Continuous-variable source-device-independent quantum key distribution against general attacks

Yichen Zhang¹, Ziyang Chen², Christian Weedbrook³, Song Yu* & Hong Guo²

The continuous-variable quantum key distribution with entanglement in the middle, a semi-device-independent protocol, places the source at the untrusted third party between Alice and Bob, and thus has the advantage of high levels of security with the purpose of eliminating the assumptions about the source device. However, previous works considered the collective-attack analysis, which inevitably assumes that the states of the source has an identical and independently distributed (i.i.d) structure, and limits the application of the protocol. To solve this problem, we modify the original protocol by exploiting an energy test to monitor the potential high energy attacks an adversary may use. Our analysis removes the assumptions of the light source and the modified protocol can therefore be called source-device-independent protocol. Moreover, we analyze the security of the continuous-variable source-device-independent quantum key distribution protocol with a homodyne-homodyne structure against general coherent attacks by adapting a state-independent entropic uncertainty relation. The simulation results indicate that, in the universal composable security framework, the protocol can still achieve high key rates against coherent attacks under the condition of achievable block lengths.

Quantum key distribution (QKD)¹–³, as one of the most practical quantum cryptography technology, allows two users (traditionally called Alice and Bob) to establish a set of secret keys exploiting both quantum mechanics and classical post-processing methods. This can provide information-theoretic security even against existing potential eavesdroppers.

Continuous-variable (CV) QKD protocol⁴,⁵, of which the characteristic is that the information is encoded on the quadratures of the light field and measured with coherent measurement methods, e.g., homodyne ⁶ and heterodyne detection ⁷, has developed rapidly. There are two main reasons resulting in CV-QKD attracting so much attention in recent years: it can be easily implemented with standard telecom components⁸,⁹ and compatible with wavelength division multiplexing¹⁰,¹¹, and it can achieve high key rate in metropolitan distance¹², which has advantages of short-range implementation.

There are plenty of CV-QKD protocols proposed to deal with different scenarios. In the case of fully trusted-device protocols, it is always assumed that both Alice and Bob are honest, and Eve can only control the quantum channels rather than the devices at the two parties. A large number of distinctive trusted-device protocols, including discrete modulation CV-QKD protocols¹³–¹⁵, two-way protocols¹⁶–²¹ and so forth, have been put forward to enrich the protocol design. However, because of the imperfection of the practical source and detection devices, a QKD system may be attacked by a potential eavesdropper, and it compromises the security of a protocol²². To eliminate all the loopholes of devices, fully device-independent protocols are proposed, which do not make any assumptions for all experimental devices and allows Eve to control them all. Nevertheless, those protocols face experimental challenges because they have to perform a detection-loophole-free Bell test²³.

As a compromise, semi-device-independent (semi-DI) protocols are proposed, such as measurement-device-independent (MDI)²⁴–²⁵ and one-sided device-independent (1sDI)²⁶–²⁸ QKD protocols, to give a trade off between the security of some devices and the performance of a protocol, which regard that part of the protocol is honest and the other part is untrusted. Remarkably, both CV-MDI²⁹–³¹ and CV-1sDI protocols³²,³³,³⁵ have been analyzed against general coherent attacks, which improves the security analysis of the protocols.

¹State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing, 100876, China. ²State Key Laboratory of Advanced Optical Communication Systems and Networks, Department of Electronics, and Center for Quantum Information Technology, Peking University, Beijing, 100871, China. ³Xanadu, 372 Richmond St W, Toronto, M5V 2L7, Canada. *email: yusong@bupt.edu.cn
CV-QKD with entanglement in the middle is the protocol of which the source is placed at the untrusted third party in the middle and controlled by the malicious eavesdropper. Alice and Bob then measure one of the modes they received separately, with either homodyne or heterodyne detection. The goal of the protocol is that we do not need to give assumptions on the source, which is sometimes ill-characterised and unsafe in communication. Nevertheless, the security analysis of the CV-QKD with entanglement in the middle protocol is only confined to the collective attack cases, which inevitably assumes that the states of the source has identical and independently distributed (i.i.d) structure, i.e., $\rho_{\text{EPR}} = \sigma_{\text{AB}}^\otimes n$, leading to the protocol unable to reach the original idea of source-device-independent (SDI).

