Quantum Cyber-Security

S. Pirandola
[1] *Computer Science and York Centre for Quantum Technologies, University of York, York YO10 5GH, UK*

Lecture notes for the "Winter College on Optics: Quantum Photonics and Information" of the Abdus Salam International Centre for Theoretical Physics (Trieste, Italy, February 2020). These notes are excerpts adapted from the review "Advances in quantum cryptography" (arXiv:1906.01645).

I. LECTURE 1: BASIC NOTIONS IN QUANTUM KEY DISTRIBUTION

A. Generic aspects of a QKD protocol

We consider both discrete-variable systems, such as qubits or other quantum systems with finite-dimensional Hilbert space, and CV systems, such as bosonic modes of the electromagnetic field which are described by an infinite-dimensional Hilbert space. There a number of reviews and books on these two general areas (e.g., see Refs. [1, 2]). Some of the concepts are repeated below.

A generic "prepare and measure" QKD protocol can be divided in two main steps: quantum communication followed by classical postprocessing. During quantum communication the sender (Alice) encodes instances of a random classical variable α into non-orthogonal quantum states. These states are sent over a quantum channel (optical fiber, free-space link) controlled by the eavesdropper (Eve), who tries to steal the encoded information. The linearity of quantum mechanics forbids to perform perfect cloning [3, 4], so that Eve can only get partial information while disturbing the quantum signals. At the output of the communication channel, the receiver (Bob) measures the incoming signals and obtains a random classical variable β. After a number of uses of the channel, Alice and Bob share raw data described by two correlated variables α and β.

The remote parties use part of the raw data to estimate the parameters of the channel, such as its transmissivity and noise. This stage of parameter estimation is important in order to evaluate the amount of post-processing to extract a private shared key from the remaining data. Depending on this information, they in fact perform a stage of error correction (EC), which allows them to detect and eliminate errors, followed by a stage of privacy amplification (PA) that allows them to reduce Eve's stolen information to a negligible amount. The final result is the secret key.

Depending on which variable is guessed, we have direct or reverse reconciliation. In direct reconciliation (DR), it is Bob that post-process its outcomes in order to infer Alice's encodings. This procedure is usually assisted by means of forward classical communication (CC) from Alice to Bob. By contrast, in reverse reconciliation (RR), it is Alice who post-process her encoding variable in order to infer Bob's outcomes. This procedure is usually assisted by a final round of backward CC from Bob to Alice. Of course, one may more generally consider two-way procedures where the extraction of the key is helped by forward and feedback CCs, which may be even interleaved with the various communication rounds of the protocol.

Let us remark that there may also be an additional post-processing routine, called sifting, where the remote parties communicate in order to agree instances while discard others, depending on the measurement bases they have independently chosen. For instance this happens in typical DV protocols, where the Z-basis is randomly switched with the X-basis, or in CV protocols where the homodyne detection is switched between the q and the p quadrature.

Sometimes QKD protocols are formulated in entanglement-based representation. This means that Alice' preparation of the input ensemble of states is replaced by an entangled state Ψ_{AB} part of which is measured by Alice. The measurement on part A has the effect to conditionally prepare a state on part B. The outcome of the measurement is one-to-one with the classical variable encoded in the prepared states. This representation is particularly useful for the study of QKD protocols, so that their prepare and measure formulation is replaced by an entanglement-based formulation for assessing the security and deriving the secret key rate.

B. Asymptotic security and eavesdropping strategies

The asymptotic security analysis is based on the assumption that the parties exchange a number $n \gg 1$ (ideally infinite) of signals. The attacks can then be divided in three classes of increasing power: Individual, collective, and general-coherent. If the attack is individual, Eve uses a fresh ancilla to interact with each transmitted signal and she performs individual measurements on each output ancillary systems. The individual measurements can be done run-by-run or delayed at the end of the protocol, so that Eve may optimize over Alice and Bob's CC (also known as delayed-choice strategy). In the presence of an individual attacks, we have three classical variables for Alice, Bob and Eve, say α, β and γ. The asymptotic key rate is then given by the difference of the mutual information [5] I among the various parties according to Csiszar and Korner's classical theorem [6]. In DR (▶), we have the key rate

$$R^{\blacktriangleright} := I(\alpha : \beta) - I(\alpha : \gamma), \tag{1}$$

where $I(\alpha : \beta) := H(\alpha) - H(\alpha|\beta)$, with H being the Shannon entropy, and $H(|)$ its conditional version [5]. In RR ($\blacktriangleleft$), we have instead

$$R^{\blacktriangleleft} := I(\alpha : \beta) - I(\beta : \gamma), \tag{2}$$

If the attack is collective then Eve still uses a fresh ancilla for each signal sent but now her output ancillary systems are all stored in a quantum memory which is collectively measured at the end of the protocol after Alice and Bob's CCs. In this case, we may compute a lower bound to the key rate by replacing Eve's mutual information with Eve's Holevo information [7] on the relevant variable. In DR, one considers Eve's ensemble of output states conditioned to Alice's variable α, i.e., $\{\rho_{\mathrm{E}|\alpha}, P(\alpha)\}$ where $P(\alpha)$ is the probability of the encoding α. Consider then Eve's average state $\rho_{\mathrm{E}} := \int d\alpha P(\alpha)\rho_{\mathrm{E}|\alpha}$. Eve's Holevo information on α is equal to

$$I(\alpha : E) := S(\rho_{\mathrm{E}}) - \int d\alpha P(\alpha) S(\rho_{\mathrm{E}|\alpha}), \tag{3}$$

where $S(\rho) := -\mathrm{Tr}(\rho \log_2 \rho)$ is the von Neumann entropy. In RR, Eve's Holevo information on β is given by

$$I(\beta : E) := S(\rho_{\mathrm{E}}) - \int d\beta P(\beta) S(\rho_{\mathrm{E}|\beta}), \tag{4}$$

where $\rho_{\mathrm{E}|\beta}$ is Eve's output state conditioned to the outcome β with probability $P(\beta)$. Thus, we may write the two key rates [8]

$$R^{\blacktriangleright} := I(\alpha : \beta) - I(\alpha : E), \tag{5}$$
$$R^{\blacktriangleleft} := I(\alpha : \beta) - I(\beta : E). \tag{6}$$

In a general-coherent attack, Eve's ancillae and the signal systems are collectively subject to a joint unitary interaction. The ancillary output is then stored in Eve's quantum memory for later detection after the parties' CCs. In the asymptotic scenario, it has been proved [9] that this attack can be reduced to a collective one by running a random symmetrization routine which exploits the quantum de Finetti theorem [9–11]. By means of random permutations, one can in fact transform a general quantum state of n systems into a tensor product $\rho^{\otimes n}$, which is the structure coming from the identical and independent interactions of a collective attack.

II. PRELIMINARY NOTIONS

Recall that a qubit is represented as a vector in a bidimensional Hilbert space, which is drawn by the following basis vectors

$$|0\rangle \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle \equiv \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{7}$$

Any pure qubit state can thus be expressed as a linear superposition of these basis states,

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \cos(\theta/2)|0\rangle + e^{i\phi}\sin(\theta/2)|1\rangle, \tag{8}$$

with $\theta \in (0, \pi)$, $\phi \in (0, 2\pi)$ and i the imaginary unit. This state can be pictorially represented as a vector in the so-called "Bloch sphere". When $\theta = 0$ or $\theta = \pi$, we recover the basis states $|0\rangle$ and $|1\rangle$, respectively, which are placed at the poles of the sphere. When $\theta = \pi/2$, the qubit pure state is a vector lying on the equator of the sphere. Here we can identify the four vectors aligned along the $\hat{x}$ and $\hat{y}$ axes, which are obtained in correspondence of four specific values of ϕ, i.e., we have

$$\phi = 0 : \quad |+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \tag{9}$$

$$\phi = \pi : \quad |-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix}, \tag{10}$$

$$\phi = \pi/2 : \quad |+i\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ i \end{pmatrix}, \tag{11}$$

$$\phi = 3\pi/2 : |-i\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -i \end{pmatrix}. \tag{12}$$

The basis vectors in Eq. (7) are eigenstates of the Pauli operator (matrix)

$$\sigma_z = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{13}$$

We call them the "Z basis", as it is customary in QKD. Similarly, the states in Eqs. (9) and (10) are eigenstates of the Pauli operator (matrix)

$$\sigma_x = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \tag{14}$$

and are known as the X basis. Finally, the states in Eqs. (11) and (12) are eigenstates of the Pauli operator (matrix)

$$\sigma_y = Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \tag{15}$$

and are known as the Y basis. These pairs of eigenstates form two mutually unbiased bases (MUB). Formally, two orthogonal basis of a d-dimensional Hilbert space, say $\{|\psi_1\rangle, ..., |\psi_d\rangle\}$ and $\{|\phi_1\rangle, ..., |\phi_d\}\rangle$, are mutually unbiased if $|\langle\psi_i|\phi_j\rangle|^2 = 1/d$ for any i and j. Measuring a state of one MUB using the other basis would produce a completely random result.

Using the three Pauli matrices and the bidimensional identity operator (matrix)

$$\mathbb{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \tag{16}$$

it is possible to write the most generic state of a qubit in the form of a density operator,

$$\rho = \frac{1}{2}\mathbb{1} + \vec{n} \cdot \vec{\sigma}, \tag{17}$$

with $\vec{n}$ the Bloch vector and $\vec{\sigma} = \{\sigma_x, \sigma_y, \sigma_z\}$. This notation comes handy when the qubit states are mixed, which can be described with a vector $\vec{n}$ whose modulo is less than 1, as opposed to pure states, for which $|\vec{n}| = 1$.

To give a physical meaning to the representation of a qubit, we can interpret the qubit state in Eq. (8) as the polarization state of a photon. This is also known as "polarization qubit". In this case, the Bloch sphere is conventionally called the Poincaré sphere, but its meaning is unchanged. The basis vectors on the poles of the Poincaré sphere are usually associated with the linear polarization states $|H\rangle = |0\rangle$ and $|V\rangle = |1\rangle$, where H and V refer to the horizontal or vertical direction of oscillation of the electromagnetic field, respectively, with respect to a given reference system. The X basis states are also associated with linear polarization but along diagonal ($|D\rangle = |+\rangle$) and anti-diagonal ($|A\rangle = |-\rangle$) directions. Finally, the Y basis states are associated with right-circular ($|R\rangle = |+i\rangle$) and left-circular ($|L\rangle = |-i\rangle$) polarization states. Any other state is an elliptical polarization state and can be represented by suitably choosing the parameters θ and ϕ.

It is worth noting that polarization can be cast in one-to-one correspondence with another degree of freedom of the photon which is particularly relevant from an experimental point of view. This is illustrated in Fig. 1. The light source emits a photon that is split into two arms by the first beam-splitter (BS). The transmission of this BS represents the angle θ of the Bloch sphere. More precisely, if r and t are the reflection and transmission coefficients of the BS, respectively, such that $|r|^2 + |t|^2 = 1$, we can write $r = \cos(\theta/2)$ and $t = e^{i\phi}\sin(\theta/2)$ so to recover Eq. (8). If the BS is 50:50, then $\theta = \pi/2$ and the state after the BS becomes

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\phi}|1\rangle\right). \tag{18}$$

The phase ϕ now has a clear physical meaning, i.e., it represents the relative electromagnetic phase between the upper and lower arms of the interferometer in Fig. 1. This phase can be modified by acting on the phase shifters in Fig. 1 and this is one of the most prominent methods to encode and decode information in QKD. In fact, it is fair to say that the vast majority of QKD experiments were performed using either the polarization or the relative phase to encode information.

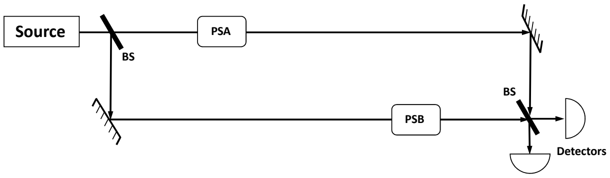

FIG. 1. Fundamental phase-based interferometer. BS: beam-splitter; PSA: phase shift Alice; PSB: phase shift Bob. Adapted with permission from Ref. [20] ©APS (1992).

III. HISTORICAL DEVELOPMENT OF QKD

As we well know, from a historical perspective, the first QKD protocols were introduced using DVs, especially polarization. This remains even today one of the simplest ways to describe an otherwise complex subject. The seminal BB84 protocol [12] was described using polarization. In 1991 Ekert suggested a scheme, the "E91" [15], that for the first time exploits entanglement for cryptographic purposes. The conceptual equivalence of this scheme with the BB84 protocol was demonstrated in 1992 by Bennett, Brassard and Mermin [16], who also proposed a simplified version of the E91 later called BBM92 or more simply Einstein-Podolsky-Rosen (EPR) scheme. However, this supposed equivalence cannot be taken strictly as it can be shown that the entangled based protocol of E91 can provide device independent security, which is impossible for the BB84 using separable states even in a noise free scenario [17].

A few years later, Lo and Chau [18] and Shor and Preskill [19] exploited this equivalence between the prepare-and-measure BB84 and the entanglement-based BBM92 to demonstrate the unconditional security of the BB84 protocol. Another important protocol, the "B92" [20], was proposed in 1992 by Bennett, showing that QKD can be performed with even only two non-orthogonal states [3, 4]. The idea of exploiting non-orthogonality was later extended to more sophisticated bipartite schemes by Goldenberg and Vaidman [21], Koashi and Imoto [23] and Noh [22]. Even though these protocols are based on bipartite states that are orthogonal, their security relies on the fact the eavesdropper cannot simultaneously access both the systems prepared by the sender, but only one of them which is instead described by non-orthogonal states [24]. Finally, note that non-orthogonality also has a bipartite formulation in terms of quantum discord [25, 26], so that the presence of the latter can be shown to be a necessary (but not sufficient) condition for security [27].

In the following, we outline the most intuitive and practical DV-QKD protocols, called "prepare-and-measure" protocols. The transmitting user, Alice, prepares the signals by encoding a discrete random variable (typically a binary variable) in a quantum system with finite degrees of freedom, typically the polarization of an optical photon (polarization qubit). These signals are then sent to the receiving user, Bob, who measures them in order to retrieve the encoded information. In order to describe the modus operandi of the various protocols, here we assume the ideal case of single-photon sources.

IV. BB84 PROTOCOL

In the BB84 protocol with polarization qubits, Alice prepares a random sequence of four states in two MUBs.

These are usually chosen as $|0\rangle$, $|1\rangle$ (Z basis), and $|+\rangle$, $|-\rangle$ (X basis). However, other choices are possible, including the four states in Eqs. (9)-(12). The users associate the binary digit 0 with the non-orthogonal states $|0\rangle$ and $|+\rangle$, and the binary digit 1 with the other non-orthogonal states $|1\rangle$ and $|-\rangle$. The non-orthogonality condition guarantees that Eve (an eavesdropper) cannot clone the states with perfect fidelity [3, 4]. This implies that: (i) Eve cannot perfectly retrieve the information encoded by Alice; and (ii) Eve's action causes a disturbance on the quantum states that can be detected by the legitimate users.

