Chapter 13
Applications of Quantum Information

Main Acronyms

PTNG	Pseudo-random number generation
QRNG	Quantum random number generation
LCG	Linear congruential generators
QKD	Quantum key distribution
DV–QKD	QKD with discrete variables
CV–QKD	QKD with continuous variables

13.1 Introduction

Besides the problem of reliably transmitting classical information through quantum means, which is the focus of this book, Quantum Information has seen an impressive diversity of applications, ranging from quantum computing to quantum cryptography, and from quantum teleportation to quantum metrology (for an extensive review see [1]). In this chapter we briefly present some examples of application, with the sole purpose of illustrating the many potential uses of Quantum Information.

In fact, the inherent randomness in quantum measurements lends itself to devising methods for the fast automatic generation of *true random numbers* with quantum devices. Similarly, the possibility (granted by Postulate 3) of detecting that some measurement operation has been performed on a single quantum system by employing a different measurement on the same system, has opened the way to *quantum cryptography*. This constitutes an unconditionally secure replacement for the schemes that currently lie at the core of many protocols for securing the transmission and storing of information from a rational attacker. Eventually, we devote a paragraph to the topic of *quantum teleportation*, that is, the transfer of an unknown quantum state between two different locations that is achieved by making use of entanglement and only transmitting classical information.

G. Cariolaro, *Quantum Communications*, Signals and Communication Technology,
DOI 10.1007/978-3-319-15600-2_13

13.2 Quantum Random Number Generation

One of the most striking applications of Quantum Mechanics in the field of Quantum Information is the generation of true random numbers. Random numbers represent a resource in many areas of science and technology. They provide the main ingredient of Monte Carlo methods and cryptographic protocols. In particular, for what concerns the former, whenever it is too difficult to solve a problem analytically, numerical simulations provide the most viable solution.

Regarding cryptographic applications, random numbers are fundamental to the ciphering of information. At the time of writing, most of the random numbers used in the cited fields, are obtained by means of *pseudo-random number generators* (PRNG). The adjective *pseudo* stands for *false* because PRNGs can only mimic the task of a generator, that is, to yield an identical and independent distribution of random variables. PRNGs are indeed nothing more that algorithms recursively executed by computers, which output a number at every operation. Unfortunately, these numbers seem random if one does not know the initial state, the so-called *seed*, of the generator, or if one has not exceeded its *period*, that is, the number of times the algorithm can be run before it goes back to outputting the same numbers. Clearly, when PRNGs are used in cryptography one has to take all the precautions to prevent a possible eavesdropper from predicting the generated number and then getting a copy of the key. In addition, a third problem is related to the way RNG algorithms are often engineered. More in detail, it happens that only after many years of use some widely employed PRNGs reveal dramatic nonrandom features, as was the case for the RAND-U generator, which belongs to the class of Linear Congruential Generators (LCG). In this generator a random number s_n is obtained according to the algorithm $s_n = (65{,}539\, s_{n-1})_{\mathrm{mod}\, 231}$ with the initial state s_0 being an arbitrary seed. The dangerous feature of this generator is that it lacks randomness in a subtle way: indeed, if one maps consecutive triplets $\{s_n, s_{n-1}, s_{n-2}\}$ in 3D space, one can see that the numbers *mainly fall on parallel planes*, as shown in Fig. 13.1.[1] It is then clear that PRNGs not only represent a very weak point in cryptographic protocols but may also be the cause for erroneous results in simulations. Indeed John Von Neumann, one of the fathers of modern Computer Science and one of the first to employ random numbers in simulations, pointed out that *anyone who attempts to generate random numbers by deterministic means is, of course, living in a state of sin.*

Now, we will present two recipes showing how Quantum Mechanics can solve the problem of the generation of random numbers impossible to be forecast in any way.

[1] Citing the paper of Marsaglia [2] the mathematician that was the first to discover this weird behavior.

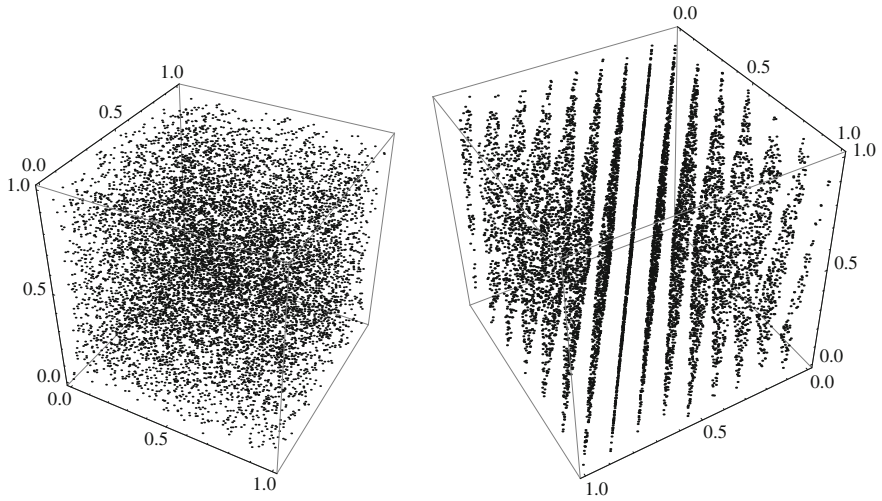

Fig. 13.1 *Left* Triplets of random numbers produced by employing the Linear Congruential Generator RAND-U are mapped in the space. *Right* If the point of sight is conveniently tilted, one can see that the points have the tendency to distribute along planes, a clear mark of lack of spatial uniformity

13.2.1 A Discrete Variable Quantum RNG

A solution to the issue of predictability is given by considering a physical quantum system. The latest step in the technology of random number generation devices is indeed the quantum random number generation (QRNG). The underlying principle of a QRNG is the impossibility of predicting the outcome of a measurement on a quantum system S prepared in a proper state ρ_S. As a simple example to understand how a QRNG works, one can consider a single photon state $|1\rangle$ impinging on a 50:50 beam-splitter. Let us suppose that the photon enters through input arm 1, whereas the unused port 2 carries the vacuum state $|0\rangle$. The overall input state is then given by

$$\psi = |1, 0\rangle_{1,2} = |1\rangle_1 \otimes |0\rangle_2 \tag{13.1}$$

which is equivalent to

$$\psi = a_1^* |0, 0\rangle_{1,2} \tag{13.2}$$

having introduced the field creation operator a_1^* for the mode of input 1. Considering that the beam splitter is modeled as a unitary transformation $U_{\mathrm{b.s}}(\theta)$ on the field operators (see Sects. 9.2.2 and 11.18), one has that in the balanced case the field creation operator transforms according to

$$a_1^* = \frac{1}{\sqrt{2}} \left(\mathrm{i}\, a_1^* + a_4^* \right) \tag{13.3}$$

so that the output state is then given by

$$\psi' = \frac{1}{\sqrt{2}} \left(\mathrm{i}\, |1, 0\rangle_{3,4} + |0, 1\rangle_{3,4} \right). \tag{13.4}$$

The state ψ' is an entangled state of the modes 3 and 4: the photon is at the same time in both and none of the output arms of the beam splitter. By placing in front of the two outputs a pair of single-photon detectors, one realizes the following measurement operators:

$$P_{\text{out}}^{\text{no}} = |0\rangle\langle 0|_{\text{out}}\,, \qquad P_{\text{out}}^{\text{yes}} = |1\rangle\langle 1|_{\text{out}} \tag{13.5}$$

which measure, respectively, the absence or the presence of the photon in the respective output arm with out $\in \{3, 4\}$. Since the two measurements are independent, after the interaction of the single photon with the beam-splitter, the detectors perform the two possible bit-generating measurements

$$\Pi_0 = P_3^{\text{no}} \otimes P_4^{\text{yes}}\,, \qquad \Pi_1 = P_4^{\text{no}} \otimes P_3^{\text{yes}}. \tag{13.6}$$

By computing the outcome probability from (13.6) on the state $\rho_S = |\psi'\rangle\langle\psi'|$,

$$\mathrm{Tr}\left[\Pi_0 \rho_S\right] = \mathrm{Tr}[\Pi_1 \rho_S] = \frac{1}{2} \tag{13.7}$$

one sees that in a completely unpredictable way, as stated by the Born probability rule, it is possible to get 0 or 1 with exactly the same probability.

This approach was suggested and realized for the first time in [3] and it superseded the first attempts to generate random numbers by employing radioactive sources. Indeed, by using controllable optical photon sources as LEDs or lasers, one can easily prepare the state to be measured and fit both the sources and the detectors into compact and small devices (see for example [4] or [5]).

A drawback of these QRNGs is that they are limited by the count rate of the single photon counters, which at the present time do not allow one to extract random numbers at a rate higher than tens of gigabits per second. A way to overcome this limit is by changing the paradigm from discrete to continuous variables.