Inspired by the security analysis technique used in the 1sDI protocol by F. Furrer et al., we adapt one type of state-independent entropic uncertainty relation with CVs to analyse the security of the CV-QKD with entanglement in the middle protocol under coherent attacks and only consider the case that both Alice and Bob perform homodyne detections. We modify the original protocol by exploiting an energy test at the reconciliation side (Bob's side for reverse reconciliation as an example) to monitor the potential high energy attacks an adversary may use. By properly quantifying the correlation between Alice's and Bob's data, which could be used for estimating Eve's knowledge of the raw key, we obtain the secret key rate of a finite number of exchanged signals supposing that the strategy Eve exploits is a coherent attack. Our analysis removes the assumptions of the light source and assumes that the sampling process performed in Alice's and Bob's sides are i.i.d, which is needed for exploiting the entropic uncertainty relation. Therefore, The modified protocol can be called CV-SDI QKD protocol. Finally, simulation shows that even when the coherent attack is considered, CV-QKD with entanglement in the middle can still reach a non-zero key rate over short distance, without giving any constrains of the source.

**Results**

The original CV-QKD protocol with entanglement in the middle against collective attacks. We begin by describing the CV-QKD protocol with entanglement in the middle, which was originally proposed in ref. 34. A two-mode squeezed vacuum state EPR, with an unknown variance $V$, is prepared by the untrusted third party, see Fig. 1. The EPR source can be created either by an untrusted communication party Charlie or by the potential adversary Eve. The two modes of an EPR source, e.g., EPR$_1$ and EPR$_2$, are sent to Alice and Bob separately through quantum channels. As the general assumption in QKD is that both of the two quantum channels could be totally controlled by potential eavesdropper Eve; leading to the introduction of loss and noise to the states after transmission. Assuming the quadratures of the two modes of the EPR source are $\hat{X}_{\text{EPR}_1}$ and $\hat{X}_{\text{EPR}_2}$ with the covariance matrix (CM)

$$\gamma_{\text{EPR}} = \begin{pmatrix} V & \sqrt{V^2 - 1} \mathbf{I} \\ \sqrt{V^2 - 1} \mathbf{I} & V \end{pmatrix},$$

where $\mathbf{I} = \text{diag}[1, 1]$ and $\mathbf{I} = \text{diag}[1, -1]$, and the transmissivities of two channels are $\tau_A$ and $\tau_B$, respectively, then we have the quadratures after transmissions, given by

$$\hat{X}_A = \sqrt{\tau_A} \hat{X}_{\text{EPR}_1} + \sqrt{1 - \tau_A} \hat{X}_{E_1},$$
$$\hat{X}_B = \sqrt{\tau_B} \hat{X}_{\text{EPR}_2} + \sqrt{1 - \tau_B} \hat{X}_{E_2},$$

where $E_1$ and $E_2$ are the ancillary systems which Eve inject into the links to attack the protocol. The two-correlated-mode eavesdropping strategy is considered here, which is the general two-mode attack strategy, where the CM $\gamma_{E_1, E_2}$ of the two correlated modes is

$$\gamma_{E_1, E_2} = \begin{pmatrix} \omega_A & \mathbf{G} \\ \mathbf{G} & \omega_B \end{pmatrix}.$$
where $\omega_A$ and $\omega_B$ are the variance of modes $E_1$ and $E_2$, and the correlation term $G = \text{diag}[g, g']$ with the correlation parameters $g$ and $g'$ satisfying the constraints shown in ref. 35. The attack is optimal by setting modes $E_1$ and $E_2$ as coherent given in refs. 24,26,37.

Originally, Alice and Bob perform quadrature measurements via homodyne or heterodyne detections, and in this paper, we only consider the scenario that both Alice and Bob employ homodyne detections to get one measurement result, i.e., quadrature $x$ or $p$. After finishing the state preparation and measurement phases, both Alice and Bob announce which quadrature they choose through an authenticated public channel to sift their keys. They hold the data for which the selected quadratures are the same and discard the rest. Finally, the two communication parties proceed with classical data post-processing, namely parameter estimation, error correction and privacy amplification to distill their keys.

