Composable security of unidimensional continuous-variable quantum key distribution

Qin Liao · Ying Guo · Cailang Xie · Duan Huang · Peng Huang · Guihua Zeng

Received: date / Accepted: date

Abstract We investigate the composable security of unidimensional continuous-variable quantum key distribution (UCVQKD), which is based on the Gaussian modulation of a single quadrature of the coherent-state of light, aiming to provide a simple implementation of key distribution compared to the symmetrically modulated Gaussian coherent-state protocols. This protocol neglects the necessity in one of the quadrature modulation in coherent-states and hence reduces the system complexity. To clarify the influence of finite-size effect and the cost of performance degeneration, we establish the relationship of the balanced parameters of the unmodulated quadrature and estimate the precise secure region. Subsequently, we illustrate the composable security of the UCVQKD protocol against collective attacks and achieve the tightest bound of the UCVQKD protocol. Numerical simulations show the asymptotic secret key rate of the UCVQKD protocol, together with the symmetrically modulated Gaussian coherent-state protocols.

Keywords Quantum key distribution · Unidimensional modulation · Composable security

1 Introduction

Quantum key distribution (QKD) [1,2,3] is a branch of quantum cryptography, whose goal is to provide an elegant way that allows two distant legitimate

1. School of Information Science Engineering, Central South University, Changsha 410083, China
2. State Key Laboratory of Advanced Optical Communication Systems and Networks, and Center of Quantum Information Sensing and Processing, Shanghai Jiao Tong University, Shanghai 200240, China
* yingguo@csu.edu.cn
† duanhuang@foxmail.com
partners, Alice and Bob, to share a random secure key over unsecure quantum and classical channels. Its security is provided by the laws of quantum physics [4,5]. QKD has spurred lots of interest over the last three decades, giving birth to two main approaches, i.e., discrete-variable (DV) QKD [6,7,8] and continuous-variable (CV) QKD [9,10,11,12,13,14]. In the first approach, the key bits are usually encoded to the polarization status of single photons. Different from the former approach, in CVQKD, the sender Alice usually encodes key bits in the quadratures (\(\hat{x}\) and \(\hat{p}\)) of optical field with Gaussian modulation [15], while the receiver Bob can restore the secret key bits through homodyne or heterodyne detection techniques [16,17].

In the traditional CVQKD protocol, there are usually the amplitude and phase quadratures used for the symmetrical modulations. However, in an asymmetric CVQKD protocol, there is only one quadrature for information modulation (e.g., an amplitude modulator or a phase modulator), which is called the UCVQKD [18,19], was suggested to reduce the complexity and the cost of apparatus, facilitating the commercialization of the practical CVQKD. Moreover, in the UCVQKD protocol it could avoid creating a hole in the center of Gaussian probability distribution by adopting a simple single-quadrature modulation [18] and allows the implementation using more standard and cheaper devices. However, it was still challenged by the degree of performance degeneration and the influence of finite-size effect of the UCVQKD, due to the ambiguous relationship of the parameters related to the unmodulated quadratures.

As for the security CVQKD protocols, it can usually be analyzed in the asymptotic case, the finite-size regime and the composable security. In the asymptotic case, the asymptotic secure key rate can be achieved with the covariance matrix of whole quantum system. However, the asymptotic secure key rate is a theoretically computed value which ignores the finite size effect of raw keys, and its upper bound cannot be achieved in practice. In order to solve this problem, a security analysis which takes the finite-size effects into account was proposed [20]. As a result, the secure key rates are more pessimistic than those obtained in asymptotic case, but it is more closer to the practice. After that, the composable security for symmetrically modulated Gaussian coherent-state protocols [21,22,23] was proposed to provide several refined security proofs and improved bounds for the secret key rates. Leverrier [24] suggested the composable security proof for CVQKD with coherent states against collective attacks and confirmed that the Gaussian attacks are optimal asymptotically in the case of composable security framework. It is the enhancement of security based on uncertainty of the finite-size effect [25], and thus, one can achieve the best security, namely the tightest bound, by subtly dividing the failure probabilities in the CVQKD system.

In this paper, we give an overall security analysis of the UCVQKD protocol, which is based on the Gaussian modulation of a single quadrature of the coherent-state of light, in both asymptotic case and finite-size regime. We derive the relationship of the parameters related to the unmodulated quadrature in the suitable secure regions with two extreme scenarios, which show the
Fig. 1 Scheme of the UCVQKD protocol. (Top) Prepare-and-measure model. Alice prepares a coherent state using a laser source and then displaces the state along the modulated quadrature by using modulator $M$, $V_M$ is the modulation variance. The states are subsequently sent to Bob through a general phase-sensitive channel with transmittance $\eta_{x,p}$ and excess noise $\varepsilon_{x,p}$. (Bottom) Equivalent entanglement-based model using two-mode squeezed vacuum state (EPR state). Alice measures mode $A$ using homodyne detection which projects the other half of EPR state onto a squeezed state $B$, then a squeezing operation is applied to transform mode $B$ to a coherent state $B_1$. Subsequently mode $B_1$ is sent to Bob through the generally phase-sensitive channel controlled by Eve.

Theoretical performance of asymptotic secret key rate of the UCVQKD protocol. To render the performance close to the reality, we analyze the composable security of the UCVQKD protocol against collective attacks, and obtain the tightest bound of the UCVQKD protocol.

This paper is structured as follows. In Sec. II, we demonstrate the structure of the UCVQKD protocol. In Sec. III, we establish the relationship of the parameters related to the unmodulated quadrature, and derive the symptomatic secret key of the UCVQKD protocol. In Sec. IV, we illustrate the composable security of the UCVQKD protocol. Finally, conclusions are drawn in Sec. V.

2 Scheme design of the UCVQKD

The data process of the UCVQKD focuses on using only one quadrature of coherent states to modulate information. This is in stark contrast to previous protocols where two quadratures are modulated simultaneously. As can be seen from the top panel of FIG. 1, it illustrates the prepare-and-measure UCVQKD protocol. The trusted sender, Alice, prepares coherent states with laser source, where one of the quadratures $\hat{x}$ (amplitude quadrature) or $\hat{p}$ (phase quadrature) is modulated using modulator $M$. As a result, each coherent state is displaced with displacement variance $V_M$ according to a random
number drawn from a one-dimensional Gaussian alphabet. Without loss of
generality, we assume \( \tilde{x} \) is modulated for rendering the simple derivation. The
prepared states are subsequently sent to the remote trusted party Bob through
a generally phase-sensitive channel with transmittance \( \eta_x, \eta_p \) and excess noise
\( \varepsilon_x, \varepsilon_p \) in \( \tilde{x} \) and \( \tilde{p} \) quadratures, respectively \[18\]. Bob applies either heterodyne
or homodyne detector to perform coherent detection of the quadratures. Note
that although \( \tilde{p} \) quadrature is not modulated, Bob still needs to measure it
(measuring most of the time \( \tilde{x} \) quadrature and sometimes \( \tilde{p} \) quadrature) to
gather statistics on the properties of the channel in \( \tilde{p} \) quadrature \[19\]. The
data acquired by Bob while measuring the amplitude quadrature \( \tilde{x} \) is corre-
lated with Alice’s modulated data. After several runs, this correlation can be
used to extract a secret key by post-processing. The most advantage of the
UCVQKD protocol is that the protocol would well simplify the implementation
with more standard and cheaper devices, and hence reduces the complexity of
CVQKD system.

