Finite-size security proof of binary-modulation continuous-variable quantum key distribution using only heterodyne measurement

Shinichiro Yamano, Takaya Matsuura, Yui Kuramochi, Toshihiko Sasaki and Masato Koashi

1 Department of Applied Physics, Graduate School of Engineering, The University of Tokyo, 7-3-1 Hongo Bunkyo-ku, Tokyo 113-8656, Japan
2 Centre for Quantum Computation & Communication Technology, School of Science, RMIT University, Melbourne VIC 3000, Australia
3 Department of Physics, Faculty of Science, Kyushu University, 744 Motooka, Nishi-ku, Fukuoka, Japan
4 Photon Science Center, Graduate School of Engineering, The University of Tokyo, 7-3-1 Hongo, Bunkyo-ku, Tokyo 113-8656, Japan

E-mail: yamano@qi.t.u-tokyo.ac.jp

Keywords: Finite-size security, CV-QKD, discrete modulation, quantum key distribution

Abstract

Continuous-variable quantum key distribution (CV-QKD) has many practical advantages including compatibility with current optical communication technology. Implementation using heterodyne measurements is particularly attractive since it eliminates the need for active phase locking of the remote pair of local oscillators, but the full security of CV QKD with discrete modulation was only proved for a protocol using homodyne measurements. Here we propose an all-heterodyne CV-QKD protocol with binary modulation and prove its security against general attacks in the finite-key regime. Although replacing a homodyne measurement with a heterodyne measurement would be naively expected to incur a 3-dB penalty in the rate-distance curve, our proof achieves a key rate with only a 1-dB penalty.

1. Introduction

Quantum key distribution (QKD) is the technology that enables information-theoretically secure communication between two separate parties. QKD is classified into two categories: discrete-variable (DV) QKD and continuous-variable (CV) QKD. DV-QKD protocols often encode information to a photon in different optical modes such as different polarizations or time bins. They use photon detectors to read out the encoded information. This type has a long history since early studies [1, 2]. A lot of knowledge about the finite-key analysis and how to handle imperfections of actual devices has been accumulated. On the other hand, CV-QKD protocols encode information to quadrature in the phase space of an optical pulse. They use homodyne or heterodyne detection [3, 4], which is highly compatible with the coherent optical communication technology currently widespread in industry [5–14]. See [15, 16] for comprehensive reviews of the topic.

When the receiver (Bob) employs a homodyne measurement, he needs local oscillator (LO) pulses that are phase-locked to Alice’s LO, except for Gaussian-modulation protocols. In a conventional approach named a transmitting LO (TLO) scheme [17], Alice transmits a strong phase-reference pulse along with a signal pulse, and Bob directly uses the strong pulse as a phase-locked LO pulse in the homodyne measurement. This scheme has the drawback of exposing the LO pluses to an eavesdropper (Eve), leading to a serious security loophole [18–22]. It also brings about a technical issue of isolating the weak signal pulse from the strong reference pulse [23]. Although these issues are avoided if Bob uses his own laser as an LO, it then requires real-time feedback schemes such as optical phase-locked loops [24, 25], which will complicate Bob’s receiver and makes it challenging to integrate into conventional communication systems.

On the other hand, in the heterodyne measurement, we can avoid the difficulty in the actual phase locking of Bob’s own LO. In the scheme called local LO (LLO) scheme [26–28], Alice and Bob use their LOs without phase locking in preparation and measurement of signal pulses in the QKD protocol. Separately from the protocol,
they exchange pilot pulses to monitor the phase difference between the two LOs. The heterodyne measurement outputs two quadrature amplitudes that combine to form a complex amplitude. By using the monitored phase difference, Bob can adjust the observed complex amplitude through appropriate rotation [29–32]. In contrast to the reference pulses used in the TLO schemes, we can usually show that the use of the pilot pulses and the rotation of Bob’s outcome in the LLO schemes cause no security risks. Therefore, the heterodyne CV QKD can avoid the issues associated with TLO schemes without a burden of implementing actual phase locking. Note that a similar post-compensation method for Alice’s complex modulation amplitude is possible even in homodyne CV QKD. But this works only when Alice’s encoding uses many states to have rotational symmetry or a good approximation of it. Hence the use of heterodyne measurements is vital for the discrete-modulation CV QKD with a small number of states.

In terms of security analysis, due to difficulty in dealing with continuous observables, the security of CV-QKD was proved only under limited conditions, such as specific attacks [33–36] and asymptotic cases [37–42]. Although full security in the finite-size regime against general attacks has been proven for a Gaussian modulation protocol [43, 44], it does not cover the discretization of modulation required for practical implementation [45–47]. Discrete modulation protocols, especially four-state heterodyne protocols [48, 49], have been studied, but they do not support the finite-size regime. At present, full security proofs are limited to the binary modulation protocol [50] employing both homodyne and heterodyne measurements, which suffers from the aforementioned phase locking issues.

In this paper, we improve the previous protocol [50] and propose a finite-key analysis of a CV-QKD protocol with binary phase modulation that uses only heterodyne measurements. This protocol represents the first example to enjoy the implementation benefits of heterodyne detection with full security proof. Namely, it enables the application of the LLO, eliminating the risk of LO manipulation and notably simplifying the implementation. The heterodyne measurement consists of two homodyne measurements whose inputs are made by splitting the original input into two halves. Due to this apparent 3-dB loss, straightforward application of the security proof in [50] to the all-heterodyne protocol may suffer from a 3-dB penalty in the key rate as a function of distance. We reconstructed the security proof by carefully examining the POVM for heterodyne measurements. It shows that the penalty in the key rate can be suppressed to only about 1 dB. Moreover, it also reveals that the security can be guaranteed even if we simplify the protocol by omitting the random discarding of rounds required in [50].

The article is organized as follows. In section 2, we introduce our protocol with only heterodyne measurements. Section 3 outlines the security proof based on analyzing the statistics of phase errors in a virtual protocol, while we describe the detail of the proof in Methods. Section 4 includes numerical simulations of the key rates as a function of distance. We discuss how our proof mitigates the apparent 3-dB penalty in the key rate in section 5.

2. Protocol

2.1. Proposed protocol

We describe our protocol as follows (see figure 1). In the description, the outcome of the heterodyne measurement is represented by a complex number that is normalized such that its mean coincides with the complex mean amplitude of the input. The definition of the function $\Lambda_{m,r}$ will be given in the next subsection. The binary entropy function is defined by $h(x) = -x \log_2(x) - (1 - x) \log_2(1 - x)$.

![Figure 1.](image-url)
Actual protocol

Alice and Bob predetermine the protocol parameters \([N, \ \epsilon, \ \mu, \ p_{\text{sig}}, \ p_{\text{test}}, \ \beta, \ s, \ s', \ \kappa, \ \gamma, \ m, \ r]\) and acceptance functions \(f_{\text{succ,0}}(x)\) and \(f_{\text{succ,1}}(x)\) which map the real number \(\mathbb{R}\) into the closed interval \([0, 1]\). Here \(N, \ s, \ s'\) are positive integers, \(m\) is a positive odd integer, \(\mu, \ r, \ \beta, \ \epsilon > 0, \ \kappa, \ \gamma \geq 0, \ p_{\text{sig}}, \ p_{\text{test}} \in [0, 1]\), \(p_{\text{sig}} + p_{\text{test}} = 1\), \(f_{\text{succ,1}}(x) = f_{\text{succ,0}}(-x)\), and \(f_{\text{succ,1}}(x) + f_{\text{succ,0}}(x) \leq 1\).

1. Alice randomly chooses a bit \(a \in \{0, 1\}\). She sends an optical pulse \(\hat{C}\) in the coherent state with complex amplitude \((-1)^a \sqrt{\beta}\) to Bob. She repeats it \(N\) times.

2. On each pulse \(C\) of the received \(N\) pulses, Bob performs a heterodyne measurement and obtains an outcome \(\hat{\omega} = \hat{\omega}_R + i\hat{\omega}_I\) \((\hat{\omega}_R, \ \hat{\omega}_I \in \mathbb{R})\).

3. Alice and Bob process the raw data associated with each of the \(N\) transmissions, which we call a round, in the following way. Bob randomly chooses the role of the round and announces it such that a \('signal round'\) is chosen with probability \(p_{\text{sig}}\) and a \('test round'\) with \(p_{\text{test}}\). According to the announced role, Alice and Bob do one of the following procedures.

### [signal]

Bob determines the bit \(b \in \{0, 1\}\) or \('failure'\) according to the real part \(\hat{\omega}_R\) of the measurement outcome, such that the acceptance functions give the probability for each event as follows:

\[
\begin{align*}
\Pr(b = 0) &= f_{\text{succ,0}}(\hat{\omega}_R), \\
\Pr(b = 1) &= f_{\text{succ,1}}(\hat{\omega}_R) = f_{\text{succ,0}}(-\hat{\omega}_R), \\
\Pr(\text{failure}) &= 1 - f_{\text{succ,0}}(\hat{\omega}_R) - f_{\text{succ,1}}(\hat{\omega}_R).
\end{align*}
\]

Bob announces \('success'\) when he obtains the bit \(b \in \{0, 1\}\) and announces \('failure'\) otherwise. If he announces \('failure'\), Alice discards her bit \(a\).

### [test]

Alice announces the bit \(a\) to Bob, and he calculates the value \(\Lambda_{\text{m},a}(\hat{\omega} - (-1)^a \beta)\).

4. The \(N\) rounds are divided into \('signal-success', 'signal-failure'\) and \('test'\) rounds, whose numbers are denoted by \(N_{\text{succ}}\), \(N_{\text{fail}}\) and \(N_{\text{test}}\), respectively. The total number of \('signal'\) rounds is given by \(N_{\text{sig}} = N_{\text{succ}} + N_{\text{fail}}\). Alice and Bob concatenate their own bits kept in the signal-success rounds to define \(N_{\text{succ}}\)-bit sifted keys. Bob calculates the sum of \(\Lambda_{\text{m},a}(\hat{\omega} - (-1)^a \beta)\) in all test rounds, which is denoted by \(\hat{F}\).

5. Alice and Bob perform bit error correction on the sifted keys. They consume \(H_{\text{EC}}\) bits of the pre-shared key for privately transmitting the syndrome of a linear code and \(s'\) bits of that for the verification.