13.2.2 A Continuous Variable QRNG

The vacuum state of the electromagnetic field represents a source of entropy which has recently been employed to extract random numbers. When the quadratures of a pure vacuum state of the electromagnetic state are measured, one can collect a set

of unpredictable random variables distributed according to the normal distribution. This becomes evident when one considers the Wigner function of the vacuum state

$$W(q,\,p) = \frac{1}{2\pi}\exp\left(-\frac{1}{2}(q^2+p^2)\right) \tag{13.8}$$

where q and p are the eigenvalues relative to the momentum and position operators, respectively. When the state is measured along a given quadrature q, the possible measurement outcomes are distributed as follows:

$$w(q) = \int_{-\infty}^{+\infty} \mathrm{d}p\, W(q,\,p) = \frac{1}{\sqrt{2\pi}}\exp\left(-\frac{1}{2}q^2\right). \tag{13.9}$$

In the experiment, quadrature measurements are performed by means of homodyne detection, according to the scheme of Fig. 13.2. A coherent electromagnetic field, the so called *local oscillator* is mixed to the vacuum field entering through the unused port of a 50:50 beam splitter. More specifically, with respect to the single-photon discrete-variable approach, here the local oscillator is so intense that it can be treated as a classical field with amplitude $\alpha = |\alpha|\mathrm{e}^{\mathrm{i}\theta}$, playing the role of a vacuum fluctuations *amplifier*. The mixed fields exiting from the beam splitter outputs are intercepted by a couple of large bandwidth photodiodes which generate a current signal ΔI proportional to the light intensity hitting them. The two currents are respectively subtracted, so that one is left with a signal whose fluctuations are proportional to the quantum fluctuations of the field Fig. 13.3. In addition, local oscillator noise of classical origin, which would affect both incoming beams, is thus eliminated. In particular, if we denote by A and B the detectors intercepting the fields at the output of arms 3 and 4, respectively, we have that the output current of the

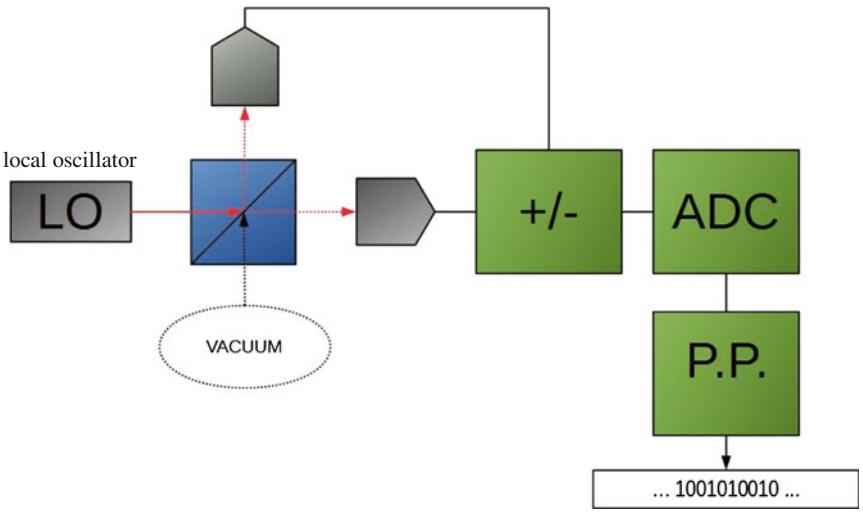

Fig. 13.2 Generic scheme to generate random numbers by homodyning the vacuum

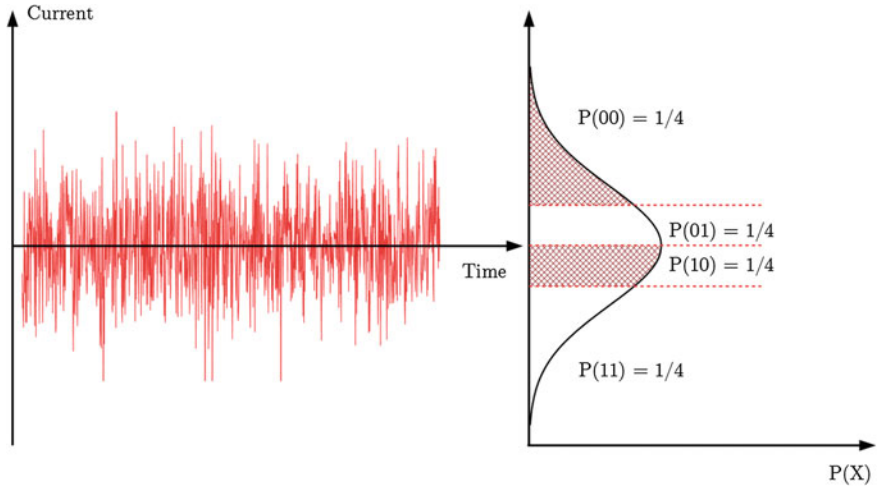

Fig. 13.3 On the *left*, the fluctuating current signal obtained by subtracting the outputs of the two photodiodes. On the *right*, the amplitude distribution of the signal is shown: in order to obtain numbers with a uniform distribution rather than a Gaussian one, the range of possible outcomes is split into a series of equal probability intervals. In the example of the picture, one has four possible intervals, each one with probability $\frac{1}{4}$ for a number in the range $[0, 4]$

setup is proportional to the difference of photon numbers given by the homodyne measurement operator $\hat{\Delta} = \hat{n}_A - \hat{n}_B$, where $\hat{n}_A = a\, a_3^*\, a\, a_3$ and $\hat{n}_B = a\, a_4^* a\, a_4$. By expressing the output operators as functions of the input ones, and considering the local oscillator classically, one has explicitly

$$\begin{aligned} \Delta &= n_A - n_B \\ &= \tfrac{1}{2}\left((\alpha^* + a\, a_1^*)(\alpha + a\, a_1) - (a\, a_1^* - \alpha^*)(a\, a_1 - \alpha)\right) \\ &= \tfrac{1}{2}\left((a\, a_1^*\alpha) + (a\, a_1\alpha^*)\right) \\ &= \tfrac{1}{2}|\alpha|\left(a\, a_1 \mathrm{e}^{\mathrm{i}\theta} + a\, a_1 \mathrm{e}^{-\mathrm{i}\theta}\right). \end{aligned} \tag{13.10}$$

At this point it is easy to see that if the local oscillator is in- (out) phase, $\theta = 0$ (respectively $\theta = \frac{\pi}{2}$), with the field entering at input 1 it is possible to measure its q (respectively p) quadrature. For example if $\theta = 0$, and the input state at arm 1 is the vacuum, one will get a ΔI proportional to $\Delta = \sqrt{2}|\alpha|q$. Random numbers are then obtained by sampling the ΔI signal with an analog-to-digital converter (ADC). However, since the quadrature values are normally distributed according to (13.9), it is necessary to make equal the appearance probability of every number. For this purpose, a post-processing algorithm splits the range of possible current values into *equal probability* intervals, as shown in Fig. 13.3, and then outputs a given number according to the interval within which the measured value falls. This approach for random number generation was presented in [6] and for further details see [7].

13.3 Introduction to Quantum Cryptography

Nowadays, cryptography represents the general instrument for protecting information against a rational adversary. Cryptographic algorithms lie at the core of most security protocols and mechanisms, such as: encryption of data to ensure confidentiality, data authentication to detect forged messages, or integrity protection against illegitimate modification of messages in transit.

The majority of classic cryptographic algorithms can only offer computational security, that is, they guarantee that an adversary with limited computational capabilities has a low probability of success in attacking the security protocol within a reasonable amount of time. Such is the case, for instance, of all public-key cryptography, e.g., RSA encryption [8] and DSA signatures [9], as well as most symmetric schemes, e.g., AES encryption [10], and deterministic hashing, e.g., SHA [11]. If the amount of computational time that is needed by any adversary to break the security scheme considerably exceeds the useful life span of the relevant information, the scheme can be deemed properly secure. However, such schemes do not offer long-term protection of secured information from possible future technological or algorithmic breakthroughs. In particular, some public-key schemes, such as the above-mentioned RSA and DSA, have already been proven vulnerable to quantum computing attacks, since Shor's quantum algorithm [12] allows one to solve the task of finding the periodicity of a function with limited error probability and in polynomial time. In fact, that task is crucial in solving the integer factorization and the finite logarithm problems, the hardness of which (for classical computers) ensures the computational security of RSA and DSA, respectively.

Other classical schemes offer unconditional security (also known as information theoretic security), where the limit to the success probability of the attacker is no longer set by his/her computational capabilities, but rather by the information that is available to him/her. However, this is typically done at the expense of requiring the legitimate users to preshare a large quantity of secret material, as in the one-time-pad scheme, where the encrypted message is obtained by summing the secret message with a random secret key with the same entropy as the message. Alternatively, some information is required at the legitimate terminals about the attacker channel, as in designing wiretap coding schemes, and in this case the diversity between the legitimate and the attacker channel is leveraged to provide the required security. However, it should be noted that the assumption of knowing the attacker channel is unrealistic in general, since it cannot rely on any collaboration from the adversary.

