npj | Quantum Information

www.nature.com/npjqi

ARTICLE OPEN

Check for updates

Simple security proofs for continuous variable quantum key distribution with intensity fluctuating sources

Chenyang Li[1,2]✉, Li Qian[1] and Hoi-Kwong Lo[1,2,3]

Despite tremendous theoretical and experimental progress in continuous variable (CV) quantum key distribution (QKD), the security has not been rigorously established for most current continuous variable quantum key distribution systems that have imperfections. Among these imperfections, intensity fluctuation is one of the principal problems affecting security. In this paper, we provide simple security proofs for continuous variable quantum key distribution systems with intensity fluctuating sources. Specifically, depending on device assumptions in the source, the imperfect systems are divided into two general cases for security proofs. In the most conservative case, we prove the security based on the tagging idea, which is a main technique for the security proof of discrete variable quantum key distribution. Our proofs are simple to implement without any hardware adjustment for current continuous variable quantum key distribution systems. Also, we show that our proofs are able to provide secure secret keys in the finite-size scenario.

npj Quantum Information (2021)7:150 ; https://doi.org/10.1038/s41534-021-00482-3

INTRODUCTION

Quantum key distribution (QKD) allows two distant parties to share a common string of secret data[1–3]. Based on the laws of quantum mechanics, QKD offers information-theoretical security. QKD has aroused much interest in both theoretical protocol and experimental demonstration, because it is considered a practical application of quantum information science to reach commercial maturity. For example, the implementation of discrete variable (DV) QKD protocols including satellite-to-ground QKD[4] and chip-based QKD[5–7] have demonstrated the potential for commercial applications in the filed of quantum information. Besides, twin-field QKD[8,9] has been proposed to outperform the well-known rate-loss limit[10] and largely extend transmission limits. Compared to DV protocols, continuous variable (CV) protocols have the potential for high-key rate and low-cost implementations using current standard telecom components such as homodyne detectors[3]. Recently, CV QKD experiment has demonstrated the secret key transmission over a long distance from 100 km[11] to more than 200 km[12].

Despite the enormous progress in the field of QKD, the most important question in quantum communication is always how secure QKD really is. For example, are QKD systems secure when implemented with practical devices? Fortunately, measurement-device-independent QKD[13] can remove all imperfections and security loopholes in the measurement devices, and therefore we only need to consider the imperfections in the source devices. Imperfect sources, such as the correlated intensity fluctuations in optical pulses[14] and setting-choice-independently correlated light sources[15], have been recently analyzed in DV QKD systems. However, the security research concerning CV QKD with imperfect source has fallen behind that of its discrete variable cousin. For instance, almost all existing CV QKD proofs require a perfect state preparation[16], i.e., Gaussian modulation, which cannot be guaranteed in a practical CV QKD system with imperfections and limitations[17,18]. The security of continuous variable quantum key distribution with noisy coherent states has been analyzed in refs. [19–21] by introducing an independent and additive Gaussian noise to a perfect Gaussian modulation. However, in the practical continuous variable modulation, the imperfections might not work independently or additively with Gaussian modulation. For example, intensity fluctuation is one of the potential practical problems affecting Gaussian modulation due to its dependence on modulated quadratures. Therefore, in this work we study intensity fluctuations in practical CV QKD systems. Our intensity fluctuation model is an arbitrary distributed random variable with a unit mean value. Depending on whether the intensity fluctuation information is accessible or not to Alice, our security analysis of a QKD system can be generally divided into two cases: (1) Alice can, and (2) Alice cannot monitor intensity fluctuation values for every pulse.

In this work, we prove the security for the two cases based on different techniques. Particularly, in case (1), because Alice's information can help modify her data, the security proof is based on the integrating over the distribution of intensity fluctuations. Also, a refined data analysis is developed to improve the QKD performance over long distance. In case (2), Alice cannot exactly monitor every signal pulse. Depending on whether Eve has the intensity fluctuation information, we divide case (2) into two subcases: (2A) Eve can, and (2B) Eve cannot monitor intensity fluctuation values for every pulse. In subcase (2A), we prove the security based on Gaussian extremality[22,23]. In the most conservative case (2B), we apply the concept of tagging, previously developed for DV QKD in ref. [24], to the security proof of CV QKD. Specifically, we divide up signals into two distinct sets, untagged and tagged. Untagged signals are those whose intensities fall inside a prescribed region, whereas tagged signals are those whose intensities might fall outside the prescribed region. In the actual protocol, the QKD system users do not need to know whether each signal is tagged or untagged. They only need to be able to set a bound for untagged signals, which would lead to the security of their generated key. Moreover, given the distribution of intensity fluctuations, the users could obtain the probability of

[1]Center for Quantum Information and Quantum Control, Department of Electrical & Computer Engineering, University of Toronto, Toronto, ON M5S 3G4, Canada. [2]Department of Physics, The University of Hong Kong, Hong Kong, China. [3]Department of Physics, University of Toronto, Toronto, ON M5S 3G4, Canada. ✉email: chenyangli@ece.utoronto.ca

untagged signals and further optimize the secret key rate by the fraction of untagged signals. In the end, we demonstrate that our proofs are able to provide secure secret keys in the finite-size scenario over distances larger than 50 km. In conclusion, our proofs for all cases are simple to implement without any hardware adjustment for the current continuous variable quantum key distribution system. Alice and Bob are free to choose different security proofs to generate the secret key based on their device assumptions.

RESULTS AND DISCUSSION

Intensity fluctuation model

Here, we define our model for experimental intensity fluctuations. For example, suppose that a desired pulse intensity is I_A; however, Alice actually prepares a pulse with the intensity of kI_A. We denote k as a random variable to characterize the intensity fluctuations, with mean value E_k and variance V_k. This intensity fluctuation can be caused by power fluctuations of a laser or imperfect intensity modulators[25]. In this paper, for simplicity, we assume the following conditions of the random variable k:

(1) k is an independent and identically distributed (i.i.d.) random variable.
(2) k has a mean value E_k and a variance V_k, where E_k is 1.
(3) k is independent of the pulse intensity I_A.
(4) the probability distribution function of k can be obtained before the experiment by testing the source device.
(5) the probability distribution function of k will not change during the QKD transmission.

