a large number N, it is necessary to search for smooth numbers (i.e. numbers with small prime factors) in $\mathbb{Z}$. GNFS, on the other hand, manages to search for smooth numbers in the ring of integers, different from $\mathbb{Z}$, of a suitable algebraic number field. Since these numbers have smaller size, they are more likely to be smooth than the numbers inspected in QS. This is the key to the efficiency of GNFS. In order to achieve this speed-up, the GNFS has to perform computations and factorizations in number fields. For this reason, the GNFS algorithm is much more complex than its ancestor QS. For more details about the GNFS algorithm see [2, 12, 13].

GNFS complexity. The estimated complexity of GNFS for factoring an integer N is of the form

$$L_o[n] = e^{(1.9229+o(1))\ln(n)^{1/3}\ln(\ln(n))^{2/3}} \tag{13.1}$$

where $n = \log_2(N)$ and $o(1)$ tends to zero for n tending to infinity. For a proof of (13.1) see [14]. Notice that this is an *asymptotic* estimate.

13.3 The Attacker Model

The strength of an attack on a cryptosystem directly depends on the computational capability of the attacker. With *computational capability* we mean the quantity of elementary operations that the attacker can carry out in a given time interval. The computational capability of an attacker is also established by the quantity of memory at his disposal. However, since the request of memory for this attack is close to $\sqrt{L[n]}$, in the following we only refer to the CPU power as parameter to evaluate the strength of the attack.

In this work we measure the computational capability of a CPU in *Floating-Point Operations Per Second (FLOPS)*. This unit of measure is better suited for the evaluation of an attack on an algebraic cryptosystem since various complex computations over algebraic structures are involved at each step. Moreover the computational capability of a supercomputer is usually estimated in FLOPS. We denote 10^9 FLOPS by *GFLOPS*.

13.3.1 Runtime for GNFS

The heuristic complexity in (13.1) of the GNFS cannot be directly used to estimate the execution time of the algorithm. Since in this work it is necessary to estimate the runtime for a real life attack, we are interested in providing a more precise estimate, at least for short lengths. From (13.1) we have the existence of a number $a \in \mathbb{R}$, $a \geq 0$, and two functions g and h, such that the runtime is

$$a \cdot e^{(1.9229 + g(n)) \ln(n)^{1/3} \ln(\ln(n))^{2/3}} + h(n)$$

with $\lim_{n\to\infty} g(n) = 0$ and $\lim_{n\to\infty} h(n)/[a \cdot e^{(1.9229+g(n)) \ln(n)^{1/3} \ln(\ln(n))^{2/3}}] = 0$.

A direct (not-so-clever) application of (13.1) would be to get the runtime for finite n using $a = 1$, $g = 0$ and $h = 0$. By keeping the assumption $h = 0$ for the n in the range of interest, we have seen that g can be approximated rather well as

$$g(n) = \frac{b}{\ln(n)}$$

where b has to be determined in $\mathbb{R}$, $b \geq 0$. Then the determination of the two constants depends on several factors, including the relationship between runtime expressed as number operations and runtime expressed as FLOPS.

We have thus arrived to the following formula

$$f(n) \doteq a \cdot e^{\left(1.9229 + \frac{b}{\ln(n)}\right) \ln(n)^{1/3} \ln(\ln(n))^{2/3}} \tag{13.2}$$

where parameters a and b are in the ranges

$$10^{-14} \leq a \leq 10^{-12}, \qquad 10 \leq b \leq 100.$$

The output of function (13.2) is the estimated duration in seconds of the factorization performed on a PC with a 2.53 GHz Pentium 4 Northwood processor. We estimate its computational power in about 2GFLOPS [5].

After proper scaling, we verified that the estimate (13.2) agrees with the runtimes of other known factorizations [1, 3, 6, 8].