3 Asymptotic security of the UCVQKD

To simplify the security analysis, we switch to the equivalent entanglement-
based (EB) scheme, which allows the explicit description of the trusted modes
and correlations, as shown at the bottom panel of FIG. 1 where quantum
channel is replaced by eavesdropper Eve and the so called entangling cloner
\[15,26,27\] can be used for launching the proven optimal collective Gaussian
attack. Eve could replace quantum channel with transmittance \( \eta_{x,p} \) and ex-
cess noise referred to the input \( \chi_{x,p} \) by preparing the ancilla \( |E\rangle \) of variance
\( W_{x,p} \) and a beam splitter of transmittance \( \eta_{x,p} \). The value \( W_{x,p} \) can be tuned
to match the noise of the real channel \( \chi_{x,p} = (1 - \eta_{x,p})/\eta_{x,p} + \varepsilon_{x,p} \). In order
to simplify the description, we only focus on the UCVQKD with reverse recon-
ciliation (RR), while the direct reconciliation (DR) version can be derived
through interchanging the sides of Alice and Bob.

According to the extremity of Gaussian quantum states \[15,28,29\], the
lower bound of the asymptotic secret key rate of the UCVQKD protocol under
collective attack strategy can be given by

\[
K = \beta I(A : B_2) - \chi_E, \tag{1}
\]

where \( \beta \) is the reconciliation efficiency, \( I(A : B_2) \) is the Shannon mutual
information on quadrature \( \tilde{x} \) available to the trusted parties Alice and Bob,
and Eve’s information \( \chi_E = S(E) - S(E|x_B) \) is the Holevo bound \[30\] of the
upper mutual information extractable from Eve and Bob for RR. After Bob
applies homodyne measurement, Eve purifies the whole system, rendering the
mutual information between Eve and Bob measurement expressed as

\[
\chi_E = S(E) - S(E|x_B) = S(AB_2) - S(A|x_B). \tag{2}
\]
Therefore, the asymptotic secret key rate of the UCVQKD protocol for RR is derived as

\[ K_{RR} = \beta I(A : B_2) - (S(AB_2) - S(A|x_B)). \quad (3) \]

As mentioned in the UCVQKD protocol, it uses only one quadrature (say \( \hat{x} \)) to modulate information, which results in its covariance matrix no longer symmetric in both quadratures as its counterpart, the symmetrical Gaussian modulation coherent-state QKD protocol (i.e. GG02 protocol [17]). In EB UCVQKD scheme, Alice prepares two-mode squeezed vacuum (TMSV) states \( |\Psi\rangle \) of variance \( V \) and each TMSV state involves two modes A and B, which can be expressed by

\[ |\Psi\rangle = \sqrt{1 - z^2} \sum_{i=0}^{\infty} z^i |i_A\rangle \otimes |i_B\rangle, \quad (4) \]

where \( z \in [0, 1) \) and \( |i\rangle \in \mathbb{N} \) denotes the Fock state. Alice keeps mode A of TMSV state to herself and sends mode B to Bob. For the UCVQKD protocol, such a scheme can be realized by performing a local squeezing operation \( S \) with a squeezing parameter \( -\log \sqrt{V} \) onto mode B before it is sent to quantum channel, which results in the following covariance matrix:

\[
\Gamma_{AB_1} = \begin{pmatrix}
V & 0 & \sqrt{V(V^2 - 1)} & 0 \\
0 & V & 0 & -\sqrt{V^2 - 1} \\
\sqrt{V(V^2 - 1)} & 0 & V^2 & 0 \\
0 & -\sqrt{V^2 - 1} & 0 & V^2 \\
\end{pmatrix}.
\quad (5)
\]

Thus, the EB scheme is then equivalent to the Gaussian displacement of coherent states along the \( \hat{x} \) quadrature with variance \( V_M = V^2 - 1 \). As the states travel through quantum channel with transmittance \( \eta_{x,p} \) and excess noise \( \epsilon_{x,p} \), the transformed covariance matrix is formed as follow:

\[
\Gamma_{AB_2} = \begin{pmatrix}
\gamma_A & \sigma_{AB_2} \\
\sigma_{AB_2}^T & \gamma_{B_2} \\
\end{pmatrix},
\quad (6)
\]

where \( \gamma_A = \sqrt{V_M + 1} \), I represent diag(1,1), and

\[
\gamma_{B_2} = \begin{pmatrix}
1 + \eta_x (V_M + \epsilon_x) & 0 \\
0 & 1 + \eta_p \epsilon_p \\
\end{pmatrix},
\quad (7)
\]

and

\[
\sigma_{AB_2} = \begin{pmatrix}
(\eta_x V_M \sqrt{V_M + 1})^{\frac{1}{2}} & 0 \\
0 & (\eta_p V_M) \left( \sqrt{V_M + 1} \right)^{\frac{1}{2}} \\
\end{pmatrix} \sigma_z,
\quad (8)
\]

where

\[
\sigma_z = \begin{pmatrix}
1 & 0 \\
0 & -1 \\
\end{pmatrix}.
\quad (9)
\]

It is worth noting that, since there is no modulation in \( \hat{p} \) quadrature at Alice’ side, the channel transmittance and excess noise thereby cannot be estimated in \( \hat{p} \) quadrature for the parameter estimation. Therefore, Bob cannot obtain
the estimated values of $\eta_p$ and $\varepsilon_p$, respectively. In fact, since Bob needs to measure $\hat{p}$ quadrature, he can acquire the result of the variance of the channel output in $\hat{p}$ quadrature rather than the parameter $\eta_p$ and $\varepsilon_p$. That is to say, the item noted as $1 + \eta_p\varepsilon_p$ in matrix $\gamma_B$ is known. However, Bob cannot acquire the correlation between the two trusted modes in $\hat{p}$ quadrature due to $\eta_p$ and $\varepsilon_p$ are unknowable. In order to estimate the asymptotic key rate of the UCVQKD protocol, we have to derive the relationship of the two unknown parameters $\eta_p$ and $\varepsilon_p$.

