Review

Distributing Secret Keys with Quantum Continuous Variables: Principle, Security and Implementations

Eleni Diamanti [1,*] **and Anthony Leverrier** [2]

[1] Laboratoire Traitement et Communication de l'Information, CNRS, Telecom ParisTech, 23 avenue d'Italie, Paris 75013, France

[2] Inria, EPI SECRET, B.P. 105, Le Chesnay Cedex 78153, France; E-Mail: anthony.leverrier@inria.fr

* Author to whom correspondence should be addressed; E-Mail: eleni.diamanti@telecom-paristech.fr; Tel.: +33-1-45817114.

Abstract: The ability to distribute secret keys between two parties with information-theoretic security, that is regardless of the capacities of a malevolent eavesdropper, is one of the most celebrated results in the field of quantum information processing and communication. Indeed, quantum key distribution illustrates the power of encoding information on the quantum properties of light and has far-reaching implications in high-security applications. Today, quantum key distribution systems operate in real-world conditions and are commercially available. As with most quantum information protocols, quantum key distribution was first designed for qubits, the individual quanta of information. However, the use of quantum continuous variables for this task presents important advantages with respect to qubit-based protocols, in particular from a practical point of view, since it allows for simple implementations that require only standard telecommunication technology. In this review article, we describe the principle of continuous-variable quantum key distribution, focusing in particular on protocols based on coherent states. We discuss the security of these protocols and report on the state-of-the-art in experimental implementations, including the issue of side-channel attacks. We conclude with promising perspectives in this research field.

Keywords: quantum key distribution; quantum information; quantum cryptography; quantum optics; security

1. Introduction

In a seminal result in 1984, Bennett and Brassard showed that it is possible for two parties to distribute a secret key in a way that is unconditionally secure against any adversary, even a quantum one [1]. This fundamental primitive, namely quantum key distribution (QKD), is of great importance for many cryptographic tasks, such as one-time pad encrypted secure communication [2] or message authentication [3]. It has been thoroughly studied both in theory and in practice; indeed, the rapid progress in the field has enabled the distribution of secret keys with information-theoretic security over deployed optical fiber networks [4,5], and QKD systems are available on the market [6]. The two communicating parties of a QKD protocol [7], Alice and Bob, can in principle share an information-theoretic secret key after the exchange of a large number of quantum signals through a physical channel, known as a quantum channel, which is subject to eavesdropping, and additional information sent on a public, but authenticated classical channel. After Alice and Bob have agreed on a set of non-commuting quantum operators, they can encode some information into these variables: any attempt by the eavesdropper, Eve, to recover this information necessarily disturbs the transmitted quantum states and is discovered after random sampling of a fraction of Alice and Bob's correlated data.

In most commonly-used QKD systems, the key information is encoded on properties of single photons, and thus, specific components for single-photon detection are required. The quest for high-performance quantum key distribution systems in the last few years has led to several successful demonstrations based on these discrete-variable or distributed-phase reference protocols [8–11]. There exists, however, a different type of protocol, in which information is carried by properties of light that are continuous, such as the values of the quadrature components of a coherent state. The use of such continuous-variable quantum information carriers, instead of qubits, constitutes a powerful alternative approach for QKD and more generally for quantum information processing [12]. From a practical point of view, for instance, continuous-variable (CV) QKD protocols present the major advantage that they only require standard telecommunication technology, and in particular, instead of dedicated photon-counting technology, they use coherent detection techniques widely used in classical optical communications. It is important to emphasize that there is a significant conceptual difference between these protocols and the standard BB84 protocol proposed by Bennett and Brassard [1] and other discrete-variable protocols, even if the latter use coherent states: as we will see in detail in the following sections, information is encoded on non-orthogonal states, which captures the quantum nature of the CVQKD protocols; however, entirely different degrees of freedom are used in this case. This brings the need for different security proof techniques while at the same time opening the way to very practical implementations.

In the following, we begin by describing, in Section 2, the principle of CVQKD protocols focusing in particular on protocols using Gaussian modulation of coherent states. We then proceed in Section 3 with an overview of the current status of security proofs for such protocols. In Section 4, we discuss the implementations of CVQKD protocols, including the first long-distance experiments of quantum key distribution using continuous variables, and in Section 5, we provide a brief overview of theoretical and experimental studies on the security of CVQKD systems in the presence of practical imperfections and side channels. Finally, in Section 6, we provide a comprehensive presentation of major challenges and

perspectives in the field. Our goal in this review article is not to describe exhaustively all of available CVQKD protocols and implementations, but to focus on specific, well-understood examples to facilitate the understanding of the main ideas behind this approach for quantum key distribution.

2. Principle of CVQKD with Coherent States

By definition, all CVQKD protocols encode information in the quadratures of the quantized electromagnetic field. This information is then recovered thanks to coherent detection techniques, in particular homodyne (or heterodyne) detection of those quadratures. From this perspective, the main distinction between discrete-variable and continuous-variable protocols lies in the detection technique that is employed: single-photon detection for the former and homodyne (or heterodyne) for the latter.

A number of CV protocols has been proposed in the literature and depend on the choice of states that are prepared: single-mode coherent or squeezed states, two-mode squeezed states; on the choice of modulation for single-mode states, Gaussian or non-Gaussian; on the choice of detection, homodyne or heterodyne; and finally, on the type of error correction (or else, reconciliation), direct or reverse. Of course, some of these protocols are easier to implement, and some have better security proofs than others. In this review, we will mainly focus on the simplest ones, which are also the best understood ones, namely one-way protocols using a Gaussian modulation. Other protocols have been investigated in the literature: two-way protocols [13,14], protocols with a non-Gaussian modulation [15–19] or post-selection [20]; but, their security analysis is less advanced, and we will not consider them further in this short review.

As usual with QKD, a given protocol has two possible implementations, prepare and measure (PM) or entanglement based (EB), which are known to be equivalent in the case of Gaussian protocols [21]. In the first case, Alice simply prepares and sends Gaussian states to Bob, who measures them with coherent detection; in the second version, Alice generates bipartite entangled states, measures the first half and sends the second half to Bob, who measures it. As long as Alice's lab and preparation is trusted, both variants have the same security. More precisely, the security of the PM version reduces to that of the EB protocol. For this reason, it is only necessary to analyze the security of EB QKD protocols.

Implementations, on the other hand, are usually simpler for PM protocols. The simplest CVQKD protocol is certainly GG02 introduced by Grosshans and Grangier in 2002 [22], or its variant with heterodyne detection [23]. We now describe the rough outline of this protocol. A much more detailed description can be found elsewhere [24], but is out of the scope of this paper. The protocol consists of four main steps: (i) state distribution and measurement; (ii) error reconciliation; (iii) parameter estimation; and (iv) privacy amplification. Note that historically, parameter estimation used to be applied before error correction, but the novel order turns out to be more efficient.

(i) State distribution and measurement: Alice prepares a large number of coherent states $|\alpha_1\rangle, \ldots, |\alpha_N\rangle$, where α_i are independent and identically distributed complex Gaussian variables $\mathcal{N}_{\mathbb{C}}(0, V_0)$ with variance V_0. Depending on the protocol (homodyne or heterodyne), Bob measures either a random quadrature (x or p) for each state and informs Alice of his choices or both quadratures. Bob then obtains a list of N or $2N$ real-valued numbers corresponding to his measurement outcomes. Alice has also access to her own list of data (she keeps only the relevant quadrature values if Bob

performed a homodyne detection). Denote the respective lists of Alice and Bob by $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ (where n is either N or $2N$).

(ii) Error reconciliation: The protocol achieves in general better performance with reverse reconciliation [25] (except at very short distances [26]): this means that Bob's string corresponds to the raw key, and Alice tries to guess its value. To achieve that objective, Alice and Bob use classical error correction techniques. More precisely, Alice and Bob agree on a linear error-correcting code before the protocol starts, and Bob sends to Alice the value of the syndrome of y for this code. To recover y, Alice simply needs to correct x, that is to decode in the coset code defined by the syndrome she received.