The states prepared by Alice are sent to Bob, who then measures them in one of the two bases Z or X, selected at random. See Table I. Note that, if Bob chooses the same basis as Alice, then Bob should exactly decode Alice's input. By contrast, If Bob chooses the wrong basis, his result, and thus the bit he reads, will be random. For this reason, when the quantum communication is over, Bob exploits a classical public channel to inform Alice about what basis he used to measure each photon. Alice reports back her bases and they discard all the events corresponding to the use of different bases. After this sifting operation, the two parties should have two identical strings of bits, forming the so-called "sifted key".

In practice, however, the communication line is noisy and this noise has to be fully ascribed to Eve in the worst-case scenario. Because of the noise, Alice's and Bob's local strings will differ by an amount that can be quantified in terms of "quantum bit error rate" (QBER). This is defined as the probability that a generic bit in Bob's sifted string is different from the corresponding bit in Alice's sifted string. In order to compute the QBER, Alice and Bob perform a session of parameter estimation, where they agree to disclose a random subset of their data. Comparing these bits (later discarded), they can quantify the QBER and check if this is lower or higher than a certain security threshold of the protocol. If it is higher, it means that Eve has gain too much information. If it is lower, it means that the parties have more shared information than Eve, and they can use the classical procedures of EC and PA to derive a secret key. As a first step, they implement EC so that their strings are transformed into shorter but identical strings. Then, they implement PA, so that their common string is further shortened into a final form which is completely decoupled from Eve.

A. Intercept-resend against the BB84 protocol

We now describe a basic eavesdropping strategy, where Eve measures Alice's signal states and, from the outcomes, she re-prepares states to be sent to Bob. This strategy is here discussed to give an idea of how eavesdropping information automatically generates a non-trivial QBER for the parties. Assume that Alice prepares her states in the Z basis and assume that this is an instance where Bob picks the same basis for his measurement, so that the instance survives the sifting stage of the protocol. For the same instance, Eve will implement randomly either the Z or the X basis. With 50% probability, she applies the right basis Z, eavesdropping all the input information without causing any noise. With 50% probability, she applies the wrong basis X, therefore projecting Alice's input into $|+\rangle$ or $|-\rangle$ with the same probability. In this case, Eve does not retrieve any information and will randomize the system, so that Bob will also get a random output which coincides with Alice's input 50% of the times. The reasoning is similar if we start from the other basis X. See Table II for the complete scenario.

Alice's encoding			Bob's decoding	
basis	bit	state	Z	X
Z	0	$\lvert 0\rangle$	0	?
	1	$\lvert 1\rangle$	1	?
X	0	$\lvert +\rangle$	?	0
	1	$\lvert -\rangle$	?	1

TABLE I. Summary of Alice's encoding (left) and Bob's decoding (right) in BB84. Here "?" means that the output is completely random, i.e., 0 or 1 with the same probability.

The noise induced by this attack is quite high, corresponding to a QBER of 25% (above the security threshold of the protocol, equal to $\simeq 11\%$ as discussed afterwards). It is also clear that Eve gets at least the same information as Bob (so that the key rate is zero). More exactly, Eve is able to steal half of the sifted bits, while Alice and Bob's mutual information is given by $1 - H_2(\text{QBER}) \simeq 0.19$ key bits per sifted bit, where

$$H_2(p) := -p \log_2 p - (1-p)\log_2(1-p) \qquad (19)$$

is binary Shannon entropy. By accounting of the sifting process, we may add a factor 1/2 and consider the information per use of the protocol or channel use. We have then $[1 - H_2(\text{QBER})]/2 < 0.1$ per channel use, compared to 0.25 bits per channel use stolen by Eve. Note also that the formula of the mutual information does not change if we use the probability of success $1 - \text{QBER}$, since the binary entropy is invariant under the exchange $p \to 1-p$.

B. Intercept-resend with an intermediate basis

The performance of the intercept-resend attack does not substantially change if Eve, instead of randomizing her measurement between the two MUBs Z and X, always applies an intermediate basis. Consider the orthogonal basis $\{|\theta\rangle, |\theta^\perp\rangle\}$, where

$$|\theta\rangle = \cos(\theta/2)|0\rangle + e^{i\phi}\sin(\theta/2)|1\rangle, \qquad (20)$$

$$|\theta^\perp\rangle = \sin(\theta/2)|0\rangle - e^{-i\phi}\cos(\theta/2)|1\rangle. \qquad (21)$$

Encoding				
basis	bit	state	Eve	Decoding after sifting
Z	0 1	$\lvert 0\rangle$ $\lvert 1\rangle$	↗ $Z\begin{cases}\lvert 0\rangle\\ \lvert 1\rangle\end{cases}$	$\longrightarrow Z\begin{cases}0\\ 1\end{cases}$
			↘ $X\begin{cases}\lvert +,-\rangle\\ \lvert +,-\rangle\end{cases}$	$\longrightarrow Z\begin{cases}?\\ ?\end{cases}$
X	0 1	$\lvert +\rangle$ $\lvert -\rangle$	↗ $Z\begin{cases}\lvert 0,1\rangle\\ \lvert 0,1\rangle\end{cases}$	$\longrightarrow X\begin{cases}?\\ ?\end{cases}$
			↘ $X\begin{cases}\lvert +\rangle\\ \lvert -\rangle\end{cases}$	$\longrightarrow X\begin{cases}0\\ 1\end{cases}$

TABLE II. BB84 scenario after sifting in the presence of an intercept-resend attack (where Eve randomly switches between Z and X bases). Here "?" means that the output value decoded by Bob is completely random, i.e., 0 or 1 with the same probability. When Eve's basis matches Alice's, then no error is introduced. When Eve's basis is different from Alice's, Eve re-sends states from the other MUB and Bob gets a random output, coinciding with Alice's input 50% of the times. As a result, we have a QBER of 25%. It is clear that Eve retrieves at least the same information as Bob. As a matter of fact, she steals half of the sifted bits. On the other hand Bob, can only reconstruct $\simeq$ 19% of the sifted bits due to the fact that, in correcting his data, he does not know which instances were perfectly eavesdropped and which ones were completely randomized by Eve.

Here the choice of parameters is not limited to $\theta = 0$ (Z basis) or $\theta = \pi/2$ and $\phi = 0$ (X basis). Another possible choice is for instance $\theta = \pi/4$ and $\phi = 0$, i.e., the so-called "Breidbart basis". In general, Eve associates Alice's bit-value 0 (i.e., her states $|0\rangle$ and $|+\rangle$) to the outcome θ, and Alice's bit-value 1 (i.e., her states $|1\rangle$ and $|-\rangle$) to the other outcome θ. It is easy to compute the conditional probabilities

$$P(\theta|0) = P(\theta^{\perp}|1) = \cos^2(\theta/2), \tag{22}$$

$$P(\theta|+) = P(\theta^{\perp}|-) = \frac{1+\sin\theta\cos\phi}{2}. \tag{23}$$

and their complementary quantities ($p \to 1-p$)

$$P(\theta^{\perp}|0) = P(\theta|1) = \sin^2(\theta/2), \tag{24}$$

$$P(\theta^{\perp}|+) = P(\theta|-) = \frac{1-\sin\theta\cos\phi}{2}. \tag{25}$$

Assuming the sifted scenario where the basis Z or X is known to Eve, then we can easily compute the success probability of Eve guessing Alice's input, starting from the probabilities above and using Bayes' theorem with identical priors. For instance, assume that Alice is using the Z basis and sending the state $|0\rangle$. The probability for Eve to guess the input 0 given her outcome θ is given by $\mathrm{P}(0|\theta) = \mathrm{P}(\theta|0) = \cos^2(\theta/2)$. In fact, from Bayes' theorem, we may write

$$P(0|\theta) = \frac{P(\theta|0)P(0)}{P(\theta)}, \tag{26}$$

$$P(\theta) = P(\theta|0)P(0) + P(\theta|1)P(1). \tag{27}$$

Then, using the conditional probabilities in Eqs. (22)-(25) and the equal priors $P(0) = P(1) = 1/2$ (due to Alice's random input), we get the result above. We find similar results for the other cases, so that we may write

$$P(0|\theta) = P(1|\theta^{\perp}) = \cos^2(\theta/2) := P_E^Z, \tag{28}$$

$$P(+|\theta) = P(-|\theta^{\perp}) = \frac{1+\sin\theta\cos\phi}{2} := P_E^X. \tag{29}$$

Given Eve's probabilities of success, P_E^Z and P_E^X, of decoding Alice's sifted bit in the two bases, Z and X, we can compute the corresponding expressions for Alice and Eve's mutual information. These are given by $I_E^Z = 1 - H_2(P_E^Z)$ and $I_E^X = 1 - H_2(P_E^X)$. Considering that Alice randomly switches between bases Z and X, Eve's information is therefore given by the average $I_E = (I_E^Z + I_E^X)/2$. We can now see that, for the specific case of the Breidbart basis ($\theta = \pi/4$, $\phi = 0$), we have the symmetric scenario $P_E^Z = P_E^X := P_E$, where Eve's overall probability of guessing Alice's sifted bit is given by $P_E = (1 + 1/\sqrt{2})/2 \simeq 0.854$ (which is higher than the 75% value of the previous intercept-resend attack with switching bases). In the present attack, Eve is able to eavesdrop $I_E = 1 - H_2(P_E) \simeq 0.4$ bits per sifted bit, which is less than the 50% value of the previous intercept-resend attack with switching bases (the apparent discrepancy of the performance between guessing probability and mutual information can be understood in terms of the concavity of the Shannon entropy).

Let us now compute the QBER, first assuming the general basis in Eqs. (20) and (21), and then specifying the result for the Breidbart basis. Let us start by considering the Z basis, with Alice sending $|0\rangle$. When Eve projects the incoming polarization qubit onto the state $|\theta\rangle$, with probability $P(\theta|0) = \cos^2(\theta/2)$, Bob gets an erroneous result with probability $P(1|\theta) = \sin^2(\theta/2)$. If Eve projects onto $|\theta^{\perp}\rangle$, with probability $P(\theta^{\perp}|0) = \sin^2(\theta/2)$, Bob has an error with probability $P(1|\theta^{\perp}) = \cos^2(\theta/2)$. Therefore, we find the error probability

$$\begin{aligned} P(1|0) &= P(1|\theta)P(\theta|0) + P(1|\theta^{\perp})P(\theta^{\perp}|0) \\ &= 2\cos^2(\theta/2)\sin^2(\theta/2) = (\sin^2\theta)/2. \end{aligned} \tag{30}$$

It is easy to check that the error probability has the same expression when Alice sends $|1\rangle$, so that we may write $P_{\mathrm{err}}^Z = P(0|1) = P(1|0)$ for the Z basis.

A similar calculation can be done when Alice uses the X basis sending $|+\rangle$ or $|-\rangle$. One finds $P_{\mathrm{err}}^{X} = P(-|+) = P(+|-) = (1 - \sin^2\theta\cos^2\phi)/2$. As a result, the average error probability (QBER) is equal to

$$P_{\mathrm{err}} = (P_{\mathrm{err}}^{Z} + P_{\mathrm{err}}^{X})/2 = [1 + (1 - \cos^2\phi)\sin^2\theta]/4. \quad (31)$$

For the Breidbart basis, a simple replacement in Eq. (31) provides a QBER of 25%, exactly as in the previous attack with switching bases. Alice and Bob's mutual information is again $\simeq 0.19$ key bits per sifted bit, lower than Eve's stolen information ($\simeq 0.4$), so that no secret key can be generated.

C. Optimal eavesdropping strategy of the BB84 protocol

A more powerful strategy that Eve can consider is to attach an ancilla E (i.e., a quantum system with possibly higher dimension than a qubit) to the incoming Alice's qubit. Let its state $|E\rangle$ unitarily interact with Alice's qubit state in the hope of gleaning some information. With respect to Alice computational Z basis $\{|0\rangle, |1\rangle\}$, this unitary interaction can be written as

$$U|0\rangle|E\rangle = |0\rangle|F_0\rangle + |1\rangle|D_0\rangle, \quad (32)$$
$$U|1\rangle|E\rangle = |1\rangle|F_1\rangle + |0\rangle|D_1\rangle, \quad (33)$$

with $|F_{0,1}\rangle$ and $|D_{0,1}\rangle$ being Eve's ancillary states after the interaction; these are generally non-orthogonal and un-normalized. There are two points worth noting here; firstly, the Stinespring dilation theorem allows us to limit our consideration of Eve's ancillae to a four dimensional quantum system or two qubits. Secondly, the interaction with respect to Alice's X basis $\{|+\rangle, |-\rangle\}$ is automatically determined using linearity. In both bases, the attack can compactly be expressed by

$$U|a\rangle|E\rangle = |a\rangle|F_a\rangle + |a^{\perp}\rangle|D_a\rangle, \quad (34)$$

where $|a\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and $\langle a|a^{\perp}\rangle = 0$. In particular, the relation between Eve's states in the two bases is given by

$$\begin{aligned} 2\,|F_{\pm}\rangle &= |F_0\rangle + |F_1\rangle \pm |D_0\rangle \pm |D_1\rangle \\ 2\,|D_{\pm}\rangle &= |F_0\rangle - |F_1\rangle \mp |D_0\rangle \pm |D_1\rangle\,. \end{aligned} \quad (35)$$

In this formalism it is easy to write an optimal collective attack which is able to saturate the minimum QBER associated with the security of the BB84 protocol. This collective attack was shown in Ref. [29], building on the individual symmetric attack described in Ref. [30, 31]. Assume that the unitary U is such that Eve's un-normalized states are orthogonal of the following form (in Eve's two-qubit computational basis)

$$\begin{aligned} |F_0\rangle &= \left(\sqrt{F},\ 0,\ 0,\ 0\right)^T \\ |F_1\rangle &= \left(\sqrt{F}\cos x,\ 0,\ 0,\ \sqrt{F}\sin x\right)^T \\ |D_0\rangle &= \left(0,\ \sqrt{D},\ 0,\ 0\right)^T \\ |D_1\rangle &= \left(0,\ \sqrt{D}\cos y,\ \sqrt{D}\sin y,\ 0\right)^T. \end{aligned} \quad (36)$$

where x, y are two arbitrary angles, $F = 1 - D$ and

$$D = \frac{1 - \cos x}{2 - \cos x + \cos y}. \quad (37)$$

This choice is such that $\langle F_a\,|F_a\rangle = F$, $\langle D_a\,|D_a\rangle = D$, $\langle F_a\,|F_{a^{\perp}}\rangle = F\cos x$, $\langle D_a\,|D_{a^{\perp}}\rangle = D\cos y$ and all the other inner products are zero, i.e., we have $\langle F_a\,|D_a\rangle = 0$ and $\langle F_a\,|D_{a^{\perp}}\rangle = 0$. We can see that the attack acts symmetrically in the two bases. Combining this choice with Eq. (34), it is easy to see that the term F represents the fidelity (probability of Bob getting the same state $|a\rangle$ sent by Alice), while D is the QBER, i.e., the probability that Bob finds the state $|a^{\perp}\rangle$ instead of $|a\rangle$. In fact, from the conditional total output state $\rho_{BE|a} := U\,|a\rangle\,\langle a| \otimes |E\rangle\,\langle E|\,U^{\dagger}$ one can check that Bob's conditional state

$$\begin{aligned} \rho_{B|a} &:= \mathrm{Tr}_E\left(\rho_{BE|a}\right) \\ &= F^{-1}\,\langle F_a|\,\rho_{BE|a}\,|F_a\rangle + D^{-1}\,\langle D_a|\,\rho_{BE|a}\,|D_a\rangle \end{aligned} \quad (38)$$

is given by

$$\rho_{B|a} = F\,|a\rangle\,\langle a| + D\,\left|a^{\perp}\right\rangle\left\langle a^{\perp}\right|, \quad (39)$$

while Eve's conditional output state is given by

$$\rho_{E|a} = |F_a\rangle\,\langle F_a| + |D_a\rangle\,\langle D_a|\,. \quad (40)$$

From Eq. (39) we can easily see that Alice and Bob's mutual information is equal to $I_{AB} = [1 - H_2(D)]/2$ where the factor 1/2 accounts for the basis reconciliation (sifting) and H_2 is the binary Shannon entropy.