Here, these conditions are assumed to simplify our model for experimental intensity fluctuations. Conditions (1)–(3) are the intrinsic constraints and assumptions for the intensity fluctuations. Conditions (4)–(5) are the assumptions for system characterization, which is required before QKD transmission.

CV QKD system description

Figure 1 shows that, with the intensity fluctuation information, QKD systems can be generally divided into two cases for security proofs. To fairly compare the results, an ideal CV QKD system is added as the baseline case (0) for benchmarking. Here, following[24] we introduce a hypothetical party Fred, who controls the intensity fluctuations k for every optical pulse, e.g., the intensity fluctuation can be controlled by temperature drift. Through secure communication, Fred would choose to reveal the value of k to Alice. In total, there are two cases:

(1) Fred discloses the actual value of k to Alice;
(2) Fred does not disclose the actual value of k to Alice.

In both cases, because the actual pulse intensity is kI_A, the actual encoded Gaussian random variable now becomes $\sqrt{k}X_A$ and Alice sends out a mode $\hat{A}_1 = \hat{0} + \sqrt{k}X_A$. In case (1), Alice has access to the intensity fluctuation values k and can further revise her data from X_A to $\sqrt{k}X_A$ for every pulse. In case (2), Alice does not have access to the intensity fluctuation values k. Depending on whether Eve has the intensity fluctuation side information, we divide case (2) into two subcases (2A) and (2B) for security proofs.

For a QKD system, it is conventionally assumed that Eve often has access to channel with only limitations from the laws of physics. But the source should always be assumed to be secure and no information in the source stage can be disclosed to Eve. Here, we divide the QKD system into different cases based on the source information leakage assumptions. It is open for Alice and Bob to consider which case is acceptable in their QKD transmission process. For case (1), the justification is that Alice can have access to the device imperfection in real time. For case (2A), the justification is that Alice should use a certified device,

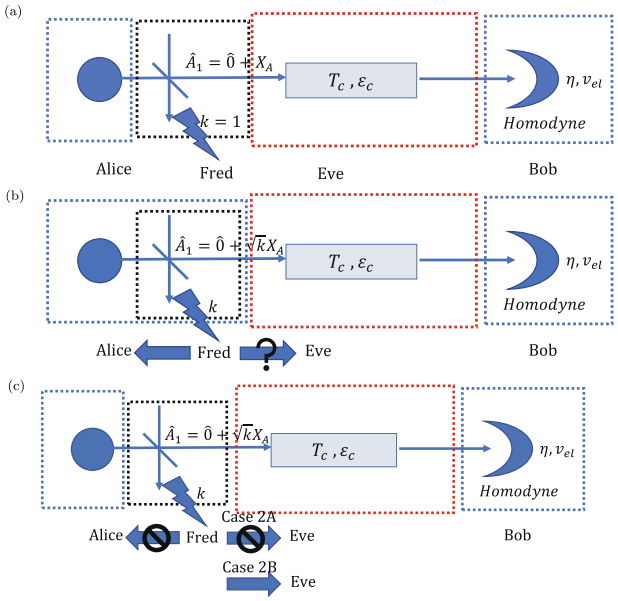

Fig. 1 Practical CV QKD system with different security assumptions. (**a**) Case (0): ideal CV QKD system (k = 1) (**b**) Case (1): k is disclosed to Alice (**c**) Case (2): k is not disclosed to Alice. Here, practical CV QKD systems can be divided into two cases based on the Alice's information about intensity fluctuations. One ideal case (0) is added for comparison. In case (0), a CV QKD system does not have any intensity fluctuations. In case (1), Alice can monitor the intensity fluctuations. In case (2), Alice cannot monitor the intensity fluctuations. Depending on whether Eve has intensity fluctuation information or not, case (2) is divided into two subcases (2A) and (2B). Here, T_c and ε_c are, respectively, the channel transmittance and excess noise between Alice and Bob. η and v_{el} are the the detection efficiency and electronic noise of the homodyne detector. Here, the symbol "?" in case (1) means that Eve may or may not have access to the intensity fluctuation information. The No Entry sign in case (2) means that the intensity fluctuation information will not be disclosed to Alice or Eve.

which come from an honest manufacturer. For case (2B), this is most conservative case. If Alice does not have enough confidence on the device, they can always choose case (2B). Note that, the authors in ref. [26] have applied a related idea to the detection stage where they assume that the detection process is inaccessible to eavesdroppers.

Security proof for case (0)

Here, we briefly review the security proof for an ideal CV QKD system. Because the security against coherent attacks can be reduced to that against collective attacks by using de Finetti representation theorem for infinite dimensions[27], for simplicity, we only consider asymptotic security against collective attack . Given reverse reconciliation communication, the asymptotic secret key rate is given by the Devetak-Winter formula[28–31]:

$$R_0 = \beta I_{AB} - \chi_{BE} \tag{1}$$

where β is the reverse reconciliation efficiency, I_{AB} is the mutual information between Alice and Bob, and χ_{BE} is the mutual Holevo information between Bob and Eve. Given parameter estimations of transmittance T and excess noise ε and modulation variance V_A, the computation for I_{AB} and χ_{BE} can be found in the Supplementary Section I.

Security proof for case (1)

In case (1), Alice has access to the intensity fluctuation values k and can further revise her data from X_A to $\sqrt{k}X_A$ for each pulse.

The security proof is based on two conclusions: (a) the strong superadditivity of secret key rate; (b) the weak law of large numbers.

Suppose Alice and Bob share n modes in a joint state $\rho_{A_{1,2,\ldots,n}B_{1,2,\ldots,n}}$, and Alice has the intensity fluctuation information k_i for the ith mode. Conditional on the k_i, The secret key rate for this joint state can be shown as

$$\begin{aligned} R_1 &= \tfrac{1}{n} R(\rho_{A_{1,2,\ldots,n}B_{1,2,\ldots,n}|k_1 k_2 \ldots k_n}) \geq \tfrac{1}{n}\sum_{i=1}^{n} R(\rho_{A_iB_i|k_i}) \\ \rightarrow E_{k_i}[R(\rho_{A_iB_i|k_i})] &= \int_{-\infty}^{+\infty} \mathrm{PDF}(k)[R(\rho_{AB}|k)] \\ dk &= \int_{-\infty}^{+\infty} \mathrm{PDF}(k) R_0(k,T) dk \end{aligned} \tag{2}$$

where $PDF(k)$ is the probability density function of k, $R(\rho_{A_iB_i|k_i})$ is the secret key rate conditional on the k_i, $R_0(k,T)$ is the secret key rate R_0 with modulation variance of kV_A and transmittance T. By parameter estimation process, T and kV_A can be directly estimated from ρ_{AB}.