In the case of collective attacks setting, the state $\rho_{AB}^{N} \otimes \rho_{E}^{N}$ after all runs can be considered as a tensor product state, namely $\rho_{AB}^{N} \otimes \rho_{E}^{N} = \rho_{\text{ABP}}^{N}$, where $N$ is the total number of quantum signals exchanged during the protocol. In this paper, we only focus on the asymptotic case under collective attacks to show the ideal performance of the protocol, where the total number of quantum states $N$ tends to infinite. The asymptotic secret key rate $K^{\text{sym}}_{\text{collective}}$ (for reverse reconciliation) is given by the Devetak-Winter formula 36, which reads

$$K^{\text{sym}}_{\text{collective}} = \max \{\beta I(A; B) - \chi(B; E), 0\},$$

(4)

where $\beta$ is the reconciliation efficiency, $I(A; B)$ is the classical mutual information between Alice’s and Bob’s data, and $\chi(B; E)$ is the Holevo information between Bob’s data and the eavesdropper 39. This is given by $\chi(B; E) = S(E) - S(E|B)$, where $S(E)$ is the von Neumann entropy of Eve and $S(E|B)$ is the conditional von Neumann entropy of Eve given Bob’s information.

$\chi(B; E)$ can be bounded with the help of the Gaussian state extremality theorem 61,40 in the case of collective attacks, hence we assume that the state $\rho_{AB}$ is Gaussian to minimize the final secret key rates, which can be calculated from the CM. A detailed derivation of the CM and the key rate can be seen in Methods section.

The modified CV-SDI QKD protocol against general coherent attacks. In the case of general coherent attacks, the assumption that $\rho_{AB}^{N} \otimes \rho_{E}^{N}$ has tensor product structure is invalid, so we cannot apply Eq. (4) directly to bound the security key rate after finite runs of the protocol. There are in general two main security-proof techniques developed in CV-QKD to handle coherent attack issues. One method is the de Finetti theorem 52,43, which have the ability to restrict the security from coherent attacks to collective attacks, and it was successfully employed to analyse the protocol which has some symmetric properties 50. The alternative is the entropic uncertainty relation 32,33,44, which requires that the protocol needs to randomly measure between two quadratures and perform the sifting process 27,31. We exploit the latter tool in this paper to obtain the security of the entanglement-in-the-middle protocol with homodyne-homodyne structure against coherent attacks. We point out that the protocol in ref. 33 has no assumption on Alice’s side (also be treated as the source side), thus it is also called one-sided device independent protocol. In our protocol, there is also no assumption on the source. However, since the structure of our protocol is a network structure, where the source is located in a third party, and Alice and Bob only perform measurements, this structure is very different from previous protocols, where the source is located in one side of the protocol. We named our protocol "source device independent" to distinguish it from previous one-sided device independent protocols.

We analyse the protocol under general coherent attacks with untrusted source in the middle by adapting the approach described in ref. 33. Thanks to the composable security framework, we have the ability to study the protocol considering some imperfect situation, such as the practical detection model, the energy test and finite-size effect, which allows us to modify the protocol in coherent-attack case.

Simulation. Using the results in the previous section, we can plot the secret key rate as a function of the total transmission distance focusing on the symmetric configuration where we set $\tau_A = \tau_B = \sqrt{T}$ and $T$ is the transmissivity of the channel. The simulations are under two-mode optimal attacks to show the performance of the protocol and both collective and coherent attack scenarios are discussed shown in Fig. 2. Note that modeling an eavesdropper’s attack behavior here does not limit the eavesdropping ability, but just for the convenience of simulations. Actually, in experiment, we only need to know the parameter estimation data $\{x_A^{pe}, p_A^{pe}\}$ and $\{x_B^{pe}, p_B^{pe}\}$ of Alice and Bob to execute the security analysis of the protocol. Therefore there is no need to assume which model Eve’s attack strategy belongs to before the protocol starts. Modeling attacks of eavesdroppers with two-mode coherent attacks yields the worst performance of the protocol 35,46,77, thus we use this modeling method to well reflect the performance of the protocol. The results are shown in Figs. 2 and 3, where Fig. 2 shows the secret key rates of the CV-SDI QKD as the function of transmission distance under different block sizes, while Fig. 3 is the key rate varying with the block size.

Discussion. In order to facilitate the analysis of the performance of the protocol, we simulate the key rate with some ideal parameters. For instance, we assume that the protocol has an ideal modulation variance $V = 10^5$ (which could replace an incomplete modulation variance) and perfect reconciliation efficiency $\beta = 1$. Also, to get the lower bound of the protocol, we set $g = \min \{\sqrt{\omega_A - 1}/\omega_A + 1, \sqrt{\omega_B - 1}/\omega_B + 1\}$ and $\omega_A = \omega_B = 1 + T\xi/(1 - T)$ with excess noise $\xi$ in one channel for two-mode optimal attacks. In the coherent attack cases, we set the interval parameter $a$ to $52^{26}$ and the overall security parameter is smaller than $10^{-20}$. Meanwhile, the parameter $M_{\text{th}}$ is set to 12 to ensure that the energy test fails with probability smaller than $10^{-20}$.