Let us compute the performance of this attack assuming it is an individual (delayed-choice) attack [30, 31]. Eve can store the ancilla in a memory in order to wait for the basis reconciliation. She can then keep the same instances of Alice and Bob and make individual measurements on her ancillas. Eve can first measure $\rho_{E|a}$ to distinguish between the orthogonal sets $\{|F_a\rangle\}$ and $\{|D_a\rangle\}$ and then she can perform a further measurement to distinguish between the non-orthogonal states $|F_a\rangle$ and $|F_{a^{\perp}}\rangle$ or between the other non-orthogonal states $|D_a\rangle$ and $|D_{a^{\perp}}\rangle$. Because two states with overlap $\cos x$ can be distinguish with probability $(1 + \sin x)/2$ [32], we have that Eve guesses the correct state up to an error

$$p_{\mathrm{Eve}} = F\left(\frac{1 + \sin x}{2}\right) + D\left(\frac{1 + \sin y}{2}\right)\,. \quad (41)$$

At fixed QBER D, this probability is minimized by the choice $x = y$, so that Eve's attack is reduced to just one parameter x. In this case, we can write $D=(1-\cos x)/2$ and the following expression of Alice and Eve's mutual information

$$I_{AE}=\left[1-H_2\left(\tfrac{1+\sin x}{2}\right)\right]/2\ . \tag{42}$$

By imposing the condition $I_{AB}=I_{AE}$, one finds the following threshold value for the QBER [30, 31]

$$D=\frac{1-1/\sqrt{2}}{2}\simeq 14.6\%\ . \tag{43}$$

Let us now consider a collective version of this attack [29], where Eve is not limited to individual measurements on her ancillas, but she is allowed to perform an optimal coherent measurement on all of them. Her accessible information is therefore upper bounded by her Holevo information χ_{AE} on Alice's variable. Due to the symmetry of the attack in the two bases, without losing generality we can assume that the sifted instances are all coming from the Z basis, i.e., $a\in\{0,1\}$. With respect to the sifted data, Eve's Holevo bound is given by

$$\chi_{AE}=S(\rho_E)-\frac{S(\rho_{E|a})+S(\rho_{E|a^{\perp}})}{2}\ , \tag{44}$$

where S is the von Neumann entropy, and $\rho_E:=(\rho_{E|a}+\rho_{E|a^{\perp}})/2$ is Eve's average output state. Setting $x=y$, one can compute $\chi_{AE}=H_2(D)$. Including the sifting $1/2$ factor and computing the rate $R=I_{AB}-\chi_{AE}$ (bits per use), we get [29]

$$R_{\mathrm{BB84}}=[1-2H_2(D)]/2\ , \tag{45}$$

which corresponds to the unconditionally-secure key-rate of the BB84 protocol [19] with a threshold QBER of $D\simeq 11\%$. Thus, the collective symmetric attack is an optimal eavesdropping strategy against the BB84 protocol. It is optimal in the sense that it provides the lowest security threshold for the protocol.

D. Unconditional security of the BB84 protocol

This security threshold value of 11% is the same as the one that is found by assuming the most general 'coherent attack' against the protocol, where all the signal states undergo a joint unitary interaction together with Eve's ancillae, and the latter are jointly measured at the end of protocol. In this general case, the unconditional security of the BB84 protocol was provided by Shor and Preskill [19]. The main idea was based on the reduction of a QKD protocol into an entanglement distillation protocol (EDP). Given a set of non-maximally entangled pairs, the EDP is a procedure to *distill* a smaller number of entangled pairs with a higher degree of entanglement using only local operations and classical communication (LOCC). In some ways, employing this for a security proof for QKD actually makes perfect sense as it involves the two parties ending with a number of maximally entangled pairs. Given the monogamous nature of entanglement, no third party can be privy to any results of subsequent measurements the two make.

In particular, Shor and Preskill [19] showed that EDP can be done using quantum error correction codes, namely the Calderbank-Shor-Steane (CSS) code [33–35] which has the interesting property which decouples phase errors from bit errors. This allows for corrections to be made independently. In this way, one can show that the key generation rate becomes

$$R_{\mathrm{BB84}}=\left[1-H_2(e_b)-H_2(e_p)\right]/2, \tag{46}$$

where e_b and e_p are bit and phase error rates. For $e_b=e_p=D$, this results in the same formula of Eq. (45) and it is simple to see that $R=0$ for QBER $D\approx 11\%$.

It is important to say that a more refined analysis of the secret key rate of the BB84 protocol should account for other imperfections, such as the finite efficiency of EC and the probability Q that Alice's (single-photon) pulses are effectively detected by Bob. Thus, one has the rate

$$R_{\mathrm{BB84}}=\frac{Q}{2}\left[1-H_2(D)-\mathrm{leak}_{\mathrm{EC}}(D)\right], \tag{47}$$

where $\mathrm{leak}_{\mathrm{EC}}(D)=f(D)H_2(D)$ is the leakage of information due to EC, with $f(D)\geq 1$ being the EC efficiency. It is interesting to derive the optimal scaling of the BB84 protocol, by setting $E=0$ in Eq. (47) and noticing that $Q=\eta$, so that we get

$$R_{\mathrm{BB84}}^{\mathrm{ideal}}=\frac{\eta}{2}. \tag{48}$$

In conclusion, it is worth to mention the 'efficient' version of the BB84 protocol, where the sifting factor 1/2 can be eliminated from the rate [36]. The idea is to make a bias used of the bases so that, e.g., the Z basis is chosen with probability p and the X basis with probability $1-p$. Instead of the standard choice of $p=1/2$, one can adopt a very asymmetric choice, so that $p\to 1^{-}$, meaning that the parties almost always use the Z basis. In the limit of large number of uses $n\to\infty$, the scheme turns out to be unconditionally secure, even though the exact choice $p=0$ would make it completely insecure at any n. Therefore, the secret key rate of the efficient BB84 protocol is given by

$$R_{\text{eff-BB84}}=1-2H_2(D). \tag{49}$$

Accounting for imperfections, it becomes the double of Eq. (47), and it leads to the ideal scaling $R_{\text{eff-BB84}}^{\mathrm{ideal}}=\eta$.

V. SIX-STATE PROTOCOL

The BB84 protocol has also been extended to use six states in three bases to enhance the key generation rate and the tolerance to noise [37]. The 6-state protocol is identical to BB84 except, as its name implies, rather than using two or four states, it uses six states on three bases X, Y and Z. This creates an obstacle to the eavesdropper who has to guess the right basis from among three possibilities rather than just two of the BB84. This extra choice causes the eavesdropper to produce a higher rate of error, for example, 1/3 when attacking all qubits with a simple intercept-resend strategy, thus becoming easier to detect. The unconditional key rate against coherent attacks has the following expression in terms of the QBER D (including the sifting factor 1/3)

$$R_{6\text{state}} = \frac{1}{3}\left[1 + \frac{3D}{2}\log_2\frac{D}{2} + \left(1-\frac{3D}{2}\right)\log_2\left(1-\frac{3D}{2}\right)\right], \tag{50}$$

which gives a security threshold value of about 12.6%, slightly improving that of the BB84 protocol [37–39]. An optimal attack achieving this rate is again provided by a symmetric collective attack [29].

Before moving on, it is worth noting that the symmetric attacks described in both the BB84 protocol as well as the 6-state protocol are equivalent to the action of quantum cloning machines (QCMs) [40]. Notwithstanding the no-cloning theorem, QCMs imperfectly clone a quantum state, producing a number of copies, not necessarily of equal fidelity. QCMs which result in copies that have the same fidelity are referred to as symmetric. In the case of the BB84, the states of interest come from only 2 MUBs, hence the relevant QCM would be the *phase covariant* QCM which clones all the states of the equator defined by two MUBs (the term 'phase covariant' comes from the original formulation of the QCM cloning states of the form $(|0\rangle + e^{i\phi}|1\rangle)/\sqrt{2}$ independently of ϕ [41]; this QCM thus copies equally well the states from the X and Y bases). As for the 6-state protocol, the relevant QCM is universal, meaning that it imperfectly clones all states from 3 MUBs with the same fidelity.

VI. B92 PROTOCOL

In 1992, Charles Bennett proposed what is arguably the simplest protocol of QKD, the "B92" [20]. It uses only two states to distribute a secret key between the remote parties. This is the bare minimum required to transmit one bit of a cryptographic key. More precisely, in the B92 protocol, Alice prepares a qubit in one of two quantum states, $|\psi_0\rangle$ and $|\psi_1\rangle$, to which she associates the bit values 0 and 1, respectively. The state is sent to Bob, who measures it in a suitable basis, to retrieve Alice's bit. If the states $|\psi_0\rangle$, $|\psi_1\rangle$ were orthogonal, it is always possible for Bob to deterministically recover the bit. For instance, if $|\psi_0\rangle = |0\rangle$ and $|\psi_1\rangle = |1\rangle$, Bob can measure the incoming states in the Z basis and recover the information with 100% probability.

However, Bob's ability to retrieve the information without any ambiguity also implies that Eve can do it too. She will measure the states midway between Alice and Bob, deterministically retrieve the information, prepare new states identical to the measured ones, and forward them to Bob, who will never notice any difference from the states sent by Alice. Orthogonal states are much alike classical ones, that can be deterministically measured, copied and cloned. Technically, the orthogonal states are eigenstates of some common observable, thus measurements made using that observable would not be subjected to any uncertainty. The no-cloning theorem [3, 4] does not apply to this case.

By contrast, measurements will be bounded by inherent uncertainties if Alice encodes the information in two non-orthogonal states, for example the following ones:

$$|\psi_0\rangle = |0\rangle, \quad |\psi_1\rangle = |+\rangle, \quad \langle\psi_0|\psi_1\rangle = s \neq 0. \tag{51}$$

As Bennett showed in his seminal paper [20], any two non-orthogonal states, even mixed, spanning disjoint subspaces of the Hilbert space can be used. In the actual case, the scalar product s is optimized to give the best performance of the protocol. For the states in Eq. (51), this parameter is fixed and amounts to $1/\sqrt{2}$; i.e. the states are derived from bases which are mutually unbiased one to the other. Given the complementary nature of the observables involved in distinguishing between these states, neither Bob nor Eve can measure or copy the states sent by Alice with a 100% success probability. However, while Alice and Bob can easily overcome this problem (as described in the following) and distil a common bit from the data, Eve is left with an unsurmountable obstacle, upon which the whole security of the B92 protocol is based.

In B92, Bob's decoding is peculiar and worth describing. It is a simple example of "unambiguous state discrimination" (USD) [42, 43]. To explain it, it is useful to remember that the state $|0\rangle$ ($|+\rangle$) is a Z (X) eigenstate and that $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$, as it is easy to verify from Eqs. (7), (9) and (10). Suppose first that Alice prepares the input state $|\psi_0\rangle = |0\rangle$. When Bob measures it in the Z basis, he will obtain $|0\rangle$ with probability 100% whereas when he measures it in the X basis, he will obtain either $|+\rangle$ or $|-\rangle$ with probability 50%. In particular, there is one state that Bob will never obtain, which is $|1\rangle$. Now suppose that Alice prepares the other state of B92, i.e., $|\psi_1\rangle = |+\rangle$. Bob will still measure in the same bases as before but in this case, if we repeat the previous argument, we conclude that Bob can never obtain the state $|-\rangle$ as a result. See Table III for a schematic representation of Bob's outcomes and their probabilities (P) depending on Alice's encoding state and Bob's chosen basis for measurement:

From Table III it is clear that, for the conditional probability $P(a|b)$ of guessing Alice's encoding a given Bob's outcome b, we may write

$$\mathrm{P}(+|1) = \mathrm{P}(0|-) = 1. \tag{52}$$

In other words, Bob can logically infer that when he detects $|1\rangle$, Alice must have prepared the state $|+\rangle$, so he

Alice	Bob (Z)	Bob (X)
$\|0\rangle$	$\|0\rangle\,,\ \mathrm{P}=1$	$\|+\rangle\,,\ \mathrm{P}=1/2$
	$\|1\rangle\,,\ \mathrm{P}=0$	$\|-\rangle\,,\ \mathrm{P}=1/2$
$\|+\rangle$	$\|0\rangle\,,\ \mathrm{P}=1/2$	$\|+\rangle\,,\ \mathrm{P}=1$
	$\|1\rangle\,,\ \mathrm{P}=1/2$	$\|-\rangle\,,\ \mathrm{P}=0$

TABLE III.

decodes the bit as '1', whereas when he detects $|-\rangle$, Alice must have prepared the state $|0\rangle$ so he decodes the bit as '0'. Whenever he detects any other state, Bob is unsure of Alice's preparation and the users decide to simply discard these "inconclusive" events from their records.

This way, using this sort of "reversed decoding", which is typical of USD, and his collaboration with Alice, Bob manages to decode the information encoded by Alice. Despite the fact that USD can also be used by Eve, the unconditional security of the B92 protocol was rigorously proven in [44] for a lossless scenario and then extended to a lossy, more realistic, case in [45], under the assumption of single photons prepared by Alice. This assumption is not necessary in the B92 version with a strong reference pulse, which has been proven secure in [46]. Remarkably, this particular scheme has been shown to scale linearly with the channel transmission at long distance, a desirable feature in QKD. Two interesting variants of this scheme appeared in [47] and [48], which allow for a much simpler implementation.

The performance of the B92 protocol is not as good as that of BB84. The presence of non-orthogonal but linearly independent states makes it possible for the eavesdropper to execute a good USD measurement on the quantum states prepared by Alice. This makes the B92 very loss dependent and reduces its tolerance to noise from a depolarizing channel [1] to about 3.34% [44]. This value is much smaller than the one pertaining to the BB84 protocol, which is 16.5% [19] (it should be stressed here that these values refer to the depolarizing parameter p of a depolarizing channel acting on a state ρ as $(1-p)\rho + p/3\sum_{i=x,y,z}\sigma_i\rho\sigma_i$ with Pauli operators σ_i).