By contrast, quantum cryptography can offer unconditional, information theoretic, security, as it is based on:

- the inherent randomness in the outcomes of quantum measurements,
- the possibility of statistically bounding the amount of measurements taken by the adversary, from the statistics of nonorthogonal measurements by the legitimate parties.

From the above two properties, one can state that there is no such thing as a purely passive, undetectable attacker in the realm of quantum information.

Starting from the pioneering work of Wiesner [13] who, as early as 1970 (even if his paper was only published many years later), set forth the possibility to create unforgettable quantum money, quantum counterparts have been subsequently developed for many cryptographic primitives, such as bit commitment, oblivious transfer, coin flipping, and random number generation (as was seen in Sect. 13.2.1). In the following sections, however, we will limit ourselves to describing the quantum cryptographic primitive that has been the earliest and most successfully implemented, that is, quantum key agreement (aka quantum key distribution).

13.4 Quantum Key Distribution (QKD)

A *key agreement protocol* is a security mechanism upon which two parties, Alice and Bob, jointly generate a common random variable or string (the *key*) $K \in \mathcal{K}$ that is uniformly distributed and unknown to any other party. Thus, K can securely be used as a cryptographic key for symmetric algorithms between them, e.g., for encryption or message authentication. To this purpose Alice and Bob can locally process separate secret random variables A and B, respectively, at each terminal, and exchange messages $m_{\mathrm{A}}, m_{\mathrm{B}}$ over a public and authenticated channel (*public discussion*), where all transmissions can be observed, but not forged or altered, by any third party.

The most widely known and adopted key agreement scheme is the Diffie-Hellman protocol [14], which allows for separate and independent generation of the initial random variables A and B at Alice and Bob, and offers computational security based on the hardness of the discrete logarithm problem.

On the other hand, *information theoretic* key agreement schemes offer unconditional security, but require that some randomness is shared beforehand between Alice and Bob, that is to say, their initial random variables A and B must be correlated. This can be obtained either by separate noisy observations of the same random quantity (in the so-called *source model*), or by generating a random signal at one end (say, A at Alice) and transmitting it to the other end (say, Bob) through a noisy channel (in the *channel model*). However, when such interaction is allowed for the legitimate terminals, the same must be granted to a generic eavesdropper Eve, who will therefore have access to a third variable C, itself correlated with A and B.

The performance measure of an information theoretic key agreement scheme is given by the *secret key rate* R_{k}, that is, the information rate (in bit/s) of the final output key under the asymptotic constraints

$$\begin{aligned} &\mathrm{P}[K_{\mathrm{A}} \neq K_{\mathrm{B}}] < \varepsilon && \text{(correctness)} \\ &\log_2 |\mathcal{K}| - H(K) < \varepsilon && \text{(uniformity)} \\ &I(K; C, m_{\mathrm{A}}, m_{\mathrm{B}}) < \varepsilon && \text{(secrecy).} \end{aligned} \tag{13.11}$$

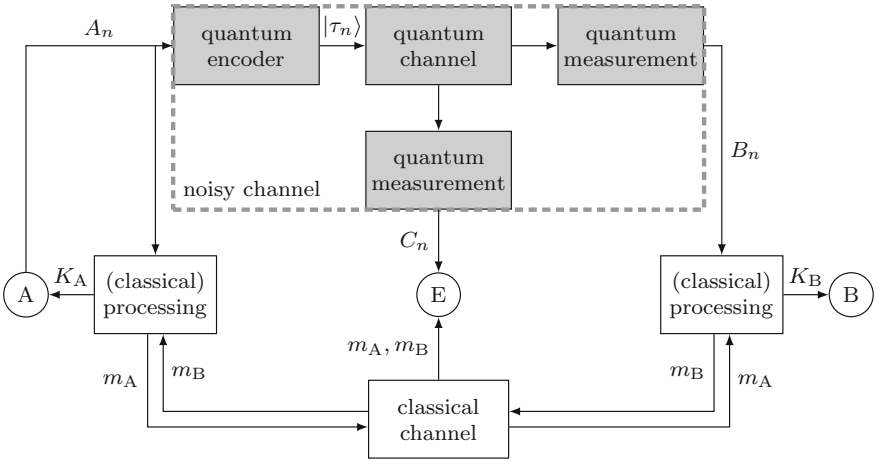

Fig. 13.4 Quantum cryptographic implementation of information theoretic key agreement in the channel model via a prepare-and-measure QKD system

If the random variables initially available to Alice, Bob, and Eve are symbol sequences, denoted by A_n, B_n, and C_n, respectively, generated by a memoryless source or noisy channel with symbol rate R_s, and joint symbol probability distribution $p(A, B, C)$, it can be shown that the maximum achievable secret key rate satisfies the bounds

$$R_s\,[I(A;B) - \min\{I(A;C), I(B;C)\}] \leq R_k \leq R_s \min\{I(A;B), I(A;B|C)\} \tag{13.12}$$

Quantum cryptography allows for an effective implementation of information theoretic key agreement schemes,[2] leading to the development of quantum key distribution (QKD) protocols. In particular, channel model schemes can be implemented through *prepare-and-measure* protocols as illustrated in Fig. 13.4, while source model schemes find a proper embodiment in *entanglement-based* protocols, as shown in Fig. 13.5.

When considering a quantum environment, the secrecy notion in (13.11) should be stated in quantum information terms, e.g., by bounding the accessible information at Eve, as $I_{acc} < \varepsilon$, since, in general Eve may optimize her measurement after Alice and Bob have performed their agreement protocol.

Traditionally, QKD protocols are divided into *discrete variable* (DV-) and *continuous variable* (CV-) QKD, according to the nature of the initial random variables A_n, B_n and of the quantum states that represent them. In the following, we shall examine an example of both prepare-and-measure and entanglement-based, DV-QKD. Eventually, we shall also briefly outline a QKD protocol with continuous variables.

[2] Historically, the first formulation of a QKD protocol [15] preceded that of general information theoretic key agreement schemes [16].

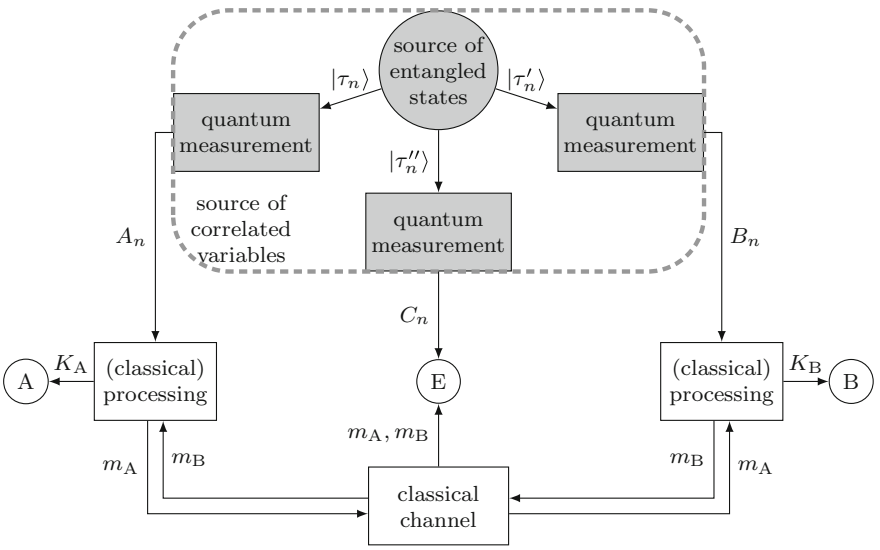

Fig. 13.5 Quantum cryptographic implementation of information theoretic key agreement in the source model via an entanglement-based QKD system

13.4.1 A Discrete-Variable-QKD Prepare-and-Measure Protocol

In this section we describe a *prepare-and-measure* protocol for DV-QKD that was proposed in [17] and is known as *efficient BB84*. It represents a variation of the original *BB84* protocol, the first to be proposed for DV-QKD in [15], and lends itself to a compact description and a precise security analysis [18, 19].

Transmission and Detection

According to this protocol, four states $|\gamma_0^+\rangle, |\gamma_1^+\rangle, |\gamma_0^\times\rangle, |\gamma_1^\times\rangle \in \mathcal{H}$ are used for transmission along the qubit channel. They are chosen to be pairwise orthogonal with $\langle\gamma_0^+|\gamma_1^+\rangle = 0$ and $\langle\gamma_0^\times|\gamma_1^\times\rangle = 0$ and hence make up two distinct bases for $\mathcal{H}$. The basis $\mathcal{B}^+ = \{|\gamma_0^+\rangle, |\gamma_1^+\rangle\}$ is called the *majority basis* (or *bit basis*), and is used to share a common binary string between the two legitimate terminals, whereas the *minority basis* $\mathcal{B}^\times = \{|\gamma_0^\times\rangle, |\gamma_1^\times\rangle\}$ (sometimes called *phase basis*) is used to detect any eavesdropping on the qubit channel. In fact, if eavesdropping is detected, the protocol aborts, and the eavesdropped key is discarded.