6. Alice and Bob perform privacy amplification on the \(N_{\text{succ}}\)-bit reconciled keys. The length is shortened by \(\hat{N}_{\text{fin}} = (\hat{N}_{\text{succ}} h(\hat{F}) / \hat{N}_{\text{succ}}) + s\), where the function \(h(\hat{F})\) is defined in equation (B14). The final key length, denoted as \(N_{\text{fin}}\), is thus given by

\[
\hat{N}_{\text{fin}} = \hat{N}_{\text{succ}} [1 - h(\hat{F}) / \hat{N}_{\text{succ}}] - s.
\]

In the above protocol, the net key gain per pulse \(\hat{G}\) is expressed as follows

\[
\hat{G} = (\hat{N}_{\text{fin}} - H_{\text{EC}} - s') / N.
\]

The above protocol is feasible even when Alice’s and Bob’s LOs are not phase-locked, as long as one can provide a good guess on their relative phase for each pulse. In such a case, the outcome \(\hat{\omega}\) in Step 2 is determined as follows. First, Bob records the complex amplitude \(\hat{\omega}'\) obtained directly from his heterodyne measurement. Then, using the guess on the relative phase, he appropriately chooses an angle \(\theta\) to define a compensated value \(\hat{\omega} := e^{i\theta} \hat{\omega}'\) such that the real axis of \(\hat{\omega}\) coincides with the direction of Alice’s binary modulation.

As previously noted [26], rotating the output of heterodyne measurement is equivalent to rotating the optical phase of the quantum signal before the measurement. Therefore, replacing the step of measuring \(\hat{\omega}\) in step 2 with the procedure of measuring \(\hat{\omega}'\) and rotating it by \(\theta\) during post-processing is equivalent to Actual protocol.

Although Alice and Bob may exchange strong pilot pulses to obtain a good guess \(\theta\) in the LLO scheme, attacks on the pilot pulses do not threaten its security, which is in stark contrast with attacks on the strong reference pulses in a TLO scheme. An attack on the pilot pulses only changes the guessed value \(\theta\), and due to the equivalence of rotations mentioned above, the effect is reduced to an optical phase shift of the quantum signal just before it reaches Bob’s receiver. That is to say, attacking the pilot pulse is equivalent to a direct attack on the quantum signal, which is already taken into account in any security analysis of the Actual protocol. Hence use of strong pilot pulses in the LLO scheme does not raise any additional security issues [26, 51]. Note that the above reasoning holds for any LLO protocol as long as it uses the information culled from the pilot pulses only for the rotation of the heterodyne outcomes.

2.2. Definition of \(\Lambda_{\text{m},a}\) and its property

The function \(\Lambda_{\text{m},a}\) relates the outcome of the heterodyne measurement to a bound on the fidelity of the input state to a coherent state [50], see also [52]. It is defined as follows:
$\Lambda_{mc}(\mu) := e^{-\mu}(1 + r) L_m^{(1)}(1 + r) \mu$, }

where $L_m^{(1)}$ is the associated Laguerre polynomial

$$L_m^{(1)}(\nu) := (-1)^m \frac{d^m L_m(\nu)}{d\nu^m},$$

and $L_m(\nu)$ is the Laguerre polynomial

$$L_m(\nu) := \frac{\nu^m}{m!} e^{-\nu} (e^{-\nu})^m.$$

For a state $\rho$ of an optical pulse, the heterodyne measurement produces an outcome $\hat{\omega} \in \mathbb{C}$ with a probability measure

$$q_{\rho}(\omega) d^2 \omega := \langle \omega | \rho | \omega \rangle \frac{d^2 \omega}{\pi},$$

where $|\omega\rangle$ is a coherent state

$$|\omega\rangle := e^{-\frac{1}{2} |\omega|^2} \sum_{n=0}^{\infty} \frac{\omega^n}{\sqrt{n!}} |n\rangle.$$

The expectation value of a function $f(\omega)$ based on the probability measure in equation (9) is denoted as $\mathbb{E}_\rho[f(\omega)]$. In [50], it has been shown that a fidelity $\langle \beta | \rho | \beta \rangle$ satisfies the following relation

$$\mathbb{E}_\rho[\Lambda_{mc}(\hat{\omega} - \beta^2)] \leq \text{Tr}(\rho | \beta \rangle \langle \beta |), \quad (m: \text{odd}).$$

### 3. Sketch of the security proof

#### 3.1. Introduction of phase error

The finite-size security of the proposed protocol against general attacks can be shown using the Shor and Preskill approach [53], similar to [50]. This approach connects the amount of the privacy amplification to the so-called phase error rate. Here, we describe the sketch of the security proof. We mainly focus on the intuitive explanation on how we can bound the number of the phase errors, and we also comment on differences between our proof and that of [50]. The full proof is presented in appendix B.

In what follows, we introduce a protocol in which Alice and Bob share pairs of noisy entangled qubits. We then describe its relation to the Actual protocol, and provide a definition to the so-called trash rounds used in [50] to simplify the protocol and the security proof.

We begin by introducing an entanglement-sharing protocol in which Alice and Bob share $N_{\text{succ}}$ pairs of qubits in the signal-success rounds in such a way that measuring those qubits should produce binary sequences equivalent to the sifted keys in Actual protocol.

**Entanglement-sharing protocol**

1. Alice prepares a qubit $A$ and an optical pulse $\tilde{C}$ in the state $|\Psi\rangle_{AC}$ defined as

$$|\Psi\rangle_{AC} = \frac{|0\rangle_A |\sqrt{\mu}\rangle_C + |1\rangle_A |\sqrt{\mu}\rangle_C}{\sqrt{2}},$$

and transmits $\tilde{C}$ to Bob. She repeats this process $N$ times.

2. For each of the $N$ rounds, with the probabilities $p_{\text{sig}}$ and $p_{\text{test}}$, Bob determines whether each round is ‘signal’ or ‘test’ and announces it. Based on this label, Alice and Bob proceed as follows.

   [signal] Bob performs a quantum operation (specified by trace-non-increasing and completely positive map) $F$ on the received optical pulse $C$, where

$$F(\rho) := \int_{\mathbb{C}} d^2 \omega K(\omega, \rho) K^{-1}(\omega),$$

$$K(\omega) := \sqrt{\frac{f_{\text{succ},0}(\omega)}{\pi}} |0\rangle_B \langle \omega|_C + \sqrt{\frac{f_{\text{succ},1}(\omega)}{\pi}} |1\rangle_B \langle -\omega|_C$$

$$= \sqrt{\frac{f_{\text{succ},0}(\omega)}{\pi}} (|0\rangle_B \langle \omega|_C + |1\rangle_B \langle -\omega|_C).$$

This operation heralds ‘success’ or ‘failure’, which Bob announces, and in the former case produces a qubit $B$ in the state $F(\rho)/\text{Tr}[F(\rho)]$. 

---

Note: The above text contains mathematical expressions and definitions that are crucial for understanding the security of the proposed protocol. These expressions are related to quantum mechanics, particularly in the context of quantum key distribution protocols.
[test] Bob performs a heterodyne measurement and obtains an outcome \( \tilde{\omega} = \omega_R + i\omega_I (\omega_R, \omega_I \in \mathbb{R}) \). Alice measures her qubit \( A \) on the Z basis (\( \{ 0 \}, \{ 1 \} \)) and announces the outcome \( a \in \{ 0, 1 \} \) to Bob. He then calculates \( \Lambda_{al}(\omega - (-1)^a\beta) \) as in Actual protocol.

3. Alice and Bob define \( \overset{\text{succ.}}{N} \), \( \overset{\text{fail.}}{N} \), \( \overset{\text{test.}}{N} \), \( \overset{\text{acc.}}{N} \), and \( \overset{\text{hat.}}{\hat{F}} \) as in Actual protocol. At this point, Alice and Bob share \( \overset{\text{acc.}}{N} \) qubits.

This entanglement-sharing protocol can be made equivalent to Actual protocol by measuring the \( \overset{\text{acc.}}{N} \) pairs of qubits left by the protocol on the Z basis. This can be confirmed by the following two observations. First, measuring the qubit \( A \) of the state \( |\Psi\rangle_{AC} \) on the Z basis reproduces the bit \( a \) as well as the state of the optical pulse \( \overset{\text{hat.}}{\hat{C}} \) of Actual protocol. Second, equations (13)-(14) lead to

\[
\langle b | \mathcal{F} (\rho) | b \rangle = \int_{-\infty}^{\infty} dx f_{\text{acc.suc}} (\omega) |\langle \omega | b \rangle|^{2},
\]

which shows that Bob’s procedure of determining the bit \( b \) is equivalent to that in Actual protocol.

Based on this entanglement-sharing protocol, we define the phase error as follows. After Entanglement-sharing protocol, suppose that Alice and Bob measure each of their \( \overset{\text{acc.}}{N} \) qubits on the X basis (\( \{ \pm \} = \{ 0, 1 \} \sqrt{2} \}) instead of the Z basis. Each outcome can be denoted by \( + \) or \( - \). The pair of Alice’s and Bob’s outcomes can thus be written as an element in \( \{(x_a, x_b) | x_a, x_b \in \{ +, - \}\} \). We call the outcomes \((+, -)\) and \((-+, +)\) as a ‘phase error’.

The number of phase errors is denoted by \( N_{\text{ph}} \).

### 3.2. Alternative choice of defining qubit

In the Entanglement-sharing protocol, we introduced a specific quantum operation \( \mathcal{F} \) to define a qubit \( B \) by equations (13) and (14), but this is not a unique choice. In fact, in order to use the Shor-Preskill protocol, the quantum operation \( \mathcal{F} \) can be chosen arbitrarily as long as it satisfies the condition equation (15). It should be emphasized that the choice of \( \mathcal{F} \) also determines the definition of the phase error, and hence it affects the secure key length.

