Composable security analysis of continuous-variable measurement-device-independent quantum key distribution with squeezed states for coherent attacks

Ziyang Chen,[1] Yichen Zhang,[2] Gan Wang,[1] Zhengyu Li,[1] and Hong Guo[1,*]

[1]*State Key Laboratory of Advanced Optical Communication System and Network, School of Electronics Engineering and Computer Science and Center for Quantum Information Technology, Peking University, Beijing 100871, China*

[2]*State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876, China*

(Received 8 February 2018; published 13 July 2018)

Measurement-device-independent quantum key distribution protocol, whose security analysis does not rely on any assumption on the detection system, can immune the attacking against detectors. We give a first composable security analysis for continuous-variable measurement-device-independent quantum key distribution using squeezed states against general coherent attacks. The security analysis is derived based on the entanglement-based scheme considering finite-size effect. A version of entropic uncertainty relation is exploited to give a lower bound on the conditional smooth min-entropy by trusting Alice's and Bob's devices. The simulation results indicate that, in the universal composable security framework, the protocol can tolerate 2.5 dB and 6.5 dB channel loss against coherent attacks with direct and reverse reconciliation, respectively.

DOI: 10.1103/PhysRevA.98.012314

I. INTRODUCTION

Quantum key distribution (QKD) [1,2], which is an indispensable part of today's quantum cryptography, allows two legitimate users (Alice and Bob) to distribute keys secretly thanks to quantum physics. The most attractive property of QKD may be the information-theoretic security against any potential attacks. Broadly speaking, QKD has two main approaches: one is discrete-variable (DV) QKD and the alternative is continuous-variable (CV) QKD [3–5]. Compared to DV-QKD protocols, CV-QKD protocols are based on variants of homodyne detection which is "off the shelf" [6–8], and can perform high secret key rates for metropolitan range. Various novel CV-QKD protocols were proposed in recent years, including a two-way quantum cryptographic protocol [9–14], single-quadrature protocols [15,16], floodlight QKD protocol [17–19], and so forth, which enrich the field of CV-QKD. A new CV protocol design framework has been proposed to design protocols according to the user's needs [20], which can be achieved by arbitrary nonorthogonal states. Experiments [21–26], especially field tests [27] for distributing secret keys over long distances, are currently achievable, making CV protocols competitive with respect to their DV counterparts.

The security-proof toolbox of CV-QKD has been enriched over the past few years, with the de Finetti theorem [28,29], postselection technique [30,31], the entropic uncertainty relations [32–34], and so forth. Many protocols show their security against collective attacks via a Gaussian optimality argument [35–38] but are only considered in the asymptotic limit. Fortunately, those security-proof tools make it possible to generalize the security analysis to the most general coherent attacks even considering finite-size effect. For instance, under Gaussian modulation, the coherent state protocol with heterodyne detection was proved secure against coherent attacks with the help of rotation invariance [28] and the squeezed state [39] protocol with homodyne detection is secure using entropic uncertainty relations [32].

Apart from theoretical security analysis, practical security analysis in QKD is gradually paid attention to take the gap between theory and practice into consideration. Measurement-device-independent (MDI) QKD protocol is a genius idea to immune the attack against detectors [40–45], moving towards practical security of QKD. CV-MDI QKD, as one of the candidate protocols to achieve multipartite communication [46–49], has been shown to guard against collective attacks and some work also takes finite-size effect into account [50–52]. Recently, the composable security analysis of CV-MDI QKD, which could be applied both to coherent-state protocols and to entangled-state protocols, has been proposed to defend general coherent attacks via Gaussian de Finetti reduction [53], while the composable security analysis of that using squeezed states under coherent attacks has not been discussed yet.

We should note that the entropic uncertainty relations are paid a lot of attention in both DV-QKD and CV-QKD's security proofs [54,55]. There is a large family of entropic uncertainty relation, among which the infinite-dimensional state-independent entropic uncertainty relation with quantum memories was studied in depth [56] and it was soon applied for the security proof of squeezed-state protocol with homodyne detection [32–34]. The entropic uncertainty method can be exploited to prove the security of squeezed-state CV-MDI QKD protocol directly.

In this paper, we use the method similar to Ref. [32] of the squeezed-state CV-MDI QKD protocol by trusting Alice's and Bob's devices, and show the performance against

*hongguo@pku.edu.cn

general coherent attacks, which is based on a state-independent entropic uncertainty relation with quantum side information for smooth entropies. Meanwhile, the analysis not only considers the finite-size effect, but also takes some necessary steps into account, such as channel parameter estimation and error correction, so that the final secret key length has to be reduced due to the fact that those estimation phases inevitably consume an amount of keys. Moreover, we analyze both direct and reverse reconciliation scenarios. Focusing on the extremely asymmetric cases, where Bob is placed on Charlie's side, the ideal case (modulation variance tending to infinity) and a practical feasible parameters case (modulation variance as small as 5.04, referring to 10 dB squeezing [57], with imperfect reconciliation efficiency $\beta = 96.9\%$ [58]) are both discussed at different block lengths. More general cases are also discussed in the Appendixes.

The paper is organized as follows. In Sec. II A, a short review on the definition of composable security in QKD is described. In Sec. II B, we provide a detailed description of the squeezed-state CV-MDI QKD protocol against general coherent attacks under the entanglement-based scheme. In Sec. II C, we introduce a version of the state-independent entropy uncertainty relation conditional on quantum side information into the security analysis of the protocol and derive the secure key rate against coherent attacks. Then, in Sec. III, we give out the simulation results of the secret key rate in both direct and reverse reconciliation cases, especially under extremely asymmetric scenarios. Finally, a summary of the paper is given in Sec. IV.

II. FRAMEWORK OF THE SECURITY ANALYSIS

In this section, a brief introduction about the definition of composable security in QKD is given, and the details can be found in Refs. [59,60]. Then the CV-MDI QKD protocol using squeezed states against coherent attacks is described in detail, followed by the entropic uncertainty relation to obtain the secret key rate of the protocol.

A. Composable security definition

Roughly speaking, a protocol can be called "security," which should satisfy three criteria called "robustness," "correctness," and "secrecy.". If the probability of producing an empty set of the secret key is not higher than ε_{rob} when the eavesdropper is inactive, a protocol is called ε_{rob} robust.

A QKD protocol can be called "correct" if Alice and Bob can get the same keys for any initial quantum state Ψ_{ABE} (no matter what strategy of the adversary may be used to the quantum state). The secret key is denoted by S_A and S_B after they finish the protocol, and a protocol is called ε_{cor} correct if the probability of producing different sets of the secret key between S_A and S_B is not higher than ε_{cor}, i.e., $\Pr[S_A \neq S_B] \leqslant \varepsilon_{\text{cor}}$.

A final key is Δ secret if it is Δ close to a uniformly distributed key that is unpredictable for the adversary. Here Δ quantifies the distance between a practical key and an ideal one, for a Δ-secret protocol, which should satisfy

$$\frac{1}{2}\|\rho_{S_A S_B E'} - \omega_l \otimes \rho_{E'}\|_1 \leqslant \Delta, \tag{1}$$

where $\rho_{S_A S_B E'}$ is the practical state mixing of Alice, Bob, and the potential adversary Eve's strings S_A, S_B, and E' and ω_l is the fully mixed state on classical strings of length l. $\omega_l \otimes \rho_{E'}$ shows the ideal classical-quantum state is separable. Hence if $\Delta = 0$ for any of Eve's attack strategies, a QKD protocol can be called secret. Moreover, a protocol is called ε_{sec} secret if it is ε_{sec} indistinguishable from an ideal secret protocol. In particular, a protocol is ε_{sec} secret if it outputs Δ-secure keys with $(1 - p_{abort})\Delta \leqslant \varepsilon_{\text{sec}}$, where p_{abort} is the probability that the protocol aborts. ε_{rob}, ε_{cor}, and ε_{sec} are parameters to qualify robustness, correctness, and secrecy respectively and they will affect the final rate of the secret key.

A QKD protocol is called secure if it satisfies both correctness and secrecy. It is called ε secure if it is ε indistinguishable from a secure protocol. In particular, a protocol is ε secure if it is ε_{cor} correct and ε_{sec} secret with $\varepsilon_{\text{cor}} + \varepsilon_{\text{sec}} \leqslant \varepsilon$.

B. CV-MDI QKD using squeezed states against coherent attacks

In this subsection, we describe the squeezed-state CV MDI QKD protocol for which we prove composable security against coherent attacks based on the entropic uncertainty relation. Here we focus on the entanglement-based (EB) model of the protocol [61] instead of the prepare and measure (PM) version, for the former scheme is often used in the security analysis of QKD, while the latter is easy to implement and, once the security of the EB scheme is proved, the security of the PM version is easily obtained because of the equivalence between two schemes [42]. The EB scheme of the squeezed-state CV-MDI QKD protocol (Fig. 1) is described as follows.

(1) *State preparation.* Alice and Bob prepare $2N$ two-mode squeezed vacuum states EPR_1 and EPR_2 with variances V_A and V_B, respectively. They keep mode A_1 and B_1 on each side and then send the other modes A_2 and B_2 to the untrusted third party (Charlie) through two insecure quantum channels, i.e., channel_{AC} and channel_{BC}.

(2) *Bell measurement.* Charlie applies Bell detection of the received quantum states. Modes A' and B' are combined with a balanced beam splitter with output C and D and, afterwards, x quadrature of mode C and p quadrature of mode D are measured with homodyne detectors. The results of joint measurement x_C and p_D are announced to Alice and Bob through public classical channel.

(3) *Displacement.* After receiving Charlie's measurement results $\{x_C, p_D\}$, Bob applies local displacement operations $D(\beta)$ on mode B_1 to get mode $B_1{}'$, where $\beta = g(x_C + p_D)$ and g is the gain of this operation related to the total channel loss.