(iii) Parameter estimation: This step is useful to obtain an upper bound on the information available to Eve. For CVQKD protocols, this typically requires estimating the covariance matrix of the bipartite state shared by Alice and Bob. Once this estimate is obtained, Alice and Bob can compute the size ℓ of a secure key that they can extract from their state.

(iv) Privacy amplification: Alice and Bob apply a random universal hash function to their respective (corrected) strings and obtain two strings S_A and S_B of length ℓ.

Variants of this protocol can differ in the type of states that are prepared (coherent, squeezed or even thermal) and in the detection (homodyne or heterodyne), but the main steps of the protocol remain basically identical.

3. Security Analysis

In this section, we address the security of CVQKD protocols with the assumption that Alice and Bob's labs, and equipment, are trusted. Note that this does not require that their source or detectors are perfect, but rather that their potential imperfections are well understood and can be modeled properly. For instance, Bob's detectors could have imperfect efficiency or add electronic noise. Such models can be easily incorporated into the security analysis. However, we exclude side-channel attacks from the present analysis and will only discuss them in Section 5.

Security analysis for quantum key distribution protocols has evolved in a tremendous manner in the last decade. For a long time, the standard was to consider collective attacks in the asymptotic limit on infinitely long keys, and the goal was to compute the corresponding asymptotic collective key rate $K_{\text{coll}}^{\text{asympt}}$, given by [27,28]:

$$K_{\text{coll}}^{\text{asympt}} = I(A;B) - \chi(B;E), \tag{1}$$

where $I(A;B)$ is the mutual information between Alice and Bob's measurements outcomes and $\chi(B;E)$ is the Holevo information between Bob's string and Eve's quantum system. Note that $\chi(B;E)$ should be replaced by $\chi(A;E)$ for protocols with direct reconciliation. In a realistic setting, Alice and Bob cannot extract all of the information from their data, and it is usual to replace $I(A;B)$ by $\beta I(A;B)$, where the factor $\beta < 1$ is the so-called reconciliation efficiency. The Devetak–Winter formula, Equation (1), is usually assumed to hold for continuous-variable protocols, and the challenge was therefore to compute $\chi(B;E)$ or at least an upper bound for it. Indeed, the quantity $\beta I(A;B)$ can be directly observed in an experiment.

The asymptotic limit assumption is very helpful for obtaining an upper bound on $\chi(B;E)$. Indeed, one is in the situation where a given state can be observed a large number of times and can therefore

be precisely estimated. In particular, one typically assumes that the covariance matrix Γ_{AB} of the bipartite state ρ_{AB} shared by Alice and Bob is known. Then, using the optimality properties of Gaussian states [29], one can show that $\chi(B; E)$ is upper bounded by its value computed for the Gaussian state of covariance matrix Γ_{AB} [30,31]:

$$\chi(B; E) \leq f(\Gamma_{AB}), \tag{2}$$

where f is an entropic function depending on the symplectic eigenvalues of Γ_{AB} and $\Gamma_{A|b}$, the covariance matrix of Alice's state conditioned on Bob's measurement result. This last step completes the analysis of the security of one-way CVQKD protocols against collective attacks in the asymptotic limit.

More recently, a new paradigm for evaluating the security of QKD protocols has been put forward, notably by Renner [32], following the universal composability framework of Canetti [33]. In this paradigm, the QKD protocol is seen as a completely positive and trace-preserving map that takes as input an arbitrary bipartite state $\rho_{A^N B^N}$ consisting of N quantum systems, *a priori* unknown to Alice and Bob, and returns a final state $\rho_{S_A S_B E}$ where S_A, S_B correspond to Alice and Bob's final keys and E denotes Eve's quantum register. The aim of this framework is to assign a number, ε, to quantify the security of the protocol: $\varepsilon = 0$ corresponding to perfect security. Moreover, we still want our notion of security to be composable (as was already the case with the Devetak–Winter approach), meaning that a protocol obtained by composing two subprotocols with respective security parameters ε_1 and ε_2 should have a security parameter $\varepsilon \leq \varepsilon_1 + \varepsilon_2$. Such a requirement is achieved by taking ε to be an upper bound on the distance between the protocol under study and an ideal protocol. In particular, one can consider the trace distance between the output state produced by the protocol, $\rho_{S_A S_B E}$ and the ideal state, which is $\tau_{SS} \otimes \rho_E$, where $\tau_{SS} = \frac{1}{2^\ell} \sum_{s \in \{0,1\}^\ell} |s, s\rangle\langle s, s|$ describes a uniformly-chosen key of length ℓ, identical for Alice and Bob, and where the tensor product indicates that Eve's system is completely uncorrelated with the final key:

$$\frac{1}{2} \|\rho_{S_A S_B E} - \tau_{SS} \otimes \rho_E\|_1 \leq \varepsilon. \tag{3}$$

Let us summarize the various notions of security proofs present in the literature from the strongest one to the weakest one:

1. Composable security against arbitrary attacks, if one can bound the trace distance of Equation (3), without any restriction on the input state $\rho_{A^N B^N}$ of the protocol.
2. Composable security against collective attacks, if one can bound the trace distance of Equation (3) under the restriction that the input state is identically and independently distributed, *i.e.*, $\rho_{A^N B^N} = \rho_{AB}^{\otimes N}$.
3. Security against collective attacks in the asymptotic limit of infinitely many uses of the channel, if one can compute an upper bound on the Holevo information, $\chi(B; E)$ from Equation (1), between the raw key and the adversary, assuming that the quantum state shared by Alice and Bob is known. In the case of CV protocols, one only needs to assume that the covariance matrix of the state is known.

Let us denote the respective secure key rates (final key length ℓ divided by the number N of channel uses) for these three notions of security by $K^\varepsilon(N), K^\varepsilon_{\text{coll}}(N)$ and $K^{\text{asympt}}_{\text{coll}}$. The first two quantities,

which involve (smooth) conditional min-entropies (defined by Renner in [32] and later extended to infinite-dimensional quantum systems [34,35]), include finite-size effects and, therefore, depend on N. On the other hand, the asymptotic key rate is independent of N. Since $K^\varepsilon(N) \leq K^\varepsilon_{\text{coll}}(N) \leq K^{\text{asympt}}_{\text{coll}}$, the main question is to determine whether $K^\varepsilon(N)$ indeed converges to $K^{\text{asympt}}_{\text{coll}}$ in the asymptotic limit and at which rate. Often, in the literature, one can read that computing the value of $K^{\text{asympt}}_{\text{coll}}$ is sufficient because de Finetti-type reductions, such as [36,37], show that the same value also holds for arbitrary attacks. The situation is unfortunately not so simple: de Finetti reductions only make sense in the composable setting, and in general, computing the Devetak–Winter formula is not sufficient to claim security against arbitrary attacks in the finite-size setting.

In general, one can either prove security against arbitrary attacks directly, for instance using the uncertainty principle as in [38,39] following the results from [40], or one can first establish security against collective attacks (in the finite-size regime) and obtain a security claim against arbitrary attacks (with a worse value of ε) using a de Finetti reduction [36,37]. So far, this second approach was only applied for the protocol [23] with coherent states and heterodyne detection [24].

Table 1. Current security status of the main one-way continuous-variable quantum key distribution (CVQKD) protocols. PM, prepare and measure.

Protocol	(PM) State Preparation	(PM) Modulation	Bob's Measurement	Best Currently-Available Security Proofs
[41]	squeezed	Gaussian	homodyne	Finite-size [38,39] $K^\varepsilon(N) > 0$ for practical N $\lim_{N\to\infty} K^\varepsilon(N) < K^{\text{asympt}}_{\text{coll}}$
[23]	coherent	Gaussian	heterodyne	Finite-size [24] $K^\varepsilon_{\text{coll}}(N) \approx K^{\text{asympt}}_{\text{coll}}$ for practical N $K^\varepsilon(N) = 0$ for practical N [37]
[22]	coherent	Gaussian	homodyne	asymptotic collective [30,31,42]
[43]	coherent	Gaussian 1D	homodyne	asymptotic collective [43]
[44]	squeezed	Gaussian	heterodyne	asymptotic collective [45]
[46]	thermal	Gaussian	homo/heterodyne	asymptotic collective [47–49]
[50]	squeezed	Gaussian + additional Gaussian	homodyne	asymptotic collective [50]
[51,52]	coherent	Gaussian	homo/heterodyne + Gaussian post-selection	asymptotic collective [51,52]

That being said, the behavior of the quantity $K^{\text{asympt}}_{\text{coll}}$ is still interesting, because it allows us to compare the various protocols and to understand the effect of losses and noise on the secret key rate. Moreover, it is reasonable to think that the proof technique of [24] can be generalized to most protocols with a Gaussian modulation and that the composable secret key rate $K^\varepsilon_{\text{coll}}(N)$ valid against collective attacks will converge to the asymptotic key rate for reasonable values of N. For this reason, computing an upper bound on the Holevo information $\chi(B;E)$, that is a lower bound on $K^{\text{asympt}}_{\text{coll}}$, is an important first step in security proofs for continuous-variable QKD.