For example, the actual implementation of the heterodyne measurement composed of double homodyne measurements (see figure 1) suggests a straightforward way to define the quantum operation, which we denote by \( \overset{\text{hat.}}{\hat{F}} \), as follows. The real part \( \omega_R \) of the heterodyne outcome is obtained by letting the measured pulse pass through a half beam splitter, performing a homodyne measurement to obtain an outcome \( x \), and rescaling it as \( \omega_R = \sqrt{2} x \). We may then use the qubit reduction of the homodyne measurement used in [50]. Denoting the vacuum state by \( |\text{vac}\rangle \) and the unitary operation for the beam splitter by \( S \), the operation \( \overset{\text{hat.}}{\hat{F}} \) is given by

\[
\overset{\text{hat.}}{\hat{F}} (\rho) = \int_{-\infty}^{\infty} dx \hat{L}(x) \mathcal{E}_{\text{bs}} (\rho) \hat{L}^\dagger (x)
\]

where

\[
\hat{L}(x) = \sqrt{f_{\text{acc.suc}} (\sqrt{2} x)} (|0\rangle \langle x| + |1\rangle \langle -x|)
\]

and

\[
\mathcal{E}_{\text{bs}} (\rho) = \text{Tr}_{Z} [\hat{S} |\text{vac}\rangle \langle \text{vac}| \hat{S}^\dagger].
\]

Here, \( \langle x| \) maps a state vector to the value of its wave function at \( x \). To make a comparison with equations (13) and (14) easier, we will rewrite them by using the coherent state \( \langle \omega | = |\omega_R + i\omega_I\rangle \). Using the relations

\[
\langle x| \omega \rangle = \left( \frac{2}{\pi} \right)^{\frac{1}{4}} \exp \left[ -(x - \omega_R)^2 + 2i\omega_I x - i\omega_R \omega_I \right]
\]

and

\[
S|\alpha\rangle = \left| \frac{\alpha}{\sqrt{2}} - \frac{\beta}{\sqrt{2}} \right| \left| \frac{\alpha}{\sqrt{2}} + \frac{\beta}{\sqrt{2}} \right|,
\]

we are able to express \( \overset{\text{hat.}}{\hat{F}} \) as

\[
\overset{\text{hat.}}{\hat{F}} (\rho) = \int_{\mathbb{C}} d\omega \hat{K} (\omega) \rho \hat{K}^\dagger (\omega)
\]

with

\[
\hat{K} (\omega) = \sqrt{f_{\text{acc.suc}} (\omega_R) / \pi} (|0\rangle b \langle \omega| c + |1\rangle b \langle -\omega| c).\]

Here \( \tilde{\omega} \) is the complex conjugate of \( \omega \). As can be seen from equations (14) and (22), \( \mathcal{F} \) and \( \overset{\text{hat.}}{\hat{F}} \) are different operations. In fact, the operation \( \overset{\text{hat.}}{\hat{F}} \) leads to a lower key rate than \( \mathcal{F} \). For example, the asymptotic key rate for a pure loss channel obtained from \( \overset{\text{hat.}}{\hat{F}} \) coincides with the broken black curve in figure 4 of section 5 below, which is lower than the solid black curve for the rate obtained from \( \mathcal{F} \). An origin of the disadvantage of \( \overset{\text{hat.}}{\hat{F}} \) will be seen in
the partial trace in equation (18), which implies that the halved pulse from the other port of the beam splitter is not used in the analysis. It means that the same key rate would be secure even if the halved pulse were given to Eve, leading to an overestimation of her ability. Our heuristic choice of equation (14) is intended to avoid such an obvious overestimation.

It should also be noted here that the issue of variation is unique to the heterodyne measurement. In the case of homodyne measurement [50], there is essentially no freedom in defining the reduction to a qubit, since the homodyne measurement is an ideal orthogonal measurement. The heterodyne measurement for the real part can be regarded as a noisy version of the homodyne measurement, and there are various ways in treating the noises in the reduction.

3.3. Finite-size bound on phase errors
It is known that if we can find a function $U$ of the data observed in the test rounds that bounds $N_{ph}$ from above, we can derive a sufficient amount of the privacy amplification to achieve the required secrecy of the protocol [54, 55]. In our case, if we can find $U$ that satisfies

$$\Pr[N_{ph} \leq U(\hat{F})] \geq 1 - \epsilon$$

in Entanglement-sharing protocol followed by X-basis measurements on the $\hat{N}^{\text{suc}}$ qubits, it is guaranteed that our protocol is $(\sqrt{2} \sqrt{\epsilon + 2^{-T} + 2^{-T'}})$-secure.

For the construction of $U(\hat{F})$, we regard occurrence of a phase error as an outcome of a generalized measurement on Alice’s qubit $A$ and the optical pulse $C$ that Bob has received. The positive-operator-valued measure (POVM) for this measurement is constructed as follows. Bob’s measurement has three outcomes, $(+,-,\text{failure})$, whose POVM elements are denoted, respectively, by $(M_{+, M_{-}, M_{\text{fail}}})$. The notation of $M_{\text{od}}$ used because the outcomes $+$ and $-$ implies even and odd photon numbers, respectively (see appendix A). The explicit form of the operators can be determined from the relations $\text{Tr}(M_{\text{ev}} |\rho_C|) = +|\mathcal{F}(\rho_C)|+$, $\text{Tr}(M_{\text{od}} |\rho_C|) = -|\mathcal{F}(\rho_C)|-$ and $M_{\text{fail}} = 1_C - M_{\text{ev}} - M_{\text{od}}$. The POVM elements $M_{x_A, x_B}$ of the outcome $(x_A, x_B)$ for Alice’s and Bob’s X-basis measurement is then given by

$$M_{x_A, x_B} = |x_A\rangle \langle x_A| \otimes M_{\text{ev/od}}.$$ (24)

The phase error is then represented by the operator

$$M_{ph} = M_{+, -} + M_{-, +}.$$ (25)

As an intuitive explanation, let us consider an asymptotic limit of $N \rightarrow \infty$, in which Eve’s attack can be fully characterized by the state $\rho_{\text{out,AC}}$ for Alice’s qubit $A$ and the optical pulse $C$ received by Bob, averaged over the $N$ rounds. In this limit, $N_{ph}/N_{\text{out}}$ converges to $\text{Tr}(M_{ph} \rho_{\text{out,AC}})$ and hence finding an upper bound $U(\hat{F})$ in equation (23) amounts to finding an upper bound on $\text{Tr}(M_{ph} \rho_{\text{out,AC}})$.

The state $\rho_{\text{out,AC}}$ is restricted by two conditions about the input states and about the observed data in the test rounds. The first condition comes from the fact that the reduced state of Alice’s qubit $A$ is unaffected by Eve’s attack, implying that $\text{Tr}_{C} \rho_{\text{out,AC}}$ is identical to the reduced state of the initial state $|\Psi⟩_{AC}$ in equation (12). It leads to a constraint written as

$$\text{Tr}_{AC}(\rho_{\text{out,AC}} \Pi^{\text{eg}}) = q_-.$$ (26)

where

$$\Pi^{\text{eg}} := |-⟩ ⟨-|_A \otimes 1_C$$ (27)

and

$$q_- := \text{Tr}(|\Psi⟩ ⟨\Psi|_{AC} \Pi^{\text{eg}})$$

$$= \frac{1}{2} (1 - \langle \sqrt{\mu} - \sqrt{\mu} \rangle)$$

$$= \frac{1}{2} (1 - e^{-2\mu}).$$ (28)

The second condition arises from equation (11):

$$\text{Tr}_{AC}(\rho_{\text{out,AC}} \Pi^{\text{fid}}) \geq E_{\text{out,AC}} [\Lambda_{m,r} (|0⟩ - (−1)^m |β⟩)] \quad (m: \text{odd}),$$ (29)

where

$$\Pi^{\text{fid}} := |0⟩ ⟨0|_A \otimes |β⟩ ⟨β|_C + |1⟩ ⟨1|_A \otimes |−⟩ ⟨−|_C.$$ (30)

We note that the right-hand side of equation (29) corresponds to $\hat{F} / N_{\text{out}}$ in the asymptotic limit.

The analysis in the asymptotic limit now reduces to finding a bound on $\text{Tr}(M_{ph} \rho_{\text{out,AC}})$ under the constraints imposed by equation (27) and equation (29). In appendix A, we derive a family of bounds $B(\kappa, \gamma)$ with
nonnegative parameters $\kappa$ and $\gamma$ satisfying
\[
\text{Tr} [\rho_{AC}(M_{ph} + \kappa \Pi^{\text{fd}} - \gamma \Pi^{\text{sig}})] \leq B(\kappa, \gamma)
\] (31)
for any density operator $\rho_{AC}$. Using $B(\kappa, \gamma)$, an upper bound on the phase error rate in the asymptotic limit is given by
\[
\frac{\hat{N}_{ph}}{N_{\text{sig}}} \leq u(\hat{F}/N_{\text{test}}) := B(\kappa, \gamma) - \kappa / N_{\text{test}} + \gamma q_{\text{th}}.
\] (32)

Next, we consider the finite-key analysis. Based on the asymptotic analysis, we anticipate that the bound $U(\hat{F})$ in equation (23) will be written in the form $U(\hat{F}) = N_{\text{sig}} u(\hat{F}/N_{\text{test}}) + \Delta$, in which the finite-size correction $\Delta$ is to be determined. In order to find $\Delta$ that bounds $\hat{N}_{ph}$ from above under general attacks, we employ Azuma’s inequality [56]. It is applicable to a series of events with general correlations, and can be used to analyze a large deviation of the total sum $\sum_{i=1}^{N} \tilde{d}^{(i)}$ of a series of random variables $\{T^{(i)}\}$ from its expectation if there is a known constraint on the conditional expectation of $T^{(i)}$, where conditioning is made on the events prior to the $i$-th. To apply this inequality to our case, we write $\hat{N}_{ph} = \sum_{i=1}^{N} \tilde{N}_{ph}^{(i)}$ and $\hat{F} = \sum_{i=1}^{N} \tilde{F}^{(i)}$ and seek a constraint on the conditional statistics of random variables $(\tilde{N}_{ph}^{(i)}, \tilde{F}^{(i)})$. A problem here is that the conditional state $\rho_{AC}^{|\xi\rangle \langle\xi|}$ on systems $A$ and $C$ has no guarantee on its reduced state on $A$, and hence does not satisfy
\[
\text{Tr}(\rho_{AC}^{|\xi\rangle \langle\xi|} \Pi^{\text{sig}}) = \beta.
\]
This prevents us from using equation (26) to impose a tight constraint on the statistics of $(\tilde{N}_{ph}^{(i)}, \tilde{F}^{(i)})$.

