arXiv:2301.03171v3 [quant-ph] 25 Aug 2023

Refined finite-size analysis of binary-modulation continuous-variable quantum key distribution

Takaya Matsuura[1,2], Shinichiro Yamano[1], Yui Kuramochi[3], Toshihiko Sasaki[1,4], and Masato Koashi[1,4]

[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

Recent studies showed the finite-size security of binary-modulation CV-QKD protocols against general attacks. However, they gave poor key-rate scaling against transmission distance. Here, we extend the security proof based on complementarity, which is used in the discrete-variable QKD, to the previously developed binary-modulation CV-QKD protocols with the reverse reconciliation under the finite-size regime and obtain large improvements in the key rates. Notably, the key rate in the asymptotic limit scales linearly against the attenuation rate, which is known to be optimal scaling but is not achieved in previous finite-size analyses. This refined security approach may offer full-fledged security proofs for other discrete-modulation CV-QKD protocols.

1 Introduction

Quantum key distribution (QKD) [1] enables two remote parties to share identical random secret bits that are secure against arbitrary eavesdropping allowed under the law of quantum mechanics. Using the one-time pad [2] with random secret bits shared by the QKD, we can realize the information-theoretic security for bipartite communication. Nowadays, there is increasing interest in implementing QKD in the real world. Among other things, continuous-variable (CV) QKD [3, 4, 5, 6, 7, 8, 9] has the advantages of low-cost implementation and high bit rates at short distances. Furthermore, it is relatively easy to multiplex several QKD channels via wavelength division multiplexing and co-propagate them with the classical telecommunication because homodyne and heterodyne detectors used in CV-QKD protocols do not require a low-temperature environment and have good wavelength selectivity. The (single-)photon detectors used in discrete-variable (DV) QKD, on the other hand, typically require a low-temperature environment for stable operation and a high-quality frequency filter for the wavelength division multiplexing.

The main problem with CV-QKD protocols is the difficulty in establishing a complete security proof. Compared to the DV-QKD protocols, most of which have complete security proofs even in the finite-size regime, almost all the CV-QKD protocols only have asymptotic security proofs [10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20] or security proofs against collective attacks [21, 22, 23, 24, 25, 26, 27]. There are, however, some results for the composable finite-size security against general attacks. One is for the protocol using the two-mode squeezed vacuum state [28, 29, 30], whose security proof is based on the entropic uncertainty relation in the infinite dimensional systems [31]. Unfortunately, this protocol is difficult to implement and has a key-rate that scales poorly as transmission distance grows. Another is for the $U(N)$-symmetric protocol that uses coherent states with their complex amplitudes modulated according to a Gaussian distribution [32, 22, 33].

Takaya Matsuura: takaya.matsuura@rmit.edu.au

The security proof for this type of protocol utilizes the de Finetti reduction theorem [34, 35] to the i.i.d. case. This methodology has proved the security of several $U(N)$-invariant CV-QKD protocols [36, 37]. However, in practice, ideal Gaussian modulation cannot be implemented and should be approximated by a finite number of coherent states. It turns out that an overwhelming number of coherent states is needed to directly approximate the Gaussian ensemble for the security condition to be satisfied [38, 39]. If we try to mitigate the required number, additional assumptions are needed, which makes it difficult to apply in the finite-size regime [15].

The alternative approach [40, 41] is to consider discrete-modulation CV QKD (See also Ref. [42] for recent alternative approach). References [40, 41] show the finite-size security against general attacks for a binary-modulation protocol. It can also take into account the discretization of the signal processing, such as binned homodyne and heterodyne measurements (see also Ref. [43] for this topic). Although it offers such a flexible framework for security proof against general attacks, the obtained key rate has very poor scaling against transmission distance. A possible reason for this bad performance is the fact that its security proof is based on entanglement distillation [44, 45]. It is known that the security proof based on entanglement distillation is too stringent in general for secure key distribution. There are alternative types of security proofs [46, 47, 48] that can be applied to general cases. In particular, for CV-QKD protocols, the security proof based on the reverse reconciliation often provides better performance than that based on the direct reconciliation [10], which may be unattainable by a security proof based on entanglement distillation due to its symmetric nature between the sender and the receiver in the security proof.

Contributions of this paper. In this article, we aim to develop another approach to carry out the finite-size security proof for the discrete-modulation CV QKD against general attacks. The approach should be able to exploit the benefit of the reverse reconciliation. To do it concretely, we develop refined security proofs based on the reverse reconciliation for the binary-modulation CV-QKD protocols proposed in Refs. [40, 41], i.e., the protocol in which the sender Alice performs BPSK-type modulation according to her randomly generated bit and the receiver Bob performs homodyne measurement, heterodyne measurement, and trash randomly [40], or performs heterodyne measurement followed by a random selection of the post-processing of the outcome [41]. We use the same apparatuses and setups as those in Refs. [40, 41] but slightly change the protocols. To refine the security proofs, we use an approach based on complementarity [47, 49] under the reverse reconciliation, which is more general than the one based on entanglement distillation [50] and treats Alice and Bob asymmetrically in the security proof. In these refined security proofs, we have degrees of freedom that did not appear in the previous analyses. By setting these degrees of freedom to be optimal in the pure-loss channel [51], we obtain a significant improvement in the key gain rates; in fact, the asymptotic key rates of the protocols scale linearly with regards to the attenuation rate of the pure-loss channel, which is known to be the optimal scaling for the one-way QKD [51]. This shows that we can exploit the benefit of using the reverse reconciliation in the approach based on complementarity. Although the protocols are still fragile against the excess noise, this approach itself may be a step towards the full-fledged security proofs for discrete-modulation CV QKD.

Organization of this paper. The article is organized as follows. In Section 2, we provide the refined security proofs based on complementarity [47] for protocols that use the same experimental setups as proposed in Refs. [40, 41]. The section is further divided into four parts. The first part 2.1 defines the actual protocols, which are almost the same as the ones in Refs. [40, 41]. The second part 2.2 develops virtual protocols for the complementarity approach [47] and evaluates the necessary amount of privacy amplification through estimation protocols. In the third part 2.3, we derive an explicit form of the phase error operator defined by the virtual procedure of the previous part. In the fourth part 2.4, we finish the finite-size security proof by developing operator inequalities. In Section 3, we numerically demonstrate the improved performance of the protocols with our refined security proof. Finally, in Section 4, we wrap up our article by discussing future works and open problems.

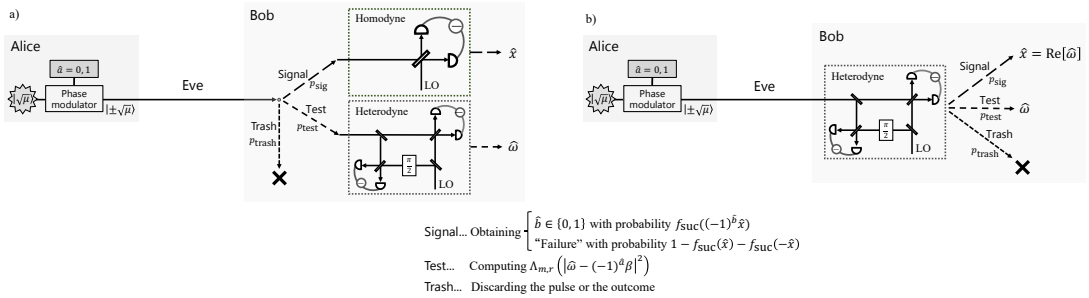


Figure 1: Setups of the protocols. In both protocols, the sender Alice modulates the optical phase of a laser pulse prepared in a coherent state $|\mu\rangle$ with 0 or π according to her random bit $\hat{a} = 0$ or 1. (a) "Homodyne protocol", which is similar to the protocol proposed in Ref. [40]. In this protocol, the receiver Bob randomly switches three types of measurements according to probabilities $p_{\rm sig}$, $p_{\rm test}$, and $p_{\rm trash}$, respectively. In "Signal", Bob performs homodyne measurement and obtains the outcome $\hat{x} \in \mathbb{R}$. Then, he obtains $\hat{b} \in \{0,1\}$ with probability $f_{\rm suc}\big((-1)^{\hat{b}}\hat{x}\big)$, respectively, or announces "Failure" with probability $1 - f_{\rm suc}(\hat{x}) - f_{\rm suc}(-\hat{x})$. In "Test", Bob performs heterodyne measurement and obtains the outcome $\hat{\omega} \in \mathbb{C}$. Then, he computes $\Lambda_{m,r}\big(|\hat{\omega} - (-1)^{\hat{a}}|^2\big)$ with Alice's bit $\hat{a}$ announced. In "Trash", Bob discards the received optical pulse and produces no outcome. (b) "Heterodyne protocol", which is similar to the protocol proposed in Ref. [41]. In this protocol, the receiver Bob performs heterodyne measurement, obtains the outcome $\hat{\omega}$, and randomly switches three types of post-processings according to probabilities $p_{\rm sig}$, $p_{\rm test}$, and $p_{\rm trash}$, respectively. In "Signal", Bob defines $\hat{x} = \Re[\hat{\omega}]$ and follows the same procedure of obtaining the bit $\hat{b}$ or "Failure" as in Homodyne protocol. In "Test", Bob follows the same procedure of computing $\Lambda_{m,r}\big(|\hat{\omega} - (-1)^{\hat{a}}|^2\big)$ as in Homodyne protocol. In "Trash", Bob discards the outcome $\hat{\omega}$.

2 Security proof

In this section, we define two binary-modulation CV-QKD protocols that are closely related to the ones proposed in Refs. [40, 41], and present their security proofs based on the reverse reconciliation. The definition of the (composable) security is the same as that in Ref. [40] and given in Appendix A.

2.1 Definition of the protocol

The setups of the protocols are illustrated in Fig. 1. In the following, a random number is denoted with a hat such as $\hat{\cdot}$. For the places where the slash "/" is used, one can adopt either its left-hand side or right-hand side depending on which of "Homodyne protocol" or "Heterodyne protocol" defined in Fig. 1 one chooses. Note that Homodyne protocol is the same as the protocol proposed in Ref. [40] except for the definition of $f_{\rm suc}(x)$ as well as the way of bit error correction, and Heterodyne protocol is the same as the protocol proposed in Ref. [41] except for the additional trash round as well as the way of bit error correction.

Prior to the protocol, Alice and Bob determine the number N of total rounds, the acceptance probability function $f_{\rm suc}(x)$ ($x \in \mathbb{R}$) of the homodyne/heterodyne measurement satisfying $f_{\rm suc}(x) + f_{\rm suc}(-x) \leq 1$, an odd integer m and a real r for the test function $\Lambda_{m,r}(\nu) := e^{-r\nu}(1+r)L_m^{(1)}((1+r)\nu)$ with $L_m^{(1)}$ being the associated Laguerre polynomial [40], and the protocol parameters $(\mu, p_{\rm sig}, p_{\rm test}, p_{\rm trash}, \beta, s, \kappa, \gamma)$ satisfying $p_{\rm sig} + p_{\rm test} + p_{\rm trash} = 1$ and $\beta < \sqrt{\mu}$, where all the parameters are positive. Alice and Bob then run the protocol described in Box 1, where the outcome $\hat{x} \in \mathbb{R}$ of a homodyne measurement and the outcome $\hat{\omega} \in \mathbb{C}$ of a heterodyne measurement shall be normalized such that their variances are $\langle(\Delta\hat{x})^2\rangle = 1/4$ and $\langle\big(\Delta\Re[\hat{\omega}]\big)^2\rangle = \langle\big(\Delta\Im[\hat{\omega}]\big)^2\rangle = 1/2$ for the vacuum. Unless aborted or $\hat{N}^{\rm suc} = 0$, the protocol generates a shared final key of length

$$\hat{N}^{\rm fin} = \max\left\{\hat{N}^{\rm suc} - \left\lceil \hat{N}^{\rm suc} h\Big(\min\big\{U(\hat{F}, \hat{N}^{\rm trash})/\hat{N}^{\rm suc}, 0.5\big\}\Big)\right\rceil - s, 0\right\}, \tag{1}$$

where $\lceil\cdot\rceil$ is the ceiling function, $h(x)$ is the binary entropy function defined as

$$h(x) := -x\log_2(x) - (1-x)\log_2(1-x), \tag{2}$$

and the function $U(\hat{F}, \hat{N}^{\rm trash})$ will be specified later.

Box 1: Actual protocol

1. For each of the N rounds, Alice generates a random bit $\hat{a} \in \{0,1\}$ and sends an optical pulse $\tilde{C}$ in a coherent state with amplitude $(-1)^{\hat{a}}\sqrt{\mu}$ to Bob. Bob receives an optical pulse C for each round.

2. For the received pulse C in each round, Bob chooses a label from $\{\text{signal}, \text{test}, \text{trash}\}$ with probabilities $p_{\text{sig}}, p_{\text{test}}$, and p_{trash}, respectively, and announces it. According to the label, Alice and Bob do one of the following procedures.

[signal] Bob performs a homodyne/heterodyne measurement on the received optical pulse C and obtains an outcome $\hat{x} \in \mathbb{R}$. (For the heterodyne measurement, $\hat{x}$ is defined as the real part of the outcome $\hat{\omega} \in \mathbb{C}$.) Bob defines a sifted-key bit $\hat{b}$ as $\hat{b} = 0$ with a probability $f_{\text{suc}}(\hat{x})$ and $\hat{b} = 1$ with a probability $f_{\text{suc}}(-\hat{x})$. When Bob has defined his sifted key bit, he announces "success", and otherwise, he announces "failure". In the case of a success, Alice (resp. Bob) records a bit $\hat{a}$ ($\hat{b}$).

[test] Bob performs a heterodyne measurement on the received optical pulse C and obtains an outcome $\hat{\omega}$. Alice announces her bit a. Bob calculates the value of $\Lambda_{m,r}(|\hat{\omega} - (-1)^{\hat{a}}\beta|^2)$.

[trash] Alice and Bob produce no outcomes.

3. We refer to the numbers of "success" and "failure" signal rounds, test rounds, and trash rounds as $\hat{N}^{\text{suc}}, \hat{N}^{\text{fail}}, \hat{N}^{\text{test}}$, and $\hat{N}^{\text{trash}}$, respectively. ($N = \hat{N}^{\text{suc}} + \hat{N}^{\text{fail}} + \hat{N}^{\text{test}} + \hat{N}^{\text{trash}}$ holds by definition.) Bob calculates the sum of $\Lambda_{m,r}(|\hat{\omega} - (-1)^{\hat{a}}\beta|^2)$ obtained in the $\hat{N}^{\text{test}}$ test rounds, which is denoted by $\hat{F}$.

4. For error correction, they use H_{EC}-bits of encrypted communication consuming a pre-shared secret key to do the following. According to (the upper bound on) the bit error rate e_{qber}, Bob randomly chooses an error-correcting code and sends it with the H_{EC}-bits syndrome to Alice. Alice reconciles her sifted key accordingly.

5. Bob computes and announces the final key length $\hat{N}^{\text{fin}}$ according to Eq. (1). Alice and Bob apply privacy amplification to obtain the final key.

For simplicity, we omitted the bit-error-sampling rounds in the above protocol. To satisfy the required correctness ε_{cor} for the final key (see Appendix A), Alice and Bob randomly insert N_{smp} sampling rounds among N rounds in which Bob performs the same measurement as that of the signal round and estimate an upper bound e_{qber} on the bit error rate. Let $\hat{N}^{\text{suc}}_{\text{smp}}$ be the number of "success" in N_{smp} sampling rounds, and let $\hat{E}_{\text{obs}}$ be the number of discrepancies between Alice's and Bob's bits observed in the "success" sampling rounds. Then, Bob sets e_{qber} to

$$e_{\text{qber}} = \left(\tilde{M}_{\hat{N}^{\text{suc}}+\hat{N}^{\text{suc}}_{\text{smp}},\hat{N}^{\text{suc}}_{\text{smp}},\varepsilon_{\text{cor}}/2}(\hat{E}_{\text{obs}}) - \hat{E}_{\text{obs}}\right) \Big/ \hat{N}^{\text{suc}}, \tag{3}$$

where the function $\tilde{M}_{N,n,\epsilon}$ is defined in Eq. (117) in Appendix B.2. The proof that this definition of e_{qber} upper-bounds the actual bit error rate with probability no smaller than $1 - \varepsilon_{\text{cor}}/2$ is also shown in Appendix B.2. The required amount H_{EC} of the error syndrome Bob sends to Alice in the bit error correction depends on the error correction method; here we assume

$$H_{\text{EC}} = \hat{N}^{\text{suc}} \left[f\, h(\min\{e_{\text{qber}}, 0.5\}) + (1 - f) \right], \tag{4}$$

where $f \in [0,1]$ denotes an error correction efficiency [52, 53, 16, 17, 18, 54] for the error correction to succeed with the probability no smaller than $1 - \varepsilon_{\text{cor}}/2$. The net key gain $\hat{G}$ per pulse is thus given by

$$\hat{G} = (\hat{N}^{\text{fin}} - H_{\text{EC}})/(N + N_{\text{smp}}). \tag{5}$$

Here, we do not use verification in the post-processing, unlike Refs. [40, 41], due to the subtleties to incorporate it in our security proof. The acceptance probability $f_{\mathrm{suc}}(x)$ should be chosen to post-select the rounds with larger values of x, for which the bit error probability is expected to be lower. The definition of $f_{\mathrm{suc}}(x)$ in this article follows Ref. [41] and is slightly more general than that of Ref. [40]. (Note that Ref. [40] can also use this definition of $f_{\mathrm{suc}}(x)$.) It is ideally a step function with a threshold $x_{\mathrm{th}}(>0)$, but our security proof applies to any form of $f_{\mathrm{suc}}(x)$. The test function $\Lambda_{m,r}(\nu)$ is the same as the one defined in Ref. [40] where it is shown to satisfy

$$\mathbb{E}_{\rho}[\Lambda_{m,r}(|\hat{\omega}-\beta|^2)] \leq \langle\beta|\,\rho\,|\beta\rangle \tag{6}$$

for any odd integer m, positive real r, and density operator ρ (see Appendix B.1). The parameter β is typically chosen to be $\sqrt{\eta\mu}$ with η being a nominal transmissivity of the quantum channel, while the security proof itself holds for any choice of β. The parameter s is related to the overall security parameter in the security proof below.

2.2 Construction of a virtual protocol and reduction to an estimation protocol

We determine a sufficient amount of the privacy amplification according to the complementarity, or in other words, the phase error correction [47, 49], which has been widely used for the DV-QKD protocols. We aim at showing the secrecy of Bob's final key against the adversary Eve (see Appendix A). To do so, we consider a virtual protocol in which Bob has a qubit for each success signal round such that the outcome of the Z-basis measurement on it is equivalent to his sifted key bit $\hat{b}$. Alice can do arbitrary quantum operations in the virtual protocol as long as all the statistics and available information to the adversary Eve are the same as those in the actual protocol. Then, after Bob's Z-basis measurement on the qubit, the reduced classical-quantum state between Bob and Eve in the virtual protocol is the same as that in the actual protocol.

In the following, we explicitly describe the virtual protocol. For Alice, we introduce a qubit A and assume that she entangles it with an optical pulse $\tilde{C}$ in a state

$$|\Psi\rangle_{A\tilde{C}} \coloneqq \frac{|0\rangle_A\,|\sqrt{\mu}\rangle_{\tilde{C}} + |1\rangle_A\,|-\sqrt{\mu}\rangle_{\tilde{C}}}{\sqrt{2}}, \tag{7}$$

where $|\omega\rangle_{\tilde{C}}$ with $\omega\in\mathbb{C}$ denotes the coherent state with the amplitude ω, which is defined as

$$|\omega\rangle_{\tilde{C}} \coloneqq e^{-\frac{|\omega|^2}{2}} \sum_{n=0}^{\infty} \frac{\omega^n}{\sqrt{n!}}\,|n\rangle_{\tilde{C}}\,. \tag{8}$$

Then, the optical pulse $\tilde{C}$ emitted by Alice is in the same state as that in the actual protocol. For Bob, we construct a process of probabilistically converting the received optical pulse C to a qubit B, which can be regarded as a coherent version of Bob's signal measurement. For Homodyne protocol, consider a map $\mathcal{K}^{\mathrm{hom}}_{C\to B}$ defined as [40]

$$\mathcal{K}^{\mathrm{hom}}_{C\to B}(x)(\rho_C) \coloneqq K^{\mathrm{hom}}_{\mathrm{suc}}(x)\,\rho_C\,\left(K^{\mathrm{hom}}_{\mathrm{suc}}(x)\right)^{\dagger} \tag{9}$$

with

$$K^{\mathrm{hom}}_{\mathrm{suc}}(x) \coloneqq \sqrt{f_{\mathrm{suc}}(x)}\big(|0\rangle_B\langle x|_C + |1\rangle_B\langle -x|_C\big), \tag{10}$$

where $\langle x|$ maps a state vector to the value of its wave function at x; i.e., for a coherent state vector $|\omega\rangle$, $\langle x|$ acts as

$$\langle x|\omega\rangle = \left(\frac{2}{\pi}\right)^{\frac{1}{4}} \exp\left[-(x-\omega_r)^2 + 2i\omega_i x - i\omega_r\omega_i\right], \tag{11}$$

where $\omega=\omega_r+i\omega_i$ with $\omega_r,\omega_i\in\mathbb{R}$. Let $\Pi_{\mathrm{ev(od)}}$ denote a projection operator onto the subspace of even(odd) photon numbers. Since $\langle x|\,(\Pi_{\mathrm{ev}}-\Pi_{\mathrm{od}}) = \langle -x|$ holds, we have

$$K^{\mathrm{hom}}_{\mathrm{suc}}(x) = \sqrt{2f_{\mathrm{suc}}(x)}\big(|+\rangle_B\langle x|_C\,\Pi_{\mathrm{ev}} + |-\rangle_B\langle x|_C\,\Pi_{\mathrm{od}}\big). \tag{12}$$

This defines an instrument $\mathcal{I}^{\mathrm{hom}}_{C\to B}$ for the process of producing the outcome $\hat{x}$ and leaving C in a post-measurement state; i.e., given a measurable set $\Delta \subseteq \mathbb{R}$, the unnormalized post-measurement state is given by

$$\mathcal{I}^{\mathrm{hom}}_{C\to B}(\Delta)(\rho_C) = \int_\Delta dx\, \mathcal{K}^{\mathrm{hom}}_{C\to B}(x)(\rho_C) \tag{13}$$

with $\mathrm{Tr}[\mathcal{I}^{\mathrm{hom}}_{C\to B}(\Delta)(\rho_C)]$ being a probability of "success" signal event with the outcome $\hat{x} \in \Delta$. Similarly, for Heterodyne protocol, consider a map $\mathcal{K}^{\mathrm{het}}_{C\to B}$ defined as [41]

$$\mathcal{K}^{\mathrm{het}}_{C\to B}(\omega)(\rho_C) \coloneqq K^{\mathrm{het}}_{\mathrm{suc}}(\omega)\, \rho_C \big(K^{\mathrm{het}}_{\mathrm{suc}}(\omega)\big)^\dagger \tag{14}$$

with

$$\begin{aligned} K^{\mathrm{het}}_{\mathrm{suc}}(\omega) &\coloneqq \sqrt{\frac{f_{\mathrm{suc}}(\omega_r)}{\pi}} \big(|0\rangle_B\langle\omega|_C + |1\rangle_B\langle -\omega|_C\big) \\ &= \sqrt{\frac{2f_{\mathrm{suc}}(\omega_r)}{\pi}} \left(|+\rangle_B\langle\omega|_C\, \Pi_{\mathrm{ev}} + |-\rangle_B\langle\omega|_C\, \Pi_{\mathrm{od}}\right), \end{aligned} \tag{15}$$

where $|\omega\rangle$ denotes a coherent state vector and $\omega = \omega_r + i\omega_i$ with $\omega_r, \omega_i \in \mathbb{R}$. Similarly to Homodyne protocol, we can define an instrument $\mathcal{I}^{\mathrm{het}}_{C\to B}$ composed of the heterodyne outcome and the (unnormalized) post-measurement state, which is given by

$$\mathcal{I}^{\mathrm{het}}_{C\to B}(\Delta')(\rho_C) = \int_{\Delta'} d\omega_r d\omega_i\, \mathcal{K}^{\mathrm{het}}_{C\to B}(\omega)(\rho_C), \tag{16}$$

where $\Delta' \subseteq \mathbb{R}^2$ is a measurable set. If Bob measures the qubit B in the Z basis after the instrument (13) (resp. (16)), he obtains the same sifted key bit with the same probability as in the actual protocol when $\hat{x} \in \Delta$ (resp. $\hat{\omega} \in \Delta'$) [40, 41].