In Table 1, we summarize the current state-of-the-art for security proofs for CVQKD with a Gaussian modulation. Two protocols have complete security proofs in the composable security framework.

Their entanglement-based version consists of preparing N two-mode squeezed states and measuring each mode with either homodyne detection (of a randomly-chosen quadrature) for [41] or with heterodyne detection for [23]. The proof techniques are quite different: the security of [41] is based on an entropic uncertainty principle for continuous variables [40], while the security of [23] is obtained in two steps (security against collective attacks followed by a reduction from general attacks). Despite this success, improvements are still called for. Indeed, in the first case of [41], the security proof provides a positive secret key rate $K^\varepsilon(N)$, which is positive for reasonable values of N, but unfortunately, the key rate does not converge to $K_{\mathrm{coll}}^{\mathrm{asympt}}$ for $N \to \infty$, which indicates that either the true secret key rate is overestimated by $K_{\mathrm{coll}}^{\mathrm{asympt}}$ or, more likely, that the proof technique should be improved. On the other hand, in the case of the heterodyne protocol with coherent states [23], the quantity $K^\varepsilon(N)$ converges to the asymptotic value $K_{\mathrm{coll}}^{\mathrm{asympt}}$, corresponding to a Gaussian attack, but the convergence is too slow to obtain a positive key rate for a reasonable block size N. The main issue lies in the reduction from general to collective attack using either de Finetti's theorem [36] or the post-selection technique [37] (also known as a de Finetti reduction). We insist on the fact that these limitations might be due to insufficient proof techniques. Indeed, it is quite possible that better security proofs will be found and establish that $K^\varepsilon(N)$ converges to $K_{\mathrm{coll}}^{\mathrm{asympt}}$ for reasonable block lengths. We believe that this is certainly the most pressing issue in the theoretical study of CVQKD.

The security of the other protocols in the finite-size regime is less clear, and only the asymptotic key rate $K_{\mathrm{coll}}^{\mathrm{asympt}}$ is known. Applying the tools of [38,39] or [24] is not straightforward in these cases, because squeezed states and homodyne detection seem to be required in order to use the entropic uncertainty relation, and the protocol must be sufficiently symmetric for the analysis of [24] to go through. Establishing the composable security of these protocols remains an open question.

To conclude this section, we note that even if security proofs improve a lot in the next few years, finite-size effects will still remain an important issue for CVQKD. Indeed, the best case scenario would be that Gaussian attacks are optimal for all of these protocols, which would imply that Alice and Bob need to estimate the covariance matrix of the state they share. In particular, they would need to compute bounds on the quantum channel parameters (see Section 4 for details), a task that necessarily requires many data in the long distance (high loss) scenario. The consequence is that very large block lengths and, therefore, extremely stable optical setups will be necessary to obtain composable security in experimental implementations.

4. Experimental Implementations

In the previous sections, we have seen that continuous-variable QKD protocols may vary in terms of required resources, in particular for state preparation (squeezed or coherent states) and detection techniques (homodyne or heterodyne). These choices are of great importance for the security achieved by the corresponding implementations (see Table 1), but also affect their performance, which is typically quantified by the maximal distance over which secret keys can be generated and the rate of their production. Another important choice is the medium used for the transmission of the quantum keys, namely optical fiber or free space, which depends on the targeted application of the QKD implementation. It is interesting to remark here on a historical note that initial proposals for CVQKD

necessitated the use of squeezed states and were burdened by a 3-dB loss limit [41,53], which greatly limited their practical interest in any realistic communication scenario. Later, however, protocols using coherent states appeared (GG02) [22], and the 3-dB limit was lifted [20,25]. These results enhanced considerably the interest in the use of continuous variables for QKD and were at the basis of a series of works that led to ever better performing systems.

As in discrete-variable QKD, PM CVQKD protocols are in general easier to implement in practice. We describe in the following in some detail PM fiber optic implementations of the GG02 protocol, whose principle and security were discussed in Sections 2 and 3, respectively. This protocol is particularly interesting from a practical point of view, since it merely necessitates the generation of coherent states, their modulation in phase space and the detection of the quadratures of the received states using homodyne (or heterodyne) techniques. The components required to achieve these functionalities are readily available at a telecommunication wavelength, which is suitable for operation with fiber optic systems.

The optical configuration for performing this protocol is shown in Figure 1. In this scheme, the signal and phase reference (or local oscillator) that is necessary for performing the coherent detection are generated from a laser diode source at Alice's site. The signal is modulated in amplitude and phase following a Gaussian distribution as required by the protocol and then attenuated at a suitable modulation variance level. It is also multiplexed both in time and in polarization with the local oscillator before entering the quantum channel. At Bob's site, the two signals are demultiplexed using, respectively, a delay line and a polarization beam splitter and superposed in time to interfere on a shot noise-limited balanced pulsed homodyne detector. The quadrature selection required by the GG02 protocol is performed by the phase modulator placed in the local oscillator path. The setup is completed by several active feedforward and control elements, which provide the necessary synchronization and stability conditions for performing the quantum key distribution.
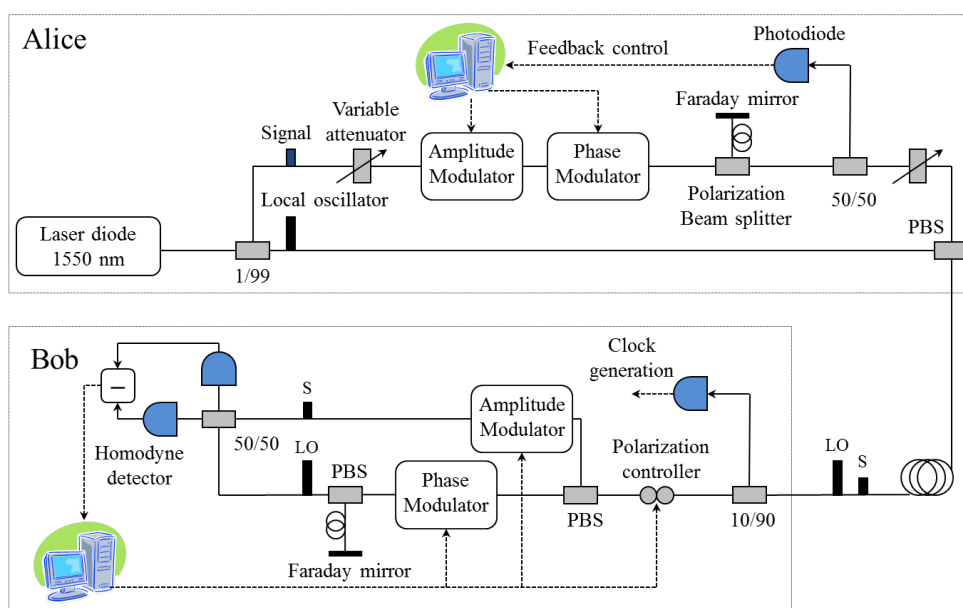
Figure 1. Optical layout of a fiber optic CVQKD system implementing the GG02 [22] protocol with homodyne detection.

The described system realizes the first part, namely (i) state distribution and measurement, of the full GG02 protocol described in Section 2; the remaining post-processing parts, namely (ii) error reconciliation, (iii) parameter estimation and (iv) privacy amplification, and, in particular, the first two, require sophisticated computational algorithms, as we will discuss further below.