In the first line of Eq. ((2)), we use the strong superadditivity of the secret key rate from ref. [23]. Then in second line, we argue that by the weak law of large numbers, the sum over all reduced modes converges to the average over its probability density function in the limit $n \to \infty$.

Given the intensity fluctuation information, we propose that a simple refined data analysis can be adopted by Alice to improve the maximum distance and defend against possible attacks based on intensity fluctuations. Here, we describe a refined data analysis process as below: (1) Based on the probability density function of k, Alice will divide k into a number of sets with equal probability. (2) Alice and Bob will perform the parameter estimation individually for each set, obtaining the channel transmittance and excess noise and verifying whether the channel transmittance matches with that from another set. This process is used to defend any possible attack for Eve based on intensity fluctuation information. (3) For certain sets, if $R_0(k,T) < 0$, Alice and Bob will simply drop all the data from such sets.

After a refined data analysis, the secret key rate can be expressed as

$$R_{1R} = \int_{-\infty}^{+\infty} \mathrm{PDF}(k) \max\{R_0(k,T), 0\} dk \tag{3}$$

Figure 2 shows the simulation result for the secret key rate R_0, R_1, and R_{1R}. We use the parameters listed in Table 1, where η and v_{el} are, respectively, the detection efficiency and electronic noise of the homodyne detector, ε_c is the excess noise in the channel, V_A is the modulation variance and β is the reverse reconciliation efficiency. In Fig. 2a, we choose the probability density function of k to be an uniform distribution from 0.9 to 1.1. In Fig. 2b, we choose the probability density function of k to be an uniform distribution from 0.8 to 1.2. Through simulation, we find that the secret key rate R_1 is approximately same as R_0. By refined data analysis, the maximum transmission distance can be improved from 94 to 130 km in Fig. 2a, and from 94 to 199 km in Fig. 2b. This maximum transmission distance improvement is expected, since the refined data analysis can be regarding as a preselection of optimal Gaussian states for long distance.

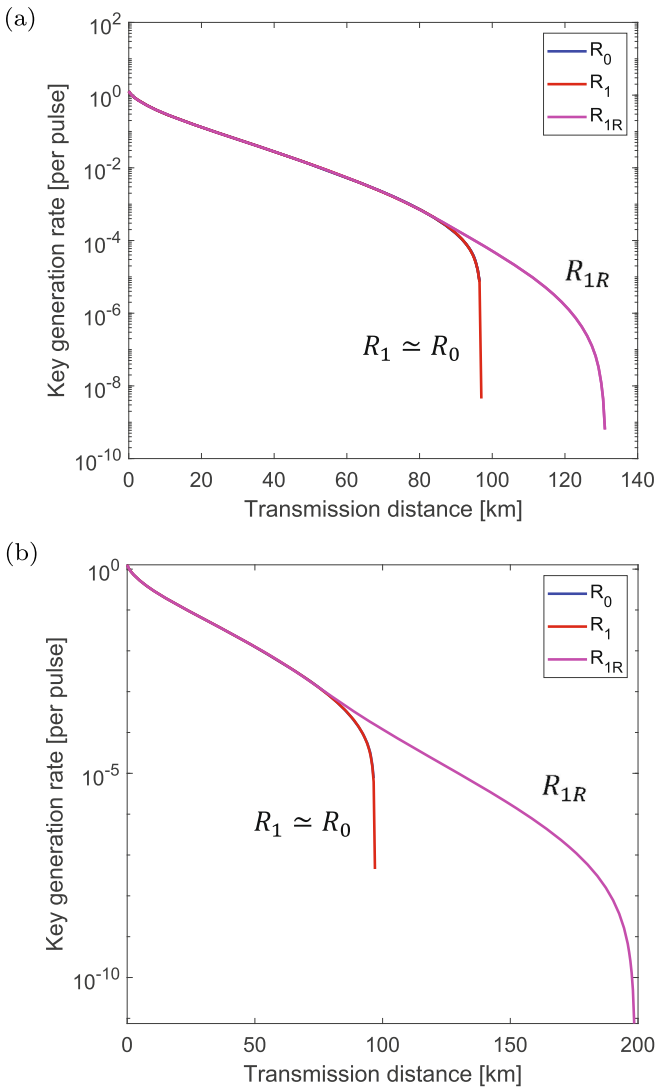

Fig. 2 The secret key rate of case (1) with uniform distribution. (**a**) Uniform distribution from 0.9 to 1.1 for R_1 (**b**) Uniform distribution from 0.8 to 1.2 for R_1. Here, we compare the secret key rate, R_0, R_1, and R_{1R}. In panel (**a**), the intensity fluctuation model is a uniform distribution from 0.9 to 1.1. The secret key rate R_1 is approximately same as the key rate R_0 for ideal CV QKD system. In panel (**b**), the intensity fluctuation model is a uniform distribution from 0.8 to 1.2. It is clearly demonstrated that both maximum transmission distances can be improved by refined data analysis.

Table 1. Evaluation parameters for fiber-based QKD.