At this point, one has a degree of freedom to perform quantum operations on the system AB for each outcome $\hat{x}$ (resp. $\hat{\omega}$) as long as it does not change the Z-basis value of the qubit B. This is because we aim at showing the secrecy of Bob's final key against the adversary Eve with Alice's system traced out. Thus, after applying the map $\mathcal{K}^{\mathrm{hom}}_{C\to B}$ (resp. $\mathcal{K}^{\mathrm{het}}_{C\to B}$), we assume that Alice and Bob perform a controlled isometry $V^{\mathrm{hom}}_{B;A\to R}(x)$ (resp. $V^{\mathrm{het}}_{B;A\to R}(\omega)$) of the form

$$V^{\mathrm{hom}}_{B;A\to R}(x) \coloneqq \Big[|0\rangle\langle 0|_B \otimes V^{(0)}_{A\to R}(x) + |1\rangle\langle 1|_B \otimes V^{(1)}_{A\to R}(x)\Big]\, \text{C-}X_{BA} \tag{17}$$

$$V^{\mathrm{het}}_{B;A\to R}(\omega) \coloneqq \Big[|0\rangle\langle 0|_B \otimes V'^{(0)}_{A\to R}(\omega) + |1\rangle\langle 1|_B \otimes V'^{(1)}_{A\to R}(\omega)\Big]\, \text{C-}X_{BA}, \tag{18}$$

where $\text{C-}X_{BA} \coloneqq |0\rangle\langle 0|_B \otimes I_A + |1\rangle\langle 1|_B \otimes X_A$ denotes the Controlled-NOT gate and $V^{(j)}_{A\to R}(x)$ (resp. $V'^{(j)}_{A\to R}(\omega)$) for $j = 0, 1$ denotes an isometry from the system A to another system R that is no smaller than A [1]. If $V^{(j)}_{A\to R}(x)$ (resp. $V'^{(j)}_{A\to R}(\omega)$) is an identity, then the analysis reduces to the previous results [40, 41]. Let $\mathcal{V}^{\mathrm{hom}}_{B;A\to R}(x)$ (resp. $\mathcal{V}^{\mathrm{het}}_{B;A\to R}(\omega)$) be the CPTP map defined as

$$\mathcal{V}^{\mathrm{hom}}_{B;A\to R}(x)(\rho_{AB}) = V^{\mathrm{hom}}_{B;A\to R}(x)\rho_{AB}\big(V^{\mathrm{hom}}_{B;A\to R}(x)\big)^\dagger, \tag{19}$$

$$\mathcal{V}^{\mathrm{het}}_{B;A\to R}(\omega)(\rho_{AB}) = V^{\mathrm{het}}_{B;A\to R}(\omega)\rho_{AB}\big(V^{\mathrm{het}}_{B;A\to R}(\omega)\big)^\dagger. \tag{20}$$

The composition of the map $\mathcal{V}^{\mathrm{hom}}_{B;A\to R}(x)$ and the map (9) (resp. map $\mathcal{V}^{\mathrm{het}}_{B;A\to R}(\omega)$ and the map (14)) with Alice's system traced out at the end defines a quantum operation $\mathcal{F}^{\mathrm{hom}}_{AC\to B}$ (resp. $\mathcal{F}^{\mathrm{het}}_{AC\to B}$) that (probabilistically) outputs Bob's qubits for his sifted key as

$$\mathcal{F}^{\mathrm{hom}}_{AC\to B}(\rho_{AC}) = \int_{-\infty}^{\infty} dx\, \mathcal{K}'^{\mathrm{hom}}_{AC\to B}(x)(\rho_{AC}), \tag{21}$$

$$\mathcal{F}^{\mathrm{het}}_{AC\to B}(\rho_{AC}) = \iint_{-\infty}^{\infty} d\omega_r d\omega_i\, \mathcal{K}'^{\mathrm{het}}_{AC\to B}(x)(\rho_{AC}), \tag{22}$$

[1] Here, a subtlety for using the verification comes in. In order to know whether verification succeeds or not, Alice has to confirm the syndrome bits for the verification. However, this procedure may not commute with the action of $V^{\mathrm{hom}}_{B;A\to R}(x)$ (resp. $V^{\mathrm{het}}_{B;A\to R}(\omega)$). We do not currently have a method to evaluate how much the verification affects the secrecy condition.

with $\mathcal{K}'^{\mathrm{hom}}_{AC\to B}(x)$ (resp. $\mathcal{K}'^{\mathrm{het}}_{AC\to B}(\omega)$) given by

$$\mathcal{K}'^{\mathrm{hom}}_{AC\to B}(x)(\rho_{AC}) \coloneqq \mathrm{Tr}_R\left[\mathcal{V}^{\mathrm{hom}}_{B;A\to R}(x)\circ\left(\mathrm{Id}_A\otimes\mathcal{K}^{\mathrm{hom}}_{C\to B}(x)\right)(\rho_{AC})\right], \tag{23}$$

$$\mathcal{K}'^{\mathrm{het}}_{AC\to B}(\omega)(\rho_{AC}) \coloneqq \mathrm{Tr}_R\left[\mathcal{V}^{\mathrm{het}}_{B;A\to R}(\omega)\circ\left(\mathrm{Id}_A\otimes\mathcal{K}^{\mathrm{het}}_{C\to B}(\omega)\right)(\rho_{AC})\right], \tag{24}$$

where Id denotes the identity map. Note that the idea of acting the isometry $V^{\mathrm{hom}}_{B;A\to R}(x)$ or $V^{\mathrm{het}}_{B;A\to R}(\omega)$ is closely related to the twisting operation on the shield system [55, 56, 57, 58, 59]. The difference is that in our case it acts on the system A in a way that is incompatible with the Z-basis measurement on A. This is allowed in a security proof based on complementarity since what we need to prove in the virtual protocol is that the outcome of the Z-basis measurement on B is secret to Eve when the system A is traced out [47]; i.e., the system A works as a shield system.

We then introduce a virtual protocol that explicitly incorporates the action of $\mathcal{F}^{\mathrm{hom}}_{AC\to B}$ in Eq. (21) (resp. $\mathcal{F}^{\mathrm{het}}_{AC\to B}$ in Eq. (22)) in Box 2.

Box 2: Virtual protocol

1′. For each of the N rounds, Alice prepares a qubit A and an optical pulse $\tilde{C}$ in a state $|\Psi\rangle_{A\tilde{C}}$ defined in (7) and sends the pulse $\tilde{C}$ to Bob. Bob receives an optical pulse C for each round.

2′. For the received pulse C in each round, Bob announces a label in the same way as that at Step 2. Alice and Bob do one of the following procedures according to the label.

[signal] Alice and Bob perform the quantum operation on the system A and the received pulse C specified by the map $\mathcal{F}^{\mathrm{hom}}_{AC\to B}$ defined in Eq. (21) (resp. $\mathcal{F}^{\mathrm{het}}_{AC\to B}$ defined in Eq. (22)) to determine success or failure of detection, obtain the qubit B upon success, and perform the controlled isometry given in Eq. (17) (resp. Eq. (18)). Bob announces the success or failure of the detection.

[test] Bob performs a heterodyne measurement on the received optical pulse C, and obtains an outcome $\hat{\omega}$. Alice measures her qubit A in the Z basis and announces the outcome $\hat{a}\in\{0,1\}$. Bob calculates the value of $\Lambda_{m,r}(|\hat{\omega}-(-1)^{\hat{a}}\beta|^2)$.

[trash] Alice measures her qubit A in the X basis to obtain $\hat{a}'\in\{+,-\}$.

3′. $\hat{N}^{\mathrm{suc}}, \hat{N}^{\mathrm{fail}}, \hat{N}^{\mathrm{test}}, \hat{N}^{\mathrm{trash}}$, and $\hat{F}$ are defined in the same way as those at Step 3. Let $\hat{Q}_-$ be the number of rounds with $\hat{a}'=-$ among the $\hat{N}^{\mathrm{trash}}$ trash rounds.

4′. According to (the upper bound on) the bit error rate e_{qber}, Bob performs H_{EC} bits of encrypted communication consuming a pre-shared secret key to send a dummy message.

5′. Bob computes and announces the final key length $\hat{N}^{\mathrm{fin}}$ according to Eq. (1). Bob performs a randomly chosen unitary on his qubits (see the main text), and measures the first $\hat{N}^{\mathrm{fin}}$ qubits in the Z bases.

In the last line of Step 5′, the random choice of a unitary is constructed so that, along with the subsequent $\hat{N}^{\mathrm{fin}}$-qubit measurement in the Z bases, it is equivalent to the privacy amplification. This is possible because for any $n\times n$ linear transformation C on the n-bit sequence, there always exists a corresponding unitary $U(C)$ that satisfies $U(C)\,|\boldsymbol{z}\rangle = |C\boldsymbol{z}\rangle$ in the Z basis. As has already been claimed, if Eve performs the same attacks as those in the actual protocol, the resulting classical-quantum state between Bob and Eve is the same as that in the actual protocol.

The complementarity argument [47] in a reverse reconciliation scenario relates the amount of privacy amplification to the so-called phase error patterns of Bob's qubits. Suppose that, just before the Z-basis measurement at Step 5′ of the virtual protocol, Bob's quantum state on the first

$\hat{N}^{\rm fin}$ qubits is $\varepsilon_{\rm sc}$-close to $|+\rangle\langle+|^{\otimes \hat{N}^{\rm fin}}$ in terms of the infidelity when averaged over $\hat{N}^{\rm fin}$, where the cases $\hat{N}^{\rm fin}=0$ are regarded to have no infidelity. Then, the secrecy condition of the final key is satisfied with a secrecy parameter $\sqrt{2\varepsilon_{\rm sc}}$ [49, 60, 61]. For this to be true, the errors in the X bases (i.e., the phase errors) on Bob's qubits should be corrected by the procedure at Step 5′ of the virtual protocol with failure probability no larger than $\varepsilon_{\rm sc}$ when averaged over $\hat{N}^{\rm fin}$ ($\hat{N}^{\rm fin}=0$ cases are regarded as no failure). To see the correctability of the phase errors at Step 5′, suppose that Bob measured his $\hat{N}^{\rm suc}$ qubits in the X basis $\{|+\rangle, |-\rangle\}$ at the end of Step 3′, and obtained a sequence of + and −. The minuses in the sequence are regarded as phase errors. It has already been known that, if we can find an upper bound on the number of possible phase-error patterns, then we can prove the security [47, 61]. To make the argument more precise, we introduce an estimation protocol in Box 3.

Box 3: Estimation protocol

1″. For each of the N rounds, Alice prepares a qubit A and an optical pulse $\tilde{C}$ in a state $|\Psi\rangle_{A\tilde{C}}$ defined in (7) and sends the pulse $\tilde{C}$ to Bob. Bob receives an optical pulse C for each round.

2″. For the received pulse C in the ith round ($i=1,\ldots,N$), Bob announces a label in the same way as that at Step 2. Alice and Bob do one of the following procedures according to the label and obtain the values of random variables $\hat{N}_{\rm ph}^{{\rm suc}\,(i)}$, $\hat{F}^{(i)}$, and $\hat{Q}_{-}^{(i)}$. Unless explicitly written, these random variables are set to be zeros.

[signal] Alice and Bob do the same procedure as that at "signal" of Step 2′. Upon "success", Bob performs the X-basis measurement on qubit B and obtains $\hat{b}'\in\{+,-\}$. When $\hat{b}'=-$, $\hat{N}_{\rm ph}^{{\rm suc}\,(i)}$ is set to be unity.

[test] Alice and Bob do the same procedure as that at "test" of Step 2′. Then $\hat{F}^{(i)}$ is set to be $\Lambda_{m,r}(|\hat{\omega}-(-1)^{\hat{a}}\beta|^2)$.

[trash] Alice does the same procedure as that at "trash" of Step 2′. When $\hat{a}'=-$, $\hat{Q}_{-}^{(i)}$ is set to be unity.

3″. Same as Steps 3′ of the virtual protocol. Note that $\hat{F}=\sum_{i=1}^{N}\hat{F}^{(i)}$ and $\hat{Q}_{-}=\sum_{i=1}^{N}\hat{Q}_{-}^{(i)}$ hold.

4″. Regarding + as zero and − as unity for each $\hat{b}'$ in success signal round, define the $\hat{N}^{\rm suc}$-bit sequence $\hat{\boldsymbol{x}}_{\rm ph}$. Let $\hat{N}_{\rm ph}^{\rm suc}$ be the Hamming weight of $\hat{\boldsymbol{x}}_{\rm ph}$, i.e., $\hat{N}_{\rm ph}^{\rm suc}=\sum_{i=1}^{N}\hat{N}_{\rm ph}^{{\rm suc}\,(i)}$.

5″. Bob performs a universal$_2$ hashing on $\hat{\boldsymbol{x}}_{\rm ph}$ and obtains $(\hat{N}^{\rm suc}-\hat{N}^{\rm fin})$-bit syndrome. From this syndrome, Bob estimates the binary string $\hat{\boldsymbol{x}}_{\rm ph}$.

If we could uniquely identify the $\hat{N}^{\rm suc}$-bit sequence $\hat{\boldsymbol{x}}_{\rm ph}$ with failure probability at most $\varepsilon_{\rm sc}$ (when averaged over $\hat{N}^{\rm fin}$ with $\hat{N}^{\rm fin}=0$ cases regarded as no failure), then we could identify the phase errors in the virtual protocol as well and correct them by appropriately acting Pauli-Z operations, and thus the actual protocol can be made $\sqrt{2\varepsilon_{\rm sc}}$-secret. Therefore, the task of proving the security of the actual protocol is now reduced to identifying the $\hat{N}^{\rm suc}$-bit sequence $\hat{\boldsymbol{x}}_{\rm ph}$ with a bounded failure probability (when averaged over $\hat{N}^{\rm fin}$) in the estimation protocol.

We show in the following that the task is further reduced to constructing a function $U(\hat{F},\hat{N}^{\rm trash})$ that satisfies

$$\Pr\left[\hat{N}_{\rm ph}^{\rm suc}>U(\hat{F},\hat{N}^{\rm trash}),\hat{N}^{\rm suc}\geq 1\right]\leq\epsilon \tag{25}$$

for any attack in the estimation protocol, and setting the final key length to $\hat{N}^{\rm fin}=\max\{\hat{N}^{\rm suc}-H_{\rm PA}-s,0\}$, where $H_{\rm PA}$ is defined as

$$H_{\rm PA}:=\left\lceil\hat{N}^{\rm suc}h\Big(\min\big\{U(\hat{F},\hat{N}^{\rm trash})/\hat{N}^{\rm suc},0.5\big\}\Big)\right\rceil. \tag{26}$$

In fact, if the condition (25) is satisfied, then the number of possible patterns of $\hat{\boldsymbol{x}}_{\rm ph}$ can be bounded from above by $2^{H_{\rm PA}}$ [62, 61] except for the failure case with its probability no larger than ϵ. When the number of candidates of $\hat{\boldsymbol{x}}_{\rm ph}$ were restricted to $2^{H_{\rm PA}}$, Bob could uniquely identify $\hat{\boldsymbol{x}}_{\rm ph}$ with failure probability no larger than 2^{-s} by extracting an $(H_{\rm PA}+s)$-bit syndrome from $\hat{\boldsymbol{x}}_{\rm ph}$ using a universal$_2$ hash function [47, 63, 50, 48, 61]. Therefore, using the union bound, the failure probability of identifying $\hat{\boldsymbol{x}}_{\rm ph}$ can be bounded from above by $\epsilon+2^{-s}$ (when averaged over $\hat{N}^{\rm fin}$) if the condition (25) is satisfied and the final key length is set to be $\max\{\hat{N}^{\rm suc}-H_{\rm PA}-s,0\}$ at the end of the estimation protocol.

Finally, we mention that Step 5′ in the virtual protocol realizes a phase error correction. In fact, the $(\hat{N}^{\rm suc}-\hat{N}^{\rm fin})$-bit syndrome extraction in the X bases via the universal$_2$ hash function can be realized through the randomly chosen unitary at Step 5′ in the virtual protocol, and the error recovery in the X bases of the rest $\hat{N}^{\rm fin}$ qubits by the Pauli-Z action leaves Z-basis values of these qubits unchanged and thus irrelevant (due to the successive Z-basis measurement at Step 5′). Since a unitary $U(C^{-1})$ that acts as the matrix C^{-1} in the Z bases acts as $C^{\top}$ in the X bases, i.e., $U(C^{-1})\left|\boldsymbol{x}_X\right\rangle=\left|C^{\top}\boldsymbol{x}_X\right\rangle$ where $\cdot_X$ denotes the X basis, the (random) unitary that acts as the universal$_2$ hashing in the X bases of the last $(\hat{N}^{\rm suc}-\hat{N}^{\rm fin})$ qubits acts as the dual universal$_2$ hashing in the Z bases of the first $\hat{N}^{\rm fin}$ qubits [63, 48] (i.e., in the actual protocol). Thus, we can conclude that the actual protocol is $\sqrt{2}\sqrt{\epsilon+2^{-s}}$-secret once the condition (25) is satisfied in the estimation protocol, the final key length is set as Eq. (1), and the privacy amplification is done by the dual universal$_2$ hashing.

Combining these, the condition (25) implies that the actual protocol with the adaptive final key length given in Eq. (1) is $\varepsilon_{\rm sec}$-secure with a security parameter $\varepsilon_{\rm sec}=\sqrt{2}\sqrt{\epsilon+2^{-s}}+\varepsilon_{\rm cor}$ [47, 49, 60]. From now on, we thus focus on the estimation protocol for finding a function $U(\hat{F},\hat{N}^{\rm trash})$ to satisfy Eq. (25).

2.3 Phase error operator

In this section, we explain how to obtain refined phase error operators that eventually lead to tighter bounds on phase errors than those in Refs. [40, 41]. The phase error operators depend on the choice of the controlled isometry $V^{\rm hom}_{B;A\to R}(x)$ or $V^{\rm het}_{B;A\to R}(\omega)$ in the virtual and the estimation protocol. As we mentioned previously, when the isometries $V^{(0)}_{A\to R}(x)$ and $V^{(1)}_{A\to R}(x)$ in the controlled isometry $V^{\rm hom}_{B;A\to R}(x)$ defined in Eq. (17) satisfy $V^{(0)}_{A\to R}(x)=V^{(1)}_{A\to R}(x)$, the analysis reduces to the previous one [40]. This is because in this case the phase error can be defined as the state $\left|-\right\rangle$ in the X basis of Bob's qubit after acting Controlled-NOT operation from Bob's qubit to Alice's, as can be seen from Eqs. (17), (21), and (23). This is equivalent to observing the discrepancy between the X-basis values of Alice's and Bob's qubits before the action of Controlled-NOT, and thus equivalent to the definition of the phase error in Ref. [40]. The relation between our new analysis for Heterodyne protocol and that in Ref. [41] can be interpreted in the same way. Here in our proposal, we have a degree of freedom to "twist" the Alice's qubit system with these isometries depending on protocol parameters as well as a homodyne (resp. heterodyne) outcome. Unfortunately, finding the optimal choice of these isometries with respect to all protocol parameters and observables in the actual protocol may be intractable. We thus take a suboptimal strategy; fix $V^{\rm hom}_{B;A\to R}(x)$ (resp. $V^{\rm het}_{B;A\to R}(\omega)$) so that the probability of the phase error event $\hat{b}'=-$ in the estimation protocol is minimized for an ideal pure-loss channel [51] with transmission $\eta=\beta^2/\mu$, where β and μ are the positive parameters predetermined in the actual protocol. There are several reasons to do this. One is that the loss is the dominant noise for CV-QKD protocols and thus we prioritize the robustness against it to obtain better performance. Another is that the optimization for the pure-loss channel is much easier since we have an analytical expression of the state when the initial state Eq. (7) in the virtual protocol is subject to the pure-loss channel. In fact, when the state $\left|\Psi\right\rangle_{A\tilde{C}}$ in Eq. (7) is put into a pure-loss channel with the channel output being $\left|\pm\beta\right\rangle_C$, the resulting state $\left|\Phi\right\rangle_{ACE}$ on systems A,C, and an adversary's system E (i.e., an environment of the pure-loss channel) is given by

$$\left|\Phi\right\rangle_{ACE}=\frac{1}{\sqrt{2}}\left(\left|0\right\rangle_A\left|\beta\right\rangle_C\left|\sqrt{\mu-\beta^2}\right\rangle_E+\left|1\right\rangle_A\left|-\beta\right\rangle_C\left|-\sqrt{\mu-\beta^2}\right\rangle_E\right). \tag{27}$$