Theoretically, the two parameters can be set to any values limited in their domain. However, according to the Heisenberg uncertainty principle [31], the unknown parameters must be bounded by the requirement of physicality, which satisfies the following constraint

$$\Gamma_{AB} + i\Omega \geq 0, \quad \text{(10)}$$

where $\Omega$ is the symplectic form with

$$\Omega = \bigoplus_{i=1}^{n} \omega, \quad \omega = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \quad \text{(11)}$$

For the UCVQKD protocol, the two unknown parameters satisfy the physical constraint

$$\left(\kappa \sqrt{\eta_x} - \sqrt{\eta_p}\right)^2 \leq (1 - \kappa \eta_x)(1 + \eta_p\varepsilon_p - \kappa), \quad \text{(12)}$$

where $\kappa = \frac{1}{1 + \eta_x\varepsilon_x}$.

In Fig. 2, we illustrate the regions bounded by physicality and the positive secret key rate with the given parameters $\eta_x = 0.4$ and $\varepsilon_x = 0.05$ (these
value could represent one of the usual cases). The whole plane is divided into three regions, i.e., unphysical region, unsecure region, and secure region. In unphysical region, it denotes the restricted zone in which the current values of $\eta_p$ and $\varepsilon_p$ cannot be set simultaneously, otherwise it will violate Heisenberg uncertainty principle. That is to say, even though the maximum secret key rate (point (1)) existing in this area, it is impractical to achieve such highest secret key rate in reality. In unsecure region, it shows (the blank area within the unphysical region excluded) that the UCVQKD protocol cannot generate the positive secret key rate. In secure region, it shows (the blank area within the unphysical region excluded) that the UCVQKD protocol cannot generate the positive secret key rate under the optimal collective attack. Therefore, the accessible maximum asymptotic secret key rate can be achieved at the point (2) instead of the unrealistic point (1). Moreover, in order to ensure the security, one should further take the more pessimistic case into account. The pessimistic case and the optimal case can be derived as the two extreme scenarios in Appendix B.

In what follows, we show the asymptotic performance of the UCVQKD protocol. In the traditional communication system, one expects the values of channel loss and excess noise in both quadratures are symmetric, namely $\eta_p = \eta_x = \eta$ and $\varepsilon_p = \varepsilon_x = \varepsilon$. Therefore, the previous covariance matrix $\Gamma_{AB}$ turns to:

$$
\Gamma_{s,AB}^{sym} = \left( \begin{array}{cc}
\frac{\gamma A}{\sigma_{AB}^{sym}} & \sigma_{AB}^{sym} \\
\sigma_{AB}^{sym} & \frac{\gamma B}{\sigma_{AB}^{sym}}
\end{array} \right),
$$

where

$$
\gamma_B = \left( 1 + \eta(\sqrt{V_M} + \varepsilon) \right) 0 \\
0 1 + \eta \varepsilon,
$$

and

$$
\sigma_{AB}^{sym} = \left( \begin{array}{cc}
(\eta V_M \sqrt{V_M + 1})^{\frac{1}{2}} & 0 \\
0 & -(\eta V_M \sqrt{V_M + 1})^{-\frac{1}{2}}
\end{array} \right).
$$

Taking the loss rate 0.2dB/km and the modulation variance $V_M = 20$, we compare the performance of the UCVQKD protocol and the symmetrical Gaussian modulation coherent-state protocol \cite{15,17,28}, as shown in Fig. 3 (See Appendix C for calculation of the asymptotic secret key rate). We find that the UCVQKD protocol is obviously outperformed by the symmetrical Gaussian modulation coherent-state protocol. Actually, this result is what we expect, since the unidimensional modulation scheme uses only one quadrature to carry the useful information, while its counterpart, the symmetrical Gaussian modulation coherent-state protocol, uses both quadrature $\hat{x}$ and $\hat{p}$ to carry information, which certainly results in a higher secret key rate. As a result, one may have to make a tradeoff between the secret key rate and the implementation for the given modulation variance.

Fortunately, a better performance of the UCVQKD protocol can be achieved by dynamically choosing an optimal modulation variance $V_M$. As shown in Fig. 4, we plot the asymptotic key rate of the UCVQKD protocol and the symmetrical coherent-state protocol with the optimized modulation variance $V_M$ at
Fig. 3 Comparison of the UCVQKD protocol with symmetrically modulated Gaussian coherent-state protocol. The blue line denotes the performance of corresponding symmetrically modulated Gaussian coherent-state protocol, while the red line represents the UCVQKD protocol. The inset shows the maximum tolerable excess noise at each channel loss. Modulation variance is $V_M = 20$, reconciliation efficiency is $\beta = 95\%$, and excess noise is $\varepsilon = 0.01$.

each channel loss. The performance of the UCVQKD protocol is dramatically improved by choosing the suitable modulation variance $V_M$, whereas the best performance of the symmetrical coherent-state protocol has been achieved. Moreover, the gap of the performance between the UCVQKD protocol and the symmetrical coherent-state protocol is shortened for the optimized $V_M$. Therefore, by choosing the optimal modulation variance $V_M$, we can achieve the relatively high performance, which approaches to the corresponding symmetrical coherent-state protocol, while paying only a little price.

4 Composable security analysis of the UCVQKD protocol

In the composable security analysis, we consider the detailed data processing in the UCVQKD system so that one can obtain the tightest secure bound of the protocol. In this section, we give the first composable security analysis of the UCVQKD protocol against collective attacks. The definitions of the composable security can be found in [24,32,33]. We, in what follows, elaborate the composable security analysis of the UCVQKD protocol when confronting collective attacks.

In this section, we focus on the EB UCVQKD protocol with RR, which can be characterized by the similar parameters derived in the composable security case as shown in Tab. 1. First of all, the two trusted parties, Alice and Bob, obtain $2n$-mode state respectively and form the global state denoted by $\rho_{AB}^{2n}$. Then, homodyne detections are applied by Alice and Bob to measure their
Fig. 4 The asymptotic security key rate of the UCVQKD protocol (red line) and the corresponding symmetrically modulated Gaussian coherent-state protocol (blue line) as a function of channel loss for every optimal modulation variance $V_M$. The inset shows the optimal $V_M$ for the current maximal secret key rate. Reconciliation efficiency is $\beta = 95\%$, and excess noise is $\varepsilon = 0.01$.