VII. LECTURE 2: CONTINUOUS-VARIABLE QKD

A. Brief introduction to CV systems

We start by providing some basic notions on CV quantum systems and bosonic Gaussian states. Here, and in the following discussions on CV-QKD protocols, the variance of the vacuum state is set to 1. This is also known as the vacuum or fundamental shot noise unit (SNU). Recall that CV quantum systems are described by infinite-dimensional Hilbert spaces [2]. In particular, we consider n bosonic modes of the electromagnetic field with tensor-product Hilbert space $\otimes_{k=1}^{n}\mathcal{H}_k$ and associated n pairs of field operators $\hat{a}_k^\dagger$, $\hat{a}_k$, with $k = 1, \ldots, n$. For each mode k we can define the following field quadratures

$$\hat{q}_k := \hat{a}_k + \hat{a}_k^\dagger, \quad \hat{p}_k := i\left(\hat{a}_k^\dagger - \hat{a}_k\right). \tag{53}$$

These operators can be arranged in an N-mode vector $\hat{\mathbf{x}} := (\hat{q}_1, \hat{p}_1, \ldots, \hat{q}_n, \hat{p}_n)^T$. Using the standard bosonic commutation relation, for field's creation ($\hat{a}_k^\dagger$) and annihilation ($\hat{a}_k$) operators, one can easily verify that any pairs of entries of vector $\mathbf{x}$ satisfy the following commutation relation

$$[\hat{x}_l, \hat{x}_m] = 2i\Omega_{lm}, \quad \Omega_{lm} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \tag{54}$$

where Ω_{lm} is the symplectic form [2].

An n-mode quantum state can be represented either as a density operator $\hat{\rho}$ acting on $\otimes_{k=1}^{n}\mathcal{H}_k$ or as a Wigner function defined over a $2n$-dimensional phase space (see Ref. [2] for more details). In particular, a state is Gaussian if its Wigner function is Gaussian, so that it is completely characterized by the first two statistical moments, i.e., the mean value $\bar{\mathbf{x}} := \langle\hat{\mathbf{x}}\rangle = \mathrm{Tr}(\hat{\mathbf{x}}\hat{\rho})$ and covariance matrix (CM) $\mathbf{V}$, whose arbitrary element is defined by

$$V_{ij} := \tfrac{1}{2}\left\langle\{\Delta\hat{x}_i, \Delta\hat{x}_j\}\right\rangle, \tag{55}$$

where $\Delta\hat{x}_i := \hat{x}_i - \langle\hat{x}_i\rangle$ and $\{,\}$ is the anti-commutator.

For a single-mode, one can consider different classes of quantum states, the most known are the coherent states. These are states with minimum (vacuum) noise uncertainty, symmetrically distributed in the two quadratures, and characterized by their complex amplitudes in the phase space. They are denoted as $|\alpha\rangle$, where $\alpha = (\bar{q} + i\bar{p})/2$, where $(\bar{q}, \bar{p})$ are the components of the mean value. Another important class is that of squeezed states, where the noise is less than the vacuum in one of the two quadratures (while greater than in the other) [2].

The basic one-way CV-QKD protocols can be classified with respect to the quantum states employed (coherent or squeezed), the type of encoding adopted (Gaussian modulation or discrete alphabet), and the type of measurement used (homodyne or heterodyne detection). In particular, Gaussian protocols based on the Gaussian modulation of Gaussian states have received an increasing attention in the latest years, not only because Gaussian states are routinely produced in quantum optics labs but also because they are relatively easy to study, due to their description based on mean value and CM.

B. Historical outline

As an alternative to DV-QKD protocols, which are ideally based on a single photon detection, CV-QKD protocols encode keys into CV observables of light fields that can be measured by shot-noise limited homodyne detection. In a homodyne detector an optical signal is coupled to a shot-noise limited strong local oscillator (LO) beam on a balanced beamsplitter and the light intensities on the output ports are measured. Depending on the optical phase difference between the signal and LO, the difference of photocurrents produced at each of the two detectors will be proportional to one of the two field quadratures. The LO therefore carries the phase reference, which allows to switch between the measurement of $q-$ and $p-$quadrature (or more generally perform the state tomography by measuring the Wigner function associated to the state).

The first proposal of using the quadratures of the bosonic field for implementing QKD dates back to 1999, when Ralph [49] considered the encoding of key bits by using four fixed quadrature displacements of bright coherent or two-mode entangled beams. Later, Ralph discussed the security of the two-mode entanglement-based scheme in more detail [50], considering not only intercept-resend attacks but also CV teleportation. The latter was identified as an optimal attack against the protocol, imposing the requirements of high signal squeezing and low channel loss [50]. Independently, Hillery [51] suggested a CV-QKD protocol based on quadrature encoding of a single-mode beam, randomly squeezed in one of the quadrature directions. Security against intercept-resend and beam-splitting attacks were assessed on the basis of the uncertainty principle. Another early CV-QKD scheme was suggested by Reid [52] and based on the verification of EPR-type correlations to detect an eavesdropper.

In 2000 Cerf et al. [53] proposed the first *all continuous* QKD protocol, where the quadratures of a squeezed beam were used to encode a Gaussian-distributed secure key. The security of the protocol was shown against individual attacks based on the uncertainty relations and the optimality of a quantum cloner. Later, reconciliation procedures were introduced for Gaussian-distributed data, which allowed to implement EC and PA close to the theoretical bounds [54]. Another CV-QKD protocol based on the Gaussian modulation of squeezed beams was suggested by Gottesman and Preskill [55]. This protocol was shown to be secure against arbitrary attacks at feasible levels of squeezing, by using quantum error-correcting codes.

In 2001 Grosshans and Grangier introduced a seminal coherent-state protocol with Gaussian quadrature modulation and showed its security against individual attacks [56] by resorting to the CV version of the no-cloning theorem [57]. The standard protocol based on DR, where Alice is the reference side for the information post-processing, was however limited to 50% channel transmittance, i.e., 3dB. As an attempt to beat the 3dB limit, the use of post-selection in CV-QKD was suggested by Silberhorn et al. [58]. Alternatively, it was shown that the use of RR, where the reference side is Bob, allowed the coherent-state protocol to be secure against individual attacks up to arbitrarily-low channel transmittances [59]. In 2004, the heterodyne detection was then suggested for coherent-state protocols [61]; this *non-switching protocol* had the advantage that both the quadratures are measured, thus increasing the key rate.

The security of CV-QKD against collective Gaussian attacks was shown independently by Navascués et al. [62] and by García-Patrón and Cerf [63]. Collective Gaussian attacks were fully characterized by Pirandola et al. [64], who later derived the secret-key capacities for CV-QKD [91, 96]. Security against collective attacks was extended to the general attacks by Renner and Cirac [11] using the quantum de Finetti theorem applied to infinite-dimensional systems. This concluded the security proofs for the basic one-way CV-QKD protocols in the asymptotic limit of infinitely large data sets [65] including those with trusted-noise [27, 66, 67]. Next developments were the study of finite-size effects and fully composable proofs. It is also worth to mention the existence of other direction lines where the limitations of a realistic eavesdropper are taken into account in the computation of the secret key rate [68, 69]

Besides the development of one-way Gaussian protocols and their security proofs, the quantum information community has developed a number of other types of protocols which are based on the use of CV systems, including two-way protocols [70–72], thermal-state protocols [73–77], unidimensional protocols [78, 79], relay-assisted protocols such as CV MDI-QKD [80, 81], and also protocols that are based on the use of non-Gaussian operations such as photon-subtraction [82], quantum catalysis [83], or quantum scissors [84].

C. One-way CV-QKD protocols

The family of one-way CV-QKD protocols can be divided into four major ones, depending on the signal states and the type of measurements applied. It was already mentioned that CV-QKD can be realized using coherent or squeezed signal states, and the homodyne measurement is used to obtain quadrature value of an incoming signal. As an alternative to the homodyne detection, the heterodyne measurement can be applied. Here the signal mode is divided on a balanced beamsplitter and q- and p-quadratures are simultaneously detected using homodyne detectors at the outputs. A vacuum noise is then unavoidably being mixed to the signal.

The "prepare and measure" realization of a generic one-way CV-QKD protocol includes the following steps:

- Alice encodes a classical variable α in the amplitudes of Gaussian states which are randomly displaced in the phase space by means of a zero-mean Gaussian distribution, whose variance is typically large. If coherent states are used, the modulation is symmetric in the phase space. If squeezed states are used instead, then the displacement is along the direction of the squeezing and Alice randomly switches between q- and p- squeezings.

- Alice then sends the modulated signal states to Bob through the quantum channel, which is typically a thermal-loss channel with transmissivity η and some thermal noise, quantified by the mean number of thermal photons in the environment $\bar{n}$ or, equivalently, by the excess noise $\varepsilon = 2\eta^{-1}(1-\eta)\bar{n}$. In some cases, one may have a fading channel where the channel's transmissivity varies over time (e.g. due to turbulence) [85].

- At the output of the quantum channel, Bob performs homodyne or heterodyne detection on the incoming signals, thus retrieving his classical variable β. If homodyne is used, this is randomly switched between the q- and the p- quadratures.

- If Alice and Bob have switched between different quadratures, they will implement a session of CC to reconcile their bases, so as to keep only the choices corresponding to the same quadratures (sifting).

- By publicly declaring and comparing part of their sifted data, Alice and Bob perform parameter estimation. From the knowledge of the parameters of the quantum channel, they can estimate the maximum information leaked to Eve, e.g., in a collective Gaussian attack. If this leakage is above a certain security threshold, they abort the protocol.

- Alice and Bob perform EC and PA on their data. This is done in DR if Bob aims to infer Alice's variable, or RR if Alice aims to infer Bob's one.

D. Computation of the key rate

In a Gaussian CV-QKD protocol, where the Gaussian signal states are Gaussianly-modulated and the outputs are measured by homodyne or heterodyne detection, the optimal attack is a collective Gaussian attack. Here Eve combines each signal state and a vacuum environmental state via a Gaussian unitary and collects the output of environment in a quantum memory for an optimized and delayed joint quantum measurement. The possible collective Gaussian attacks have been fully classified in Ref. [64]. A realistic case is the so-called entangling cloner [57] where Eve prepares a two-mode squeezed vacuum (TMSV) state with variance $\omega = 2\bar{n}+1$ and mixes one of its modes with the signal mode via a beam-splitter with transmissivity η, therefore resulting in a thermal-loss channel (see Ref. [86] for a comparison of this attack with respect to an all-optical teleportation attack). Under a collective Gaussian attack, the asymptotic secret key rates in DR (▶) or RR (◀) are respectively given by

$$R^{\blacktriangleright} = \xi I(\alpha:\beta) - I(\alpha:E), \tag{56}$$

$$R^{\blacktriangleleft} = \xi I(\alpha:\beta) - I(\beta:E), \tag{57}$$

where $\xi \in (0,1)$ is the reconciliation efficiency, defining how efficient are the steps of EC and PA, $I(\alpha:\beta)$ is Alice and Bob's mutual information on their variables α and β, while $I(\alpha:E)$ is Eve's Holevo information [7] on Alice's variable, and $I(\beta:E)$ on Bob's variable. Note that a sifting pre-factor may be present in protocols that need basis reconciliation.

Theoretical evaluation of these rates is performed in the equivalent entanglement-based representation of the protocol, where Alice's preparation of signal states on the input mode a is replaced by a TMSV state Φ^{μ}_{aA} in modes a and A. A Gaussian measurement performed on mode A is able to remotely prepare a Gaussian ensemble of Gaussian states on mode a. For instance, if A is subject to heterodyne, then mode a is projected onto a coherent state whose amplitude is one-to-one with the outcome of the heterodyne and is Gaussianly modulated in phase space with variance $\mu - 1$. In this representation, Alice's classical variable is equivalently represented by the outcome of her measurement.

Once mode a is propagated through the channel, it is perturbed by Eve and received as mode B by Bob. Therefore, Alice and Bob will share a bipartite state ρ_{AB}. In the worst case scenario, the entire purification of ρ_{AB} is assumed to be held by Eve. This means that we assume a pure state Ψ_{ABE} involving a number of extra modes E such that $\mathrm{Tr}_E(\Psi_{ABE}) = \rho_{AB}$. For a Gaussian protocol under a collective Gaussian attack, we have that Ψ_{ABE} is pure, so that the Eve's reduced output state $\rho_E := \mathrm{Tr}_{AB}(\Psi_{ABE})$ has the same entropy of ρ_{AB}, i.e.,

$$S(E) := S(\rho_E) = S(\rho_{AB}) := S(AB). \tag{58}$$

Assuming that Alice and Bob performs rank-1 Gaussian measurements (like homodyne or heterodyne), then they project on pure states. In DR, this means that the output α of Alice measurement, with probability $p(\alpha)$, generates a pure conditional Gaussian state $\Psi_{BE|\alpha}$ whose CM does not depend on the actual value of α. Then, because the reduced states $\rho_{B(E)|\alpha} := \mathrm{Tr}_{E(B)}(\Psi_{BE|\alpha})$ have the same entropy, we may write the following equality for the conditional entropies

$$\begin{aligned} S(E|\alpha) &:= \int d\alpha\ p(\alpha) S(\rho_{E|\alpha}) \\ &= S(\rho_{E|\alpha}) = S(\rho_{B|\alpha}) \\ &= \int d\alpha\ p(\alpha) S(\rho_{B|\alpha}) := S(B|\alpha). \end{aligned} \tag{59}$$

Similarly, in RR, we have Bob's outcome β with probability $p(\beta)$ which generates a pure conditional Gaussian state $\Psi_{AE|\beta}$ with similar properties as above. In terms of the reduced states $\rho_{A(E)|\beta} := \mathrm{Tr}_{E(A)}(\Psi_{AE|\beta})$ we write the conditional entropies

$$\begin{aligned} S(E|\beta) &:= \int d\beta\ p(\beta) S(\rho_{E|\beta}) \\ &= S(\rho_{E|\beta}) = S(\rho_{A|\beta}) \\ &= \int d\beta\ p(\beta) S(\rho_{A|\beta}) := S(A|\beta). \end{aligned} \tag{60}$$

By using Eqs. (58), (59) and (60) in the key rates of Eqs. (56) and (57) we may simplify the Holevo quantities as

$$I(\alpha : E) := S(E) - S(E|\alpha) = S(AB) - S(B|\alpha), \tag{61}$$
$$I(\beta : E) := S(E) - S(E|\beta) = S(AB) - S(A|\beta). \tag{62}$$

This is a remarkable simplification because the two rates are now entirely computable from the output bipartite state ρ_{AB} and its reduced versions $\rho_{B|\alpha}$ and $\rho_{A|\beta}$. In particular, because all these state are Gaussian, the von Neumann entropies in Eqs. (61) and (62) are very easy to compute from the CM of ρ_{AB}. Similarly, the mutual information $I(\alpha : \beta)$ can be computed from the CM. Given the expressions of the rates, one can also compute the security thresholds by solving $R^{\blacktriangleright} = 0$ or $R^{\blacktriangleleft} = 0$.