Tracing out the system E, the reduced state Φ_{AC} is given by

$$\Phi_{AC} = (1-q_{\mu,\beta})\,|\phi_+\rangle\langle\phi_+|_{AC} + q_{\mu,\beta}\,|\phi_-\rangle\langle\phi_-|_{AC}\,, \tag{28}$$

where

$$|\phi_+\rangle_{AC} \coloneqq \frac{1}{\sqrt{2}}(|0\rangle\,|\beta\rangle + |1\rangle\,|-\beta\rangle) = |+\rangle_A \otimes \Pi_{\rm ev}\,|\beta\rangle_C + |-\rangle_A \otimes \Pi_{\rm od}\,|\beta\rangle_C\,, \tag{29}$$

$$|\phi_-\rangle_{AC} \coloneqq \frac{1}{\sqrt{2}}(|0\rangle\,|\beta\rangle - |1\rangle\,|-\beta\rangle) = |+\rangle_A \otimes \Pi_{\rm od}\,|\beta\rangle_C + |-\rangle_A \otimes \Pi_{\rm ev}\,|\beta\rangle_C = (Z_A\otimes I_C)\,|\phi_+\rangle_{AC}\,, \tag{30}$$

and

$$q_{\mu,\beta} \coloneqq \frac{1-e^{-2(\mu-\beta^2)}}{2} (>0). \tag{31}$$

Now we aim at obtaining the optimal choice of $V^{\rm hom}_{B;A\to R}(x)$ (resp. $V^{\rm het}_{B;A\to R}(\omega)$) so that the probability that Bob obtains $\hat{b}'=-$ is minimized for the state Φ_{AC} in Eq. (28). For Homodyne protocol, we observe that

$$\text{C-}X_{BA}\left(\mathrm{Id}_A \otimes \mathcal{K}^{\rm hom}_{C\to B}(x)\right)(\Phi_{AC})\,\text{C-}X_{BA} \tag{32}$$

$$\begin{aligned}&= 2f_{\rm suc}(x)\,\text{C-}X_{BA}\Big[(1-q_{\mu,\beta})\,\hat{P}\big(\langle x|\,\Pi_{\rm ev}\,|\beta\rangle\,|{+}{+}\rangle_{AB} + \langle x|\,\Pi_{\rm od}\,|\beta\rangle\,|{-}{-}\rangle_{AB}\big)\\ &\qquad + q_{\mu,\beta}\,\hat{P}\big(\langle x|\,\Pi_{\rm od}\,|\beta\rangle\,|{+}{-}\rangle_{AB} + \langle x|\,\Pi_{\rm ev}\,|\beta\rangle\,|{-}{+}\rangle_{AB}\big)\Big]\,\text{C-}X_{BA}\end{aligned} \tag{33}$$

$$\begin{aligned}&= 2f_{\rm suc}(x)\Big[(1-q_{\mu,\beta})\,\hat{P}\big(\langle x|\,\Pi_{\rm ev}\,|\beta\rangle\,|+\rangle_A + \langle x|\,\Pi_{\rm od}\,|\beta\rangle\,|-\rangle_A\big)\otimes|+\rangle\langle+|_B\\ &\qquad + q_{\mu,\beta}\,\hat{P}\big(\langle x|\,\Pi_{\rm od}\,|\beta\rangle\,|+\rangle_A + \langle x|\,\Pi_{\rm ev}\,|\beta\rangle\,|-\rangle_A\big)\otimes|-\rangle\langle-|_B\Big]\end{aligned} \tag{34}$$

$$\begin{aligned}&= f_{\rm suc}(x)\Big[(1-q_{\mu,\beta})\,\hat{P}\Big(\sqrt{g_{\beta,1/4}(x)}\,|0\rangle_A + \sqrt{g_{-\beta,1/4}(x)}\,|1\rangle_A\Big)\otimes|+\rangle\langle+|_B\\ &\qquad + q_{\mu,\beta}\,\hat{P}\Big(\sqrt{g_{\beta,1/4}(x)}\,|0\rangle_A - \sqrt{g_{-\beta,1/4}(x)}\,|1\rangle_A\Big)\otimes|-\rangle\langle-|_B\Big]\,,\end{aligned} \tag{35}$$

where $\hat{P}(\psi) \coloneqq \psi\psi^\dagger$ (and thus $\hat{P}(|\psi\rangle) = |\psi\rangle\langle\psi|$), and $g_{m,V}$ is the normal distribution with the mean m and the variance V, i.e.,

$$g_{m,V}(x) \coloneqq \frac{1}{\sqrt{2\pi V}}\exp\left[-\frac{(x-m)^2}{2V}\right]. \tag{36}$$

In the above (i.e., Eqs. (32)–(35)), the first equality follows from Eq. (12), and the third follows from Eq. (11) as well as the fact that β is real. We define $\tau^{\rm hom}_{AB}(x)$ as

$$\begin{aligned}\tau^{\rm hom}_{AB}(x) \coloneqq&(1-q_{\mu,\beta})\,\hat{P}\Big(\sqrt{g_{\beta,1/4}(x)}\,|0\rangle_A + \sqrt{g_{-\beta,1/4}(x)}\,|1\rangle_A\Big)\otimes|+\rangle\langle+|_B\\ &+ q_{\mu,\beta}\,\hat{P}\Big(\sqrt{g_{\beta,1/4}(x)}\,|0\rangle_A - \sqrt{g_{-\beta,1/4}(x)}\,|1\rangle_A\Big)\otimes|-\rangle\langle-|_B\,.\end{aligned} \tag{37}$$

From Eqs. (17), (23), (35), and (37), the probability density of an outcome x with occurrence of the phase error is given by

$$\begin{aligned}&\mathrm{Tr}\Big[|-\rangle\langle-|_B\,\mathcal{K}'^{\rm hom}_{AC\to B}(x)(\Phi_{AC})\Big]\\ &= \frac{f_{\rm suc}(x)}{2}\,\mathrm{Tr}\Big[\langle 0|_B\,\tau^{\rm hom}_{AB}(x)\,|0\rangle_B + \langle 1|_B\,\tau^{\rm hom}_{AB}(x)\,|1\rangle_B\\ &\quad - \left(V^{(1)}_{A\to R}(x)\right)^\dagger V^{(0)}_{A\to R}(x)\,\langle 0|_B\,\tau^{\rm hom}_{AB}(x)\,|1\rangle_B - \langle 1|_B\,\tau^{\rm hom}_{AB}(x)\,|0\rangle_B\left(V^{(0)}_{A\to R}(x)\right)^\dagger V^{(1)}_{A\to R}(x)\Big]\end{aligned} \tag{38}$$

$$= f_{\rm suc}(x)\left[\frac{1}{2}\,\mathrm{Tr}\left(\tau^{\rm hom}_{AB}(x)\right) - \mathrm{Re}\left(\mathrm{Tr}\left[\left(V^{(1)}_{A\to R}(x)\right)^\dagger V^{(0)}_{A\to R}(x)\,\langle 0|_B\,\tau^{\rm hom}_{AB}(x)\,|1\rangle_B\right]\right)\right] \tag{39}$$

$$\geq f_{\rm suc}(x)\left[\frac{1}{2}\,\mathrm{Tr}\left(\tau^{\rm hom}_{AB}(x)\right) - \left\|\langle 0|_B\,\tau^{\rm hom}_{AB}(x)\,|1\rangle_B\right\|_1\right], \tag{40}$$

where the last inequality follows from the matrix Hölder inequality. If we write the polar decomposition of $\langle 0|_B \tau_{AB}^{\mathrm{hom}}(x) |1\rangle_B$ as $W_A^{\mathrm{hom}}(x)\left|\langle 0|_B \tau_{AB}^{\mathrm{hom}}(x) |1\rangle_B\right|$, the equality in (40) can be achieved by setting

$$\left(V_{A\to R}^{(1)}(x)\right)^\dagger V_{A\to R}^{(0)} = \left(W_A^{\mathrm{hom}}(x)\right)^\dagger . \tag{41}$$

From Eq. (37), $\langle 0|_B \tau_{AB}^{\mathrm{hom}}(x) |1\rangle_B$ is given by

$$\begin{aligned}\langle 0|_B \tau_{AB}^{\mathrm{hom}}(x) |1\rangle_B = \frac{1}{2}\Big[&(1-q_{\mu,\beta})\,\hat{P}\Big(\sqrt{g_{\beta,1/4}(x)}\,|0\rangle_A + \sqrt{g_{-\beta,1/4}(x)}\,|1\rangle_A\Big)\\ &-q_{\mu,\beta}\,\hat{P}\Big(\sqrt{g_{\beta,1/4}(x)}\,|0\rangle_A - \sqrt{g_{-\beta,1/4}(x)}\,|1\rangle_A\Big)\Big],\end{aligned} \tag{42}$$

which is hermitian with two eigenvalues having opposite signs. Let $|u_+^{\mathrm{hom}}(x)\rangle_A$ and $|u_-^{\mathrm{hom}}(x)\rangle_A$ be eigenvectors of $\langle 0|_B \tau_{AB}^{\mathrm{hom}}(x) |1\rangle_B$ with positive and negative eigenvalues, respectively. Then, $W_A^{\mathrm{hom}}(x)$ is given by

$$W_A^{\mathrm{hom}}(x) = |u_+^{\mathrm{hom}}(x)\rangle\langle u_+^{\mathrm{hom}}(x)|_A - |u_-^{\mathrm{hom}}(x)\rangle\langle u_-^{\mathrm{hom}}(x)|_A . \tag{43}$$

The explicit form of $|u_\pm^{\mathrm{hom}}(x)\rangle_A$ is given in Eq. (173) in Appendix C. The choice of the isometry $V_{A\to R}^{(j)}(x)$ to satisfy Eq. (41) is not unique; one of the reasons is the arbitrariness of the dimension of the system R. Here, we set $R = A$ and set

$$\begin{aligned}V_{A\to R}^{(0)}(x) &= I_A,\\ V_{A\to R}^{(1)}(x) &= W_A^{\mathrm{hom}}(x),\end{aligned} \tag{44}$$

which, with Eqs. (17) and (43), leads to

$$V_{B;A\to A}^{\mathrm{hom}}(x) = \left[|u_+^{\mathrm{hom}}(x)\rangle\langle u_+^{\mathrm{hom}}(x)|_A \otimes I_B + |u_-^{\mathrm{hom}}(x)\rangle\langle u_-^{\mathrm{hom}}(x)|_A \otimes Z_B\right] \text{C-}X_{BA}. \tag{45}$$

For Heterodyne protocol, the calculation similar to Eqs. (32)–(37) leads to

$$\text{C-}X_{BA}\left(\mathrm{Id}_A \otimes \mathcal{K}_{C\to B}^{\mathrm{het}}(\omega)\right)(\Phi_{AC})\,\text{C-}X_{BA} \tag{46}$$

$$\begin{aligned}&= \frac{2f_{\mathrm{suc}}(\omega_r)}{\pi}\,\text{C-}X_{BA}\Big[(1-q_{\mu,\beta})\,\hat{P}\big(\langle\omega|\,\Pi_{\mathrm{ev}}\,|\beta\rangle\,|{+}{+}\rangle_{AB} + \langle\omega|\,\Pi_{\mathrm{od}}\,|\beta\rangle\,|{-}{-}\rangle_{AB}\big)\\ &\qquad +q_{\mu,\beta}\,\hat{P}\big(\langle\omega|\,\Pi_{\mathrm{od}}\,|\beta\rangle\,|{+}{-}\rangle_{AB} + \langle\omega|\,\Pi_{\mathrm{ev}}\,|\beta\rangle\,|{-}{+}\rangle_{AB}\big)\Big]\,\text{C-}X_{BA}\end{aligned} \tag{47}$$

$$\begin{aligned}&= \frac{f_{\mathrm{suc}}(\omega_r)}{\pi}\Big[(1-q_{\mu,\beta})\,\hat{P}\big(\langle\omega|\beta\rangle\,|0\rangle_A + \langle -\omega|\beta\rangle\,|1\rangle_A\big)\otimes|+\rangle\langle+|_B\\ &\qquad +q_{\mu,\beta}\,\hat{P}\big(\langle\omega|\beta\rangle\,|0\rangle_A - \langle -\omega|\beta\rangle\,|1\rangle_A\big)\otimes|-\rangle\langle-|_B\Big],\end{aligned} \tag{48}$$

Since $\langle\omega|\beta\rangle = e^{-\frac{1}{2}[(\omega_r-\beta)^2+\omega_i^2+2i\omega_i\beta]}$ is not real in general, we heuristically insert a θ-rotation around the Z basis

$$R_A^Z(\theta) \coloneqq \exp(-i\theta Z_A/2) \tag{49}$$

in order to have

$$\left(R_A^Z(2\omega_i\beta)\right)^\dagger \text{C-}X_{BA}\left(\mathrm{Id}_A \otimes \mathcal{K}_{C\to B}^{\mathrm{het}}(\omega)\right)(\Phi_{AC})\,\text{C-}X_{BA}\,R_A^Z(2\omega_i\beta) \tag{50}$$

$$\begin{aligned}&= \frac{e^{-\omega_i^2} f_{\mathrm{suc}}(\omega_r)}{\sqrt{\pi}}\Big[(1-q_{\mu,\beta})\,\hat{P}\Big(\sqrt{g_{\beta,1/2}(\omega_r)}\,|0\rangle_A + \sqrt{g_{-\beta,1/2}(\omega_r)}\,|1\rangle_A\Big)\otimes|+\rangle\langle+|_B\\ &\qquad +q_{\mu,\beta}\,\hat{P}\Big(\sqrt{g_{\beta,1/2}(\omega_r)}\,|0\rangle_A - \sqrt{g_{-\beta,1/2}(\omega_r)}\,|1\rangle_A\Big)\otimes|-\rangle\langle-|_B\Big].\end{aligned} \tag{51}$$

We define $\tau_{AB}^{\mathrm{het}}(\omega_r)$ as

$$\begin{aligned}\tau_{AB}^{\mathrm{het}}(\omega_r) \coloneqq\ &(1-q_{\mu,\beta})\,\hat{P}\Big(\sqrt{g_{\beta,1/2}(\omega_r)}\,|0\rangle_A + \sqrt{g_{-\beta,1/2}(\omega_r)}\,|1\rangle_A\Big)\otimes|+\rangle\langle+|_B\\ &+ q_{\mu,\beta}\,\hat{P}\Big(\sqrt{g_{\beta,1/2}(\omega_r)}\,|0\rangle_A - \sqrt{g_{-\beta,1/2}(\omega_r)}\,|1\rangle_A\Big)\otimes|-\rangle\langle-|_B .\end{aligned} \tag{52}$$

Thus, the structure of the matrix $\tau^{\rm het}_{AB}(\omega_r)$ is essentially the same as $\tau^{\rm hom}_{AB}(x)$ of Homodyne protocol. (The heuristics of inserting $R^Z_A(\theta)$ above is for this reduction.) In the same way as Homodyne protocol, the probability density of outcome ω with the occurrence of a phase error is given by

$$\begin{aligned}
&\mathrm{Tr}\Big[|-\rangle\langle -|_B\ \mathcal{K}'^{\rm het}_{AC\to B}(\omega)(\Phi_{AC})\Big] \\
&= \frac{e^{-\omega_i^2} f_{\rm suc}(\omega_r)}{\sqrt{\pi}} \left[\frac{1}{2}\ \mathrm{Tr}\left(\tau^{\rm het}_{AB}(\omega_r)\right)\right. \\
&\qquad\qquad \left. -\mathrm{Re}\left(\mathrm{Tr}\left[\left(V'^{(1)}_{A\to R}(\omega_r)\right)^\dagger V'^{(0)}_{A\to R}(\omega_r) R^Z_A(2\omega_i\beta)\,\langle 0|_B\,\tau^{\rm het}_{AB}(\omega_r)\,|1\rangle_B\,\left(R^Z_A(2\omega_i\beta)\right)^\dagger\right]\right)\right]
\end{aligned} \tag{53}$$

$$\geq \frac{e^{-\omega_i^2} f_{\rm suc}(\omega_r)}{\sqrt{\pi}} \left[\frac{1}{2}\ \mathrm{Tr}\left(\tau^{\rm het}_{AB}(\omega_r)\right) - \left\|\langle 0|_B\,\tau^{\rm het}_{AB}(\omega_r)\ |1\rangle_B\right\|_1\right]. \tag{54}$$

If we write the polar decomposition of $\langle 0|_B\,\tau^{\rm het}_{AB}(\omega_r)\ |1\rangle_B$ by $W^{\rm het}_A(\omega_r)\left|\langle 0|_B\,\tau^{\rm het}_{AB}(\omega_r)\ |1\rangle_B\right|$, then the equality of Eq. (54) can be achieved by setting

$$\left(R^Z_A(2\omega_i\beta)\right)^\dagger \left(V'^{(1)}_{A\to R}(\omega)\right)^\dagger V'^{(0)}_{A\to R}(\omega) R^Z_A(2\omega_i\beta) = \left(W^{\rm het}_A(\omega_r)\right)^\dagger. \tag{55}$$

From Eq. (52), $\langle 0|_B\,\tau^{\rm het}_{AB}(\omega_r)\ |1\rangle_B$ is given by

$$\begin{aligned}
\langle 0|_B\,\tau^{\rm het}_{AB}(\omega_r)\ |1\rangle_B = \frac{1}{2}\Big[&(1-q_{\mu,\beta})\,\hat{P}\Big(\sqrt{g_{\beta,1/2}(\omega_r)}\,|0\rangle_A + \sqrt{g_{-\beta,1/2}(\omega_r)}\,|1\rangle_A\Big) \\
&-q_{\mu,\beta}\,\hat{P}\Big(\sqrt{g_{\beta,1/2}(\omega_r)}\,|0\rangle_A - \sqrt{g_{-\beta,1/2}(\omega_r)}\,|1\rangle_A\Big)\Big],
\end{aligned} \tag{56}$$

which is hermitian. Let $|u^{\rm het}_+(\omega_r)\rangle_A$ and $|u^{\rm het}_-(\omega_r)\rangle_A$ be eigenvectors of $\langle 0|_B\,\tau^{\rm het}_{AB}(\omega_r)\ |1\rangle_B$ with positive and negative eigenvalues, respectively. Then, $W^{\rm het}_A(\omega_r)$ is given by

$$W^{\rm het}_A(\omega_r) = |u^{\rm het}_+(\omega_r)\rangle\langle u^{\rm het}_+(\omega_r)|_A - |u^{\rm het}_-(\omega_r)\rangle\langle u^{\rm het}_-(\omega_r)|_A. \tag{57}$$

We can choose $V'^{(j)}_{A\to R}(\omega)$ to satisfy Eq. (55) in the same way as Homodyne protocol. We set $R=A$ and set

$$\begin{aligned}
V'^{(0)}_{A\to R}(\omega) &= \left(R^Z_A(2\omega_i\beta)\right)^\dagger, \\
V'^{(1)}_{A\to R}(\omega) &= W^{\rm het}_A(\omega_r)\left(R^Z_A(2\omega_i\beta)\right)^\dagger,
\end{aligned} \tag{58}$$

which, with Eqs. (18) and (57), leads to

$$V^{\rm het}_{B;A\to A}(\omega) = \left[|u^{\rm het}_+(\omega_r)\rangle\langle u^{\rm het}_+(\omega_r)|_A \otimes I_B + |u^{\rm het}_-(\omega_r)\rangle\langle u^{\rm het}_-(\omega_r)|_A \otimes Z_B\right]\left(R^Z_A(2\omega_i\beta)\right)^\dagger \text{C-}X_{BA}. \tag{59}$$

We thus obtained the optimal choice of the controlled isometry $V^{\rm hom}_{B;A\to R}(x)$ in Eq. (45) for Homodyne protocol (resp. $V^{\rm het}_{B;A\to R}(\omega)$ in Eq. (59) for Heterodyne protocol) so that the probability that Bob obtains $\hat{b}'=-$ is minimized for the pure-loss channel. As explained previously, we set $V^{(j)}_{A\to R}(x)$ to the one in Eq. (44) (resp. $V'^{(j)}_{A\to R}(\omega)$ to the one in Eq. (58)) also for arbitrary channels, i.e., arbitrary coherent attacks by Eve. This choice is suboptimal for general channels but is expected to be close to optimal for channels that are close to the pure-loss one. Now that the controlled isometry $V^{\rm hom}_{B;A\to A}(x)$ (resp. $V^{\rm het}_{B;A\to A}(\omega)$) is fixed, we can interpret the event that Bob announces "success" and obtains $\hat{b}'=-$ (i.e., the phase error) at the signal round of Estimation protocol as the outcome of a generalized measurement on Alice's qubit A and the optical pulse C, and define the corresponding POVM element $M^{\rm hom/het}_{\rm ph}$ (i.e., the phase error operator) through Eq. (21) (resp. Eq. (22)) as

$$M^{\rm hom}_{\rm ph} \coloneqq \mathcal{F}^{\rm hom\ \ddagger}_{AC\to B}\left(|-\rangle\langle -|_B\right) = \int_{-\infty}^{\infty} dx\ \left(\mathcal{K}'^{\rm hom}_{AC\to B}(x)\right)^\ddagger \left(|-\rangle\langle -|_B\right), \tag{60}$$

$$M^{\rm het}_{\rm ph} \coloneqq \mathcal{F}^{\rm het\ \ddagger}_{AC\to B}\left(|-\rangle\langle -|_B\right) = \iint_{-\infty}^{\infty} d\omega_r\, d\omega_i\ \left(\mathcal{K}'^{\rm het}_{AC\to B}(\omega)\right)^\ddagger \left(|-\rangle\langle -|_B\right), \tag{61}$$

where ‡ denotes the adjoint map. Then, for any density operator ρ on the joint system AC, $M_{\rm ph}^{\rm hom}$ (resp. $M_{\rm ph}^{\rm het}$) satisfies

$$\mathbb{E}_\rho\left[\hat{N}_{\rm ph}^{{\rm suc}\,(i)}\right] = p_{\rm sig}{\rm Tr}\left[\rho\, M_{\rm ph}^{\rm hom/het}\right] \tag{62}$$

in Homodyne (resp. Heterodyne) protocol, where $\hat{N}_{\rm ph}^{{\rm suc}\,(i)}$ is defined in Estimation protocol (see Box 3). For Homodyne protocol, by using Eqs. (9), (23), and (45), we have

$$M_{\rm ph}^{\rm hom} = \int_{-\infty}^{\infty} dx\, \left[I_A \otimes \left(K_{\rm suc}^{\rm hom}(x)\right)^\dagger\right] \left(V_{B;A\to A}^{\rm hom}(x)\right)^\dagger \left(I_A \otimes |-\rangle\langle -|_B\right) V_{B;A\to A}^{\rm hom}(x) \left[I_A \otimes K_{\rm suc}^{\rm hom}(x)\right] \tag{63}$$

$$\begin{aligned} = \int_{-\infty}^{\infty} dx \Big[\hat{P}\Big(\left[I_A \otimes \left(K_{\rm suc}^{\rm hom}(x)\right)^\dagger\right] {\rm C}\text{-}X_{BA}\, |u_+^{\rm hom}(x)\rangle_A \otimes |-\rangle_B\Big) \\ + \hat{P}\left(\left[I_A \otimes \left(K_{\rm suc}^{\rm hom}(x)\right)^\dagger\right] {\rm C}\text{-}X_{BA}\, |u_-^{\rm hom}(x)\rangle_A \otimes |+\rangle_B\right)\Big], \end{aligned} \tag{64}$$

where we used the fact that the adjoint map of the tracing-out ${\rm Tr}_A$ is taking the tensor product with I_A. Using the relation ${\rm C}\text{-}X_{BA} = |+\rangle\langle +|_A \otimes I_B + |-\rangle\langle -|_A \otimes Z_B$ as well as Eq. (12), we have

$$\begin{aligned} M_{\rm ph}^{\rm hom} = \int_{-\infty}^{\infty} 2 f_{\rm suc}(x) dx \Big[\hat{P}\Big(\Pi_{AC}^{(+,{\rm od}),(-,{\rm ev})}\, |u_+^{\rm hom}(x)\rangle_A \otimes |x\rangle_C\Big) \\ + \hat{P}\Big(\Pi_{AC}^{(-,{\rm od}),(+,{\rm ev})}\, |u_-^{\rm hom}(x)\rangle_A \otimes |x\rangle_C\Big)\Big], \end{aligned} \tag{65}$$

where two orthogonal projections $\Pi_{AC}^{(+,{\rm od}),(-,{\rm ev})}$ and $\Pi_{AC}^{(-,{\rm od}),(+,{\rm ev})}$ are defined as

$$\Pi_{AC}^{(+,{\rm od}),(-,{\rm ev})} := |+\rangle\langle +|_A \otimes \Pi_{\rm od} + |-\rangle\langle -|_A \otimes \Pi_{\rm ev}, \tag{66}$$

$$\Pi_{AC}^{(-,{\rm od}),(+,{\rm ev})} := |-\rangle\langle -|_A \otimes \Pi_{\rm od} + |+\rangle\langle +|_A \otimes \Pi_{\rm ev}. \tag{67}$$