η	ε_c	v_{el}	V_A	β
0.60	0.02	0.02	18	95.6

Security proof for case (2A)

Here, we consider case (2A): Alice and Eve both have no intensity fluctuation information. As shown in Fig. 3, for each pulse, Alice has no intensity fluctuation information and can only record the data X_A. However, what Alice really encodes is the mode $\hat{A}_1 = \hat{0} + \sqrt{k}X_A$. By considering reverse reconciliation with the Bob's recorded data X_B, The secret key rate can be expressed as

$$R_{2A} = \beta I(X_A, X_B) - \chi(X_B, E)_{|\sqrt{k}X_A} \tag{4}$$

where $I(X_A, X_B)$ is the mutual information between Alice's and Bob's classical recorded data X_A and X_B, and $\chi(X_B, E)_{|\sqrt{k}X_A}$ is the Holevo mutual information between Bob and Eve given the actual input mode $\hat{A}_1$ before the channel. Here, $I(X_A, X_B)$ can be directly obtained from the datasets, while an upper bound for $\chi(X_B, E)_{|\sqrt{k}X_A}$ is needed. Next, we use the Gaussian extremality[22,23] that the Holevo information $\chi(X_B, E)_{|\sqrt{k}X_A}$ between Eve's and Bob's classical variables, is maximized when then the state ρ_{AB} shared by Alice and Bob is Gaussian. In other words, we can obtain the upper bound of $\chi(X_B, E)_{|\sqrt{k}X_A}$ by substituting Alice's and Bob's actual mode $\hat{A}_1, \hat{B}$ with Gaussian modes, which have

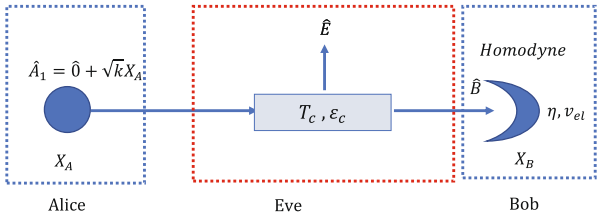

Fig. 3 CV QKD system for case (2A). Here, we consider case (2A) that Eve also has no intensity fluctuation information. Therefore, Eve can only manipulate the signal states in the channel. Due to intensity fluctuation, Alice will have a recorded data mismatched with what she really encodes.

the same first and second quadrature moments. By calculating the mean value and variance of $\sqrt{k}X_A$, we can obtain that $<\sqrt{k}X_A> = <X_A> = 0, <kX_A^2> = <X_A^2> = V_A$. Furthermore, we obtain the upper bound that

$$\chi(X_B, E)_{|\sqrt{k}X_A} \leq \chi(X_B^G, E)_{|X_A^G} \tag{5}$$

where X_A^G and X_B^G are, respectively, the Gaussian random variable with the same first and second moments as X_A and X_B.

Next, we will estimate the equivalent transmittance T_s and excess noise ε_s in the source caused by the data mismatch. According to the Supplementary Section II, suppose Alice records X_A and the actual encoded data are $\sqrt{k}X_A$, the equivalent T_s and ε_s can be expressed as

$$\begin{aligned} T_s &= <\sqrt{k}>^2 \simeq (1 - \tfrac{1}{8}V_k)^2, \\ \varepsilon_s &= \tfrac{V_A}{T_s} - V_A \simeq \tfrac{1}{4}V_A V_k, \end{aligned} \tag{6}$$

In addition to the channel transmittance T_c and excess noise ε_c, Alice and Bob would estimate an overall transmittance T and excess noise ε such that

$$\begin{aligned} T &= T_s T_c, \\ \varepsilon &= \varepsilon_c / T_s + \varepsilon_s \end{aligned} \tag{7}$$

Figure 4 shows the secret key rate for case (2A). We still use the channel and detector parameters listed in Table 1. In Fig. 4a, we compute the secret key rates for the uniform distributed intensity. Even if the pulse intensity fluctuate 5%, the maximum transmission distance will still drop about 10 km. In Fig. 4b, the secret key rates are obtained for the Gaussian distributed intensity. The variances of the Gaussian distribution range from 0 to 10^{-2}. When the variance increases to 10^{-2}, the maximum transmission distance will decrease by about 40 km. In other words, when the standard deviation of Gaussian distribution is 10%, the maximum transmission distance will drop significantly.

Security proof for case (2B)

In this section, we consider case (2B): Eve has intensity fluctuation information while Alice has no information. Before we jump into security proof, we first define the untagged Gaussian state. Here, we apply the concept of "tagging"[24] to case (2B) of CV QKD. Suppose Alice sends out n Gaussian modulated coherent pulses to Bob and the ith pulse has a intensity fluctuation value k_i. However, Alice has no information about the intensity fluctuation value for each pulse, and Alice can only record dataset as $k_i = 1$. Now we define the Gaussian modulated coherent states with intensity fluctuation value $k_i < 1$ as untagged Gaussian states. It is easy to verify that when Alice sends out a stronger pulse than what she is supposed to send, Alice and Bob will definitely overestimate the secret key rate by underestimating the channel loss and excess noise. Therefore, the untagged Gaussian states are defined to be the states from which Alice and Bob will not overestimate the secret key rate. In other words, the untagged Gaussian states are always conservative secure. Next, we can introduce an cutoff k_{max} based on the intensity fluctuation probability density function. As depicted in Fig. 5, if Alice chooses a cutoff k_{max}, the Gaussian states associated with lower intensities than $k_{max}I_A$ would always

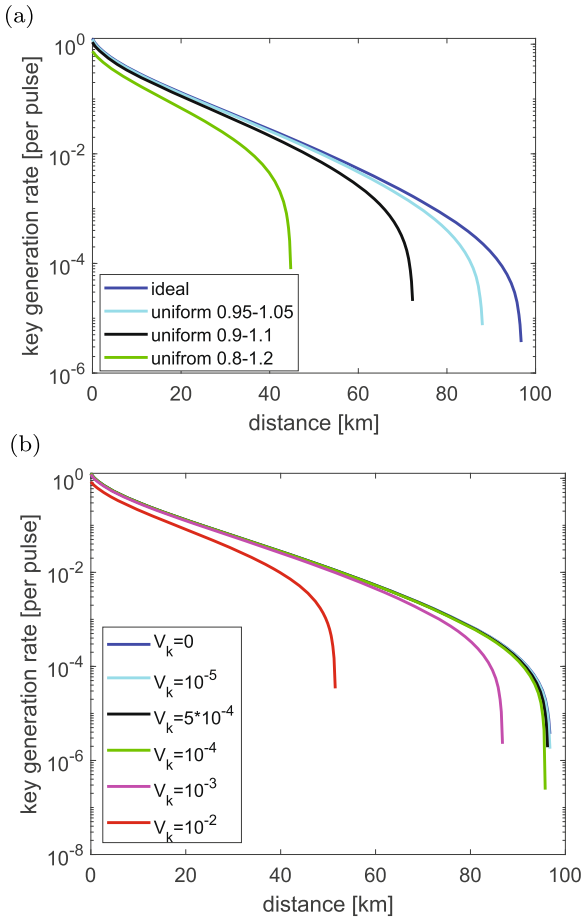

Fig. 4 The secret key rate of case (2A). (**a**) Uniform distribution (**b**) Gaussian distribution. Here, we compute the secret key rates R_{2A} with two intensity fluctuation models. **a** The secret key rates versus transmission distance for different intensity fluctuation models of uniform distribution. **b** The secret key rates versus transmission distance for different intensity fluctuation models of Gaussian distribution.