13.3.2 Hardware Purchasing Power of the Attacker

The duration of an attack depends on the budget that the attacker wants to invest to buy hardware. We consider two scenarios:

- Network of PCs: we follow the approach used by Lenstra and Verheul [9] and we estimate the market price for GFLOPS of hardware currently in commerce, considering the average prices of popular processors on amazon.com;
- Supercomputers: we consider the cost of the most powerful supercomputer in the world at the time of writing, i.e. Tianhe-2 [16].

Comparing the two scenarios, we assume that the attacker buys hardware at the lowest market price and we fix the parameter

$$P \doteq 1.75\,\$/\text{GFLOPS}$$

as estimate of the purchasing power of the attacker. Our analysis was carried out in June 2014.

13.3.3 Future Development of Standard Microprocessor Performances

Since the CA Certificates can be used for years, it is necessary to analyze how the costs estimated in the previous section evolve over time.

We consider a more useful reformulation of Moore's law [10] to estimate the future development of the microprocessor computational power. The reformulation states that *The processing power for computers doubles every 18 months*. Hence we assume that the purchasing power of the attackers increases with time, i.e.

$$P(d) \doteq P \cdot 2^{-\frac{d}{18}} \tag{13.3}$$

where d is the number of months passed since June 2014.

13.3.4 Future Development of Cryptanalytic Capabilities of the Attacker

The last theoretical development of GNFS dates back to 2006 [7] and in general there have been no significant improvements in the last years, both in the algorithm or in its implementations. Anyway, in a pessimistic scenario, we assume that *the cryptanalytic capabilities of an attacker double every 18 months*, starting from June 2014, similar to what predicted by Lenstra and Verheul in 2001 [9].

13.4 Estimate of the Attack Duration

We are ready to provide the formula for the estimate of the runtime of the algorithm GNFS. Let

n be the bits of the RSA modulus to factorize,
d be the months passed since June 2014,

c be the budget (in \$) in hand of the attacker for purchasing an hardware, and
$f(n)$ be the formula (13.2) which estimates the time (in seconds) to factorize an RSA modulus of n bits with a single processor of 2GFLOPS.

We obtain that the time t to factorize an RSA modulus of n bits, spending c dollars and performing the attack d months after June 2014 is estimated to be

$$t = f(n) \cdot \frac{2}{c/P} \cdot 2^{-\frac{d}{18}} = f(n) \cdot \frac{1.75}{c} \cdot 2^{1-\frac{d}{9}}. \tag{13.4}$$

We provide an example. We suppose that an attacker wants to factorize a 1024-bit RSA modulus in May 2015, in other words $d \doteq 11$. We assume that the budget in hand of the attacker for purchasing hardware is $c \doteq 20{,}000\$$. So we estimate the time of factorization in

$$t = f(1024) \cdot \frac{1.75}{20{,}000} \cdot 2^{1-\frac{11}{9}} \approx 3 \cdot 10^9 \text{ seconds},$$

i.e. about 95 years.

13.5 Results and Conclusions

Our analysis provides a non-asymptotic version of the GNFS runtime formula (13.2) that is well suited for estimation of concrete attacks. Moreover, our discussion considers factors as attacker budget, advancement in microprocessor performances and in cryptanalytic techniques. Our final formula (13.4) combines all these factors and provides a real life estimation of GNFS attacks runtimes. Notably, our results suggest that the considered CA keys are chosen with cryptoperiod, i.e. the time period during which a specific cryptographic key is authorized for use, too large with respect to their bit-strength; we advise the CA to either use stronger keys or shorten the cryptoperiod of all the keys that are currently employed in their network.