The transmitter (Alice) generates a sequence of independent–identically distributed binary symbols $\{A_n\}$ with equally likely 0 and 1 and encodes each bit randomly

and independently into either basis, so that the transmitted state at the nth symbol period is

$$|\tau_n\rangle = \begin{cases} |\gamma_{A_n}^{+}\rangle & \text{with probability } p \\ |\gamma_{A_n}^{\times}\rangle & \text{with probability } 1-p \end{cases}$$

for some fixed probability p.

On the other side of the channel, the receiver (Bob) measures each incoming state $|\tau_n\rangle$ with a POVM M_n, that is composed of a pair of orthogonal rank-1 projectors along the states that make up either basis. In fact, the measurement operators are chosen randomly and independently at each symbol period, and independently of the encoding choices made by Alice, with

$$M_n = \begin{cases} \{\Pi_0^{+}, \Pi_1^{+}\} & \text{with probability } p' \\ \{\Pi_0^{\times}, \Pi_1^{\times}\} & \text{with probability } 1-p' \end{cases}$$

where $\Pi_0^{+} = |\gamma_0^{+}\rangle\langle\gamma_0^{+}|$ and analogously for $\Pi_1^{+}, \Pi_0^{\times}, \Pi_1^{\times}$, and for some fixed p'. We denote by $B_n \in \{0, 1\}$ the corresponding outcome.

Hence, from (3.29) the channel transition probabilities are

$$p_{\mathrm{c}}(i|j) = \begin{cases} \left|\left\langle \gamma_i^{+} | \gamma_j^{+} \right\rangle\right|^2 & \text{when both Alice and Bob use } \mathcal{B}^{+} \\ \left|\left\langle \gamma_i^{\times} | \gamma_j^{\times} \right\rangle\right|^2 & \text{when both Alice and Bob use } \mathcal{B}^{\times} \\ \left|\left\langle \gamma_i^{\times} | \gamma_j^{+} \right\rangle\right|^2 & \text{when Alice uses } \mathcal{B}^{+} \text{ and Bob uses } \mathcal{B}^{\times} \\ \left|\left\langle \gamma_i^{+} | \gamma_j^{\times} \right\rangle\right|^2 & \text{when Alice uses } \mathcal{B}^{\times} \text{ and Bob uses } \mathcal{B}^{+}. \end{cases}$$

In particular, observe that, due to the orthogonality between states in the same basis, whenever Alice and Bob choose the same basis they have a correct transition with probability 1, whereas when the chosen bases differ, there will be a bit error with probability $\delta = |\langle\gamma_0^{+}|\gamma_1^{\times}\rangle|^2 = |\langle\gamma_1^{+}|\gamma_0^{\times}\rangle|^2$.

Eavesdropping

Now, consider that an eavesdropper (Eve) sitting along the Alice-Bob channel has observed (measured) each single qubit coming from Alice. Her best chance is to always use the $\{\Pi_0^{+}, \Pi_1^{+}\}$ measurement operators, as this will give her full information on the secret bits that will be shared between Alice and Bob. Let C_n denote the outcome of her measurement; because of the no-cloning theorem, in order to share the same information with Bob, she must re-encode it as

$$|\tilde{\tau}_n\rangle = |\gamma_{C_n}^{+}\rangle$$

and transmit it along the channel to Bob. Whenever both Alice and Bob choose the majority basis, both measurements by Eve and Bob will yield a correct transition, and it will be $A_n = B_n = C_n$. However, if both Alice and Bob choose the minority basis, it will be

$$p_{C_n|A_n}(i|j) = \left|\left\langle \gamma_i^{+}|\gamma_j^{\times}\right\rangle\right|^2$$

and

$$p_{B_n|C_n}(i|j) = \left|\left\langle \gamma_i^{\times}|\gamma_j^{+}\right\rangle\right|^2.$$

By conditioning on C_n, and applying the total probability theorem, we then obtain

$$\begin{aligned} p_{\mathrm{c}}(i|j) &= \sum_{\ell=0}^{1} p_{B_n|A_nC_n}(i|j,\ell)\, p_{C_n|A_n}(\ell|j) \\ &= \sum_{\ell=0}^{1} p_{B_n|C_n}(i|\ell)\, p_{C_n|A_n}(\ell|j) \\ &= |\langle \gamma_i^{\times}|\gamma_0^{+}\rangle|^2 \left|\left\langle \gamma_0^{+}|\gamma_j^{\times}\right\rangle\right|^2 + |\langle \gamma_i^{\times}|\gamma_1^{+}\rangle|^2 \left|\left\langle \gamma_1^{+}|\gamma_j^{\times}\right\rangle\right|^2 \\ &= \begin{cases} \delta^2 + (1-\delta)^2 & \text{for } i = j \\ 2\delta(1-\delta) & \text{for } i \neq j. \end{cases} \end{aligned} \tag{13.13}$$

Therefore, when both Alice and Bob choose the minority basis and Eve performs the measurement and re-encoding on the transmitted qubit using the majority basis, Alice and Bob will experience a bit error with probability $\delta' = 2\delta(1-\delta)$.

Sifting and Eavesdropping Detection

After the transmission is completed, Alice and Bob can share the following information along the public channel, that is, by m_{A} and m_{B}

1. In m_{A}, Alice tells Bob the subset of indices $N_{\mathrm{A}} = \left\{n \mid \tau_n \in \mathcal{B}^{+}\right\}$ in which she used the majority basis;
2. In m_{B}, Bob tells Alice the subset of indices $N_{\mathrm{B}} = \left\{n \mid M_n = \{\Pi_0^{+}, \Pi_1^{+}\}\right\}$ in which he used the majority basis;

so that each of them can infer the subset of indices $N = N_{\mathrm{A}} \cap N_{\mathrm{B}}$ in which they have both used the majority basis, and $N' = N_{\mathrm{A}}^{\mathrm{c}} \cap N_{\mathrm{B}}^{\mathrm{c}}$ in which they have both used the minority basis. Then:

- the bits A_n, B_n for $n \notin N \cup N'$ are discarded (*sifting*);
- the bits A_n, B_n for $n \in N$ are kept undisclosed and will be used to build the secret key;
- the bits A_n, B_n for $n \in N'$ are exchanged by Alice and Bob over the public channel, so that by comparing their values they can detect any errors.

Assume that n_{tot} total qubits have been transmitted, and that Alice and Bob declare that eavesdropping has been detected if for some $n \in N'$, $A_n \neq B_n$. The probability that Eve observing all qubits goes undetected is the probability that there are no errors in all the bits where both Alice and Bob use the minority basis, that is,

$$P_{\text{md}} = \prod_{n=1}^{n_{\text{tot}}} \big(\text{P}[n \notin N'] + (1-\delta')\text{P}[n \in N']\big) = \big[1 - \delta'(1-(p+p') + pp')\big]^{n_{\text{tot}}}.$$

Choice of the Parameters p', δ, δ'

So far, we have left the values of parameters p, p', δ, δ' unspecified, subject to system design choices. We will now show that some optimal choice can be made straight away, with the aim of maximizing the number of bits that can be used to build the secret key, and at the same time of minimizing the probability that an attack by Eve goes undetected.

Consider the probability that a particular bit A_n (and correspondingly, B_n) is used to build the secret key, called the *sifted key rate*, which is given by $\text{P}[n \in N] = pp'$. This is clearly maximized by the choice $p = p' = 1$ (always using the majority basis), which, unfortunately, would eliminate the possibility of detecting Eve's attack, and yield $P_{\text{md}} = 1$. Therefore, a tradeoff must be sought between increasing the sifted key rate and the attack detection probability. However, one can notice that for any fixed value of sifted rate pp', the value of P_{md} is minimized by making the sum $p + p'$ as small as possible, that is, by choosing $p' = p$, and by maximizing δ'.