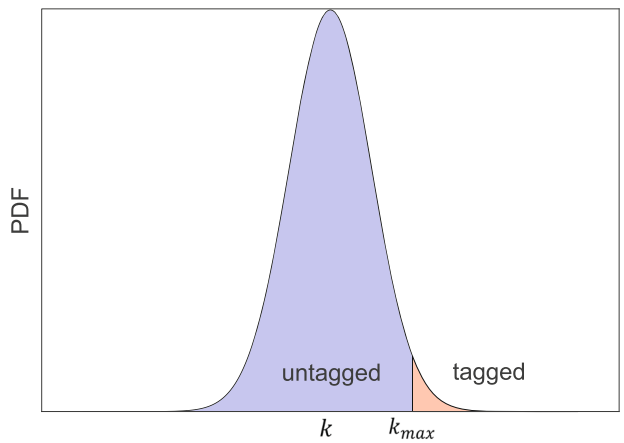

Fig. 5 A cutoff for untagged state. Here, we apply a cutoff k_{max} to increase the probability of untagged Gaussian states.

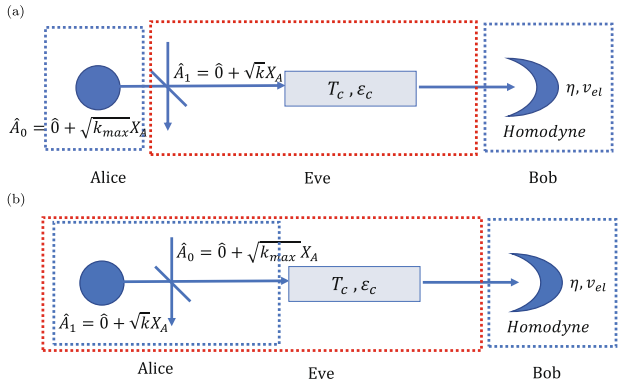

Fig. 6 CV QKD system for case (2B). (**a**) Untagged Gaussian state ($k \le k_{\max}$) (**b**) Tagged Gaussian state k > $k_{\max}$. Here, we show the CV QKD system with untagged and tagged Gaussian states. Suppose that Alice always records the data as $\sqrt{k_{\max}}X_A$ and has a virtual mode $\hat{A}_0$ corresponding to the modulation $\hat{A}_0 = \hat{0} + \sqrt{k_{\max}}X_A$. Alice's actual output mode is $\hat{A}_1 = \hat{0} + \sqrt{k}X_A$. In panel (**a**), untagged states are always secure because we conservatively assume the attenuation from a virtual mode $\hat{A}_0$ to a actual output $\hat{A}_1$ can be controlled by Eve. In panel (**b**), tagged states are insecure if we consider the same attenuation mentioned before is controlled by Eve.

be untagged. Then the probability to get untagged Gaussian states can be expressed as

$$p_s = \int_{-\infty}^{k_{\max}} \mathrm{PDF}(k)dk \tag{8}$$

Note that a modified QKD protocol is needed to implement an optimal cutoff for CV QKD. The modified protocol only requires a different data recording process on the state preparation stage while maintaining the same output states. In other words, suppose Alice desires to encode X_A and the actual encoded data are $\sqrt{k}X_A$, Alice should always record the data as

$$X_{A'} = \sqrt{k_{\max}}X_A \tag{9}$$

rather than X_A for each pulse.

Figure 6 shows the CV QKD system with untagged and tagged Gaussian states. In Fig. 6a, an untagged Gaussian state is always secure for Alice. Here, we conservatively assume the attenuation from a stronger pulse A_0 to a weaker pulse A_1 can be controlled by Eve. In Fig. 6b, for each tagged signal, the intensity is always larger than the threshold value recorded by Alice. Following GLLP security proof[24], we conservatively assume that tagged signals are insecure. Therefore, we only consider the secret key rate extracted from untagged Gaussian states.

Suppose that a fraction p_s of the pulses emitted by the source are untagged by Eve. The secret key for direct reconciliation can be extracted from untagged Gaussian states at an asymptotic rate as[24]

$$R_{2B}^D = p_s H(X_{A'}) - H(X_{A'}|X_B) - \chi_{A'E,p_s} \tag{10}$$

$$= I_{A'B} - (1-p_s)H(X_{A'}) - \chi_{A'E,p_s} \tag{11}$$

The secret key for reverse reconciliation can be shown as

$$\begin{aligned} R_{2B}^R &= p_s H(X_B) - H(X_B|X_{A'}) - \chi_{BE,p_s} \\ &= p_s H(X_B) - [H(X_B) - H(X_{A'}) + H(X_{A'}|X_B)] - \chi_{BE,p_s} \\ &= I_{A'B} - (1-p_s)H(X_B) - \chi_{BE,p_s} \end{aligned} \tag{12}$$

where $X_{A'}$ and X_B are Alice's and Bob's recording data, $p_s H(X_{A'})$ and $p_s H(X_{B'})$ is the differential entropy used to generate the secret key rate depending on direct reconciliation or reverse reconciliation, $H(X_{A'}|X_B)$ and $H(X_B|X_{A'})$ is the conditional differential entropy for error correction, $\chi_{A'E,p_s}$ is the Holevo information between Alice and Eve for the untagged states, and χ_{BE,p_s} is the Holevo information between Bob and Eve for the untagged states. The Holevo information between Alice/Bob and Eve should be eliminated by the privacy amplification process. $H(X_{A'})$ and $H(X_{A'}|X_B)$ and $H(X_B)$ can be directly estimated by Alice and Bob's data. Given the reconciliation efficiency β, the secret key rate can be shown as

$$\begin{aligned} R_{2B}^D &= \beta I_{A'B} - (1-p_s)H(X_{A'}) - \chi_{A'E,p_s} \\ R_{2B}^R &= \beta I_{A'B} - (1-p_s)H(X_B) - \chi_{BE,p_s} \end{aligned} \tag{13}$$

Next, we need to find a bound for the Holevo information. Mathematically, it can be shown that Holevo information is monotonically increasing on the domain of k. Physically, when the input pulse has a stronger intensity, Eve can obtain more information about Alice's and Bob's recorded results. Therefore, for the untagged states, the Holevo information can be bounded

$$\begin{aligned} \chi_{BE,p_s} &\le p_s \chi_{BE}, \\ \chi_{A'E,p_s} &\le p_s \chi_{A'E}, \end{aligned} \tag{14}$$

where $\chi_{A'E}$ and χ_{BE} are the Holevo mutual information between Alice/Bob and Eve estimated from Alice's and Bob's recording results $X_{A'}$ and X_B.