A similar relation holds for Heterodyne protocol by replacing $K_{\rm suc}^{\rm hom}(x)$ with $K_{\rm suc}^{\rm het}(\omega)$ and $V_{B;A\to A}^{\rm hom}(x)$ with $V_{B;A\to A}^{\rm het}(\omega)$ as well as using Eqs. (15), (59), (66), and (67):

$$\begin{aligned} M_{\rm ph}^{\rm het} = \iint_{-\infty}^{\infty} d\omega_r d\omega_i \Big[\hat{P}\Big(\left[I_A \otimes \left(K_{\rm suc}^{\rm het}(\omega)\right)^\dagger\right] {\rm C}\text{-}X_{BA}\, R_A^Z(2\omega_i\beta)\, |u_+^{\rm het}(\omega_r)\rangle_A \otimes |-\rangle_B\Big) \\ + \hat{P}\Big(\left[I_A \otimes \left(K_{\rm suc}^{\rm het}(\omega)\right)^\dagger\right] {\rm C}\text{-}X_{BA}\, R_A^Z(2\omega_i\beta)\, |u_-^{\rm het}(\omega_r)\rangle_A \otimes |+\rangle_B\Big)\Big] \end{aligned} \tag{68}$$

$$\begin{aligned} = \iint_{-\infty}^{\infty} \frac{2 f_{\rm suc}(\omega_r)}{\pi} d\omega_r d\omega_i \Big[\hat{P}\Big(\Pi_{AC}^{(+,{\rm od}),(-,{\rm ev})} R_A^Z(2\omega_i\beta)\, |u_+^{\rm het}(\omega_r)\rangle_A \otimes |\omega\rangle_C\Big) \\ + \hat{P}\Big(\Pi_{AC}^{(-,{\rm od}),(+,{\rm ev})} R_A^Z(2\omega_i\beta)\, |u_-^{\rm het}(\omega_r)\rangle_A \otimes |\omega\rangle_C\Big)\Big]. \end{aligned} \tag{69}$$

Using Eq. (11), we observe that

$$\frac{1}{\pi}\int d\omega_i \exp(\pm 2i\omega_i\beta)\, |\omega\rangle\langle\omega| = \frac{1}{\pi}\iiint d\omega_i dx dx' \sqrt{\frac{2}{\pi}} e^{\pm 2i\omega_i\beta - (x-\omega_r)^2 + 2i\omega_i x - (x'-\omega_r)^2 - 2i\omega_i x'}\, |x\rangle\langle x'| \tag{70}$$

$$= 2\iint dx dx'\, \delta(2(x \pm \beta - x'))\, |x\rangle\langle x|\omega_r\rangle\langle\omega_r|x'\rangle\langle x'| \tag{71}$$

$$= \int dx\, |x\rangle\langle x|\omega_r\rangle\langle\omega_r|x \pm \beta\rangle\langle x \pm \beta|\,. \tag{72}$$

Applying this to Eq. (69) and changing the integration variable appropriately, we have

$$\begin{aligned} M_{\rm ph}^{\rm het} = \iint_{-\infty}^{\infty} 2 f_{\rm suc}(\omega_r) d\omega_r dx \Big[\hat{P}\left(\Pi_{AC}^{(+,{\rm od}),(-,{\rm ev})} O_{AC}^{\beta}(x)\, |u_+^{\rm het}(\omega_r)\rangle_A \otimes |\omega_r\rangle_C\right) \\ + \hat{P}\left(\Pi_{AC}^{(-,{\rm od}),(+,{\rm ev})} O_{AC}^{\beta}(x)\, |u_-^{\rm het}(\omega_r)\rangle_A \otimes |\omega_r\rangle_C\right)\Big], \end{aligned} \tag{73}$$

where the operator $O_{AC}^{\beta}(x)$ is defined as

$$O_{AC}^{\beta}(x) := |0\rangle\langle 0|_A \otimes |x\rangle\langle x|_C + |1\rangle\langle 1|_A \otimes |x-\beta\rangle\langle x-\beta|_C\,. \tag{74}$$

2.4 Finite-size analysis

Since the phase error operator was defined on systems A and C, we can follow essentially the same analysis as that in Ref. [40]. Let us define the following operators:

$$\Pi^{\rm fid} := |0\rangle\langle 0|_A \otimes |\beta\rangle\langle\beta|_C + |1\rangle\langle 1|_A \otimes |-\beta\rangle\langle -\beta|_C \tag{75}$$

$$= |\phi_-\rangle\langle\phi_-|_{AC} + |\phi_+\rangle\langle\phi_+|_{AC}\,, \tag{76}$$

$$\Pi_-^{\rm trash} := |-\rangle\langle -|_A \otimes I_C, \tag{77}$$

where $|\phi_\pm\rangle_{AC}$ are defined in Eqs. (29) and (30). For any density operator ρ on the joint system AC, these operators satisfy

$$\mathbb{E}_\rho\left[\hat{F}^{(i)}\right] \le p_{\rm test}\,{\rm Tr}\left[\rho\,\Pi^{\rm fid}\right], \tag{78}$$

$$\mathbb{E}_\rho\left[\hat{Q}_-^{(i)}\right] = p_{\rm trash}\,{\rm Tr}\left[\rho\,\Pi_-^{\rm trash}\right], \tag{79}$$

where the first inequality follows from Corollary 1 in Appendix B.1 as well as the definition of $\hat{F}^{(i)}$ in Estimation protocol (see Box 3), and the second equality follows from the definition of $\hat{Q}_-^{(i)}$ in Estimation protocol (see Box 3). Let $M^{\rm hom/het}[\kappa,\gamma]$ for positive numbers κ and γ determined prior to the protocol be defined as

$$M^{\rm hom/het}[\kappa,\gamma] := M_{\rm ph}^{\rm hom/het} + \kappa\Pi^{\rm fid} - \gamma\Pi_-^{\rm trash}. \tag{80}$$

In Corollaries 3 and 4 in Appendix C, we show an inequality

$$M^{\rm hom/het}[\kappa,\gamma] \le B^{\rm hom/het}(\kappa,\gamma)\,I_{AC} \tag{81}$$

with a computable convex function $B^{\rm hom/het}(\kappa,\gamma)$. Let $\hat{T}^{(i)}[\kappa,\gamma]$ be a linear combination of random variables at ith round in Estimation protocol given by

$$\hat{T}^{(i)}[\kappa,\gamma] := p_{\rm sig}^{-1}\hat{N}_{\rm ph}^{{\rm suc}\,(i)} + p_{\rm test}^{-1}\kappa\hat{F}^{(i)} - p_{\rm trash}^{-1}\gamma\hat{Q}_-^{(i)}. \tag{82}$$

From Eqs. (62), (78), (79), and (81), we have

$$\mathbb{E}_\rho\left[\hat{T}^{(i)}[\kappa,\gamma]\right] \le {\rm Tr}\left[\rho M^{\rm hom/het}[\kappa,\gamma]\right] \le B^{\rm hom/het}(\kappa,\gamma), \tag{83}$$

for any density operator ρ. Furthermore, from the definition of $\hat{N}_{\rm ph}^{{\rm suc}\,(i)}$, $\hat{F}^{(i)}$, and $\hat{Q}_-^{(i)}$ in Estimation protocol (see Box 3), we have

$$\min\left\{p_{\rm test}^{-1}\kappa\min_{\nu\ge 0}\Lambda_{m,r}(\nu), -p_{\rm trash}^{-1}\gamma\right\} \le \hat{T}^{(i)}[\kappa,\gamma] \le \max\left\{p_{\rm sig}^{-1}, p_{\rm test}^{-1}\kappa\max_{\nu\ge 0}\Lambda_{m,r}(\nu)\right\}. \tag{84}$$

Let $\delta_1(\epsilon)$ be defined as

$$\delta_1(\epsilon) := \left(\max\left\{p_{\rm sig}^{-1}, p_{\rm test}^{-1}\kappa\max_{\nu\ge 0}\Lambda_{m,r}(\nu)\right\} - \min\left\{p_{\rm test}^{-1}\kappa\min_{\nu\ge 0}\Lambda_{m,r}(\nu), -p_{\rm trash}^{-1}\gamma\right\}\right)\sqrt{\frac{N}{2}\ln\left(\frac{1}{\epsilon}\right)}. \tag{85}$$

Then, by applying Proposition 2 in Appendix B.3 to $\{\hat{T}^{(k)}[\kappa,\gamma]\}_{k=1,\ldots,N}$ as well as using Eqs. (82)–(85), we have

$$\Pr\left[\left(\sum_{k=1}^N \hat{T}^{(k)}[\kappa,\gamma] =\right) p_{\rm sig}^{-1}\hat{N}_{\rm ph}^{\rm suc} + p_{\rm test}^{-1}\kappa\hat{F} - p_{\rm trash}^{-1}\gamma\hat{Q}_- \ge NB^{\rm hom/het}(\kappa,\gamma) + \delta_1(\epsilon/2)\right] \le \epsilon/2. \tag{86}$$

Since $\hat{Q}_-$ is determined solely by Alice's qubits, each in the state ${\rm Tr}_{\tilde{C}}(|\Phi\rangle\langle\Phi|_{A\tilde{C}})$ with $|\Phi\rangle_{A\tilde{C}}$ given in Eq. (7), it follows the same statistics as a tally of $\hat{N}^{\rm trash}$ Bernoulli trials with a probability $q_- := \|\langle -|_A|\Psi\rangle_{A\tilde{C}}\|^2 = (1-e^{-2\mu})/2$. Hence, by using the Chernoff-Hoeffding inequality [64, 62], we have

$$\Pr\left[\hat{Q}_- \ge q_-\hat{N}^{\rm trash} + \delta_2(\epsilon/2;\hat{N}^{\rm trash})\right] \le \epsilon/2. \tag{87}$$

Here, $\delta_2(\epsilon;n)$ is defined as [40]

$$\begin{cases} D(q_- + \delta_2(\epsilon;n)/n \| q_-) = -\frac{1}{n}\log_2(\epsilon) & (\epsilon > q_-^n) \\ \delta_2(\epsilon;n) = (1-q_-)n & (\epsilon \le q_-^n) \end{cases}, \tag{88}$$

where

$$D(x\|y) \coloneqq x\log_2\frac{x}{y} + (1-x)\log_2\frac{1-x}{1-y} \tag{89}$$

is the Kullback-Leibler divergence. Combining Eqs. (86), and (87), by setting

$$U(\hat{F},\hat{N}^{\mathrm{trash}}) = p_{\mathrm{sig}}\big(NB^{\mathrm{hom/het}}(\kappa,\gamma) + \delta_1(\epsilon/2)\big) - \frac{p_{\mathrm{sig}}}{p_{\mathrm{test}}}\kappa\hat{F} + \frac{p_{\mathrm{sig}}}{p_{\mathrm{trash}}}\gamma\big(q_-\hat{N}^{\mathrm{trash}} + \delta_2(\epsilon/2;\hat{N}^{\mathrm{trash}})\big), \tag{90}$$

we observe that Eq. (25) holds from the union bound.

3 Numerical simulations

We compute (the lower bound on) the net key gain per pulse (i.e., key rate $\hat{G}$) against the transmission distance with various values of excess noise at the channel output. In this model, Bob receives Gaussian states $\rho_{\mathrm{model}}^{(\hat{a})}$ obtained by randomly displacing attenuated coherent states $|(-1)^{\hat{a}}\sqrt{\eta\mu}\rangle$ with attenuation rate η to increase their variances via factor of $(1+\xi)$, i.e.,

$$\rho_{\mathrm{model}}^{(\hat{a})} \coloneqq \frac{2}{\pi\xi}\int_{\mathbb{C}} e^{-2|\gamma|^2/\xi}\,|(-1)^{\hat{a}}\sqrt{\eta\mu}+\gamma\rangle\langle(-1)^{\hat{a}}\sqrt{\eta\mu}+\gamma|\,d^2\gamma. \tag{91}$$

For simplicity, the number N_{smp} of the sampling rounds is set to be $N/100$, and the bit error correction efficiency f in Eq. (4) is to be 0.95 [2]. The acceptance probability $f_{\mathrm{suc}}(x)$ is assumed to be a step function $\Theta(x-x_{\mathrm{th}})$ with a threshold $x_{\mathrm{th}}(>0)$, where $\Theta(x)$ denotes the Heaviside step function. The expected amplitude of the coherent state β is chosen to be $\sqrt{\eta\mu}$. We set the security parameter $\varepsilon_{\mathrm{sec}} = 2^{-50}$, and set $\varepsilon_{\mathrm{cor}} = \varepsilon_{\mathrm{sec}}/2$ and $\epsilon = 2^{-s} = \varepsilon_{\mathrm{sec}}^2/16$.

We assume that the number of "success" signal rounds $\hat{N}^{\mathrm{suc}}$ is equal to its expectation, i.e.,

$$\mathbb{E}[\hat{N}^{\mathrm{suc}}] = p_{\mathrm{sig}}N\int_{-\infty}^{\infty}(f_{\mathrm{suc}}(x)+f_{\mathrm{suc}}(-x))\,\langle x|\,\frac{1}{2}\sum_{a\in\{0,1\}}\rho_{\mathrm{model}}^{(a)}\,|x\rangle\,dx \tag{92}$$

$$\begin{aligned} &= p_{\mathrm{sig}}N\int_{-\infty}^{\infty}\frac{1}{2}\Big[(f_{\mathrm{suc}}(x)+f_{\mathrm{suc}}(-x))\,\langle x|\,\rho_{\mathrm{model}}^{(0)}\,|x\rangle \\ &\qquad\qquad +(f_{\mathrm{suc}}(-x)+f_{\mathrm{suc}}(x))\,\langle -x|\,\rho_{\mathrm{model}}^{(1)}\,|-x\rangle\Big]\,dx \end{aligned} \tag{93}$$

$$= p_{\mathrm{sig}}N\int_{-\infty}^{\infty}\frac{1}{2}\sum_{a\in\{0,1\}}(f_{\mathrm{suc}}(x)+f_{\mathrm{suc}}(-x))\,\langle(-1)^a x|\,\rho_{\mathrm{model}}^{(a)}\,|(-1)^a x\rangle\,dx \tag{94}$$

$$= p_{\mathrm{sig}}N(P_{\mathrm{hom}}^{+}+P_{\mathrm{hom}}^{-}), \tag{95}$$

where

$$P_{\mathrm{hom}}^{\pm} \coloneqq \int_{-\infty}^{\infty} f_{\mathrm{suc}}(\pm x)\,\langle(-1)^a x|\,\rho_{\mathrm{model}}^{(a)}\,|(-1)^a x\rangle\,dx \tag{96}$$

$$= \int_{x_{\mathrm{th}}}^{\infty}\langle\pm(-1)^a x|\,\rho_{\mathrm{model}}^{(a)}\,|\pm(-1)^a x\rangle\,dx \tag{97}$$

$$= \frac{1}{2}\mathrm{erfc}\left((x_{\mathrm{th}}\mp\sqrt{\eta\mu})\sqrt{\frac{2}{1+\xi}}\right), \tag{98}$$

for Homodyne protocol [40]. In the above, P_{hom}^{+} (resp. P_{hom}^{-}) denotes the probability that Alice and Bob obtain coincident (resp. incoincident) bit values in the signal round. (Note that the apparent

[2] Currently, this level of efficiency may be too optimistic because the bit error correction in our protocol must succeed with probability no smaller than $1-\varepsilon_{\mathrm{cor}}/2$ without the use of the verification.

a-dependence in the definition of $P^{\pm}_{\rm hom}$ above is not the case because of the symmetry of $\rho^{(a)}_{\rm model}$ defined in Eq. (91).) In a similar way, we obtain for Heterodyne protocol that

$$\mathbb{E}[\hat{N}^{\rm suc}] = p_{\rm sig} N (P^{+}_{\rm het} + P^{-}_{\rm het}), \tag{99}$$

$$P^{\pm}_{\rm het} := \iint_{-\infty}^{\infty} \frac{f_{\rm suc}(\pm\omega_r)}{\pi} \langle (-1)^a \omega | \, \rho^{(a)}_{\rm model} \, | (-1)^a \omega \rangle \, d\omega_r d\omega_i \tag{100}$$

$$= \int_{-\infty}^{\infty} d\omega_i \int_{x_{\rm th}}^{\infty} d\omega_r \frac{f_{\rm suc}(\pm\omega_r)}{\pi} \langle (-1)^a \omega | \, \rho^{(a)}_{\rm model} \, | (-1)^a \omega \rangle \tag{101}$$

$$= \frac{1}{2} {\rm erfc}\left((x_{\rm th} \mp \sqrt{\eta\mu}) \sqrt{\frac{2}{2+\xi}} \right). \tag{102}$$

We also assume that the number of "success" sampling rounds is equal to $(P^{+}_{\rm hom/het} + P^{-}_{\rm hom/het}) N_{\rm smp}$, the number of test rounds $\hat{N}^{\rm test}$ is equal to $p_{\rm test} N$, and the number of trash rounds $\hat{N}^{\rm trash}$ is equal to $p_{\rm trash} N$. The test outcome $\hat{F}$ is assumed to be equal to its expectation given by [40]

$$\mathbb{E}[\hat{F}] = p_{\rm test} N \frac{1}{2} \sum_{a \in \{0,1\}} \mathbb{E}_{\rho^{(a)}_{\rm model}} [\Lambda_{m,r}(|\hat{\omega} - (-1)^a \sqrt{\eta\mu}|^2)] \tag{103}$$

$$= \frac{p_{\rm test} N}{1 + \xi/2} \left[1 - (-1)^{m+1} \left(\frac{\xi/2}{1 + r(1+\xi/2)} \right)^{m+1} \right]. \tag{104}$$

For the test function $\Lambda_{m,r}$ in the above, we adopt $m = 1$ and $r = 0.4120$, which leads to $(\max_{\nu \geq 0} \Lambda_{m,r}(\nu), \min_{\nu \geq 0} \Lambda_{m,r}(\nu)) = (2.824, -0.9932)$. We assume that the number $\hat{E}_{\rm obs}$ of bit errors observed in the "success" sampling rounds is equal to its expectation $\hat{E}_{\rm obs} = P^{-}_{\rm hom/het} N_{\rm smp}$. The upper-bound $e_{\rm qber}$ on the bit error rate is thus given by Eq. (3) with the parameters $\hat{N}^{\rm suc}$, $\hat{N}^{\rm suc}_{\rm smp}$, and $\hat{E}_{\rm obs}$ given above. Under these assumptions, the remaining parameters to be determined are six parameters $(\mu, x_{\rm th}, p_{\rm sig}, p_{\rm test}, \kappa, \gamma)$. We determined (κ, γ) via a convex optimization using CVXPY 1.2.1 and $(\mu, x_{\rm th}, p_{\rm sig}, p_{\rm test})$ via the Nelder-Mead in the scipy.minimize library in Python, for each transmission distance L with the attenuation rate η assumed to be $10^{-0.02L}$.

Figure 2 shows the key rates of Homodyne protocol for the channel model explained above. Figures show that under the condition of low excess noise, our refined analysis results in significantly higher key rates and longer transmission distance than that of the previous results [40] even in the finite-key case. Furthermore, the logarithm of the asymptotic key rate in the pure-loss case (i.e., $\xi = 0$) is in parallel to the PLOB bound [51] against the transmission distance; that is, it achieves a linear scaling against the channel transmission, which is known to be optimal for one-way QKD in the pure-loss channel. When the excess noise ξ is around $10^{-3.0}$–$10^{-2.0}$, however, the improvements in our refined analysis are lost. The result of the parameter optimization implies that our refined analysis generates the key with relatively small intensity μ of the input coherent states compared to the previous analyses; e.g., the optimized input intensity μ of Homodyne protocol is ~ 0.04 in our refined analysis compared to ~ 0.2 in the previous analysis [40] at $\eta = 0.1$ (i.e., 50 km) for the asymptotic pure-loss case.

The key rate of Heterodyne protocol has a similar behavior. Figure 3 shows the key rates of Heterodyne protocol with the same noise model as above. Figures show that our refined analysis significantly improves the key rate against the pure-loss channel, but is fragile against excess noise. One can see, however, that, while the key rate of Heterodyne protocol is still low compared to that of Homodyne protocol, the achievable distance (i.e., the distance with a non-zero key rate) now becomes comparable with our refined analysis. This implies that our refined analysis based on the reverse reconciliation is more effective for Heterodyne protocol.

4 Discussion

We propose a refined security analysis for the protocol proposed in Ref. [40] based on the reverse reconciliation. The motivating ideas of our refinement come from the facts that the distillability of a secret key from a quantum state is a looser condition than the distillability of an entanglement from

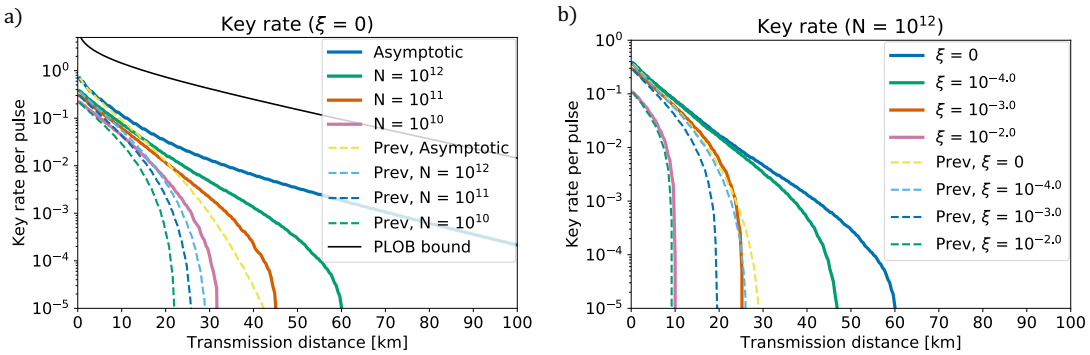


Figure 2: Key rates of the Homodyne protocol against transmission distance over an optical fiber. The attenuation rate of the optical fiber is assumed to be $10^{-0.02L}$ with transmission distance L km, an error correction efficiency f in Eq. (4) is set to be 0.95, and the number of sampling rounds $N_{\rm smp}$ is set to be $N/100$. a) Key rates when the excess noise ξ at the channel output is zero; that is, the channel is pure loss. The bold solid lines show the key rates with our refined analysis developed here, the broken lines show those with the previous analysis [40], and the black thin line shows the PLOB bound, which is the ultimate limit of the key rate of one-way QKD [51]. One can see that the logarithm of the asymptotic key rate decreases in parallel to the PLOB bound with our refined analysis against the transmission distance ($\gg 1$ km) as opposed to the previous results [40]. Improvement in the key rate is sustained in the finite-size case. b) Key rates when $N = 10^{12}$ with various values of excess noise parameter ξ. (The detail of the noise model is given in the main text.) The solid lines show the key rates with our refined analysis, and the broken lines show those with the previous results [40]. One can see that, although the key rate significantly improves for the pure-loss channel, the excess noise as high as $\xi = 10^{-3}$–10^{-2} degrades the performance to almost the same level as that of the previous results.

it [55, 56, 57, 46, 58, 47] and that the reverse reconciliation can increase the key rate for CV QKD protocols [10]. To exploit the ideas, we developed the procedure of "twisting" Alice's system with $V^{\rm hom}_{B;A\to R}(x)$ (resp. $V^{\rm het}_{B;A\to R}(\omega)$) controlled by Bob's qubit. Similar techniques have already appeared in previous works [55, 46, 57, 58, 47, 59]. Our finding is that by using the twisting operation that minimizes the phase error probability for the pure-loss channel, the protocol has asymptotically optimal scaling in the key rates both for Homodyne and Heterodyne protocols. This is a clear distinction from the previous results [40, 41]; there, the asymptotic key rate non-linearly decreases against the channel transmission. This results challenge conventionally considered limitations on the phase error correction applied to the CV QKD. For example, in Ref. [30], the security proof based on the entropic uncertainty relation and the phase error correction did not achieve optimal linear key-rate scaling in the asymptotic case even with reverse reconciliation. The author ascribed this bad performance to the gap between a conditional entropy with a quantum conditioning and one with a classical conditioning, where the latter corresponds to measuring the quantum system with a fixed basis. Here, our security proof can be seen from Eqs. (45), (59) and the definitions of $|u^{\rm hom/het}_{\pm}(x)\rangle_A$ as "twisting" the (measurement) basis in which Alice's system is reduced to classical depending on the expected amplitude of a received optical signal as well as an observed homodyne/heterodyne outcome. This may minimize the above mentioned gap and thus achieve the asymptotically optimal scaling. In this sense, the conventionally-thought limitation may not be an actual limitation.