Table 1 The parameters of the UCVQKD protocol in the composable security analysis

| parameter | definition |
|-----------|------------|
| $2n$ | number of light pulses (with single-quadrature-modulation) exchanged in the UCVQKD. |
| $\lambda$ | percentage of the modulated quadratures detected correctly by Bob. |
| $l$ | size of the final key when the protocol did not abort. |
| $d$ | number of bits on which each measurement result is encoded. |
| $\text{leak}_{EC}$ | size of Bob's communication to Alice for error correction. |
| $\epsilon_{PE}$ | maximum failure probability of parameter estimation. |
| $\epsilon_{cor}$ | small probability of the failure that the keys of Alice and Bob do not identical and the protocol did not abort. |
| $n_{PE}$ | number of bits that Bob sends to Alice in parameter estimation. |
| $\Omega_{max}$ | bounds on covariance matrix elements, which must be apt in the realization of the protocol. |

respective obtained modes. It is known that homodyne detection on mode A of two-mode squeezed vacuum state will project mode B onto a squeezed state, which is subsequently transformed to a coherent state after passing a squeezing operation. Note that it is not necessary to measure mode B$_2$ using heterodyne detection since only one quadrature has been modulated. Bob continues to apply homodyne measurements over mode B$_2$ with the probability $\lambda$, obliging Alice to discard the measurement results of unmodulated quadrature. After that, Alice and Bob obtain two continuous variables $X, Y \in \mathbb{R}^{2\lambda n}$. Bob discretizes his $2\lambda n$-vector $Y$ to obtain $m$-bit string $U$, where $m = 2\lambda dn$, i.e. each correct measurement result is encoded with $d$ bits. During the error
corrections, Bob sends syndrome of $U$ which agreed on in advance to Alice and lets Alice guess $U_A$ for the string of Bob. Bob computes a hash of $U$ of length $\lceil \log(1/\epsilon_{cor}) \rceil$ and sends it to Alice who compares it with her own hash. The protocol resumes if both hashes coincide. The value $\text{leak}_{EC}$ corresponds to the total number of bits sent by Bob during this step. Subsequently, in parameter estimation, Bob sends $n_{PE}$ bits of $U$ to Alice, which is required for calculations of $\omega_a$, $\omega_b$ and $\omega_c$ in Eqs. (17) (18) and (19). The protocol continues for $\omega_a \leq \Omega_{\text{max}}^a$ and $\omega_b \leq \Omega_{\text{max}}^b$ and $\omega_c \geq \Omega_{\text{min}}^c$. Finally, Alice and Bob apply a random universal 2 hash function to their respective strings, resulting in the two final strings $S_A$ and $S_B$ of size $l$. In the following, we elaborate the detailed composable security analysis of the UCVQKD protocol.

4.1 State preparation

Alice prepares $2^n$ TMSV states $|\Psi\rangle^{\otimes 2n}$ of variance $V$ and each state involves two modes A and B, as expressed in Eq. (4). Without loss of generality, we assume quadrature $\hat{x}$ is the modulated quadrature. The transformed covariance matrix can be derived in Eq. (6) after the state is transmitted through quantum channel with transmittance $\eta_{x,p}$ and excess noise $\epsilon_{x,p}$. Once Alice and Bob collect $2^n$ pulses, the protocol will start to the next step.

4.2 Measurement

In the measurement, both Alice and Bob have access to $2^n$ modes, where Alice measures with heterodyne detector and Bob measures with homodyne detector, respectively. Because only one quadrature $\hat{x}$ is modulated, Alice discards the measurement results derived from quadrature $\hat{p}$ meanwhile Bob measures quadrature $\hat{x}$ with probability $\lambda$. The reason is that Eve may know the protocol that Alice and Bob obeyed, and hence the two trusted parties must measure the correct quadrature with a certain probability $\lambda$. Assume that the two trusted parties are perfect so that Eve cannot know the executive probability. After that, Alice and Bob then form two vectors of length $2\lambda n$ that can be denoted by $X = (X_1, \ldots, X_{2\lambda n})$ for Alice and $Y = (Y_1, \ldots, Y_{2\lambda n})$ for Bob, respectively. Notice that $X$ and $Y$ are continuous variables, and hence we have to discretize them in order to let the data suitable for processing. Firstly, the real axis can be divided into $2^d$ intervals and this partition should be chosen to maximize the secret key rate when the quantum channel acts as a Gaussian channel with the fixed transmittance and excess noise. The average variance of Bob’s measurement can be calculated as $\frac{1}{2\lambda n} ||Y||^2$. Thus, each interval (that follows normal distribution $\mathcal{N}(0, \frac{1}{2\lambda n} ||Y||^2)$) can be assigned a distinct value by applying the discretization map $D : Y \mapsto U$. The detailed discretization discretization schemes can be found in the literature [34]. Finally, Alice obtains $X \in \mathbb{R}^{2\lambda n}$, whereas Bob obtains $Y \in \mathbb{R}^{2\lambda n}$ and $U \in \{1, \ldots, 2^d\}^{2\lambda n}$. 
4.3 Error correction

Reverse reconciliation is applied for Alice to generate the string $U$. More specifically, Bob sends the value of $||Y||^2$, which is used for discretization function $D$, to Alice. An effective technique for error correction is to perform sparse parity-check code (LDPC) \cite{35,36}, which can be functionally defined by a sparse parity-check matrix $H$ of size $(2\lambda dn) \times (2\lambda dn - K)$, where $K$ represents the length of check bits. Bob computes the syndrome $HU$ of his vector (after discretization) and sends the syndrome to Alice. This syndrome can be deemed side information for most of the leakage in error correction. Thus, a parameter $\beta$ called reconciliation efficiency can be used to assess the quality of error correction

$$\beta = \frac{2\lambda dn - \text{leak}_{EC}}{2\lambda n \log_2(1 + SNR)}$$

where $SNR = \eta_{x,p} V_M / (2 + \eta_{x,p} \varepsilon_{x,p})$ stands for signal-to-noise ratio, which is that of the expected Gaussian channel mapping $X$ and $Y$. The value of reconciliation efficiency $\beta$ quantifies the performance of error correction procedure and $\beta = 1$ denotes the perfect reconciliation efficiency. In practice, this parameter can be achieved to about 0.95 for Gaussian channel \cite{36}.

After receiving the side information from Bob, Alice can recover the estimated $\hat{U}$ of $U$ by decoding the code in the coset corresponding to the syndrome $HU$. For a part of the composable security analysis, it is necessary to know whether error correction works, i.e. whether $\hat{U} = U$ or not. As mentioned above, Bob chooses a hash function to map $2\lambda dn$-bit strings to strings of length $\lceil \log(1/\varepsilon_{cor}) \rceil$, and then he sends it to Alice who compares it with her own hash. If both hashes are the identical, the protocol is $\varepsilon_{cor}$-correct \cite{32}.

4.4 Parameter estimation

The goal of parameter estimation is to infer the transmitted quantum state when one has access to a small number outcomes of parameters of the underlying quantum state. It can be deemed a rough version of quantum tomography \cite{37}, which allows us to estimate the covariance matrix of the whole UCVQKD system.