References

1. Aoki K, Kida Y, Shimoyama T, Ueda H (2004) GNFS factoring statistics of RSA-100, 110,...,150. Technical report, IACR. https://eprint.iacr.org/2004/095.pdf
2. Buhler JP, Jr Lenstra HW, Pomerance C (1993) Factoring integers with the number field sieve. The development of the number field sieve, Lecture notes in mathematics, vol 1554. Springer, Berlin, pp 50–94
3. Bai S, Thomé E, Zimmermann P (2012) Factorisation of RSA-704 with CADO-NFS. Technical report, IACR. https://eprint.iacr.org/2012/369.pdf
4. Boneh D, Venkatesan R (1998) Breaking RSA may not be equivalent to factoring. In Proceedings of EUROCRYPT 98, LNCS, vol 1403. Springer, Berlin, pp. 59–71

5. Dongarra JJ (2013) Performance of various computers using standard linear equations software. Technical report, University of Manchester
6. Danilov SA, Popovyan IA (2010) Factorization of RSA-180. Technical report, IACR. https://eprint.iacr.org/2010/270.pdf
7. Kleinjung T (2006) On polynomial selection for the general number field sieve. Math Comput 75(256):2037–2047
8. Kleinjung T et al. (2010) Factorization of a 768-bit RSA modulus. In Proceedings of CRYPTO 10, LNCS, vol 6223, Springer, pp. 333–350
9. Lenstra AK, Verheul ER (2001) Selecting cryptographic key sizes. J Cryptol 14(4):255–293
10. Moore GE (1965) Cramming more components onto integrated circuits. Electronics 38(8): 114–117
11. Pomerance C (1985) The quadratic sieve factoring algorithm. Advances in cryptology, LNCS, vol 209, Springer, Berlin, pp 169–182
12. Pomerance C (1994) The number field sieve. In mathematics of computation 1943–1993: a half-century of computational mathematics. Proceedings of symposia applied mathematics, vol 48, pp. 465–480. American Mathematics Society
13. Pomerance C (1996) A tale of two sieves. Not Am Math Soc 43(12):1473–1485
14. Pomerance C (1996) Multiplicative independence for random integers. Prog Math 139:703–712
15. Rivest RL, Shamir A, Adleman LM (1978) A method for obtaining digital signatures and public-key cryptosystems. Commun ACM 21(2):120–126
16. Top500 Supercomputer sites http://www.top500.org/system/177999

Chapter 14
Encoding in the DTMF Channel for Two-Channel Authentication

Alessio Meneghetti, Pietro Peterlongo and Massimiliano Sala

Abstract A typical situation of authentication happens when an Internet service needs to verify the identity of a user. The channel used for the communication could be under attack and it is envisaged that a second channel should be employed to thwart this threat. A type of channel which is widely available and that might be suitable for this goal is the DTMF signaling. Telephone lines use Dual-Tone Multi-Frequency signaling (DTMF) to communicate between devices such as a telephone and a server. DTMF uses a sixteen symbols code. The channel presents noise which may produce missing or doubled symbols. Given the extremely limited bandwidth, it is essential to provide some encoding that can protect the exchanged secret from the channel noise. This problem requires the use of Insertion Deletion Codes. In this contribution we describe the problem and our solution, which employs a concatenation of Reed-Solomon codes and Tenengolts codes, that solves it in our particular context, i.e. reduced bandwith with the goal of exchanging a secret for a two-channel authentication protocol.

14.1 Introduction

In a communication when sensitive data are transmitted, one major issue is that of the authentication of the user. For example, we can think of logging on an online bank account, on an e-commerce site where credit card informations are stored, or verify the identity of a chat user.

We can assume that the channel used for sending and receiving data is the same, such as an Internet data connection. This brings a security problem: whatever

A. Meneghetti (✉) · P. Peterlongo · M. Sala
University of Trento, Sommarive, 14, 38123 Trento, Italy
e-mail: alessio.meneghetti@unitn.it

P. Peterlongo
e-mail: pietro.peterlongo@unitn.it

M. Sala
e-mail: massimiliano.sala@unitn.it

M. Baldi and S. Tomasin (eds.), *Physical and Data-Link Security Techniques for Future Communication Systems*, Lecture Notes in Electrical Engineering 358, DOI 10.1007/978-3-319-23609-4_14