One way to connect the property of equation (26) to Azuma’s inequality is to add a measurement corresponding to the operator $\Pi^{\text{sig}}$ to the protocol. In [50], the trash round, in which Alice and Bob discard every data, is randomly chosen with a probability $P_{\text{trash}}$ in Actual protocol. This modification allows us to assume that, after Entanglement-sharing protocol, Alice performs measurement $(\Pi^{\text{sig}}, 1 - \Pi^{\text{sig}})$ in the trash round to determine the total number $\tilde{Q}_{\text{ph}}$ of the events corresponding to $\Pi^{\text{sig}}$. Its purpose is to treat the property of equation (26) as that of a measurement outcome. In fact, the expectation of $\tilde{Q}_{\text{ph}}$ is $N_{\text{trash}} q_{\text{th}}$, and its deviation can be easily analyzed. Azuma’s inequality is then used to analyze the large deviation of the three variables, $(\tilde{N}_{ph}^{(i)}, \tilde{F}^{(i)}, \tilde{Q}_{\text{ph}})$, for which the conditional statistics can be directly bounded using equation (31). An obvious drawback in this approach is that it wastes $N_{\text{trash}}$ rounds in Actual protocol and lowers the finite-size key rate.

Here we improve the above approach in such a way that one does not need to waste rounds. Our strategy is based on the observation that the operator $\Pi^{\text{sig}}$ commutes with $M_{ph}$. It means that we can perform the measurement $(\Pi^{\text{sig}}, 1 - \Pi^{\text{sig}})$ at the same time as the measurement of the phase error at the signal round. Thus, we do not have to add the trash rounds to obtain $\tilde{Q}_{\text{ph}}$. Since this structure is in common with [50], the same trick is also applicable to the protocol of [50]. An explicit form of $U(\hat{F})$ and the proof of equation (23) is given in appendix B.

4. Numerical simulation

We conducted simulations of the key rate $G$ for the Gaussian channel characterized by a transmissivity $\eta$ and an excess noise $\xi$. The transmissivity $\eta$ represents the amplitude damping of a coherent state. The excess noise $\xi$ represents an environmental noise generated on Bob’s side, which increases the variance by a factor of $(1 + \xi)$ [57, 58] (see appendix D for the explicit definition). For our simulations, we set $s = 104$, $s' = 51$, and $\epsilon = 2^{-s}$, ensuring that the protocol is $2^{-50}$-secure.

For the predetermined parameters $(m, r)$ of the bounded function $L_{m,r}$, we adopt $(m, r) = (1, 0.4120)$, which leads to $(\max L_{m,r}, \min L_{m,r}) = (2.824, -0.9932)$ as shown in [50]. As for $\beta$ and $f_{\text{acc}}(x)$, we adopt $\beta = \sqrt{\eta_{\text{acc}}}$ and $f_{\text{acc}}(x) = \Theta(x - x_{\text{th}})$, respectively, where $\Theta(x)$ is defined as $\Theta(x) = 1$ for $x \geq 0$ and $\Theta(x) = 0$ for $x < 0$. For each transmissivity $\eta$, we determined two coefficients $(\kappa, \gamma)$ via a convex optimization using the CVXPY 1.0.25 [59, 60] and four parameters $(\mu, P_{\text{sig}}, P_{\text{test}}, x_{\text{th}})$ via the Nelder-Mead in the scipy.optimize library in Python, in order to maximize the key rate.

We present a comparative analysis of the key rate in our proposed protocol with the previous protocol [50], which we refer to as the ‘homodyne protocol’ hereafter, in figure 2. The values of excess noise $\xi$ are assumed to be $0, 10^{-3}, 10^{-2.75}, 10^{-2.5}, 10^{-2.25}$, and $10^{-2.0}$, and we consider $N = 10^{11}$ and the asymptotic limit.

Our protocol can adopt the LLO scheme, but for the purpose of comparing the key rates, we assume the same noise model as the previous study with TLO. As expected, the key rate of our protocol using only the heterodyne measurement is lower than that of the homodyne protocol. We see that if we shift each curve for the homodyne protocol by $-1$ dB, it will be close to the corresponding curve for our protocol, except in the case of $\xi = 0$ and $N \to \infty$. 
5. Discussion

Since our protocol adopts a binary phase modulation, the heterodyne measurement in the signal rounds is utilized solely for measuring the amplitude in one quadrature. This is also seen in equations (1)–(3), where only $\omega_R$ is used, and there is no reference to $\omega_I$. This observation may lead to an alternative way of proving its security as follows.

Although the main motivation for employing the heterodyne measurement is to dispense with the phase locking of the two LOs, for the sake of proving the security, one can assume that Bob uses an LO phase-locked to Alice’s and configure his apparatus in figure 1 such that outcome $\omega_R$ is obtained from the upper-right pair of detectors, while outcome $\omega_I$ is from the lower-left pair. Then, in a signal round, the lower part is redundant, and the measurement of $\omega_R$ is equivalent to a homodyne measurement placed behind a half beam splitter. This suggests that one may just repurpose the security proof and the key length formula of the homodyne protocol \[50\], as it is, to our protocol. In what follows, we argue that it is indeed true in the asymptotic limit but the achievable key rate is much worse than that of the security proof presented in the previous sections.

To examine Eve’s strategy, let us introduce four protocols, summarized in figure 3, by modifying our protocol in stages toward the homodyne protocol of \[50\].
(I) (Our protocol) Bob performs the heterodyne measurement on the received pulse \( C \) for the signal and test. Based on the test results, Alice and Bob confirm that the fidelity of the pulse \( C \) to the coherent state \( |\beta\rangle \) is no smaller than \( F \).

(II) (Equivalent protocol) In the test round, Bob performs the heterodyne measurement on the received pulse \( C \). Based on the test results, Alice and Bob confirm that the fidelity of the pulse \( C \) is no smaller than \( F \). In the signal round, Bob sends the received pulse \( C \) to a 3-dB-pure-loss channel which is out of Eve’s reach. Then he performs the homodyne measurement on the output \( C' \) of the 3-dB-pure-loss channel. As described below, this protocol is equivalent to (I).

(III) (Homodyne protocol with trusted loss channel) The signal round is the same with the protocol (II). In the test round, Bob performs the heterodyne measurement on \( C' \). Based on the results, Alice and Bob confirm that the fidelity of the pulse \( C' \) is no smaller than \( F \).

(IV) (Homodyne protocol with untrusted loss channel) This protocol itself is the same with the protocol (III). In this case, unlike (II) and (III), we assume that Eve can attack the channel from \( C \) to \( C' \).

Protocol (I) is the all-heterodyne protocol proposed in this paper. Protocol (IV) is the case where the homodyne protocol of [50] is carried out on a channel whose transmission is lower by 3 dB. In the following, we compare the above four protocols under the assumption of the same value of the fidelity bound \( F \).

Let us begin by comparing protocols (I) and (II). As explained above, the heterodyne protocol (I) is equivalent to a half beam splitter followed by a homodyne measurement. Since a half beam splitter corresponds to a 3-dB-pure-loss channel, protocol (II) is equivalent to (I).

To analyze protocols (II), (III), and (IV), we introduce a CPTP map \( \mathcal{N}^{C\rightarrow C'} \), which represents the 3-dB-pure-loss channel appearing in protocols (II) and (III), and satisfies the following condition for any coherent state \( |\omega\rangle \):

\[
\mathcal{N}^{C\rightarrow C'}(|\omega\rangle \langle \omega|) = |\omega/\sqrt{2}\rangle \langle \omega/\sqrt{2}|.
\]

(33)

We compare these protocols by considering Eve’s possible attacks in each case, assuming that the same value of the fidelity bound \( F \) was observed in the test. An attack by Eve can be characterized by a CPTP map from \( \tilde{C} \) to \( CE \), where \( E \) means Eve’s system. We denote the allowed sets of maps for the three protocols by \( \mathcal{L}_{II} \), \( \mathcal{L}_{III} \), and \( \mathcal{L}_{IV} \). To simplify the notation, we introduce an abbreviation

\[
\mathcal{E} := (\mathcal{N}^{C\rightarrow C'} \otimes \text{id}_E) \circ \mathcal{E}^{C\rightarrow CE},
\]

(34)

and the density operator for the state of \( \tilde{C} \) prepared by Alice as

\[
\rho_{in}^\tilde{C} = \left[ (-1)^a \sqrt{\eta \mu} \right] \left[ (-1)^a \sqrt{\eta \mu} \right].
\]

(35)

Then, the sets \( \mathcal{L}_{II} \), \( \mathcal{L}_{III} \), and \( \mathcal{L}_{IV} \) can be written as

\[
\mathcal{L}_{II} = \left\{ \tilde{\chi} : \frac{1}{2} \sum_{a=0,1} (-1)^a \sqrt{\eta \mu} \text{Tr}_{E} \mathcal{E}^{C\rightarrow CE}(\rho_{in}^a) \tilde{\chi} \geq F \right\},
\]

(36)
From the monotonicity of the fidelity and equation (33), we find
\[
\langle (-1)^a \sqrt{\eta_\mu} | \text{Tr}_E \hat{\rho}^a_m \rangle \leq \langle (-1)^a \sqrt{\eta_\mu / 2} | \text{Tr}_E \hat{\rho}^a_m \rangle \leq \langle (-1)^a \sqrt{\eta_\mu / 2} | \text{Tr}_E \hat{\rho}^a_m \rangle \leq \langle (-1)^a \sqrt{\eta_\mu / 2} | \text{Tr}_E \hat{\rho}^a_m \rangle \leq \langle (-1)^a \sqrt{\eta_\mu / 2} | \text{Tr}_E \hat{\rho}^a_m \rangle.
\]
It means \( \mathcal{L}_{\text{III}} \subseteq \mathcal{L}_{\text{IV}} \). Since the map \( \hat{\mathcal{E}} \) is a special case of the general CPTP map \( \hat{\mathcal{E}}_{C-E} \), \( \mathcal{L}_{\text{III}} \subseteq \mathcal{L}_{\text{IV}} \) holds. We thus obtain
\[
\mathcal{L}_{\text{II}} \subseteq (\mathcal{L}_{\text{III}} \subseteq (\mathcal{L}_{\text{IV}}). \tag{41}
\]

The above inclusive relation with the equivalence between Protocols (I) and (II) justifies that we are able to repurpose the key rate formula for the homodyne protocol of [50] to achieve a secure key rate for the heterodyne protocol. In figure 4, the key rates from such a repurposed formula are plotted as broken curves. Because of the property of our channel model that the noise characteristics [see equation (D2)] are independent of the channel transmission, those curves are exactly the ones shifted by 3 dB from the rate curves of the homodyne protocol.