The improvement in the performance remains in the finite-key case but is lost under the existence of excess noise as high as $\xi = 10^{-3}$–10^{-2} at the channel output. This may limit the feasibility of our binary-modulation protocol, but current theoretical progress in CV QKD reveals that the discrete-modulation CV-QKD protocols with four types of modulation have more tolerance against excess noise than those with binary modulation [16, 17, 18]. What is important is that our security proof can be extended to the four-state protocols with binary outcomes, such as Protocol 2 in Ref. [17] and a protocol in Ref. [18], by replacing the bit-extracting measurements of these protocols with the qubit-extracting maps as shown in Eq. (9) and constructing the corresponding phase error operator. This is, however, much more complicated than the previous analysis, and we leave the problem as future work.

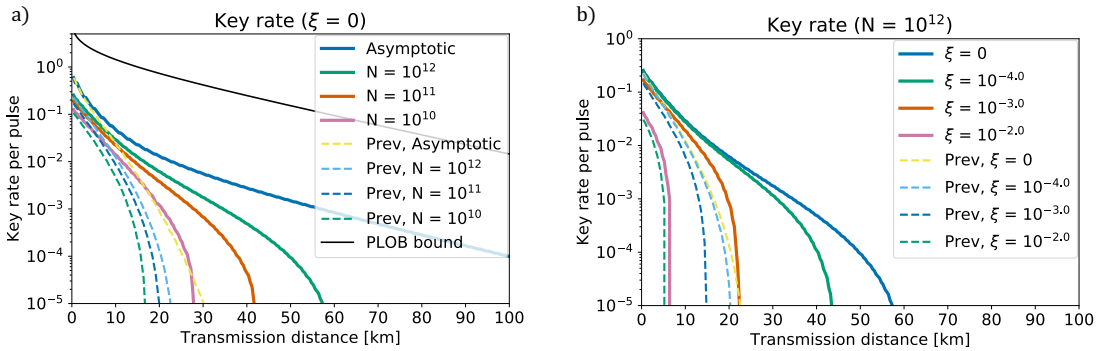


Figure 3: Key rates of the Heterodyne protocol against transmission distance over an optical fiber. The noise models are the same as those of Homodyne protocol. a) Key rates when the excess noise ξ at the channel output is zero; that is, the channel is pure loss. The bold solid lines show the key rates with our refined analysis developed here, the broken lines show those with the previous analysis [41], and the black thin line shows the PLOB bound, which is the ultimate limit of the key rate of one-way QKD [51]. One can see that the logarithm of the asymptotic key rate is in parallel to the PLOB bound when the transmission distance is large in the same way as that of Homodyne protocol. The key rate is still less (about half) than that of Homodyne protocol. b) Key rates when $N = 10^{12}$ with various values of excess noise parameter ξ. The solid lines show the key rates with our refined analysis, and the broken lines show those with the previous result [41].

There are several remaining questions with our present results. The first and foremost is whether we can obtain higher tolerance against excess noise by extending our analysis to the four-state protocols. As explained above, our analysis can be extended to the four-state protocols with binary outputs [17, 18], i.e., protocols that use homodyne measurement to distinguish signals. With the same type of argument based on the phase error estimation, we can carry out the finite-size security proof for these protocols in principle. However, developing the analyses that preserve the robustness against excess noise for these protocols still has non-triviality. A more challenging problem is to apply our finite-size security proof to the four-state protocols with more than two outputs, such as a protocol in Ref. [16] and Protocol 1 in Ref. [17]. In this case, the definition of phase errors is already non-trivial as opposed to those with binary outputs, and we have to develop more elaborated finite-size security proof. Whether we can extend our techniques to these protocols or protocols with even more constellations [20] is still open.

Another important theoretical question is whether the trusted-noise model can be applied to our security analysis. In practice, even the excess noise of $\xi = 10^{-3}$ at the channel output is difficult to realize if all the noises are untrusted. Recently, efforts have been made in the field of CV QKD on how to incorporate noises that are intrinsic to apparatuses and thus inaccessible to Eve into the security proof as trusted noises. This effectively eases the requirement on the experimental apparatuses. In the present security analysis as well as ones in Refs. [40, 41], the fidelity test measures the fidelity to a pure coherent state, which cannot be naively generalized to the fidelity to a mixed state. Whether we can incorporate trusted noises into the fidelity test may be crucial in this direction.

From the viewpoint of the feasibility of the protocol, the total number of 10^{12} of rounds to obtain a tolerable finite-size performance may be demanding. The finite-size performance may be improved by applying recently developed refinement [65] of the Azuma's inequality [66] that utilizes unconfirmed knowledge. What is non-trivial for the application of this is that the random variable in our application of Azuma's inequality can not directly be observed even at the end of the protocol. Whether we can apply the refined concentration inequality [65] with the information accessible in our protocol (in a similar fashion to Ref. [67]) may be an interesting problem.

Acknowledgments

This work was supported by the Ministry of Internal Affairs and Communications (MIC), R&D of ICT Priority Technology Project (grant number JPMI00316); Cross-ministerial Strategic Innovation Promotion Program (SIP) (Council for Science, Technology and Innovation (CSTI)); JSPS KAKENHI Grant Number JP22K13977; JSPS Overseas Research Fellowships.

Code availability

Computer codes to calculate the key rates are available from the corresponding author upon reasonable request.

A Definition of (composable) security

In this section, we give a definition of security, which can be divided into two conditions, secrecy and correctness. The definition satisfies the so-called universal composability [68]. Since the correctness is satisfied by the procedure in the actual protocol, it is the secrecy that is the focus of our security proof. In this section, when the index to denote a system is dropped from a joint quantum state, the partial trace is implicitly taken for that system; e.g., for the state ρ_{AB}, $\rho_A = \mathrm{Tr}_B[\rho_{AB}]$.

Let us assume that a given (prepare-and-measure) QKD protocol generates the final key bits $\hat{\boldsymbol{z}}_A^{\mathrm{fin}}$ and $\hat{\boldsymbol{z}}_B^{\mathrm{fin}}$ between Alice and Bob with the length denoted as $\hat{N}^{\mathrm{fin}}$. When the protocol generates null key or is aborted, we set $\hat{\boldsymbol{z}}_A^{\mathrm{fin}} = \hat{\boldsymbol{z}}_B^{\mathrm{fin}} = \emptyset$ and $\hat{N}^{\mathrm{fin}} = 0$. Given the final key length $\hat{N}^{\mathrm{fin}} = N \geq 1$, let $\rho_{ABE|N}^{\mathrm{fin}}$ be a quantum state between Alice's and Bob's N-bit final key as well as Eve's system at the end of the actual protocol.

Definition 1. *Given an arbitrary positive real number $\varepsilon_{\mathrm{sec}} > 0$, a QKD protocol is called $\varepsilon_{\mathrm{sec}}$-secure if it satisfies the following:*

$$\frac{1}{2}\sum_{N\geq 1}\Pr(\hat{N}^{\mathrm{fin}} = N)\left\|\rho_{ABE|N}^{\mathrm{fin}} - \rho_{ABE|N}^{\mathrm{ideal}}\right\|_1 \leq \varepsilon_{\mathrm{sec}}, \tag{105}$$

where $\rho_{ABE|N}^{\mathrm{ideal}}$ is defined as

$$\rho_{ABE|N}^{\mathrm{ideal}} \coloneqq \sum_{\boldsymbol{z}\in\{0,1\}^N}\frac{1}{2^N}|\boldsymbol{z}\rangle\langle\boldsymbol{z}|_A \otimes |\boldsymbol{z}\rangle\langle\boldsymbol{z}|_B \otimes \rho_{E|N}^{\mathrm{fin}}. \tag{106}$$

Proposition 1. *For arbitrary positive real numbers $\varepsilon_{\mathrm{cor}} > 0$ and $\varepsilon_{\mathrm{sc}} > 0$, let us assume that the following two conditions are satisfied:*

$$\Pr(\hat{N}^{\mathrm{fin}} \geq 1, \hat{\boldsymbol{z}}_A^{\mathrm{fin}} \neq \hat{\boldsymbol{z}}_B^{\mathrm{fin}}) \leq \varepsilon_{\mathrm{cor}}, \tag{107}$$

$$\frac{1}{2}\sum_{N\geq 1}\Pr(\hat{N}^{\mathrm{fin}} = N)\left\|\rho_{AE|N}^{\mathrm{fin}} - \rho_{AE|N}^{\mathrm{ideal}}\right\|_1 \leq \varepsilon_{\mathrm{sc}}. \tag{108}$$

Then, the protocol is $(\varepsilon_{\mathrm{cor}} + \varepsilon_{\mathrm{sc}})$-secure as long as the protocol uses direct reconciliation.

Proof. See e.g. Ref. [47]. □

The condition Eq. (107) is called the correctness condition and the condition Eq. (108) is called the secrecy condition.

Remark. *Proposition 1 holds for protocols with reverse reconciliation if the system A is replaced with B in the secrecy condition Eq. (108).*

B Lemmas and Theorems used in the main text

B.1 Lower bound on the fidelity to a coherent state

This section summarizes the technical result of Ref. [40].

Theorem 1. *For an integer $m \geq 0$ and a real number $r > 0$, let $\Lambda_{m,r}(\nu)$ $(\nu \geq 0)$ be a bounded function defined as*

$$\Lambda_{m,r}(\nu) \coloneqq e^{-r\nu}(1+r)L_m^{(1)}((1+r)\nu), \tag{109}$$

where $L_m^{(k)}$ is the associated Laguerre polynomials given by

$$L_n^{(k)}(\nu) \coloneqq (-1)^k \frac{d^k L_{n+k}(\nu)}{d\nu^k}, \tag{110}$$

$$L_n(\nu) \coloneqq \frac{e^\nu}{n!}\frac{d^n}{d\nu^n}(e^{-\nu}\nu^n). \tag{111}$$

Then, we have

$$\mathbb{E}_\rho[\Lambda_{m,r}(|\hat{\omega}|^2)] = \iint_{\omega\in\mathbb{C}} \frac{d^2\omega}{\pi}\Lambda_{m,r}(|\omega|^2)\langle\omega|\rho|\omega\rangle = \langle 0|\rho|0\rangle + \sum_{n=m+1}^{\infty}\frac{\langle n|\rho|n\rangle}{(1+r)^n}I_{n,m}, \tag{112}$$

where $I_{n,m}$ are constants satisfying $(-1)^m I_{n,m} > 0$.

As a Corollary, we obtain the following.

Corollary 1. *Let $|\beta\rangle$ $(\beta \in \mathbb{C})$ be the coherent state with amplitude β. Then, for any $\beta \in \mathbb{C}$ and for any odd positive integer m, we have*

$$\mathbb{E}_\rho[\Lambda_{m,r}(|\hat{\omega}-\beta|^2)] \leq \langle\beta|\rho|\beta\rangle. \tag{113}$$

The proofs of Theorem 1 and Corollary 1 are given in Ref. [40].

B.2 Bit error sampling

In this section, we summarize how to determine an upper bound on the bit error rate from the given sample. As explained in the main text, $N_{\rm smp}$ sampling rounds are randomly inserted in the actual protocol in which Alice and Bob announce their bit values if Bob's detection succeeds (in the same way as in the signal round). The number of "success" sampling rounds is denoted by $\hat{N}_{\rm smp}^{\rm suc}$, and the observed number of discrepancies between Alice and Bob is denoted by $\hat{E}_{\rm obs}$.

Let us first introduce a Chernoff-type bound for the hypergeometric distribution.

Lemma 1 (Tail bound for the hypergeometric distribution [69])**.** *Let $X_1,\ldots,X_N$ be a binary sequence, and M be the number of elements with $X_i = 1$, i.e, $M \coloneqq \sum_{i=1}^N X_i$. Let $\hat{Y}_1,\ldots,\hat{Y}_n$ $(n \leq N)$ be randomly sampled from $X_1,\ldots,X_N$ without replacement. Let $\hat{m} \coloneqq \sum_{i=1}^n \hat{Y}_i$ be the number of ones in $\hat{Y}_1,\ldots,\hat{Y}_n$. Then, for any $\delta \in [0, M/N]$, the following inequality holds:*

$$\Pr\left(\frac{\hat{m}}{n} \leq \frac{M}{N} - \delta\right) \leq 2^{-nD\left(\frac{M}{N}-\delta\middle\|\frac{M}{N}\right)}, \tag{114}$$

where $D(\cdot\|\cdot)$ is defined in Eq. (89).

Then, the following corollary is essential for the bit error sampling.

Corollary 2 (Estimation by the simple random sampling without replacement)**.** *Let $X_1,\ldots,X_N$ be a binary sequence with $M \coloneqq \sum_{i=1}^N X_i$. Let $\hat{Y}_1,\ldots,\hat{Y}_n$ $(n \leq N)$ be randomly sampled from $X_1,\ldots,X_N$ without replacement, and define $\hat{m} \coloneqq \sum_{i=1}^n \hat{Y}_i$. Then, for any $\epsilon \in (0,1)$, the following inequality holds:*

$$\Pr\left(\tilde{M}_{N,n,\epsilon}(\hat{m}) < M\right) \leq \epsilon, \tag{115}$$

where the function $\tilde{M}_{N,n,\epsilon}(m)$ *is defined to satisfy*

$$\frac{m}{n} \leq \frac{\tilde{M}_{N,n,\epsilon}(m)}{N} \leq 1 \tag{116}$$

and for $0 \leq m < n$,

$$D\left(m/n \middle\| \tilde{M}_{N,n,\epsilon}(m)/N\right) = -\frac{1}{n}\log\epsilon. \tag{117}$$

Proof. Let $f(M)$ be a function of M satisfying $0 \leq f(M)/n \leq M/N$. Then, from Lemma 1, we have

$$\Pr\left(\frac{\hat{m}}{n} \leq \frac{M}{N} - \left(\frac{M}{N} - \frac{f(M)}{n}\right)\right) \leq 2^{-nD\left(\frac{f(M)}{n}\middle\|\frac{M}{N}\right)}. \tag{118}$$

We set the function $f(M)$ to the restriction of the function $f_{N,n,\epsilon}(\bar{M})$ of the real number $\bar{M}$ that satisfies

$$D\left(f_{N,n,\epsilon}(\bar{M})/n \middle\| \bar{M}/N\right) = -\frac{1}{n}\log\epsilon, \tag{119}$$

for $\bar{M} \in [(1-\sqrt[n]{\epsilon})N, N)$. The function $f_{N,n,\epsilon}(\bar{M})$ increases monotonically with increasing $\bar{M}$ in $[(1-\sqrt[n]{\epsilon})N, N)$, and its image lies in $[0, n)$. Thus, from Eq. (118), we have

$$\Pr\left(f^{-1}_{N,n,\epsilon}(\hat{m}) \leq M\right) \leq \epsilon \tag{120}$$

for any $\hat{m} \in [0, n)$. We define the function $\tilde{M}_{N,n,\epsilon}(m) \coloneqq f^{-1}_{N,n,\epsilon}(m)$ for $m \in [0, n)$. To incorporate the case $\hat{m} = n$, we use the following weaker condition that trivially follows from Eq. (120):

$$\Pr\left(\tilde{M}_{N,n,\epsilon}(\hat{m}) < M\right) \leq \epsilon, \tag{121}$$

and define $\tilde{M}_{N,n,\epsilon}(n) = N$ so that the above holds also for $\hat{m} = n$. These show that Eq. (115) holds while $\tilde{M}_{N,n,\epsilon}(m)$ satisfies Eqs. (116) and (117) by construction in Eq. (119). □

With Corollary 2, we can bound the number of total bit-error events from the sample under the given failure probability $\varepsilon_{\mathrm{cor}}/2$ by setting $N = \hat{N}^{\mathrm{suc}} + \hat{N}^{\mathrm{suc}}_{\mathrm{smp}}$, $n = \hat{N}^{\mathrm{suc}}_{\mathrm{smp}}$, and $\epsilon = \varepsilon_{\mathrm{cor}}/2$ for $\tilde{M}_{N,n,\epsilon}$. As a result, we have the following statement; the number E of bit errors in $\hat{N}^{\mathrm{suc}}$-bit sifted key is bounded from above by

$$\Pr\left(E \leq \tilde{M}_{\hat{N}^{\mathrm{suc}}+\hat{N}^{\mathrm{suc}}_{\mathrm{smp}},\hat{N}^{\mathrm{suc}}_{\mathrm{smp}},\varepsilon_{\mathrm{cor}}/2}(\hat{E}_{\mathrm{obs}}) - \hat{E}_{\mathrm{obs}}\right) \geq 1 - \varepsilon_{\mathrm{cor}}/2. \tag{122}$$

Thus, we can define an upper bound e_{qber} of the bit error rate as in Eq. (3), which holds with probability no smaller than $1 - \varepsilon_{\mathrm{cor}}/2$.

B.3 Azuma's inequality combined with the Doob decomposition

This section summarizes the Azuma's inequality [66, 70, 71] adapted to our security analysis. The main claim is the following.

Proposition 2. *Let* $\{\hat{X}^{(i)}\}_{i=1,\ldots,N}$ *be a sequence of random variables and* $\hat{X}^{(<i)}$ *be* $\{\hat{X}^{(k)}\}_{k=0,\ldots,i-1}$, *where* $\hat{X}^{(0)}$ *is defined to be zero. Let* $\{a_i\}_{i=1,\ldots,N}$ *and* $\{b_i\}_{i=1,\ldots,N}$ *be predictable processes with respect to* $\{\hat{X}^{(k)}\}_{k=0,\ldots,N}$, *i.e.,* a_i *and* b_i *are constants conditioned on* $\hat{X}^{(<i)}$. *Assume the following condition is satisfied for all* $i \in \{1, \ldots, N\}$:

$$a_i \leq \hat{X}^{(i)} \leq b_i. \tag{123}$$

Then, for any $t \geq 0$, *we have*

$$\Pr\left(\sum_{i=1}^{N}\left(\hat{X}^{(i)} - \mathbb{E}[\hat{X}^{(i)} \mid \hat{X}^{(<i)}]\right) \geq t\right) \leq \exp\left(-\frac{2t^2}{\sum_{i=1}^{N}(b_i - a_i)^2}\right). \tag{124}$$

Proof. For $1 \leq i \leq N$, let $\hat{Y}^{(i)}$ be defined as

$$\hat{Y}^{(i)} \coloneqq \sum_{k=1}^{i} (\hat{X}^{(k)} - \mathbb{E}[\hat{X}^{(k)} \mid \hat{X}^{(<k)}]). \tag{125}$$

Then, the sequence $\{\hat{Y}^{(i)}\}_{i=1,\ldots,N}$ is a martingale with respect to $\{\hat{X}^{(k)}\}_{k=0,\ldots,N}$, since $\hat{Y}^{(i)}$ satisfies

$$\mathbb{E}[\hat{Y}^{(i)} \mid \hat{X}^{(<i)}] = \sum_{k=1}^{i} \left(\mathbb{E}[\hat{X}^{(k)} \mid \hat{X}^{(<i)}] - \mathbb{E}\left[\mathbb{E}[\hat{X}^{(k)} \mid \hat{X}^{(<k)}] \,\middle|\, \hat{X}^{(<i)} \right] \right) \tag{126}$$

$$= \sum_{k=1}^{i-1} (\hat{X}^{(k)} - \mathbb{E}[\hat{X}^{(k)} \mid \hat{X}^{(<k)}]) \tag{127}$$

$$= \hat{Y}^{(i-1)} \tag{128}$$

for $1 \leq i \leq N$. (Note that $\hat{Y}^{(0)} \coloneqq 0$.) The second equality follows from the fact that $\mathbb{E}[\hat{X}^{(k)} \mid \hat{X}^{(<i)}] = \hat{X}^{(k)}$ holds when $k < i$. Furthermore, the sequence $\{\hat{Y}^{(i)}\}_{i=1,\ldots,N}$ satisfies

$$a_i - \mathbb{E}[\hat{X}^{(i)} \mid \hat{X}^{(<i)}] \leq \hat{Y}^{(i)} - \hat{Y}^{(i-1)} \leq b_i - \mathbb{E}[\hat{X}^{(i)} \mid \hat{X}^{(<i)}], \tag{129}$$

for $1 \leq i \leq n$. Since $a_i - \mathbb{E}[\hat{X}^{(i)} \mid \hat{X}^{(<i)}]$ and $b_i - \mathbb{E}[\hat{X}^{(i)} \mid \hat{X}^{(<i)}]$ are predictable process with respect to $\{\hat{X}^{(k)}\}_{k=0,\ldots,N}$, we can apply Azuma's inequality [66] to the sequence $\{\hat{Y}^{(i)}\}_{i=1,\ldots,N}$ and prove the statement. □

C Proof of the operator inequality

In this section, we prove the inequality (81) used in the security proof in the main text. We first prove the following lemma.