In Fig. 2, the gray dot line shows the Pirandola-Laurenza-Ottaviani-Banchi (PLOB) bound 45, which gives an upper bound of the secret key capacity of the lossy channel. The black solid line is the asymptotic key rate under
collective attacks, and the longest transmission distance is over 18 km, which is a little shorter than that of the two-mode individual attacks case (where the correlation parameter $g = 0$)\textsuperscript{34}. The other five curves, from top to bottom, describe the key rates under coherent attacks. The red solid curve is obtained for $N \to \infty$, and the other dashed lines describe the rate for $N = 10^{10}$ to $N = 10^7$ with finite exchanged signals. In Fig. 3, we also plot the secret key rate under coherent attacks as a function of block size for different distances. The distances are 5 km, 10 km and 14 km, respectively. We point out that when the block size reduces, the secret key rate decreases, and it is not achievable if the block size is below $10^7$.

**Figure 2.** Secret key rates of the CV-SDI QKD protocol. The protocol is under symmetric configuration with $\tau = \sqrt{T}$ where $T$ is the total transmissivity of the channel. We consider the protocol with perfect reconciliation efficiency $\beta = 1$ and ideal modulation variance $\gamma = 10^5$. We also set the excess noise as $\xi = 0.001$ in each channel and the overall security parameter is smaller than $10^{-20}$. The gray dot line is the PLOB bound\textsuperscript{45} and the black solid line is the key rate under collective attacks. The red solid line is the key rate under coherent attacks with infinite exchanged signals. The four dashed lines, from top to bottom, are the secret key rates under coherent attacks, with the block lengths from $10^{10}$ to $10^7$.

**Figure 3.** Secret key rates as functions of block size of the CV-SDI QKD protocol. The black solid line shows the performance with the distance of 5 km. The red dot-dashed line and the blue dashed line are the key rates of the protocol with distances of 10 km and 14 km, respectively. The other parameters are as in Fig. 2.
composable security framework, the protocol is still secure, achieving high key rates against coherent attacks
under the condition of achievable block lengths ($N$ from $10^7$ to $10^{10}$).

**Methods**

**Covariance matrix and the secret key rate under collective attacks.** The final bipartite quantum state $\rho_{AB}$ of Alice and Bob has the form

$$\gamma_{AB} = \begin{pmatrix} aI & cZ \\ cZ & bI \end{pmatrix},$$

where

$$a = \tau_A V + (1 - \tau_A)\omega_A,$$

$$b = \tau_B V + (1 - \tau_B)\omega_B,$$

$$c = \sqrt{\tau_A \tau_B} \sqrt{V^2 - 1} - g\sqrt{1 - \tau_A} \sqrt{1 - \tau_B},$$

and we let

$$g = \min \{ (\omega_A - 1)(\omega_B + 1), (\omega_A + 1)(\omega_B - 1) \}$$

by setting modes $E_1$ and $E_2$ are coherent. Then the secret key rate $K_{collective}^{asym}$ can be calculated by Eq. (4) if we restrict our discussion in reverse reconciliation cases. The mutual information between Alice's and Bob's data can be described as

$$I(A: B) = \frac{1}{2} \log \left( \frac{a}{a - c^2/b} \right).$$

To obtain the von Neumann entropy $S(E)$ and $S(E|B)$, we always assume that Eve can purify the whole system in order to maximize her information, thus we have $S(E) = S(AB)$ and $S(E|B) = S(A|B)$. $S(AB)$ is a function of the symplectic eigenvalues $\lambda_{1,2}$ of $\gamma_{AB}$, which reads

$$S(AB) = G(\lambda_1 - 1)/2 + G(\lambda_2 - 1)/2,$$

where

$$G(x) = (x + 1) \log_2(x + 1) - x \log_2 x,$$

and

$$\lambda_{1,2}^2 = \frac{1}{2} \left[ \Delta \pm \sqrt{\Delta^2 - 4D^2} \right],$$

where we use the notations that $\Delta = a^2 + b^2 - 2c^2$ and $D = ab - c^2$. After Bob performs homodyne detection, Alice's CM conditioned on Bob's measurement results will transform to