The initial realization of the optical setup of Figure 1 was used in the European SECOQC QKD network [4], which was deployed over installed optical fibers and integrated various QKD technologies [4,54]. It was also used in a field test of a point-to-point classical symmetric encryption link with fast key renewal provided by the quantum layer, which demonstrated the reliability of the CVQKD system operation over a long period of time in a server room environment [55]. These implementations, together with a few others [56–59], were suited for securing communications in metropolitan area size networks (involving distances up to 25 km) with high-speed requirements. Although there are several interesting applications of short-range experiments, from a quantum information network point of view, it is important to be able to extend the communication distance beyond this limit. In discrete-variable QKD implementations, the distance limitation is essentially determined by the characteristics of single-photon detectors, and in particular their dark counts. In CVQKD, it used to be the efficiency of the complex post-processing techniques that limited the range. Although this is no longer the case, it is instructive to understand the origin of this limitation: the efficient reconciliation of correlated Gaussian variables is in fact hard, especially at low signal-to-noise (SNR) ratios, which are inherent in long-distance experiments, hence reducing the β factor introduced in Section 3. An an indicative value, β = 0.9 was achieved for an SNR = 3 (at Bob's site) in the aforementioned experiments. In recent years, a series of works successfully addressed this issue leading to the development of highly-efficient error-correcting codes at low SNR. These combine multidimensional reconciliation techniques [60] with efficient multi-edge low density parity check (LDPC) codes [61] and can also be optimized for short distances [26]. With these codes, it is possible to reach, for example, an efficiency β = 0.96 at SNR = 0.075, opening the way to experiments over significantly longer distances. We note that with the help of non-binary LDPC codes, similar efficiencies can also be obtained for higher values of the SNR [62].

In addition to error correction, the parameter estimation procedure is also crucial for the extraction of the secret key in practice. For the optical setup of Figure 1, the relevant experimental parameters are Alice's modulation variance V_A, the channel transmittance T and the excess noise ξ, which is the noise added by the channel beyond the fundamental shot noise and corresponds to the usual quantum bit error rate found in discrete-variable QKD implementations. Both V_A and ξ are typically expressed in shot noise units. The parameter V_A is adjusted in real time in order to be at all times as close as possible to the SNR corresponding to the threshold of an available error correcting code, while the parameters T and ξ need to be estimated in real time by randomly revealing a fraction of the samples. Two additional experimental parameters that are used to compute an estimate of the secret information that can be extracted from the shared data are the electronic noise v_{el} and the efficiency η of the homodyne detection. In the so-called realistic CVQKD scenario, these are assumed to not be accessible to Eve and are measured during a secure calibration procedure that takes place before the deployment of the system. In general, however, these parameters may be available to Eve. The parameter estimation procedure allows one to compute bounds for the eavesdropper's information, taking calibrated value uncertainties into account [63].

Following error reconciliation and parameter estimation, privacy amplification allows extracting the secret information from the identical strings shared by Alice and Bob. For the scheme of Figure 1, the upper bound on Eve's information on the corrected string can be computed for collective attacks in both the asymptotic regime [30,31], where all of the experimental parameters are assumed to be known with an infinite precision, and in the finite-size regime, where the parameters are estimated over large, but finite data pulse sets [63] (see Section 3 for rigorous security definitions). The secret key generation rates obtained with a system implementing this scheme, operating at a 1-MHz repetition rate, are shown in Figure 2 as a function of distance. Secret key generation is possible in this case at distances as long as 80 km with a data block size of 10^9 [64]. These results correspond to the current state-of-the-art in communication range for the continuous-variable QKD technology. In the same figure, we include some representative results of implementations of other CVQKD protocols. We note in particular a recent implementation involving the use of squeezed states and homodyne detectors with the goal of demonstrating composable security against arbitrary attacks (see Table 1), albeit at short distances [62]. Composable security against this type of attack has yet to be shown with coherent states. In this case, as was discussed in Section 3, a security proof is available for heterodyne detection [24], but this setting was only been studied experimentally a few years ago and, therefore, does not take finite-size effects into account [65]. Finally, we note an early implementation of the protocol employing Gaussian post-selection [66], whose security proof was extended later in [51,52].
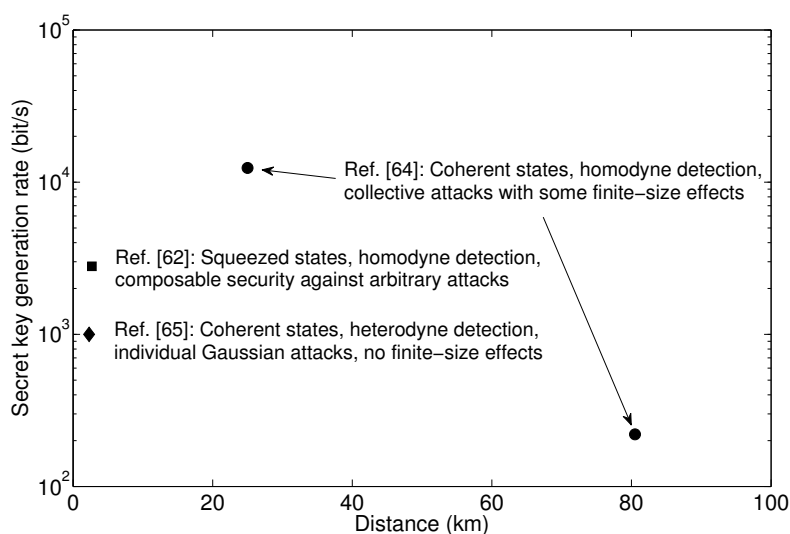
Figure 2. Experimental results obtained for various CVQKD protocols offering different levels of security. The distance for the results of [62] and [65] has been calculated from data obtained with free-space experiments (expressed in dB) assuming an optical fiber with an attenuation coefficient of 0.2 dB/km, which is standard at telecommunication wavelengths.

A few remarks are in order on possible improvements for practical CVQKD implementations. First, it is important to emphasize that thanks to the aforementioned advances, the distance limitation is no longer determined by the efficiency of the post-processing algorithms, but rather by the excess noise present in the setup and especially by the capacity to properly estimate the relevant experimental parameters, as explained above. In terms of reducing the excess noise, recent protocols based on

the so-called "noiseless amplification" [52,67,68] might be promising. Efficient parameter estimation over large data blocks, which requires a very stable experimental setup, plays a role not only for the distance, but also for achieving composable security, as discussed in Section 3, and for increasing the secret key generation rate. Indeed, in the implementation of the GG02 protocol described above, a big fraction of the light pulses was used for this process [64]; this fraction can be reduced by improving the hardware stability and, hence, by enabling the estimation of experimental parameters over larger blocks. Furthermore, the secret key generation rate may be increased by increasing the initial repetition rate of the experiments. This necessitates shortening the pulse duration and the time-multiplexing data sampling period, increasing the homodyne detection bandwidth [69] and performing faster error correction on multiple devices, up to the capacity of the network link used for the transmission of the classical data.

5. Imperfections and Side Channels in Practical CVQKD

Bringing theoretical protocols to the realm of practical implementations unavoidably implies that some assumptions need to be made, such that real-life constraints can be satisfied. This may be innocuous in some cases; however, when it comes to cryptographic applications where rigorous security proofs are required, such assumptions may have dramatic consequences for the security obtained in practice. This is of course true for quantum key distribution implementations, as well, especially as this technology is reaching a certain maturity. Let us consider, for example, the CVQKD implementation of the GG02 protocol described above. While we saw that a phase reference, the local oscillator (LO), is necessary for the implementation, in fact, this signal does not appear in any way in the description of the protocol and in the security proof. The implicit assumption made then is that Eve does not tamper with the LO; under this assumption, the security proof holds. In reality, though, there is nothing preventing Eve from manipulating this strong classical signal in order to obtain information on the transmitted key. Indeed, this is possible, as we will see below. This is a simple example of a so-called side-channel attack, which illustrates that it is crucial to consider the practical security of CVQKD implementations.