Lemma 2. *Let $\Pi_\pm$ be orthogonal projections that have the rank no smaller than three or infinite. Let M be a self-adjoint operator satisfying $M = (\Pi_+ + \Pi_-)M(\Pi_+ + \Pi_-) \leq \alpha(\Pi_+ + \Pi_-)$, where α is a real constant. Let $|\psi\rangle$ be a vector satisfying $(\Pi_+ + \Pi_-)|\psi\rangle = |\psi\rangle$ and $\Pi_\pm |\psi\rangle \neq 0$. Assume $\Pi_\pm |\psi\rangle$ are not proportional to eigenvectors of $\Pi_\pm M \Pi_+$ (if they have). Define the following quantities with respect to $|\psi\rangle$:*

$$C_\pm \coloneqq \langle\psi| \Pi_\pm |\psi\rangle \ (> 0), \tag{130}$$

$$\lambda_{++} \coloneqq C_+^{-1} \langle\psi| M_{++} |\psi\rangle, \quad \lambda_{--} \coloneqq C_-^{-1} \langle\psi| M_{--} |\psi\rangle, \tag{131}$$

$$\lambda_{+-} \coloneqq (C_+ C_-)^{-\frac{1}{2}} \langle\psi| M_{+-} |\psi\rangle, \quad \lambda_{-+} \coloneqq \lambda_{+-}^*, \tag{132}$$

$$\sigma_{\pm+} \coloneqq \left(C_+^{-1} \| M_{\pm+} |\psi\rangle \|^2 - |\lambda_{\pm+}|^2 \right)^{\frac{1}{2}}, \tag{133}$$

$$\sigma_{\pm-} \coloneqq \sigma_{\pm+}^{-1} \left((C_+ C_-)^{-\frac{1}{2}} \langle\psi| M_{+\pm} M_{\pm-} |\psi\rangle - \lambda_{+-} \lambda_{\pm\pm} \right), \tag{134}$$

$$\Delta_{\pm-} \coloneqq \left(C_-^{-1} \| M_{\pm-} |\psi\rangle \|^2 - |\lambda_{\pm-}|^2 - |\sigma_{\pm-}|^2 \right)^{\frac{1}{2}}, \tag{135}$$

where M_{++}, M_{--}, M_{+-}, and M_{-+} are given respectively by

$$M_{\pm\pm} \coloneqq \Pi_\pm M \Pi_\pm, \quad M_{+-} \coloneqq \Pi_+ M \Pi_-, \quad M_{-+} \coloneqq M_{+-}^\dagger. \tag{136}$$

Then, for any real numbers $\gamma_\pm$, we have

$$\sigma_{\sup}(M + |\psi\rangle\langle\psi| - \gamma_+ \Pi_+ - \gamma_- \Pi_-) \leq \sigma_{\sup}(M_{6\mathrm{d}}), \tag{137}$$

where $\sigma_{\sup}(X)$ denotes the supremum of the spectrum of the operator X, and $M_{6\mathrm{d}}$ is given by

$$M_{6\mathrm{d}} \coloneqq \begin{pmatrix} \alpha - \gamma_+ & 0 & 0 & \Delta_{+-} & 0 & 0 \\ 0 & \alpha - \gamma_+ & \sigma_{++} & \sigma_{+-} & 0 & 0 \\ 0 & \sigma_{++} & C_+ + \lambda_{++} - \gamma_+ & \sqrt{C_+ C_-} + \lambda_{+-} & \sigma_{-+} & 0 \\ \Delta_{+-} & \sigma_{+-}^* & \sqrt{C_+ C_-} + \lambda_{-+} & C_- + \lambda_{--} - \gamma_- & \sigma_{--}^* & \Delta_{--} \\ 0 & 0 & \sigma_{-+} & \sigma_{--} & \alpha - \gamma_- & 0 \\ 0 & 0 & 0 & \Delta_{--} & 0 & \alpha - \gamma_- \end{pmatrix}. \tag{138}$$

Proof. We are able to choose orthonormal vectors $\{|e_+^{(1)}\rangle, |e_+^{(2)}\rangle, |e_+^{(3)}\rangle\}$ and $\{|e_-^{(1)}\rangle, |e_-^{(2)}\rangle, |e_-^{(3)}\rangle\}$ in the domains of Π_+ and Π_-, respectively, to satisfy

$$\sqrt{C_\pm}\left|e_\pm^{(1)}\right\rangle = \Pi_\pm|\psi\rangle, \tag{139}$$

$$M\left|e_+^{(1)}\right\rangle = (M_{++}+M_{-+})\left|e_+^{(1)}\right\rangle = \lambda_{++}\left|e_+^{(1)}\right\rangle + \sigma_{++}\left|e_+^{(2)}\right\rangle + \lambda_{-+}\left|e_-^{(1)}\right\rangle + \sigma_{-+}\left|e_-^{(2)}\right\rangle, \tag{140}$$

$$\begin{aligned} M\left|e_-^{(1)}\right\rangle = (M_{+-}+M_{--})\left|e_-^{(1)}\right\rangle &= \lambda_{+-}\left|e_+^{(1)}\right\rangle + \sigma_{+-}\left|e_+^{(2)}\right\rangle + \Delta_{+-}\left|e_+^{(3)}\right\rangle \\ &\quad + \lambda_{--}\left|e_-^{(1)}\right\rangle + \sigma_{--}\left|e_-^{(2)}\right\rangle + \Delta_{--}\left|e_-^{(3)}\right\rangle. \end{aligned} \tag{141}$$

The coefficients satisfy Eqs. (130)–(136), and $M = (\Pi_+ + \Pi_-)M(\Pi_+ + \Pi_-)$. This can be seen by applying the following general property. For an operator A and a unit vector $|v\rangle$, $A|v\rangle$ can always be written as $A|v\rangle = a|v\rangle + b|v^\perp\rangle$, where $|v^\perp\rangle$ is a unit vector orthogonal to $|v\rangle$, b is a nonnegative coefficient satisfying $b^2 = \|A|v\rangle\|^2 - |a|^2$, and $a = \langle v|A|v\rangle$. From $(\Pi_+ + \Pi_-)|\psi\rangle = |\psi\rangle$, we have

$$|\psi\rangle = \sqrt{C_+}\left|e_+^{(1)}\right\rangle + \sqrt{C_-}\left|e_-^{(1)}\right\rangle. \tag{142}$$

Let us now define the following projection operators:

$$\Pi_\pm^{(j)} := \left|e_\pm^{(j)}\right\rangle\!\left\langle e_\pm^{(j)}\right| \quad (j=1,2,3), \tag{143}$$

$$\Pi_\pm^{(\geq 2)} := \Pi_\pm - \Pi_\pm^{(1)}, \tag{144}$$

$$\Pi_\pm^{(\geq 4)} := \Pi_\pm^{(\geq 2)} - \Pi_\pm^{(2)} - \Pi_\pm^{(3)}. \tag{145}$$

Since Eqs. (140) and (141) imply $(\Pi_+^{(\geq 4)} + \Pi_-^{(\geq 4)})M(\Pi_+^{(1)} + \Pi_-^{(1)}) = 0$, we have

$$M = (\Pi_+ + \Pi_-)M(\Pi_+ + \Pi_-) \tag{146}$$

$$\begin{aligned} &= (\Pi_+^{(1)} + \Pi_-^{(1)})M(\Pi_+^{(1)} + \Pi_-^{(1)}) + (\Pi_+^{(2)} + \Pi_+^{(3)} + \Pi_-^{(2)} + \Pi_-^{(3)})M(\Pi_+^{(1)} + \Pi_-^{(1)}) \\ &\quad + (\Pi_+^{(1)} + \Pi_-^{(1)})M(\Pi_+^{(2)} + \Pi_+^{(3)} + \Pi_-^{(2)} + \Pi_-^{(3)}) + (\Pi_+^{(\geq 2)} + \Pi_-^{(\geq 2)})M(\Pi_+^{(\geq 2)} + \Pi_-^{(\geq 2)}) \end{aligned} \tag{147}$$

$$\begin{aligned} &\leq \lambda_{++}\Pi_+^{(1)} + \lambda_{--}\Pi_-^{(1)} + \lambda_{+-}\left|e_+^{(1)}\right\rangle\!\left\langle e_-^{(1)}\right| + \lambda_{-+}\left|e_-^{(1)}\right\rangle\!\left\langle e_+^{(1)}\right| \\ &\quad + \Big(\sigma_{++}\left|e_+^{(2)}\right\rangle\!\left\langle e_+^{(1)}\right| + \sigma_{-+}\left|e_-^{(2)}\right\rangle\!\left\langle e_+^{(1)}\right| + \sigma_{+-}\left|e_+^{(2)}\right\rangle\!\left\langle e_-^{(1)}\right| \\ &\qquad + \Delta_{+-}\left|e_+^{(3)}\right\rangle\!\left\langle e_-^{(1)}\right| + \sigma_{--}\left|e_-^{(2)}\right\rangle\!\left\langle e_-^{(1)}\right| + \Delta_{--}\left|e_-^{(3)}\right\rangle\!\left\langle e_-^{(1)}\right|\Big) + (\quad \text{h.c.} \quad) \\ &\quad + \alpha(\Pi_+^{(\geq 2)} + \Pi_-^{(\geq 2)}), \end{aligned} \tag{148}$$

where h.c. denotes the hermitian conjugate of the terms in the preceding parenthesis. The last inequality comes from $M \leq \alpha(\Pi_+ + \Pi_-)$. Using Eq. (148), we have

$$M + |\psi\rangle\langle\psi| - \gamma_+\Pi_+ - \gamma_-\Pi_- \leq M_{6\mathrm{d}} \oplus (\alpha-\gamma_+)\Pi_+^{(\geq 4)} \oplus (\alpha-\gamma_-)\Pi_-^{(\geq 4)}, \tag{149}$$

where $M_{6\mathrm{d}}$ is given in Eq. (138) with the basis $\{|e_+^{(3)}\rangle, |e_+^{(2)}\rangle, |e_+^{(1)}\rangle, |e_-^{(1)}\rangle, |e_-^{(2)}\rangle, |e_-^{(3)}\rangle\}$. Since $\alpha - \gamma_\pm = \langle e_\pm^{(3)}|M_{6\mathrm{d}}|e_\pm^{(3)}\rangle \leq \sigma_{\sup}(M_{6\mathrm{d}})$, the supremum of the spectrum of the right-hand side of Eq. (149) is equal to the maximum eigenvalue of the six-dimensional matrix $M_{6\mathrm{d}}$. We then obtain Eq. (137). □

As a corollary of this lemma, we obtain the followings. First, we consider Homodyne protocol.

Corollary 3. *Let $|\beta\rangle$ be a coherent state and $\theta_{\mu,\beta}^{\mathrm{hom}}(x)$ be defined to satisfy*

$$|\theta_{\mu,\beta}^{\mathrm{hom}}(x)| \leq \frac{\pi}{2}, \qquad \tan\theta_{\mu,\beta}^{\mathrm{hom}}(x) = e^{-2(\mu-\beta^2)}\sinh(4\beta x). \tag{150}$$

Let $\Pi_{\mathrm{ev(od)}}$ *and* $M^{\mathrm{hom}}[\kappa,\gamma]$ *be as defined in the main text, and let* $M^{\mathrm{hom}}_{\mathrm{oo}}$, $M^{\mathrm{hom}}_{\mathrm{ee}}$, $M^{\mathrm{hom}}_{(\pm,\mathrm{o})(\mp,\mathrm{e})}$, *and* $M^{\mathrm{hom}}_{(\mp,\mathrm{e})(\pm,\mathrm{o})}$ *be defined as follows:*

$$M^{\mathrm{hom}}_{\mathrm{oo}} \coloneqq \int_{-\infty}^{\infty} f_{\mathrm{suc}}(x)[1+\cos\theta^{\mathrm{hom}}_{\mu,\beta}(x)]dx\ \Pi_{\mathrm{od}}\,|x\rangle\langle x|\,\Pi_{\mathrm{od}}, \tag{151}$$

$$M^{\mathrm{hom}}_{\mathrm{ee}} \coloneqq \int_{-\infty}^{\infty} f_{\mathrm{suc}}(x)[1-\cos\theta^{\mathrm{hom}}_{\mu,\beta}(x)]dx\ \Pi_{\mathrm{ev}}\,|x\rangle\langle x|\,\Pi_{\mathrm{ev}}, \tag{152}$$

$$M^{\mathrm{hom}}_{(+,\mathrm{o})(-,\mathrm{e})} \coloneqq \int_{-\infty}^{\infty} f_{\mathrm{suc}}(x)\sin\theta^{\mathrm{hom}}_{\mu,\beta}(x)\,dx\ \Pi_{\mathrm{od}}\,|x\rangle\langle x|\,\Pi_{\mathrm{ev}}, \tag{153}$$

$$M^{\mathrm{hom}}_{(-,\mathrm{e})(+,\mathrm{o})} \coloneqq \left(M^{\mathrm{hom}}_{(+,\mathrm{o})(-,\mathrm{e})}\right)^{\dagger}, \tag{154}$$

$$M^{\mathrm{hom}}_{(-,\mathrm{o})(+,\mathrm{e})} \coloneqq \int_{-\infty}^{\infty} -f_{\mathrm{suc}}(x)\ \sin\theta^{\mathrm{hom}}_{\mu,\beta}(x)\,dx\ \Pi_{\mathrm{od}}\,|x\rangle\langle x|\,\Pi_{\mathrm{ev}} = -M^{\mathrm{hom}}_{(+,\mathrm{o})(-,\mathrm{e})}, \tag{155}$$

$$M^{\mathrm{hom}}_{(+,\mathrm{e})(-,\mathrm{o})} \coloneqq \left(M^{\mathrm{hom}}_{(-,\mathrm{o})(+,\mathrm{e})}\right)^{\dagger} = -\left(M^{\mathrm{hom}}_{(+,\mathrm{o})(-,\mathrm{e})}\right)^{\dagger}. \tag{156}$$

Define the following (real) parameters:

$$C_{\mathrm{o}} \coloneqq \langle\beta|\,\Pi_{\mathrm{od}}\,|\beta\rangle = e^{-|\beta|^2}\sinh|\beta|^2, \quad C_{\mathrm{e}} \coloneqq \langle\beta|\,\Pi_{\mathrm{ev}}\,|\beta\rangle = e^{-|\beta|^2}\cosh|\beta|^2, \tag{157}$$

$$\lambda^{\mathrm{hom}}_{\mathrm{oo}} \coloneqq C_{\mathrm{o}}^{-1}\,\langle\beta|\,M^{\mathrm{hom}}_{\mathrm{oo}}\,|\beta\rangle\,, \quad \lambda^{\mathrm{hom}}_{\mathrm{ee}} \coloneqq C_{\mathrm{e}}^{-1}\,\langle\beta|\,M^{\mathrm{hom}}_{\mathrm{ee}}\,|\beta\rangle\,, \tag{158}$$

$$\lambda^{\mathrm{hom}}_{(+,\mathrm{o})(-,\mathrm{e})} \coloneqq (C_{\mathrm{o}}C_{\mathrm{e}})^{-\frac{1}{2}}\,\langle\beta|\,M^{\mathrm{hom}}_{(+,\mathrm{o})(-,\mathrm{e})}\,|\beta\rangle = (\lambda^{\mathrm{hom}}_{(+,\mathrm{o})(-,\mathrm{e})})^{*}, \tag{159}$$

$$\sigma^{\mathrm{hom}}_{\mathrm{oo}} \coloneqq \left(C_{\mathrm{o}}^{-1}\|M^{\mathrm{hom}}_{\mathrm{oo}}\,|\beta\rangle\,\|^2 - (\lambda^{\mathrm{hom}}_{\mathrm{oo}})^2\right)^{\frac{1}{2}}, \tag{160}$$

$$\sigma^{\mathrm{hom}}_{\mathrm{eo}} \coloneqq \left(C_{\mathrm{o}}^{-1}\|M^{\mathrm{hom}}_{(-,\mathrm{e})(+,\mathrm{o})}\,|\beta\rangle\,\|^2 - |\lambda^{\mathrm{hom}}_{(+,\mathrm{o})(-,\mathrm{e})}|^2\right)^{\frac{1}{2}}, \tag{161}$$

$$\sigma^{\mathrm{hom}}_{(+,\mathrm{o})(-,\mathrm{e})} \coloneqq (\sigma^{\mathrm{hom}}_{\mathrm{oo}})^{-1}\left((C_{\mathrm{o}}C_{\mathrm{e}})^{-\frac{1}{2}}\,\langle\beta|\,M^{\mathrm{hom}}_{\mathrm{oo}}M^{\mathrm{hom}}_{(+,\mathrm{o})(-,\mathrm{e})}\,|\beta\rangle - \lambda^{\mathrm{hom}}_{\mathrm{oo}}\lambda^{\mathrm{hom}}_{(+,\mathrm{o})(-,\mathrm{e})}\right) = (\sigma^{\mathrm{hom}}_{(+,\mathrm{o})(-,\mathrm{e})})^{*}, \tag{162}$$

$$\sigma^{\mathrm{hom}}_{(-,\mathrm{e})(-,\mathrm{e})} \coloneqq (\sigma^{\mathrm{hom}}_{(-,\mathrm{e})(+,\mathrm{o})})^{-1}\left((C_{\mathrm{o}}C_{\mathrm{e}})^{-\frac{1}{2}}\,\langle\beta|\,M^{\mathrm{hom}}_{(+,\mathrm{o})(-,\mathrm{e})}M^{\mathrm{hom}}_{\mathrm{ee}}\,|\beta\rangle - \lambda^{\mathrm{hom}}_{(+,\mathrm{o})(-,\mathrm{e})}\lambda^{\mathrm{hom}}_{\mathrm{ee}}\right) = (\sigma^{\mathrm{hom}}_{(-,\mathrm{e})(-,\mathrm{e})})^{*}, \tag{163}$$

$$\Delta^{\mathrm{hom}}_{\mathrm{oe}} \coloneqq \left(C_{\mathrm{e}}^{-1}\|M^{\mathrm{hom}}_{(+,\mathrm{o})(-,\mathrm{e})}\,|\beta\rangle\,\|^2 - |\lambda^{\mathrm{hom}}_{(+,\mathrm{o})(-,\mathrm{e})}|^2 - |\sigma^{\mathrm{hom}}_{(+,\mathrm{o})(-,\mathrm{e})}|^2\right)^{\frac{1}{2}}, \tag{164}$$

$$\Delta^{\mathrm{hom}}_{\mathrm{ee}} \coloneqq \left(C_{\mathrm{e}}^{-1}\|M^{\mathrm{hom}}_{\mathrm{ee}}\,|\beta\rangle\,\|^2 - (\lambda^{\mathrm{hom}}_{\mathrm{ee}})^2 - |\sigma^{\mathrm{hom}}_{(-,\mathrm{e})(-,\mathrm{e})}|^2\right)^{\frac{1}{2}}. \tag{165}$$

Define the following two matrices $M^{(0)}_{\mathrm{6d}}$ *and* $M^{(1)}_{\mathrm{6d}}$.

$$M^{(0)}_{\mathrm{6d}} \coloneqq \begin{pmatrix} 1 & 0 & 0 & \Delta^{\mathrm{hom}}_{\mathrm{oe}} & 0 & 0 \\ 0 & 1 & \sigma^{\mathrm{hom}}_{\mathrm{oo}} & \sigma^{\mathrm{hom}}_{(+,\mathrm{o})(-,\mathrm{e})} & 0 & 0 \\ 0 & \sigma^{\mathrm{hom}}_{\mathrm{oo}} & \kappa C_{\mathrm{o}} + \lambda^{\mathrm{hom}}_{\mathrm{oo}} & \kappa\sqrt{C_{\mathrm{o}}C_{\mathrm{e}}} + \lambda^{\mathrm{hom}}_{(+,\mathrm{o})(-,\mathrm{e})} & \sigma^{\mathrm{hom}}_{\mathrm{eo}} & 0 \\ \Delta^{\mathrm{hom}}_{\mathrm{oe}} & \sigma^{\mathrm{hom}}_{(+,\mathrm{o})(-,\mathrm{e})} & \kappa\sqrt{C_{\mathrm{o}}C_{\mathrm{e}}} + \lambda^{\mathrm{hom}}_{(+,\mathrm{o})(-,\mathrm{e})} & \kappa C_{\mathrm{e}} + \lambda^{\mathrm{hom}}_{\mathrm{ee}} - \gamma & \sigma^{\mathrm{hom}}_{(-,\mathrm{e})(-,\mathrm{e})} & \Delta^{\mathrm{hom}}_{\mathrm{ee}} \\ 0 & 0 & \sigma^{\mathrm{hom}}_{\mathrm{eo}} & \sigma^{\mathrm{hom}}_{(-,\mathrm{e})(-,\mathrm{e})} & 1-\gamma & 0 \\ 0 & 0 & 0 & \Delta^{\mathrm{hom}}_{\mathrm{ee}} & 0 & 1-\gamma \end{pmatrix}, \tag{166}$$

$$M^{(1)}_{\mathrm{6d}} \coloneqq \begin{pmatrix} 1-\gamma & 0 & 0 & \Delta^{\mathrm{hom}}_{\mathrm{oe}} & 0 & 0 \\ 0 & 1-\gamma & \sigma^{\mathrm{hom}}_{\mathrm{oo}} & -\sigma^{\mathrm{hom}}_{(+,\mathrm{o})(-,\mathrm{e})} & 0 & 0 \\ 0 & \sigma^{\mathrm{hom}}_{\mathrm{oo}} & \kappa C_{\mathrm{o}} + \lambda^{\mathrm{hom}}_{\mathrm{oo}} - \gamma & \kappa\sqrt{C_{\mathrm{o}}C_{\mathrm{e}}} - \lambda^{\mathrm{hom}}_{(+,\mathrm{o})(-,\mathrm{e})} & \sigma^{\mathrm{hom}}_{\mathrm{eo}} & 0 \\ \Delta^{\mathrm{hom}}_{\mathrm{oe}} & -\sigma^{\mathrm{hom}}_{(+,\mathrm{o})(-,\mathrm{e})} & \kappa\sqrt{C_{\mathrm{o}}C_{\mathrm{e}}} - \lambda^{\mathrm{hom}}_{(+,\mathrm{o})(-,\mathrm{e})} & \kappa C_{\mathrm{e}} + \lambda^{\mathrm{hom}}_{\mathrm{ee}} & -\sigma^{\mathrm{hom}}_{(-,\mathrm{e})(-,\mathrm{e})} & \Delta^{\mathrm{hom}}_{\mathrm{ee}} \\ 0 & 0 & \sigma^{\mathrm{hom}}_{\mathrm{eo}} & -\sigma^{\mathrm{hom}}_{(-,\mathrm{e})(-,\mathrm{e})} & 1 & 0 \\ 0 & 0 & 0 & \Delta^{\mathrm{hom}}_{\mathrm{ee}} & 0 & 1 \end{pmatrix}. \tag{167}$$

Define a convex function

$$B^{\mathrm{hom}}(\kappa,\gamma) \coloneqq \max\{\sigma_{\mathrm{sup}}(M_{\mathrm{6d}}^{(0)}), \sigma_{\mathrm{sup}}(M_{\mathrm{6d}}^{(1)})\}. \tag{168}$$

Then, for $\kappa,\gamma \geq 0$, we have

$$M^{\mathrm{hom}}[\kappa,\gamma] \leq B^{\mathrm{hom}}(\kappa,\gamma) I_{AC}. \tag{169}$$

Proof. We first derive the explicit form of $|u_{\pm}^{\mathrm{hom}}(x)\rangle_A$ introduced in Eq. (43). Notice that

$$1 - 2q_{\mu,\beta} = e^{-2(\mu-\beta^2)}, \tag{170}$$

$$\sqrt{\frac{g_{\beta,1/4}(x)}{g_{-\beta,1/4}(x)}} = e^{4\beta x}. \tag{171}$$

Let $\theta(x)$ be defined to satisfy

$$|\theta(x)| < \frac{\pi}{2}, \qquad \tan\theta(x) = \mathrm{Tr}\left(Z_A \langle 0|_B \tau_{AB}^{\mathrm{hom}}(x) |1\rangle_B\right) \Big/ \mathrm{Tr}\left(X_A \langle 0|_B \tau_{AB}^{\mathrm{hom}}(x) |1\rangle_B\right). \tag{172}$$

Noticing that $\mathrm{Tr}\left(Y_A \langle 0|_B \tau_{AB}^{\mathrm{hom}}(x) |1\rangle_B\right) = 0$, we have

$$|u_{\pm}^{\mathrm{hom}}(x)\rangle_A = \cos\frac{\theta(x)}{2} |\pm\rangle_A \pm \sin\frac{\theta(x)}{2} |\mp\rangle_A. \tag{173}$$

From Eqs. (42), (170), (171), and (172), we can see that $\theta(x)$ coincides with $\theta_{\mu,\beta}^{\mathrm{hom}}(x)$ defined in Eq. (150). We now observe that

$$|\langle +|u_+^{\mathrm{hom}}(x)\rangle|^2 = |\langle -|u_-^{\mathrm{hom}}(x)\rangle|^2 = \cos^2\left(\frac{\theta_{\mu,\beta}^{\mathrm{hom}}(x)}{2}\right) = \frac{1+\cos\theta_{\mu,\beta}^{\mathrm{hom}}(x)}{2}, \tag{174}$$

$$|\langle -|u_+^{\mathrm{hom}}(x)\rangle|^2 = |\langle +|u_-^{\mathrm{hom}}(x)\rangle|^2 = \sin^2\left(\frac{\theta_{\mu,\beta}^{\mathrm{hom}}(x)}{2}\right) = \frac{1-\cos\theta_{\mu,\beta}^{\mathrm{hom}}(x)}{2}, \tag{175}$$

$$\begin{aligned} &\langle +|u_+^{\mathrm{hom}}(x)\rangle\langle u_+^{\mathrm{hom}}(x)|-\rangle = \langle -|u_+^{\mathrm{hom}}(x)\rangle\langle u_+^{\mathrm{hom}}(x)|+\rangle = \sin\left(\frac{\theta_{\mu,\beta}^{\mathrm{hom}}(x)}{2}\right)\cos\left(\frac{\theta_{\mu,\beta}^{\mathrm{hom}}(x)}{2}\right) \\ &= -\langle +|u_-^{\mathrm{hom}}(x)\rangle\langle u_-^{\mathrm{hom}}(x)|-\rangle = -\langle -|u_-^{\mathrm{hom}}(x)\rangle\langle u_-^{\mathrm{hom}}(x)|+\rangle = \frac{\sin\theta_{\mu,\beta}^{\mathrm{hom}}(x)}{2}. \end{aligned} \tag{176}$$