Note that there is a more generalized framework for security analysis, where Alice and Bob have trusted loss and noise in their devices and they cannot purify into a TMSV state. This is a device-dependent scenario which is typical in realistic implementations where both the preparation of the signals and the measurements of the outputs are affected by imperfections. In this case, a generalized treatment is possible following Refs. [27, 87].

E. Ideal performances in a thermal-loss channel

The ideal performances of the main one-way Gaussian protocols can be studied in a thermal-loss channel, assuming asymptotic security, perfect reconciliation ($\xi = 1$), and infinite Gaussian modulation. Let us consider the entropic function

$$s(x) := \frac{x+1}{2} \log_2 \frac{x+1}{2} - \frac{x-1}{2} \log_2 \frac{x-1}{2}, \tag{63}$$

so that $s(1) = 0$ for the vacuum noise. For the protocol with Gaussian-modulated coherent states and homodyne detection [57], one has

$$\begin{aligned} R^{\blacktriangleright}_{\mathrm{coh,hom}} &= \frac{1}{2} \log_2 \frac{\eta\,(1-\eta+\eta\omega)}{(1-\eta)\,[\eta + (1-\eta)\omega]} - s(\omega) \\ &\quad + s\left[\sqrt{\frac{\eta+(1-\eta)\omega}{1-\eta+\eta\omega}\omega}\right], \end{aligned} \tag{64}$$

$$R^{\blacktriangleleft}_{\mathrm{coh,hom}} = \frac{1}{2} \log_2 \frac{\omega}{(1-\eta)\,[\eta + (1-\eta)\omega]} - s(\omega). \tag{65}$$

For the non-switching protocol with Gaussian-modulated coherent states and heterodyne detection [61], one instead has

$$\begin{aligned} R^{\blacktriangleright}_{\mathrm{coh,het}} &= \log_2 \frac{2}{e} \frac{\eta}{(1-\eta)\,[1+\eta+(1-\eta)\omega]} - s(\omega) \\ &\quad + s\,[\eta + \omega(1-\eta)]\,, \end{aligned} \tag{66}$$

$$\begin{aligned} R^{\blacktriangleleft}_{\mathrm{coh,het}} &= \log_2 \frac{2}{e} \frac{\eta}{(1-\eta)\,[1+\eta+(1-\eta)\omega]} - s(\omega) \\ &\quad + s\left[\frac{1+(1-\eta)\omega}{\eta}\right]. \end{aligned} \tag{67}$$

For the protocol with Gaussian-modulated squeezed states (in the limit of infinite squeezing) and homodyne detection [53], here we analytically compute

$$R^{\blacktriangleright}_{\mathrm{sq,hom}} = \frac{1}{2}\left[\log_2 \frac{\eta}{1-\eta} - s(\omega)\right], \tag{68}$$

$$R^{\blacktriangleleft}_{\mathrm{sq,hom}} = \frac{1}{2}\left[\log_2 \frac{1}{1-\eta} - s(\omega)\right]. \tag{69}$$

Note that, for this specific protocol, a simple bound can be derived at low η and low $\bar{n}$, which is given by [88] $R^{\blacktriangleleft}_{\mathrm{sq,hom}} \simeq (\eta - \bar{n}) \log_2 e + \bar{n} \log_2 \bar{n}$, which provides a security threshold $\bar{n}_{max}(\eta) = \exp[1 + W_{-1}(-\eta/e)]$ in terms of the Lambert W-function.

Finally, for the protocol with Gaussian-modulated infinitely-squeezed states and heterodyne detection [89], here we analytically compute

$$R^{\blacktriangleright}_{\mathrm{sq,het}} = \frac{1}{2} \log_2 \frac{\eta^2 \omega}{(1-\eta)\,[1+(1-\eta)\omega]} - s(\omega), \tag{70}$$

$$\begin{aligned} R^{\blacktriangleleft}_{\mathrm{sq,het}} &= \frac{1}{2} \log_2 \frac{1-\eta+\omega}{(1-\eta)\,[1+(1-\eta)\omega]} - s(\omega) \\ &\quad + s\left[\sqrt{\frac{\omega\,[1+\omega(1-\eta)]}{1+\omega-\eta}}\right]. \end{aligned} \tag{71}$$

Note that this is a particular case of protocol where trusted noise added at the detection can have beneficial effects on its security threshold [66, 67]. In CV-QKD this effect was studied in Refs. [27, 89–92], and later in Refs. [93–95] as a tool to increase the lower bound to the secret key capacity of the thermal-loss and amplifier channels. In particular, the protocol presented in Ref. [95] has the highest-known security threshold so far.

Also note that for a pure-loss channel ($\omega = 1$), we find

$$R^{\blacktriangleleft}_{\mathrm{sq,het}} = R^{\blacktriangleleft}_{\mathrm{sq,hom}} = \frac{1}{2} \log_2 \frac{1}{1-\eta}, \tag{72}$$

which is half of the secret-key capacity of the pure-loss channel $-\log_2(1-\eta)$ [96](see next lecture). According to Ref. [91], this capacity is achievable if one of these two protocols is implemented in the entanglement-based representation and with a quantum memory. In particular for the squeezed-state protocol with homodyne detection, the use of the memory allows Alice and Bob to always choose the same quadrature, so that we may remove the sifting factor 1/2 from $R^{\blacktriangleleft}_{\mathrm{sq,hom}}$ in Eq. (72).

VIII. LECTURE 3: ULTIMATE LIMITS OF QKD

A. Overview of the main contributions

One of the crucial problems in QKD is to achieve long distances at reasonably-high rates. However, since the proposal of the BB84 protocol [12], it was understood that this is a daunting task because even an ideal implementation of this protocol (based on perfect single-photon sources, ideal detectors and perfect EC) shows a linear decay of the secret key rate R in terms of the loss η in the channel, i.e., $R = \eta/2$. One possible way to overcome the rate problem was to introduce CV QKD protocols. Their ideal implementation can in fact beat any DV QKD protocol at any distance, even though current practical demonstrations can achieve this task only for limited distances due to practical problems related to finite reconciliation efficiency and other technical issues.

One of the breakthroughs in CV QKD was the introduction of the reverse reconciliation (RR) [56], where it is Alice to infer Bob's outcomes β, rather than Bob guessing Alice's encodings α, known as direct reconciliation (DR). This led the CV QKD community to considering a modified Devetak-Winter rate [8] in RR. This takes the form of $I(\alpha : \beta) - \chi(E : \beta)$, where the latter is Eve's Holevo information on Bob's outcomes. In a CV QKD setup, where both the energy and the entropy may hugely vary at the two ends of a lossy communication channel, there may be a non-trivial difference between the two reconciliation methods. Most importantly, it was soon realized that RR allowed one to achieve much longer distances, well beyond the 3dB limit of the previous CV approaches. At long distances (i.e., small transmissivity η), an ideal implementation of the CV QKD protocols proposed in Refs. [60, 61] has rate $R \simeq \eta/(2\ln 2) \simeq 0.72\eta$. An open question was therefore raised:

- What is the maximum key rate (secret key capacity) achievable at the ends of a pure-loss channel?

With the aim of answering this question, a 2009 paper [91] introduced the notion of reverse coherent information (RCI) of a bosonic channel. This was quantity was previously defined in the setting of DVs [90, 97]. It was called "negative cb-entropy of a channel" in Ref. [97] and "pseudocoherent information" in Ref. [98]; Ref. [90] introduced the terminology of RCI and, most importantly, it showed its fundamental use as lower bound for entanglement distribution over a quantum channel (thus extending the hashing inequality [8] from states to channels). Ref. [91] extended the notion to CVs where it has its more natural application.

Given a bosonic channel $\mathcal{E}$, consider its asymptotic Choi matrix $\sigma_{\mathcal{E}} := \lim_\mu \sigma^\mu_{\mathcal{E}}$. This is defined over a sequence of Choi-approximating states of the form $\sigma^\mu_{\mathcal{E}} := \mathcal{I}_A \otimes \mathcal{E}_B(\Phi^\mu_{AB})$, where Φ^μ_{AB} is a TMSV state [2] with $\bar{n} = \mu - 1/2$ mean thermal photons in each mode. Then, we define its RCI as [91]

$$I_{\text{RCI}}(\mathcal{E}) := \lim_\mu I(A\rangle B)_{\sigma^\mu_{\mathcal{E}}}, \tag{73}$$

$$I(A\rangle B)_{\sigma^\mu_{\mathcal{E}}} := S[\text{Tr}_B(\sigma^\mu_{\mathcal{E}})] - S(\sigma^\mu_{\mathcal{E}}), \tag{74}$$

with $S(\sigma) := -\text{Tr}(\sigma \log_2 \sigma)$ is the von Neumann entropy of σ. Here first note that, by changing Tr_B with Tr_A in Eq. (74), one defines the coherent information (CI) of a bosonic channel [91], therefore extending the definition of Refs. [99, 100] to CV systems. Also note that $I_{\text{RCI}}(\mathcal{E})$ is easily computable for a bosonic Gaussian channel, because $\sigma^\mu_{\mathcal{E}}$ would be a two-mode Gaussian state.

Operationally, the RCI of a bosonic channel represents a lower bound for its secret key capacity and, more weakly, its entanglement distribution capacity [91]. A powerful CV QKD protocol reaching the RCI of a bosonic channel consists of the following steps:

- Alice sends to Bob the B-modes of TMSV states Φ^μ_{AB} with variance μ.
- Bob performs heterodyne detections of the output modes sending back a classical variable to assist Alice.
- Alice performs an optimal and conditional joint detection of all the A-modes.

The achievable rate can be computed as a difference between the Alice Holevo information $\chi(A : \beta)$ and Eve's Holevo information $\chi(E : \beta)$ on Bob's outcomes. Note that this is not a Devetak-Winter rate (in RR) but rather a generalization, where the parties' mutual information is replaced by the Holevo bound. Because Eve holds the entire purification of $\sigma^\mu_{\mathcal{E}}$, her reduced state ρ_E has entropy $S(\rho_E) = S(\sigma^\mu_{\mathcal{E}})$. Then, because Bob's detections are rank-1 measurements (projecting onto pure states), Alice and Eve's global state $\rho_{AE|\beta}$ conditioned to Bob's outcome β is pure. This means that $S(\rho_{E|\beta}) = S(\rho_{A|\beta})$. As a result, Eve's Holevo information becomes

$$\chi(E : \beta) := S(\rho_E) - S(\rho_{E|\beta}) = S(\sigma^\mu_{\mathcal{E}}) - S(\rho_{A|\beta}). \tag{75}$$

On the other hand, we also write

$$\chi(A : \beta) := S(\rho_A) - S(\rho_{A|\beta}), \tag{76}$$

where $\rho_A := \text{Tr}_B(\sigma^\mu_{\mathcal{E}})$ and $\rho_{A|\beta}$ is conditioned to Bob's outcome. As a result we get the following achievable rate

$$R^\mu(\mathcal{E}) := \chi(A : \beta) - \chi(E : \beta) = I(A\rangle B)_{\sigma^\mu_{\mathcal{E}}}. \tag{77}$$

By taking the limit for large μ, this provides the key rate $R(\mathcal{E}) := \lim_\mu R^\mu(\mathcal{E}) = I_{\text{RCI}}(\mathcal{E})$, so that the secret key capacity of the channel can be bounded as

$$K(\mathcal{E}) \geq I_{\text{RCI}}(\mathcal{E}) \ . \tag{78}$$

In particular, for a pure-loss channel $\mathcal{E}_\eta$ with transmissivity η, Pirandola, García-Patrón, Braunstein and Lloyd wrote the lower bound [91]

$$K(\mathcal{E}_\eta) \geq I_{\text{RCI}}(\mathcal{E}_\eta) = -\log_2(1-\eta). \tag{79}$$

Later, in 2015, Ref. [96] derived the upper bound

$$K(\mathcal{E}_\eta) \leq -\log_2(1-\eta), \tag{80}$$

which is known as the Pirandola-Laurenza-Ottaviani-Banchi (PLOB) bound. This was done by employing the relative entropy of entanglement (REE) [101–103], suitably extended to quantum channels, combined with an adaptive-to-block reduction of quantum protocols. Because of the coincidence between Eqs. (79) and (80), Ref. [96] finally established the secret key capacity of the pure-loss channel to be

$$\mathcal{K}(\mathcal{E}_\eta) = -\log_2(1-\eta), \tag{81}$$

which, in turn, completely characterizes the fundamental rate-loss scaling of QKD to be $\simeq 1.44\eta$ bits per channel use at long distances.

This capacity cannot be beaten by any point-to-point QKD protocol at the two ends of the lossy channel. It can only be outperformed if Alice and Bob pre-share some secret randomness or if there is a quantum repeater splitting the quantum communication channel and assisting the remote parties. For this reason, the PLOB bound not only completely characterizes the fundamental rate-loss scaling of point-to-point QKD but also provides the exact benchmark for testing the quality of quantum repeaters.

Soon after the introduction of the PLOB bound, in early 2016, Ref. [104] (later published as Ref. [105]) established the secret key capacities achievable in chains of repeaters and, more generally, quantum networks connected by pure-loss channels. In particular, in the presence of a single repeater, in the middle between the remote parties and equally splitting the overall pure-loss channel $\mathcal{E}_\eta$ of transmissivity η, one finds the following single-repeater secret key capacity

$$\mathcal{K}_{1\text{rep}}(\mathcal{E}_\eta) = -\log_2(1-\sqrt{\eta}), \tag{82}$$

At long distances $\eta \simeq 0$, this rate provides the fundamental rate-loss scaling in the presence of a single repeater. This is given by [105, Supp. Note 1, Eq. (25)]

$$\mathcal{K}_{1\text{rep}}(\mathcal{E}_\eta) \simeq 1.44\sqrt{\eta} \text{ bits per repeater use.} \tag{83}$$

In Fig. 2 we show the ideal key rates of point-to-point QKD protocols and those of relay-assisted end-to-end QKD protocols (i.e., exploiting an untrusted QKD repeater). These rates are compared with the PLOB bound of Eq. (81) and the single-repeater bound of Eq. (82). By ideal rates we mean the optimal ones that can be computed assuming zero dark counts, perfect detector efficiency, zero misalignment error, as well as perfect EC and reconciliation efficiency. Point-to-point protocols cannot beat the PLOB bound and asymptotically scales as $\simeq \eta$ bits per channel use. This is the case for the BB84 protocol (both with single-photon sources and decoy-state implementation) and one-way CV-QKD protocols. Even though MDI-QKD is relay assisted, its relay is not efficient, which is why DV MDI-QKD is below the PLOB bound. After TF-QKD [106] was introduced, a number of TF-inspired protocols were developed, all able to beat the PLOB bound. The middle untrusted relays of these protocols are therefore efficient (i.e., they are able to 'repeat'). Their key rates cannot overcome the single-repeater bound, but clearly follow its asymptotic rate-loss scaling of $\simeq \sqrt{\eta}$ bits per channel use.

In the following subsections, we provide the main mathematical definitions, tools, and formulas related to the study of the ultimate limits of point-to-point QKD protocols over an arbitrary quantum channel. In particular, we show the main steps needed for proving the PLOB bound. Then, we will discuss the extension of these results to repeater-assisted quantum communications.