(4) *Measurement.* Alice and Bob measure the $2N$ modes using homodyne detection which randomly detects the x quadrature or p quadrature and the measurement outcomes are discretized with the finite range analog-to-digital converter (ADC). For every two modes A_1 and $B_1{}'$, Alice gets the data $\{X_A(P_A)\}$ and Bob gets the data $\{X_B(P_B)\}$, respectively.

(5) *Sifting.* Both of two communication parties announce which quadrature they choose through an authentic pubic channel. They hold the data in which the selected quadratures are the same and discard the rest. The length of effective data after this step reduces to about N in each party.

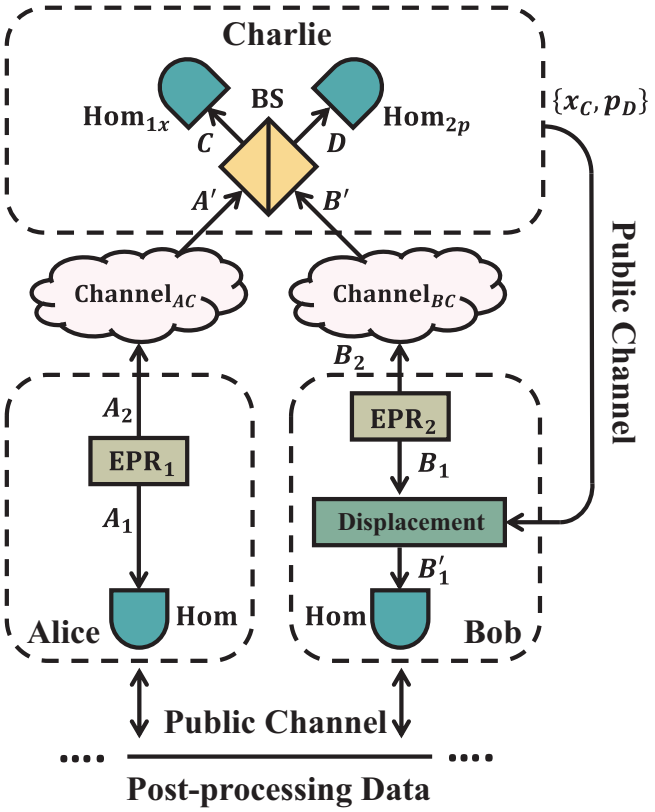

FIG. 1. EB scheme of the squeezed-state CV-MDI QKD protocol. EPR: two-mode squeezed state. Hom: homodyne detection. Hom$_{1x}$: homodyne detection of measuring the x quadrature. Hom$_{2p}$: homodyne detection of measuring the p quadrature. X_C (P_D): measurement results of Hom$_{1x}$ (Hom$_{2p}$). BS: 50:50 balanced beam splitter. Channel$_{AC}$ (Channel$_{BC}$): totally untrusted quantum channel between Alice (Bob) and Charlie controlled by adversary. Public channel: authenticated channel used for classical communication.

(6) *Channel parameter estimation.* Once Alice and Bob have collected sufficient correlated data, they use the public channel to perform parameter estimation to check the correlation between their data. The two parties randomly choose a common subset of length k_{pe} from the sifted data and estimate the average distance between their samples:

$$d\left(X_A^{pe}, X_B^{pe}\right) = \frac{1}{k_{pe}} \sum_{i=1}^{k_{pe}} \left| X_{A,i}^{pe} - X_{B,i}^{pe} \right|, \tag{2}$$

where $X_A^{pe} = (X_{A,i}^{pe})_{i=1}^{k_{pe}}$ and $X_B^{pe} = (X_{B,i}^{pe})_{i=1}^{k_{pe}}$. If $d(X_A^{pe}, X_B^{pe})$ is smaller than a certain parameter d_0, they proceed and, otherwise, the protocol aborts. The parameter d_0 is the distance between the measurement results of Alice and Bob, which should be chosen small enough to ensure the data are correlated enough. Data X_A^{pe} and X_B^{pe} are also used to estimate the amount of information needed in the error correction step.

(7) *Error correction.* Alice sends some information to Bob and Bob corrects the errors in his data using an error reconciliation algorithm (direct reconciliation), or Alice corrects the errors in her data with the help of Bob sending information (reverse reconciliation). It may cost a length of ℓ_{EC} secret keys during the error correction phase. After that, two parties do the hash check [28], i.e., they expend the length of k_{check} extra data to check if both hashes coincide. If this check passes, the protocol resumes; otherwise, it aborts.

(8) *Calculation of secret key length.* Alice and Bob calculate the secret key length ℓ according to the presented secret key length formula and entropic uncertainty relation which will be shown in Sec. II C. If the secret key length is negative, they abort the protocol.

(9) *Privacy amplification.* Both of two communication parties apply a hash function [62] on their corrected strings respectively to generate the secret key of length ℓ.

C. Uncertainty relation and secret key rate

In previous researches of CV-QKD, in general, a practical homodyne detector is modeled as an ideal homodyne detector and an ADC with finite range [28]. To illustrate the measurement phase in our protocol more clearly, without loss of generality, we model the homodyne detector as an ideal homodyne detector followed by an ADC with finite range and divide the measurement process into two steps. First, Alice and Bob use ideal homodyne detectors to measure the quadratures of the states that they received (ρ_{A_1} and $\rho_{B_1'}$ in Fig. 1). The outputs of ideal homodyne detectors ($\{Q_A, P_A\}$, $\{Q_B, P_B\}$) in two sides are ideal continuous variables with infinite range, and the statistical distribution of each outcome should generally follow a Gaussian distribution.

It is important for the protocol to have high correlations between two parties' outcomes. However, due to the channel losses, the quadratures x and p at Alice and Bob's sides ($\{Q_A, P_A\}$,$\{Q_B, P_B\}$) will decay. In order to handle that, the quadrature measurements in one of two parties $\{Q_A, P_A\}$ or $\{Q_B, P_B\}$ need to be rescaled before grouping into the intervals. We use the transformations below (using Alice as an example):

$$Q_A \to \tilde{Q}_A = t_q Q_A, \quad P_A \to \tilde{P}_A = t_p P_A, \tag{3}$$

where t_q and t_p denote the rescaling factors related to the channel loss of channel$_{AC}$ and channel$_{BC}$ (see Appendix A about the estimation). After that, the data between Alice and Bob should be correlated enough.

In step (2), Alice and Bob use ADCs with finite sampling range and finite resolution to discretize the continuous quadratures $\{\tilde{Q}_A, \tilde{P}_A\}$ and $\{Q_B, P_B\}$ into different intervals: $(-\infty, -\alpha]$, $(-\alpha, -\alpha+\delta]$, …, (α, ∞). Here, α is the maximum discretization range of ADC, which takes the finite range of detectors into consideration in the security proof, and δ denotes the precision of the measurement. The corresponding outcome alphabet is denoted by $\chi = \{1, 2, \ldots, 2\alpha/\delta\}$, where we assume $2\alpha/\delta \in \mathbb{N}$ and every measurement outcome corresponds to one of the intervals. Therefore, the data $\{X_A, P_A\}$ in Alice's side is obtained by discretizing the quadrature measurements $\{\tilde{Q}_A, \tilde{P}_A\}$; likewise the data in Bob's side.

It should be noted that practical homodyne detection may lead to security problems since its outputs lack information of the quadratures. For instance, in equal-length intervals $(-\alpha, -\alpha+\delta]$, …, $(\alpha-\delta, \alpha]$, owing to the finite sampling bits, any measurement outcomes inside of one sampling interval will map to the same value and it may cause a lack of the details about the state within each sampling interval, for one cannot determine whether the distribution of measured states is Gaussian distribution or other non-Gaussian distribution.

Moreover, we assume that any information in another two infinite-length intervals $(-\infty, -\alpha]$ and $[\alpha,\infty)$ will also map to one value as a result of the finite sampling range property of ADC, e.g., one cannot distinguish whether the measured pulse is a low-energy pulse or a high-energy pulse, which makes the measurement outcomes short of the information about the state outside the range. Those imperfect features of detection may open the loophole to a potential Eve and a number of attacks, such as large energy attack, may be exploited to reduce the security of the protocol. There are in general two approaches to handle that problem. One is using the method as Ref. [32] did by trusting Alice's and Bob's devices and another solution is adding the energy test to provide detailed information about measured states (as Ref. [33] did) to replace the trusted source assumption. This paper follows the former solution and assumes that Alice and Bob produce trusted states with quadratures being larger than α with very small probability p_α.

After the measurement step is done, the physical steps of the protocol are finished, and the rest of the protocol is treated as the postprocessing part aiming at extracting secure keys from the raw keys. Due to the leftover hash lemma, the ε_c-correct and ε_s-secret key of length ℓ can be extracted [63], which satisfies

$$\ell \leqslant H_{\min}^{\varepsilon}(X_A|E)_\omega - \ell_{EC} - O\left(\log_2 \frac{1}{\varepsilon_s \varepsilon_c}\right), \tag{4}$$

where ℓ_{EC} denotes the leakage information in the error correction phase and $H_{\min}^{\varepsilon}(\cdot)$ is the smooth min-entropy with smoothing parameter ε. $H_{\min}^{\varepsilon}(X_A|E)$ is the smooth conditional min-entropy of data X_A conditioned on the information Eve may have, which quantifies Eve's uncertainty about Alice's measurement outcomes. In the coherent attack cases, the goal is to bound the smooth min-entropy $H_{\min}^{\varepsilon}(X_A|E)$ conditioned on the event that the protocol does not abort. Different from the parameter estimation method in Ref. [53], the smooth min-entropy $H_{\min}^{\varepsilon}(X_A|E)$ can be estimated with the help of the entropic uncertainty relation conditioned on side information with infinite-dimensional quantum memories [32] in our paper.