From Eq. (65) as well as Eqs. (75)–(80), it is obvious that

$$M^{\mathrm{hom}}[\kappa,\gamma] = \Pi_{AC}^{(+,\mathrm{od}),(-,\mathrm{ev})} M^{\mathrm{hom}}[\kappa,\gamma] \Pi_{AC}^{(+,\mathrm{od}),(-,\mathrm{ev})} + \Pi_{AC}^{(-,\mathrm{od}),(+,\mathrm{ev})} M^{\mathrm{hom}}[\kappa,\gamma] \Pi_{AC}^{(-,\mathrm{od}),(+,\mathrm{ev})}, \tag{177}$$

where the two orthogonal projections $\Pi_{AC}^{(+,\mathrm{od}),(-,\mathrm{ev})}$ and $\Pi_{AC}^{(-,\mathrm{od}),(+,\mathrm{ev})}$ are defined in Eqs. (66) and (67). Then we apply Lemma 2 respectively to the operators $\Pi_{AC}^{(+,\mathrm{od}),(-,\mathrm{ev})} M^{\mathrm{hom}}[\kappa,\gamma] \Pi_{AC}^{(+,\mathrm{od}),(-,\mathrm{ev})}$ and $\Pi_{AC}^{(-,\mathrm{od}),(+,\mathrm{ev})} M^{\mathrm{hom}}[\kappa,\gamma] \Pi_{AC}^{(-,\mathrm{od}),(+,\mathrm{ev})}$. For $\Pi_{AC}^{(+,\mathrm{od}),(-,\mathrm{ev})} M^{\mathrm{hom}}[\kappa,\gamma] \Pi_{AC}^{(+,\mathrm{od}),(-,\mathrm{ev})}$, we set, by using Eqs. (174)–(176), that

$$\Pi_{\pm} = |\pm\rangle\langle\pm|_A \otimes \Pi_{\mathrm{od(ev)}}, \tag{178}$$

$$M = \Pi_{AC}^{(+,\mathrm{od}),(-,\mathrm{ev})} M_{\mathrm{ph}}^{\mathrm{hom}} \Pi_{AC}^{(+,\mathrm{od}),(-,\mathrm{ev})} \tag{179}$$

$$= |+\rangle\langle+|_A \otimes M_{\mathrm{oo}}^{\mathrm{hom}} + |-\rangle\langle-|_A \otimes M_{\mathrm{ee}}^{\mathrm{hom}} + \left(|+\rangle\langle-|_A \otimes M_{(+,\mathrm{o})(-,\mathrm{e})}^{\mathrm{hom}} + |-\rangle\langle+|_A \otimes M_{(-,\mathrm{e})(+,\mathrm{o})}^{\mathrm{hom}}\right), \tag{180}$$

$$|\psi\rangle = \sqrt{\kappa}\, |\phi_-\rangle_{AC}, \tag{181}$$

$$\alpha = 1, \quad \gamma_+ = 0, \quad \gamma_- = \gamma, \tag{182}$$

where $|\phi_-\rangle_{AC}$ is defined in Eq. (30). Since so-defined M only has continuous spectrum, we can apply Lemma 2 and obtain

$$\sigma_{\mathrm{sup}}\left(\Pi_{AC}^{(+,\mathrm{od}),(-,\mathrm{ev})} M^{\mathrm{hom}}[\kappa,\gamma] \Pi_{AC}^{(+,\mathrm{od}),(-,\mathrm{ev})}\right) \leq \sigma_{\mathrm{sup}}(M_{\mathrm{6d}}^{(0)}). \tag{183}$$

In the same way, we apply Lemma 2 to $\Pi_{AC}^{(-,\mathrm{od}),(+,\mathrm{ev})} M^{\mathrm{hom}}[\kappa,\gamma]\, \Pi_{AC}^{(-,\mathrm{od}),(+,\mathrm{ev})}$. Using Eqs. (174)–(176), we set

$$\Pi_{\pm} = |\mp\rangle\langle\mp|_A \otimes \Pi_{\mathrm{od(ev)}}, \tag{184}$$

$$M = \Pi_{AC}^{(-,\mathrm{od}),(+,\mathrm{ev})} M_{\mathrm{ph}}^{\mathrm{hom}} \Pi_{AC}^{(-,\mathrm{od}),(+,\mathrm{ev})} \tag{185}$$

$$= |-\rangle\langle-|_A \otimes M_{\mathrm{oo}}^{\mathrm{hom}} + |+\rangle\langle+|_A \otimes M_{\mathrm{ee}}^{\mathrm{hom}} + \Big(|-\rangle\langle+|_A \otimes M_{(-,\mathrm{o})(+,\mathrm{e})}^{\mathrm{hom}} + |+\rangle\langle-|_A \otimes M_{(+,\mathrm{e})(-,\mathrm{o})}^{\mathrm{hom}}\Big), \tag{186}$$

$$= |-\rangle\langle-|_A \otimes M_{\mathrm{oo}}^{\mathrm{hom}} + |+\rangle\langle+|_A \otimes M_{\mathrm{ee}}^{\mathrm{hom}} - \Big(|-\rangle\langle+|_A \otimes M_{(+,\mathrm{o})(-,\mathrm{e})}^{\mathrm{hom}} + |+\rangle\langle-|_A \otimes M_{(-,\mathrm{e})(+,\mathrm{o})}^{\mathrm{hom}}\Big), \tag{187}$$

$$|\psi\rangle = \sqrt{\kappa}\,|\phi_+\rangle_{AC}\,, \tag{188}$$

$$\alpha = 1, \quad \gamma_+ = \gamma, \quad \gamma_- = 0, \tag{189}$$

where $|\phi_+\rangle_{AC}$ is defined in Eq. (29). Then, we observe

$$\sigma_{\sup}\Big(\Pi_{AC}^{(-,\mathrm{od}),(+,\mathrm{ev})} M^{\mathrm{hom}}[\kappa,\gamma]\, \Pi_{AC}^{(-,\mathrm{od}),(+,\mathrm{ev})}\Big) \leq \sigma_{\sup}(M_{\mathrm{6d}}^{(1)}). \tag{190}$$

Combining inequalities (183) and (190) completes the proof. □

Next, we consider Heterodyne protocol.

Corollary 4. *Let $|\beta\rangle$ be a coherent state and $\theta_{\mu,\beta}^{\mathrm{hom}}(x)$ be defined to satisfy*

$$|\theta_{\mu,\beta}^{\mathrm{het}}(\omega_r)| \leq \frac{\pi}{2}, \qquad \tan\theta_{\mu,\beta}^{\mathrm{het}}(\omega_r) = e^{-2(\mu-\beta^2)} \sinh(2\beta\omega_r). \tag{191}$$

Let $\Pi_{\mathrm{ev(od)}}$ and $M^{\mathrm{het}}[\kappa,\gamma]$ be as defined in the main text, and let $M_{\mathrm{oo}}^{\mathrm{het}}$, $M_{\mathrm{ee}}^{\mathrm{het}}$, $M_{(\pm,\mathrm{o})(\mp,\mathrm{e})}^{\mathrm{het}}$, and $M_{(\mp,\mathrm{e})(\pm,\mathrm{o})}^{\mathrm{het}}$ be defined as follows:

$$M_{\mathrm{oo}}^{\mathrm{het}} \coloneqq \iint_{-\infty}^{\infty} f_{\mathrm{suc}}(\omega_r) d\omega_r dx\, \Pi_{\mathrm{od}} \Big[|x\rangle\langle x|\omega_r\rangle\langle\omega_r|x\rangle\langle x| + \frac{\cos\theta_{\mu,\beta}^{\mathrm{het}}(\omega_r)}{2} \big(|x\rangle\langle x|\omega_r\rangle\langle\omega_r|x-\beta\rangle\langle x-\beta| + |x-\beta\rangle\langle x-\beta|\omega_r\rangle\langle\omega_r|x\rangle\langle x|\big)\Big] \Pi_{\mathrm{od}}, \tag{192}$$

$$M_{\mathrm{ee}}^{\mathrm{het}} \coloneqq \iint_{-\infty}^{\infty} f_{\mathrm{suc}}(\omega_r) d\omega_r dx\, \Pi_{\mathrm{ev}} \Big[|x\rangle\langle x|\omega_r\rangle\langle\omega_r|x\rangle\langle x| - \frac{\cos\theta_{\mu,\beta}^{\mathrm{het}}(\omega_r)}{2} \big(|x\rangle\langle x|\omega_r\rangle\langle\omega_r|x-\beta\rangle\langle x-\beta| + |x-\beta\rangle\langle x-\beta|\omega_r\rangle\langle\omega_r|x\rangle\langle x|\big)\Big] \Pi_{\mathrm{ev}}, \tag{193}$$

$$M_{(+,\mathrm{o})(-,\mathrm{e})}^{\mathrm{het}} \coloneqq \iint_{-\infty}^{\infty} f_{\mathrm{suc}}(\omega_r) d\omega_r dx\, \Pi_{\mathrm{od}} \Big[\sin\theta_{\mu,\beta}^{\mathrm{het}}(\omega_r)\, |x\rangle\langle x|\omega_r\rangle\langle\omega_r|x\rangle\langle x| - \frac{\cos\theta_{\mu,\beta}^{\mathrm{het}}(\omega_r)}{2} \big(|x\rangle\langle x|\omega_r\rangle\langle\omega_r|x-\beta\rangle\langle x-\beta| - |x-\beta\rangle\langle x-\beta|\omega_r\rangle\langle\omega_r|x\rangle\langle x|\big)\Big] \Pi_{\mathrm{ev}}, \tag{194}$$

$$M_{(-,\mathrm{e})(+,\mathrm{o})}^{\mathrm{het}} \coloneqq \Big(M_{(+,\mathrm{o})(-,\mathrm{e})}^{\mathrm{het}}\Big)^{\dagger}, \tag{195}$$

$$M_{(-,\mathrm{o})(+,\mathrm{e})}^{\mathrm{het}} \coloneqq \iint_{-\infty}^{\infty} f_{\mathrm{suc}}(\omega_r) d\omega_r dx\, \Pi_{\mathrm{od}} \Big[-\sin\theta_{\mu,\beta}^{\mathrm{het}}(\omega_r)\, |x\rangle\langle x|\omega_r\rangle\langle\omega_r|x\rangle\langle x| - \frac{\cos\theta_{\mu,\beta}^{\mathrm{het}}(\omega_r)}{2} \big(|x\rangle\langle x|\omega_r\rangle\langle\omega_r|x-\beta\rangle\langle x-\beta| - |x-\beta\rangle\langle x-\beta|\omega_r\rangle\langle\omega_r|x\rangle\langle x|\big)\Big] \Pi_{\mathrm{ev}}, \tag{196}$$

$$M_{(+,\mathrm{e})(-,\mathrm{o})}^{\mathrm{het}} \coloneqq \Big(M_{(-,\mathrm{o})(+,\mathrm{e})}^{\mathrm{het}}\Big)^{\dagger}, \tag{197}$$

Define the following parameters:

$$C_{\mathrm{o}} \coloneqq \langle\beta|\,\Pi_{\mathrm{od}}\,|\beta\rangle = e^{-|\beta|^2}\sinh|\beta|^2, \quad C_{\mathrm{e}} \coloneqq \langle\beta|\,\Pi_{\mathrm{ev}}\,|\beta\rangle = e^{-|\beta|^2}\cosh|\beta|^2, \tag{198}$$

$$\lambda^{\mathrm{het}}_{\mathrm{oo}} \coloneqq C_{\mathrm{o}}^{-1}\,\langle\beta|\,M^{\mathrm{het}}_{\mathrm{oo}}\,|\beta\rangle\,, \quad \lambda^{\mathrm{het}}_{\mathrm{ee}} \coloneqq C_{\mathrm{e}}^{-1}\,\langle\beta|\,M^{\mathrm{het}}_{\mathrm{ee}}\,|\beta\rangle\,, \tag{199}$$

$$\lambda^{\mathrm{het}}_{(+,\mathrm{o})(-,\mathrm{e})} \coloneqq (C_{\mathrm{o}}C_{\mathrm{e}})^{-\frac{1}{2}}\,\langle\beta|\,M^{\mathrm{het}}_{(+,\mathrm{o})(-,\mathrm{e})}\,|\beta\rangle = (\lambda^{\mathrm{het}}_{(+,\mathrm{o})(-,\mathrm{e})})^*, \tag{200}$$

$$\lambda^{\mathrm{het}}_{(-,\mathrm{o})(+,\mathrm{e})} \coloneqq (C_{\mathrm{o}}C_{\mathrm{e}})^{-\frac{1}{2}}\,\langle\beta|\,M^{\mathrm{het}}_{(-,\mathrm{o})(+,\mathrm{e})}\,|\beta\rangle = (\lambda^{\mathrm{het}}_{(-,\mathrm{o})(+,\mathrm{e})})^*, \tag{201}$$

$$\sigma^{\mathrm{het}}_{\mathrm{oo}} \coloneqq \left(C_{\mathrm{o}}^{-1}\left\|M^{\mathrm{het}}_{\mathrm{oo}}\,|\beta\rangle\right\|^2 - (\lambda^{\mathrm{het}}_{\mathrm{oo}})^2\right)^{\frac{1}{2}}, \tag{202}$$

$$\sigma^{\mathrm{het}}_{(-,\mathrm{e})(+,\mathrm{o})} \coloneqq \left(C_{\mathrm{o}}^{-1}\left\|M^{\mathrm{het}}_{(-,\mathrm{e})(+,\mathrm{o})}\,|\beta\rangle\right\|^2 - |\lambda^{\mathrm{het}}_{(+,\mathrm{o})(-,\mathrm{e})}|^2\right)^{\frac{1}{2}}, \tag{203}$$

$$\sigma^{\mathrm{het}}_{(+,\mathrm{e})(-,\mathrm{o})} \coloneqq \left(C_{\mathrm{o}}^{-1}\left\|M^{\mathrm{het}}_{(+,\mathrm{e})(-,\mathrm{o})}\,|\beta\rangle\right\|^2 - |\lambda^{\mathrm{het}}_{(-,\mathrm{o})(+,\mathrm{e})}|^2\right)^{\frac{1}{2}}, \tag{204}$$

$$\sigma^{\mathrm{het}}_{(+,\mathrm{o})(-,\mathrm{e})} \coloneqq \sigma_{\mathrm{oo}}^{-1}\left((C_{\mathrm{o}}C_{\mathrm{e}})^{-\frac{1}{2}}\,\langle\beta|\,M^{\mathrm{het}}_{\mathrm{oo}}M^{\mathrm{het}}_{(+,\mathrm{o})(-,\mathrm{e})}\,|\beta\rangle - \lambda^{\mathrm{het}}_{\mathrm{oo}}\lambda^{\mathrm{het}}_{(+,\mathrm{o})(-,\mathrm{e})}\right) = (\sigma^{\mathrm{het}}_{(+,\mathrm{o})(-,\mathrm{e})})^*, \tag{205}$$

$$\sigma^{\mathrm{het}}_{(-,\mathrm{o})(+,\mathrm{e})} \coloneqq \sigma_{\mathrm{oo}}^{-1}\left((C_{\mathrm{o}}C_{\mathrm{e}})^{-\frac{1}{2}}\,\langle\beta|\,M^{\mathrm{het}}_{\mathrm{oo}}M^{\mathrm{het}}_{(-,\mathrm{o})(+,\mathrm{e})}\,|\beta\rangle - \lambda^{\mathrm{het}}_{\mathrm{oo}}\lambda^{\mathrm{het}}_{(-,\mathrm{o})(+,\mathrm{e})}\right) = (\sigma^{\mathrm{het}}_{(-,\mathrm{o})(+,\mathrm{e})})^*, \tag{206}$$

$$\sigma^{\mathrm{het}}_{(-,\mathrm{e})(-,\mathrm{e})} \coloneqq [\sigma^{\mathrm{het}}_{(-,\mathrm{e})(+,\mathrm{o})}]^{-1}\left((C_{\mathrm{o}}C_{\mathrm{e}})^{-\frac{1}{2}}\,\langle\beta|\,M^{\mathrm{het}}_{(+,\mathrm{o})(-,\mathrm{e})}M^{\mathrm{het}}_{\mathrm{ee}}\,|\beta\rangle - \lambda^{\mathrm{het}}_{(+,\mathrm{o})(-,\mathrm{e})}\lambda^{\mathrm{het}}_{\mathrm{ee}}\right) = (\sigma^{\mathrm{het}}_{(-,\mathrm{e})(-,\mathrm{e})})^*, \tag{207}$$

$$\sigma^{\mathrm{het}}_{(+,\mathrm{e})(+,\mathrm{e})} \coloneqq [\sigma^{\mathrm{het}}_{(+,\mathrm{e})(-,\mathrm{o})}]^{-1}\left((C_{\mathrm{o}}C_{\mathrm{e}})^{-\frac{1}{2}}\,\langle\beta|\,M^{\mathrm{het}}_{(-,\mathrm{o})(+,\mathrm{e})}M^{\mathrm{het}}_{\mathrm{ee}}\,|\beta\rangle - \lambda^{\mathrm{het}}_{(-,\mathrm{o})(+,\mathrm{e})}\lambda^{\mathrm{het}}_{\mathrm{ee}}\right) = (\sigma^{\mathrm{het}}_{(+,\mathrm{e})(+,\mathrm{e})})^*, \tag{208}$$

$$\Delta^{\mathrm{het}}_{(+,\mathrm{o})(-,\mathrm{e})} \coloneqq \left(C_{\mathrm{e}}^{-1}\left\|M^{\mathrm{het}}_{(+,\mathrm{o})(-,\mathrm{e})}\,|\beta\rangle\right\|^2 - |\lambda^{\mathrm{het}}_{(+,\mathrm{o})(-,\mathrm{e})}|^2 - |\sigma^{\mathrm{het}}_{(+,\mathrm{o})(-,\mathrm{e})}|^2\right)^{\frac{1}{2}}, \tag{209}$$

$$\Delta^{\mathrm{het}}_{(-,\mathrm{o})(+,\mathrm{e})} \coloneqq \left(C_{\mathrm{e}}^{-1}\left\|M^{\mathrm{het}}_{(-,\mathrm{o})(+,\mathrm{e})}\,|\beta\rangle\right\|^2 - |\lambda^{\mathrm{het}}_{(-,\mathrm{o})(+,\mathrm{e})}|^2 - |\sigma^{\mathrm{het}}_{(-,\mathrm{o})(+,\mathrm{e})}|^2\right)^{\frac{1}{2}}, \tag{210}$$

$$\Delta^{\mathrm{het}}_{(-,\mathrm{e})(-,\mathrm{e})} \coloneqq \left(C_{\mathrm{e}}^{-1}\left\|M^{\mathrm{het}}_{\mathrm{ee}}\,|\beta\rangle\right\|^2 - (\lambda^{\mathrm{het}}_{\mathrm{ee}})^2 - |\sigma^{\mathrm{het}}_{(-,\mathrm{e})(-,\mathrm{e})}|^2\right)^{\frac{1}{2}}, \tag{211}$$

$$\Delta^{\mathrm{het}}_{(+,\mathrm{e})(+,\mathrm{e})} \coloneqq \left(C_{\mathrm{e}}^{-1}\left\|M^{\mathrm{het}}_{\mathrm{ee}}\,|\beta\rangle\right\|^2 - (\lambda^{\mathrm{het}}_{\mathrm{ee}})^2 - |\sigma^{\mathrm{het}}_{(+,\mathrm{e})(+,\mathrm{e})}|^2\right)^{\frac{1}{2}}. \tag{212}$$

Define the following two matrices $M'^{(0)}_{6\mathrm{d}}$ and $M'^{(1)}_{6\mathrm{d}}$.

$$M'^{(0)}_{6\mathrm{d}} \coloneqq \begin{pmatrix} 1 & 0 & 0 & \Delta^{\mathrm{het}}_{(+,\mathrm{o})(-,\mathrm{e})} & 0 & 0 \\ 0 & 1 & \sigma^{\mathrm{het}}_{\mathrm{oo}} & \sigma^{\mathrm{het}}_{(+,\mathrm{o})(-,\mathrm{e})} & 0 & 0 \\ 0 & \sigma^{\mathrm{het}}_{\mathrm{oo}} & \kappa C_{\mathrm{o}} + \lambda^{\mathrm{het}}_{\mathrm{oo}} & \kappa\sqrt{C_{\mathrm{o}}C_{\mathrm{e}}} + \lambda^{\mathrm{het}}_{(+,\mathrm{o})(-,\mathrm{e})} & \sigma^{\mathrm{het}}_{(-,\mathrm{e})(+,\mathrm{o})} & 0 \\ \Delta^{\mathrm{het}}_{(+,\mathrm{o})(-,\mathrm{e})} & \sigma^{\mathrm{het}}_{(+,\mathrm{o})(-,\mathrm{e})} & \kappa\sqrt{C_{\mathrm{o}}C_{\mathrm{e}}} + \lambda^{\mathrm{het}}_{(+,\mathrm{o})(-,\mathrm{e})} & \kappa C_{\mathrm{e}} + \lambda^{\mathrm{het}}_{(-,\mathrm{e})(-,\mathrm{e})} - \gamma & \sigma^{\mathrm{het}}_{(-,\mathrm{e})(-,\mathrm{e})} & \Delta^{\mathrm{het}}_{(-,\mathrm{e})(-,\mathrm{e})} \\ 0 & 0 & \sigma^{\mathrm{het}}_{(-,\mathrm{e})(+,\mathrm{o})} & \sigma^{\mathrm{het}}_{(-,\mathrm{e})(-,\mathrm{e})} & 1-\gamma & 0 \\ 0 & 0 & 0 & \Delta^{\mathrm{het}}_{(-,\mathrm{e})(-,\mathrm{e})} & 0 & 1-\gamma \end{pmatrix}, \tag{213}$$

$$M'^{(1)}_{6\mathrm{d}} \coloneqq \begin{pmatrix} 1-\gamma & 0 & 0 & \Delta^{\mathrm{het}}_{(-,\mathrm{o})(+,\mathrm{e})} & 0 & 0 \\ 0 & 1-\gamma & \sigma^{\mathrm{het}}_{\mathrm{oo}} & \sigma^{\mathrm{het}}_{(-,\mathrm{o})(+,\mathrm{e})} & 0 & 0 \\ 0 & \sigma^{\mathrm{het}}_{\mathrm{oo}} & \kappa C_{\mathrm{o}} + \lambda^{\mathrm{het}}_{\mathrm{oo}} - \gamma & \kappa\sqrt{C_{\mathrm{o}}C_{\mathrm{e}}} + \lambda^{\mathrm{het}}_{(-,\mathrm{o})(+,\mathrm{e})} & \sigma^{\mathrm{het}}_{(+,\mathrm{e})(-,\mathrm{o})} & 0 \\ \Delta^{\mathrm{het}}_{(-,\mathrm{o})(+,\mathrm{e})} & \sigma^{\mathrm{het}}_{(-,\mathrm{o})(+,\mathrm{e})} & \kappa\sqrt{C_{\mathrm{o}}C_{\mathrm{e}}} + \lambda^{\mathrm{het}}_{(-,\mathrm{o})(+,\mathrm{e})} & \kappa C_{\mathrm{e}} + \lambda^{\mathrm{het}}_{\mathrm{ee}} & \sigma^{\mathrm{het}}_{(+,\mathrm{e})(+,\mathrm{e})} & \Delta^{\mathrm{het}}_{(+,\mathrm{e})(+,\mathrm{e})} \\ 0 & 0 & \sigma^{\mathrm{het}}_{(+,\mathrm{e})(-,\mathrm{o})} & \sigma^{\mathrm{het}}_{(+,\mathrm{e})(+,\mathrm{e})} & 1 & 0 \\ 0 & 0 & 0 & \Delta^{\mathrm{het}}_{(+,\mathrm{e})(+,\mathrm{e})} & 0 & 1 \end{pmatrix}. \tag{214}$$