B. Adaptive protocols and two-way assisted capacities

Let us start by defining an adaptive point-to-point protocol $\mathcal{P}$ through a quantum channel $\mathcal{E}$. Assume that Alice has register $\mathbf{a}$ and Bob has register $\mathbf{b}$. These registers are (countable) sets of quantum systems which are prepared in some state $\rho^0_{\mathbf{ab}}$ by an adaptive LOCC Λ_0 applied to some fundamental separable state $\rho^0_{\mathbf{a}} \otimes \rho^0_{\mathbf{b}}$. Then, for the first transmission, Alice picks a system $a_1 \in \mathbf{a}$ and sends it through channel $\mathcal{E}$; at the output, Bob receives a system b_1 which is included in his register $b_1\mathbf{b} \to \mathbf{b}$. Another adaptive LOCC Λ_1 is applied to the registers. Then, there is the second transmission $\mathbf{a} \ni a_2 \to b_2$ through $\mathcal{E}$, followed by another LOCC Λ_2 and so on (see Fig. 3). After n uses, Alice and Bob share an output state $\rho^n_{\mathbf{ab}}$ which is epsilon-close to some target private state [107] ϕ^n with nR^ε_n secret bits. This means that, for any $\varepsilon > 0$, one has $\|\rho^n_{\mathbf{ab}} - \phi^n\| \leq \varepsilon$ in trace norm. This is also called an $(n, R^\varepsilon_n, \varepsilon)$-protocol. Operationally, the protocol $\mathcal{P}$ is completely characterized by the sequence of adaptive LOCCs $\mathcal{L} = \{\Lambda_0, \Lambda_1 \ldots\}$. The secret key capacity of the quantum channel is defined by taking the limit of the asymptotic weak-converse rate $\lim_{\varepsilon,n} R^\varepsilon_n$ and maximizing over all adaptive protocols $\mathcal{P}$, i.e.,

$$K(\mathcal{E}) := \sup_{\mathcal{P}} \lim_{\varepsilon} \lim_{n} R^\varepsilon_n. \tag{84}$$

C. General weak-converse upper bound

The secret key capacity can be bounded by a general expression in terms of the REE [101–103]. First of all, recall that the REE of a quantum state σ is given by

$$E_{\text{R}}(\sigma) = \inf_{\gamma \in \text{SEP}} S(\sigma||\gamma), \tag{85}$$

where γ is a separable state and S is the quantum relative entropy, defined by [101]

$$S(\sigma||\gamma) := \text{Tr}\left[\sigma(\log_2 \sigma - \log_2 \gamma)\right]. \tag{86}$$

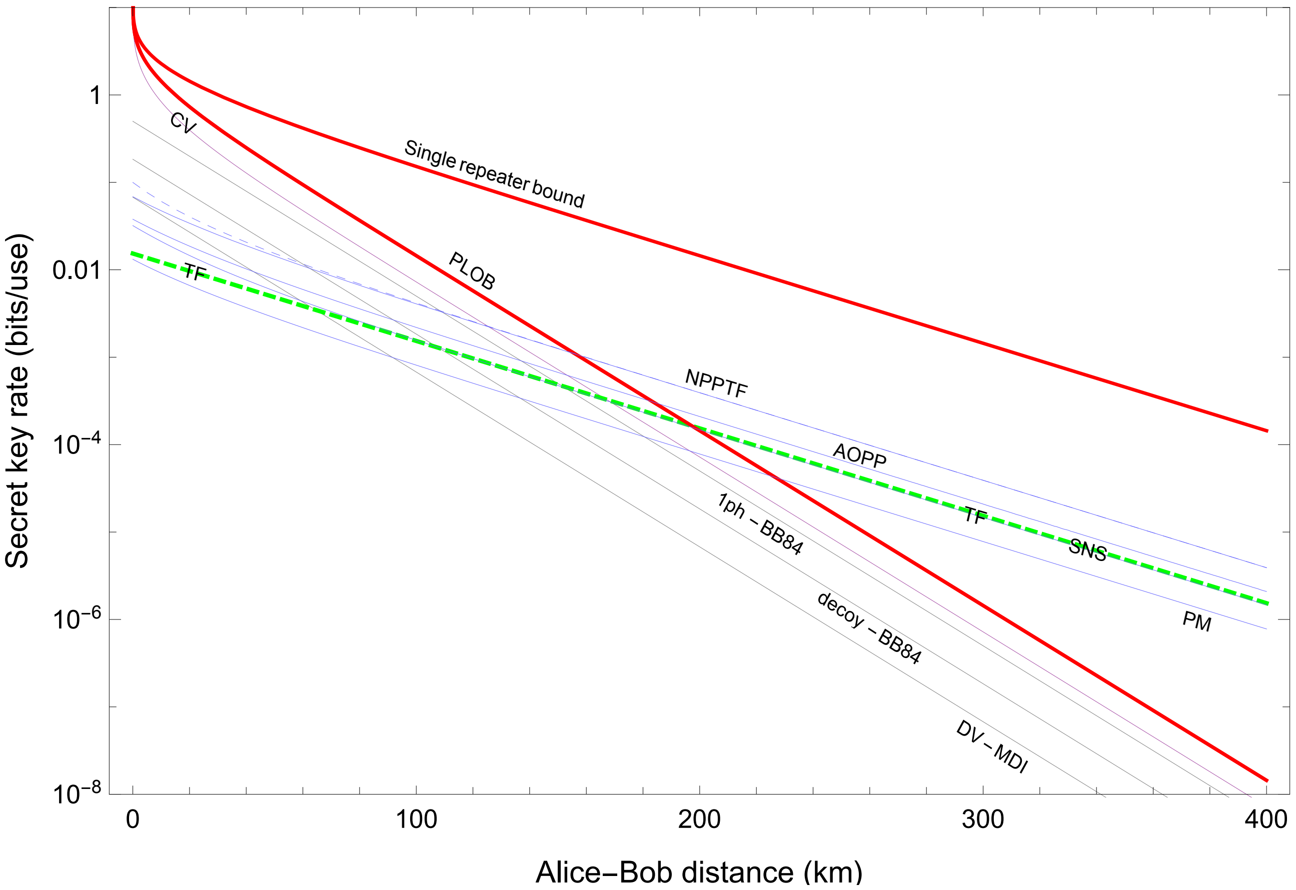

FIG. 2. State of the art in high-rate QKD. We plot the ideal key rates of several point-to-point and relay-assisted end-to-end protocols with respect to the PLOB bound [96] of Eq. (81), having the asymptotic scaling of 1.44η bits per use, and the single-repeater bound [104, 105] of Eq. (82), having the asymptotic scaling of $1.44\sqrt{\eta}$ bits per use. The key rates are expressed in terms of bits per channel use and plotted versus distance (km) at the standard fiber-loss rate of 0.2 dB per km.

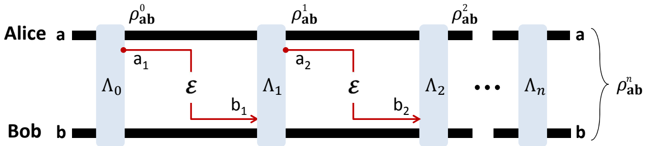

FIG. 3. Point-to-point adaptive protocol. Each transmission $a_i \to b_i$ through the quantum channel $\mathcal{E}$ is interleaved by two adaptive LOCCs, Λ_{i-1} and Λ_i, applied to Alice's and Bob's local registers $\mathbf{a}$ and $\mathbf{b}$. After n transmissions, Alice and Bob share an output state $\rho^n_{\mathbf{ab}}$ close to some target state ϕ^n. Adapted with permission from Ref. [95] ©IOPP (2018).

With these notions in hand, we may write a general upper bound. In fact, for any quantum channel $\mathcal{E}$, we have [96]

$$\mathcal{C}(\mathcal{E}) \leq E^{\bigstar}_{\mathrm{R}}(\mathcal{E}) := \sup_{\mathcal{P}} \lim_{n} \frac{E_R(\rho^n_{\mathbf{ab}})}{n} , \qquad (87)$$

where $E^{\bigstar}_{\mathrm{R}}(\mathcal{E})$ is defined by computing the REE of the output state $\rho^n_{\mathbf{ab}}$, taking the limit for many channels uses, and optimizing over all the adaptive protocols $\mathcal{P}$.

To simplify the REE bound $E^{\bigstar}_{\mathrm{R}}(\mathcal{E})$ into a single-letter quantity, we adopt a technique of adaptive-to-block reduction or protocol "stretching" [95, 96, 108]. A preliminary step consists in using a suitable simulation of the quantum channel, where the channel is replaced by a corresponding resource state. Then, this simulation argument can be exploited to stretch the adaptive protocol into a much simpler block-type protocol, where the output is decomposed into a tensor product of resource states up to a trace-preserving LOCC.

D. LOCC simulation of quantum channels

Given an arbitrary quantum channel $\mathcal{E}$, we may consider a corresponding simulation $S(\mathcal{E}) = (\mathcal{T}, \sigma)$ based on some LOCC $\mathcal{T}$ and resource state σ. This simulation is such that, for any input state ρ, the output of the channel can be expressed as

$$\mathcal{E}(\rho) = \mathcal{T}(\rho \otimes \sigma). \qquad (88)$$

See also Fig. 4. A channel $\mathcal{E}$ which is simulable as in Eq. (88) can also be called "σ-stretchable". Note that there are different simulations for the same channel. One is trivial because it just corresponds to choosing σ as a maximally-entangled state and $\mathcal{T}$ as teleportation followed by $\mathcal{E}$ completely pushed in Bob's local operations. Therefore, it is implicitly understood that one has to carry out an optimization over these simulations, which also depend on the specific functional under study.

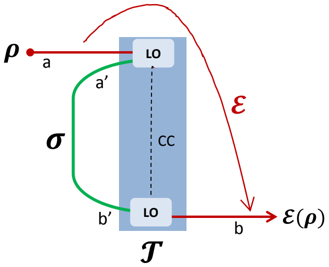

FIG. 4. LOCC simulation of an arbitrary quantum channel $\mathcal{E}$ by means of an LOCC $\mathcal{T}$ applied to the input state ρ and a resource state σ, according to Eq. (88).

E. Teleportation covariance and simulability

For some channels, the LOCC simulation takes a very convenient form. This is the case for the "teleportation covariant" channels, that are those channels commuting with the random unitaries of quantum teleportation [109–112], i.e., Pauli operators in DVs [1], phase-space displacements in CVs [2]. More precisely, a quantum channel $\mathcal{E}$ is called teleportation covariant if, for any teleportation unitary U, we may write

$$\mathcal{E}(U\rho U^{\dagger}) = V\mathcal{E}(\rho)V^{\dagger} \ , \tag{89}$$

for another (generally-different) unitary V [96].

Note that this is a wide family, which includes Pauli channels (e.g., depolarizing or dephasing), erasure channels and bosonic Gaussian channels. Thanks to the property in Eq. (89), the random corrections of the teleportation protocol can be pushed at the output of these channels. For this reason, they may be simulated by teleportation. In fact, a teleportation-covariant channel $\mathcal{E}$ can be simulated as

$$\mathcal{E}(\rho) = \mathcal{T}_{\text{tele}}(\rho \otimes \sigma_{\mathcal{E}}), \tag{90}$$

where $\mathcal{T}_{\text{tele}}$ is a teleportation LOCC (based on Bell detection and conditional unitaries) and $\sigma_{\mathcal{E}}$ is the Choi matrix of the channel, defined as $\sigma_{\mathcal{E}} := \mathcal{I} \otimes \mathcal{E}(\Phi)$, with Φ being a maximally entangled state.

For a teleportation-covariant bosonic channel (Gaussian or non-Gaussian), we may write the asymptotic simulation [96]

$$\mathcal{E}(\rho) = \lim_{\mu} \mathcal{T}^{\mu}_{\text{tele}}(\rho \otimes \sigma^{\mu}_{\mathcal{E}}), \tag{91}$$

where $\mathcal{T}^{\mu}_{\text{tele}}$ is a sequence of teleportation-LOCCs (based on finite-energy versions of the ideal CV Bell detection) and $\sigma^{\mu}_{\mathcal{E}} := \mathcal{I} \otimes \mathcal{E}(\Phi^{\mu})$ is a sequence of Choi-approximating states (recall that Φ^{μ} is a TMSV state with $\bar{n} = (\mu - 1)/2$ mean thermal photons in each mode). When a quantum channel can be simulated as in Eq. (90) or (91) it may be called "Choi-stretchable" or "teleportation simulable".

F. Stretching of an adaptive protocol

By exploiting the LOCC simulation $S(\mathcal{E}) = (\mathcal{T}, \sigma)$ of a quantum channel $\mathcal{E}$, we may completely simplify an adaptive protocol. In fact, the output state $\rho^n_{\mathbf{ab}}$ can be decomposed into a tensor-product of resources states $\sigma^{\otimes n}$ up to a trace-preserving LOCC $\bar{\Lambda}$. In other words, we may write [96, Lemma 3]

$$\rho^n_{\mathbf{ab}} = \bar{\Lambda}\left(\sigma^{\otimes n}\right). \tag{92}$$

As shown in Fig. 5, for the generic ith transmission, we replace the original quantum channel $\mathcal{E}$ with a simulation $S(\mathcal{E}) = (\mathcal{T}, \sigma)$. Then, we collapse the LOCC $\mathcal{T}$ into the adaptive LOCC Λ_i to form the composite LOCC Δ_i. As a result, the pre-transmission state $\rho^{i-1}_{\mathbf{ab}} := \rho_{\mathbf{a}a_i\mathbf{b}}$ is transformed into the following post-transmission state

$$\rho^i_{\mathbf{ab}} = \Delta_i\left(\rho^{i-1}_{\mathbf{ab}} \otimes \sigma\right). \tag{93}$$

The next step is to iterate Eq. (93). One finds

$$\rho^n_{\mathbf{ab}} = (\Delta_n \circ \cdots \circ \Delta_1)(\rho^0_{\mathbf{ab}} \otimes \sigma^{\otimes n}). \tag{94}$$

Because $\rho^0_{\mathbf{ab}}$ is separable, its preparation may be included in the LOCCs and we get Eq. (92) for a complicated but single trace-preserving LOCC $\bar{\Lambda}$.

For a teleportation-covariant channel, we may write the decomposition in terms of its Choi matrix, i.e.,

$$\rho^n_{\mathbf{ab}} = \bar{\Lambda}\left(\sigma^{\otimes n}_{\mathcal{E}}\right). \tag{95}$$

Then, for a teleportation-covariant bosonic channel, we need to consider the issue of the asymptotic simulation in Eq. (91), so that we have

$$\rho^n_{\mathbf{ab}} = \lim_{\mu} \bar{\Lambda}_{\mu}(\sigma^{\mu \otimes n}_{\mathcal{E}}), \tag{96}$$

where $\bar{\Lambda}_{\mu}$ is a sequence of trace-preserving LOCCs.