Entropic uncertainty relations are used in some security proofs of QKD protocols giving their power to describe the bounds of guessing uncertainty Eve may have, when both Alice and Bob perform measurements in two random bases in a certain tripartite quantum system. There is a large family of entropy uncertainty relations with both infinite-dimensional and finite-spacing formulas [55]. However, a more operational way to express uncertainty is in terms of the discrete Shannon entropy rather than differential relations, so we follow the above to calculate the secret key length with the discrete Shannon entropy version of uncertainty relation, and quantum side information is considered with smooth min- and max-entropies.

The scenario of uncertainty relations can be understood as follows. The tripartite state ω_{ABE} with Alice, Bob, and Eve holds infinite-dimensional quantum systems A, B, and E, respectively. Alice randomly measures quadrature x or p on state $\omega_A = \mathrm{Tr}_{BE}[\omega_{ABE}]$ in each run and stores the outcomes in one of two classical systems. The same operation is done at Bob's side acting at $\omega_B = \mathrm{Tr}_{AE}[\omega_{ABE}]$. The outcome strings are denoted by $\{X_A, P_A\}$ and $\{X_B, P_B\}$, respectively. After sifting, two pairs of random strings $\{X_A, X_B\}$ and $\{P_A, P_B\}$ should obey the uncertainty principle and Eve cannot predict Alice and Bob's measurement outcomes precisely. Hence the relation between smooth min- and max-entropies satisfies

$$H_{\min}^{\varepsilon}(X_A|E)_\omega \geqslant n \log_2 \frac{1}{c(\delta)} - H_{\max}^{\varepsilon'}(X_A|X_B)_\omega. \tag{5}$$

Here we assume the random selection is identically and independently distributed. The term $c(\delta)$ is the "incompatibility" of the measurement operators and $H_{\max}^{\varepsilon'}(X_A|X_B)_\omega$ is the smooth max-entropy between the data of Alice and Bob with smoothing parameter ε', which reads

$$\varepsilon' = \varepsilon_s/(4p_{\text{pass}}) - 2f(p_\alpha, n)/\sqrt{p_{\text{pass}}}, \tag{6}$$

with $f(p_\alpha, n) = \sqrt{2[1-(1-p_\alpha)^n]}$ [32], which is the function considered about the probability of the event outside of the detection range $[-\alpha,\alpha]$. $c(\delta)$ takes the measurement discretization into consideration, which is

$$c(\delta) = \frac{1}{2\pi}\delta^2 S_0^{(1)}\left(1, \frac{\delta^2}{4}\right)^2, \tag{7}$$

where $S_0^{(1)}$ denotes the zeroth radial prolate spheroidal wave function of the first kind [64]. $c(\delta)$ can be well approximated with $c(\delta) \approx \delta^2/(2\pi)$ when the length of interval δ is small. For a certain value of δ, $c(\delta)$ is a constant also, so the value of smooth min-entropy $H_{\min}^{\varepsilon}(X_A|E)$ can be estimated by upper bounding the smooth max-entropy $H_{\max}^{\varepsilon'}(X_A|X_B)$ between random strings X_A and X_B.

To estimate the upper bound of $H_{\max}^{\varepsilon'}(X_A|X_B)$, the correlation of the data between Alice and Bob needs to be qualified first. Alice and Bob randomly choose a subset $\chi^{k_{pe}}$ with string length k_{pe} to calculate the average distance $d(X_A^{pe}, X_B^{pe})$ between their data X_A^{pe} and X_B^{pe} in the parameter estimation step, where pe stands for parameter estimation. If $d(X_A^{pe}, X_B^{pe}) < d_0$, the ε'-smooth max-entropy can be bounded by

$$H_{\max}^{\varepsilon'}(X_A|X_B) \leqslant n \log_2 \gamma(d(X_A, X_B)), \tag{8}$$

where γ is a function arising from a large deviation consideration, which reads

$$\gamma(t) = (t + \sqrt{t^2+1})[t/(\sqrt{t^2+1} - 1)]^t. \tag{9}$$

Using sampling theory, the quantity $d(X_A, X_B)$ can be estimated by $d(X_A^{pe}, X_B^{pe})$ plus a correction μ with high probability. μ quantifies its deviation to $d(X_A, X_B)$ considered about the finite-size statistical fluctuation. Finally, the ℓ length secret key can be extracted from the remaining data $X_A, X_B \in \chi^n$ with the length of n, which is written as

$$\ell = n\left[\log_2 \frac{1}{c(\delta)} - \log_2 \gamma(d_0 + \mu)\right] - \ell_{EC} - \log_2 \frac{1}{\varepsilon_s^2 \varepsilon_c} \tag{10}$$

and

$$\mu = \frac{2\alpha}{\delta}\sqrt{\frac{N(k_{pe}+1)}{nk_{pe}^2} \ln \frac{1}{\varepsilon'}}. \tag{11}$$

Here the remaining data has a length $n = N - k_{pe} - k_{\text{check}}$ approximately, for some raw keys were cut off from the test steps above.

There are two main elements of Eq. (10): one is the estimation of smooth min-entropy $H_{\min}^{\varepsilon}(X_A|E)$ and the other

is the leakage information ℓ_{EC} during error correction. The former, as mentioned above, can be estimated by the date X_A^{pe} and X_B^{pe}, which is independent to the reconciliation methods [65], while the latter is determined by the information reconciliation; hence Eq. (10) can be exploited to calculate the secret key rate in both direct and reverse reconciliation cases.

For the direct reconciliation case, the leakage information in the error correction step reads

$$\ell_{EC}^{DR} = H(X_A) - \beta I(X_B : X_A), \tag{12}$$

and in the reverse reconciliation case it reads

$$\ell_{EC}^{RR} = H(X_B) - \beta I(X_B : X_A), \tag{13}$$

where $H(X_A)$ and $H(X_B)$ denote the discrete Shannon entropies and $I(X_B : X_A)$ is the mutual information between Alice and Bob.

III. NUMERICAL SIMULATION AND DISCUSSION

In this section, we focus on the simulation results of the squeezed-state CV-MDI QKD protocol in the ideal detection case against coherent attacks. Section II C illustrates that the simulation of secret key rate in our protocol can be divided into two parts: one is the estimation of smooth min-entropy $H_{\min}^{\varepsilon}(X_A|E)$ considering finite-size effect; the other is the leakage information ℓ_{EC} in error correction, which could be calculated with the help of the covariance matrix. Only the extremely asymmetric cases are discussed here as the examples, where Bob is located at Charlie's side ($T_{BC} = 0$), for the transmission distance can reach the maximum [43]. The discussion of symmetric cases can be seen in Appendix D considering more general attack strategy.

Considering the EB version of the squeezed-state CV-MDI QKD protocol (Fig. 1), the covariance matrix can be estimated by Alice and Bob's data directly in experiment, and here, without loss of generality, we assume that channels$_{AC}$ and channels$_{BC}$ are under two independent entangling cloner attacks to estimate the covariance matrix. We should point out that Eve's attack described here is not the optimal one [44,66]. The entangling cloner attack is usually used to model a Gaussian channel affected by the environment and is analyzed to get a sense of a protocol's performance in experiment [43], and, in experiment, we can calculate the amount of information used in the error correction phase in a parameter estimation step without assuming which attack Eve may use. Moreover, the estimation of leakage information does affect the final secret key rate, but does not induce statistical fluctuation introduced by the parameter estimation step, and all the statistical fluctuation introduced by parameter estimation has been considered in the estimation of max-entropy. Detailed derivation of the covariance matrix can be seen in Appendix B. First, Alice and Bob generate two-mode squeezed states $\rho_{A_1A_2}$ and $\rho_{B_1B_2}$, respectively. The covariance matrices $\gamma_{A_1A_2}$ and $\gamma_{B_1B_2}$ read

$$\gamma_{A_1A_2} = \begin{pmatrix} V_A\mathbb{I}_2 & \sqrt{V_A^2-1}\sigma_z \\ \sqrt{V_A^2-1}\sigma_z & V_A\mathbb{I}_2 \end{pmatrix}, \tag{14}$$

$$\gamma_{B_1B_2} = \begin{pmatrix} V_B\mathbb{I}_2 & \sqrt{V_B^2-1}\sigma_z \\ \sqrt{V_B^2-1}\sigma_z & V_B\mathbb{I}_2 \end{pmatrix}, \tag{15}$$

where $\mathbb{I}_2$ is the identity matrix, $V_{A(B)}$ stands for the variance of Alice (Bob)'s two-mode squeezed state from Eve's view, and $\sigma_z = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$.

