Improving Parameter Estimation of Entropic Uncertainty Relation in Continuous-Variable Quantum Key Distribution

Ziyang Chen [1] [ID], Yichen Zhang [2], Xiangyu Wang [2] [ID], Song Yu [2] and Hong Guo [1,*]

[1]   State Key Laboratory of Advanced Optical Communication, Systems and Networks,
     Department of Electronics, and Center for Quantum Information Technology, Peking University,
     Beijing 100871, China
[2]   State Key Laboratory of Information Photonics and Optical Communications,
     Beijing University of Posts and Telecommunications, Beijing 100876, China
*   Correspondence: hongguo@pku.edu.cn

Abstract: The entropic uncertainty relation (EUR) is of significant importance in the security proof of continuous-variable quantum key distribution under coherent attacks. The parameter estimation in the EUR method contains the estimation of the covariance matrix (CM), as well as the max-entropy. The discussions in previous works have not involved the effect of finite-size on estimating the CM, which will further affect the estimation of leakage information. In this work, we address this issue by adapting the parameter estimation technique to the EUR analysis method under composable security frameworks. We also use the double-data modulation method to improve the parameter estimation step, where all the states can be exploited for both parameter estimation and key generation; thus, the statistical fluctuation of estimating the max-entropy disappears. The result shows that the adapted method can effectively estimate parameters in EUR analysis. Moreover, the double-data modulation method can, to a large extent, save the key consumption, which further improves the performance in practical implementations of the EUR.

Keywords: entropic uncertainty relation; continuous-variable quantum key distribution; finite-size effect; composable security; double-data modulation

1. Introduction

The quantum key distribution (QKD) [1–5] is one of the most mature quantum cryptography technologies, which can provide information-theoretical provable security together with the one-time pad method. The idea of QKD is to employ the basic principles of quantum physics to ensure the security of random keys and to use classical post-processing methods to find potential eavesdropping behaviors. Based on the dimension of the Hilbert space of the encoding, QKD can be roughly divided into two categories. One kind of protocol is called the discrete-variable (DV) protocol, in which the dimension of the Hilbert space is finite. DV-QKD protocols have the superiority of long transmission distance, but depending on high-performance dedicated devices such as single-photon detectors. As an alternative, continuous-variable (CV) protocols, which use the infinite dimension of Hilbert space as the key space, give us opportunities to achieve the QKD process via off-the-shelf commercial components, e.g., homodyne detector and heterodyne detector.

The first idea of the CV-QKD protocol was exploiting squeezed states to carry the key information [6–9]. Then, in order to weaken the dependence on the squeezed-state sources, the coherent-state-based CV-QKD protocols were proposed [10–12]. During these twenty years, research on protocol design and corresponding experimental verification was developing rapidly. Different

novel CV-QKD protocols have been proposed, such as the two-way protocol [13–18], the discrete modulation protocol [19–21], the measurement-device-independent (MDI) protocol [22–28], etc., each of which has its own advantages in different scenarios. Besides the protocol design, the experiments also have made a tremendous step forward with the progress of today's technology [29–31].

The core of QKD is the security, and there have been many security analysis methods proposed to investigate the security of different CV-QKD protocols [4]. For the convenience of the security analysis, the eavesdropper's ability is usually restricted to three different levels, namely individual attacks, collective attacks, and coherent attacks. Individual attacks and collective attacks are, to some extent, to restrict the eavesdropper's (Eve's) attack ability, so that the exchanged state between Alice (sender) and Bob (receiver) can be treated as an identical and independently distributed (i.i.d.) state, i.e., $\rho_{A^N B^N} = \sigma_{AB}^{\otimes N}$ (where N is the number of exchanged signals), which can simplify the security analysis. However, a protocol is unconditionally secure only when it is secure under coherent attacks, due to the fact that coherent attacks do not limit the ability of eavesdroppers, thereby the most general attacks. In the case of coherent attacks, the exchanged states between Alice and Bob do not have the i.i.d. structure anymore; thus, the security proof is complicated.

Diverse security analysis techniques have been developed to analyze the security of different protocols under coherent attacks, typically the de Finetti theorem [32,33], the post-selection technique [34,35], and the entropic uncertainty relation (EUR) [36–38]. Those analysis methods can also be applied to analyze the quantum random number generation protocols [39,40]. Different analysis methods have their advantages and disadvantages, so they are suitable for the analysis of different protocols (see [4] for detailed discussions). The advantages of the EUR lies in its intuitive physical meaning (corresponding to the guessing game [41]) and the simple estimation method. Most of the work has been done in the EUR in [36], except for the finite-size effect in estimating the covariance matrix (CM). However, in practical experiments, the estimation of the CM is always achieved by limited data; thus, the finite-size effect not only affects the estimation of min-entropy, but also the estimation of leakage information.

In this work, we focus on the parameter estimation of the EUR in CV-QKD, especially on the finite-size estimation of the CM, and the modified estimation on the max-entropy. The discussion involves only the squeezed state/homodyne detection-type protocols and has no assumption on Eve's ability, namely under coherent-attack cases. Due to the influence of the finite block length of the key, the estimation of the CM is inaccurate in the case of a short block length, compared with the ideal CM estimation cases (as shown in [36,37]). We exploit the parameter estimation technique developed in [42] to consider the estimation of the CM under practical block sizes. Furthermore, inspired by the double-modulation method developed in [42], we propose a double-data modulation method to estimate the parameters in the security analysis effectively, and only one modulation is needed rather than two, which simplifies the experimental structure of the double-modulation protocol. Since the exchanged state can be used for both parameter estimation and key generation, the estimation of the max-entropy is modified, and the statistical fluctuation of estimating the max-entropy disappears. The simulation result shows that the modified estimation method can, to a large extent, save the key consumption.

This paper is organized as follows. In Section 2, we review the composable security frameworks in QKD and give the description of the discussed protocol. In Section 3, we discuss in detail the channel parameter estimation process with finite-size. In Section 4, the modified parameter estimation method is proposed with double-data modulation. The numerical simulation and discussion are give in Section 5, and the conclusions are drawn in Section 6.

2. Composable Security and Description of the Protocol

In this work, we investigate the CV-QKD protocol under the universal composable framework (UCF), which can be seen in [43,44] for the details, and the discussion is under the coherent-attack cases. The UCF is of great importance to compose sequential rounds of a protocol, and even if some of

the rounds are imperfect and deviate from the ideal model, the UCF can well describe their defects. A general QKD protocol can always be divided into different parts; thus, one of the benefits of UCFs is that even if part of the protocol is imperfect, this imperfection can still be applied to subsequent analysis of the rest part of the protocol to obtain the final non-ideal key. Another advantage of UCFs is that the final imperfect key generated from a QKD system can be well quantified as ε-secure and then can be applied to other classical communication tasks, such as the one-time pad scenario.