G. Single-letter upper bound

A crucial insight from Ref. [96] has been the combination of protocol stretching with the REE, so that its properties of monotonicity and sub-additivity can be powerfully exploited. This is the key observation that leads to a single-letter upper bound for all the two-way capacities of a quantum channel. In fact, let us compute the REE of the output state decomposed as in Eq. (92). We derive

$$E_{\text{R}}(\rho^n_{\mathbf{ab}}) \overset{(1)}{\leq} E_{\text{R}}(\sigma^{\otimes n}) \overset{(2)}{\leq} nE_{\text{R}}(\sigma) \ , \tag{97}$$

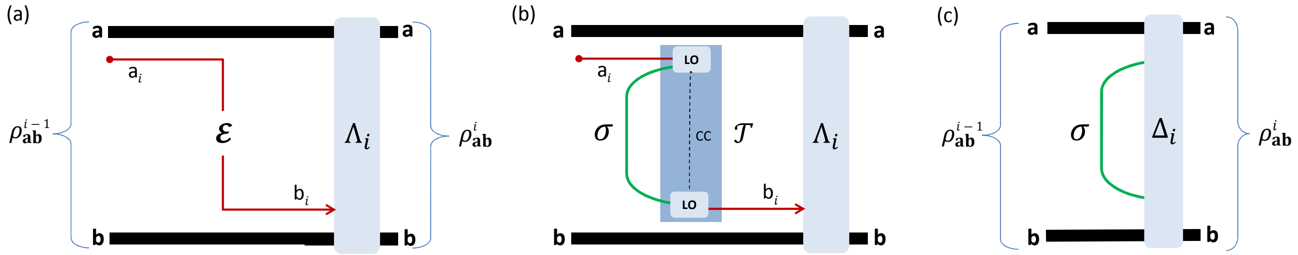

FIG. 5. Stretching of the ith transmission of an adaptive protocol. (a) We depict the original transmission through the channel $\mathcal{E}$ which transforms the register state $\rho^{i-1}_{\mathbf{ab}} := \rho_{\mathbf{a}a_i\mathbf{b}}$ into the output $\rho^{i}_{\mathbf{ab}}$. (b) We simulate the channel by means of an LOCC $\mathcal{T}$ and a resource state σ, as in previous Fig. 4. (c) We collapse $\mathcal{T}$ and the adaptive LOCC Λ_i into a single LOCC Δ_i applied to the tensor product $\rho^{i-1}_{\mathbf{ab}} \otimes \sigma$, as in Eq. (93). Adapted with permission from Ref. [96] ©NPG (2017).

using (1) the monotonicity of the REE under trace-preserving LOCCs and (2) its subadditive over tensor products. By replacing Eq. (97) in Eq. (87), we then find the single-letter upper bound

$$K(\mathcal{E}) \leq E_{\mathrm{R}}(\sigma) \ . \tag{98}$$

In particular, if the channel $\mathcal{E}$ is teleportation-covariant, it is Choi-stretchable, and we may write

$$K(\mathcal{E}) \leq E_{\mathrm{R}}(\sigma_{\mathcal{E}}) \leq S(\sigma_{\mathcal{E}}||\tilde{\gamma}), \tag{99}$$

for a suitable separable state $\tilde{\gamma}$.

For a teleportation-covariant bosonic channel, like a single-mode Gaussian channel, we have the asymptotic decomposition in Eq. (91). As a result, the upper bound in Eq. (99) must be expressed in terms of its asymptotic Choi matrix $\sigma_{\mathcal{E}} := \lim_\mu \sigma^\mu_{\mathcal{E}}$, and takes the form [96]

$$K(\mathcal{E}) \leq \liminf_{\mu\rightarrow+\infty} S(\sigma^\mu_{\mathcal{E}}||\tilde{\gamma}^\mu) \ , \tag{100}$$

for a suitable sequence of separable states $\tilde{\gamma}^\mu$. For a Gaussian channel $\sigma^\mu_{\mathcal{E}} := \mathcal{I}\otimes\mathcal{E}(\Phi^\mu)$ is Gaussian and also $\tilde{\gamma}^\mu$ can be chosen to be Gaussian, so that we are left with computing the relative entropy between two Gaussian states, for which we have a closed analytical formula [96, Theorem 7].

Consider the most important Gaussian channel for CV-QKD, which is the thermal-loss channel $\mathcal{E}_{\eta,\bar{n}}$. This transforms input quadratures $\hat{\mathbf{x}} = (\hat{q},\hat{p})^T$ as $\hat{\mathbf{x}} \rightarrow \sqrt{\eta}\hat{\mathbf{x}} + \sqrt{1-\eta}\hat{\mathbf{x}}_E$, where $\eta \in (0,1)$ is the transmissivity and E is the thermal environment with $\bar{n}$ mean photons. For this channel, we may derive [96, Eq. (23)]

$$K(\mathcal{E}_{\eta,\bar{n}}) \leq \begin{cases} -\log_2\left[(1-\eta)\eta^{\bar{n}}\right] - h(\bar{n}), & \text{if } \bar{n} < \frac{\eta}{1-\eta}, \\ \\ 0, \ \text{ if } \ \bar{n} \geq \frac{\eta}{1-\eta}, \end{cases} \tag{101}$$

where we have set

$$h(x) := (x+1)\log_2(x+1) - x\log_2 x. \tag{102}$$

For $\bar{n}$=0 we have the particular case of a bosonic pure-loss channel $\mathcal{E}_\eta$ with transmissivity η, and we may write the PLOB bound [96]

$$K(\mathcal{E}_\eta) := K(\eta) \leq -\log_2(1-\eta) \ . \tag{103}$$

Combining this with upper bound with the lower bound in Eq. (79), we conclude that the secret key capacity of the pure-loss channel is given by [96, Eq. (19)]

$$K(\eta) = -\log_2(1-\eta) \ . \tag{104}$$

This capacity determines the maximum rate achievable by any QKD protocol in the presence of a lossy communication line (see also Fig. 2). Note that the PLOB bound can be extended to a multiband lossy channel, for which we write $K = -\sum_i \log_2(1-\eta_i)$, where η_i are the transmissivities of the various bands or frequency components. For instance, for a multimode telecom fibre with constant transmissivity η and bandwidth W, we have

$$K = -W\log_2(1-\eta). \tag{105}$$

H. Ultimate limits for lossy repeater chains

Consider a linear chain of N quantum repeaters, labeled by $\mathbf{r}_1,\ldots,\mathbf{r}_N$. This is characterized by an ensemble of $N+1$ quantum channels $\{\mathcal{E}_i\}$ describing the sequence of transmissions $i = 0,\ldots,N$ between the two end-points Alice $\mathbf{a} := \mathbf{r}_0$ and Bob $\mathbf{b} := \mathbf{r}_{N+1}$ (see Fig. 6). Assume the most general adaptive protocol $\mathcal{P}$, where the generation of the secret key between Alice and Bob is ideally assisted by adaptive LOCCs involving all the parties in the chain. After n uses of the chain, Alice and Bob will share an output state $\rho^n_{\mathbf{ab}}$ which depends on $\mathcal{P}$. By taking the limit of large n and optimizing over all possible protocols $\mathcal{P}$, we define the repeater-assisted secret key capacity $K(\{\mathcal{E}_i\})$. This quantity satisfies the bound

$$K(\{\mathcal{E}_i\}) \leq E^\bigstar_R(\{\mathcal{E}_i\}) := \sup_{\mathcal{P}} \lim_n E_R(\rho^n_{\mathbf{ab}}). \tag{106}$$

where the REE E_R is defined in Eq. (85) with an implicit extension to asymptotic states.

In order to bound this capacity, let us perform a cut "i" which disconnects channel $\mathcal{E}_i$ between $\mathbf{r}_i$ and $\mathbf{r}_{i+1}$. We may then simulate channel $\mathcal{E}_i$ with a resource state σ_i, as in Eq. (88). By stretching the protocol with respect to $\mathcal{E}_i$, we may decompose Alice and Bob's output state as $\rho^n_{\mathbf{ab}} = \bar{\Lambda}_i\left(\sigma_i^{\otimes n}\right)$ for a trace-preserving LOCC $\bar{\Lambda}_i$, which is

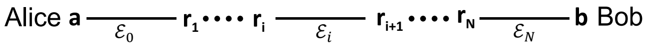

FIG. 6. Chain of N quantum repeaters $\mathbf{r}_1, \ldots, \mathbf{r}_N$ between Alice $\mathbf{a} := \mathbf{r}_0$ and Bob $\mathbf{b} := \mathbf{r}_{N+1}$. The chain is connected by $N+1$ quantum channels $\{\mathcal{E}_i\}$.

local between "super-Alice" (i.e., all the repeaters with $\leq i$) and the "super-Bob" (i.e., all the others with $\geq i+1$).

If we now compute the REE on the output state, we find $E_R(\rho^n_{\mathbf{ab}}) \leq nE_R(\sigma_i)$ for any i and protocol $\mathcal{P}$. By replacing this inequality in Eq. (106), we establish the single-letter bound [104, 105]

$$K(\{\mathcal{E}_i\}) \leq \min_i E_R(\sigma_i) \ . \tag{107}$$

Consider now a chain of teleportation-covariant channels $\{\mathcal{E}_i\}$, so that each quantum channel satisfies the condition in Eq. (89). These channels $\{\mathcal{E}_i\}$ can all be simulated by their (possibly-asymptotic) Choi matrices $\{\sigma_{\mathcal{E}_i}\}$. Therefore, Eq. (107) takes the form

$$K(\{\mathcal{E}_i\}) \leq \min_i E_R(\sigma_{\mathcal{E}_i}) \ . \tag{108}$$

For a chain connected by pure-loss channels with transmissivities η_i, we can replace $E_R(\sigma_{\mathcal{E}_i})$ with $-\log_2(1-\eta_i)$. Therefore, the bound takes the form

$$K(\{\mathcal{E}_i\}) \leq \min_i[-\log_2(1-\eta_i)] = -\log_2\left[1-\min_i \eta_i\right] \ . \tag{109}$$

This upper bound coincides with a lower bound. Assume that each pair of neighbor repeaters, $\mathbf{r}_i$ and $\mathbf{r}_{i+1}$, exchange a key at their channel capacity $K(\mathcal{E}_i) = -\log_2(1-\eta_i)$ and one-time pad is applied to all the keys to generate an end-to-end key at the minimum rate $\min_i K(\mathcal{E}_i)$. As a result, the upper bound above is saturated and we have an exact result for the secret key capacity of a lossy chain [104, 105]

$$K(\{\mathcal{E}_i\}) = -\log_2\left[1-\min_i \eta_i\right] \ . \tag{110}$$

Note that this capacity is fully determined by the minimum transmissivity in the chain. In particular, consider an optical fiber with transmissivity η which is split into $N+1$ parts by inserting N equidistant repeaters, so that each part has transmissivity $\sqrt[N+1]{\eta}$. Then, we write the capacity

$$K_{\text{loss}}(\eta, N) = -\log_2\left(1-\sqrt[N+1]{\eta}\right) \ . \tag{111}$$

For a single-repeater lossy chain, this gives exactly the result of Eq. (82).

[1] M. A. Nielsen, and I. L. Chuang, "Quantum computation and quantum information," (Cambridge University Press, Cambridge, 2000).

[2] C. Weedbrook, S. Pirandola, R. Garcia-Patron, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, "Gaussian quantum information," Rev. Mod. Phys. **84**, 621 (2012).

[3] W. Wootters, W. Zurek, "A Single quantum cannot be cloned," Nature **299**, 802 (1982).

[4] J. Park, "The concept of transition in quantum mechanics," Found. Phys. **1**, 23 (1970).

[5] T. M. Cover and J. A. Thomas, "Elements of Information Theory," 2nd Ed., Wiley Series in Telecommunications and Signal Processing, Wiley, New York (1996).

[6] I. Csiszar and J. Korner, "Information Theory: Coding Theorems for Discrete Memoryless Systems," Akademiai Kiado: 2nd edition, (1997).

[7] A. Holevo, "Bounds for the Quantity of Information Transmitted by a Quantum Communication Channel," Probl. Peredachi Inf. **9**, 3-11 (1973).

[8] I. Devetak and A. Winter, "Distillation of secret key and entanglement from quantum states," Proc. R. Soc. A **461**, 207 (2005).

[9] R. Renner, "Symmetry of large physical systems implies independence of subsystems," Nat. Phys. **3**, 645 (2007).

[10] R. Renner, "Security of quantum key distribution," Int. J. Quant. Inf. **6**, 1 (2008).

[11] R. Renner and J. I. Cirac, "de Finetti Representation Theorem for Infinite-Dimensional Quantum Systems and Applications to Quantum Cryptography," Phys.Rev. Lett. **102**, 110504 (2009).

[12] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," Int. Conf. on Computers, Systems & Signal Processing, Bangalore, India, Dec 9-12, 1984. Also at Theor. Comput. Sci. **560**, 7 (2014).

[13] G. Brassard, "Brief History of Quantum Cryptography: A Personal Perspective," Proceedings of IEEE Information Theory Workshop on Theory and Practice in Information Theoretic Security, Awaji Island, Japan, 19 (2005).

[14] C. H. Bennett, G. Brassard, S. Breidbart and S. Wiesner,"Quantum cryptography, or Unforgeable subway tokens", Advances in Cryptology: Proceedings of Crypto '82, Santa Barbara, Plenum Press, 267 (1982).

[15] A. K. Ekert, "Quantum cryptography based on Bell's theorem," Phys. Rev. Lett. **67**, 661 (1991).

[16] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without Bell's theorem," Phys. Rev. Lett. **68**, 557 (1992).

[17] A. Acín, N. Gisin and L. Masanes, "From Bell's Theorem to Secure Quantum Key Distribution," Phys. Rev. Lett. **97**, 120405 (2006).

[18] H.-K. Lo and H. F. Chau, "Unconditional security of quantum key distribution over arbitrarily long distances," Science **283**, 2050 (1999).

[19] P. W. Shor and J. Preskill, "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol," Phys.

Rev. Lett. **85**, 441 (2000).

[20] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," Phys. Rev. Lett. **68**, 3121 (1992).

[21] L. Goldenberg and L. Vaidman, "Quantum Cryptography Based on Orthogonal States," Phys. Rev. Lett. **75**, 1239-1243 (1995).

[22] T.-G. Noh, "Counterfactual Quantum Cryptography," Phys. Rev. Lett. **103**, 230501 (2009).

[23] M. Koashi and N. Imoto, "Quantum Cryptography Based on Split Transmission of One-Bit Information in Two Steps," Phys. Rev. Lett. **79**, 2383 (1997).

[24] T. Mor, "No Cloning of Orthogonal States in Composite Systems," Phys. Rev. Lett. **80**, 3137 (1998).

[25] H. Ollivier, and W. H. Zurek, "Quantum Discord: A Measure of the Quantumness of Correlations," Phys. Rev. Lett. **88**, 017901 (2001).

[26] K. Modi, A. Brodutch, H. Cable, T. Paterek, and V. Vedral, "The classical-quantum boundary for correlations: Discord and related measures," Rev. Mod. Phys. **84**, 1655 (2012).