Before Charlie applies Bell measurement to mode C and mode D, the whole state $\rho_{A_1CDB_1}$ can be described by an 8×8 covariance matrix $\gamma_{A_1CDB_1}$. Then modes A' and B' received by Charlie interfere at a beam splitter (BS) with two output C and D modes measured by homodyne detections, respectively. The measurement results x_C and p_D are announced by Charlie in a public channel so that Bob can displace mode B_1 to B_1'. It is easy to get the covariance matrix $\gamma_{A_1B_1'}$ of the state $\rho_{A_1B_1'}$ shared by Alice and Bob, which reads

$$\gamma_{A_1B_1'} = \begin{pmatrix} V_A\mathbb{I}_2 & \sqrt{T\left(V_A^2-1\right)}\sigma_z \\ \sqrt{T\left(V_A^2-1\right)}\sigma_z & [T(V_A-1)+1+Te]\mathbb{I}_2 \end{pmatrix}, \tag{16}$$

where

$$T = \frac{T_1}{2}g^2. \tag{17}$$

T stands for the equivalent channel transmittance between Alice and Bob, T_1 is the channel transmittance between Alice and Charlie, and g is the gain of displacement. The equivalent excess noise e is given by

$$e = 1 + \frac{1}{T_1}[2 + T_2(\varepsilon_2 - 2) + T_1(\varepsilon_1 - 1)] + \frac{1}{T_1}\left(\frac{\sqrt{2}}{g}\sqrt{V_B - 1} - \sqrt{T_2}\sqrt{V_B + 1}\right)^2. \tag{18}$$

In the numerical simulation, one can select $g = \sqrt{\frac{2}{T_2}}\sqrt{\frac{V_B-1}{V_B+1}}$ so that the equivalent excess noise e is optimal [42]. Therefore, we can get

$$e = \varepsilon_1 + \frac{1}{T_1}[T_2(\varepsilon_2 - 2) + 2]. \tag{19}$$

Accordingly, the discrete Shannon entropies $H(X_A)$ and $H(X_B)$ have the following forms when δ is small (see Appendix C about the detailed derivation):

$$H(X_A) \approx \log_2(\sqrt{2\pi e V_A}) - \log_2(\delta) \tag{20}$$

and

$$H(X_B) \approx \log_2(\sqrt{2\pi e V_B'}) - \log_2(\delta), \tag{21}$$

where $V_B' = T(V_A - 1) + 1 + Te$. The mutual information between Alice and Bob can be well approximated, which reads

$$I(X_A : X_B) \approx \frac{1}{2}\log_2\left(\frac{V_A + \chi}{\chi + \frac{1}{V_A}}\right), \tag{22}$$

where $\chi = \frac{1}{T} - 1 + e$. Once we have obtained the form of the covariance matrix in the EB model, with the help of Eq. (10), the secret key rate against coherent attack in both direct reconciliation and reverse reconciliation cases can be calculated.

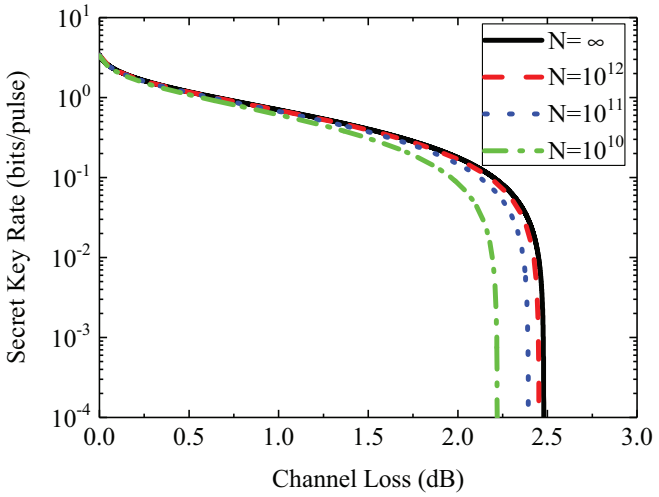

FIG. 2. Secret key rates of squeezed-state CV-MDI QKD protocol against coherent attack in the extremely asymmetric cases ($T_{BC} = 0$) with direct reconciliation in the frame of composable security. Those lines are under the ideal conditions with ideal modulation variances $V_A = V_B = 10^5$ and perfect reconciliation efficiency $\beta = 1$. The block lengths from left to right curves show $N = 10^{10}$ (green dot-dashed line), 10^{11} (blue dot line), 10^{12} (red dashed line), and ∞ (black solid line), respectively. Here the discretization parameter is set to $d = 13$, the excess noise $\varepsilon_1 = \varepsilon_2 = 0.002$, and the overall security parameter is smaller than 10^{-20}.

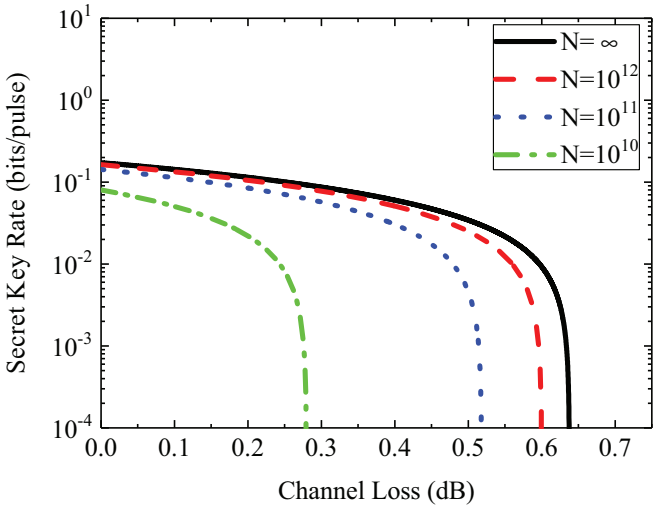

FIG. 3. Secret key rates of squeezed-state CV-MDI QKD protocol against coherent attack in the extremely asymmetric cases ($T_{BC} = 0$) with direct reconciliation. The protocol with practical modulation variances $V_A = V_B = 5.04$ and imperfect reconciliation efficiency $\beta = 96.9\%$ is considered. The block lengths from left to right curves are $N = 10^{10}$ (green dot-dashed line), 10^{11} (blue dot line), 10^{12} (red dashed line), and ∞ (black solid line), respectively. The discretization parameter, excess noises, and security parameters are chosen as in the case of ideal modulation.

A. Direct reconciliation protocol

First, numerical simulations of the secret-key rate in the direct reconciliation cases are performed. The performance of the extremely asymmetric structure with ideal modulation variances ($V_a = V_b = 10^5$) is given in Fig. 2. The perfect reconciliation efficiency ($\beta = 1$) is set to get the optimal performance of this protocol against coherent attacks. The interval parameter is set to $\alpha = 52$ [32], the discretization parameter $d = 13$, the excess noises $\varepsilon_1 = \varepsilon_2 = 0.002$, and the overall security parameter is smaller than 10^{-20}. The block length of information reconciliation k_{pe} can be optimized in experiment. If k_{pe} is too large, the final key rate may decrease due to a small quantity of raw key using for generating secret keys. On the contrary, one may not get accurate estimation of the channel parameters if k_{pe} is too small. In this simulation, we choose the block length of information reconciliation about $1/10$ of the total length, i.e., $k_{pe} = N/10$. It can be seen that, when the block length is infinite size ($N = \infty$), the protocol reaches the longest transmission distance, with a corresponding channel loss of about 2.5 dB. In the $N = 10^{12}$ case, the protocol is closed to the asymptotic rate.

The realistic performance is described under the condition that the practical variances are $V_A = V_B = 5.04$ (referring to 10 dB squeezing) and imperfect reconciliation efficiency is set to $\eta = 96.9\%$. The key rate of a realistic extremely asymmetric case of the CV-MDI QKD protocol is described in Fig. 3. We plot the key rate as a function of the channel loss T_{AC}, while the channel loss T_{BC} is set to 0 dB, with different block lengths of 10^{10}, 10^{11}, 10^{12} and infinite size. For the asymptotic case $N \to \infty$, the maximum tolerable channel loss can reach approximately 0.64 dB (black solid line), which shows a distance between practical and ideal cases. The practical performance can be optimized using squeezed states with higher squeeze factor [67].

What's more, for given distances, we plot the secret key rate vs the block size when both ideal and practical parameters are given (Fig. 4). The channel losses are 0.2 dB, 0.4 dB, and 0.5 dB, respectively. When the block length reduces, the secret key rate decreases rapidly and one cannot generate secret key when the block length is smaller than 10^{10} under the practical parameters.

B. Reverse reconciliation protocol

Similar to the direct reconciliation case, the protocol's performance under reverse reconciliation can be illustrated using the same method. The smooth maximum entropy is the same with that of the direct reconciliation case, while the leakage information is different.

Both ideal cases and practical cases are taken into consideration and the parameters we choose are the same with those of the direct reconciliation cases. Here large variances $V_A = V_B = 10^5$ are chosen first to illustrate the performance of ideal modulation (Fig. 5), then the practical variances $V_A = V_B = 5.04$ are exploited to show the realistic performance (Fig. 6). $N = 10^{10}$, $N = 10^{11}$, $N = 10^{12}$, and the asymptotic regime are considered here as well. For a realistic performance of fiber loss 0.2 dB/km, the total loss can be up to 6.5 dB in the ideal condition and 3.6 dB in the practical condition, corresponding to 32.5 km and 18 km, respectively. Hence the reverse reconciliation cases could be feasible in metropolitan range communications.

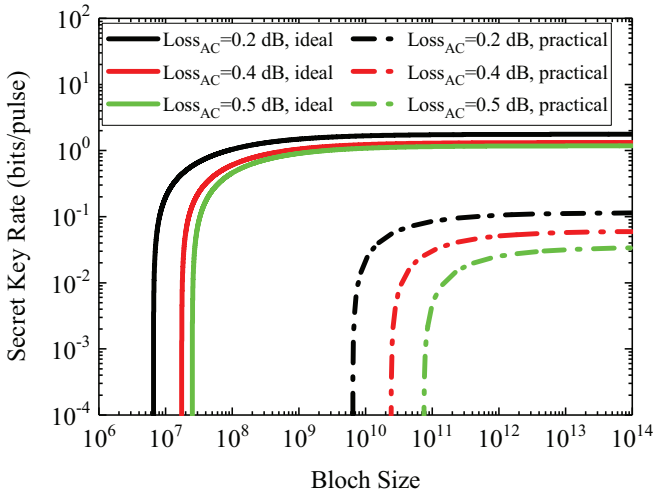

FIG. 4. Secret key rates vs block size for the extremely asymmetric case ($T_{BC} = 0$) with direct reconciliation. The solid lines are under the ideal condition where modulation variances $V_A = V_B = 10^5$ and perfect reconciliation efficiency $\beta = 1$. The dot-dashed lines are under the practical condition where practical modulation variances $V_A = V_B = 5.04$ and imperfect reconciliation efficiency $\beta = 96.9\%$. From left to right, the transmittance of the quantum channel corresponds to loss of 0.2 dB (black line), 0.4 dB (red line), and 0.5 dB (green line), respectively.