In order to address this issue of great practical relevance, one solution is to consider exhaustively all of the possible discrepancies between the underlying theoretical model and the actual implementation, to take into account the assumptions due to experimental requirements or imperfections and to refine the model accordingly. This approach has been pursued extensively for discrete-variable QKD, where powerful side-channel attacks have been demonstrated, in particular against commercial systems [70–72]. In CVQKD, this process involves developing better models for the state preparation, the local oscillator manipulation and the detection stages of the implementation. We summarize below a few concrete examples of security issues that have been studied in recent years.

5.1. State Preparation

In practical CVQKD systems, the modulation applied to the signal according, for instance, to the GG02 protocol can only approach the Gaussian modulation required in theory. Indeed, a Gaussian distribution is not only continuous, but unbounded and, therefore, cannot be exactly achieved, since an infinite amount of randomness would be required. Using a bounded, discrete approximation, it is possible to show that the impact on security is not significant in practice [63].

Additionally, similarly to the aforementioned realistic scenario by which the characteristics of the homodyne (or heterodyne) detector are assumed to be trusted (and hence, not controlled by Eve), it is possible to make the same assumption for the phase noise that is always present in the state prepared by Alice. It is then possible to show that precisely characterizing and calibrating this noise leads to an increased secret key generation rate [63].

Finally, it is clear that obtaining information on the state prepared by Alice after modulation is valuable for the eavesdropper. To this end, the so-called Trojan horse attacks were studied and implemented in the discrete-variable QKD case [73]. These attacks exploit back reflections coming from optical components, such as modulators induced by bright pulses sent by the eavesdropper, and may open a substantial security breach. They are also effective against CVQKD systems, where Alice's modulators may be probed in this way [74]. Countermeasures against this type of attack include placing an optical isolator and a monitoring detector at the output of Alice's setup. The role of these components would then need to be explicitly included in the security proof of the implemented protocol.

5.2. Local Oscillator Manipulation

As was mentioned above, the presence of the intense phase reference signal, for which the no-cloning theorem does not apply, in the quantum channel is specific to standard CVQKD implementations and opens the way to potential security loopholes. Attacks based on the LO typically involve control of its intensity [75,76], and so, a monitoring detector at the entrance of Bob's site is useful in this case. The eavesdropper can also exploit a subtle link between the local oscillator calibration procedure and the clock generation procedure employed in practical setups, such as the one illustrated in Figure 1. In this case, suitable manipulation of the LO leads to an overestimation of the shot noise by Alice and Bob, who then underestimate the excess noise present in the system and establish a key under conditions where no key could normally be securely generated [77]. A suitable countermeasure for this attack consists of implementing a rigorous and robust real-time measurement of the shot noise [78]. Another possible countermeasure against this threat is to generate the LO locally in Bob's lab, and preliminary results have recently been obtained in this direction [79,80].

5.3. Detection

The proposed side-channel attacks targeting the coherent detectors employed in CVQKD systems exploit either the nonlinear behavior of these detectors that can lead to their saturation [81] or the dependence of the beam splitter included in both homodyne and heterodyne detectors on the wavelength of the incoming signal [82,83]. A wavelength filter is effective against the second attack, but a more general solution consists again in performing the real-time shot noise measurement analyzed in [78]. In fact, this countermeasure defeats all currently known attacks on the detection apparatus for CVQKD protocols with Gaussian modulation.

The security issues that we have discussed highlight the importance of refining security proofs of CVQKD protocols to consider practical imperfections as a means to bypass attacks based on improperly-modeled devices and procedures. Although this approach is of great practical relevance, it may be difficult in practice to identify all possible side channels present in experimental systems. A more

radical approach to overcome side-channel attacks is the so-called device-independent QKD [84,85], where the security is guaranteed by the violation of a Bell inequality: intuitively, if Alice and Bob maximally violate the Clauser-Horne-Shimony-Holt (CHSH) inequality [86], then they necessarily share a maximally-entangled state, and the eavesdropper cannot have any information about their measurement results. Unfortunately, an implementation of device-independent QKD requires a loophole-free violation, a feat not yet achieved in the lab. Interestingly, a much more practical variant, named measurement device-independent (MDI) QKD, is available and offers protection against all side-channel attacks targeting the detectors of the QKD implementation; [87] considered an MDI-QKD protocol using weak coherent pulses and decoy states, while [88] considered a MDI-QKD protocol in the entanglement-based representation with general finite-dimensional systems. These results were recently extended to continuous variables in [89,90], which provide an unconditional security proof in the asymptotic limit (see also [91,92] for a more restricted security analysis).

In MDI-QKD, Alice and Bob both prepare and send some states through quantum channels to a third party, Charlie, who performs an entangled measurement and announces his measurement result publicly. Conditioned on this classical information, Alice and Bob's data become correlated, and one might try to use them to extract a secure key. This scheme can be interpreted as a time-reversal of a QKD protocol, where Charlie would send bipartite entangled states to Alice and Bob. In particular, the security of the key does not require that Charlie is trusted: if Charlie sends erroneous data, the correlations between Alice and Bob's data will not be sufficient to allow for the extraction of a key, and the protocol will simply abort. This means that a side-channel attack can only be applied against Alice and Bob's preparation procedures, which are typically easier to model properly than the detection stage. In the continuous-variable version of MDI-QKD, Alice and Bob can, for instance, prepare coherent states with a Gaussian modulation and send them to Charlie, who mixes them on a balanced beam splitter, measures a different quadrature for both output modes and publicly announces his measurement results. Alice and Bob can then update their data using Charlie's information in order to obtain correlated continuous variables (see [89] for details).

The security of CV MDI-QKD can be analyzed by considering the entanglement-based version of the protocol. In that case, both Alice and Bob prepare a two-mode squeezed vacuum state, keep one half of their state and send the second half to Charlie. Once Charlie has measured his two modes and communicated his measurement result, Alice and Bob can apply suitable displacements to their respective modes. At this stage, they share a bipartite state $\rho_{A^N B^N}$ (possibly correlated by Charlie or Eve's state), which they measure with heterodyne detection. This is similar to the CVQKD protocol with entanglement in the middle of [93]. As in Equation (2), the optimality of Gaussian states [29] guarantees that it is sufficient to know the covariance matrix of the state $\rho_{A^N B^N}$ in order to obtain an upper bound on the Holevo information between Eve and the raw key, and in turn, a lower bound on $K_{\mathrm{coll}}^{\mathrm{asympt}}$. Composable security against collective attacks, *i.e.*, for bipartite states of the form $\rho_{AB}^{\otimes N}$, can be established by adapting the proof of [24], and composable security against arbitrary attacks can finally be obtained thanks, for instance, to de Finetti reductions [36,37].

In terms of practical implementations, MDI-QKD is very promising for discrete-variable protocols over long distances [94]; however, the obtained secret key generation rates remain currently relatively low. On the other hand, CV MDI-QKD implementations are limited in range, as Charlie needs to be

located close to Alice's (or Bob's) lab and the channel between Bob (or Alice) and Charlie needs to feature small losses and, so, cannot exceed a few kilometers. However, the achievable rates in this case can be very high, within an order of magnitude from the known secret key capacity bounds [45,95]. This configuration is therefore particularly interesting in a network setting with untrusted nodes for achieving high-speed secure communication over relatively short distances [89].

6. Conclusions and Perspectives

In the previous sections, we have provided an overview of the current achievements in the field of continuous-variable quantum key distribution, focusing in particular on the status of the security proofs for the various CVQKD protocols and the performance and limitations of practical fiber optic implementations using coherent states. These developments have undoubtedly established CVQKD as a major technology for performing secure quantum communications.

Some challenges for improving the performance of current systems, with respect in particular to the communication rate, the range of the implementations and the perspective of achieving composable security against arbitrary attacks in practice, have been discussed previously. Another major challenge for the widespread use of this technology for high-security applications involves the reduction of the size and cost of the corresponding implementations by means of photonic integration. Continuous-variable QKD is particularly well suited for integration using, for instance, silicon photonic chips, because of the standard components that it requires. Indeed, the first steps in this direction are currently being pursued [96].

Furthermore, an important practical issue concerns the ability of QKD systems to be integrated into classical network infrastructures by means of wavelength division multiplexing techniques; here, again, CVQKD is a good candidate to achieve this goal, as has been shown recently [97,98].

