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.

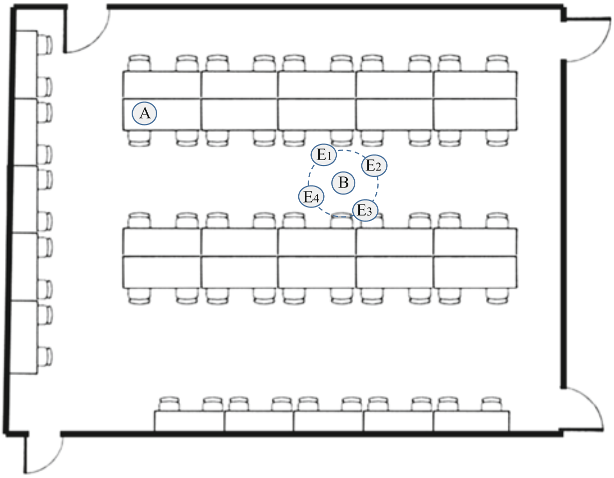

Fig. 7.1 Indoor scenario where the waveforms acquisition experiments were carried out. Alice and Bob were in fixed positions; four different Eve's locations were considered for each Bob-Eve distance

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].

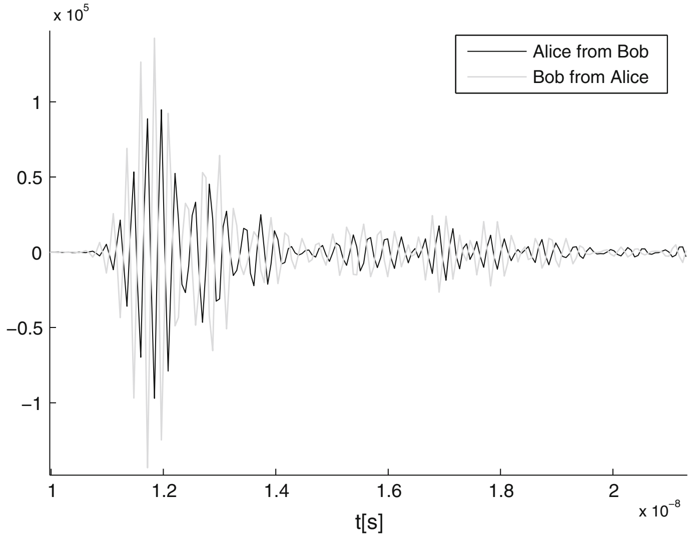

Fig. 7.2 Examples of UWB waveforms acquired by Alice and Bob over some time window having the same amplitude for both users. The two waveforms are approximately equal to each other apart from a shift in the time domain (synchronization error) and from a scaling factor (this latter due to different front-end 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

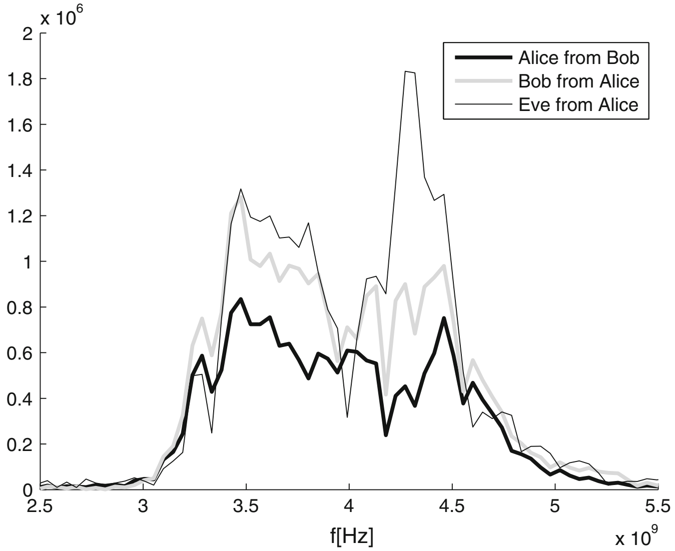

Fig. 7.3 Example of amplitude spectra at Alice, Bob and Eve, with Eve at 20 cm from Bob. Eve's spectrum has bee derived starting from the signal received from Alice

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.