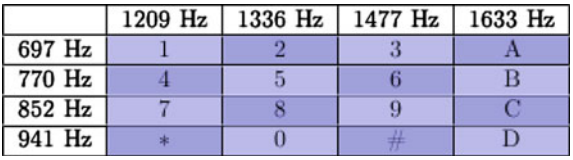
authentication method you have chosen, whether login/password or cryptographic challenge or some unusual approach, if the channel is compromised then your authentication will fail or can be attacked by a man-in-the-middle attack. The only way to overcome this limitation is by using a second communication channel, which is used in conjunction with the first *only* to ensure the authentication. An example which is often encountered is when one logs in to her online bank account, tries to transfer funds to a different IBAN address and an SMS is sent to her phone with an OTP (One-Time Password) to confirm the transaction. In this example the first channel is the Internet and the second channel is the GSM network. In order to be useful, the second channel must be as unrelated as possible from the first channel. Also, the two channels should be accessed using different devices, e.g. a pc and a smartphone, otherwise the compromission of the device will make the use of two channels moot.

While the ubiquity of Internet can be taken for granted, it is not so easy to identify alternative channels that could be used. As said, one obvious could be the GSM network, especially with SMS's. In this chapter we propose to use a channel which is implicit in most telephony protocols, including GSM: the use of the DTMF (Dual-Tone Multi-Frequency). In next section we will describe the DTMF and in subsequent sections we will show how to handle noise in this channel, which is the main difficulty to overcome if we want to use it as a second channel for authentication.

14.2 Introduction to the DTMF Channel

Dual-Tone Multi-Frequency signaling (DTMF) is a communication system capable of encoding and decoding up to 16 symbols [2]. This system is based on the presence of an integrated circuit digital encoder, which generates a standard telephone frequency—the DTMF output—in response to input data.

Modern telephones usually have at least 12 keys keypads, namely the numbers from 0 to 9 and other two symbols generally identified with $*$ and #. A complete 16-keys keyboard also include four more symbols, called A, B, C and D. This set of 16 symbols is thought to be a 4×4 matrix, and the DTMF protocol associates to each row and each column a unique and fixed frequency. Hence, the protocol associates two frequencies to each symbol, and the superposition of the two is the tone that will be sent. In Fig. 14.1 the frequencies associated to the DTMF keyboard are specified.It is worth to remark that the 8 frequencies are specified by the protocol in order to avoid that the sum and difference of two frequencies are not valid frequencies themselves.



	1209 Hz	1336 Hz	1477 Hz	1633 Hz
697 Hz	1	2	3	A
770 Hz	4	5	6	B
852 Hz	7	8	9	C
941 Hz	*	0	#	D

Fig. 14.1 Frequencies associated to the DTMF keypad

All symbols are encoded individually and the resulting tones are sent over the channel separated by a period of silence. A transmitted tone is called *mark*, while the silence between two marks is called *space*. The standard is a mark/space of 40/40, namely both the marks and the spaces last 40 ms. This choice is related to the fact that most of the devices are able to decode with no errors any signal that lasts more than 23 ms. In the same way a silence that lasts more than 20 ms is recognized with no errors.

Due to the properties of the channel, in DTMF we cannot assume the classical Binary Symmetric Channel environment. In particular, defects of the transmission can induce insertions or deletions in the transmitted sequence, while noise can introduce erasures and errors. In addition, insertions, deletions and errors might also be caused by user's mistakes.

We assume here that the quantity of data to be sent is small, namely few bits of information. This allows the utilization of classical coding theory even for correcting insertions and deletions. In fact, few bits can be encoded as a single codeword, hence we are not interested here in the problem of separating two consecutive codewords.

14.3 Edit Distance and Block Codes

In algebraic coding theory the distances between the codewords are strictly related to the ability of correcting errors. For example, in the case of a binary symmetric channel no insertions or deletions can happen, hence when we receive a bitstring we can compute the Hamming distance between the received vector and all the codewords, and it is proved that the optimal decoding consists of finding the codeword that minimizes the Hamming distance.