Next, we will estimate the equivalent transmittance T_s and excess noise ε_s. According to the Supplementary Section III, the equivalent T_s and ε_s can be expressed as

$$\begin{aligned} T_s &= <\sqrt{k}>^2/k_{\max} \simeq (1 - \tfrac{1}{8}V_k)^2/k_{\max}, \\ \varepsilon_s &= \tfrac{V_A}{T_s} - k_{\max}V_A \simeq \tfrac{1}{4}V_A V_k k_{\max}, \end{aligned} \tag{15}$$

In addition to the channel transmittance T_c and excess noise ε_c, Alice and Bob would estimate an overall transmittance T and excess noise ε such that

$$\begin{aligned} T &= T_s T_c, \\ \varepsilon &= \varepsilon_c/T_s + \varepsilon_s \end{aligned} \tag{16}$$

For the secret key rate evaluation, we compare the secret key rates for two intensity fluctuation models: Gaussian distribution and uniform distribution. We still use the parameters in the Table 1. For the optimization, if we increase the k_{max}, p_s will be increased, while T_s will be decreased. Therefore, we need to optimize k_{max} to get the maximum secret key rates.

Figure 7 shows the key rate optimization results for the uniform distribution. Here, we consider the reverse reconciliation scheme. Compared to case (2A), the maximum transmission distance decreases faster due to intensity fluctuations. The maximum transmission distance will drop by about 20 km even if the pulse intensity fluctuates 5%. Meanwhile, the optimal k_{max} will always be the maximum value of its domain for a uniform distribution.

Figure 8 shows the key rate optimization results for the Gaussian distribution. Here, we also consider the reverse reconciliation scheme. The maximum transmission distance decreases rapidly when the intensity fluctuations increase. Other than the uniform distribution, the optimal k_{max} will be monotonically increasing as a function of distance. When comparing these two intensity fluctuation models with same variance, we find that QKD with Gaussian distributed variation will have a lower key rate and transmission distance, since it always has a tail part for tagged Gaussian states.

Secret key rate with finite-size effects

In this section, we compute the secret key rate under finite-size scenario. Without loss of generality, we consider case (2B) as an example. As discussed in refs. [32,33], by setting confidence intervals for both T and ε, we can can obtain the lower bound of the transmittance, T^L, and the upper bound of the excess noise, ε^U. By incorporating our tagging idea, we should also obtain the lower

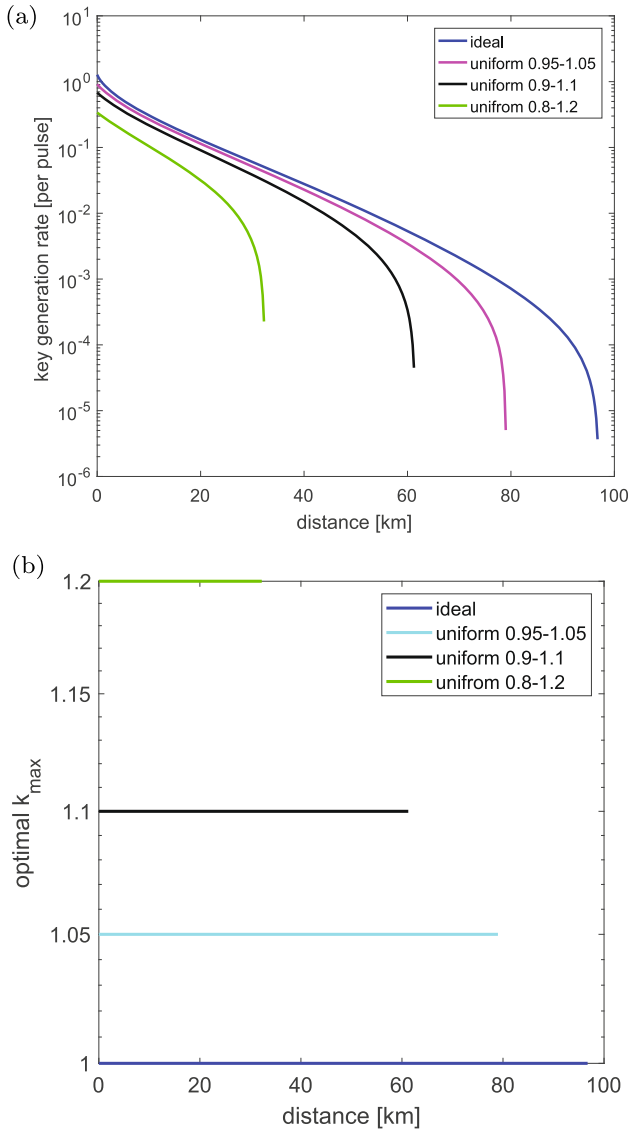

Fig. 7 Optimization for case (2B) with uniform distribution. (**a**) Secret key rate vs transmission distance. (**b**) Optimal $k_{\max}$ versus transmission distance. Here, we optimize the secret key rate R^R_{2B} for uniform distribution. **a** Optimal secret key rate versus transmission distance for different uniform distributions. **b** Optimal k_{max} versus transmission distance for different uniform distributions.

bound of the number of the untagged Gaussian states, m^L. With the three bounds, the secret key rate with finite-size effects, R_f, can be shown as[32,33]:

$$R_f = \frac{n}{N}\{R^R_{2B}(m^L, T^L, \varepsilon^U) - \triangle(m^L)\} \tag{17}$$

where n is the number of Gaussian states used for secret key transmission, m^L is the lower bound of the number of the untagged Gaussian states, N is the total number of received Gaussian states, and $\Delta(m^L)$ is related to the security of the privacy amplification in the finite case. The details of estimating m^L, T^L, ε^U, and $\Delta(m^L)$ can be found in the supplementary section IV. Note that the probability of the untagged Gaussian states satisfy $p^L_s = m^L/n$. Here we consider the case (2B) with reverse reconciliation, and the form of Eq. ((17)) can also be applied to other key rate formulas such as R^D_{2B}.