An impairment towards further development of CVQKD systems is linked to the local oscillator that needs to be sent over the quantum channel together with the signal in current standard implementations (see Figure 1). Its presence leads to security breaches, as discussed in Section 5, but also is at the source of several practical problems in long-distance implementations, where, for instance, it prevents reaching a very low signal-to-noise ratio [64]. This will be even more the case in future on-chip CVQKD experiments or systems adapted for free-space or satellite communications [99,100]. Recent preliminary theoretical and experimental studies of a scheme that does not require the transfer of the local oscillator are promising [79,80], and further advances in this direction are likely to lead to important simplifications of practical CVQKD implementations.

These research directions, together with the possibility of using encoding on continuous variables for quantum cryptographic protocols beyond key distribution, such as bit commitment [101–103], secret sharing [104] or position-based cryptography [105], will bring this technology a step closer to a wide range of applications within future quantum information networks.

Conflicts of Interest

The authors declare no conflict of interest.

References

1. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, 10–19 December 1984; Volume 175.

2. Shannon, C.E. A mathematical theory of communication. *Bell Syst. Tech. J.* **1948**, *27*, 379–423 and 623–656.

3. Portmann, C. Key recycling in authentication. *IEEE Trans. Inf. Theory* **2014**, *60*, 4383–4396.

4. Peev, M.; Pacher, C.; Alléaume, R.; Barreiro, C.; Bouda, J.; Boxleitner, W.; Debuisschert, T.; Diamanti, E.; Dianati, M.; Dynes, J.F.; *et al.* The SECOQC quantum key distribution in Vienna. *New J. Phys.* **2009**, *11*, 075001.

5. Sasaki, M.; Fujiwara, M.; Ishizuka, H.; Klaus, W.; Wakui, K.; Takeoka, M.; Tanaka, A.; Yoshino, K.; Nambu, Y.; Takahashi, S.; *et al.* Field test of quantum key distribution in the Tokyo QKD Network. *Opt. Express* **2011**, *19*, 10387–10409.

6. ID Quantique. Available online: http://www.idquantique.com (accessed on 31 August 2015).

7. Scarani, V.; Bechmann-Pasquinucci, H.; Cerf, N.J.; Dušek, M.; Lütkenhaus, N.; Peev, M. The security of practical quantum key distribution. *Rev. Modern Phys.* **2009**, *81*, 1301.

8. Takesue, H.; Nam, S.W.; Zhang, Q.; Hadfield, R.H.; Honjo, T.; Tamaki, K.; Yamamoto, Y. Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors. *Nat. Photonics* **2007**, *1*, 343–348.

9. Rosenberg, D.; Peterson, C.G.; Harrington, J.W.; Rice, P.R.; Dallmann, N.; Tyagi, K.T.; McCabe, K.P.; Nam, S.; Baek, B.; Hadfield, R.H.; *et al.* Practical long-distance quantum key distribution system using decoy levels. *New J. Phys.* **2009**, *11*, 045009.

10. Dixon, A.R.; Yuan, Z.L.; Dynes, J.F.; Sharpe, A.W.; Shields, A.J. Continuous operation of high bit rate quantum key distribution. *Appl. Phys. Lett.* **2010**, *96*, 161102.

11. Korzh, B.; Lim, C.C.W.; Houlmann, R.; Gisin, N.; Li, M.J.; Nolan, D.; Sanguinetti, B.; Thew, R.; Zbinden, H. Provably Secure and Practical Quantum Key Distribution over 307 km of Optical Fibre. *Nat. Photonics* **2015**, *9*, 163–168.

12. Weedbrook, C.; Pirandola, S.; García-Patrón, R.; Cerf, N.J.; Ralph, T.; Shapiro, J.; Lloyd, S. Gaussian quantum information. *Rev. Modern Phys.* **2012**, *84*, 621.

13. Pirandola, S.; Mancini, S.; Lloyd, S.; Braunstein, S.L. Continuous-variable quantum cryptography using two-way quantum communication. *Nat. Phys.* **2008**, *4*, 726–730.

14. Weedbrook, C.; Ottaviani, C.; Pirandola, S. Two-way quantum cryptography at different wavelengths. *Phys. Rev. A* **2014**, *89*, 012309.

15. Lorenz, S.; Korolkova, N.; Leuchs, G. Continuous-variable quantum key distribution using polarization encoding and post-selection. *Appl. Phys. B* **2004**, *79*, 273–277.

16. Heid, M.; Lütkenhaus, N. Efficiency of coherent-state quantum cryptography in the presence of loss: Influence of realistic error correction. *Phys. Rev. A* **2006**, *73*, 052316.

17. Leverrier, A.; Grangier, P. Unconditional Security Proof of Long-Distance Continuous-Variable Quantum Key Distribution with Discrete Modulation. *Phys. Rev. Lett.* **2009**, *102*, 180504.

18. Sych, D.; Leuchs, G. Coherent state quantum key distribution with multi letter phase-shift keying. *New J. Phys.* **2010**, *12*, 053019.

19. Leverrier, A.; Grangier, P. Continuous-variable quantum-key-distribution protocols with a non-Gaussian modulation. *Phys. Rev. A* **2011**, *83*, 042312.

20. Silberhorn, C.; Ralph, T.C.; Lütkenhaus, N.; Leuchs, G. Continuous Variable Quantum Cryptography: Beating the 3 dB Loss Limit. *Phys. Rev. Lett.* **2002**, *89*, 167901.

21. Grosshans, F.; Cerf, N.J.; Wenger, J.; Tualle-Brouri, R.; Grangier, P. Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables. *Quantum Inf. Comput.* **2003**, *3*, 535–552.

22. Grosshans, F.; Grangier, P. Continuous Variable Quantum Cryptography Using Coherent States. *Phys. Rev. Lett.* **2002**, *88*, 057902.

23. Weedbrook, C.; Lance, A.M.; Bowen, W.P.; Symul, T.; Ralph, T.C.; Lam, P.K. Quantum cryptography without switching. *Phys. Rev. Lett.* **2004**, *93*, 170504.

24. Leverrier, A. Composable Security Proof for Continuous-Variable Quantum Key Distribution with Coherent States. *Phys. Rev. Lett.* **2015**, *114*, 070501.

25. Grosshans, F.; Assche, G.V.; Wenger, J.; Brouri, R.; Cerf, N.J.; Grangier, P. Quantum key distribution using Gaussian-modulated coherent states. *Nature* **2003**, *421*, 238.

26. Jouguet, P.; Elkouss, D.; Kunz-Jacques, S. High Bit Rate Continuous-Variable Quantum Key Distribution. *Phys. Rev. A* **2014**, *90*, 042329.

27. Devetak, I.; Winter, A. Distillation of secret key and entanglement from quantum states. *Proc. R. Soc. A* **2005**, *461*, 207–235.

28. Kraus, B.; Gisin, N.; Renner, R. Lower and upper bounds on the secret-key rate for quantum key distribution protocols using one-way classical communication. *Phys. Rev. Lett.* **2005**, *95*, 080501.

29. Wolf, M.M.; Giedke, G.; Cirac, J.I. Extremality of Gaussian Quantum States. *Phys. Rev. Lett.* **2006**, *96*, 080502.

30. García-Patrón, R.; Cerf, N.J. Unconditional Optimality of Gaussian Attacks against Continuous-Variable Quantum Key Distribution. *Phys. Rev. Lett.* **2006**, *97*, 190503.

31. Navascués, M.; Grosshans, F.; Acín, A. Optimality of Gaussian Attacks in Continuous-Variable Quantum Cryptography. *Phys. Rev. Lett.* **2006**, *97*, 190502.

32. Renner, R. Security of quantum key distribution. *Int. J. Quantum Inf.* **2008**, *6*, 1–127.

33. Canetti, R. Universally Composable Security: A New Paradigm for Cryptographic Protocols. In Proceedings of the 42nd IEEE Symposium on Foundations of Computer Science, Las Vegas, NV, USA, 14–17 October 2001; pp. 136–145.