As the protocol goes on, Bob sends $n_{PE}$ bits of $U$ to Alice so that allows her to calculate the estimated values $\omega_a$, $\omega_b$, and $\omega_c$, where

$$\omega_a = \frac{||X||^2}{2\lambda n} \left[ 1 + 2 \sqrt{\frac{\log(36/\varepsilon_{PE})}{n}} \right] - 1,$$

$$\omega_b = \frac{||Y||^2}{2\lambda n} \left[ 1 + 2 \sqrt{\frac{\log(36/\varepsilon_{PE})}{n}} \right] - 1,$$

$$\omega_c = \frac{\langle X,Y \rangle}{2\lambda n} - 5(\frac{||X||^2 + ||Y||^2}{2}) \sqrt{\frac{\log(8/\varepsilon_{PE})}{n^3}}.$$

\textbf{Note: The equation numbers \(17\) and \(18\) are not clearly visible in the image.}
Thanks to the parameter estimation performed after error correction, therefore knows the values of $||X||^2$, $||Y||^2$ and $(X,Y)$ at the end of error correction. Subsequently, she applies a PE test to obtain a confidence region for the covariance matrix of the states $|TMSV\rangle \otimes^{2n}$. If the estimated values are all obey the restraint of $\omega_a \leq \Omega^{\text{max}}_a$ and $\omega_b \leq \Omega^{\text{max}}_b$ and $\omega_c \geq \Omega^{\text{min}}_c$, the protocol continues, otherwise aborts. The failure probability of parameter estimation is denoted by $\epsilon_{\text{PE}}$.

However, for specific the UCVQKD protocol with $\hat{x}$ quadrature modulation, the corresponding coefficients of the covariance matrices of quadrature $\hat{x}$ and quadrature $\hat{p}$ are not identical, and only quadrature $\hat{x}$ carries the useful information. Thus, in order to give the rigorous restraint of composable security analysis for the UCVQKD protocol, one should choose the three apt bounds as

\begin{align}
\Omega^{\text{max}}_a &= \sqrt{V_M + 1} + \delta_a, \\
\Omega^{\text{max}}_b &= 1 + \eta_x (V_M + \epsilon_x) + \delta_b, \\
\Omega^{\text{min}}_c &= (\eta_x V_M \sqrt{V_M + 1})^{\frac{1}{2}} - \delta_c,
\end{align}

where $\delta_a$, $\delta_b$ and $\delta_c$ are small positive constants which are optimized to ensure maximum secret key rate.

### 4.5 Privacy amplification

According to the above-mentioned data processing, Alice and Bob now obtain two strings $\hat{U}$ and $U$, respectively. In order to discard the information known by Eve, Alice chooses an universal hash function and extracts $l$ bits of secret key $S_A$ from $\hat{U}$. Subsequently, Alice informs Bob which function she has chosen and Bob uses it to compute $S_B$.

In this step, the string $U$ can be utilized for generating a key of size $l$ which is $\epsilon_{\text{sec}}$-secret provided that

\begin{equation}
\epsilon_{\text{sec}} = \min \left[ \frac{1}{2} \sqrt{2^l - H_{\text{min}}(U|E')} + 2\epsilon' \right]
\end{equation}

where $E'$ represents all the information that Eve learns from the UCVQKD.

Subsequently, we can calculate the secret key rate of the UCVQKD protocol (See Appendix D for the derivation of secret key rate when taking composable security into account). In Fig. 5 we show the secret key rate of the UCVQKD protocol against collective attacks in the frame of composable security. The brown line shows the maximum transmission distance (about 15 km) of the UCVQKD protocol, leading to the limitation of signal numbers $10^{12}$. As a comparison, we also plot the performance of symmetrically modulated Gaussian GG02 protocol with the transmittance of the quantum channel corresponds to distances of 15 km for losses of 0.2 dB/km. The simulation result, which shows that the UCVQKD protocol is outperformed by GG02 protocol, is meet our expectation and the trend of previous asymptotic
Fig. 5 Secret key rate of the UCVQKD protocol against collective attacks in the frame of composable security, as a function the number of exchanged signals $2n$. The black dashed line denotes 15 km performance of the symmetrically modulated Gaussian GG02 protocol, while the other lines, from top to bottom, represent 10 km (blue line), 12 km (red line), 13 km (green line) and 15 km (brown line) performances of the UCVQKD protocol, respectively. The modulation variance is optimized, reconciliation efficiency is $\beta = 95\%$, the excess noise is $\varepsilon_x = 0.01$, and the discretization parameter is $d = 5$.

5 Conclusion

We have investigated the composable security of the UCVQKD protocol in the asymptotic finite-size regime. We illustrate the relationship of the parameters related to the unmodulated quadrature of the UCVQKD system and estimate the precise secure region with two extreme scenarios. We propose the composable security against collective attacks, and achieve the tightest bound of the UCVQKD protocol. Numerical simulations show the balanced secret key rate of the UCVQKD protocol. Although the key rate of the UCVQKD protocol is slightly low in the case of the composable security analysis, it is can be simply implemented in practice at the low cost.

Acknowledgements We would like to thank V. C. Usenko for the helpful discussions. This work is supported by the National Natural Science Foundation of China (Grant No. 61379153, No. 61572529), and the Fundamental Research Funds for the Central Universities of Central South University (Grant No. 2017zzts147), and partly by China Postdoctoral
References

1. Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dušek, Norbert Lindenhaus, and Moníčka Peov, The security of practical quantum key distribution, Rev. Mod. Phys., 81, 13011350 (2009)
2. Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden, Quantum cryptography, Rev. Mod. Phys., 74, 145-195 (2002)
3. C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, In Proc. IEEE International Conference on Computers Systems and Signal Processing, 175-179 (1984)
4. Jang Young Bang and Micheal S. Berger, Quantum mechanics and the generalized uncertainty principle, Phys. Rev. D, 74, 125012 (2006)
5. Samuel L. Braunstein and Peter van Loock, Quantum information with continuous variables, Rev. Mod. Phys., 77, 513577 (2005)
6. Manuel Gessner, Luca Pozzi, and Augusto Smerzi, Efficient entanglement criteria for discrete, continuous, and hybrid variables, Phys. Rev. A, 94, 020101 (2016)
7. Shuntaro Takeda, Maria Fiwa, Peter van Loock, and Akira Furusawa, Entanglement swapping between discrete and continuous variables, Phys. Rev. Lett, 114, 100501 (2015)
8. Hoi Kwong Lo, Marcos Curty, and Kiyoshi Tamaki, Secure quantum key distribution, Nature Photonics, 8(8), 595604 (2014)
9. Ying Guo, Qin Liao, Yijun Wang, Duan Huang, Peng Huang, and Guihua Zeng, Performance improvement of continuous-variable quantum key distribution with an entangled source in the middle via photon subtraction, Phys. Rev. A, 95, 032304 (2017)
10. Stefano Pirandola, Carlo Ottaviani, Gaetana Spedalieri, Christian Weedbrook, Samuel L. Braunstein, Seth Lloyd, Tobias Gehring, Christian S. Jacobsen, and Ulrik L. Andersen, High-rate measurement-device-independent quantum cryptography, Nature Photonics, 9(6), 397402, (2015)
11. Jian Fang, Peng Huang, and Guihua Zeng, Multichannel parallel continuous-variable quantum key distribution with Gaussian modulation, Phys. Rev. A, 89, 022315 (2014)
12. Xiangchun Ma, Shihai Sun, Musheng Jiang, Ming Gui, and Limmei Liang, Gaussian-modulated coherent-state measurement-device-independent quantum key distribution, Phys. Rev. A, 89, 042335 (2014)
13. Peng Huang, Jian Fang, and Guihua Zeng, State-discrimination attack on discretely modulated continuous-variable quantum key distribution, Phys. Rev. A, 89, 042330 (2014)
14. Andrew M. Lance, Thomas Symul, Vikram Sharma, Christian Weedbrook, Timothy C. Ralph, and Ping Koy Lam, No-switching quantum key distribution using broadband modulated coherent light, Phys. Rev. Lett., 95, 180503 (2005)
15. Raúl García-Pratón and Nicolas J. Cerf, Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution, Phys. Rev. Lett., 97, 190503 (2006)
16. Zhengyu Li, Yichen Zhang, Feihu Xu, Xiang Peng, and Hong Guo, Continuous-variable measurement-device-independent quantum key distribution, Phys. Rev. A, 89, 052301 (2014)
17. Frédéric Grosshans and Philippe Grangier, Continuous variable quantum cryptography using coherent states, Phys. Rev. Lett., 88, 057902 (2002)
18. Vladyslav C. Usenko and Frédéric Grosshans, Unidimensional continuous-variable quantum key distribution, Phys. Rev. A, 92, 062337 (2015)
19. Tobias Gehring, Christian S. Jacobsen, and Ulrik L. Andersen, Single-quadrature continuous-variable quantum key distribution, arXiv:1507.01033 (2015)
20. Anthony Leverrier, Frédéric Grosshans, and Philippe Grangier, Finite-size analysis of a continuous-variable quantum key distribution, Phys. Rev. A, 81, 062343 (2010)
21. Gehring Tobias, Hudchen Vitus, Duhme Jrg, Furrer Fabian, Franz Torsten, Pacher Christoph, Reinhard F Werner, and Schnabel Roman, Implementation of continuous-variable quantum key distribution with composable and one-sided-device-independent security against coherent attacks, Nature Communications, 6, 8795 (2015)
22. Fabian Furrer, Reverse-reconciliation continuous-variable quantum key distribution based on the uncertainty principle, Phys. Rev. A, 90, 042325 (2014)
23. F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, and R. F. Werner, Continuous variable quantum key distribution: Finite-key analysis of composable security against coherent attacks, Phys. Rev. Lett., 109, 100502 (2012)
24. Anthony Leverrier, Composable security proof for continuous-variable quantum key distribution with coherent states, Phys. Rev. Lett., 114, 070501 (2015)
25. Mario Berta, Matthias Christandl, Fabian Furrer, Volkher B. Scholz, and Marco Tomamichel, Continuous variable entropic uncertainty relations in the presence of quantum memory, Journal of Mathematical Physics, 55(12) (2013)
26. Stefano Pirandola, Samuel L. Braunstein, and Seth Lloyd, Characterization of collective Gaussian attacks and security of coherent-state quantum cryptography, Phys. Rev. Lett., 101, 200504 (2008)
27. Fabrizio Furrer and Antonio Acín, Security bounds for continuous variables quantum key distribution, Phys. Rev. Lett., 94, 020505 (2005)
28. Miguel Navascués, Frédéric Grosshans, and Antonio Acín Optimality of Gaussian attacks in continuous-variable quantum cryptography Phys. Rev. Lett., 97, 190502 (2006)
29. Michael M. Wolf, Geza Giedke, and J. Ignacio Cirac, Extremality of Gaussian quantum states, Phys. Rev. Lett., 96, 080502, (2006)
30. Michael A. Nielsen and Isaac L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press (2000)
31. Serafini, A, Paris, MGA, Illuminati, F, and De Siena, S, Quantifying decoherence in continuous variable systems, Journal of Optics B-Quantum and Semicausal Optics, 7(4), R19R36 (2005)
32. Marco Tomamichel, Charles Ci Wen Lim, Nicolas Gisin, and Renato Renner, Tight finite-key analysis for quantum cryptography, Nature Communications, 3, 634 (2012)
33. Matthias Christandl, Robert Koenig, and Renato Renner, Postselection Technique for Quantum Channels with Applications to Quantum Cryptography, Phys. Rev. Lett., 102(2), 020504 (2009)
34. Anthony Leverrier, Romain Alléaume, Joseph Boutros, Gilles Zémor, and Philippe Grangier, Multidimensional reconciliation for a continuous-variable quantum key distribution, Phys. Rev. A, 77, 042325 (2008)
35. R. Konig, U Maurer, and R Renner, On the power of quantum memory, IEEE Transactions on Information Theory, 51(7), 23912401 (2005)
36. C. H Bennett, G Brassard, C Crepeau, and U. M Maurer, Generalized privacy amplification, IEEE Transactions on Information Theory, 41(6), 19151923 (1995)
37. Matthias Christandl and Renato Renner, Reliable quantum state tomography, Phys. Rev. Lett., 109, 120403 (2012)
38. Paul Jouguet, David Elkouss, and Sébastien Kunz-Jacques, High-bit-rate continuous-variable quantum key distribution, Phys. Rev. A, 90, 042329 (2014)
39. Xueqin Jiang, Peng Huang, Duan Huang, Duan Lin, and Guihua Zeng, Secret information reconciliation based on punctured low-density parity-check codes for continuous-variable quantum key distribution, Phys. Rev. A, 95, 022318 (2017)
40. R Konig, U Maurer, and R Renner, On the power of quantum memory, IEEE Transactions on Information Theory, 51(7), 23912401 (2005)
41. C. H Bennett, G Brassard, C Crepeau, and U. M Maurer, Generalized privacy amplification, IEEE Transactions on Information Theory, 41(6), 19151923 (1995)
42. M Tomamichel, C Schaffner, A Smith and R Renner, Leftover hashing against quantum side information, IEEE Transactions on Information Theory, 57(8), 55245535 (2010)