Figure 9 shows the secret key rate,R^R_{2B}, with the finite-size effects. Our method also works well for block sizes from 10^8 to

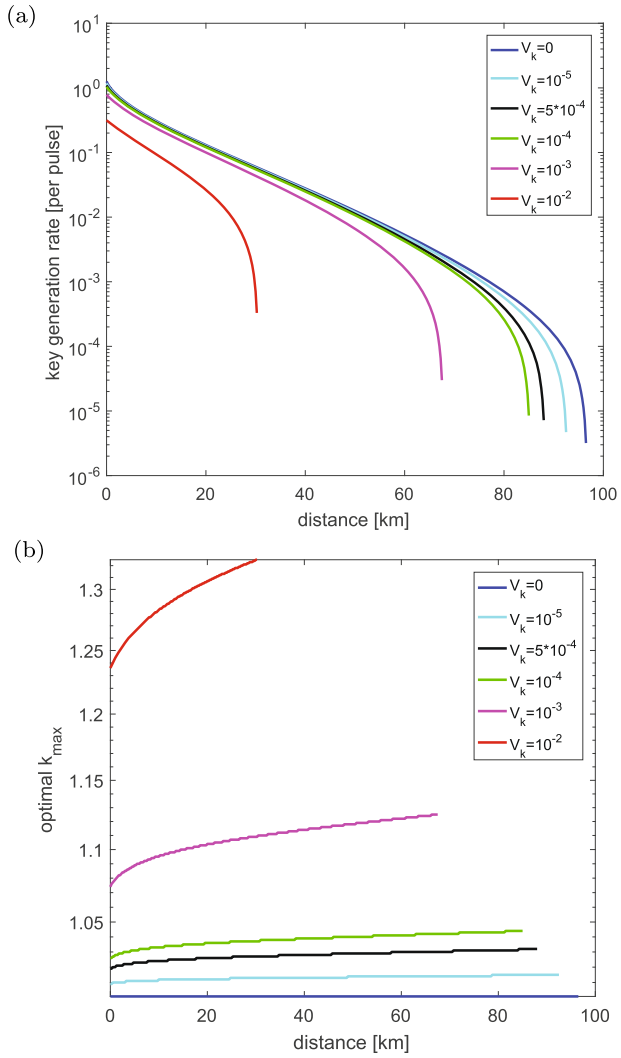

Fig. 8 Optimization for case (2B) with Gaussian distribution. Here, we optimize the secret key rate R^R_{2B} for uniform distribution. **a** Optimal secret key rate versus transmission distance for different uniform distribution. **b** Optimal k_{max} versus transmission distance for different uniform distribution.

10^{12}. For the distance less than 30 km, there is no distinct advantage in terms of the secret key rate for larger block sizes, which suggests that it may not be necessary to go to a very large block size, especially for a small distance. On the other hand, it is also expected that the key rates are approaching the asymptotic limit when the block size increases.

Discussion

We have studied the security of CV QKD with intensity fluctuating sources. Generally, We divide current CV QKD systems into two cases for security proof. Depending on Alice's realistic assumptions for the devices, Alice and Bob can choose different security proofs and obtain different secret key rates. In case (1), Alice can monitor the intensity fluctuation value for each pulse. She can revise her data and obtain almost the same secret key rate as what she can obtain from the ideal CV QKD systems. Furthermore, by a refined data analysis, the maximum transmission distance can be observably improved. In case (2), depending on the devices assumptions, we also divide CV QKD systems into two subcases (2A) and (2B). In case (2A), both Alice and Eve cannot obtain any intensity fluctuation information of each pulse. Here, we prove the

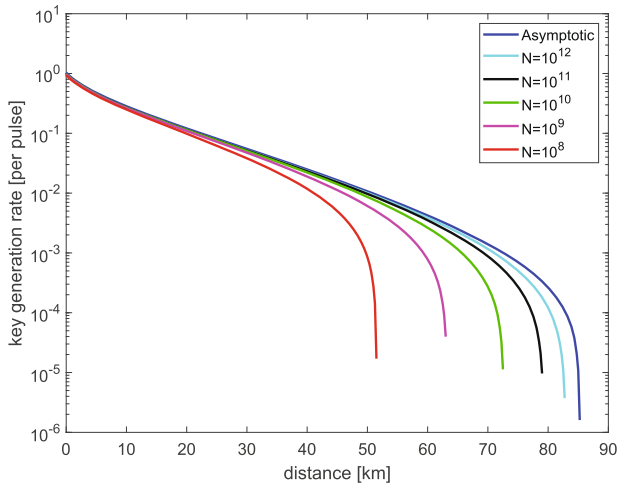

Fig. 9 The secret key rate with finite-size effects. Here, we compute the secret key rate vs distance with finite-size effects. Numerically optimized secret key rates are obtained for a fixed block size $N = 10^s$ with $s = 8$, 9, 10, 11, and 12. The rightmost curve corresponds to the asymptotic secret key rate. Here, we consider the Gaussian distribution model with variance 10^{-4}. The failure probability of parameter estimation is $\epsilon_{PE} = 10^{-10}$. The failure probability of untagged Gaussian states is $\epsilon_{ugs} = 10^{-10}$. The failure probability of privacy amplification is $\epsilon_{PA} = 10^{-10}$.

security based on Gaussian extremality. The secret key rate will decrease if the intensity fluctuation increases. In case (2B), Eve could have the intensity fluctuation information of each pulse while Alice cannot. Here, we apply the tagging idea from[24]. We divide the signals into tagged and untagged signals, and the secret key will only be generated from untagged signals. After considering the total error correction cost and privacy amplification, the security of case (2B) can be proved. In addition, we also compute the secret key rates under the finite-size regime. Overall, our security proofs are simple to implement without any hardware adjustment for current CV QKD systems. In the future, we are looking for applying our methods to solve other imperfections such as phase modulation errors or atmospheric channel effects.