This approach cannot be used in a channel in which the probabilities of insertions and deletions are non-zero. Assuming an insertion happened during the transmission, the received vector does not necessarily have the same number of components than any codeword, hence we cannot use the Hamming distance.

A generalization of the Hamming distance was introduced by V.I. Levenshtein, which is now known as the Levenshtein distance or edit distance [4]. Given two vectors a and b, not necessarily of the same length, we measure their distance as the minimum number of insertions, deletions and substitutions that are needed to change a into b.

Proposition 14.1 *Consider a code able to recognize and correct up to* $2t$ *insertions or deletions. Then the code can also correct up to* t *errors.*

Proof Each error can be thought as a deletion followed by an insertion. Hence if we can correct an insertion and a deletion, we can also correct an error.

Due to this proposition we could focus on codes able to correct insertions and deletions, then, provided that the correction capability is high enough, we would also be able to correct errors and erasures.

Example 14.1 Let C be a d repetition code, namely each symbol of the message $(m_1, \ldots, m_k)$ is repeated d times, hence the corresponding codeword is

$$(m_1, \ldots, m_1, m_2, \ldots, m_2, \ldots, m_k, \ldots, m_k).$$

Assuming that the number of insertions and deletions is less that $d - 1$, then we can correct safely.

Moreover, if $d \geq 3$, then we can correct with no mistake up to 2 deletions, 2 insertions, or 1 insertion and 1 deletion, and the latter implies that we can correct up to 1 error.

However, we need more sophisticated codes, otherwise the redundacy would be too large.

Let us note that the converse of Proposition 14.1 is not true. Assume for example to have a cyclic code able to correct up to t errors. Then we cannot correct any insertion or deletion. As an example, let us assume to send the codeword (a, b, c, d), and that a deletion occurs in the first symbol during the transmission. The received vector is (b, c, d), but then both the codeword (a, b, c, d) and (b, c, d, a) are at distance 1 from (b, c, d). The following proposition is a consequence of this remark.

Proposition 14.2 *Cyclic codes cannot correct insertions or deletions.*

Proof Consider a pair of codewords c and $\bar{c}$ such that $\bar{c}$ is obtained by shifting c by one position, namely

$$c = (c_0, c_1, \ldots, c_{n-1}), \qquad \bar{c} = (c_1, \ldots, c_n, c_0).$$

If we send c and a deletion happens in the first position of c, then the receiver obtain the vector of $n-1$ elements $y = (c_1, \ldots, c_n)$. Clearly both c and $\bar{c}$ have edit distance 1 from y, hence we cannot safely decode.

14.4 Block Codes for the DTMF Channel

We consider here the problem of correcting a sent message through the DTMF channel, under the following hypothesis:

1. Erasures, errors, deletions and insertions can happen during the transmission.
2. The message has short length.

The second hypothesis can be rephrased as

2. During the transmission a single codeword is sent.

In this work we consider the case in which the number of all possible messages is at most 9^5, due to our physical constraint (see Sect. 14.5). Most of the error correcting codes are designed to solve both the problem of separating the received vectors of symbols into blocks, and the problem of correcting each block. The main procedure for addressing these problems is the usage of two codes, an external code able to identify and separate the vector of symbols into blocks, and an internal code used to correct the errors inside each block. The importance of the second assumption we made is the knowledge that all received symbols belongs to a single codeword, hence we do not need an external code to separate the symbols into blocks.

Many solutions can be applied to this problem, as the utilization of a repetition code, whose properties were already addressed in Example 14.1, or the construction of a code meeting a designed edit distance. However, this can be a challenge, due to the fact that an efficient algorithm (polynomial time) computing the distance distribution of a linear code would solve an NP-hard problem. This challenge can be faced by the implicit construction of a code able to correct a certain number of insertions and deletions. For example we can focus on codes able to correct a single insertion or deletion, ingoring possible errors or erasures. Such codes can be found in [9], and a lot of research has been made following this approach [1, 3, 5, 7]. An advantage of the Tenengolts code is the systematic encoding, which allows efficient encoding and decoding procedures. On the other hand, the assumption that no errors can occur during the transmission is often irrealistic.