To illustrate the composable security of QKD, we first use s_A to denote Alice's key and use s_B to denote Bob's key. In the ideal case, the keys should be correct, secret, and robust. Correctness means, for each round of the protocol, the keys of Alice and Bob are always the same, namely $s_A = s_B = S$. Secrecy means the key is independent of the third part and only known to Alice and Bob themselves. Robustness requires that, in every round of the protocol, Alice and Bob can always generate a non-empty key, namely $S \neq \perp$. If a QKD protocol can satisfy correctness, secrecy, and robustness, the protocol then can be called perfectly secure. We denote by $\{|s\rangle\}_{s \in S}$ the orthogonal bases of the key, by ρ_E Eve's auxiliary quantum systems, and by $p_\perp$ the probability of generating an empty key set. The perfectly secure classical-quantum (cq) state between the key S and the environment E can be shown as follows,

$$\rho_{sE}^{perfect} = (1 - p_\perp) \sum_{s \in S} \frac{1}{|S|} |s\rangle \langle s| \otimes \rho_E^s + p_\perp |\perp\rangle \langle \perp| \otimes \rho_E^\perp. \tag{1}$$

Nevertheless, a protocol is always imperfect with practical issues, resulting in the security deviating from the ideal model. Therefore, the ε-security can be used to describe the practical security with imperfect features. We denote by $\varepsilon_c, \varepsilon_r, \varepsilon_s$ the smoothness parameters of practical correctness, robustness, and secrecy, respectively. ε_c-correctness requires that the key in Alice and Bob's sides be different only with very small probability ε_c, namely $\Pr(s_A \neq s_B) \leq \varepsilon_c$. ε_r-robustness requires that the set of the keys is empty only with a small probability, given by $\Pr(S = \perp) \leq \varepsilon_r$. ε_s-secrecy can be treated as the distance between the practical security and the perfect security, in terms of the trace distance, given by $\frac{1}{2} \left\| \rho_{sE} - \rho_{sE}^{perfect} \right\|_1 \leq \varepsilon_s$. In summary, if a QKD protocol can contain ε_c-correctness, ε_r-robustness, and ε_s-secrecy, then the protocol can be called ε-secure, with $\varepsilon = \varepsilon_c + \varepsilon_r + \varepsilon_s$.

Let us start with the execution of the prepare-and-measure (PM) version of the squeezed-states protocol. The protocol can be divided into sequential parts, as shown in Figure 1, which can be described by the following steps:

1. **State preparation**: Alice holds the squeezed states with squeezed variance V_S before the protocol begins, where $V_S \in (0, 1]$. In every run of the protocol, Alice uses Gaussian random numbers x_M to encode the displacement of quadratures by using modulators (generally containing amplitude and phase modulators), and the total modulation variance is denoted by V_M.

2. **State transmission**: Alice sends the modulated state in the quantum channel, which is treated as a totally untrusted channel and controlled by Eve.

3. **State measurement**: Bob receives the quantum state and randomly measures x or p quadrature by an ideal homodyne detector. Resulting from the fact that the practical measurement phase is always discrete, the ideal measurement outcomes should be discretized by the analogue-to-digital converter (ADC). The final discretized results are denoted by x_B.

4. **Parameter estimation**: Alice and Bob repeat the above steps many times until they have enough raw data (e.g., N). Then, Alice or Bob reveals some of the raw data (with length m) through the classical channel to estimate the key parameters of the channel, especially the data distance d_0 between Alice's and Bob's data, the transmittance τ, and the excess noise ε. See Section 3 for a detailed explanation of the parameter estimation step.

5. **Error correction**: According to the estimation parameters τ and ε, the communication parts estimate the leakage information ℓ_{EC} during the error correction phase and choose an appropriate

classical error reconciliation algorithm, e.g., low-density-parity-check (LDPC) code, to correct Alice's error (in reverse reconciliation cases) or Bob's error (in direct reconciliation cases).

6.　**Privacy amplification**: Alice and Bob randomly choose a universal$_2$ hash function [45] and apply it to their respective keys to get the final private keys s_A and s_B with length ℓ, which are only known to themselves.
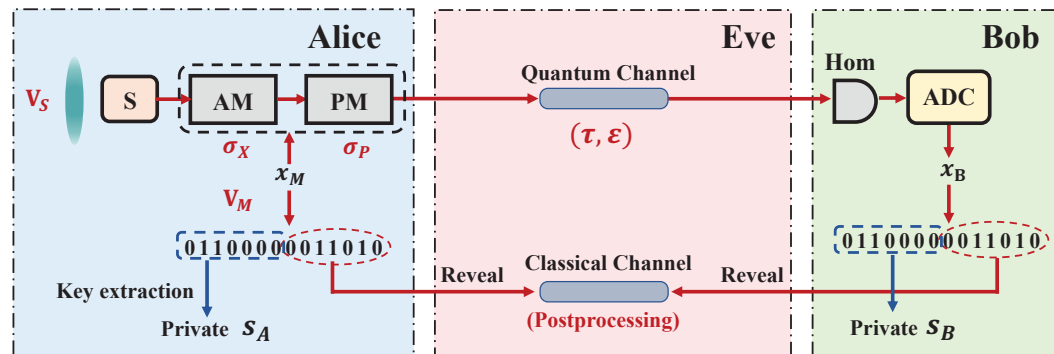

Figure 1. Prepare-and-measure (PM) scheme of continuous-variable (CV)-quantum key distribution (QKD) using squeezed states. Source: squeezed-state source with squeezed variance V_S; Mod: modulators containing amplitude and phase quadrature modulators with total modulation variance V_M; Hom: homodyne detection; x_M: Gaussian modulation data on Alice's side; x_B: measurement results on Bob's side; Quantum channel: channel for the transmission of quantum states, with the transmittance τ and the excess noise ε; Classical channel: channel for the transmission of classical data during the post-processing procedure.

According to the UCF, one can write the upper bound of the final key length ℓ_{low}, even if the above steps are not ideal, given by [43]:

$$\ell_{low} = H_{\min}^{\varepsilon}\left(x_B|E\right) - \ell_{EC} - \log_2 \frac{1}{\varepsilon_1^2 \varepsilon_c} + 2, \tag{2}$$

where $H_{\min}^{\varepsilon}\left(x_B|E\right)$ is the smooth min-entropy of x_B conditioned on the information Eve may hold, with smoothing parameter ε, and ε_1 is the smoothness of the physical part of the protocol.

3. Channel Parameter Estimation with Finite-Size

There are roughly two parameters that need to be bounded in the protocol. One is the smooth min-entropy $H_{\min}^{\varepsilon}\left(x_B|E\right)$, and the other is the leakage information ℓ_{EC}. We separately discuss the estimation of the two parameters in two parts.

3.1. Estimation of Smooth Min-Entropy

There are different ways to estimate the min-entropy under coherent attacks. For instance, the de Finetti theorem [32,33], which can reduce the analysis from the coherent attack case to the collective attack case, has been successfully used to prove the security of CV-QKD protocols with the source of coherent states [27,46]. The EUR has also been exploited to prove the security of squeezed-state-type protocols [28,36,37]. In this work, we focus on using the uncertainty relation to bound the min-entropy of the key.