As δ' is a quadratic function of δ, it is easily seen that its maximum is achieved at $\delta = 1/2$ yielding $\delta' = 1/2$. Observe that this choice corresponds to having the inner products

$$\left|\left\langle \gamma_i^{+} | \gamma_j^{\times} \right\rangle\right| = \frac{1}{\sqrt{2}}, \quad i, j = 0, 1 \tag{13.14}$$

that are obtained by choosing the two bases in a symmetric fashion in the qubit space, which intuitively justifies our $\mathcal{B}^+, \mathcal{B}^\times$ notation. For instance, if the information is encoded into the polarization state τ_n of a single photon, one may choose horizontal, vertical, and diagonal polarization states as follows:

$$\gamma_0^{+} = |\uparrow\rangle, \gamma_1^{+} = |\rightarrow\rangle, \gamma_0^{\times} = |\nearrow\rangle, \gamma_1^{\times} = |\nwarrow\rangle$$

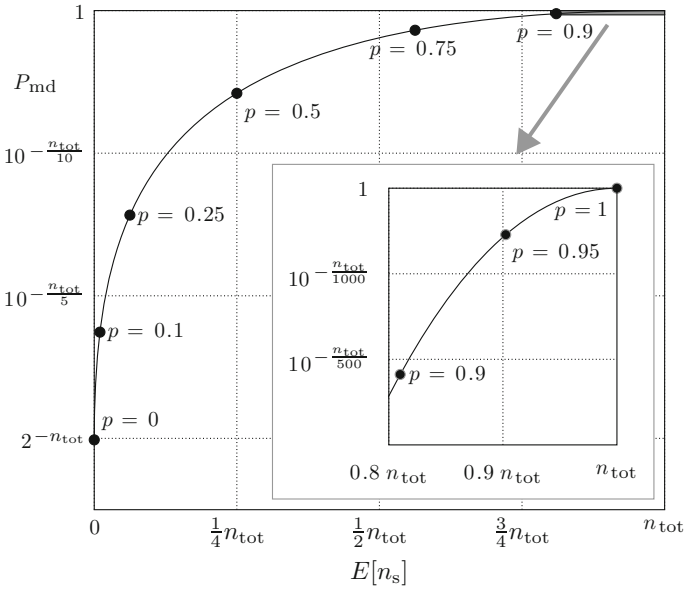

Fig. 13.6 Illustration of the tradeoff between the expected length of the sifted key $\mathrm{E}[n_{\mathrm{s}}]$ and the missed detection probability P_{md}, depending on the value of the probability p of the majority basis. In the *lower right* corner an expanded view of the *upper right* corner, which is typically the region of practical interest. For instance observe that, with $n_{\mathrm{tot}} = 10^4$ transmitted qubits, if it is required to keep $P_{\mathrm{md}} < 10^{-20}$, one has to choose $p \leq 0.9$, and hence obtain no more than 8 200 sifted bits, on average

From now on, we will therefore assume that (13.14) holds and $p' = p$, thus yielding the missed detection probability and the expected sifted key length

$$P_{\mathrm{md}} = \left(\frac{1}{2} + p - \frac{1}{2}p^2\right)^{n_{\mathrm{tot}}}, \quad \mathrm{E}[n_{\mathrm{s}}] = n_{\mathrm{tot}}\, p^2$$

where the value of p allows us to trade the sifted key length for the attack detection capabilities of the scheme. The tradeoff is illustrated in Fig. 13.6.

Note that in this ideal setting the sifted keys $A' = [A'_1, \ldots, A'_{n_{\mathrm{s}}}] = [A_n]_{n \in N}$ and $B' = [B'_1, \ldots, B'_{n_{\mathrm{s}}}] = [B_n]_{n \in N}$ can be directly used as a secret cryptographic key pair, since they are identical with unit probability, and provided P_{md} is sufficiently low, any eavesdropping would have been detected with high probability.[3]

[3] A somewhat subtle point should be made here. The security of the protocol does not guarantee that eavesdropping is unlikely, given that no errors have been detected in the minority basis. Rather, it states that if eavesdropping takes place, it will be detected with high probability. In symbols, let E denote the event that eavesdropping has taken place and D the event that no errors have been detected, we can only upper bound $P_{\mathrm{md}} = \mathrm{P}[D|E]$, but nothing can be said about $\mathrm{P}[E|D]$, since no assumption can be made on the probability of event E which is totally under the control of the attacker.

13.4.2 A DV-QKD Entanglement-Based Protocol

In this section we present a QKD protocol which makes use of entangled particles to share a secret key between two parties. The BBM92 protocol (Fig. 13.7), described here, was first proposed by Bennett, Brassard and Mermin in [20], as a simpler version of the Ekert protocol [21].

In the BBM92 scheme the channel consists of a source, called Charlie, that emits entangled particles and sends them to opposite directions.

The particles are received by two users, Alice and Bob, who perform measurements M_n^{A} and M_n^{B}. Both Alice and Bob choose their measurement operators randomly, independently and with equal probability between $\{\Pi_0^+, \Pi_1^+\}$ and $\{\Pi_0^\times, \Pi_1^\times\}$. Similar to BB84, we have that $\{\Pi_0^+, \Pi_1^+\}$ and $\{\Pi_0^\times, \Pi_1^\times\}$ should be selected symmetrically in the qubit space. Usually the bases are chosen to be the Pauli operator, i.e., $\Pi_0^\times = \sigma_z$ and $\Pi_0^+ = \sigma_x$, which satisfy the nonorthogonality condition. After a sequence of n_{tot} entangled particles are received and measured, Alice and Bob publicly announce which basis they used for each particle, but not the outcomes of the measurements. During sifting, Alice and Bob discard the events in which they measured in different bases, or in which the measurement failed because of imperfect detection. The remaining instances, in which both measured in the same basis, should be perfectly correlated if they actually measured entangled pairs. In order to verify this, Alice and Bob publicly compare their outcomes A_n, B_n in a subset $n \in N'$ of the undiscarded events. If Alice and Bob find perfect correlation on the tested set N', they can state that the transmission was secure and no eavesdropping was performed, and keep the remaining A_n, B_n, $n \in N = N_{AB}\ N'$ to produce the secret key K.

Security Proof

In examining the security of the BBM92 protocol, it is interesting to notice that this protocol bears many analogies to the BB84 presented in the previous section. We consider the most common attacks, i.e., *intercept and resend*, and *source substitution*. The discussion of the protocol robustness against the former kind of attack is analogous to the one given for the BB84 protocol and we refer to the previous section. The source substitution attack happens when an eavesdropper Eve sends Alice and Bob

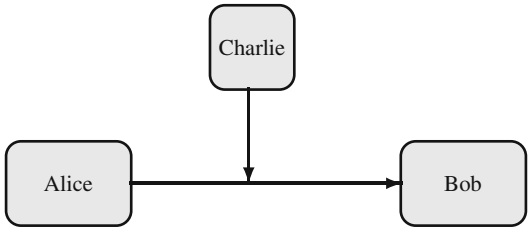

Fig. 13.7 BBM92 scheme. Alice and Bob: receiving users. Charlie: source of entangled particles

pairs that are somehow entangled with systems available to her. The most general entangled state Eve can prepare is equal to

$$|\Phi\rangle = |11\rangle|e_0\rangle + |00\rangle|e_1\rangle + |10\rangle|e_2\rangle + |01\rangle|e_3\rangle,$$

where $|1\rangle$ and $|0\rangle$ form an orthonormal qubit basis and $|e_0\rangle$,$|e_1\rangle$,$|e_2\rangle$ and $|e_3\rangle$ are the states of Eve's system. We can notice that in general Eve does not even have to decide her measurements until Alice and Bob have published theirs. Eve's aim is to be completely invisible, therefore, if Alice and Bob measure in the $\mathcal{B}^+$ basis, in order that they have fully correlated outcomes, the state $|\Phi\rangle$ must be an eigenstate of $\sigma_z^a \sigma_z^b$ with eigenvalue -1. This implies that $|\Phi\rangle$ must assume the form:

$$|\Phi\rangle = |10\rangle|e_2\rangle + |01\rangle|e_3\rangle.$$

At the same time, if Alice and Bob measure in the $\mathcal{B}^\times$ bases, the state $|\Phi\rangle$ must be an eigenstate of $\sigma_x^a \sigma_x^b$ with eigenvalue -1. This further restricts $|\Phi\rangle$ as follows:

$$|\Phi\rangle = (|10\rangle - |01\rangle)\,|e_2\rangle.$$

From this, the only Eve's source that will surely be undetected by Alice's and Bob's test is the one in which Eve's system is completely uncorrelated with the entangled particles. Thus, every measurement gives her no information about Alice's and Bob's outcomes.

Out of Curiosity

In 1992 there was a heated discussion between Ekert and Bennett, Brassard and Mermin, about the described protocol. Ekert stated that the security proof must be based on "non-locality" and "non-reality" tests given by Bell's theorem. Bennett et al. demonstrated their protocol without these assumptions using a simpler scheme. Recently, Vallone et al. [22] proposed a new protocol which uses a simple scheme as Bennett et al. and bases its security on Bell's theorem thanks to the use of non-maximally entangled particles.

13.4.3 Key Processing

In introducing the above protocols, we have ideally supposed that, provided Alice and Bob choose the same basis and Eve does not interfere, the sharing of a bit through the quantum channel is error-free. In that case, the sifted keys are also the final secret keys.

In a more realistic environment, however, distortion introduced by the quantum channel, temporal or spatial misalignment between the two terminals, and quantum

noise in the receiver may introduce some errors, even for bits A_n, B_n with $n \in N \cup N'$, and without any attack. This has two potentially fatal consequences:

1. errors $A_n \neq B_n$ for $n \in N$ will propagate to the distilled secret key;
2. errors $A_n \neq B_n$ for $n \in N'$ will make Alice and Bob abort the protocol, even in the absence of an attacker.

The two problems above can be solved with techniques for the processing of random signals in the classical domain, to yield the final secret keys where both the mismatch between Alice and Bob's keys and the information leaked to the attacker have been removed with high probability.

In the following we assume that errors in each basis are symmetric and independent across symbols, so that the transformation linking A_n to B_n for $n \in N$ (respectively, $n \in N'$) is a binary symmetric channel with error rate ε^+ (respectively, $\varepsilon^\times$).