$$\gamma_{A^b}^\psi = \gamma_A - \Sigma_C^T (X \gamma_B X)^{-1} \Sigma_C,$$

where $\gamma_A = aI$, $\gamma_B = bI$, $\Sigma_C = cZ$ and $X = [1,0;0,0]$. $S(A|B) = G(\lambda_2 - 1)/2$ is a function of the symplectic eigenvalue $\lambda_1$ of the covariance matrix $\gamma_B^\psi$ with $\lambda_2 = a(a - c^2/b)$. Therefore, the secret key rate under collective attacks when the reverse reconciliation is performed is

$$K_{collective}^{asym} = \beta I(A: B) - [S(AB) - S(A|B)].$$

**The practical detection model and the measurement phase.** We model the practical detector as an ideal homodyne detector followed by an analog-to-digital converter (ADC) with finite sampling range, and therefore the measurement process can be divided into two steps.

In Step 1, Alice and Bob exploit ideal homodyne detectors to measure the input signal with infinite ranges and resolutions. The measurement quadratures are ideal continuous variables with infinite dimensions, hence the measurement results are also continuous. Assuming that the sifting process is done, we denote the outputs of ideal homodyne detectors as $Q_A$ and $Q_B$ in two sides. In general CV-QKD scenario, the statistical distribution of each outcome should follow a Gaussian distribution.

In order to obtain a tight bound using the entropic uncertainty relation, we need to rescale one of two results, $Q_A$ or $Q_B$, and ensure that Alice's and Bob's measurement outcomes have high correlations after transmission through untrusted channels. We use the transformations below (using Alice as an example) to scale the quadrature measurements:

$$Q_A \rightarrow \tilde{Q}_A = t_Q Q_A,$$

where $t_Q$ denotes the rescaling factor related to the channel losses of Alice and Bob, which can be determined by matching the variances of Alice's and Bob's measurement results. Supposing that $m$ signals are randomly chosen
to do the parameter estimation, the average value of quadrature measurement results both in Alice’s and Bob’s sides can be estimated by

$$\hat{E}(Q_A) = \frac{1}{m} \sum_{i=1}^{m} Q_{A,i}, \quad \hat{E}(Q_B) = \frac{1}{m} \sum_{i=1}^{m} Q_{B,i}. \tag{15}$$

where $Q_A = \{Q_{A,i}\}_{i=1}^{m}$ and $Q_B = \{Q_{B,i}\}_{i=1}^{m}$, and it is easy to estimate the parameter $t_q$ by

$$\hat{t}_q = \frac{\sum_{i=1}^{m} (Q_{B,i} - \hat{E}(Q_B))^2 - \sum_{i=1}^{m} (Q_{A,i} - \hat{E}(Q_A))^2}{\sum_{i=1}^{m} (Q_{A,i} - \hat{E}(Q_A))^2}. \tag{16}$$

In the symmetric case, where the channel losses and noises of Alice and Bob are approximately the same, we can simplify the analysis by assuming that $t_q \approx 1$.

In Step 2, the ADCs with finite range and finite precision followed by homodyne detectors are exploited to discretize continuous measuring intervals into discrete intervals, and the continuous variables $Q_A$ and $Q_B$ are also discretized. The measurement results are grouped into intervals:

$$(-\infty, -\alpha], (-\alpha, -\alpha + \delta], \ldots, (\alpha - \delta, \alpha], (\alpha, \infty), \tag{17}$$

where $\alpha$ is the maximum discretization range of the ADCs, which takes the finite range of detectors into consideration, and $\delta$ denotes the resolution of the measurement, which shows how much detail the detector can detect. 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. After this step, the continuous outcomes are replaced by the discrete results, which are denoted by

$$\hat{Q}_A^{\text{discrete}}, \hat{Q}_B^{\text{discrete}}. \tag{18}$$

This detection model can effectively illustrate the practical detector with finite range and resolution, without considering the efficiency of the detector, which could be modeled by a beam splitter with transmissivity $T_d^{\text{se}}$. However, the “discretization” process may cause security issues when compared with the ideal detection case since the detection results are missing information about the quadratures. One issue is that any measurement outcomes inside one of the equal-length intervals $(-\alpha, -\alpha + \delta], \ldots, (\alpha - \delta, \alpha]$ will map to the same value and it may cause a reduction in the information about the state within each sampling interval due to the finite sampling bits. The other problem is caused by two intervals with infinite length, namely $(-\infty, -\alpha]$ and $[\alpha, \infty)$, and users cannot know the full information about the state outside the detection range. In other word, users cannot distinguish whether the energy of the measured pulse is low or high, which may leave some loopholes for eavesdropping. This problem can be solved by the energy test solution.