In practical experiments, x_M and x_B are always discretized. We denote α as the maximum discretization range of the sampling interval and denote δ as the discrete precision of the measurement, which satisfy $2\alpha/\delta = 2^L \in \mathbb{N}$, where L is the number of discrete bits. Therefore, the measurement result will fall into different intervals, namely,

$$(-\infty, -\alpha], (-\infty, -\alpha+\delta], \ldots (-\alpha+(k-1)\delta, -\alpha+k\delta], \ldots (\alpha-\delta, \alpha], (\alpha, +\infty), \tag{3}$$

where $k = \{1, 2, \ldots, 2\alpha/\delta\}$. One can bound the smooth min-entropy of the discretized data x_B conditioned on Eve's information $H_{\min}^\varepsilon (x_B|E)$ according to the CV version of EUR, given by:

$$H_{\min}^\varepsilon (x_B|E) \geq -n \log c\,(\delta) - H_{\max}^{\varepsilon'} (x_M|x_B),\tag{4}$$

where c quantifies the maximum overlap of the two measurements, namely $c = \max\limits_{x,z} |\langle \mathbb{X}^x \mid \mathbb{Z}^z \rangle|^2$ and $\mathbb{X}$ and $\mathbb{Z}$ are mutually unbiased bases; hence, $c\,(\delta)$ is the overlap between discrete quadrature measurements related to the interval length δ, which reads:

$$c\,(\delta) = \frac{1}{2\pi} \delta^2 S_0^{(1)} \left(1, \frac{\delta^2}{4}\right)^2,\tag{5}$$

where $S_0^{(1)}(.)$ is the zeroth radial prolate spheroidal wave function of the first kind [47] and $S_0^{(1)}\left(1, \frac{\delta^2}{4}\right)^2$ is approximately one if δ is small. The term $H_{\max}^{\varepsilon'} (x_M|x_B)$ in Equation (4) denotes the max-entropy between Alice's and Bob's data, with smoothing parameter $\varepsilon' = \varepsilon_s/4p_{pass} - 2\sqrt{2\left[1 - (1 - p_\alpha)^n\right]}\Big/\sqrt{p_{pass}}$, where p_α is the probability that the measurement is outside of the detection range.

According to Equation (4), in order to give a lower bound of the min-entropy, one should estimate the upper bound of the max-entropy using some of the raw keys during the parameter estimation phase. First, the average distance, which quantifies the correlation between Alice's and Bob's data, should be estimated, given by:

$$d\left(x_M^{PE}, x_B^{PE}\right) = \frac{1}{m} \sum_{i=1}^{m} |M_i - B_i|,\tag{6}$$

where we use M_i to denote the ith modulating value and B_i denotes the ith measurement result, for $i = 1, 2, \ldots, m$, respectively. If the data distance $d\left(x_M^{PE}, x_B^{PE}\right)$ is smaller than a certain threshold d_0, the parameter estimation step passes. Then, one can bound the max-entropy according to Serfling's large deviation bound [48], given by:

$$H_{\max}^\varepsilon (x_M|x_B) \leq n\log_2 \gamma\,(d_0 + \mu),\tag{7}$$

where γ is a large deviation function, which reads:

$$\gamma(t) = \left(t + \sqrt{t^2 + 1}\right) \left[\frac{t}{\sqrt{t^2 + 1} - 1}\right]^t,\tag{8}$$

and μ quantifies the impact of statistical fluctuations resulting from estimating "data parameter" $H_{\max}^\varepsilon (x_M|x_B)$ by "PEparameter" $H_{\max}^\varepsilon (x_M^{PE}|x_B^{PE})$, which reads:

$$\mu = \frac{2\alpha}{\delta} \sqrt{\frac{N\,(m+1)}{nm^2} \ln \frac{1}{\varepsilon'}},\tag{9}$$

where N denotes the total number of exchanged signals and satisfies $N = n + m$.

3.2. Ideal Estimation of Leakage Information with Infinite-Size

To estimate the leakage information in the error correction phase, we model Eve's behavior by the entangling cloner attack model, which is the most common example of a Gaussian attack [49]. We point out that the whole analysis of this paper is under the most general coherent attacks and has no restriction on Eve's ability. The model of the entangling cloner attack is only for intuitive understanding, and it is convenient to investigate the performance of the protocol, which can be used

to estimate the lower bound of the key rate. Even if Eve's attack is not the entangling cloner attack, the following analysis also holds, resulting from the fact that in a practical experiment, we do not need to assume the eavesdropper's strategy in advance and only need to estimate the channel parameters by the existing data that Alice and Bob hold.

The quadrature of the quantum state sent by Alice's side is denoted by $x_A = x_s + x_M$. In order to obtain the correlation between Alice and Bob after passing through the channel, we assume Eve performs the entangling cloner attack, where Eve's state is modeled by a two-mode squeezed vacuum (TMSV) state ρ_{eE_0} with the CM γ_{eE_0}, which reads:

$$\gamma_{eE_0} = \begin{pmatrix} \omega\mathbf{I} & \sqrt{\omega^2 - 1}\mathbf{Z} \\ \sqrt{\omega^2 - 1}\mathbf{Z} & \omega\mathbf{I} \end{pmatrix},$$ (10)

where ω is the variance of the TMSV, $\mathbf{I} = \mathrm{diag}\,(1,1)$, and $\mathbf{Z} = \mathrm{diag}\,(1,-1)$. The channel is modeled by a beam splitter with the transmittance τ, whose CM is given by:

$$S_\tau = \begin{pmatrix} \sqrt{\tau}\mathbf{I} & \sqrt{1-\tau}\mathbf{I} \\ -\sqrt{1-\tau}\mathbf{I} & \sqrt{\tau}\mathbf{I} \end{pmatrix},$$ (11)

and the excess noise ε can be defined as $\varepsilon := (1-\tau)\,(\omega - 1)/\tau$. Thus, it is easy to deduce the quadrature on Bob's side after passing through the quantum channel, given by:

$$x_B = \sqrt{\tau}x_A + \sqrt{1-\tau}x_0 + x_\varepsilon = \sqrt{\tau}x_M + x_N,$$ (12)

where $x_N = \sqrt{\tau}x_s + \sqrt{1-\tau}x_0 + x_\varepsilon$. Assuming that the squeezing operation is performed for x quadrature, the mutual information between Alice and Bob reads:

$$I^x\,(A:B) = \frac{1}{2}\log_2\frac{V_B}{V_{B|A}} = \frac{1}{2}\log_2\left(1 + \frac{\tau\sigma_x}{V_N}\right),$$ (13)

and V_N has the form:

$$V_N = 1 + \tau\varepsilon + \tau\,(V_S - 1) := 1 + V_\varepsilon + \tau\,(V_S - 1).$$ (14)

When Alice and Bob perform the error correction step, they need to randomly announce part of the information through the public channel, which is also revealed to Eve. It is assumed that eavesdroppers can monitor all classical communication processes; thus, the amount of information leaked in the error correction process must be well estimated and then removed from the final keys. The leakage information ℓ_{EC} in the error correction step can be described as

$$\ell_{EC}^{DR} = H(x_M) - \beta I^x\,(A:B),$$ (15)

in the direct reconciliation (DR) case and:

$$\ell_{EC}^{RR} = H(x_B) - \beta I^x\,(A:B),$$ (16)

in the reverse reconciliation (RR) case, where β is the reconciliation efficiency.