On the other hand, as seen in section 4, the key rate obtained from the present security proof (also plotted in figure 4) has only about 1-dB degradation.

Since the removal of trash rounds does not affect the asymptotic key rate, we can ascribe the origin of the key rate difference between the two security proofs shown in figure 4 to two factors deduced from the inclusive relation of equation (41): (i) the repurposed formula assumes the fidelity test at a different point and may fail to fully utilize the observed fidelity bound \( F \) and (ii) the repurposed formula overestimates Eve’s ability as if she could eavesdrop on the fictitious 3-dB loss channel.

In conclusion, we propose a full security proof of the protocol composed solely of heterodyne measurement. Our protocol enables the use of LLO to solve the security issues associated with the attacks on the strong reference pulses in the TLO schemes. It also eliminates the need for the phase locking of the LOs employed by the sender and the receiver. It thus makes its implementation easier and enhances the practical advantages of the CV-QKD protocol. In comparison with the homodyne protocol [50] under the same level of noises, our all-heterodyne protocol suffers only 1-dB penalty in the rate-distance curve. This is much better than the naive expectation based on the fact that a heterodyne detection in one quadrature is equivalent to a homodyne measurement with a 3-dB loss. In addition, we improved the proof technique to remove the ‘trash rounds’ required in the previous protocol, which also simplifies the actual procedures in the protocol.

One issue with this study is that our protocol has the serious limitation of distance when compared to the four-state protocol [48, 49]. These four-state protocols employ heterodyne measurement for signal acquisition,
which is also common in the proposed protocol. We leave it for future work to extend binary modulation to four-state modulation to achieve an improved performance.

**Acknowledgments**

This work was supported by the Ministry of Internal Affairs and Communications (MIC), ‘R&D of ICT Priority Technology Project (JP M1 00 316); Cross-ministerial Strategic Innovation Promotion Program (SIP) (Council for Science, Technology and Innovation (CSTI)); CREST(Japan Science and Technology Agency) JPMJCR1671; JSPS Grants-in-Aid for Scientific Research No. JP22K13977; JST Moonshot R&D, Grant Number JPMJMS2061; JSPS KAKENHI Grant Number JP18K13469; JSPS Overseas Research Fellowships.

**Data availability statement**

All data that support the findings of this study are included within the article (and any supplementary files).

**Appendix A. Derivation of operator bound \( B(\kappa, \gamma) \)**

Here we construct a computable bound \( B(\kappa, \gamma) \), which satisfies an operator inequality

\[
M[\kappa, \gamma] := M_{\text{ph}} + \kappa \Pi_{\text{od}} - \gamma \Pi_{\text{ev}} \leq B(\kappa, \gamma)1
\]

for \( \kappa \geq 0 \) and \( \gamma \geq 0 \). Note that equation (A2) implies that

\[
\text{Tr}(M[\kappa, \gamma] \rho_{\text{AC}}) \leq B(\kappa, \gamma)
\]

for any density operator \( \rho_{\text{AC}} \).

We denote by \( \sigma_{\text{sup}}(O) \) the supremum of the spectrum of a bounded self-adjoint operator \( O \). The following lemma is shown in \([50]\).

**Lemma 1.** Let \( \Pi_{\text{ev}} \) be orthogonal projections satisfying \( \Pi_{\text{ev}} \Pi_{\text{od}} = 0 \). Suppose that the rank of \( \Pi_{\text{ev}} \) is no smaller than 2 or infinite. Let \( M_{\text{ev}} \) be self-adjoint operators satisfying \( \Pi_{\text{ev}} M_{\text{ev}} \Pi_{\text{ev}} = M_{\text{ev}} \leq \alpha_{\pm} \Pi_{\text{ev}} \), where \( \alpha_{\pm} \) are real constants. Let \( |\psi\rangle \) be an unnormalized vector satisfying \( (\Pi_{\text{ev}} + x\Pi_{\text{od}})|\psi\rangle = |\psi\rangle \) and \( \Pi_{\text{ev}}|\psi\rangle = 0 \). Define the following quantities with respect to \( |\psi\rangle \):

\[
C_{\pm} := \langle \psi | \Pi_{\text{ev}} | \psi \rangle (>0)
\]

\[
D_{\pm} := C_{\pm}^{-1} \langle \psi | M_{\text{ev}} | \psi \rangle
\]

\[
V_{\pm} := C_{\pm}^{-1} \langle \psi | M_{\text{ev}}^2 | \psi \rangle - D_{\pm}^2.
\]

Then, for any real numbers \( \gamma_{\pm} \), we have

\[
\sigma_{\text{sup}}(M_{\text{ev}} + \gamma_{\pm}) (\gamma_{\pm} - \gamma) \Pi_{\text{ev}} \Pi_{\text{od}} \leq \sigma_{\text{sup}}(M_{\text{od}}),
\]

where \( M_{\text{od}} \) is defined as

\[
M_{\text{od}} := \begin{bmatrix}
\alpha_{+} - \gamma_{+} & \sqrt{V_{+}} & 0 & 0 \\
\sqrt{V_{+}} & C_{+} + D_{+} - \gamma_{+} & \sqrt{C_{+} C_{-}} & 0 \\
0 & \sqrt{C_{+} C_{-}} & C_{-} + D_{-} - \gamma_{-} & \sqrt{V_{-}} \\
0 & 0 & \sqrt{V_{-}} & \alpha_{-} - \gamma_{-}
\end{bmatrix}.
\]

In order to apply this lemma to our case, we first derive an explicit form of \( M_{\text{ev(od)}} \). Let \( \Pi_{\text{ev}} \) (resp. \( \Pi_{\text{od}} \)) be the projection to the subspace with even (resp. odd) photon numbers, i.e., \( \Pi_{\text{ev}} + \Pi_{\text{od}} = 1 \) and \( (\Pi_{\text{ev}} - \Pi_{\text{od}})|\omega\rangle = | - \omega \rangle \). Rewriting equation (14) in the \( X \) basis leads to

\[
K(\omega) = \sqrt{2f_{\text{sc}0}(\omega_{\pm}) \pi} (| + \rangle_{\omega} \langle \omega | \Pi_{\text{ev}} + | - \rangle_{\omega} \langle \omega | \Pi_{\text{od}}).
\]

Then we have

\[
M_{\text{ev(od)}} = \int d^2 \omega K^d(\omega) (| + \rangle \langle + |) + (| - \rangle \langle - |) K(\omega).
\]
\begin{equation}
\frac{2}{\pi} \int_C d^2 \omega f_{\text{sc},\delta}(\omega) \Pi_{\text{ev}(od)}(\omega) \langle \omega | \Pi_{\text{ev}(od)} \rangle.
\end{equation}

We introduce
\begin{align*}
&|\phi_{\text{err}}\rangle := |1\rangle \otimes \Pi_{\text{od}}(\beta) + |0\rangle \otimes \Pi_{\text{ev}}(\beta), \\
&|\phi_{\text{cor}}\rangle := |1\rangle \otimes \Pi_{\text{ev}}(\beta) + |0\rangle \otimes \Pi_{\text{od}}(\beta),
\end{align*}

\begin{align}
M^{\text{err}}(\kappa, \gamma) &:= |1\rangle \langle +1 | \otimes M_{\text{od}} + |1\rangle \langle -1 | \otimes M_{\text{ev}} + \kappa (|\phi_{\text{err}}\rangle \langle \phi_{\text{err}}| - \gamma | -1 \rangle \langle -1 | \otimes \Pi_{\text{ev}},
M^{\text{cor}}(\kappa, \gamma) &:= \kappa (|\phi_{\text{cor}}\rangle \langle \phi_{\text{cor}}| - \gamma |0\rangle \langle 0| -1 \otimes \Pi_{\text{od}}.
\end{align}

Compared with equation (30), we see that the following relation holds:

\begin{equation}
\Pi_{\text{fid}}^\dagger = |\phi_{\text{err}}\rangle \langle \phi_{\text{err}}| + |\phi_{\text{cor}}\rangle \langle \phi_{\text{cor}}|.
\end{equation}

From equations (24), (25), (27), (A1), (A12), (A13), we can then decompose $M(\kappa, \gamma) = M_{\text{ph}} + \kappa \Pi_{\text{fid}} - \gamma \Pi_{\text{sig}}$ into a direct sum as

\begin{equation}
M(\kappa, \gamma) = M^{\text{err}}(\kappa, \gamma) \oplus M^{\text{cor}}(\kappa, \gamma).
\end{equation}

We apply Lemma 1 to $M^{\text{err}}(\kappa, \gamma)$ by choosing
\begin{align}
M_\pm &= |\pm\rangle \langle \pm| \otimes M_{\text{od}(\text{ev})} \\
|\psi\rangle &= \sqrt{\kappa} |\phi_{\text{err}}\rangle \\
\Pi_\pm &= |\pm\rangle \langle \pm| \otimes M_{\text{od}(\text{ev})} \\
\alpha_\pm &= 1 \\
\gamma_+ &= 0, \quad \gamma_- = \gamma.
\end{align}

This leads to

\begin{equation}
\sigma_{\text{sup}}(M^{\text{err}}(\kappa, \gamma)) \leq \sigma_{\text{sup}}(M_{\text{fid}}^{\text{err}}[\kappa, \gamma]),
\end{equation}

where

\begin{equation}
M_{\text{fid}}^{\text{err}}[\kappa, \gamma] := \begin{bmatrix}
1 & \sqrt{V_{\text{od}}} & 0 & 0 \\
\sqrt{V_{\text{ev}}} & \kappa C_{\text{ev}} + D_{\text{od}} & \kappa \sqrt{C_{\text{od}}C_{\text{ev}}} & 0 \\
0 & \kappa \sqrt{C_{\text{od}}C_{\text{ev}}} & \kappa C_{\text{ev}} + D_{\text{ev}} - \gamma & \sqrt{V_{\text{ev}}} \\
0 & 0 & \sqrt{V_{\text{ev}}} & 1 - \gamma
\end{bmatrix}
\end{equation}

with
\begin{align}
C_{\text{ev}} &= \langle \beta | \Pi_{\text{ev}} | \beta \rangle = e^{-|\beta|^2} \cosh |\beta|^2, \\
C_{\text{od}} &= \langle \beta | \Pi_{\text{od}} | \beta \rangle = e^{-|\beta|^2} \sinh |\beta|^2, \\
D_{\text{ev}(\text{od})} &= C_{\text{ev}(\text{od})}^{-1} \langle \beta | M_{\text{ev}(\text{od})} | \beta \rangle, \\
V_{\text{ev}(\text{od})} &= C_{\text{ev}(\text{od})}^{-1} \langle \beta | (M_{\text{ev}(\text{od})})^2 | \beta \rangle - D_{\text{ev}(\text{od})}^2.
\end{align}