Our solution is discussed in Sect. 14.4.2 and employs two concatenated codes, achieving the correction of a single correction or deletion or error or erasure, wherever it occurs, and achieving the correction of two erasures if they happen in the systematic part.

14.4.1 The Tenengolts Encoding Procedure

In this section we present briefly the Tenengolts code, in which the correction of a single insertion or deletion is addressed using a non-binary systematic code with small redundancy.

Let us consider a finite alphabet A containing $q > 2$ elements, identified with the set $\mathbb{Z}_q$, and consider a fixed value k. Each codeword is therefore a sequence $(c_1, c_2, \ldots, c_n)$, to which we associate a binary sequence $(b_1, \ldots, b_n)$ obtained from the formula

$$b_i = \begin{cases} 1 \; i = 1 \\ 1 \; c_i \geq c_{i-1} \\ 0 \; c_i < c_{i-1} \end{cases}$$

Example 14.2 The binary sequence associated to the codeword $(3, 2, 6, 6)$ is $(1, 0, 1, 1)$.

Theorem 14.1 *Consider a set C of sequences $(c_1, \ldots, c_n)$ which, together with the corresponding binary sequences $(b_1, \ldots, b_n)$, solves the system*

$$\begin{cases} \sum_{i=1}^{n} c_i = \beta \quad \mod q \\ \\ \sum_{i=1}^{n} (i-1)\, b_i = \gamma \quad \mod q \end{cases}$$

for some fixed values β and γ. Then C is a code of length n which can correct up to a single insertion or deletion.

Consider now a fixed value k, namely the dimension of the code, and let C be the set of codewords c such that

$$c = (c_1, \ldots, c_k, c_{k+1}, c_{k+2}, c_{k+3}, c_{k+4}, \ldots, c_{k+3+r},)$$

where

- $c_1, \ldots, c_k$ is the message $m_1, \ldots, m_k$.
- $c_{k+1} = c_{k+2} = c_k + 1 \mod q$; these symbols separate the systematic part of the codeword from the redundacy part.
- $c_{k+3} = \sum_{i=1}^{k} c_i \mod q$.
- $(c_{k+4}, \ldots, c_{k+3+r})$ are r symbols obtained from the q-ary representation of the value:

  $$v = \sum_{i=1}^{k} (i-1)b_i \mod q^r,$$

  and $r = \lceil \log_q k \rceil$. This means that

  $$v = \sum_{i=1}^{r} c_{k+3+i} q^{i-1}.$$

The set C is a systematic code

$$(\mathbb{Z}_q)^k \to (\mathbb{Z}_q)^n,$$

where

$$n = k + 3 + r.$$

The decoding procedure can be found in [9].

Remark 14.1 This code, as all codes able to correct one deletion, can also correct one erasure.

14.4.2 A Code for the DTMF Channel

We now address the problem of simultaneously correcting errors, insertions and deletions. Consider the set of possible messages Ω, such that $|\Omega| \leq 9^5$. In this case we can map each message to a distinct element of $(\mathbb{F}_9)^5$. A possible choice for an error correcting code over $\mathbb{F}_9$ is the $[8, 5, 4]$ Reed-Solomon code $\bar{C}$, which can correct up to 1 error.

Proposition 14.3 *Let C be a $[n, k, d]$ Reed-Solomon code. Then a code obtained by puncturing C in any position is a $[n-1, k, d-1]$ code.*

By applying Proposition 14.3 to $\bar{C}$ we obtain a $[7, 5, 3]$ code C' over $\mathbb{F}_9$, hence it can still correct up to a single error.