3.3. Practical Estimation of Leakage Information with Finite-Size

In the previous works, the estimator of the leakage information $\hat{\ell}_{EC}$ was treated as an asymptotic parameter, which is independent of the total key length. However in practice, the estimation of $\hat{\ell}_{EC}$ cannot be accurate especially when the key length is not large, further affecting the performance of the error correction. To take finite-size effects into consideration, the estimator $\hat{\ell}_{EC}$ under a practical block length needs to be estimated. We adapt the estimation method shown in [42] to analyze the

characteristics of the channel. Here, we only give the main results of the previous work, and the detailed derivation can be seen in [42]. In the practical experiment, the data on Alice's side is actually the modulated data x_M; thus, the key of parameter estimation is to estimate the CM γ_{MB}, namely $\gamma_{MB} = [V_M\mathbf{I}, c_{MB}\mathbf{Z}; c_{MB}\mathbf{Z}, V_B\mathbf{I}]$. The relation of x_M and x_B (Alice's and Bob's data) has the form of $x_B = \sqrt{\tau}x_M + x_N$, where x_N is the aggregated noise with zero mean, and the variance is shown in Equation (14). The covariance of x_M and x_B is:

$$Cov\,(x_M, x_B) = \sqrt{\tau}V_M =: c_{MB}. \tag{17}$$

For obtaining the estimator of covariance $\hat{c}_{MB}$, we also use M_i denoting the ith modulating value and B_i denoting the ith measurement result, for $i = 1, 2, \ldots, m$, respectively. According to the maximum likelihood estimation, we can get:

$$\hat{c}_{MB} = \frac{1}{m}\sum_{i=1}^{m} M_i B_i. \tag{18}$$

and it is easy to compute the expectation value $\mathbb{E}\,[\hat{c}_{MB}]$ and the variance $\mathbb{V}\,[\hat{c}_{MB}]$ by assuming M_i and B_i are two independent Gaussian variables with zero mean values, which read:

$$\mathbb{E}\,[\hat{c}_{MB}] = c_{MB}, \tag{19}$$

$$\mathbb{V}\,[\hat{c}_{MB}] = \frac{\tau V_M^2}{m}\left(2 + \frac{V_N}{\tau V_M}\right). \tag{20}$$

According to Equation (17), we can get the estimator $\hat{\tau}$ of τ, which reads:

$$\hat{\tau} = \frac{\hat{c}_{MB}^2}{V_M^2} = \frac{\mathbb{V}\,[\hat{c}_{MB}]}{V_M^2}\left(\frac{\hat{c}_{MB}}{\sqrt{\mathbb{V}\,[\hat{c}_{MB}]}}\right)^2, \tag{21}$$

where $\left(\frac{\hat{c}_{MB}}{\sqrt{\mathbb{V}[\hat{c}_{MB}]}}\right)^2$ follows the χ^2-distribution, namely,

$$\left(\frac{\hat{c}_{MB}}{\sqrt{\mathbb{V}\,[\hat{c}_{MB}]}}\right)^2 \sim \chi^2\left(1, \frac{\hat{c}_{MB}^2}{\mathbb{V}\,[\hat{c}_{MB}]}\right). \tag{22}$$

Then, we can calculate the expectation value of $\hat{\tau}$, which reads:

$$\mathbb{E}\,(\hat{\tau}) = \tau + O\,(1/m), \tag{23}$$

and the variance is given by:

$$\mathbb{V}\,(\hat{\tau}) = \frac{4\tau^2}{m}\left(2 + \frac{V_N}{\tau V_M}\right) + O\left(1/m^2\right). \tag{24}$$

For $m \gg 1$, which is practical in experiments, the term $O\left(1/m^2\right)$ can be negligible due to the order $1/m^2$ being small. Thus, we define new variance of $\hat{\tau}$ under a practical block length, which reads:

$$\sigma_{\hat{\tau}}^2 = \frac{4\tau^2}{m}\left(2 + \frac{V_N}{\tau V_M}\right), \tag{25}$$

so that the confidence interval of estimating τ can be well quantified.

In order to estimate the upper bound of the leakage information ℓ_{EC}^{up}, one should give the lower bound of the transmittance τ. For practical purposes, we set the failure probability of the parameter

estimation to $\varepsilon_{PE} = 10^{-10}$, which corresponds to the confidence interval of $6.5\sigma_{\hat{\tau}}$, and one can estimate the lower bound of $\hat{\tau}^{low}$, given by:

$$\hat{\tau}^{low} = \mathbb{E}\left(\tau^{low}\right) := \hat{\tau} - 6.5\sigma_{\hat{\tau}}. \tag{26}$$

According to:

$$x_B = \sqrt{\tau}\left(x_M + x_S\right) + \sqrt{1-\tau}x_0 + x_\varepsilon = \sqrt{\tau}x_M + x_N, \tag{27}$$

the estimator of V_ε can also be calculated by the maximum likelihood estimation with the following form:

$$\hat{V}_\varepsilon = \frac{1}{m}\sum_{i=1}^{m}\left(B_i - \sqrt{\hat{\tau}}M_i\right)^2 + \hat{\tau}\left(1 - V_S\right) - 1. \tag{28}$$

In the case of $m \gg 1$, the estimator $\hat{\tau}$ converges rapidly to the actual value τ as m increases, owing to the variance of $\hat{\tau}$ being negligible. Thus, here, we use τ to replace $\hat{\tau}$ to simplify the estimation process. Noticing that the term $\frac{1}{m}\sum_{i=1}^{m}\left(\frac{B_i - \sqrt{\tau}M_i}{\sqrt{V_N}}\right)^2$ also follows the χ^2-distribution with the expectation value $\mathbb{E}\left(\frac{1}{m}\sum_{i=1}^{m}\left(\frac{B_i - \sqrt{\tau}M_i}{\sqrt{V_N}}\right)^2\right) = m$ and variance $\mathbb{V}\left(\frac{1}{m}\sum_{i=1}^{m}\left(\frac{B_i - \sqrt{\tau}M_i}{\sqrt{V_N}}\right)^2\right) = 2m$, respectively, resulting from $B_i - \sqrt{\tau}M_i$ being Gaussian distributed with variance V_N, therefore, one can get the following approximation when m is large:

$$\sum_{i=1}^{m}\left(B_i - \sqrt{\tau}M_i\right)^2 \approx V_N \cdot \sum_{i=1}^{m}\left(\frac{B_i - \sqrt{\tau}M_i}{\sqrt{V_N}}\right)^2. \tag{29}$$

The expectation value of $\hat{V}_\varepsilon$ can be obtained, which reads:

$$\mathbb{E}\left(\hat{V}_\varepsilon\right) \approx \frac{1}{m}V_N \cdot \mathbb{E}\left(\sum_{i=1}^{m}\left(\frac{B_i - \sqrt{\tau}M_i}{\sqrt{V_N}}\right)^2\right) + \tau\left(1 - V_S\right) - 1 = V_\varepsilon, \tag{30}$$

and the variance of $\hat{V}_\varepsilon$ can also be calculated, given by:

$$\mathbb{V}\left(\hat{V}_\varepsilon\right) \approx \frac{2}{m}V_N^2 + \sigma_{\hat{\tau}}^2(1 - V_S)^2 := \sigma_{\hat{V}_\varepsilon}^2. \tag{31}$$

The upper bound of the variance of excess noise can be given, also considering the failure probability of the parameter estimation to $\varepsilon_{PE} = 10^{-10}$, which is:

$$\hat{V}_\varepsilon^{up} = \mathbb{E}\left(V_\varepsilon^{up}\right) := \hat{V}_\varepsilon + 6.5\sigma_{\hat{V}_\varepsilon}. \tag{32}$$

4. Double-Data Modulation Method and the Modified Estimation Process

Inspired by the double-modulation method developed in [42], we find that this estimation method is also useful in the parameter estimation of the EUR analysis method.