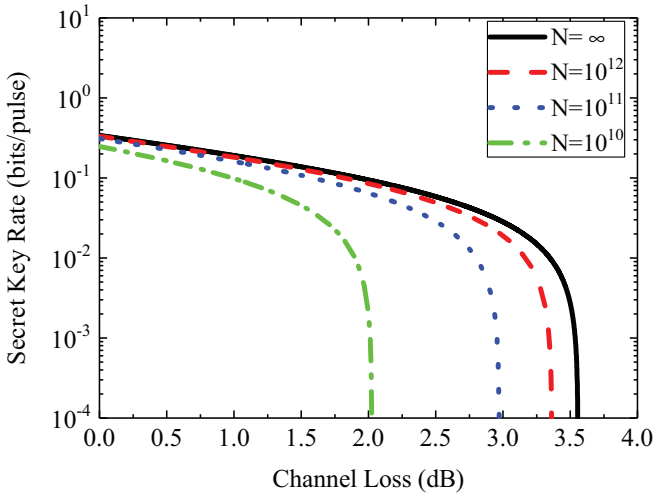

FIG. 6. Secret key rates of squeezed-state CV-MDI QKD protocol against coherent attack in the extremely asymmetric case ($T_{BC} = 0$) with reverse reconciliation. The protocol is under practical modulation variances $V_A = V_B = 5.04$ and imperfect reconciliation efficiency $\beta = 96.9\%$. The block lengths from left to right curves are $N = 10^{10}$ (green dot-dashed line), 10^{11} (blue dot line), 10^{12} (red dashed line), and ∞ (black solid line), respectively. The discretization parameter, excess noises, and security parameters are chosen as in the case of ideal modulation.

Figure 7 shows the relation between block size and secret key rate in the extremely asymmetric circumstance. It illustrates that it is in principle possible to generate secret keys for block sizes of $10^7 - 10^{12}$ in the reverse reconciliation case, depending on channel losses and the required level of security, which is easier to achieve than the direct case.

In general, our numerical simulation results show that the protocol can tolerate at most 2.5 dB channel loss with direct reconciliation and 6.5 dB channel loss with reverse

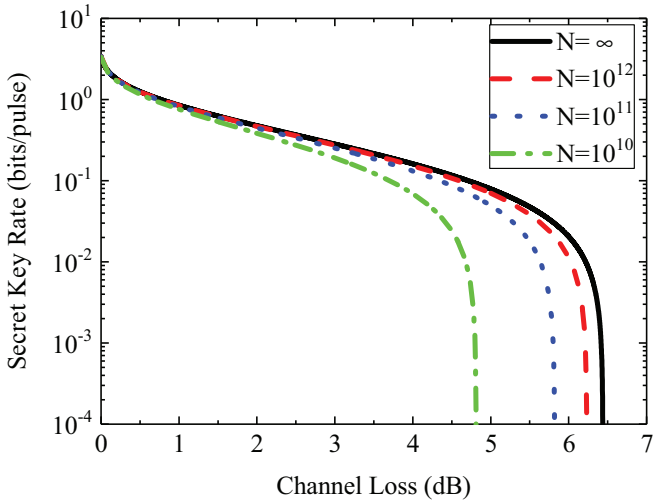

FIG. 5. Secret key rates of squeezed-state CV-MDI QKD protocol against coherent attack in the extremely asymmetric case ($T_{BC} = 0$) with reverse reconciliation. The protocol is under ideal modulation variances $V_A = V_B = 10^5$ and perfect reconciliation efficiency $\beta = 1$. The block lengths from left to right curves correspond to $N = 10^{10}$ (green dot-dashed line), 10^{11} (blue dot line), 10^{12} (red dashed line), and ∞ (black solid line), respectively. Here the discretization parameter is set to $d = 13$, the excess noise to $\varepsilon_1 = \varepsilon_2 = 0.002$, and the overall security parameter is smaller than 10^{-20}.

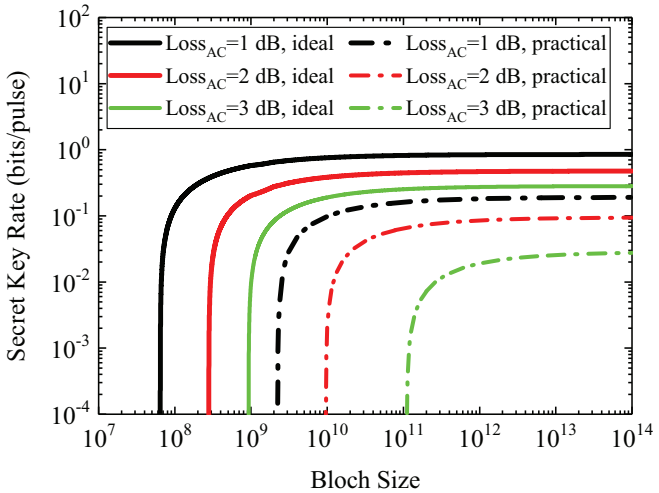

FIG. 7. Secret key rates vs block size for the extremely asymmetric case ($T_{BC} = 0$) with reverse reconciliation. The solid lines are under the ideal condition that modulation variances $V_A = V_B = 10^5$ and perfect reconciliation efficiency $\beta = 1$. The dot-dashed lines are under the practical condition that practical modulation variances $V_A = V_B = 5.04$ and imperfect reconciliation efficiency $\beta = 96.9\%$. From left to right, the transmittance of the quantum channel corresponds to loss of 1 dB (black line), 2 dB (red line), and 3 dB (green line), respectively.

reconciliation against coherent attacks in the extremely asymmetric scenario. Meanwhile, the secret key rate is reduced considering the practical squeezing parameter and imperfect reconciliation efficiency. Finite-size effect is also discussed apart from asymptotic regime. When the block size is of the order of 10^7–10^{12}, one can achieve high secret key rates depending on the channel loss; thus it is practical on the metropolitan scale with current technologies.

IV. CONCLUSION

In this paper, we present a composable security analysis for squeezed-state CV-MDI QKD against general coherent attacks. Its security analysis is derived based on the entanglement-based scheme and a version of state-independent entropic uncertainty relation is exploited to give a lower bound on the conditional smooth min-entropy by trusting Alice's and Bob's devices. Finite-size effect is also taken into consideration, and we use two independent entangling cloner attacks to simulate the performance of the method in both direct and reverse reconciliation cases. The simulation results show that, in extremely asymmetric scenarios, the protocol can tolerate 2.5 dB and 0.64 dB channel losses under ideal and practical conditions with direct reconciliation, and 6.5 dB and 3.6 dB channel losses under ideal and practical conditions with reverse reconciliation. An interesting extension to this paper would be to further add the energy test to remove the trusted source assumption.

ACKNOWLEDGMENTS

This work is supported by the National Natural Science Foundation (Grant No. 61531003), the National Science Fund for Distinguished Young Scholars of China (Grant No. 61225003), and China Postdoctoral Science Foundation (Grant No. 2018M630116).

APPENDIX A: ESTIMATION OF t_q AND t_p IN MEASUREMENT STAGE

The usage of t_q and t_p in Eq. (3) in the main text is to ensure that the discreted data between Alice and Bob have strong correlation after states passing through channels. In order to guarantee the difference between the data collected by Alice and Bob is small enough, one possible solution is to rescale one of two communicated parties' data such that the second moments of Alice's and Bob's amplitude and phase measurement match.

Suppose Alice and Bob randomly choose amplitude strings $\{X_A, X_B\}$ of length m and phase strings $\{P_A, P_B\}$ of length j to estimate parameters t_q and t_p, respectively. Here the estimation of t_q is demonstrated as an example and that of t_p can be calculated using the same method.

First, considering the scenario where there is no rescaled and discretization processes in the measurement phase, theoretically the average value of amplitude measurement outcomes both in Alice's and Bob's sides can be estimated by

$$\hat{E}(Q_A) = \frac{1}{m}\sum_{i=1}^{m} Q_A^i, \quad \hat{E}(Q_B) = \frac{1}{m}\sum_{i=1}^{m} Q_B^i, \tag{A1}$$

and the variance of amplitude measurement outcomes both in Alice's and Bob's sides can be written as

$$\hat{\sigma}(Q_A) = \frac{1}{m}\sum_{i=1}^{m}\left(Q_A^i - \hat{E}(Q_A)\right)^2 \tag{A2}$$

and

$$\hat{\sigma}(Q_B) = \frac{1}{m}\sum_{i=1}^{m}\left(Q_B^i - \hat{E}(Q_B)\right)^2. \tag{A3}$$

After taking the rescaled process into account, the estimators of new date $\tilde{Q}_A$ should satisfy the following forms:

$$\hat{E}(\tilde{Q}_A) = \frac{1}{m}\sum_{i=1}^{m}\tilde{Q}_A^i, \tag{A4}$$

$$\hat{\sigma}(\tilde{Q}_A) = \frac{1}{m}\sum_{i=1}^{m}\left[\tilde{Q}_A^i - \hat{E}(\tilde{Q}_A)\right]^2. \tag{A5}$$