**The energy test.** For fear of the large energy attack that Eve may exploit during the communication process, the protocol should be modified by adding the energy test step to ensure that the energy of measured states is below a certain threshold. We adapt the energy test method proposed in ref. $^{33}$ to study entanglement-in-the-middle protocol to remove the assumption of the source in the security analysis, which should be considered in trusted source scenario$^{32}$, hence this protocol also can be called **source-device-independent** protocol.

Assuming that the protocol is performed with reverse reconciliation, the energy test is exploited in Bob’s side before Bob performs the measurement step, which is described in Fig. 4. Bob uses a beam splitter with almost
perfect transmissivity $T$ to split incoming mode $X_B$ into two parts, and $a$ is the vacuum mode introduced by the other port of the beam splitter. Mode $X'_B$ is the transmitted mode of the output used for generating Bob’s raw data using a homodyne detector, and $a'$ is the reflected mode for the energy test. The reflected mode $a'$ is measured by a heterodyne detector, which consists of a balanced beam splitter and two homodyne detectors. Modes $t_i$ and $t_i'$ are the output modes of the balanced beam splitter used for checking whether the amplitude of one output $|q_{t_i}|$ and the phase of the other output $|p_{t_i'}|$ are below a certain threshold. If for every measured signal both the amplitude $|q_{t_i}|$ and the phase $|p_{t_i'}|$ are not larger than the threshold $M_{th}$, we say that the energy test passes; and the protocol aborts otherwise. The probability that Bob measures with homodyne detection larger than the detection range $\varepsilon$ can be bounded by the function $\Gamma(\alpha, T, M_{th})$, which reads

$$\Pi(\alpha, T, M_{th}) = \sqrt{\frac{1 + \lambda + 1 + \lambda^2}{2}} \exp\left(-\frac{(\mu\alpha - M_{th})^2}{T(1 + \lambda)/2}\right), \tag{19}$$

where $\mu = \sqrt{\frac{1 - T}{2T}}$ and $\lambda = \left(\frac{2T - 1}{T}\right)^2$. The smoothness of the energy test $\varepsilon$ further can be bounded by

$$\varepsilon = \frac{2n\Gamma(\alpha, T, M_{th})}{P_{pass}}. \tag{20}$$

**Finite-size effect and the key rate.** In the coherent-attack scenario, due to the leftover hash lemma, the $\varepsilon$-correct and $\varepsilon$-secret key of length $\ell_{sec}$ can be extracted, which can be expressed by

$$\ell_{sec} \leq H^{\varepsilon}(X^{key}_B|E)_B - H^{\varepsilon}(X^{key}_B|X_A)_B - \log_2\frac{1}{\varepsilon^2} + 2, \tag{21}$$

where $\ell_{sec}$ denotes the leaked information in error correction step, and it can be estimated before the error correction begins during the parameter estimation phase. $H^{\varepsilon}(X^{key}_B|E)_B$ is the smooth conditional min-entropy of data $X^{key}_B$ with smoothing parameter $\varepsilon$, conditioned on the information Eve may have, which quantifies Eve’s uncertainty about the Alice’s measurement outcomes. $\varepsilon$ satisfies $\varepsilon \leq (\varepsilon_S - \varepsilon)/2P_{pass} - 2\varepsilon$, where $P_{pass}$ is the probability that the parameter estimation step passes, $\varepsilon$ is the security parameter related to the energy test given in Eq. (20) and we choose $\varepsilon_S = \varepsilon/2$ for simplification. Equation (21) is a CV type key formula considering the quantum side information $E$ in infinite-dimensional Hilbert space.

The parameter $\ell_{EC}$ can be easily obtained by publishing some of Bob’s data (in the reverse reconciliation case), which is

$$\ell_{EC} = H(X_B) - H(X_B: X_A), \tag{22}$$

where $H(X_B)$ denotes the discrete Shannon entropy of the data in Bob side, which can be described by

$$H(X_B)_B = -\sum_{i=1}^{n} p(x_i)\log_2 p(x_i) = \log_2\delta, \tag{23}$$

and $I(X_B: X_A)$ is the mutual information between Alice and Bob.

Our target is to bound the smooth min-entropy $H^{\varepsilon}(X^{key}_B|E)_B$ in the presence of quantum adversaries. The entropic uncertainty relations were originally introduced in discrete variable QKD to bound the min-entropy and to show the protocols’ security. They were thereafter extended to infinite dimensions by F. Furrer et al. Therefore we exploit one type of uncertainty relation formula shown in ref. 33 to bound the min-entropy in the entanglement-in-the-middle protocol, and the feature of the entropic uncertainty relation together with the energy test, resulting in making the protocol being source-device-independent.