Here, we slightly modify the double-modulation method by pre-generating two sets of Gaussian random numbers, namely x_{M1} and x_{M2}, with variances V_{M1} and V_{M2} and zero mean values, encoding quantum states by new random variable x_M, where $x_M = x_{M1} + x_{M2}$. In this double-data modulation method, Alice holds both data x_{M1} and x_{M2} in her memories and then generates data x_M according to data x_{M1} and x_{M2}. The generated data x_M are used to modulate the quantum states. After Alice and Bob finish the key distribution processes, Alice reveals data x_{M2} to perform the channel parameter estimation, and all the information about data x_{M1} is not announced throughout the parameter estimation phase; thus, x_{M1} can be used for the key extraction step without leaking information about the key during the parameter estimation step. The idea is very similar to that in [42], and the difference is that this double-data modulation method only needs one modulation rather than two, since we

perform the pre-processing of two independent random variables, which simplifies the experimental setup of the double-modulation method.

Since all the exchanged signals can be used for both parameter estimation and key extraction, the estimation of the max-entropy needs to be modified. Recalling that in Section 3, the key point of estimating the max-entropy is to quantify the data distance $d\left(x_M^{total}, x_B^{total}\right)$. However, in traditional EUR method, not all the data can be used for the parameter estimation, and only part of the data (parameter estimation data) can be used to estimate the total data distance, resulting in the statistical fluctuation of the estimating distance, thereby $d\left(x_M^{total}, x_B^{total}\right)$ is approximately replaced by $d\left(x_M^{PE}, x_B^{PE}\right) + \mu$, where the first term is the distance between the parameter estimation data and the second term is the statistical fluctuation of estimating the total data distance by using the parameter estimation data. In the double-data modulation protocol, we modify the L_1 distance between the key-extraction data x_{M1} and Bob's data x_B by exploiting the absolute value inequality, given by:

$$
\begin{aligned}
d\left(x_{M1}, x_B\right) &= \frac{1}{N} \sum_N \left| x_B^i - x_{M1}^i \right| \\
&\leq \frac{1}{N} \sum_N \left| x_B^i - x_{M2}^i \right| + \frac{1}{N} \sum_N \left| x_{M2}^i - x_{M1}^i \right| = d\left(x_{M2}, x_B\right) + d\left(x_{M1}, x_{M2}\right),
\end{aligned}
\tag{33}
$$

where $d\left(x_{M2}, x_B\right)$ denotes the L_1 distance between data x_{M2} and x_B, which can be estimated after Alice reveals data x_{M2}, and $d\left(x_{M1}, x_{M2}\right)$ denotes the L_1 distance between data x_{M1} and x_{M2}, which can be calculated on Alice's side locally. Here, we replace the number of parameter estimation signals m by N since all the exchanged signals are used in this step. Therefore, the max-entropy can be bounded after modifying the parameter estimation step, which reads:

$$
H_{\max}^\varepsilon \left(x_{M1}|x_B\right) \leq N\log_2 \left(d\left(x_{M2}, x_B\right) + d\left(x_{M1}, x_{M2}\right)\right).
\tag{34}
$$

Due to the fact that all the states are exploited to perform parameter estimation, the statistical fluctuation of estimating L_1 distance disappears, which reduces the finite-size effect on estimating the max-entropy, especially in the short block size regime, where the statistical fluctuation cannot be negligible.

The remaining task is to estimate the confidence intervals of the channel parameters by using data x_{M2} and x_B, which is the standard estimation method shown in [42]. The quadrature of the received states on Bob's side can be rewritten in the following form after using the double-data modulation method,

$$
x_B = \sqrt{\tau}\left(x_M + x_S\right) + \sqrt{1-\tau}x_0 + x_\varepsilon = \sqrt{\tau}x_{M2} + x_N^*,
\tag{35}
$$

where $x_N^* = \sqrt{\tau}\left(x_s + x_1\right) + \sqrt{1-\tau}x_0 + x_\varepsilon$ is the aggregated noise when we use x_{M2} to perform the parameter estimation, with variance $V_N^* = \tau\left(x_s + x_1 - 1\right) + 1 + V_\varepsilon$.

After comparing Equation (35) with Equation (27), it is easy to obtain the variances of the estimators $\hat{\tau}$ and $\hat{V}_\varepsilon$ by replacing V_M with V_{M2}, V_N with V_N^*, and m with N, which are given by:

$$
\sigma_{\hat{\tau}^*}^2 = \frac{4\tau^2}{N} \left(2 + \frac{V_N^*}{\tau V_{M2}}\right),
\tag{36}
$$

$$
\sigma_{\hat{V}_\varepsilon^*}^2 = \frac{2}{N} V_N^{*2} + \sigma_{\hat{\tau}^*}^2 \left(1 - V_S\right)^2.
\tag{37}
$$

5. Numerical Simulation and Discussion

In this section, we focus on the simulation analysis of the protocol with the finite-size effect, containing the comparison of the protocol's performances between ideal and practical estimations of the CM and the comparison between standard estimation method and the modified double-data modulation method. The simulation assumes that Eve's attack is the entangling cloner attack. We stress

again that this attack model does not affect the security of the protocol and is just for the convenience of the simulation. In practice, we do not need to assume the attack model in advance and only need to estimate the correlation through the data in the hands of Alice and Bob. The correlation between Alice's and Bob's data can be verified according to whether the L_1 distance $d\left(x_M^{PE}, x_B^{PE}\right)$ shown in Equation (6) is greater than the threshold parameter d_0. If the relation $d\left(x_M^{PE}, x_B^{PE}\right) < d_0$ holds, we think the data between Alice and Bob are correlated. Otherwise, we abort the protocol. In order to determine whether the amount of data is sufficient for the parameter estimation, one needs to use the experimental data of Alice and Bob with a finite block size to estimate the practical parameters and to determine whether the finite-size effect is acceptable by simulation.