Define a convex function

$$B^{\mathrm{het}}(\kappa,\gamma) \coloneqq \max\{\sigma_{\mathrm{sup}}(M'^{(0)}_{6\mathrm{d}}), \sigma_{\mathrm{sup}}(M'^{(1)}_{6\mathrm{d}})\}. \tag{215}$$

Then, for $\kappa, \gamma \geq 0$, we have

$$M^{\mathrm{het}}[\kappa,\gamma] \leq B^{\mathrm{het}}(\kappa,\gamma) I_{AC}. \tag{216}$$

Proof. In the same way as Homodyne protocol, we have from Eqs. (56) and (57) that

$$|u_{\pm}^{\mathrm{het}}(\omega_r)\rangle_A = \cos\left(\frac{\theta_{\mu,\beta}^{\mathrm{het}}(\omega_r)}{2}\right)|\pm\rangle_A \pm \sin\left(\frac{\theta_{\mu,\beta}^{\mathrm{het}}(\omega_r)}{2}\right)|\mp\rangle_A . \tag{217}$$

Combining this with Eqs. (73) and (74), we observe that

$$(\langle+|_A \otimes \Pi_{\mathrm{od}}) M_{\mathrm{ph}}^{\mathrm{het}} (|+\rangle_A \otimes \Pi_{\mathrm{od}}) = (\langle-|_A \otimes \Pi_{\mathrm{od}}) M_{\mathrm{ph}}^{\mathrm{het}} (|-\rangle_A \otimes \Pi_{\mathrm{od}}) = M_{\mathrm{oo}}^{\mathrm{het}}, \tag{218}$$

$$(\langle-|_A \otimes \Pi_{\mathrm{ev}}) M_{\mathrm{ph}}^{\mathrm{het}} (|-\rangle_A \otimes \Pi_{\mathrm{ev}}) = (\langle+|_A \otimes \Pi_{\mathrm{ev}}) M_{\mathrm{ph}}^{\mathrm{het}} (|+\rangle_A \otimes \Pi_{\mathrm{ev}}) = M_{\mathrm{ee}}^{\mathrm{het}} \tag{219}$$

$$(\langle+|_A \otimes \Pi_{\mathrm{od}}) M_{\mathrm{ph}}^{\mathrm{het}} (|-\rangle_A \otimes \Pi_{\mathrm{ev}}) = \left[(\langle-|_A \otimes \Pi_{\mathrm{ev}}) M_{\mathrm{ph}}^{\mathrm{het}} (|+\rangle_A \otimes \Pi_{\mathrm{od}})\right]^{\dagger} = M_{(+,\mathrm{o})(-,\mathrm{e})}^{\mathrm{het}} \tag{220}$$

$$(\langle-|_A \otimes \Pi_{\mathrm{od}}) M_{\mathrm{ph}}^{\mathrm{het}} (|+\rangle_A \otimes \Pi_{\mathrm{ev}}) = \left[(\langle+|_A \otimes \Pi_{\mathrm{ev}}) M_{\mathrm{ph}}^{\mathrm{het}} (|-\rangle_A \otimes \Pi_{\mathrm{od}})\right]^{\dagger} = M_{(-,\mathrm{o})(+,\mathrm{e})}^{\mathrm{het}} \tag{221}$$

As can be seen from Eq. (73) as well as Eqs. (75)–(80), we have

$$M^{\mathrm{het}}[\kappa,\gamma] = \Pi_{AC}^{(+,\mathrm{od}),(-,\mathrm{ev})} M^{\mathrm{het}}[\kappa,\gamma]\, \Pi_{AC}^{(+,\mathrm{od}),(-,\mathrm{ev})} + \Pi_{AC}^{(-,\mathrm{od}),(+,\mathrm{ev})} M^{\mathrm{het}}[\kappa,\gamma]\, \Pi_{AC}^{(-,\mathrm{od}),(+,\mathrm{ev})}, \tag{222}$$

where $\Pi_{AC}^{(+,\mathrm{od}),(-,\mathrm{ev})}$ and $\Pi_{AC}^{(-,\mathrm{od}),(+,\mathrm{ev})}$ are defined in Eqs. (66) and (67). Then we apply Lemma 2 to the operators $\Pi_{AC}^{(+,\mathrm{od}),(-,\mathrm{ev})} M^{\mathrm{het}}[\kappa,\gamma]\, \Pi_{AC}^{(+,\mathrm{od}),(-,\mathrm{ev})}$ and $\Pi_{AC}^{(-,\mathrm{od}),(+,\mathrm{ev})} M^{\mathrm{het}}[\kappa,\gamma]\, \Pi_{AC}^{(-,\mathrm{od}),(+,\mathrm{ev})}$, respectively. For $\Pi_{AC}^{(+,\mathrm{od}),(-,\mathrm{ev})} M^{\mathrm{het}}[\kappa,\gamma]\, \Pi_{AC}^{(+,\mathrm{od}),(-,\mathrm{ev})}$, using Eqs. (218), (219), and (220), we set

$$\Pi_{\pm} = |\pm\rangle\langle\pm|_A \otimes \Pi_{\mathrm{od(ev)}}, \tag{223}$$

$$M = \Pi_{AC}^{(+,\mathrm{od}),(-,\mathrm{ev})} M_{\mathrm{ph}}^{\mathrm{het}} \Pi_{AC}^{(+,\mathrm{od}),(-,\mathrm{ev})} \tag{224}$$

$$= |+\rangle\langle+|_A \otimes M_{\mathrm{oo}}^{\mathrm{het}} + |-\rangle\langle-|_A \otimes M_{\mathrm{ee}}^{\mathrm{het}} + |+\rangle\langle-|_A \otimes M_{(+,\mathrm{o})(-,\mathrm{e})}^{\mathrm{het}} + |-\rangle\langle+|_A \otimes M_{(-,\mathrm{e})(+,\mathrm{o})}^{\mathrm{het}}, \tag{225}$$

$$|\psi\rangle = \sqrt{\kappa}\,|\phi_-\rangle_{AC}\,, \tag{226}$$

$$\alpha = 1, \quad \gamma_+ = 0, \quad \gamma_- = \gamma, \tag{227}$$

where $|\phi_-\rangle_{AC}$ is defined in Eq. (30). Since so-defined M only has continuous spectrum, we can apply Lemma 2 and obtain

$$\sigma_{\mathrm{sup}}\left(\Pi_{AC}^{(+,\mathrm{od}),(-,\mathrm{ev})} M^{\mathrm{het}}[\kappa,\gamma]\, \Pi_{AC}^{(+,\mathrm{od}),(-,\mathrm{ev})}\right) \leq \sigma_{\mathrm{sup}}(M_{\mathrm{6d}}'^{(0)}). \tag{228}$$

We also apply Lemma 2 to $\Pi_{AC}^{(-,\mathrm{od}),(+,\mathrm{ev})} M^{\mathrm{het}}[\kappa,\gamma]\, \Pi_{AC}^{(-,\mathrm{od}),(+,\mathrm{ev})}$. Using Eqs. (218), (219), and (221), we set

$$\Pi_{\pm} = |\mp\rangle\langle\mp|_A \otimes \Pi_{\mathrm{od(ev)}}, \tag{229}$$

$$M = \Pi_{AC}^{(-,\mathrm{od}),(+,\mathrm{ev})} M_{\mathrm{ph}}^{\mathrm{het}} \Pi_{AC}^{(-,\mathrm{od}),(+,\mathrm{ev})} \tag{230}$$

$$= |-\rangle\langle-|_A \otimes M_{\mathrm{oo}}^{\mathrm{het}} + |+\rangle\langle+|_A \otimes M_{\mathrm{ee}}^{\mathrm{het}} + |-\rangle\langle+|_A \otimes M_{(-,\mathrm{o})(+,\mathrm{e})}^{\mathrm{het}} + |+\rangle\langle-|_A \otimes M_{(+,\mathrm{e})(-,\mathrm{o})}^{\mathrm{het}}, \tag{231}$$

$$|\psi\rangle = \sqrt{\kappa}\,|\phi_+\rangle_{AC}\,, \tag{232}$$

$$\alpha = 1, \quad \gamma_+ = \gamma, \quad \gamma_- = 0. \tag{233}$$

where $|\phi_+\rangle_{AC}$ is defined in Eq. (29). Then, we observe

$$\sigma_{\mathrm{sup}}\left(\Pi_{AC}^{(-,\mathrm{od}),(+,\mathrm{ev})} M^{\mathrm{het}}[\kappa,\gamma]\, \Pi_{AC}^{(-,\mathrm{od}),(+,\mathrm{ev})}\right) \leq \sigma_{\mathrm{sup}}(M_{\mathrm{6d}}'^{(1)}). \tag{234}$$

Combining inequalities (228) and (234) completes the proof. □

Note that the elements of the matrices $M_{\mathrm{6d}}^{(0)}$ and $M_{\mathrm{6d}}^{(1)}$ in Eqs. (166) and (167) depend linearly on the parameters κ and γ. Since the largest eigenvalue of a matrix is a convex function of its elements [72, 73], the largest eigenvalues $\sigma_{\mathrm{sup}}(M_{\mathrm{6d}}^{(0)})$ and $\sigma_{\mathrm{sup}}(M_{\mathrm{6d}}^{(1)})$ are convex functions of κ and γ, and so is $B^{\mathrm{hom}}(\kappa,\gamma)$ in Eq. (168). The same fact can also be applied to $B^{\mathrm{het}}(\kappa,\gamma)$ in Eq. (215).

References

[1] Charles H. Bennett and Gilles Brassard. "Quantum cryptography: Public key distribution and coin tossing". Theoretical Computer Science **560**, 7–11 (2014).

[2] C. E. Shannon. "Communication theory of secrecy systems". The Bell System Technical Journal **28**, 656–715 (1949).

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

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

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

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

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

[8] Frédéric Grosshans, Gilles Van Assche, Jérôme Wenger, Rosa Brouri, Nicolas J. Cerf, and Philippe Grangier. "Quantum key distribution using gaussian-modulated coherent states". Nature **421**, 238–241 (2003).

[9] Christian Weedbrook, Andrew M. Lance, Warwick P. Bowen, Thomas Symul, Timothy C. Ralph, and Ping Koy Lam. "Quantum Cryptography Without Switching". Phys. Rev. Lett. **93**, 170504 (2004).

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

[11] Yi-Bo Zhao, Matthias Heid, Johannes Rigas, and Norbert Lütkenhaus. "Asymptotic security of binary modulated continuous-variable quantum key distribution under collective attacks". Phys. Rev. A **79**, 012307 (2009).

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

[13] Anthony Leverrier and Philippe Grangier. "Unconditional Security Proof of Long-Distance Continuous-Variable Quantum Key Distribution with Discrete Modulation". Phys. Rev. Lett. **102**, 180504 (2009).

[14] Anthony Leverrier and Philippe Grangier. "Erratum: Unconditional Security Proof of Long-Distance Continuous-Variable Quantum Key Distribution with Discrete Modulation [Phys. Rev. Lett. 102, 180504 (2009)]". Phys. Rev. Lett. **106**, 259902 (2011).

[15] Eneet Kaur, Saikat Guha, and Mark M. Wilde. "Asymptotic security of discrete-modulation protocols for continuous-variable quantum key distribution". Phys. Rev. A **103**, 012412 (2021).

[16] Shouvik Ghorai, Philippe Grangier, Eleni Diamanti, and Anthony Leverrier. "Asymptotic Security of Continuous-Variable Quantum Key Distribution with a Discrete Modulation". Phys. Rev. X **9**, 021059 (2019).

[17] Jie Lin, Twesh Upadhyaya, and Norbert Lütkenhaus. "Asymptotic Security Analysis of Discrete-Modulated Continuous-Variable Quantum Key Distribution". Phys. Rev. X **9**, 041064 (2019).

[18] Wen-Bo Liu, Chen-Long Li, Yuan-Mei Xie, Chen-Xun Weng, Jie Gu, Xiao-Yu Cao, Yu-Shuo Lu, Bing-Hong Li, Hua-Lei Yin, and Zeng-Bing Chen. "Homodyne Detection Quadrature Phase Shift Keying Continuous-Variable Quantum key Distribution with High Excess Noise Tolerance". PRX Quantum **2**, 040334 (2021).

[19] Twesh Upadhyaya, Thomas van Himbeeck, Jie Lin, and Norbert Lütkenhaus. "Dimension Reduction in Quantum Key Distribution for Continuous- and Discrete-Variable Protocols". PRX Quantum **2**, 020325 (2021).

[20] Aurélie Denys, Peter Brown, and Anthony Leverrier. "Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation". Quantum **5**, 540 (2021).

[21] Anthony Leverrier, Frédéric Grosshans, and Philippe Grangier. "Finite-size analysis of a continuous-variable quantum key distribution". Phys. Rev. A **81**, 062343 (2010).

[22] Anthony Leverrier. "Composable Security Proof for Continuous-Variable Quantum Key Distribution with Coherent States". Phys. Rev. Lett. **114**, 070501 (2015).

[23] E. Samsonov, R. Goncharov, A. Gaidash, A. Kozubov, V. Egorov, and A. Gleim. "Subcarrier wave continuous variable quantum key distribution with discrete modulation: mathematical model and finite-key analysis". Scientific Reports **10**, 10034 (2020).
[24] Panagiotis Papanastasiou and Stefano Pirandola. "Continuous-variable quantum cryptography with discrete alphabets: Composable security under collective Gaussian attacks". Phys. Rev. Research **3**, 013047 (2021).
[25] Panagiotis Papanastasiou, Carlo Ottaviani, and Stefano Pirandola. "Security of continuous-variable quantum key distribution against canonical attacks". In 2021 International Conference on Computer Communications and Networks (ICCCN). Pages 1–6. (2021).
[26] Alexander G. Mountogiannakis, Panagiotis Papanastasiou, Boris Braverman, and Stefano Pirandola. "Composably secure data processing for Gaussian-modulated continuous-variable quantum key distribution". Phys. Rev. Research **4**, 013099 (2022).
[27] Florian Kanitschar, Ian George, Jie Lin, Twesh Upadhyaya, and Norbert Lütkenhaus. "Finite-Size Security for Discrete-Modulated Continuous-Variable Quantum Key Distribution Protocols" (2023). arXiv:2301.08686.
[28] 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).
[29] F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, and R. F. Werner. "Erratum: Continuous Variable Quantum Key Distribution: Finite-Key Analysis of Composable Security Against Coherent Attacks [Phys. Rev. Lett. 109, 100502 (2012)]". Phys. Rev. Lett. **112**, 019902 (2014).
[30] Fabian Furrer. "Reverse-reconciliation continuous-variable quantum key distribution based on the uncertainty principle". Phys. Rev. A **90**, 042325 (2014).
[31] Mario Berta, Fabian Furrer, and Volkher B. Scholz. "The smooth entropy formalism for von Neumann algebras". Journal of Mathematical Physics **57**, 015213 (2016).
[32] Anthony Leverrier, Raúl García-Patrón, Renato Renner, and Nicolas J. Cerf. "Security of Continuous-Variable Quantum Key Distribution Against General Attacks". Phys. Rev. Lett. **110**, 030502 (2013).
[33] Anthony Leverrier. "Security of Continuous-Variable Quantum Key Distribution via a Gaussian de Finetti Reduction". Phys. Rev. Lett. **118**, 200501 (2017).
[34] A Leverrier, E Karpov, P Grangier, and N J Cerf. "Security of continuous-variable quantum key distribution: towards a de Finetti theorem for rotation symmetry in phase space". New Journal of Physics **11**, 115009 (2009).
[35] Anthony Leverrier. "SU(p,q) coherent states and a Gaussian de Finetti theorem". Journal of Mathematical Physics **59**, 042202 (2018).
[36] Cosmo Lupo, Carlo Ottaviani, Panagiotis Papanastasiou, and Stefano Pirandola. "Continuous-variable measurement-device-independent quantum key distribution: Composable security against coherent attacks". Phys. Rev. A **97**, 052327 (2018).
[37] Shouvik Ghorai, Eleni Diamanti, and Anthony Leverrier. "Composable security of two-way continuous-variable quantum key distribution without active symmetrization". Phys. Rev. A **99**, 012311 (2019).
[38] Paul Jouguet, Sébastien Kunz-Jacques, Eleni Diamanti, and Anthony Leverrier. "Analysis of imperfections in practical continuous-variable quantum key distribution". Phys. Rev. A **86**, 032309 (2012).
[39] Cosmo Lupo. "Towards practical security of continuous-variable quantum key distribution". Phys. Rev. A **102**, 022623 (2020).
[40] Takaya Matsuura, Kento Maeda, Toshihiko Sasaki, and Masato Koashi. "Finite-size security of continuous-variable quantum key distribution with digital signal processing". Nature Communications **12**, 252 (2021).
[41] Shinichiro Yamano, Takaya Matsuura, Yui Kuramochi, Toshihiko Sasaki, and Masato Koashi. "Finite-size security proof of binary-modulation continuous-variable quantum key distribution using only heterodyne measurement" (2022). arXiv:2208.11983.
[42] Stefan Bäuml, Carlos Pascual García, Victoria Wright, Omar Fawzi, and Antonio Acín. "Security of discrete-modulated continuous-variable quantum key distribution" (2023). arXiv:2303.09255.

[43] Cosmo Lupo and Yingkai Ouyang. "Quantum Key Distribution with Nonideal Heterodyne Detection: Composable Security of Discrete-Modulation Continuous-Variable Protocols". PRX Quantum **3**, 010341 (2022).
[44] Peter W. Shor and John Preskill. "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol". Phys. Rev. Lett. **85**, 441–444 (2000).
[45] Hoi-Kwong Lo and H. F. Chau. "Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances". Science **283**, 2050–2056 (1999).
[46] RENATO RENNER. "SECURITY OF QUANTUM KEY DISTRIBUTION". International Journal of Quantum Information **06**, 1–127 (2008).
[47] M Koashi. "Simple security proof of quantum key distribution based on complementarity". New Journal of Physics **11**, 045018 (2009).
[48] Toyohiro Tsurumaru. "Equivalence of Three Classical Algorithms With Quantum Side Information: Privacy Amplification, Error Correction, and Data Compression". IEEE Transactions on Information Theory **68**, 1016–1031 (2022).
[49] Masahito Hayashi and Toyohiro Tsurumaru. "Concise and tight security analysis of the Bennett-Brassard 1984 protocol with finite key lengths". New Journal of Physics **14**, 093014 (2012).
[50] Toyohiro Tsurumaru. "Leftover Hashing From Quantum Error Correction: Unifying the Two Approaches to the Security Proof of Quantum Key Distribution". IEEE Transactions on Information Theory **66**, 3465–3484 (2020).
[51] Stefano Pirandola, Riccardo Laurenza, Carlo Ottaviani, and Leonardo Banchi. "Fundamental limits of repeaterless quantum communications". Nature Communications **8**, 15043 (2017).
[52] Jérôme Lodewyck, Matthieu Bloch, Raúl García-Patrón, Simon Fossier, Evgueni Karpov, Eleni Diamanti, Thierry Debuisschert, Nicolas J. Cerf, Rosa Tualle-Brouri, Steven W. McLaughlin, and Philippe Grangier. "Quantum key distribution over 25 km with an all-fiber continuous-variable system". Phys. Rev. A **76**, 042305 (2007).
[53] Paul Jouguet, David Elkouss, and Sébastien Kunz-Jacques. "High-bit-rate continuous-variable quantum key distribution". Phys. Rev. A **90**, 042329 (2014).
[54] Xuan Wen, Qiong Li, Haokun Mao, Xiaojun Wen, and Nan Chen. "Rotation Based Slice Error Correction Protocol for Continuous-variable Quantum Key Distribution and its Implementation with Polar Codes" (2021). arXiv:2106.06206.
[55] Karol Horodecki, Debbie Leung, Hoi-Kwong Lo, and Jonathan Oppenheim. "Quantum Key Distribution Based on Arbitrarily Weak Distillable Entangled States". Phys. Rev. Lett. **96**, 070501 (2006).
[56] Joseph M. Renes and Graeme Smith. "Noisy Processing and Distillation of Private Quantum States". Phys. Rev. Lett. **98**, 020502 (2007).
[57] K. Horodecki, M. Horodecki, P. Horodecki, D. Leung, and J. Oppenheim. "Unconditional Privacy over Channels which Cannot Convey Quantum Information". Phys. Rev. Lett. **100**, 110502 (2008).
[58] Karol Horodecki, Michal Horodecki, Pawel Horodecki, and Jonathan Oppenheim. "General Paradigm for Distilling Classical Key From Quantum States". IEEE Transactions on Information Theory **55**, 1898–1929 (2009).
[59] J. Eli Bourassa, Ignatius William Primaatmaja, Charles Ci Wen Lim, and Hoi-Kwong Lo. "Loss-tolerant quantum key distribution with mixed signal states". Phys. Rev. A **102**, 062607 (2020).
[60] Takaya Matsuura, Toshihiko Sasaki, and Masato Koashi. "Refined security proof of the round-robin differential-phase-shift quantum key distribution and its improved performance in the finite-sized case". Phys. Rev. A **99**, 042303 (2019).
[61] Takaya Matsuura. "Digital quantum information processing with continuous-variable systems". Springer Nature. (2023). url: https://doi.org/10.1007/978-981-19-8288-0.
[62] Thomas M. Cover and Joy A. Thomas. "Elements of Information Theory (Wiley Series in Telecommunications and Signal Processing)". Wiley-Interscience. USA (2006).
[63] Toyohiro Tsurumaru and Masahito Hayashi. "Dual Universality of Hash Functions and Its Applications to Quantum Cryptography". IEEE Transactions on Information Theory **59**, 4700–4717 (2013).

[64] Wassily Hoeffding. "Probability Inequalities for Sums of Bounded Random Variables". Journal of the American Statistical Association **58**, 13–30 (1963).
[65] Go Kato. "Concentration inequality using unconfirmed knowledge" (2020). arXiv:2002.04357.
[66] Kazuoki Azuma. "Weighted sums of certain dependent random variables". Tohoku Mathematical Journal **19**, 357 – 367 (1967).
[67] Hongyi Zhou, Toshihiko Sasaki, and Masato Koashi. "Numerical method for finite-size security analysis of quantum key distribution". Phys. Rev. Res. **4**, 033126 (2022).
[68] Jörn Müller-Quade and Renato Renner. "Composability in quantum cryptography". New Journal of Physics **11**, 085006 (2009).
[69] V. Chvátal. "The tail of the hypergeometric distribution". Discrete Mathematics **25**, 285–287 (1979).
[70] Maxim Raginsky and Igal Sason. "Concentration of Measure Inequalities in Information Theory, Communications, and Coding". Foundations and Trends® in Communications and Information Theory **10**, 1–246 (2013).
[71] Colin McDiarmid. "Concentration". Pages 195–248. Springer Berlin Heidelberg. Berlin, Heidelberg (1998).
[72] Roger A. Horn and Charles R. Johnson. "Matrix Analysis". Cambridge University Press. (1985).
[73] M. L. Overton and R. S. Womersley. "Optimality conditions and duality theory for minimizing sums of the largest eigenvalues of symmetric matrices". Mathematical Programming **62**, 321–357 (1993).