In order to match the variances of Alice's and Bob's measurement data, the values of Eqs. (A3) and (A5) should be the same. When the discretization process is done, the parameter t_q can be estimated by

$$t_q = \sqrt{\frac{\sum_{i=1}^{m}\left(X_B^i - \hat{E}(X_B)\right)^2}{\sum_{i=1}^{m}\left(X_A^i - \hat{E}(X_A)\right)^2}}, \tag{A6}$$

where $\hat{E}(\cdot)$ is the estimator of the average value of measured data. Therefore, parameter t_p can be written using the same estimation method, which reads

$$t_p = \sqrt{\frac{\sum_{i=1}^{j}\left(P_B^i - \hat{E}(P_B)\right)^2}{\sum_{i=1}^{j}\left(P_A^i - \hat{E}(P_A)\right)^2}}. \tag{A7}$$

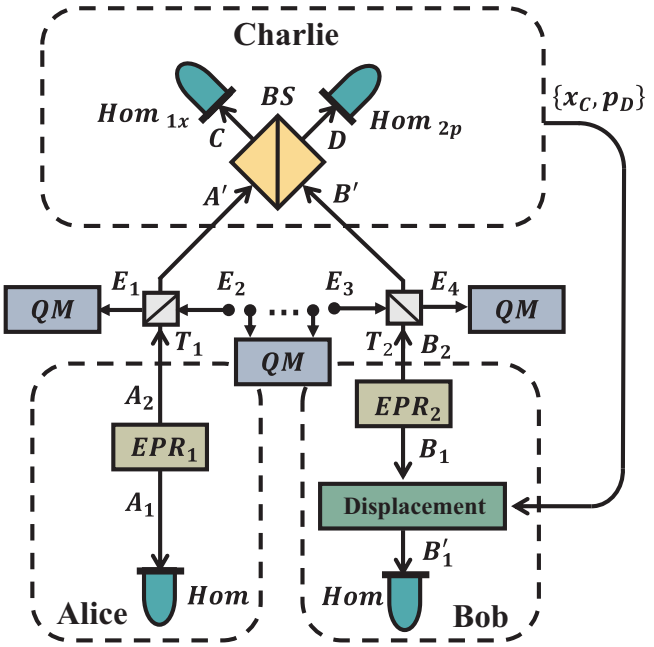

FIG. 8. EB scheme of the squeezed-state CV-MDI QKD protocol with Eve's attacks. After two channels, mode A_2 becomes A' and mode B_2 becomes B'. QM is the quantum memory.

APPENDIX B: DERIVATION OF COVARIANCE MATRICES

Considering the EB version of the squeezed-state CV-MDI QKD protocol, Eve's attacks can be modeled by two independent entangled-cloner attacks (shown in Fig. 8 and supposing modes E_2 and E_3 are independent for simplification), where channel$_{AC}$ and channel$_{BC}$ are replaced by two BS with transmittances T_1 and T_2, respectively. The covariance matrices of two BS can be written as

$$S_{BS}^{A(B)} = \begin{pmatrix} \sqrt{T_{1(2)}} & \sqrt{1-T_{1(2)}} \\ -\sqrt{1-T_{1(2)}} & \sqrt{T_{1(2)}} \end{pmatrix}, \tag{B1}$$

After passing two channels, mode A_2 becomes A', and mode B_2 becomes B', and the following relationships of quadratures hold:

$$\hat{A}' = \sqrt{T_1}\hat{A}_2 + \sqrt{1-T_1}\hat{E}_2 \tag{B2}$$

and

$$\hat{B}' = \sqrt{T_2}\hat{B}_2 + \sqrt{1-T_2}\hat{E}_3. \tag{B3}$$

Then Charlie applies Bell detection of the measured states. Modes A' and B' are combined with a balanced beam splitter with output modes C and D. Therefore, we can get modes C and D as

$$\hat{C} = \frac{1}{\sqrt{2}}(\hat{A}' - \hat{B}') = \frac{1}{\sqrt{2}}(\sqrt{T_1}\hat{A}_2 - \sqrt{T_2}\hat{B}_2) + \frac{1}{\sqrt{2}}(\sqrt{1-T_1}\hat{E}_2 - \sqrt{1-T_2}\hat{E}_3) \tag{B4}$$

and

$$\hat{D} = \frac{1}{\sqrt{2}}(\hat{A}' + \hat{B}') = \frac{1}{\sqrt{2}}(\sqrt{T_1}\hat{A}_2 + \sqrt{T_2}\hat{B}_2) + \frac{1}{\sqrt{2}}(\sqrt{1-T_1}\hat{E}_2 + \sqrt{1-T_2}\hat{E}_3). \tag{B5}$$

Before Charlie makes a Bell measurement to the C and D modes, the whole state $\rho_{A_1CDB_1}$ can be described by the 8×8 covariance matrix $\gamma_{A_1CDB_1}$, given by

$$\gamma_{A_1CDB_1} = \begin{pmatrix} V_A\mathbb{I}_2 & \sqrt{\frac{1}{2}T_1(V_A^2-1)}\sigma_z & \sqrt{\frac{1}{2}T_1(V_A^2-1)}\sigma_z & 0\mathbb{I}_2 \\ \sqrt{\frac{1}{2}T_1(V_A^2-1)}\sigma_z & \left[\frac{1}{2}T_1(V_A+\chi_1)+\frac{1}{2}T_2(V_A+\chi_2)\right]\mathbb{I}_2 & \left[\frac{1}{2}T_1(V_A+\chi_1)-\frac{1}{2}T_2(V_A+\chi_2)\right]\mathbb{I}_2 & \sqrt{\frac{1}{2}T_2(V_B^2-1)}\sigma_z \\ \sqrt{\frac{1}{2}T_1(V_A^2-1)}\sigma_z & \left[\frac{1}{2}T_1(V_A+\chi_1)-\frac{1}{2}T_2(V_A+\chi_2)\right]\mathbb{I}_2 & \left[\frac{1}{2}T_1(V_A+\chi_1)+\frac{1}{2}T_2(V_A+\chi_2)\right]\mathbb{I}_2 & -\sqrt{\frac{1}{2}T_2(V_B^2-1)}\sigma_z \\ 0\mathbb{I}_2 & \sqrt{\frac{1}{2}T_2(V_B^2-1)}\sigma_z & -\sqrt{\frac{1}{2}T_2(V_B^2-1)}\sigma_z & V_B\mathbb{I}_2 \end{pmatrix}, \tag{B6}$$

where ε_1 and ε_2 in $\chi_1 = 1/T_1 - 1 + \varepsilon_1$, $\chi_2 = 1/T_2 - 1 + \varepsilon_2$ are the excess noises of the corresponding channels.

The measurement results x_C and p_D are announced by Charlie in a public channel so that Bob can displace mode B_1 to B_1', whose relationships of quadratures read

$$\hat{B}'_{1x} = \hat{B}_{1x} + g\hat{C}_x = \left(\hat{B}_{1x} - g\sqrt{\frac{T_2}{2}}\hat{B}_{2x}\right) + g\sqrt{\frac{T_1}{2}}\hat{A}_{2x} + \frac{g}{\sqrt{2}}(\sqrt{1-T_1}\hat{E}_{2x} - \sqrt{1-T_2}\hat{E}_{3x}) \tag{B7}$$

and

$$\hat{B}'_{1p} = \hat{B}_{1p} + g\hat{D}_p = \left(\hat{B}_{1p} + g\sqrt{\frac{T_2}{2}}\hat{B}_{2p}\right) + g\sqrt{\frac{T_1}{2}}\hat{A}_{2p} + \frac{g}{\sqrt{2}}(\sqrt{1-T_1}\hat{E}_{2p} + \sqrt{1-T_2}\hat{E}_{3p}). \tag{B8}$$

Hence the covariance matrix $\gamma_{A_1B_1'}$ of the state $\rho_{A_1B_1'}$ can be written as Eq. (16) in the main text.

APPENDIX C: DERIVATION OF DISCRETE SHANNON ENTROPY

A continuous variable can always be approximated as a discrete variable with finite resolution digital discretization, and the smaller the discreted unit is, the closer the discrete variable is to the continuous variable.

Assuming that the variable x belongs to the interval $x \in [a,b]$, whose probability density function is denoted by $p(x)$, we divide this interval into n continuous intervals with same length δ, where $\delta = \frac{b-a}{n}$. According to the mean value theorem of integrals, there is a value x_i in each interval $x_i \in [a+(i-1)\delta, a+i\delta]$, where $i = 1,2,\ldots,n$, and x_i should satisfy

$$p_i = p(x_i)\delta = \int_{a+(i-1)\delta}^{a+i\delta} p(x)dx, \tag{C1}$$

where p_i is the probability in each interval. Therefore, the discrete Shannon entropy $H(x^\delta)$ can be derived by

$$\begin{aligned} H(x^\delta) &= -\sum_{i=1}^{n} p_i \log_2 p_i \\ &= -\sum_{i=1}^{n} p(x_i)\delta \log_2 [p(x_i)\delta] \\ &= -\sum_{i=1}^{n} p(x_i)\delta \log_2 p(x_i) - (\log_2 \delta)\sum_{i=1}^{n} p(x_i)\delta \\ &= -\sum_{i=1}^{n} p(x_i)\delta \log_2 p(x_i) - \log_2 \delta. \end{aligned} \tag{C2}$$

Here we use the relation $\sum_{i=1}^{n} p(x_i)\delta = 1$. The limit of $H(x^\delta)$ as δ approaches zero goes toward the entropy of continuous variable, which reads

$$\begin{aligned}\lim_{\delta\to 0} H_n(x^\delta) &= \lim_{\delta\to 0}\left[-\sum_{i=1}^{n} p_n(x_i)\delta\ \log_2 p_n(x_i) - \log_2\delta\right]\\ &= -\int_a^b p(x)\log_2 p(x)dx - \lim_{\delta\to 0}(\log_2\delta)\\ &\triangleq h(x) + H(\delta),\end{aligned} \tag{C3}$$

where $h(x) = -\int_a^b p(x)\log_2 p(x)dx$ denotes the differential entropy and $H(\delta) = -\lim_{\delta\to 0}(\log_2\delta)$.