34. Furrer, F.; Åberg, J.; Renner, R. Min-and max-entropy in infinite dimensions. *Commun. Math. Phys.* **2011**, *306*, 165–186.

35. Berta, M.; Furrer, F.; Scholz, V.B. The smooth entropy formalism on von Neumann algebras. **2011**, arXiv:1107.5460 .

36. Renner, R.; Cirac, J.I. De Finetti Representation Theorem for Infinite-Dimensional Quantum Systems and Applications to Quantum Cryptography. *Phys. Rev. Lett.* **2009**, *102*, 110504.

37. Leverrier, A.; García-Patrón, R.; Renner, R.; Cerf, N.J. Security of Continuous-Variable Quantum Key Distribution Against General Attacks. *Phys. Rev. Lett.* **2013**, *110*, 030502.

38. Furrer, F.; Franz, T.; Berta, M.; Leverrier, A.; Scholz, V.B.; Tomamichel, M.; Werner, R.F. Continuous variable quantum key distribution: Finite-key analysis of composable security against coherent attacks. *Phys. Rev. Lett.* **2012**, *109*, 100502.

39. Furrer, F. Reverse-reconciliation continuous-variable quantum key distribution based on the uncertainty principle. *Phys. Rev. A* **2014**, *90*, 042325.

40. Furrer, F.; Berta, M.; Tomamichel, M.; Scholz, V.B.; Christandl, M. Position-momentum uncertainty relations in the presence of quantum memory. *J. Math. Phys.* **2014**, *55*, 122205.

41. Cerf, N.J.; Levy, M.; Assche, G.V. Quantum distribution of Gaussian keys using squeezed states. *Phys. Rev. A* **2001**, *63*, 052311.

42. Pirandola, S.; Braunstein, S.L.; Lloyd, S. Characterization of collective Gaussian attacks and security of coherent-state quantum cryptography. *Phys. Rev. Lett.* **2008**, *101*, 200504.

43. Usenko, V.C.; Grosshans, F. Unidimensional continuous-variable quantum key distribution. **2015**, arXiv:1504.07093.

44. García-Patrón, R.; Cerf, N.J. Continuous-variable quantum key distribution protocols over noisy channels. *Phys. Rev. Lett.* **2009**, *102*, 130501.

45. Pirandola, S.; García-Patrón, R.; Braunstein, S.L.; Lloyd, S. Direct and reverse secret-key capacities of a quantum channel. *Phys. Rev. Lett.* **2009**, *102*, 050503.

46. Filip, R. Continuous-variable quantum key distribution with noisy coherent states. *Phys. Rev. A* **2008**, *77*, 022310.

47. Usenko, V.C.; Filip, R. Feasibility of continuous-variable quantum key distribution with noisy coherent states. *Phys. Rev. A* **2010**, *81*, 022318.

48. Weedbrook, C.; Pirandola, S.; Lloyd, S.; Ralph, T.C. Quantum cryptography approaching the classical limit. *Phys. Rev. Lett.* **2010**, *105*, 110501.

49. Weedbrook, C.; Pirandola, S.; Ralph, T.C. Continuous-variable quantum key distribution using thermal states. *Phys. Rev. A* **2012**, *86*, 022318.

50. Madsen, L.S.; Usenko, V.C.; Lassen, M.; Filip, R.; Andersen, U.L. Continuous variable quantum key distribution with modulated entangled states. *Nat. Commun.* **2012**, *3*, 1083.

51. Fiurášek, J.; Cerf, N.J. Gaussian post-selection and virtual noiseless amplification in continuous-variable quantum key distribution. *Phys. Rev. A* **2012**, *86*, 060302.

52. Walk, N.; Ralph, T.C.; Symul, T.; Lam, P.K. Security of continuous-variable quantum cryptography with Gaussian post-selection. *Phys. Rev. A* **2013**, *87*, 020303(R).

53. Silberhorn, C.; Korolkova, N.; Leuchs, G. Quantum Key Distribution with Bright Entangled Beams. *Phys. Rev. Lett.* **2002**, *88*, 167902.

54. Fossier, S.; Diamanti, E.; Debuisschert, T.; Villing, A.; Tualle-Brouri, R.; Grangier, P. Field test of a continuous-variable quantum key distribution prototype. *New J. Phys.* **2009**, *11*, 045023.

55. Jouguet, P.; Kunz-Jacques, S.; Debuisschert, T.; Fossier, S.; Diamanti, E.; Alléaume, R.; Tualle-Brouri, R.; Grangier, P.; Leverrier, A.; Pache, P.; *et al.* Field test of classical symmetric encryption with continuous variables quantum key distribution. *Opt. Express* **2012**, *20*, 14030–14041.

56. Qi, B.; Huang, L.; Qian, L.; Lo, H.K. Experimental study on the Gaussian-modulated coherent-state quantum key distribution over standard telecommunication fibers. *Phys. Rev. A* **2007**, *76*, 052323.

57. Lodewyck, J.; Bloch, M.; García-Patrón, R.; Fossier, S.; Karpov, E.; Diamanti, E.; Cerf, N.J.; Debuisschert, T.; Tualle-Brouri, R.; McLaughlin, S.W.; *et al.* Quantum key distribution over 25 km with an all-fiber continuous-variable system. *Phys. Rev. A* **2007**, *76*, 042305.

58. Xuan, Q.D.; Zhang, Z.; Voss, P.L. A 24 km fiber-based discretely signaled continuous variable quantum key distribution system. *Opt. Express* **2009**, *17*, 24244.

59. Shen, Y.; Zou, H.; Tian, L.; Chen, P.; Yuan, J. Experimental study on discretely modulated continuous-variable quantum key distribution. *Phys. Rev. A* **2010**, *82*, 022317.

60. Leverrier, A.; Alléaume, R.; Boutros, J.; Zémor, G.; Grangier, P. Multidimensional reconciliation for a continuous-variable quantum key distribution. *Phys. Rev. A* **2008**, *77*, 042325.

61. Jouguet, P.; Kunz-Jacques, S.; Leverrier, A. Long-distance continuous-variable quantum key distribution with a Gaussian modulation. *Phys. Rev. A* **2011**, *84*, 062317.

62. Gehring, T.; Händchen, V.; Duhme, J.; Furrer, F.; Franz, T.; Pacher, C.; Werner, R.F.; Schnabel, R. Implementation of Quantum Key Distribution with Composable Security against Coherent Attacks Using Einstein-Podolsky-Rosen Entanglement. **2014**, arXiv:1406.6174.

63. Jouguet, P.; Kunz-Jacques, S.; Diamanti, E.; Leverrier, A. Analysis of Imperfections in Practical Continuous-Variable Quantum Key Distribution. *Phys. Rev. A* **2012**, *86*, 032309.

64. Jouguet, P.; Kunz-Jacques, S.; Leverrier, A.; Grangier, P.; Diamanti, E. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nat. Photonics* **2013**, *7*, 378–381.

65. Lance, A.M.; Symul, T.; Sharma, V.; Weedbrook, C.; Ralph, T.C.; Lam, P.K. No-Switching Quantum Key Distribution Using Broadband Modulated Coherent Light. *Phys. Rev. Lett.* **2005**, *95*, 180503.

66. Symul, T.; Alton, D.J.; Assad, S.M.; Lance, A.M.; Weedbrook, C.; Ralph, T.C.; Lam, P.K. Experimental demonstration of post-selection-based continuous-variable quantum key distribution in the presence of Gaussian noise. *Phys. Rev. A* **2007**, *76*, 030303.

67. Blandino, R.; Leverrier, A.; Barbieri, M.; Etesse, J.; Grangier, P.; Tualle-Brouri, R. Improving the maximum transmission distance of continuous-variable quantum key distribution using a noiseless amplifier. *Phys. Rev. A* **2012**, *86*, 012327.

68. Fiurasek, J.; Cerf, N.J. Gaussian post-selection and virtual noiseless amplification in continuous-variable quantum key distribution. *Phys. Rev. A* **2012**, *86*, 060302(R).

69. Huang, D.; Fang, J.; Wang, C.; Huang, P.; Zeng, G. A 300-MHz Bandwidth Balanced Homodyne Detector for Continuous Variable Quantum Key Distribution. *Chin. Phys. Lett.* **2013**, *30*, 114209.