Information Reconciliation

In order to solve problem 1, techniques similar to traditional forward error correction coding for the binary symmetric channel can be used, providing they are suitably adapted to the secrecy requirement in the QKD framework. In fact, since the binary sifted sequence $A' = [A'_1, \ldots, A'_{n_s}] = [A_n]_{n \in N}$, (and the analogous B') is only known after sifting, the redundancy bits that allow error correction must be transmitted later, along the public classical channel, and can be observed by any attacker. The amount of redundancy must therefore be kept to a minimum, not for efficiency reasons, but to limit as far as possible the amount of information that leaks to an eavesdropper. As is well known, a lower bound on the amount of redundancy that must be transmitted in order to have reliable error correction is given by $r = n_s h_2(\varepsilon^+)$, with $h_2(\cdot)$ denoting the binary entropy function (see Chap. 12) $h_2(\varepsilon) = -\varepsilon \log_2 \varepsilon - (1-\varepsilon)\log_2(1-\varepsilon)$.

One possibility is to generate the redundancy bits m'_{A} by using systematic encoding for a block channel code, where properly sized blocks taken from the sifted sequence make up the information words, that is, $m'_{\mathrm{A}} = GA'$, where A' and m'_{A} are seen as columns vectors, and G denotes the nonidentity portion of the systematic generating matrix. Thus, upon receiving $\tilde{m}'_{\mathrm{A}}$ over the public channel, Bob can perform minimum distance decoding, that is replace B' by

$$B'' = \arg \min_{\beta \in \{0,1\}^{n_s}} d_{\mathrm{H}}([\beta, G\beta], [B', \tilde{m_{\mathrm{A}}}])$$

with $d_{\mathrm{H}}(\cdot, \cdot)$ representing the Hamming distance between two binary strings.[4]

However, typically the public channel is assumed error-free and authenticated (that is, each message can be verified to actually come from Alice and not having been altered in transit), so that $\tilde{m}'_{\mathrm{A}} = m'_{\mathrm{A}}$ and there is no need to protect the redundancy bits from channel errors. In this case, it is more efficient in terms of error correction capability to obtain the redundancy bits as a hash of the sifted sequence, given, for

[4] That is, the number of positions at which they differ.

instance, through the parity check matrix G' of a linear code, yielding $m'_{\mathrm{A}} = G'A'$. Thus, upon receiving $\tilde{m}'_{\mathrm{A}}$ over the public channel, Bob can perform minimum distance decoding, that is, replace B' by

$$B'' = \arg \min_{\beta \in \{0,1\}^{n_{\mathrm{s}}}} d_{\mathrm{H}}([\beta, G'\beta], [B', \tilde{m_{\mathrm{A}}}]).$$

The latter approach is currently the most widely used in the QKD literature, typically by employing LDPC codes (see [23]), especially with stable channels and long processing blocks, where the code parameters can be precisely tuned to require an amount of redundancy that is close to the lower bound. On the other hand, when the channel conditions are varying, and/or shorter blocks need to be used, other ad hoc solutions are considered that require more interaction between the terminals along the public channel and intrinsically adapt to the channel conditions (see [19]).

In a symmetric fashion, one can have Alice correct A' to match Bob's sifted sequence B' based on a public message m_{B} sent by Bob. Alternatively, one can use a two-way reconciliation scheme where both Alice and Bob send public messages and each one partially correct their sifted keys.

Privacy Amplification

The obvious solution to problem 2 above is to allow for some errors in the bits with $n \in N'$ without aborting the protocol, as long as the number of errors n_{err} is below some specified threshold θ. The threshold is typically chosen depending on the cardinality of N' and the channel error rate.

However, this would introduce a vulnerability in the protocol. It makes it possible for the eavesdropper to perform a *selective intercept and resend* attack on a limited, yet significant, fraction of the qubits shared between Alice and Bob, by retransmitting them through an error-free channel. In this way, Eve's observations may not be detected, as Alice and Bob will attribute the errors to the channel and tolerate them, whereas they were actually induced by the eavesdropper measurements.

Therefore, a conservative countermeasure requires Alice and Bob to remove the partial information that Eve may have acquired through undetected qubit observations or by accessing the redundancy transmitted over the public channel for the purpose of reconciliation. *Privacy amplification* is the process of removing any information available to the attacker from the reconciled keys to yield the final *secret key* K.

This is done through the application of a common hashing function $f : \{0,1\}^{n_{\mathrm{s}}} \to \{0,1\}^{\ell}$ at each reconciled sequence A''_n and B''_n, where $\ell < n_{\mathrm{s}}$ represents the length of the final key. Clearly, applying the same function allows to maintain correctness. In fact, since the sequences A''_n and B''_n are supposedly identical with very high probability, so will be the corresponding outputs K_{A}, K_{B}. On the other hand, compressing the sequence with a function that is surjective, but not injective, makes it possible to remove bits that have been learnt by Eve, and the redundancy that has been inserted for reconciliation purposes, to obtain a key that is as uniform and independent of the eavesdropper observations as possible.

Typically, the hash function is simply a multiplication by a matrix $F \in \{0,1\}^{\ell \times n_s}$ on the binary field. Also, a potential eavesdropper knowledge (C, m_A, m_B) about the reconciled sequence $A'' = B''$ can itself be described as a matrix function $M \in \{0,1\}^{t \times n_s}$. For instance, suppose that Eve has performed selective intercept and resend so that she knows a subset $C'' = \{A''_n, n \in N_E\}$ of the reconciled sequence, for some N_E, and that she has observed the bits $m'_A = GA''$ transmitted along the public channel for reconciliation. Then, we can write

$$M = \begin{bmatrix} I_{N_E} \\ G \end{bmatrix}$$

where I_{N_E} is made of the rows from the $n_s \times n_s$ identity matrix with indices in N_E, and $t = r + |N_E|$.

If the eavesdrop matrix M were known to Alice and Bob, it would in principle be possible to choose the privacy amplification matrix F to yield a perfectly secret key. In fact, in this case, since A'' is uniform over $\{0,1\}^{n_s}$ (as a consequence of the fact that A_n and B_n are assumed to be iid uniform sequences), it can be easily seen that the final key K is uniform in as $\{0,1\}^{\ell}$ and independent of the eavesdropper observations if and only if the null spaces of F and M satisfy

$$\dim \mathcal{N}(M) - \dim\left(\mathcal{N}(M) \cap \mathcal{N}(F)\right) = \ell \,. \tag{13.15}$$

On the other hand, if M is not known, but the value of t is (or can at least be upper bounded), Alice and Bob can choose the hashing function f randomly after sifting (so that Eve can not tailor her observations to it) and communicate the choice over the public channel. It was shown in [24] that the average of the mutual information in (13.11) over the choice of f can be upper bounded as

$$I(K; C, m_A, m_B, f) < \frac{1}{\log 2} \frac{1}{2^{n_s - t - \ell}} \tag{13.16}$$

by choosing f uniformly within a universal hashing class,[5] such as that of all $\ell \times n_s$ binary Toeplitz matrices.

In general, however, it is more realistic to assume that neither the exact position, nor even the exact amount of the qubits observed by the eavesdropper are known to the legitimate parties.

Therefore, privacy amplification is usually performed in two steps. First, since the matrix G of information reconciliation is perfectly known, a matrix $F_1 \in \{0,1\}^{\ell_1 \times n_s}$

[5] A class $\mathcal{F}$ of functions mapping the same domain X to the same range Y is called *universal hashing* if it maps inputs to outputs "uniformly", that is,

$$\begin{cases} |\{f \mid f(x) = y\}| = |\mathcal{F}|/|Y| & \text{for all } x \in X, y \in Y \\ |\{f \mid f(x_1) = f(x_2)\}| = |\mathcal{F}|/|Y| & \text{for all } x_1, x_2 \in X. \end{cases}$$

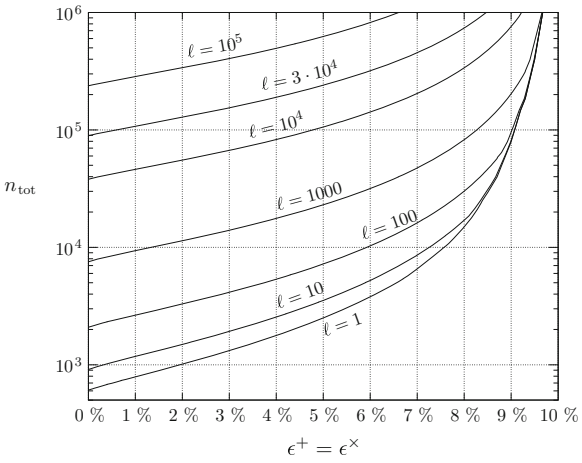

Fig. 13.8 Minimum amount of qubits n_{tot} that need to be transmitted in the efficient BB84 protocol, as a function of the quantum BER (assumed equal on both bases, $\varepsilon^+ = \varepsilon^\times$), for different target values of the final secret key length ℓ. The plot is based on an optimization of the finite key bound in [18]

that satisfies (13.15) with F_1 replacing F and G replacing M is applied. Then, the amount of information that is available to Eve from undetected qubit observations is upper bounded probabilistically in terms of the abort threshold on the number of detected errors, that is, t_{ub} is chosen so that $\mathrm{P}[n_{\text{err}} < \theta | t > t_{\text{ub}}]$ is acceptably low. Eventually, a matrix $F_2 \in \{0, 1\}^{\ell \times \ell_1}$ chosen randomly from a universal hashing class is applied so that (13.16) is satisfied with very high probability.