Now consider a normal distribution

$$g(x) = \frac{1}{\sqrt{2\pi}\sigma}\exp\left(-\frac{x^2}{2\sigma^2}\right), \tag{C4}$$

with variance σ^2. The differential entropy of a normal distribution reads

$$\begin{aligned}h(x) &= -\int g(x)\log_2[g(x)]\\ &= -\int dx\ g(x)\left(-\frac{x^2}{2\sigma^2} + \frac{1}{2}\log_2(2\pi\sigma^2)\right)\\ &= \frac{1}{2} + \frac{1}{2}\log_2(2\pi\sigma^2)\\ &= \log_2(\sqrt{2\pi e\sigma^2}).\end{aligned} \tag{C5}$$

Supposing another continuous variable $y \in [a,b]$, the relationships $\int p(y)dy = 1$ and $\int p(x/y)dx = 1$ hold, where $p(x/y)$ is the conditional probability density function of x given y. Then

$$\begin{aligned}H(x^\delta/y^\delta) &= -\sum_j p(y_j)\delta\sum_i p(x_i/y_j)\delta\ \log_2[p(x_i/y_j)\delta]\\ &= -\sum_j p(y_j)\delta\sum_i p(x_i/y_j)\delta\ \log_2[p(x_i/y_j)]\\ &\quad - \log_2\delta,\end{aligned} \tag{C6}$$

and the limit of $H(x^\delta y^\delta)$ as δ approaches zero reads

$$\lim_{\delta\to 0} H(x^\delta/y^\delta) = h(x/y) + H(\delta), \tag{C7}$$

where $h(xy)$ is the conditional entropy of x given y, which reads

$$h(x/y) = -\iint p(y)p(x/y)\log_2 p(x/y)dx\,dy. \tag{C8}$$

Hence the mutual information $I(x^\delta : y^\delta)$ between discrete variables x^δ and y^δ, as approaches zero, can be approximated,

$$\begin{aligned}\lim_{\delta\to 0} I(x^\delta : y^\delta) &= \lim_{\delta\to 0}[H(x^\delta) - H(x^\delta/y^\delta)]\\ &= h(x) - \log_2\delta - (h(x/y) - \log_2\delta)\\ &= I(x : y),\end{aligned} \tag{C9}$$

where $I(x : y)$ is the mutual information between continuous variables x and y. Therefore, if the length of intervals δ is small enough, we can always regard the continuous variable mutual information $I(x : y)$ as the approximation of the discrete one.

APPENDIX D: SYMMETRIC CASES UNDER TWO CORRELATED MODE ATTACKS AND THE COMPARISON WITH THE PLOB BOUND

In the main text, the performance of squeezed-state CV-MDI QKD under coherent attacks has been discussed focusing on the extremely asymmetric cases ($T_{BC} = 0$). However, in the calculation of security key rate, all of the effects caused by the channel are usually treated as Eve's contribution. The optimal attack strategy provides the maximum information for Eve to reduce the security of the protocol to the greatest extent, so it is important to study the protocol under more general attack strategies.

According to Ref. [66], the covariance matrix of two correlated modes E_2 and E_3 measured by Eve (Fig. 8) has the following form:

$$\gamma_{E_2E_3} = \begin{pmatrix} V_{E_2}\mathbb{I}_2 & G\\ G & V_{E_3}\mathbb{I}_2\end{pmatrix}, \tag{D1}$$

where G is the correlation term. Supposing $V_{E_2} = V_{E_3} = V_E$, to achieve maximum correlation between Eve's modes, G is chosen as $\sqrt{V_E^2 - 1}\sigma_z$ due to the uncertainty principle, and the final covariance matrix of $\rho_{A_1B_1'}$ under the two correlated mode attack model is given by

$$\gamma_{A_1B_1'} = \begin{pmatrix} V_A\mathbb{I}_2 & \sqrt{T\left(V_A^2-1\right)}\sigma_z\\ \sqrt{T\left(V_A^2-1\right)}\sigma_z & [T(V_A-1)+1+Te']\mathbb{I}_2\end{pmatrix}. \tag{D2}$$

The equivalent excess noise e' reads

$$\begin{aligned}e' &= 1 + \frac{1}{T_1}[2 + T_2(\varepsilon_2 - 2) + T_1(\varepsilon_1 - 1) - C_E]\\ &\quad + \frac{1}{T_1}\left(\frac{\sqrt{2}}{g}\sqrt{V_B - 1} - \sqrt{T_2}\sqrt{V_B + 1}\right)^2,\end{aligned} \tag{D3}$$

where $C_E = \frac{2}{T_1}\sqrt{(1-T_1)(1-T_2)}\langle E_{2x}E_{3x}\rangle$ is the noise contribution of x quadrature induced by the correlation of Eve's two modes and $C_E = -\frac{2}{T_1}\sqrt{(1-T_1)(1-T_2)}\langle E_{2p}E_{3p}\rangle$ is the corresponding noise contribution of p quadrature.

If one of T_1 and T_2 is equal to zero, corresponding to the extremely asymmetric case (discussed in our main text), the contribution of the two modes' correlation in Eve's attack disappears, and the independent entangling cloner attack and two correlated mode attack are equivalent in this situation. Therefore, the model of the two independent entangling cloner attack can simplify our numerical simulation in the main text.

Under correlated mode attacks, the secret key rate formula is the same as that in the main text [Eq. (10)], but compared with independent entangling cloner attacks, the cases that both T_1 and T_2 are not equal to zero will increase the leakage information and then decrease the key rate in the two correlated mode attack model. Typically, in the symmetric case, where the

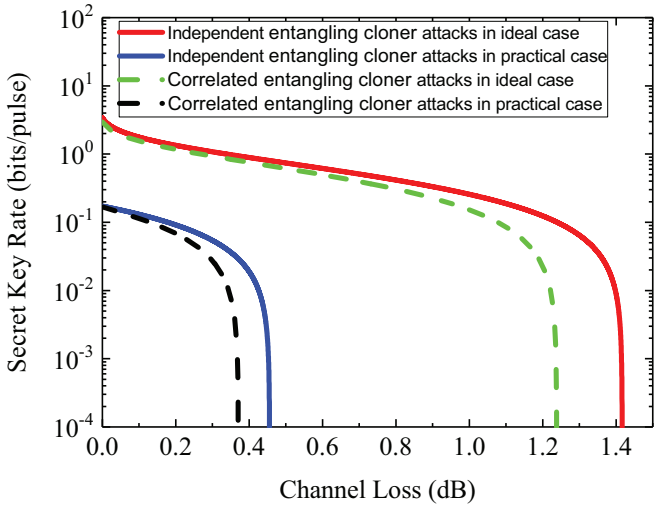

FIG. 9. Comparison of the secret key between the independent entangling cloner attacks model and correlated mode attacks model in the symmetric case. The ideal case is under ideal modulation variances $V_A = V_B = 10^5$ and perfect reconciliation efficiency $\beta = 1$. The practical case is with practical modulation variances $V_A = V_B = 5.04$ and imperfect reconciliation efficiency $\beta = 96.9\%$. The solid lines are the secret key rates under two independent entangling cloner attacks models. The dashed lines are the secret key rates under two correlated mode attacks models.

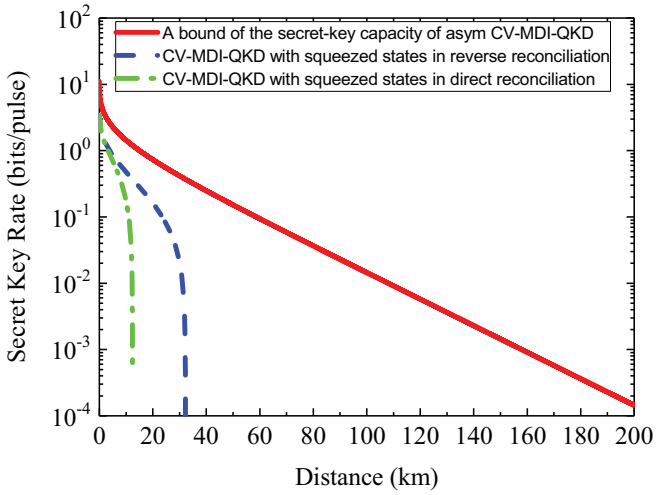

FIG. 10. Comparison of the secret key between the extremely asymmetric results and the PLOB bound. Our protocol is under ideal modulation variances $V_A = V_B = 10^5$ and perfect reconciliation efficiency $\beta = 1$. The red solid line is the bound of secret key capacity of asymmetric CV-MDI-QKD. The green dot-dashed line and the blue dashed line are the secret key rates of CV-MDI-QKD with squeezed states in direct and reverse reconciliation cases, respectively.

relay is located in the middle of Alice and Bob, we compare the results between two independent entangling cloner attacks and the two correlated mode attacks in Fig. 9, and the discussion is under the asymptotic regime.

It can be seen that, in the symmetric case, which is the worst case for the two correlated mode attacks (because the correlation term C_E reaches the maximum value), this correlated attack model will slightly degrade the performance of the protocol. Moreover, the more asymmetric the protocol, the smaller the impact of the correlated attack on the secret key rate.

In experiment, the covariance matrices can be obtained by data statistics, so there is no need to assume which model Eve's attack strategy belongs to before the protocol starts. If Eve's attack is stronger than the model we give in our simulation, the correlation between Alice and Bob's data will decline, so the estimation of max-entropy will increase, causing the decrease of the min-entropy. Moreover, Alice and Bob need to sacrifice more keys to do the error correction in classical postprocessing process, and it will leak more information to Eve. Therefore, if the two correlated mode attack is exploited by Eve, the secret key rate can still be calculated using Eq. (10) and it will not influence the security analysis of the protocol, but the secret key rate will decrease.