Proposition 14.4 *Let C be the code obtained by using the encoding procedure described for the Tenengolts code to C'. Then C is a code able to correct a single error, insertion or deletion.*

Proof Suppose that at most one insertion or deletion happens during the transmission. The decoding procedure for the Tenengolts code will give us a sequence $(c_1, \dots, c_7)$ of elements in $\mathbb{F}_9$, which can be decoded using the Reed-Solomon decoding procedure.

We finally recall that the Tenengolts systematic encoding procedure will add to the codewords of C' a redundacy of length $3 + \lceil \log_q n \rceil$. In our case C' is a $[7, 5, 3]$ code, hence $r = 1$. Putting everything together, C is a code over $\mathbb{F}_9$ of length 11 and dimension 5.

14.5 An Application

Given the ubiquity of telephones nowadays, one might think of using the DTMF channel as a secure channel where a shared secret could be sent. Once the two peers have a shared secret, they can use it to establish a secure communication over an insecure channel. For example, the secret could be used to derive a symmetric key for a block cipher or a seed for a stream cipher [6, 8]. Also, the secret could be used in a challenge related to authentication, when one of the peers wants to prove her identity. Of course, there are physical limitations that have to be taken into account in this case. In particular, we cannot assume to be able to send more than 11 tones without interfering with the telephone signalling protocols. It is this application that we have in mind and that forces us to consider no more than 9^5 distinct messages. This limitation forces the security-related applications to use the secret as an ephemeral secret, since a brute force could easily break it.

14.6 Conclusions and Future Developments

The use of the DTMF channel for exchanging authentication tokens is heavily constrained by the small bandwidth and the channel noise. The reliability of the transmission is affected by both defects of the channel and user's mistakes, therefore we need to add redundacy to protect the message from errors, insertions and deletions. While classical coding theory could be applied to protect the sent informations from errors, to address the problem of insertions and deletions we need to rely on particular classes of non-binary codes, which however do not correct errors. Also, in a context of reduced bandwidth we need to add few symbols of redundacy. To solve this problem, in this work we combine the utilization of MDS codes and insertion/deletion codes. The proposed code is obtained by combining a Reed-Solomon code with a Tenengolts code, and is able to correct a single error, insertion or deletion.

We have thus shown that, limited to the use of sharing a short secret for authentication in a two-channel protocol, the DTMF channel may be used effectively.

As regards possible future developments, on the DTMF channel we are limited by its bandwidth but we could construct much longer codes for other channels, achieving the simultaneous correction of many errors/deletions/insertions/erasures. This is ongoing research in our group.

Acknowledgments The first author would like to thank his PHD supervisor: the third author.

References

1. Abdel-Ghaffar KAS, Paluncic F, Ferreira HC, Clarke WA (2012) On Helberg's generalization of the Levenshtein code for multiple deletion/insertion error correction. IEEE Trans Inf Theory 58(3):1804–1808
2. Hayes JC, Tunzi BR (1978) DTMF Communication system. US Patent 4087638
3. Helberg ASJ, Ferreira HC (2002) On multiple insertion/deletion correcting codes. IEEE Trans Inf Theory 48(1):305–308
4. Levenshtein VI (1966) Binary codes capable of correcting deletions, insertions and reversals. Sov Phys Dokl 10
5. Paluncic F, Swart TG, Weber JH, Ferreira HC, Clarke WA (2011) A note on non-binary multiple insertion/deletion correcting codes. Proceedings of the IEEE Information Theory Workshop (ITW) (2011)
6. Schneier B (1996) Applied cryptography: protocols, algorithms, and source code in C. Wiley, New York
7. Sloane NJA (2002) On single-deletion-correcting codes. codes and designs. de Gruyter, Berlin
8. Stinson DR (1995) Cryptography: theory and practice. CRC Press, Boca Raton
9. Tenengolts G (1984) Nonbinary codes, correcting single deletion or insertion. IEEE Trans Inf Theory 30(5):766–769