Entropic uncertainty relation gives a bound of guessing the uncertainty that the eavesdropper may have, when our target is to bound the smooth min-entropy $H^{\varepsilon}(X^{key}_B|E)_B$. The feature of the entropic uncertainty relation together with the energy test, resulting in making the protocol being source-device-independent.
are i.i.d. The goal of estimating the smooth min-entropy \( H_{\text{min}}^{\varepsilon}(X_B^k|E) \) is to give an upper bound of the smooth max-entropy \( H_{\text{max}}^{\varepsilon}(X_B^k|A^k) \).

To estimate the upper bound of \( H_{\text{max}}^{\varepsilon}(X_B^k|A^k) \), first due to the data processing inequality\(^{24}\), we can obtain that
\[
H_{\text{max}}^{\varepsilon}(X_B^k|A^k) \leq H_{\text{max}}^{\varepsilon}(X_B^k|X_A^k),
\]
and we need to bound the correlation between data \( X_B^k \) and \( X_A^k \). For that we exploit the average distance,
\[
d(X, Y) = \frac{1}{N} \sum_{i=1}^{N} |X_i - Y_i|,
\]
(27)
to give the bound of the smooth max-entropy. It has been shown in ref.\(^{32}\) that if \( \text{Pr}[d(X_B^k, X_A^k) \geq d] \leq \varepsilon^2 \) holds, we can always give a bound by
\[
H_{\text{max}}^{\varepsilon}(X_B^k|X_A^k) \leq n \log_2 \gamma(d).
\]
(28)
where \( \gamma \) is a function arising from a large deviation consideration, which reads
\[
\gamma(t) = (t + \sqrt{t^2 + 1})/[t/(\sqrt{t^2 + 1} - 1)]^t.
\]
(29)

However, we have only data \( X_B^{pe} \) and \( X_A^{pe} \) with \( m \) length to perform the parameter estimation rather than data \( X_A^k \) and \( X_B^k \), thus parameter \( d \) needs to be bounded by exploiting the data only consumed in parameter estimation step. Two functions need to be defined first, one is the average second moment of the difference between two sequences, which reads
\[
d_d(X, Y) = \frac{1}{N} \sum_{k=1}^{N} |X^k - Y^k|^2,
\]
(30)
and the other is the average second moment for the discretized data measurements, which is denoted by
\[
m_d(X) = \frac{1}{N} \sum_{k=1}^{N} \frac{|X^k - \alpha/\delta|^2}{\delta^2}.
\]
(31)

Then we check whether the average distance \( d^{pe} = d(X_A^{pe}, X_B^{pe}) \) is not larger than a certain threshold \( d_0 \). They continue the protocol if \( d^{pe} \leq d_0 \) and abort the protocol otherwise. In the case of the protocol proceeding, Alice and Bob calculate the average second moments of their data respectively, which denote \( V_{X_A}^{pe} = m_d(X_A^{pe}) \) and \( V_{X_B}^{pe} = m_d(X_B^{pe}) \) according to Eq. (31), and they also compute the average second moments between their data by \( V_d^{pe} = d(X_A^{pe}, X_B^{pe}) \) according to Eq. (30).