We also compare the extremely asymmetric results with the PLOB bound [68] shown in Fig. 10, which is the secret-key capacity of the lossy channel. It can be seen that, even though there is still a gap between the secret key rate of our protocol and the key capacity bound above, the final key rate can be improved using current technologies, such as the photon subtraction method [69–71] and the adding trusted noise method [43,72].

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
[3] S. L. Braunstein and P. van Loock, Rev. Mod. Phys. **77**, 513 (2005).
[4] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Rev. Mod. Phys. **84**, 621 (2012).
[5] E. Diamanti and A. Leverrier, Entropy **17**, 6072 (2015).
[6] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).
[7] F. Grosshans, G. Van Ache, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature (London) **421**, 238 (2003).
[8] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, Phys. Rev. Lett. **93**, 170504 (2004).
[9] S. Pirandola, S. Mancini, S. Lloyd, and S. L. Braunstein, Nat. Phys. **4**, 726 (2008).
[10] M. Sun, X. Peng, Y. Shen, and H. Guo, Int. J. Quantum Inf. **10**, 1250059 (2012).
[11] Y. C. Zhang, Z. Li, C. Weedbrook, S. Yu, W. Gu, M. Sun, X. Peng, and H. Guo, J. Phys. B **47**, 035501 (2014).
[12] C. Ottaviani, S. Mancini, and S. Pirandola, Phys. Rev. A **92**, 062323 (2015).
[13] C. Ottaviani and S. Pirandola, Sci. Rep. **6**, 22225 (2016).
[14] Y. Zhang, Z. Li, Y. Zhao, S. Yu, and H. Guo, J. Phys. B: At., Mol., Opt. Phys. **50**, 035501 (2017).

[15] V. C. Usenko and F. Grosshans, Phys. Rev. A **92**, 062337 (2015).
[16] T. Gehring, C. S. Jacobsen, C. Seffmann, and U. L. Andersen, Quantum Inf. Comput. **16**, 1081 (2016).
[17] Q. Zhuang, Z. Zhang, J. Dove, F. N. C. Wong, and J. H. Shapiro, Phys. Rev. A **94**, 012322 (2016).
[18] Z. Zhang, Q. Zhuang, F. N. C. Wong, and J. H. Shapiro, Phys. Rev. A **95**, 012332 (2017).
[19] Z. Zhang, C. Chen, Q. Zhuang, F. N. C. Wong, and J. H. Shapiro, arXiv:1712.04973.
[20] Z. Li, Y. Zhang, and H. Guo, arXiv:1805.04249.
[21] A. M. Lance, T. Symul, V. Sharma, C. Weedbrook, T. C. Ralph, and P. K. Lam, Phys. Rev. Lett. **95**, 180503 (2005).
[22] J. Lodewyck, M. Bloch, R. Garcia-Patron, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin, and P. Grangier, Phys. Rev. A **76**, 042305 (2007).
[23] B. Qi, L.-L. Huang, L. Qian, and H.-K. Lo, Phys. Rev. A **76**, 052323 (2007).
[24] I. Khan, C. Wittmann, N. Jain, N. Killoran, N. Lutkenhaus, C. Marquardt, and G. Leuchs, Phys. Rev. A **88**, 010302 (2013).
[25] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, Nat. Photon. **7**, 378 (2013).
[26] H. M. Chrzanowski *et al.*, Nat. Photon. **8**, 333 (2014).
[27] Y. Zhang, Z. Li, Z. Chen, C. Weedbrook, Y. Zhao, X. Wang, C. Xu, X. Zhang, Z. Wang, M. Li, X. Zhang, Z. Zheng, B. Chu, X. Gao, N. Meng, W. Cai, Z. Wang, G. Wang, S. Yu, and H. Guo, arXiv:1709.04618.
[28] A. Leverrier, Phys. Rev. Lett. **114**, 070501 (2015).
[29] A. Leverrier, Phys. Rev. Lett. **118**, 200501 (2017).
[30] M. Christandl, R. König, and R. Renner, Phys. Rev. Lett. **102**, 020504 (2009).
[31] A. Leverrier, R. García-Patrón, R. Renner, and N. J. Cerf, Phys. Rev. Lett. **110**, 030502 (2013).
[32] F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, and R. F. Werner, Phys. Rev. Lett. **109**, 100502 (2012).
[33] F. Furrer, Phys. Rev. A **90**, 042325 (2014).
[34] T. Gehring, V. Handchen, J. Duhme, F. Furrer, T. Franz, C. Pacher, R. F. Werner, and R. Schnabel, Nat. Commun. **6**, 8795 (2015).
[35] M. M. Wolf, G. Giedke, and J. I. Cirac, Phys. Rev. Lett. **96**, 080502 (2006).
[36] R. García-Patrón and N. J. Cerf, Phys. Rev. Lett. **97**, 190503 (2006).
[37] M. Navascués, F. Grosshans, and A. Acín, Phys. Rev. Lett. **97**, 190502 (2006).
[38] S. Pirandola, S. L. Braunstein, and S. Lloyd, Phys. Rev. Lett. **101**, 200504 (2008).
[39] R. Schnabel, Phys. Rep. **684**, 1 (2017).
[40] S. L. Braunstein and S. Pirandola, Phys. Rev. Lett. **108**, 130502 (2012).
[41] H. K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).
[42] Z. Li, Y.-C. Zhang, F. Xu, X. Peng, and H. Guo, Phys. Rev. A **89**, 052301 (2014).
[43] Y.-C. Zhang, Z. Li, S. Yu, W. Gu, X. Peng, and H. Guo, Phys. Rev. A **90**, 052325 (2014).
[44] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, Nat. Photon. **9**, 397 (2015).
[45] Y. Zhang, Z. Li, C. Weedbrook, K. Marshall, S. Pirandola, S. Yu, and H. Guo, Entropy **17**, 4547 (2015).
[46] Y. Wu *et al.*, Phys. Rev. A **93**, 022325 (2016).
[47] C. Ottaviani, C. Lupo, R. Laurenza, and S. Pirandola, arXiv:1709.06988.
[48] P. Papanastasiou, C. Weedbrook, and S. Pirandola, Phys. Rev. A **97**, 032311 (2018).
[49] N. Hosseinidehaj and R. A. Malaney, Quantum Inf. Comput. **17**, 361 (2017).
[50] X. Zhang, Y. Zhang, Y. Zhao, X. Wang, S. Yu, and H. Guo, Phys. Rev. A **96**, 042334 (2017).
[51] P. Papanastasiou, C. Ottaviani, and S. Pirandola, Phys. Rev. A **96**, 042332 (2017).
[52] S. Yu, Z. Li, Y. Zhang, and H. Guo, in *Frontiers in Optics (FiO 2017)* (Optical Society of America, Washington, DC, 2017), p. JW4A.33.
[53] C. Lupo, C. Ottaviani, P. Papanastasiou, and S. Pirandola, Phys. Rev. A **97**, 052327 (2018).
[54] M. Tomamichel, C. Lim, N. Gisin, and R. Renner, Nat. Commun. **3**, 634 (2012).
[55] P. J. Coles, M. Berta, M. Tomamichel, and S. Wehner, Rev. Mod. Phys. **89**, 015002 (2017).
[56] F. Furrer, J. Aberg, and R. Renner, Commun. Math. Phys. **306**, 165 (2011).
[57] T. Eberle, V. Handchen, and R. Schnabel, Opt. Express **21**, 11546 (2013).
[58] X. Wang, Y. Zhang, S. Li, B. Xu, S. Yu, and H. Guo, Quantum Inf. Comput. **17**, 1123 (2017).
[59] R. Canetti, in *Proceedings of the 42nd IEEE Symposium on Foundations of Computer Science* (IEEE, New York, 2001), pp. 136–145.
[60] J. Müller-Quade and R. Renner, New J. Phys. **11**, 085006 (2009).
[61] F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, Quantum Inf. Comput. **3**, 535 (2003).
[62] J. Carter and M. Wegman, J. Comput. Syst. Sci. **18**, 143 (1979).
[63] R. Renner Ph.D. thesis, Swiss Federal Institute of Technology (ETH) Zurich, 2006; arXiv:quant-ph/0512258.
[64] J. Kiukas and R. F. Werner, J. Math. Phys. **51**, 072105 (2010).
[65] Note that, in general, the smooth min-entropy $H_{\min}^{\varepsilon}(X_A|E)$ depends on the selection of information reconciliation methods. However, in our analysis the estimation of max-entropy is reduced by the function $n \log_2 \gamma(d_0 + \mu)$, which is the same as the reverse reconciliation case, and only depends on the collected data between Alice and Bob. Therefore, we assume that $H_{\min}^{\varepsilon}(X_A|E)$ is unrelated to the reconciliation methods in our paper.
[66] C. Ottaviani, G. Spedalieri, S. L. Braunstein, and S. Pirandola, Phys. Rev. A **91**, 022320 (2015).
[67] A. Schönbeck, F. Thies, and R. Schnabel, Opt. Lett. **43**, 110 (2018).
[68] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Nat. Commun. **8**, 15043 (2017).
[69] Z. Li, Y. Zhang, X. Wang, B. Xu, X. Peng, and H. Guo, Phys. Rev. A **93**, 012310 (2016).
[70] Y. Zhao, Y. Zhang, Z. Li, S. Yu, and H. Guo, Quantum Inf. Process. **16**, 184 (2017).
[71] Y. Zhao, Y. Zhang, B. Xu, S. Yu, and H. Guo, Phys. Rev. A **97**, 042328 (2018).
[72] R. García-Patrón and N. J. Cerf, Phys. Rev. Lett. **102**, 130501 (2009).