Similarly, we apply Lemma 1 to $M^{\text{cor}}(\kappa, \gamma)$ by choosing
\begin{align}
M_\pm &= 0 \\
|\psi\rangle &= \sqrt{\kappa} |\phi_{\text{cor}}\rangle \\
\Pi_\pm &= |\pm\rangle \langle \pm| \otimes M_{\text{od}(\text{ev})} \\
\alpha_\pm &= 0 \\
\gamma_+ &= 0, \quad \gamma_- = \gamma.
\end{align}

This leads to

\begin{equation}
\sigma_{\text{sup}}(M^{\text{cor}}(\kappa, \gamma)) \leq \sigma_{\text{sup}}(M_{\text{fid}}^{\text{cor}}[\kappa, \gamma]),
\end{equation}

where

\begin{equation}
M_{\text{fid}}^{\text{cor}}[\kappa, \gamma] := \begin{bmatrix}
0 & 0 & 0 & 0 \\
0 & \kappa C_{\text{ev}} & \kappa \sqrt{C_{\text{od}}C_{\text{ev}}} & 0 \\
0 & \kappa \sqrt{C_{\text{od}}C_{\text{ev}}} & \kappa C_{\text{ev}} - \gamma & 0 \\
0 & 0 & 0 & -\gamma
\end{bmatrix}
\end{equation}
Next we define one of its block matrices by

\[
M_{2d}^{\text{cor}}[\kappa, \gamma] := \begin{bmatrix} \kappa C_{\text{ev}} & \kappa \sqrt{C_{\text{od}} C_{\text{ev}}} \\ \kappa \sqrt{C_{\text{od}} C_{\text{ev}}} & \kappa C_{\text{od}} - \gamma \end{bmatrix},
\]

which then satisfies

\[
\sigma_{\text{sup}}(M_{2d}^{\text{cor}}[\kappa, \gamma]) = \max \{ \sigma_{\text{sup}}(M_{2d}^{\text{cor}}[\kappa, \gamma]), 0, -\gamma \}.
\]

(A34)

Since \( \gamma, \kappa > 0 \), we have \( \det(M_{2d}^{\text{cor}}[\kappa, \gamma]) = -\gamma \kappa C_{\text{ev}} < 0 \) and hence \( \sigma_{\text{sup}}(M_{2d}^{\text{cor}}[\kappa, \gamma]) > 0 \). We can thus simplify equation (A34) as

\[
\sigma_{\text{sup}}(M_{2d}^{\text{cor}}[\kappa, \gamma]) = \sigma_{\text{sup}}(M_{2d}^{\text{cor}}[\kappa, \gamma]).
\]

(A35)

Then, from equations (A14), (A20), (A31), and (A35), we finally obtain an upper bound \( B(\kappa, \gamma) \) as

\[
B(\kappa, \gamma) = \max(\sigma_{\text{sup}}(M_{2d}^{\text{cor}}[\kappa, \gamma]), \sigma_{\text{sup}}(M_{2d}^{\text{cor}}[\kappa, \gamma])),
\]

(A36)

which satisfies equation (A2).

Appendix B. Detailed security proof

Here, we construct a function \( U \) satisfying equation (23), which determines the final key length through equation (4) and guarantees the security.

For that purpose, we will define a protocol which we call the estimation protocol. It reproduces the statistics of \( (\hat{N}_{\text{ph}}, \hat{F}) \) and is suited to the use of Azuma’s inequality. The main difference from Entanglement-sharing protocol followed by the X-basis measurements is that Alice conducts the X-basis measurement on her qubit \( A \) even when Bob’s measurement outcome is a failure. We thus define the operators for such measurements as

\[
M_{\text{est, fail}} := |x_A\rangle \langle x_A| \otimes M_{\text{fail}}
\]

for \( x_A = +, - \). The protocol is then formally defined as follows.

**Estimation protocol**

1. Alice prepares a qubit \( A \) and an optical pulse \( \hat{C} \) in the state \( |\Psi\rangle_{A\hat{C}} \) defined in equation (12) and sends \( \hat{C} \) to Bob. She repeats it \( N \) times.

2. For each of the \( N \) rounds, with the probabilities \( p_{\text{sig}} \) and \( p_{\text{fail}} \), Bob determines whether each round is ‘signal’ or ‘test’ and announces it. Based on this label, Alice and Bob proceed as follows.

   - **[signal]** Alice and Bob measure their systems and obtain \( (\hat{x}_A, \hat{x}_B) \), where the POVM elements are given by \( \{M_{kA, kB}|k_A \in \{+,-\}, k_B \in \{+,-,\text{fail}\}\} \) as defined in equation (24).

   - **[test]** Alice measures her qubit \( A \) on the Z basis (\( \{|0\rangle, |1\rangle\} \)) to obtain a bit \( \hat{a} \). Bob performs a heterodyne measurement to obtain a complex number \( \hat{\omega} \).

3. For \( i = 1, \ldots, N \), variables \( n_{\text{ph}}^{(i)}, \hat{F}^{(i)}, \hat{Q}^{(i)}, \hat{T}^{(i)} \) are defined according to table 1 by using the outcomes in Step 2 for the \( i \)-th round. Finally, the sum of these variables are defined as

\[
\hat{N}_{\text{ph}} = \sum_{i=1}^{N} n_{\text{ph}}^{(i)},
\]

(B2)

\[
\hat{F} = \sum_{i=1}^{N} \hat{F}^{(i)},
\]

(B3)

\[
\hat{Q} = \sum_{i=1}^{N} \hat{Q}^{(i)},
\]

(B4)

\[
\hat{T} = \sum_{i=1}^{N} \hat{T}^{(i)}.
\]

(B5)

The way to determine \( (\hat{N}_{\text{ph}}, \hat{F}) \) is equivalent to Entanglement-sharing protocol followed by the X-basis measurement. Therefore, if we can show that equation (23) holds true in Estimation protocol, the security of Actual protocol immediately follows.

In contrast to [30], here we defined \( \hat{Q} \) without introducing the trash rounds. It is achieved because \( \hat{Q}^{(i)} \) can be simultaneously measured with \( n_{\text{ph}}^{(i)} \) in Estimation protocol, which can be seen from the commutativity of the corresponding POVMs \( \Pi^{\text{sig}}_A \) and \( M_{\text{ph}} \). Thus, we can dispense with the trash rounds and improve the finite-key performance.

To find an upper bound \( U(\hat{F}) \) satisfying equation (23), we first find an upper bound on the expectation of \( \hat{T}^{(i)} \) for arbitrary state \( \rho_{\text{AC}} \) on Alice’s qubit \( A \) and Bob’s received pulse \( C \). From table 1, we see that \( \hat{T}^{(i)} \) and \( \hat{T} \) are
related to other variables as

$$\hat{T}^{(i)} = \frac{\hat{N}_{ph}^{(i)}}{P_{\text{sig}}} + \frac{\hat{F}^{(i)}}{P_{\text{test}}} - \gamma \frac{\hat{Q}^{(i)}}{P_{\text{sig}}}.$$  \hfill (B6)

$$\hat{T} = \frac{\hat{N}_{ph}}{P_{\text{sig}}} + \frac{\hat{F}}{P_{\text{test}}} - \gamma \frac{\hat{Q}}{P_{\text{sig}}}.$$  \hfill (B7)

For state $\rho_{AC}$ we have

$$\mathbb{E}_{\rho_{AC}}[\hat{N}_{ph}^{(i)}] = P_{\text{sig}} \text{Tr}(M_{ph}\rho_{AC})$$  \hfill (B8)

and

$$\mathbb{E}_{\rho_{AC}}[\hat{Q}^{(i)}] = P_{\text{sig}} \text{Tr}[(M_{\\text{...test}} \rho_{AC})]$$  \hfill (B9)

According to equation (11), the operator $\Pi^{\text{fid}}$ satisfies

$$\mathbb{E}_{\rho_{AC}}[\hat{F}^{(i)}] \leq P_{\text{test}} \text{Tr}(\Pi^{\text{fid}}\rho_{AC}).$$  \hfill (B10)

From the relations equations $\mathbb{1},$ (B6), (B8), (B9) and (B10), we have

$$\mathbb{E}_{\rho_{AC}}[\hat{T}^{(i)}] \leq \text{Tr}[(M_{ph} + \kappa \Pi^{\text{fid}} - \gamma \Pi^{\text{sig}})\rho_{AC}]$$

$$\leq B(\kappa, \gamma)$$  \hfill (B11)

for any state $\rho_{AC}.$ Using this property, we can derive a bound on $\hat{T}$ in the form of

$$\text{Pr}[\hat{T} - NB(\kappa, \gamma) \leq \delta_1(\epsilon/2)] \geq 1 - \frac{\epsilon}{2}$$  \hfill (B12)

by using Azuma’s inequality [56]. The detail is given in the next subsection and $\delta_1(\epsilon)$ is defined in equation (C9).

Since the variables $\{\hat{Q}^{(i)}\}_i$ are outcomes on Alice’s qubits, they are not affected by Eve’s attack. From the initial state (12), we see that they are $N$ independent Bernoulli trials. As a result, $\hat{Q}$ follows the binomial distribution with probability $P_{\text{sig}}q,$ where $q_-$ is defined in equation (28). We may then derive a bound in the form of

$$\text{Pr}[\hat{Q} - N P_{\text{sig}}q_- \leq \delta_2(\epsilon)] \geq 1 - \frac{\epsilon}{2}$$  \hfill (B13)

by using the Chernoff–Hoeffding bounding bound [61]. The detail is given in the next subsection and $\delta_2(\epsilon)$ is defined in equation (C13).