With the help of Serfling’s large deviation bound\(^{55}\), we can finally bound the max-entropy by
\[
H_{\text{max}}^{\varepsilon}(X_B^k|X_A^k) \leq n \log_2 \gamma(d_0 + \mu),
\]
(32)
where \( \mu \) describes the statistical fluctuation deviating from \( d(X_B^k, X_A^k) \), which denotes
\[
\mu = \sqrt{2\log_2 \xi} \frac{N\sigma}{m\sqrt{\pi}} + \frac{4(\alpha/\delta)\log_2 \xi^{-1}}{3} \frac{N}{nm},
\]
(33)
with
\[
\sigma^2 = \frac{m}{N} \left( V_{X_A}^{pe} - \frac{m}{N} (d^{pe})^2 \right) + \frac{m}{N} \left( V_{X_B}^{pe} + V_{X_B}^{pe} + 2 \frac{\nu}{\delta^2} \right) + 2 \frac{m}{N} \left( V_{X_A}^{pe} + V_{X_B}^{pe} \right) - \frac{2m}{N} \left( V_{X_A}^{pe} \right)^2 - \frac{2m}{N} \left( V_{X_B}^{pe} \right)^2,
\]
(34)
and
\[
\xi = (\varepsilon_1 - \varepsilon_1 - 2\sqrt{2m\Gamma(\alpha, T, M_0)})^2 - 2\exp \left\{ -\frac{2m}{N} \frac{n^2 m^2 (n+1)}{N}\right\},
\]
(35)
\( \nu \) is the smallest real number making \( \xi \) positive. If there exist \( \nu \) such that \( \xi \) is positive and \( \varepsilon_1 - 2\sqrt{2m\Gamma(\alpha, T, M_0)} < \varepsilon_1 \) is satisfied, the final secret key rate under coherent attacks can be written as
\[
K_{\text{coherent}} = \ell_{\text{low}}/N,\]
(36)
where \( \ell_{\text{low}} \) is the lower bound of the secure key length, which reads
\[
\ell_{\text{low}} = \left[ n \log_2 \frac{1}{\varepsilon_1^2} - \log \gamma(d_0 + \mu) \right] - \ell_{\text{EC}} - \log_2 \frac{1}{\varepsilon_1^2} + 2.
\]
(37)
Otherwise, we denote that the key rate \( K_{\text{coherent}} = 0 \). The detailed proof of this section can be seen in ref.\(^{33}\).
44. Chen, Z., Zhang, Y., Wang, X., Yu, S. & Guo, H. Improving parameter estimation of entropic uncertainty relation in continuous-variable quantum key distribution. *Entropy* **21**, 652 (2019).
45. Pirandola, S., Laurenza, R., Ottaviani, C. & Banchi, L. Fundamental limits of repeaterless quantum communications. *Nat. Commun.* **8**, 15043 (2017).
46. García-Patrón, R. & Cerf, N. J. Continuous-variable quantum key distribution protocols over noisy channels. *Phys. Rev. Lett.* **102**, 130501 (2009).
47. Renner, R. Security of quantum key distribution. Ph.D. thesis, Swiss Federal Institute of Technology (ETH) Zurich, arXiv:quant-ph/0512258 (2006).
48. Eberle, T. *et al.* Gaussian entanglement for quantum key distribution from a single-mode squeezing source. *New J. Phys.* **15**, 053049 (2013).
49. Berta, M., Christandl, M., Colbeck, R., Renes, J. M. & Renner, R. The uncertainty principle in the presence of quantum memory. *Nat. Phys.* **6**, 659 (2010).
50. Tomamichel, M. & Renner, R. *Phys. Rev. Lett.* **106**, 110506 (2011).
51. Furrer, F., Åberg, J. & Renner, R. Min- and max-entropy in infinite dimensions. *Commun. Math. Phys.* **306**, 165 (2011).
52. Furrer, F., Berta, M., Tomamichel, M., Scholz, V. B. & Christandl, M. Position-momentum uncertainty relations in the presence of quantum memory. *J. Math. Phys.* **55**, 122208 (2014).
53. Kiukas, J. & Werner, R. F. Maximal violation of Bell inequalities by position measurements. *J. Math. Phys.* **51**, 072105 (2010).
54. Tomamichel, M., Colbeck, R. & Renner, R. Duality between smooth min- and max-entropies. *IEEE Trans. Inf. Theory* **56**, 4674 (2010).
55. Serfling, R. J. Probability inequalities for the sum in sampling without replacement. *Ann. Stat.* **2**, 39 (1974).

**Acknowledgements**

This work was supported in part by the Key Program of National Natural Science Foundation of China under Grants 61531003, the National Science Fund for Distinguished Young Scholars of China under Grant No. 61225003, the National Natural Science Foundation under Grants 61427813, China Postdoctoral Science Foundation under Grant 2018M630116, and the Fund of State Key Laboratory of Information Photonics and Optical Communications.

**Author contributions**

H.G. and S.Y. proposed and guided the work. Y.Z., Z.C. and C.W. designed the protocol and performed the analysis. All authors analysed the results and wrote the manuscript.

**Competing interests**

The authors declare no competing interests.

**Additional information**

**Correspondence** and requests for materials should be addressed to S.Y.

**Reprints and permissions information** is available at [www.nature.com/reprints](http://www.nature.com/reprints).

**Publisher’s note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

**Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made. The images or other third party material in this article are included in the article’s Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the article’s Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this license, visit [http://creativecommons.org/licenses/by/4.0/](http://creativecommons.org/licenses/by/4.0/).

© The Author(s) 2020