Appendix

Appendix A: Derivation of the covariance matrix

In what follows, we illustrate the derivation of Eq. (6) from Eq. (5). As the states travel through quantum channel with transmittance $\eta_{x,p}$ and excess noise $\epsilon_{x,p}$, we have

$$\gamma_A = \begin{pmatrix} V & 0 \\ 0 & V \end{pmatrix}. \quad (24)$$
\[ \gamma_{B_2} = \begin{pmatrix} \eta_x (V^2 + \chi_x) & 0 \\ 0 & \eta_p (1 + \chi_p) \end{pmatrix}, \]
\[ \sigma_{AB_2} = \begin{pmatrix} \sqrt{\eta_x} V (V^2 - 1) & 0 \\ 0 & -\sqrt{\eta_p (V^2 - 1)} \end{pmatrix}. \]

Substituting \( V_M = V^2 - 1 \) into Eqs. (24-26), we finally obtain the covariance matrix in the presentation modulation variance \( V_M \), namely

\[ \Gamma_{AB_2} = \begin{pmatrix} \sqrt{V_M + 1} & 0 & (\eta_x V_M \sqrt{V_M + 1})^{\frac{1}{2}} & 0 & 0 \\ 0 & \sqrt{V_M + 1} & 0 & -\left(\frac{\eta_p V_M}{V_M + 1}\right)^{\frac{1}{2}} \\ (\eta_x V_M \sqrt{V_M + 1})^{\frac{1}{2}} & 0 & 1 + \eta_x (V_M + \varepsilon_x) & 0 \\ 0 & (\eta_p V_M / V_M + 1)^{\frac{1}{2}} & 0 & 1 + \eta_p \varepsilon_p \end{pmatrix}. \]

Appendix B: Two extreme scenarios

We consider two extreme scenarios, i.e., the maximum excess noise \( \varepsilon_x = 1 \) (Fig. 6) and the maximum transmittance \( \eta_x = 1 \) (Fig. 7).

As shown in Fig. 6, we set the \( \varepsilon_x = 1 \) and a relatively small value of \( \eta_x = 0.01 \), which is almost corresponding to the worst case in CVQKD system. Although the unphysical region expands as parameter \( \varepsilon_x \) increases, even occupies most of the colored regions (including secure region and unphysical region in this case), the secure region still exists in the mazarine blue area,
which means the UCVQKD protocol can still generate positive secret key rate in the worst case scenario. In other word, even in the pessimistic scenario, there still exist a 'secure window' in the UCVQKD protocol that ensures secure communication. On the other hand, Fig. 7 shows the simulation result conditioned

by the parameters $\eta_x = 1$ and $\varepsilon_x = 0.01$. This case, essentially, denotes the approximately best scenario in CVQKD system, because the transmittance is maximum and excess noise is very small. Although the colored region (including secure region and partly unphysical region in this case) is smaller, the accessible maximum secret key rate can be acquired at point (1). Note that the colored scale in this scenario is the largest comparing with other scenarios (including the general scenario in main text), which means the highest asymptotic secret key rate can be achieved in this scenario.

Appendix C: Calculation of the asymptotic secret key rate

We illustrate the calculation of asymptotic secret key rate of UCVQKD with RR. After obtaining the expression of $K_{RR}$ in Eq. (3) and the transformed covariance matrix $\Gamma_{AB2}$ in Eq. (6), the covariance matrix of the state which is conditioned by Bob’s homodyne detection in quadrature $\hat{x}$ is given by

$$\gamma_{A|x_B} = \gamma_A - \sigma_{AB2}^T X \gamma_{B2} X)^{MP} \sigma_{AB2},$$

with $X = \text{diag}(1, 0, 1, 0, ..., 1, 0)$ and $\text{MP}$ being the inverse operation on the range; $\gamma_A$ and $\gamma_{B2}$ are the submatrices of transformed covariance matrix $\Gamma_{AB2}$.
representing each mode A and B individually; $\sigma_{AB^2}$ is the correlation between mode A and B in $\Gamma_{AB^2}$.

One can derive the conditional matrix after Bob’s measurement with

$$
\gamma_{A|x_B} = \begin{pmatrix}
\sqrt{\nu_3 + (1 + \eta_x \epsilon_x)} & 0 \\
\frac{1}{1 + \eta_x \epsilon_x} & \sqrt{\nu_3 + 1}
\end{pmatrix}.
$$

(28)

Thus, Alice and Bob’s mutual information can be estimated by calculating the following equation

$$
I(A : B_2) = \frac{1}{2} \log \frac{V_A}{V_{A|x_B}},
$$

(29)

where $V_A$, which is the variance of mode A, and $V_{A|x_B}$ are easily calculated from the first diagonal elements of the matrices $\gamma_A$ and $\gamma_{A|x_B}$ respectively. Finally we obtain

$$
I(A : B_2) = \frac{1}{2} \log \left( 1 + \frac{\eta_x V_M}{1 + \eta_x \epsilon_x} \right).
$$

(30)

Due to the fact that Eve can provide a purification of Alice and Bobs density matrix, we first achieve $S(E) = S(AB_2)$, which is a function of the symplectic eigenvalues $\nu_{1,2}$ of $\Gamma_{AB_2}$, given by

$$
S(AB_2) = G\left( \frac{\nu_1 - 1}{2} \right) + G\left( \frac{\nu_2 - 1}{2} \right),
$$

(31)

where

$$
G(x) = (x + 1) \log(x + 1) - x \log x
$$

(32)

is the von Neumann entropy and the symplectic eigenvalues $\nu_{1,2}$ are calculated by the square roots of the solutions of equation

$$
\zeta^2 - \Delta \zeta + \det \Gamma_{AB^2} = 0,
$$

(33)

where $\Delta = \det \gamma_A + \det \gamma_B + 2 \det \sigma_{AB^2}$. After Bob performs the projective measurement $x_B$, system $AB_2$ is pure, and hence, we have $S(E|x_B) = S(A|x_B)$, then the conditional von Neumann entropy $S(A|x_B) = G([\nu_3 - 1]/2)$ is a function of the symplectic eigenvalue $\nu_3$ of the covariance matrix $\gamma_{A|x_B}$, which can be calculated from $\nu_3 = \sqrt{\det \gamma_{A|x_B}}$.

Finally we are able to calculate the asymptotic secret key rate $K_{RR}$ of the UCVQKD protocol.