Clearly, in the limit of $n_{\text{tot}}, |N'| \to \infty$ the rate of information that is available to Eve can be precisely estimated. On the other hand, when n_{tot} is limited (in the so-called *finite key* regime) such estimates have a large amount of uncertainty, and significant margins must be allowed when choosing t_{ub} and ℓ. Several bounds for ℓ have been formulated in the finite key regime [18, 19]. Figure 13.8 shows a contour plot of the final key length as a function of the total transmitted qubits and the error rates in the channel for the efficient BB84 protocol, according to the bound provided in [18] and for optimal choices of the threshold θ and the majority basis rate p. Observe that ℓ decreases rapidly following n_{tot}.

13.4.4 A Continuous Variable QKD Protocol

As an example of CV-QKD, we consider the GG02 protocol [25], as introduced in [26], a *prepare-and-measure* scheme, which makes use of coherent states with Gaussian displacements.

In fact, the transmitter Alice generates a sequence A_n of iid complex Gaussian random variables with circular symmetry.[6] Then she encodes each variable A_n into the coherent state with displacement given by the corresponding realization of A_n, that is,

$$A_n = \alpha \Rightarrow |\tau_n\rangle = |\alpha\rangle.$$

Alternatively, this can be viewed as encoding $\Re A_n$ into the position and $\Im A_n$ into the momentum displacement of $|\tau_n\rangle$.

The protocol is based on the fact that the uncertainty principle prevents measuring both quadratures with full accuracy. On the other side of the quantum channel, Bob measures either the position or momentum of each incoming state $|\tau_n\rangle$, by randomly and independently choosing each measurement observable as

$$M_n = \begin{cases} q & \text{with probability } 1/2 \\ p & \text{with probability } 1/2 \end{cases}$$

and we denote by $B_n \in \mathbb{R}$ the corresponding continuous-valued outcome.

Thus, B_n will be a Gaussian random variable correlated with either $\Re A_n$ of $\Im A_n$ according to whether $M_n = q$ or $M_n = p$. After the transmission is completed, Bob tells Alice via the message m_{B} the sequence of measurements $\{M_n\}$ so that Alice can sift her sequence and obtain

$$A'_n = \begin{cases} \Re A_n & \text{if } M_n = q \\ \Im A_n & \text{if } M_n = p. \end{cases}$$

The mutual information between A_n (or equivalently A'_n) and B_n is therefore given by

$$I(A; B) = \frac{1}{2} \log_2 \left(1 + \frac{\sigma_A^2}{\sigma_0^2} \right)$$

where σ_0^2 represents the fluctuations of the coherent state around its displacement.

The possibility of detecting an intercept and resend attack by Eve lies in the impossibility for Eve to perform both a position and momentum observation on τ_n, analogously to what was shown for discrete variable protocols.

13.5 Teleportation

Quantum teleportation is one of the many important applications of entanglement. It allows an *unknown* quantum state to be transported from Alice to Bob by transmitting only classical information. In particular, a qubit can be teleported by using two

[6] A complex-valued random variable X is called circular symmetric Gaussian if $\Re X$ and $\Im X$ are independent Gaussian variables with zero mean and the same variance σ_X^2.

classical bits. Let us consider the simplest example, given by a single qubit in a generic state unknown to Alice

$$|\varphi\rangle_{\mathrm{C}} = \alpha|0\rangle_{\mathrm{C}} + \beta|1\rangle_{\mathrm{C}}. \tag{13.17}$$

Due to the no-cloning theorem, Alice cannot clone such state and cannot know all the quantum information by measuring the qubit. Indeed, the parameters α and β can only be obtained if Alice has many copies of the state $|\varphi\rangle_{\mathrm{C}}$ and performs several measurements on them. It is important to note that the state $|\varphi\rangle_{\mathrm{C}}$ contains an infinite amount of classical information, parameterized by the complex (continuous) parameters α and β.

Quantum teleportation [27] allows Alice to send such qubit by sending Bob only two bits of classical information. The key resource to achieve such goal is a maximally entangled state between Alice and Bob. We recall the four Bell states, which are maximally entangled states forming a basis in the Hilbert space of two qubits

$$|\phi^{\pm}\rangle = \tfrac{1}{\sqrt{2}}\left(|00\rangle_{\mathrm{AB}} \pm |11\rangle_{\mathrm{AB}}\right), \qquad |\psi^{\pm}\rangle = \tfrac{1}{\sqrt{2}}\left(|01\rangle_{\mathrm{AB}} \pm |10\rangle_{\mathrm{AB}}\right). \tag{13.18}$$

Any Bell state can be used for quantum teleportation. Here we show how to achieve it with the state $|\psi^{-}\rangle_{\mathrm{AB}}$. Alice holds the unknown qubit $|\varphi\rangle_{\mathrm{C}}$ and her part of the entangled state, A. The total state shared by Alice and Bob can be written as

$$|\Psi\rangle_{\mathrm{CAB}} = |\varphi\rangle_{\mathrm{C}} \otimes |\psi^{-}\rangle_{\mathrm{AB}} \tag{13.19}$$

By expanding the state we obtain

$$|\Psi\rangle_{\mathrm{CAB}} = \tfrac{1}{\sqrt{2}}\left(\alpha|001\rangle_{\mathrm{CAB}} - \alpha|010\rangle_{\mathrm{CAB}} + \beta|101\rangle_{\mathrm{CAB}} - \beta|110\rangle_{\mathrm{CAB}}\right) \tag{13.20}$$

with the easy notation $|001\rangle_{\mathrm{CAB}} \equiv |0\rangle_C \otimes |0\rangle_A \otimes |1\rangle_B$. From the definition of the Bell states, it is possible to show that the following equalities hold

$$\begin{aligned} |00\rangle_{\mathrm{CA}} &= \tfrac{1}{\sqrt{2}}\left(|\phi^{+}\rangle + |\phi^{-}\rangle\right), \qquad |11\rangle_{\mathrm{CA}} = \tfrac{1}{\sqrt{2}}\left(|\phi^{+}\rangle - |\phi^{-}\rangle\right) \\ |01\rangle_{\mathrm{CA}} &= \tfrac{1}{\sqrt{2}}\left(|\psi^{+}\rangle + |\psi^{-}\rangle\right), \qquad |10\rangle_{\mathrm{CA}} = \tfrac{1}{\sqrt{2}}\left(|\psi^{+}\rangle - |\psi^{-}\rangle\right). \end{aligned}$$

Thus the total state can be written in the following form:

$$\begin{aligned} |\Psi\rangle_{\mathrm{CAB}} = \tfrac{1}{2}\big(&|\phi^{+}\rangle_{\mathrm{CA}} \otimes \sigma_x\sigma_z|\varphi\rangle_B + |\phi^{-}\rangle_{\mathrm{CA}} \otimes \sigma_x|\varphi\rangle_B \\ &-|\psi^{+}\rangle_{\mathrm{CA}} \otimes \sigma_z|\varphi\rangle_B - |\psi^{-}\rangle_{\mathrm{CA}} \otimes |\varphi\rangle_B\big). \end{aligned} \tag{13.21}$$

The above equation contains all the information needed to understand quantum teleportation. To complete the protocol, Alice needs to perform a measurement on the two qubits C and A. Indeed, she performs a *Bell measurement*, consisting in a projective measurement that distinguishes between the four orthogonal Bell states

$\{|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle\}$. If she obtains $|\phi^+\rangle$, relation (13.21) indicates that Bob obtains the state $\sigma_x\sigma_z|\varphi\rangle_B$. If she obtains $|\phi^-\rangle$, $|\psi^+\rangle$ or $|\psi^-\rangle$, Bob is left with the state $\sigma_x|\varphi\rangle_B$, $\sigma_z|\varphi\rangle_B$, or $|\varphi\rangle_B$, respectively. Then Alice communicates to Bob which state she has measured (since she has four possibilities, two classical bits are sufficient). Bob performs a different unitary transformation $\mathcal{U}$ depending on the outcomes obtained by Alice to recover the input state (unknown to both Alice and Bob). The operation performed by Bob is summarized in the following table:

Alice outcome	Bob Operation ($\mathcal{U}$)
$\|\phi^+\rangle$	$\sigma_z\sigma_x$
$\|\phi^-\rangle$	σ_x
$\|\psi^+\rangle$	σ_z
$\|\psi^-\rangle$	$\mathbb{1}$

It is important to underline that the Bell measurement gives no information on the input state $|\varphi\rangle_C$ and that for any input state Alice has equal probability, 1/4, of obtaining each of the four Bell states.