We point out that the analysis using the EUR does not rely on Eve's attack method in the experiment, which is due to two reasons. One reason is that the EUR security analysis method itself does not restrict Eve's ability [36], which means there is no need to assume that the quantum state is a product state $\sigma_{AB}^{\otimes N}$, like the collective-attack analysis. Another reason is that the parameter estimation does not need to assume Eve's attacking model. The estimation of max-entropy only needs to estimate the data distance $d\left(x_M^{PE}, x_B^{PE}\right)$ by x_M and x_B. The estimation of ℓ_{EC} needs the variance of the measured data and the signal-to-noise ratio after transmission, which can be obtained from the statistical CM directly. Using the entangling cloner attack model to model Eve's behavior just aims at getting the lower bound of the transmittance τ and the upper bound of the excess noise ε, and then, the lower bound of the key rate can be calculated.

In the following discussion, we consider the squeezed vacuum states with a squeezing level of 13.1 dB and an anti-squeezing level of 25.8 dB, which has experimentally been achieved at 1550 nm with today's technology [50]. We set the reconciliation efficiency β to 95%, which is also easily achievable with CV-QKD's post-processing method [51,52]. The excess noise is chosen as $\varepsilon = 0.01$, and the security parameters are chosen as $\varepsilon_c = \varepsilon_s = 10^{-9}$.

In Figure 2, we plot the key rate as a function of the transmission distance, expressed in terms of km. The lower bound of the key length is given by Equation (2), and the secret key rate is calculated by ℓ_{low}/N. The left panel and the right panel are the performances under the DR and RR cases, respectively. We give the comparison between the ideal CM estimation and the practical CM estimation with different practical block sizes, namely 10^7, 10^8, and 10^9. The solid lines are the protocol under ideal CM estimation, and the dashed lines are the performances under practical CM estimation. We can find that the finite-size effect of estimating the CM will slightly influence the final key rates, and the larger the block size, the smaller the impact. For a practical block size of the order of 10^9, there is almost no influence on the secret key rate.

In Figure 3, we plot the key rate of the protocol as a function of the block size and compare the performances under different transmission distances. In the DR case (left panel), the performances under transmission distances of 3 km, 5 km, and 10 km are illustrated, while the key rates under transmission distances of 3 km, 10 km, and 15 km are plotted in the RR case (right panel), respectively. We can see that the block length of the order of 10^7–10^9 is sufficient for the protocol under the composable security analysis, achieving rates over 10^{-1} bits per channel use for transmission distances of about 10 km in DR and 15 km in RR, respectively. The results also show that, in the case of short transmission distance, the limited block length has a small impact on the performance of the protocol, which will be weakened with the increase of the block length. Moreover, in the case of relatively long transmission distance (approximately more than 10 km), the estimation of leakage information with finite-size has little effect on the final key since the case of long transmission distance requires a larger block size for the error correction.
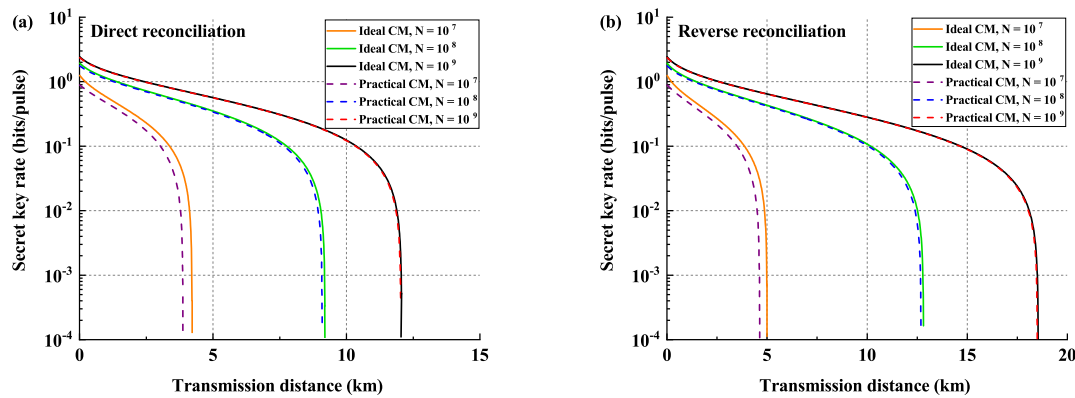
Figure 2. Comparison of performances between the previous key rates and the modified results under different block lengths, namely, 10^7, 10^8, and 10^9. (**a**) shows the direct reconciliation (DR) cases, and (**b**) shows the reverse reconciliation (RR) cases. The solid lines are the performances under the ideal covariance matrix (CM) estimation, and the dashed lines are the performances under practical CM estimation considering finite-size. The reconciliation efficiency β is under a practical value of 95%, and the excess noise is chosen as $\varepsilon = 0.01$. We set the security parameters $\varepsilon_c = \varepsilon_s = 10^{-9}$ and the detection range to $\alpha = 61.6$.
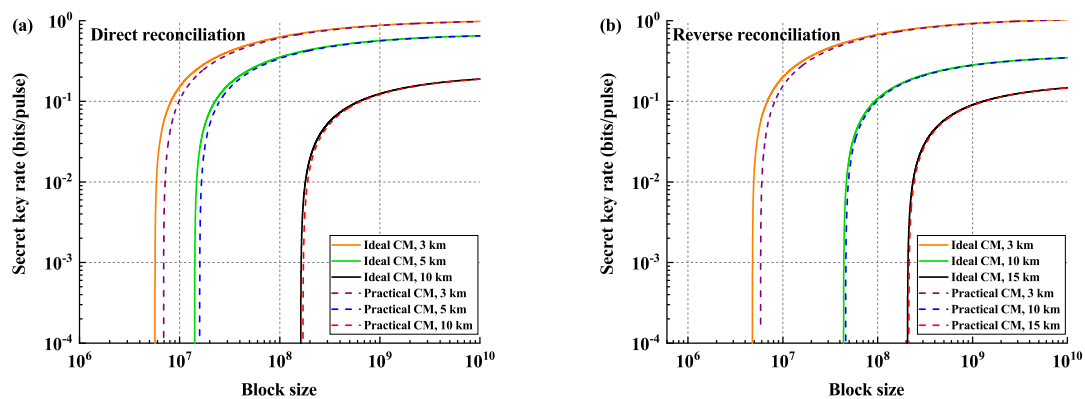
Figure 3. Comparison of performances between the previous key rates and the modified results under different transmission distances. (**a**) shows the direct reconciliation cases, and (**b**) shows the reverse reconciliation cases. The solid lines are the performances under ideal CM estimation, and the dashed lines are the performances under practical CM estimation considering finite-size. The parameters are chosen as in Figure 2.
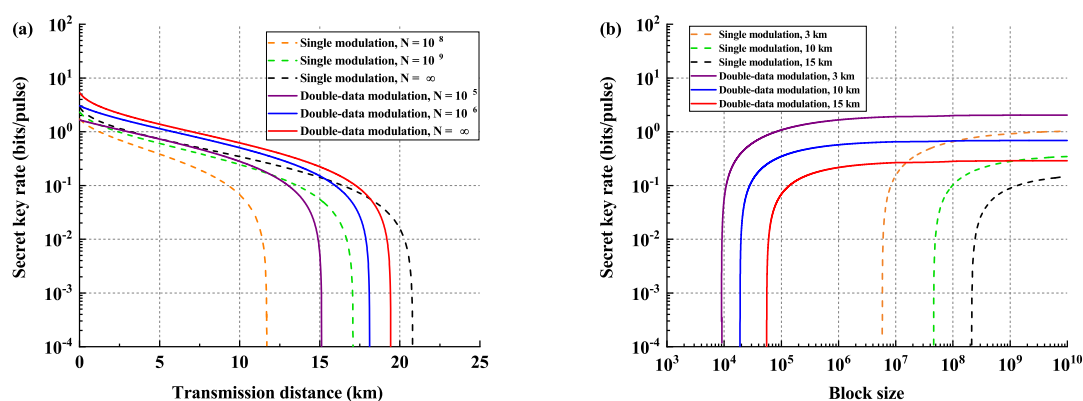
The comparison of the performances between the standard estimation method and the modified double-data modulation method is shown in Figure 4, where the left panel shows the performances of two scenarios under different block sizes, while the right panel shows the protocol's performances under different transmission distances. We optimize the performance of the double-data method by adopting the optimization method shown in [42]. In the left panel, we plot the performances of the double-data modulation method under block sizes of 10^5 and 10^6 and the asymptotic case, respectively, which are shown with solid lines, while the performances of the standard estimation method are depicted with dashed lines, under block sizes of 10^8 and 10^9 and the asymptotic case. It can be seen that, with the help of the double-data modulation method, using less quantum states can achieve better performance than the standard estimation method in a short block-size regime, due to the fact that the data fluctuation term μ in the previous estimation method is not negligible when the block-size is not large, which makes the statistical fluctuation of the finite-size effect more significant in short key