### Appendix D: Secret key rate of the composable security

We, here, detail the generation of secret key rate of UCVQKD provided by the composable security analysis. Before illustrating the calculation, we give a theorem of composable security for UCVQKD [24].
The UCVQKD protocol is $\epsilon$-secure against collective attacks if $\epsilon = 2\epsilon_{sm} + \bar{\epsilon} + \epsilon_{PE}/\epsilon + \epsilon_{cor}/\epsilon + \epsilon_{ent}/\epsilon$ and if the final key length $l$ is chosen such that

$$l \leq 4\lambda n \hat{H}_{MLE}(U) - 2\lambda n F(\Omega_{\text{max}}^a, \Omega_{\text{max}}^b, \Omega_{\text{min}}^c)$$

$$- \text{leak}_{EC} - \Delta_{AEP} - \Delta_{ent} - 2\log \frac{1}{2\epsilon},$$

(34)

where $\hat{H}_{MLE}(U)$ is the empiric entropy of $U$, the Maximum Likelihood Estimator (MLE) for $H(U)$ to be $\hat{H}_{MLE}(U) = -\sum_{i=1}^{2^d} \hat{p}_i \log \hat{p}_i$ with $\hat{p}_i = \frac{\hat{n}_i}{2\lambda n}$ denotes the relative frequency of obtaining the value $i$ and $\hat{n}_i$ is the number of times the variable $U$ takes the value $i$ for $i \in \{1, \ldots, 2^d\}$, and

$$\Delta_{AEP} = \sqrt{2\lambda n(d+1)^2 + \sqrt{32}\lambda n(d+1)} \log_2 \frac{2}{\epsilon_{sm}}$$

$$+ \sqrt{8}\lambda n \log_2 \frac{2}{\epsilon_{sm}} - 4\epsilon_{sm}d,$$

(35)

$$\Delta_{ent} = \log_2 \frac{1}{\epsilon} - \sqrt{8}\lambda n \log^2 (4\lambda n)(\log(2/\epsilon)),$$

(36)

and $F$ is the function computing the Holevo information between Eve and Bob. It is given by

$$F = G(\mu_1 - \frac{1}{2}) + G(\mu_2 - \frac{1}{2}) - G(\mu_3 - \frac{1}{2}),$$

(37)

where $\mu_1$ and $\mu_2$ are the symplectic eigenvalues of the covariance matrix $\Gamma_{AB}$, the variables follow Eq. (20) (21) and (22). $\mu_3 = \Omega_{\text{max}}^a - (\Omega_{\text{min}}^c)^2 / (1 + \Omega_{\text{max}}^b)$, the entropy function $G$ is identical with Eq. (B6). Moreover, the symplectic eigenvalues $\mu_1$ and $\mu_2$ need to satisfy the following relations:

$$\mu_1^2 + \mu_2^2 = \Omega_{\text{max}}^a + \Omega_{\text{max}}^b - 2\Omega_{\text{min}}^c,$$

(38)

$$\mu_1^2 \mu_2^2 = (\Omega_{\text{max}}^a + \Omega_{\text{max}}^b - \Omega_{\text{min}}^c)^2.$$

(39)

Now, let’s consider the calculation of secret key rate provided by UCVQKD composable security analysis. Assuming that the calculation is based on a Gaussian channel with transmissivity $\eta_{x,p}$ and excess noise $\varepsilon_{x,p}$. The following model is used for error correction

$$\beta S(A_x; B_x) = 2\hat{H}_{MLE}(U) - \frac{1}{2\lambda n} \text{leak}_{EC},$$

(40)

where $\beta$ denotes the reconciliation efficiency, and $S(A_x; B_x)$ represents the mutual information between Alice and Bob. For the UCVQKD protocol in Gaussian channel and the modulation variance $V_M$ on quadrature $\hat{x}$, we obtain

$$S(A_x; B_x) = \frac{1}{2} \log_2 (1 + \text{SNR})$$

$$= \frac{1}{2} \log_2 \left(1 + \frac{\eta_x V_M}{2 + \eta_x \varepsilon_x}\right).$$

(41)
Moreover, here, assuming that the probability of passing the parameter estimation step is at least \(0.99\), which means the robustness of the UCVQKD protocol to be \(\epsilon_{\text{rob}} \leq 10^{-2}\). This assumption can be achieved by taking values for \(\Omega_{a}^{\text{max}}\), \(\Omega_{b}^{\text{max}}\), \(\Omega_{c}^{\text{min}}\) differing by 3 standard deviations from the expected values of \(\omega_{a}, \omega_{b}, \omega_{c}\). By doing this, the values of random variables \(||X||^2\), \(||Y||^2\) and \(\langle X, Y \rangle\) satisfy the following restraints

\[
||X||^2 \leq \delta(\delta + 3)\sqrt{V_{M} + 1},
\]

\[
||Y||^2 \leq \delta(\delta + 3)[1 + \eta_{x}(V_{M} + \epsilon_{x})],
\]

\[
\langle X, Y \rangle \geq \delta(\delta - 3)(\eta_{x}V_{M}\sqrt{V_{M} + 1})^{\frac{1}{2}},
\]

where \(\delta = \sqrt{2\lambda n}\). Note that these restraints are obtained from the covariance matrix \(\Gamma_{AB}\) of the UCVQKD protocol with \(\hat{x}\) quadrature modulation and the value of modulation variance \(V_{M}\) must be optimized to obtain the optimal performance. Finally, we use these bounds on Eqs. (42-44) and define:

\[
\Omega_{a}^{\text{max}} = \frac{||X||^2}{2\lambda n} \left[ 1 + 2\sqrt{\frac{\log(36/\epsilon_{PE})}{n}} \right] - 1,
\]

\[
\Omega_{b}^{\text{max}} = \frac{||Y||^2}{2\lambda n} \left[ 1 + 2\sqrt{\frac{\log(36/\epsilon_{PE})}{n}} \right] - 1,
\]

\[
\Omega_{c}^{\text{min}} = \frac{\langle X, Y \rangle}{2\lambda n} - 5(||X||^2 + ||Y||^2)\sqrt{\frac{\log(8/\epsilon_{PE})}{n^3}}.
\]

With all the equations, we now can calculate the secret key rate of the UCVQKD protocol provided by composable security

\[
K_{\text{composable}}^{\hat{x}} = (1 - \epsilon_{\text{rob}})\{\beta S(A_{x}; B_{x}) - F(\Omega_{a}^{\text{max}}, \Omega_{b}^{\text{max}}, \Omega_{c}^{\text{min}}) - \frac{1}{2\lambda n} (\Delta_{AE} + \Delta_{ent} + 2\log_{2} \frac{1}{2\epsilon})\}.
\]

In addition, we should optimize over all parameters compatible with \(\epsilon = 10^{-20}\). However, in order to simplify the description and give a fair comparison, we make the following choices which slightly suboptimal the performance of the UCVQKD protocol and identical with corresponding symmetrically modulated Gaussian coherent-state protocol \[24\]

\[
\epsilon_{\text{sm}} = \tau = 10^{-21}, \epsilon_{\text{PE}} = \epsilon_{\text{cor}} = \epsilon_{\text{ent}} = 10^{-41}.
\]