In the quantum teleportation protocol (Fig. 13.9), the input quantum state is not traveling between Alice and Bob: what is "traveling" is the *quantum information* contained in the parameters α and β. Indeed, it is worth noticing that the input and the teleported qubits can be implemented in different physical systems. For instance, the input qubit can be encoded in the polarization of a photon, while the teleported qubit can be represented by a two-energy-level atom system. Moreover, there is no

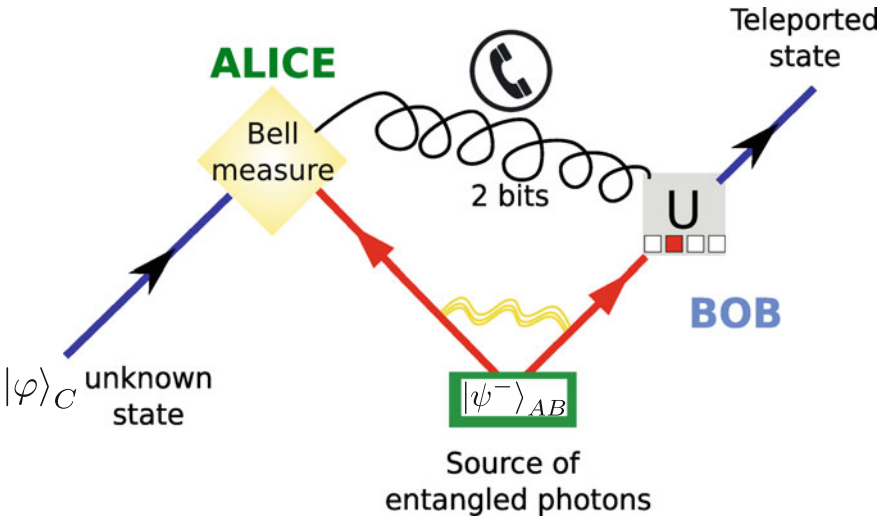

Fig. 13.9 Teleportation environment

contradiction with the no-cloning theorem: indeed, the unknown state vanishes at Alice's side and appears at Bob's location. Then there is no "cloning" of the input state.

Finally, even if the collapse of the wave function is instantaneous (at the moment in which Alice obtains her outcome), Bob's state immediately collapses to $\sigma_x\sigma_z|\varphi\rangle_B$, $\sigma_x|\varphi\rangle_B$, $\sigma_z|\varphi\rangle_B$, or $|\varphi\rangle_B$, a classical communication is necessary between Alice and Bob to correctly recover the input qubit. Then teleportation does not violate the "no faster than light" communication principle.

The first experimental demonstrations were performed with photons in Rome and Vienna in 1997 [28, 29]. Further experiments were realized with coherent states [30] and nuclear magnetic resonance [31]. Recent experiments reported quantum teleportation of photons along distances of more than 100 km [32, 33].

References

1. C. Weedbrook, S. Pirandola, R. García-Patrón, N.J. Cerf, T.C. Ralph, J.H. Shapiro, S. Lloyd, Gaussian quantum information. Rev. Mod. Phys. **84**, 621–669 (2012)
2. G. Marsaglia, Random numbers fall mainly in the planes. Proc. Natl. Acad. Sci. **61**(1), 25–28 (1968)
3. T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, A. Zeilinger, A fast and compact quantum random number generator. Rev. Sci. Instrum. **71**(4), paper no. 1675 (2000)
4. M. Fürst, H. Weier, S. Nauerth, D.G. Marangon, C. Kurtsiefer, H. Weinfurter, High speed optical quantum random number generation. Opt. Express **18**(12), 13029–13037 (2010)
5. M. Stipčević, B.M. Rogina, Quantum random number generator based on photonic emission in semiconductors. Rev. Sci. Instrum. **78**(4), paper no. 045104 (2007)
6. C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Mauerer, U.L. Andersen, C. Marquardt, G. Leuchs, A generator for unique quantum random numbers based on vacuum states. Nat. Photonics **4**(10), 711–715 (2010)
7. T. Symul, S.M. Assad, P.K. Lam, Real time demonstration of high bitrate quantum random number generation with coherent laser light. Appl. Phys. Lett. **1**, 2–5 (2011)
8. R.L. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM **21**(2), 120–126 (1978)
9. T. Elgamal, A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans. Inf. Theory **31**(4), 469–472 (1985)
10. National Institute of Standards and Technology (NIST), Advanced Encryption Standard (AES). *Federal Information Processing Standards*, Publication 197 (FIPS PUB 197), November 2001
11. National Institute of Standards and Technology (NIST), Secure Hash Standard (SHS), *Federal Information Processing Standards*, Publication 180-4 (FIPS PUB 180-4), March 2012
12. P.W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Comput. **26**(5), 1484–1509 (1997)
13. S. Wiesner, Conjugate coding. ACM SIGACT News **15**(1), 78–88 (1983)
14. W. Diffie, M.E. Hellman, New directions in cryptography. IEEE Trans. Inf. Theory **22**(6), 644–654 (1976)
15. C.H. Bennett, G. Brassard, in *Quantum cryptography: public-key distribution and coin tossing*. IEEE International Conference on Computers, Systems and Signal Processing (IEEE Computer Society, Bangalore, 1984), pp. 175–179
16. U.M. Maurer, Secret key agreement by public discussion from common information. J. IEEE Trans. Inf. Theory **39**(3), 733–742 (1993)

17. H.K. Lo, H. Chau, M. Ardehali, Efficient quantum key distribution scheme and a proof of its unconditional security. J. Cryptol. **18**(2), 133–165 (2004)
18. M. Tomamichel, C.C.W. Lim, N. Gisin, R. Renner, Tight finite-key analysis for quantum cryptography. Nat. Commun. **3**, 634 (2012)
19. D. Bacco, M. Canale, N. Laurenti, G. Vallone, P. Villoresi, Experimental quantum key distribution with finite-key security analysis for noisy channels. Nat. Commun. **4**, paper no. 2363, (2013)
20. C.H. Bennett, G. Brassard, N.D. Mermin, Quantum cryptography without Bell's theorem. Phys. Rev. Lett. **68**(5), 557–559 (1992)
21. A.K. Ekert, Quantum cryptography based on Bell's theorem. Phys. Rev. Lett. **67**, 661–663 (1991)
22. G. Vallone, A. Dall'Arche, M. Tomasin, P. Villoresi, Loss tolerant device-independent quantum key distribution: a proof of principle. New J. Phys. **16**(6), paper no. 063064 (2014)
23. D. Elkouss, J. Martinez-Mateo, V. Martin, Information reconciliation for quantum key distribution. Quantum Inf. Comput. **11**(3&4), 226–238 (2011)
24. C.H. Bennett, G. Brassard, C. Crepeau, U.M. Maurer, Generalized privacy amplification. IEEE Trans. Inf. Theory **41**(6), 1915–1923 (1995)
25. F. Grosshans, P. Grangier, Continuous variable quantum cryptography using coherent states. Phys. Rev. Lett. **88**(5), paper n. 057902 (2002)
26. F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N.J. Cerf, P. Grangier, Quantum key distribution using Gaussian-modulated coherent states. Nature **421**(6920), 41–238 (2003)
27. C.H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, W.K. Wootters, Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. Phys. Rev. Lett. **70**, 1895–1899 (1993)
28. D. Bouwmeester, J.W. Pan, K. Mattle, M. Eibl, H. Weinfurter, A. Zeilinger, Experimental quantum teleportation. Nature **390**, 575–579 (1997)
29. D. Boschi, S. Branca, F. De Martini, L. Hardy, S. Popescu, Experimental realization of teleporting an unknown pure quantum state via dual classical and Einstein-Podolsky-Rosen channels. Phys. Rev. Lett. **80**, 1121–1125 (1998)
30. A. Furusawa, J.L. Srensen, S.L. Braunstein, C.A. Fuchs, H.J. Kimble, E.S. Polzik, Unconditional quantum teleportation. Science **282**(5389), 706–709 (1998)
31. M.A. Nielsen, E. Knill, R. Laflamme, Complete quantum teleportation using nuclear magnetic resonance. Nature **396**(6706), 52–55 (1998)
32. J. Yin, J.G. Ren, H. Lu, Y. Cao, H.L. Yong, Y.P. Wu, C. Liu, S.K. Liao, F. Zhou, Y. Jiang, X.D. Cai, P. Xu, G.S. Pan, J.J. Jia, Y.M. Huang, H. Yin, J.Y. Wang, Y.A. Chen, C.Z. Peng, J.W. Pan, Quantum teleportation and entanglement distribution over 100-kilometre free-space channels. Nature **488**(7410), 185–188 (2012)
33. X.S. Ma, T. Herbst, T. Scheidl, D. Wang, S. Kropatschek, W. Naylor, B. Wittmann, A. Mech, J. Kofler, E. Anisimova, V. Makarov, T. Jennewein, R. Ursin, A. Zeilinger, Quantum teleportation over 143 kilometres using active feed-forward. Nature **489**(7415), 269–273 (2012)