lengths. Thus, the double-data modulation method can efficiently improve the parameter estimation process when the block size is not large. We also note that since we use all the states to extract the key, leading to a high utilization of quantum states, the key rate of the modified method is higher than that of the previous method. However, the double-data modulation method cannot achieve the transmission distance as far as the single-modulation method in the asymptotic case. This is intuitive since the statistical fluctuation in the standard estimation method converges to zero with N going to infinity, while there still exit some noises in estimating data distance in double-data modulation method, namely $d(x_{M1}, x_{M2})$, which will compromise the transmission distance. In the right panel of Figure 4, we can see that the block length of the order of $10^5 - 10^7$ is sufficient for the protocol to support the previous transmission distances with the block size of the order of $10^7 - 10^9$, which we believe, to a large extent, saves the key consumption.

Figure 4. Comparison of the performances between the standard estimation method and the modified double-data modulation method under the reverse reconciliation case. (**a**) shows the performances of two scenarios under different block sizes, while (**b**) shows the protocol's performances under different transmission distances. The dashed lines are the performances using the standard estimation method, and the solid lines are the performances using double-data modulation method.

6. Conclusions

In this work, we investigated the EUR used for the composable security analysis of the CV-QKD protocol and focused on the parameter estimation step, containing the finite-size effect on estimating the CM and the improvement of the parameter the estimation phase using the double-data modulation method, which were not discussed in previous works [36–38]. We believe it is necessary to study the finite-size effect on the parameter estimation in the EUR method, as well as its improvement, since in practice, only limited exchanged states can be used for the parameter estimation, making the estimation process non-ideal.

The analysis showed that the finite-size effect of estimating the CM had a slight influence on the key rate. The larger the block size, the smaller the influence. For a practical block length of the order of 10^9, the influence on the protocol's performance was almost negligible. Thus, in a practical experiment, if the amount of data is large, treating the estimators of parameters as ideal parameters will not have a great influence on the key rate. The result also showed that the parameter estimation method developed in [42] was very effective at handling the finite-size analysis of the covariance matrix in EUR analysis.

To further reduce the impact of the finite-size effect in the parameter estimation phase, we also improved the parameter estimation process by exploiting the double-data modulation method, which was inspired by L. Ruppert, et al. [42]. All the quantum states can be used for both parameter estimation and key extraction, which improves the utilization of exchanged states. After modifying the estimation of the max-entropy, we found that the finite-size effect was to a large extent suppressed when the block

size was not large, which saved the key consumption, while the longest transmission distances in the asymptotic case were compromised.

Our work is an improvement of previous works [36,37]. We believe that the modified estimation method is practical by using less states to perform parameter estimation.

Abbreviations

The following abbreviations are used in this manuscript:

CV　　Continuous-variable
DV　　Discrete-variable
QKD　Quantum key distribution
EUR　Entropic uncertainty relation
CM　　Covariance matrix
DR　　Direct reconciliation
RR　　Reverse reconciliation

References

1. Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **2002**, *74*, 145–195. [CrossRef]
2. Scarani, V.; Bechmann-Pasquinucci, H.; Cerf, N.J.; Dušek, M.; Lütkenhaus, N.; Peev, M. The security of practical quantum key distribution. *Rev. Mod. Phys.* **2009**, *81*, 1301–1350. [CrossRef]
3. Weedbrook, C.; Pirandola, S.; García-Patrón, R.; Cerf, N.J.; Ralph, T.C.; Shapiro, J.H.; Lloyd, S. Gaussian quantum information. *Rev. Mod. Phys.* **2012**, *84*, 621–669. [CrossRef]
4. Diamanti, E.; Leverrier, A. Distributing secret keys with quantum continuous variables: Principle, security and implementations. *Entropy* **2015**, *17*, 6072–6092. [CrossRef]
5. Pirandola, S.; Andersen, U.L.; Banchi, L.; Berta, M.; Bunandar, D.; Colbeck, R.; Englund, D.; Gehring, T.; Lupo, C.; Ottaviani, C.; et al. Advances in quantum cryptography. *arXiv* **2019**, arXiv:1906.01645.
6. Ralph, T.C. Continuous variable quantum cryptography. *Phys. Rev. A* **1999**, *61*, 010303(R). [CrossRef]
7. Hillery, M. Quantum cryptography with squeezed states. *Phys. Rev. A* **2000**, *61*, 022309. [CrossRef]
8. Cerf, N.J.; Lévy, M.; Van Assche, G. Quantum distribution of Gaussian keys using squeezed states. *Phys. Rev. A* **2001**, *63*, 052311. [CrossRef]
9. Usenko, V.C.; Filip, R. Squeezed-state quantum key distribution upon imperfect reconciliation. *New J. Phys.* **2011**, 13, 113007. [CrossRef]
10. Grosshans, F.; Grangier, P.; Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.* **2002**, *88*, 057902. [CrossRef]
11. Grosshans, F.; van Assche, G.; Wenger, J.; Brouri, R.; Cerf, N.J.; Grangier, P. Quantum key distribution using gaussian-modulated coherent states. *Nature* **2003**, *421*, 238–241. [CrossRef] [PubMed]
12. 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. [CrossRef] [PubMed]
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. [CrossRef]