Combining equations (B7), (B12) and (B13), we obtain an explicit form of $U(\hat{F})$ as

$$U(\hat{F}) = -\kappa \frac{P_{\text{sig}}}{P_{\text{test}}} \hat{F} + \gamma \left[ N P_{\text{sig}}q_+ + \delta_2(\zeta) \right] + P_{\text{sig}}\left[ N B(\kappa, \gamma) + \delta_1(\zeta) \right],$$

which satisfies

$$\text{Pr}[\hat{N}_{ph} \leq U(\hat{F})] \geq 1 - \epsilon.$$  \hfill (B15)

This formula refers to equations (28), (A9)–(A11), (A21)–(A25), (A33), (A36), (C7)–(C9) and (C13) for the definitions used in it.
Appendix C. Derivation of finite-size corrections $\delta_1(\varepsilon)$ and $\delta_2(\varepsilon)$

Here we derive explicit forms of $\delta_1(\varepsilon)$ and $\delta_2(\varepsilon)$ appearing in equations (B12) and (B13). For $\delta_1(\varepsilon)$, we utilize Azuma’s inequality [56] in the form of the following proposition:

**Proposition 1. Azuma’s inequality** Suppose that $(X^{(k)}_i)_{k=0,1,\ldots}$ is a martingale and $(\hat{Y}^{(k)}_k)_{k=0,1,\ldots}$ is a predictable process with regard to $(X^{(k)}_i)_{k=0,1,\ldots}$, which satisfies

$$-\hat{Y}^{(k)}_k + \epsilon_{\min} \leq X^{(k)}_i - X^{(k-1)}_i \leq -\hat{Y}^{(k)}_k + \epsilon_{\max}$$

for constants $\epsilon_{\min}$ and $\epsilon_{\max}$. Then for all positive integers $N$ and all positive reals $\delta$,

$$\Pr[X^{(N)}_N - X^{(0)}_0 \geq \delta] \leq \exp\left(-\frac{2\delta^2}{(\epsilon_{\max} - \epsilon_{\min})^2 N}\right).$$

(C1)

(C2)

Here, we say a sequence $(\hat{Y}^{(k)}_k)_{k=1,2,\ldots}$ is a predictable process with respect to a sequence $(X^{(k)}_i)_{k=0,1,\ldots}$ when $\mathbb{E}[\hat{Y}^{(k)}_k | X^{<k}] = \hat{Y}^{(k)}_k$ for all $k \geq 1$, where $X^{<k} := (X^{(0)}_0, X^{(1)}_1, \ldots, X^{(k-1)}_{k-1})$. To apply Azuma’s inequality for $\hat{T}$, we use Doob decomposition of $(T^{(k)}_k)_{k=0,1,\ldots}$, given by

$$\hat{X}^{(0)}_0 = 0,$$

$$\hat{X}^{(k)}_i = \sum_{i=1}^{k} (T^{(i)}_i - \hat{Y}^{(i)}_i), \quad k \geq 1,$$

$$\hat{Y}^{(i)}_i = \mathbb{E}[T^{(i)}_i | \hat{X}^{<i}].$$

This definition guarantees that $(\hat{X}^{(k)}_k)_{k=0,1,\ldots,N}$ is a martingale, and $(\hat{Y}^{(k)}_k)_{k=0,1,\ldots,N}$ is a predictable process. According to table 1, $\hat{T}^{(i)}_i$ satisfies

$$\epsilon_{\min} \leq \hat{T}^{(i)}_i \leq \epsilon_{\max}$$

with

$$\epsilon_{\min} = \min(p_{\text{test}}^{-1} \kappa \min_{\nu \geq 0} \Lambda_{m,r}(\nu), -p_{\text{sig}}^{-1} \gamma),$$

(C7)

$$\epsilon_{\max} = \max(p_{\text{test}}^{-1} \kappa \max_{\nu \geq 0} \Lambda_{m,r}(\nu), p_{\text{sig}}^{-1}),$$

(C8)

and hence this choice fulfills equation (C1). We define

$$\delta_1(\varepsilon) := (\epsilon_{\max} - \epsilon_{\min}) \sqrt{\frac{\ln N}{2 \ln \left(\frac{1}{\varepsilon}\right)}}. \quad (C9)$$

By setting $\delta = \delta_1(\varepsilon/2)$ in Proposition 1, we obtain

$$\Pr\left[\hat{T}[\kappa, \gamma] \leq \sum_{i=1}^{N} \hat{Y}^{(i)}_i + \delta_1(\varepsilon/2)\right] \geq 1 - \frac{\varepsilon}{2}. \quad (C10)$$

Since equations (B11) and (C5) imply $\hat{Y}^{(i)}_i \leq B(\kappa, \gamma)$, we obtain equation (B12).

Next, we derive an explicit form of $\delta_2(\varepsilon)$. Since the sequence of outcomes $\{\hat{Q}^{(i)}_i\}$ obeys the Bernoulli distribution with probability $p_{\text{sig}} q_-$, we can use the Chernoff-Hoeffding bound [61] to obtain

$$\Pr[\hat{Q}_i \geq N p_{\text{sig}} q_- + \delta] \leq \exp\left[-N D\left(p_{\text{sig}} q_- + \frac{\delta}{N} || p_{\text{sig}} q_- \right)\right], \quad (C11)$$

with $0 < \delta < (1 - p_{\text{sig}} q_-) N$, where

$$D(x || y) := x \log \frac{x}{y} + (1 - x) \log \frac{1 - x}{1 - y}$$

is the Kullback-Leibler divergence. We use $\delta_2(\varepsilon) > 0$ as the unique solution for the following equations:

$$\left\{D\left(p_{\text{sig}} q_- + \frac{\delta_2(\varepsilon)}{N} || p_{\text{sig}} q_- \right) = \frac{-\log \varepsilon}{N} \quad (\varepsilon > (p_{\text{sig}} q_-)^N) \right\}$$

$$\delta_2(\varepsilon) = (1 - p_{\text{sig}} q_-) N \quad (\varepsilon \leq (p_{\text{sig}} q_-)^N). \quad (C13)$$

Then, combined with equation (C11), we have

$$\Pr[\hat{Q}_i \leq N p_{\text{sig}} q_- + \delta_2(\varepsilon)] \geq 1 - \varepsilon, \quad (C14)$$

from which equation (B13) follows.
Appendix D. Channel model and simulation

Calculation of the final key length $\hat{N}^{\text{fin}}$ in section 4 was done by assuming a channel model, from which we determined the values of parameters $\hat{N}^{\text{suc}}$, $\hat{F}$, and $H_{\text{EC}}$. We adopted a Gaussian channel as a model, and here we describe its detail.

Our model is characterized by transmissivity $\eta$ and excess noise $\xi$. When Alice sends $|(-1)^m \sqrt{\mu}|$ through this channel, the state $\rho_{\text{model}}^m$ that Bob receives is written as

$$\rho_{\text{model}}^m = \int_C d^2p_\xi \langle (-1)^m \sqrt{\mu} + \gamma | (-1)^m \sqrt{\mu} + \gamma \rangle,$$

(D1)

with

$$p_\xi(\gamma) := \frac{2}{\pi \xi} e^{-\gamma^2/\xi}.$$

(D2)

Under this channel model, the expectation value of $\hat{F}$ is calculated as

$$\mathbb{E}[\hat{F}] = N_{\text{test}} \mathbb{E}[\Lambda_{m,r}(\omega - (-1)^m \sqrt{\mu})^2]$$

$$= \frac{p_{\text{test}} N}{1 + \xi/2} \left[ 1 - (-1)^{m+1} \left( \frac{\xi/2}{1 + r(1 + \xi/2)} \right)^{m+1} \right].$$

(D3)

We used this value as the observed value of $\hat{F}$ in Actual protocol.

For $\hat{N}^{\text{suc}}$, let us define the probability $P^+$ that Alice and Bob succeed in the detection and have the same/different bits in the signal round in Actual protocol. Under our model and the choice of the step function $f_{\text{suc},0}(x) = \Theta(x - x_t)$ in section 4, it can be written as

$$P^+ = \frac{\langle 0|\mathcal{F}(\rho_{\text{model}}^m)|0 \rangle + \langle 1|\mathcal{F}(\rho_{\text{model}}^m)|1 \rangle}{2}$$

(D4)

$$P^- = \frac{\langle 0|\mathcal{F}(\rho_{\text{model}}^m)|0 \rangle + \langle 1|\mathcal{F}(\rho_{\text{model}}^m)|1 \rangle}{2}$$

(D5)

$$P^\pm = \frac{1}{2} \text{erfc} \left( x_{\text{th}} \mp \sqrt{\mu} \right) \sqrt{\frac{2}{2 + \xi}},$$

(D6)

where

$$\text{erfc}(x) := \frac{2}{\sqrt{\pi}} \int_x^\infty dt \ e^{-t^2}.$$

(D7)

With $P^\pm$, we have

$$\mathbb{E}[\hat{N}^{\text{suc}}] = N_{\text{test}} (P^+ + P^-),$$

(D8)

which was used as the value of $\hat{N}^{\text{suc}}$ in the simulation of the key rate.