70. Zhao, Y.; Fung, C.H.F.; Qi, B.; Chen, C.; Lo, H.K. Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems. *Phys. Rev. A* **2008**, *78*, 042333.

71. Xu, F.; Qi, B.; Lo, H.K. Experimental demonstration of phase-remapping attack in a practical quantum key distribution system. *New J. Phys.* **2010**, *12*, 113026.

72. Lydersen, L.; Wiechers, C.; Wittmann, C.; Elser, D.; Skaar, J.; Makarov, V. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nat. Photonics* **2010**, *4*, 686–689.

73. Gisin, N.; Fasel, S.; Kraus, B.; Zbinden, H.; Ribordy, G. Trojan-horse attacks on quantum-key-distribution systems. *Phys. Rev. A* **2006**, *73*, 022320.

74. Khan, I.; Jain, N.; Stiller, B.; Jouguet, P.; Kunz-Jacques, S.; Diamanti, E.; Marquardt, C.; Leuchs, G. Trojan horse attacks on practical continuous-variable quantum key distribution systems. In Proceedings of Conference on Quantum Cryptography (QCRYPT), Paris, France, 1–5 September 2014.

75. Ferenczi, A.; Grangier, P.; Grosshans, F. Calibration Attack and Defense in Continuous Variable Quantum Key Distribution. In Proceedings of the European Conference on Lasers and Electro-Optics/International Quantum Electronics Conference (CLEO/Europe-IQEC), Munich, Germany, 17–22 June 2007.

76. Ma, X.C.; Sun, S.H.; Jiang, M.S.; Liang, L.M. Local oscillator fluctuation opens a loophole for Eve in practical continuous-variable quantum-key-distribution systems. *Phys. Rev. A* **2013**, *88*, 022339.

77. Jouguet, P.; Kunz-Jacques, S.; Diamanti, E. Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution. *Phys. Rev. A* **2013**, *87*, 062313.

78. Jouguet, P.; Kunz-Jacques, S. Robust Shot Noise Measurement for Continuous Variable Quantum Key Distribution. *Phys. Rev. A* **2015**, *91*, 022307.

79. Qi, B.; Lougovski, P.; Pooser, R.; Grice, W.; Bobrek, M. Generating the local oscillator "locally" in continuous-variable quantum key distribution based on coherent detection. **2015**, arXiv:1503.00662.

80. Soh, D.B.S.; Brif, C.; Coles, P.J.; Lütkenhaus, N.; Camacho, R.M.; Urayama, J.; Sarovar, M. Self-referenced continuous-variable quantum key distribution. **2015**, arXiv:1503.04763.

81. Qin, H.; Kumar, R.; Alléaume, R. Saturation attack on continuous-variable quantum key distribution system. *Proc. SPIE* **2013**, *8899,* doi:10.1117/12.2028543.

82. Ma, X.C.; Sun, S.H.; Jiang, M.S.; Liang, L.M. Wavelength attack on practical continuous-variable quantum-key-distribution system with a heterodyne protocol. *Phys. Rev. A* **2013**, *87*, 052309.

83. Huang, J.Z.; Kunz-Jacques, S.; Jouguet, P.; Weedbrook, C.; Yin, Z.Q.; Wang, S.; Chen, W.; Guo, G.C.; Han, Z.F. Quantum Hacking on Quantum Key Distribution Using Homodyne Detection. *Phys. Rev. A* **2014**, *89*, 032304.

84. Acín, A.; Brunner, N.; Gisin, N.; Massar, S.; Pironio, S.; Scarani, V. Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.* **2007**, *98*, 230501.

85. Vazirani, U.; Vidick, T. Fully device-independent quantum key distribution. *Phys. Rev. Lett.* **2014**, *113*, 140501.

86. Clauser, J.F.; Horne, M.A.; Shimony, A.; Holt, R.A. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.* **1969**, *23*, 880.

87. Lo, H.K.; Curty, M.; Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **2012**, *108*, 130503.

88. Braunstein, S.L.; Pirandola, S. Side-channel-free quantum key distribution. *Phys. Rev. Lett.* **2012**, *108*, 130502.

89. Pirandola, S.; Ottaviani, C.; Spedalieri, G.; Weedbrook, C.; Braunstein, S.L.; Lloyd, S.; Gehring, T.; Jacobsen, C.S.; Andersen, U.L. High-rate measurement-device-independent quantum cryptography. *Nat. Photonics* **2015**, *9*, 397–402.

90. Ottaviani, C.; Spedalieri, G.; Braunstein, S.L.; Pirandola, S. Continuous-variable quantum cryptography with an untrusted relay: Detailed security analysis of the symmetric configuration. *Phys. Rev. A* **2015**, *91*, 022320.

91. Ma, X.C.; Sun, S.H.; Jiang, M.S.; Gui, M.; Liang, L.M. Gaussian-modulated coherent-state measurement-device-independent quantum key distribution. *Phys. Rev. A* **2014**, *89*, 042335.

92. Li, Z.; Zhang, Y.C.; Xu, F.; Peng, X.; Guo, H. Continuous-variable measurement-device-independent quantum key distribution. *Phys. Rev. A* **2014**, *89*, 052301.

93. Weedbrook, C. Continuous-variable quantum key distribution with entanglement in the middle. *Phys. Rev. A* **2013**, *87*, 022308.

94. Tang, Y.L.; Yin, H.L.; Chen, S.J.; Liu, Y.; Zhang, W.J.; Jiang, X.; Zhang, L.; Wang, J.; You, L.X.; Guan, J.Y.; *et al.* Measurement-device-independent quantum key distribution over 200 km. *Phys. Rev. Lett.* **2014**, *113*, 190501.

95. Takeoka, M.; Guha, S.; Wilde, M.M. Fundamental rate-loss tradeoff for optical quantum key distribution. *Nat. Commun.* **2014**, *5*, 5235.

96. Ziebell, M.; Persechino, M.; Harris, N.; Galland, C.; Marris-Morini, D.; Vivien, L.; Diamanti, E.; Grangier, P. Towards On-Chip Continuous-Variable Quantum Key Distribution. In Proceedings of the Conference on Lasers and Electo-Optics/European Quantum Electronics Conference (CLEO/Europe-EQEC), Munich, Germany, 21–25 June 2015.

97. Qi, B.; Zhu, W.; Qian, L.; Lo, H.K. Feasibility of quantum key distribution through dense wavelength division multiplexing network. *New J. Phys.* **2010**, *12*, 103042.

98. Kumar, R.; Qin, H.; Alléaume, R. Coexistence of continuous variable QKD with intense DWDM classical channels. *New J. Phys.* **2015**, *17*, 043027.

99. Heim, B.; Peuntinger, C.; Killoran, N.; Khan, I.; Wittmann, C.; Marquardt, C.; Leuchs, G. Atmospheric continuous-variable quantum communication. *New J. Phys.* **2014**, *16*, 113018.

100. Vallone, G.; Bacco, D.; Dequal, D.; Gaiarin, S.; Luceri, V.; Bianco, G.; Villoresi, P. Experimental Satellite Quantum Communications. *Phys. Rev. Lett.* **2015**, *115*, 040502.

101. Magnin, L.; Magniez, F.; Leverrier, A.; Cerf, N.J. Strong no-go theorem for Gaussian quantum bit commitment. *Phys. Rev. A* **2010**, *81*, 010302(R).

102. Mandilara, A.; Cerf, N.J. Quantum bit commitment under Gaussian constraints. *Phys. Rev. A* **2012**, *85*, 062310.

103. Furrer, F.; Schaffner, C.; Wehner, S. Continuous-Variable Protocols in the Noisy Quantum Storage Model. In Proceedings of Conference on Quantum Cryptography (QCRYPT), Tokyo, Japan, 28 September–2 October 2015.

104. Lau, H.K.; Weedbrook, C. Quantum secret sharing with continuous-variable cluster states. *Phys. Rev. A* **2013**, *88*, 042313.

105. Qi, B.; Siopsis, G. Loss-tolerant position-based quantum cryptography. *Phys. Rev. A* **2015**, *91*, 042337.