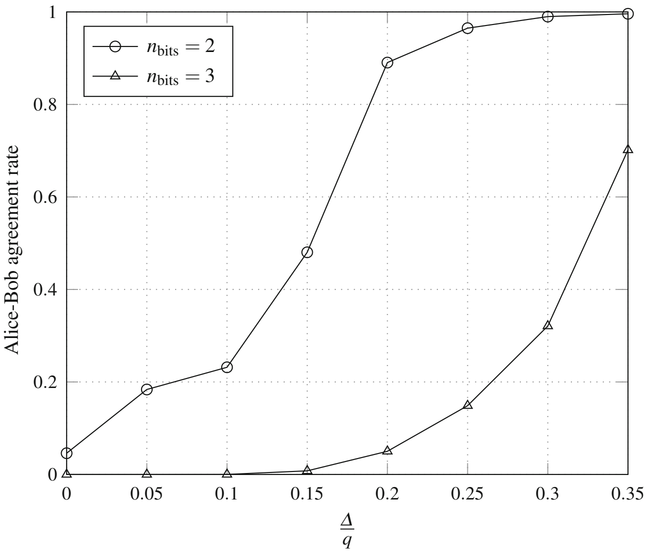

Fig. 7.4 Alice and Bob agreement rate for $d_{\text{Eve}} = 20\,\text{cm}$

- 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

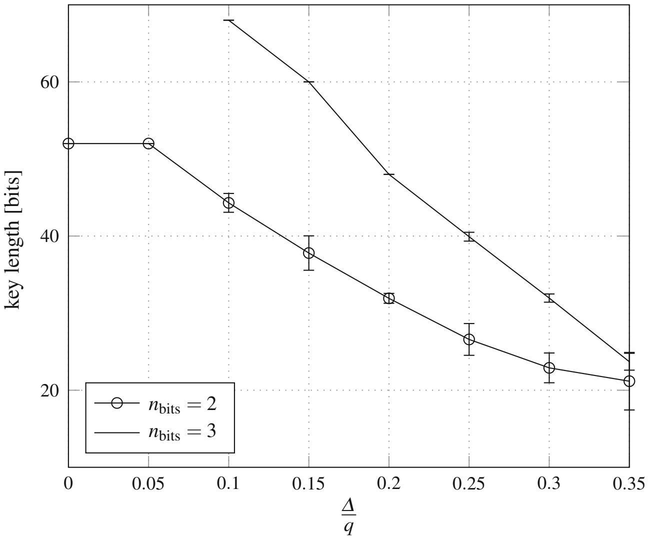

Fig. 7.5 Mean key length and related standard deviation for $d_{\text{Eve}} = 20\,\text{cm}$

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.

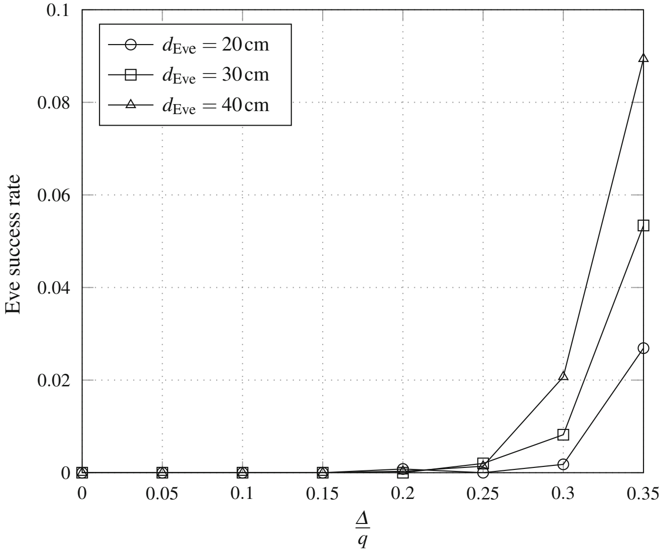

Fig. 7.6 Eve's success rate as a function of $\frac{\Delta}{q}$ and d_{Eve}, $n_{bits} = 2$

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/