For the cost $H_{\text{EC}}$ of the error correction, we assume that the efficiency of the error correction is 1.1. It means that $H_{\text{EC}}$ can be given by

$$H_{\text{EC}} = 1.1 \times \hat{N}^{\text{suc}} h(e_{\text{bit}}),$$

(D9)

with

$$e_{\text{bit}} = \frac{P^-}{P^+ + P^-}.$$

(D10)

ORCID iDs

Shinichiro Yamano @ https://orcid.org/0000-0003-3245-5344
Takaya Matsuura @ https://orcid.org/0000-0003-4164-4307
Yui Kuramochi @ https://orcid.org/0000-0003-0512-5446
Toshihiko Sasaki @ https://orcid.org/0000-0003-0745-6791
Masato Koashi @ https://orcid.org/0000-0002-4518-1461
References

[1] Bennett C H and Brassard G 1984 Quantum cryptography: public key distribution and coin tossing Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing 175–9

[2] Bennett C H 1992 Quantum cryptography using any two nonorthogonal states Phys. Rev. Lett. 68 3121

[3] Ralph T C 1999 Continuous variable quantum cryptography Phys. Rev. A 61 010303(R)

[4] Grosshans F and Grangier P 2002 Continuous variable quantum cryptography using coherent states Phys. Rev. Lett. 88 057902

[5] Eriksson T A, Luis R S, Puttnam B J, Rademacher G, Fujisawa M, Awaji Y, Furukawa H, Wada N, Takeoka M and Sasaki M 2020 Wavelength division multiplexing of 194 continuous variable quantum key distribution channels J. Light. Technol. 38 2214

[6] Huang D, Lin D, Wang C, Liu W, Fang S, Peng J, Huang P and Zeng G 2015a Continuous-variable quantum key distribution with 1 mbps secure key rate Opt. Express 23 17511

[7] Kumar R, Qin H and Alleaume R 2015 Coexistence of continuous variable qkd with intense dwdm classical channels New J. Phys. 17 043027

[8] Huang D, Huang P, Li H, Wang T, Zhou Y and Zeng G 2016a Field demonstration of a continuous-variable quantum key distribution network Opt. Lett. 41 3511

[9] Karinou F et al 2017 Experimental evaluation of the impairments on a qkd system in a 20-channel wdm co-existence scheme 2017 IEEE Photonics Society Summer Topical Meeting Series (SUM), (IEEE, 2017) 145–6

[10] Karinou F et al 2018 Toward the integration of cv quantum key distribution in deployed optical networks IEEE Photonics Technol. Lett. 30 650

[11] Eriksson T A, Hirano T, Ono M, Fujisawa M, Namiki R, Yoshino K I, Tajima A, Takeoka M and Sasaki M 2018 Coexistence of continuous variable quantum key distribution and 7 x 12.5 gbit/s classical channels 2018 IEEE Photonics Society Summer Topical Meeting Series (SUM), (IEEE, 2018) 71–2

[12] Eriksson T A et al 2019 Wavelength division multiplexing of continuous variable quantum key distribution and 18.3 bit/s data channels Commun. Phys. 2 1

[13] Zhou J, Feng Y, Shi J and Shi R 2023 Plug-and-play continuous variable measurement-device-independent quantum key distribution Ann. Phys. 355 220614

[14] Zhou J, Huang D and Guo Y 2018 Long-distance continuous-variable quantum key distribution using separable gaussian states Phys. Rev. A 98 042303

[15] Xu F, Ma X, Zhang Q, LHo-K and Pan J-W 2020 Secure quantum key distribution with realistic devices Rev. Mod. Phys. 92 022302

[16] Pirandola S et al 2020 Advances in quantunm cryptography Adv. Opt. Photonics 12 1012

[17] Jouguet P, Kunz-Jacques S, Leverrier A, Grangier P and Diamanti E 2013a Experimental demonstration of long-distance continuous-variable quantum key distribution Nat. Photonics 7 378

[18] Jouguet P, Kunz-Jacques S and Diamanti E 2013b Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution Phys. Rev. A 87 062313

[19] Ma X-C, Sun S-H, Jiang M-S and Liang L-M 2013 Local oscillator fluctuation opens a loophole for eve in practical continuous-variable quantum-key-distribution systems Phys. Rev. A 88 022339

[20] Huang J-Z, Weedbrook C, Yin Z-Q, Wang S, Li H-W, Chen W, Guo G-C and Han Z-F 2013 Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack Phys. Rev. A 87 062329

[21] Huang J-Z, Kunz-Jacques S, Jouguet P, Weedbrook C, Yin Z-Q, Wang S, Chen W, Guo G-C and Han Z-F 2014 Quantum hacking on quantum key distribution using homodyne detection Phys. Rev. A 89 032304

[22] Zhao Y, Zhang Y, Huang Y, Xu B, Yu S and Guo H 2018 Polarization attack on continuous-variable quantum key distribution J. Phys. B 52 015501

[23] Huang D, Huang P, Lin D and Zeng G 2016b Long-distance continuous-variable quantum key distribution by controlling excess noise Sci. Rep. 6 1

[24] Kazovsky L G 1986 Balanced phase-locked loops for optical homodyne receivers: Performance analysis, design considerations, and laser linewidth requirements J. Lightwave Technol. 4 182

[25] Kazovsky L G and Atlas D 1990 A 1230-mm experimental optical phase-locked loop: performance investigation and psk homodyne experiments at 140 mb/s and 2 gb/s J. Lightwave Technol. 8 1411

[26] Qi B, Lougovski P, Poozer R, Grice W and Bobrek M 2013 Generating the local oscillator locally in continuous-variable quantum key distribution Nat. Photonics 7 378

[27] Huang D, Huang P, Lin D and Zeng G 2016c High-speed continuous-variable quantum key distribution with discrete modulation: mathematical model and finite-key analysis Sci. Rep. 10 1

[28] Wang H, Pi Y, Huang W, Li Y, Shao Y, Yang J, Liu J, Zhang C, Zhang Y and Xu B 2020 High-speed gaussian-modulated continuous-variable quantum key distribution with a local laser based on pilot-tone-assisted phase compensation Opt. Express 28 32882

[29] Wang H et al 2022 Sub-gbps key rate four-state continuous-variable quantum key distribution within metropolitan area Commun. Phys. 5 1

[30] Wang T, Huang P, Zhou Y, Liu W and Zeng G 2018 Pilot-multiplexed continuous-variable quantum key distribution with a real local oscillator Phys. Rev. A 97 012310

[31] Shao Y, Wang H, Pi Y, Huang W, Li Y, Liu J, Yang J, Zhang Y and Xu B 2021 Phase noise model for continuous-variable quantum key distribution using a local laser oscillator Phys. Rev. A 104 032608

[32] Papanastasiou P, Ottaviani C and Pirandola S 2017 Finite-size analysis of measurement-device-independent quantum cryptography Phys. Rev. A 96 042332

[33] Papanastasiou P and Pirandola S 2021 Continuous-variable quantum cryptography with discrete alphabets: Composable security under collective gaussian attacks Phys. Rev. Res. 3 013047

[34] Samsonov E, Goncharov R, Gaidash A, Kozubov A, Egorov V and Gleim A 2020 Subcarrier wave continuous variable quantum key distribution with discrete modulation: mathematical model and finite-key analysis Sci. Rep. 10 1

[35] Lupo C and Ouyang Y 2022 Quantum key distribution with nonideal heterodyne detection: Composable security of discrete-modulation continuous-variable protocols PRX Quantum 3 010341

[36] Leverrier A and Grangier P 2009 Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation Phys. Rev. Lett. 102 180504
[38] Zhao Y-B, Heid M, Rigas J and Lütkenhaus N 2009 Asymptotic security of binary modulated continuous-variable quantum key distribution under collective attacks Phys. Rev. A 79 012307
[39] Bridle K and Weedbrook C 2018 Security proof of continuous-variable quantum key distribution using three coherent states Phys. Rev. A 97 022310
[40] Lin J, Upadhyaya T and Lütkenhaus N 2019a Asymptotic security analysis of discrete-modulated continuous-variable quantum key distribution Phys. Rev. X 9 041064
[41] Ghorai S, Grangier P, Diamanti E and Leverrier A 2019 Asymptotic security of continuous-variable quantum key distribution with a discrete modulation Phys. Rev. X 9 021059
[42] Namiki R 2022 Security against collective attacks for a continuous-variable quantum key distribution protocol using homodyne detection and postselection arXiv:2205.11820
[43] Leverrier A, García-Patrón R, Renner R and Cerf N J 2013 Security of continuous-variable quantum key distribution against general attacks Phys. Rev. Lett. 110 030502
[44] Leverrier A 2017 Security of continuous-variable quantum key distribution via a gaussian de finetti reduction Phys. Rev. Lett. 118 200501
[45] Jouguet P, Kunz-Jacques S, Diamanti E and Leverrier A 2012 Analysis of imperfections in practical continuous-variable quantum key distribution Phys. Rev. A 86 032309
[46] Luo C 2020 Towards practical security of continuous-variable quantum key distribution Phys. Rev. A 102 022623
[47] Kaur E, Guha S and Wilde M M 2021 Asymptotic security of discrete-modulation protocols for continuous-variable quantum key distribution Phys. Rev. A 103 012412
[48] Hirano T, Ichikawa T, Matsubara T, Ono M, Oguri Y, Namiki R, Kasai K, Matsumoto R and Tsurumaru T 2017a Implementation of continuous-variable quantum key distribution with discrete modulation Quantum Science and Technology 2024010
[49] Lin J, Upadhyaya T and Lütkenhaus N 2019b Asymptotic security analysis of discrete-modulated continuous-variable quantum key distribution Phys. Rev. X 9 041064
[50] Matsuura T, Maeda K, Sasaki T and Koashi M 2021 Finite-size security of continuous-variable quantum key distribution with digital signal processing Nat. Commun. 12 252
[51] Koashi M 2004 Unconditional security of coherent-state quantum key distribution with a strong phase-reference pulse Phys. Rev. Lett. 93 120501
[52] Chabaud U, Grosshans F, Kashefi E and Markham D 2021 Efficient verification of boson sampling Quantum 5 578
[53] Shor P W and Preskill J 2000 Simple proof of security of the bb84 quantum key distribution protocol Phys. Rev. Lett. 85 441
[54] Hayashi M and Tsurumaru T 2012 Concise and tight security analysis of the Bennett-brassard 1984 protocol with finite key lengths New J. Phys. 14 095014
[55] Koashi M 2009 Simple security proof of quantum key distribution based on complementarity New J. Phys. 11 045018
[56] Raginsky M and Sason I 2013 Concentration of measure inequalities in information theory, communications, and coding Found. Trends Commun. Inf. Theory 10 1
[57] Namiki R and Hirano T 2004 Practical limitation for continuous-variable quantum cryptography using coherent states Phys. Rev. Lett. 92 117901
[58] Hirano T, Ichikawa T, Matsubara T, Ono M, Oguri Y, Namiki R, Kasai K, Matsumoto R and Tsurumaru T 2017b Implementation of continuous-variable quantum key distribution with discrete modulation Quantum Sci. Technol. 2024010
[59] Diamond S and Boyd S 2016 Cvxpy: A python-embedded modeling language for convex optimization J. Mach. Learn. Res. 17 2909
[60] Agrawal A, Verschuuren R, Diamond S and Boyd S 2018 A rewriting system for convex optimization problems J. Control. Decis. 5 42
[61] Hoeffding W 1994 Probability inequalities for sums of bounded random variables The collected works of Wassily Hoeffding (Springer) pp. 409–26