14. Sun, M.; Peng, X.; Shen, Y.; Guo, H. Security of a new two-way continuous-variable quantum key distribution protocol. *Int. J. Quantum Inf.* **2012**, *10*, 1250059. [CrossRef]

15. Zhang, Y.-C.; Li, Z.; Weedbrook, C.; Yu, S.; Gu, W.; Sun, M.; Peng, X.; Guo, H. Improvement of two-way continuous-variable quantum key distribution using optical amplifiers. *J. Phys. B* **2014**, *47*, 035501. [CrossRef]

16. Ottaviani, C.; Mancini, S.; Pirandola, S. Two-way Gaussian quantum cryptography against coherent attacks in direct reconciliation. *Phys. Rev. A* **2015**, *92*, 062323. [CrossRef]

17. Ottaviani, C.; Pirandola, S. General immunity and superadditivity of two-way Gaussian quantum cryptography. *Sci. Rep.* **2016**, *6*, 22225. [CrossRef]

18. Zhang, Y.; Li, Z.; Zhao, Y.; Yu, S.; Guo, H. Numerical simulation of the optimal two-mode attacks for two-way continuous-variable quantum cryptography in reverse reconciliation. *J. Phys. B At. Mol. Opt. Phys.* **2017**, *50*, 035501. [CrossRef]

19. Leverrier, A.; Grangier, P. Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation. *Phys. Rev. Lett.* **2009**, *102*, 180504. [CrossRef]

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

21. Li, Z.; Zhang, Y.; Guo, H. User-defined quantum key distribution. *arXiv* **2018**, arXiv: 1805.04249.

22. 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. [CrossRef]

23. Zhang, Y.-C.; Li, Z.; Yu, S.; Gu, W.; Peng, X.; Guo, H. Continuous-variable measurement-device-independent quantum key distribution using squeezed states. *Phys. Rev. A* **2014**, *90*, 052325. [CrossRef]

24. 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. Photon.* **2015**, *9*, 397–402. [CrossRef]

25. Zhang, X.; Zhang, Y.; Zhao, Y.; Wang, X.; Yu, S.; Guo, H. Finite-size analysis of continuous-variable measurement-device-independent quantum key distribution. *Phys. Rev. A* **2017**, *96*, 042334. [CrossRef]

26. Papanastasiou, P.; Ottaviani, C.; Pirandola, S. Finite-size analysis of measurement-device-independent quantum cryptography with continuous variables. *Phys. Rev. A* **2017**, *96*, 042332. [CrossRef]

27. Lupo, C.; Ottaviani, C.; Papanastasiou, P.; Pirandola, S. Continuous-variable measurement-device-independent quantum key distribution: Composable security against coherent attacks. *Phys. Rev. A* **2018**, *97*, 052327. [CrossRef]

28. Chen, Z.; Zhang, Y.; Wang, G.; Li, Z.; Guo, H. Composable security analysis of continuous-variable measurement-device-independent quantum key distribution with squeezed states for coherent attacks. *Phys. Rev. A* **2018**, *98*, 012314. [CrossRef]

29. 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. [CrossRef]

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

31. Zhang, Y.; Li, Z.; Chen, Z.; Weedbrook, C.; Zhao, Y.; Wang, X.; Huang, Y.; Xu, C.; Zhang, X.; Wang, Z.; et al. Continuous-variable QKD over 50km commercial fiber. *Quantum Sci. Technol.* **2019**, *4*, 035006. [CrossRef]

32. Leverrier, A. Composable security proof for continuous-variable quantum key distribution with coherent states. *Phys. Rev. Lett.* **2015**, *114*, 070501. [CrossRef] [PubMed]

33. Leverrier, A. Security of continuous-variable quantum key distribution via a Gaussian de Finetti reduction. *Phys. Rev. Lett.* **2017**, *118*, 200501. [CrossRef] [PubMed]

34. Christandl, M.; König, R.; Renner, R. Postselection technique for quantum channels with applications to quantum cryptography. *Phys. Rev. Lett.* **2009**, *102*, 020504. [CrossRef] [PubMed]

35. 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. [CrossRef] [PubMed]

36. 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. [CrossRef]

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

38. Gehring, T.; Händchen, V.; Duhme, J.; Furrer, F.; Franz, T.; Pacher, C.; Werner, R.F.; Schnabel, R. Implementation of continuous-variable quantum key distribution with composable and one-sided-device-independent security against coherent attacks. *Nat. Commun.* **2015**, *6*, 8795. [CrossRef]

39. Marangon, D.G.; Vallone, G.; Villoresi, P. Source-device-independent ultrafast quantum random number generation. *Phy. Rev. Lett.* **2017**, *118*, 060503. [CrossRef]

40. Xu, B.; Chen, Z.; Li, Z.; Yang, J.; Su, Q.; Huang, W.; Zhang, Y.; Guo, H. High speed continuous variable source-independent quantum random number generation. *Quantum Sci. Technol.* **2019**, *4*, 025013. [CrossRef]

41. Coles, P.J.; Berta, M.; Tomamichel, M.; Wehner, S. Entropic uncertainty relations and their applications. *Rev. Mod. Phys.* **2017**, *89*, 015002. [CrossRef]

42. Ruppert, L.; Usenko, V.C.; Filip, R. Long-distance continuous-variable quantum key distribution with efficient channel estimation. *Phys. Rev. A* **2014**, *90*, 062310. [CrossRef]

43. Renner, R. Security of Quantum Key Distribution. Ph.D. Thesis, Swiss Federal Institute of Technology (ETH) Zurich, Zurich, Switzerland, 2006.

44. Müller-Quade, J.; Renner, R. Composability in quantum cryptography. *New J. Phys.* **2009**, *11*, 085006. [CrossRef]

45. Carter, J.L.; Wegman, M.N. Universal classes of hash functions. *J. Comput. Syst. Sci.* **1979**, *18*, 143. [CrossRef]

46. Ghorai, S.; Diamanti, E.; Leverrier, A. Composable security of two-way continuous-variable quantum key distribution without active symmetrization. *Phys. Rev. A* **2019**, *99*, 012311. [CrossRef]

47. Kiukas, J.; Werner, R.F. Maximal violation of Bell inequalities by position measurements. *J. Math. Phys.* **2010**, *51*, 072105. [CrossRef]

48. Serfling, R.J. Probability inequalities for the sum in sampling without replacement. *Ann. Stat.* **1974**, *2*, 39. [CrossRef]

49. 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.

50. Schönbeck, A.; Thies, F.; Schnabel, R. 13 dB squeezed vacuum states at 1550 nm from 12 mW external pump power at 775 nm. *Opt. Lett.* **2018**, *43*, 110. [CrossRef]

51. Wang, X.; Zhang, Y.; Li, Z.; Xu, B.; Yu, S.; Guo, H. Efficient rate-adaptive reconciliation for CV-QKD protocol. *Quantum Inf. Comput.* **2017**, *17*, 1123.

52. Wang, X.; Zhang, Y.; Yu, S.; Guo, H. High speed error correction for continuous-variable quantum key distribution with multi-edge type LDPC code. *Sci. Rep.* **2018**, *8*, 10543. [CrossRef] [PubMed]