[27] S. Pirandola, "Quantum discord as a resource for quantum cryptography," Sci. Rep. **4**, 6956 (2014).

[28] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum Cryptography," Rev. Mod. Phys. **74**, 145 (2002).

[29] S. Pirandola, "Symmetric collective attacks for the eavesdropping of symmetric quantum key distribution," Int. J. Quant. Inf. **6**, 765 (2008).

[30] C. A. Fuchs, N. Gisin, R. B. Griffiths, C.-S. Niu, and A. Peres "Optimal eavesdropping in quantum cryptography. I. Information bound and optimal strategy," Phys. Rev. A **56**, 1163-1172 (1997).

[31] C. S. Niu, and R. B. Griffiths, "Two-qubit copying machine for economical quantum eavesdropping" Phys. Rev. A **60**, 2764-2776 (1999).

[32] A. Peres, *Quantum Theory: Concepts and Methods* (Kluwer, Dordrecht, 1997).

[33] A. M. Steane, "Error Correcting Codes in Quantum Theory," Phys. Rev. Lett. **77**, 793-767 (1996).

[34] A. R. Calderbank, and P. W. Shor, "Good quantum error-correcting codes exist," Phys. Rev. A **54**, 1098-1105 (1996).

[35] A. M. Steane, "Multiple-particle interference and quantum error correction," Proc. Roy. Soc. Lond. A **452**, 2551-2577 (1996).

[36] H.-K. Lo, H. F. Chau, and M. Ardehali, "Efficient quantum key distribution scheme and a proof of its unconditional security," J. Cryptol. **18**, 133 (2005).

[37] D. Bruss, "Optimal Eavesdropping in Quantum Cryptography with Six States," Phys. Rev. Lett. **81**, 3018 (1998)

[38] H. Inamori, "Security of EPR-based Quantum Key Distribution using three bases," preprint quant-ph/0008076 (2000)

[39] H-.K. Lo, "Proof of unconditional security of six-state quantum key distribution scheme," Quant. Inf. Comp. **1**, 81-94 (2001).

[40] V. Scarani, S. Iblisdir, N. Gisin and A. Acín, "Quantum Cloning," Rev. Mod. Phys. **77**, 1225 (2005).

[41] D. Bruss, M. Cinchetti, G. M. D'Ariano and C. Macchiavello, "Phase-covariant quantum cloning," Phys. Rev. A. **62**, 012302 (2000).

[42] A. Chefles, "Quantum State Discrimination," Contemp. Phys. **41**, 401–424 (2000).

[43] S. M. Barnett and S. Croke, "Quantum state discrimination," Advances in Optics and Photonics **1**, 238-278 (2009).

[44] K. Tamaki, M. Koashi, and N. Imoto, "Unconditionally Secure Key Distribution Based on Two Nonorthogonal States," Phys. Rev. Lett. **90**, 167904 (2003).

[45] K. Tamaki and N. Lütkenhaus, "Unconditional security of the Bennett 1992 quantum key-distribution protocol over a lossy and noisy channel," Phys. Rev. A **69**, 032316 (2004).

[46] M. Koashi, "Unconditional Security of Coherent-State Quantum Key Distribution with a Strong Phase-Reference Pulse," Phys. Rev. Lett. **93**, 120501 (2004).

[47] K. Tamaki, "Unconditionally secure quantum key distribution with relatively strong signal pulse," Phys. Rev. A **77**, 032341 (2008).

[48] K. Tamaki, N. Lütkenhaus, M. Koashi, and J. Batuwantudawe, "Unconditional security of the Bennett 1992 quantum-key-distribution scheme with a strong reference pulse," Phys. Rev. A **80**, 032302 (2009).

[49] T. C. Ralph, "Continuous variable quantum cryptography," Phys. Rev. A **61**, 010303 (1999).

[50] T. C. Ralph, "Security of continuous-variable quantum cryptography," Phys. Rev. A **62**, 062306 (2000).

[51] M. Hillery, "Quantum cryptography with squeezed states," Phys. Rev. A **61**, 022309 (2000).

[52] M. D. Reid, "Quantum cryptography with a predetermined key, using continuous-variable Einstein-Podolsky-Rosen correlations," Phys. Rev. A **62**, 062308 (2000).

[53] N. J. Cerf, M. Lévy, and G. V. Assche, "Quantum distribution of Gaussian keys using squeezed states," Phys. Rev. A **63**, 052311 (2001).

[54] G. Van Assche, J. Cardinal, and N. Cerf, "Reconciliation of a Quantum-Distributed Gaussian Key," IEEE Trans. Inf. Theory **50**, 3940 (2004).

[55] D. Gottesman and J. Preskill, "Secure quantum key distribution using squeezed states," Phys. Rev. A **63**, 022309 (2001).

[56] F. Grosshans and P. Grangier, "Continuous Variable Quantum Cryptography Using Coherent States," Phys. Rev. Lett. **88**, 057902 (2002).

[57] F. Grosshans and P. Grangier, "Quantum cloning and teleportation criteria for continuous quantum variables," Phys. Rev. A **64**, 010301 (2001).

[58] C. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs, "Continuous Variable Quantum Cryptography: Beating the 3 dB Loss Limit," Phys. Rev. Lett. **89**, 167901 (2002).

[59] F. Grosshans and P. Grangier, "Reverse reconciliation protocols for quantum cryptography with continuous variables," arXiv preprint quant-ph/0204127 (2002).

[60] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and Ph. Grangier,"Quantum key distribution using gaussian-modulated coherent states," Nature **421**, 238 (2003).

[61] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, "Quantum Cryptography Without Switching," Phys. Rev. Lett. **93**, 170504 (2004).

[62] M. Navascués, F. Grosshans, and A. Acín, "Optimality of Gaussian Attacks in Continuous-Variable Quantum Cryptography," Phys. Rev. Lett. **97**, 190502 (2006).

[63] R. García-Patrón and N. J. Cerf, "Unconditional Optimality of Gaussian Attacks against Continuous-Variable Quantum Key Distribution," Phys. Rev. Lett. **97**, 190503 (2006).

[64] S. Pirandola, S.Lloyd and S.L. Braunstein, "Characterization of Collective Gaussian Attacks and Security of Coherent-State Quantum Cryptography," Phys. Rev. Lett. **101**, 200504 (2008).

[65] R. García-Patrón, "Quantum information with optical continuous variables," Ph.D. thesis, Université Libre de Bruxelles (2007).

[66] V. Usenko and R. Filip, "Trusted Noise in Continuous-Variable Quantum Key Distribution: A Threat and a Defense," Entropy **18**, 20 (2016).

[67] F. Laudenbach and C. Pacher, "Analysis of the Trusted-Device Scenario in Continuous-Variable Quantum Key Distribution," Advanced Quantum Technologies **2**, 1900055 (2019).

[68] N. Hosseinidehaj, N. Walk, and T. C. Ralph, "Optimal realistic attacks in continuous-variable quantum key distribution," Phys. Rev. A **99**, 052336 (2019).

[69] Z. Pan, K. P. Seshadreesan, W. Clark, M. R. Adcock, I. B. Djordjevic, J. H. Shapiro, and S. Guha, "Secret key distillation across a quantum wiretap channel under restricted eavesdropping," preprint arXiv:1903.03136 (2019).

[70] S. Pirandola, S. Mancini, S. Lloyd, S. L. Braunstein, "Continuous Variable Quantum Cryptography using Two-Way Quantum Communication," Nat. Phys. **4**, 726 (2008).

[71] C. Ottaviani, S. Mancini, and S. Pirandola, "Gaussian two-mode attacks in one-way quantum cryptography," Phys. Rev. A **92**, 062323 (2015).

[72] C. Ottaviani and S. Pirandola, "General immunity and superadditivity of two-way Gaussian quantum cryptography," Sci. Rep **6**, 22225 (2016).

[73] R. Filip, "Continuous-variable quantum key distribution with noisy coherent states," Phys. Rev. A **77**, 022310 (2008).

[74] V. C. Usenko and R. Filip, "Feasibility of continuous-variable quantum key distribution with noisy coherent states," Phys. Rev. A **81**, 022318 (2010).

[75] C. Weedbrook, S. Pirandola, S. Lloyd, and T. C. Ralph, "Quantum Cryptography Approaching the Classical Limit," Phys. Rev. Lett. **105**, 110501 (2010).

[76] C. Weedbrook, S. Pirandola, and T. C. Ralph, "Continuous-variable quantum key distribution using thermal states," Phys. Rev. A **86**, 022318 (2012).

[77] C. Weedbrook, C. Ottaviani, S. Pirandola, "Two-way quantum cryptography at different wavelengths," Phys. Rev. A **89**, 012309 (2014).

[78] V. C. Usenko and F. Grosshans, "Unidimensional continuous-variable quantum key distribution," Phys. Rev. A **92**, 062337 (2015).

[79] T. Gehring, C. S. Jacobsen, and U. L. Andersen, "Single-quadrature continuous-variable quantum key distribution," Quantum Information and Computation **16**, 1081 (2016).

[80] S. Pirandola, C. Ottaviani Gaetana Spedalieri, Christian Weedbrook, Samuel L. Braunstein, Seth Lloyd, Tobias Gehring, Christian S. Jacobsen and Ulrik L. Andersen, "High-rate quantum cryptography in untrusted networks," Nature Photon. **9**, 397 (2015). See also preprint arXiv:1312.4104 (2013).

[81] C. Ottaviani, G. Spedalieri, S. L. Braunstein and S. Pirandola, "Continuous-variable quantum cryptography with an untrusted relay: Detailed security analysis of the symmetric configuration," Phys. Rev. A **91**, 022320 (2015).

[82] Y. Guo, Q. Liao, Y. Wang, D. Huang, P. Huang, and G. Zeng, "Performance improvement of continuous-variable quantum key distribution with an entangled source in the middle via photon subtraction," Phys. Rev. A **95**, 032304 (2017).

[83] Y. Guo, W. Ye, H. Zhong, and Q. Liao, "Continuous-variable quantum key distribution with non-Gaussian quantum catalysis," Phys. Rev. A **99**, 032327 (2019).

[84] M. Ghalaii, C. Ottaviani, R. Kumar, S. Pirandola, M. Razavi, "Long-distance continuous-variable quantum key distribution with quantum scissors," preprint arXiv:1808.01617 (2018).

[85] P. Papanastasiou, C. Weedbrook, and S. Pirandola, "Continuous-variable quantum key distribution in fast fading channels," Phys. Rev. A **97**, 032311 (2018).

[86] S. Tserkis, N. Hosseinidehaj, N. Walk, and T. C. Ralph, "Teleportation-based collective attacks in Gaussian quantum key distribution," preprint arXiv:1908.07665 (2019).

[87] V. C. Usenko, "Generalized security analysis framework for continuous-variable quantum key distribution," preprint arXiv:1908.01127 (2019).

[88] M. Lasota, R. Filip, and V. C. Usenko, "Robustness of quantum key distribution with discrete and continuous variables to channel noise," Phys. Rev. A **95**, 062312 (2017).

[89] R. García-Patrón and N. J. Cerf, "Continuous-Variable Quantum Key Distribution Protocols Over Noisy Channels," Phys. Rev. Lett. **102**, 130501 (2009).

[90] R. García-Patrón, S. Pirandola, S. Lloyd, and J. H. Shapiro, "Reverse Coherent Information," Phys. Rev. Lett. **102**, 210501 (2009).

[91] S. Pirandola, R. García-Patrón, S. L. Braunstein, and S. Lloyd, "Direct and Reverse Secret-Key Capacities of a Quantum Channel," Phys. Rev. Lett. **102**, 050503 (2009).

[92] L. S. Madsen, V. C. Usenko, M. Lassen, R. Filip, and U. L. Andersen, "Continuous variable quantum key distribution with modulated entangled states," Nat. Commun. **3**, 1083 (2012).

[93] C. Ottaviani, R. Laurenza, T. P. W. Cope, G. Spedalieri, S. L. Braunstein, S. Pirandola, "Secret key capacity of the thermal-loss channel: improving the lower bound," SPIE proceedings Quantum Information Science and technology II, **9996**, 999609 (2016).

[94] G. Wang, C. Ottaviani, H. Guo, S. Pirandola, "Improving the lower bound to the secret-key capacity of the thermal amplifier channel," Eur. Phys. J. D **73**, 17 (2019).

[95] S. Pirandola, S L Braunstein, R. Laurenza, C. Ottaviani, T. P. W. Cope, G. Spedalieri, and L. Banchi, "Theory of channel simulation and bounds for private communication," Quantum Sci. Technol. **3**, 035009 (2018).

[96] S. Pirandola, R. Laurenza, C. Ottaviani and L. Banchi, "Fundamental Limits of Repeaterless Quantum Communications," Nature Comm. **8**, 15043 (2017). See also arXiv:1510.08863 (2015).

[97] I. Devetak, M. Junge, C. King, and M. B. Ruskai, "Mul-

tiplicativity of Completely Bounded p-Norms Implies a New Additivity Result," Commun. Math. Phys. **266**, 37 (2006).

[98] M. Hayashi, "Quantum Information Theory: Mathematical Foundation," (Springer-Verlag, Berlin, 2017).

[99] B. Schumacher and M. A. Nielsen, "Quantum data processing and error correction," Phys. Rev. A **54**, 2629 (1996).

[100] S. Lloyd, "Capacity of the noisy quantum channel," Phys. Rev. A **55**, 1613 (1997).

[101] V. Vedral, "The role of relative entropy in quantum information theory," Rev. Mod. Phys. **74**, 197 (2002).

[102] V. Vedral, M. B. Plenio, M. A. Rippin, and P. L. Knight, "Quantifying Entanglement," Phys. Rev. Lett. **78**, 2275 (1997).

[103] V. Vedral and M. B. Plenio, "Entanglement measures and purification procedures," Phys. Rev. A **57**, 1619 (1998).

[104] S. Pirandola, "Capacities of repeater-assisted quantum communications," Preprint arXiv:1601.00966 (2016).

[105] S. Pirandola, "End-to-end capacities of a quantum communication network," Commun. Phys. **2**, 51 (2019).

[106] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Overcoming the rate-distance limit of quantum key distribution without quantum repeaters," Nature **557**, 400 (2018).

[107] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, "Secure Key from Bound Entanglement," Phys. Rev. Lett. **94**, 160502 (2005).

[108] R. Laurenza, S. L. Braunstein, and S. Pirandola, "Finite-resource teleportation stretching for continuous-variable systems," Sci. Rep. **8**, 15267 (2018).

[109] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," Phys. Rev. Lett. **70**, 1895 (1993).

[110] S. L. Braunstein and H. J. Kimble, "Teleportation of Continuous Quantum Variables," Phys. Rev. Lett. **80**, 869–872 (1998).

[111] S. L. Braunstein, G. M. D'Ariano, G. J. Milburn, and M. F. Sacchi, "Universal Teleportation with a Twist," Phys. Rev. Lett. **84**, 3486 (2000).

[112] S. Pirandola, J. Eisert, C. Weedbrook, A. Furusawa, and S. L. Braunstein, "Advances in Quantum Teleportation," Nature Photonics **9**, 641-652 (2015).