DATA AVAILABILITY

Datasets generated and analyzed for simulation are available from the corresponding author upon reasonable request.

Received: 4 December 2019; Accepted: 1 September 2021;
Published online: 14 October 2021

REFERENCES

1. Lo, H.-K., Curty, M. & Tamaki, K. Secure quantum key distribution. *Nat. Photonics* **8**, 595–604 (2014).
2. Weedbrook, C. et al. Gaussian quantum information. *Rev. Mod. Phys.* **84**, 621 (2012).
3. Diamanti, E. & Leverrier, A. Distributing secret keys with quantum continuous variables: principle, security and implementations. *Entropy* **17**, 6072 (2015).
4. Liao., S.-K. et al. Satellite-to-ground quantum key distribution. *Nature* **549**, 43–47 (2017).
5. Ma, C. et al. Silicon photonic transmitter for polarization-encoded quantum key distribution. *Optica* **3**, 1274 (2016).
6. Sibson, P. et al. Integrated silicon photonics for high-speed quantum key distribution. *Optica* **4**, 172 (2017).
7. Li, C., Curty, M., Xu, F., Bedroya, O. & Lo, H.-K. Secure quantum communication in the presence of phase- and polarization-dependent loss. *Phys. Rev. A* **98**, 042324 (2018).
8. Lucamarini, M., Yuan, Z. L., Dynes, J. F. & Shields, A. J. Overcoming the rate-distance limit of quantum key distribution without quantum repeaters. *Nature* **557**, 400–403 (2018).
9. Zhong, X., Hu, J., Curty, M., Qian, L. & Lo, H.-K. Proof-of-principle experimental demonstration of twin-field type quantum key distribution. *Phys. Rev. Lett.* **123**, 100506 (2019).
10. Pirandola, S., Laurenza, R., Ottaviani, C. & L, B. Fundamental limits of repeaterless quantum communications. *Nat. Commun.* **8**, 15043 (2017).
11. Huang, D., Huang, P., Lin, D. & Zeng, G. Long-distance continuous-variable quantum key distribution by controlling excess noise. *Sci. Rep.* **6**, 19201 (2016).
12. Zhang, Y. et al. Long-distance continuous-variable quantum key distribution over 202.81 km fiber. *Phys. Rev. Lett.* **125**, 010502 (2020).
13. Lo, H.-K., Curty, M. & Qing, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **108**, 130503 (2012).
14. Yoshino, K. et al. Quantum key distribution with an efficient countermeasure against correlated intensity fluctuations in optical pulses. *npj Quantum Inf.* **4**, 8 (2018).
15. Mizutani, A. et al. Quantum key distribution with setting-choice-independently correlated light sources. *npj Quantum Inf.* **5**, 8 (2019).
16. Jouguet, P., Kunz-Jacques, S., Leverrier, A., Grangierand, P. & Diamanti, E. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nat. Photonics* **7**, 378C381 (2013).
17. Jouguet, P., Kunz-Jacques, S., Diamanti, E. & Leverrier, A. Analysis of imperfections in practical continuous-variable quantum key distribution. *Phys. Rev. A* **86**, 032309 (2012).
18. Liu, W., Wang, X., Wang, N., Du, S. & Li, Y. Imperfect state preparation in continuous-variable quantum key distribution. *Phys. Rev. A* **96**, 042312 (2017).
19. Filip, R. Continuous-variable quantum key distribution with noisy coherent states. *Phys. Rev. A* **77**, 022310 (2008).
20. Usenko, V. C. & Filip, R. Feasibility of continuous-variable quantum key distribution with noisy coherent states. *Phys. Rev. A* **81**, 022318 (2010).
21. Shen, Y., Peng, X., Yang, J. & Guo, H. Continuous-variable quantum key distribution with Gaussian source noise. *Phys. Rev. A* **83**, 052304 (2011).
22. Wolf, M. M., Giedke, G. & Cirac, J. I. Extremality of Gaussian quantum states. *Phys. Rev. Lett.* **96**, 080502 (2006).
23. Garca-Patron, R. & Cerf, N. J. Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution. *Phys. Rev. Lett.* **97**, 190503 (2006).
24. Gottesman, D., Lo, H.-K., Ltkenhaus, N. & Preskill, J. Security of quantum key distribution with imperfect devices. *Quant. Inf. Comput.* **5**, 325–360 (2004).
25. Laudenbach, F. et. al. Continuous variable quantum key distribution with Gaussian modulation the theory of practical implementations. *Adv. Quantum Technol.* https://doi.org/10.1002/qute.201800011 (2018).
26. Namiki, R., Kitagawa, A. & Hirano, T. Secret key rate of a continuous-variable quantum-key-distribution scheme when the detection process is inaccessible to eavesdroppers. *Phys. Rev. A* **98**, 042319 (2018).
27. Renner, R. & Cirac, J. I. de Finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography. *Phys. Rev. Lett.* **102**, 110504 (2009).
28. Devetak, I. & Winter, A. Distillation of secret key and entanglement from quantum state. *Proc. R. Soc. Lond. A* **461**, 207 (2005).
29. Lodewyck, J. et al. Quantum key distribution over 25 km with an all-fiber continuous-variable system. *Phys. Rev. A* **76**, 042305 (2007).
30. Jouguet, P., Kunz-Jacques, S. & Leverrier, A. Long distance continuous-variable quantum key distribution with a Gaussian modulation. *Phys. Rev. A* **84**, 062317 (2011).
31. Jouguet, P., Elkouss, D. & Kunz-Jacques, S. High-bit-rate continuous-variable quantum key distribution. *Phys. Rev. A* **90**, 042329 (2014).
32. Leverrier, A., Grosshans, F. & Grangier, P. Finite-size analysis of a continuous-variable quantum key distribution. *Phys. Rev. A* **81**, 062343 (2010).
33. Ruppert, L., Usenko, V. C. & Filip, R. Long-distance continuous-variable quantum key distribution with efficient channel estimation. *Phys. Rev. A* **90**, 062310 (2014).

ACKNOWLEDGEMENTS

We acknowledge the financial support from the Natural Sciences and Engineering Research Council of Canada (NSERC) and Huawei Technologies Canada Co., Ltd. We also acknowledge the funding from the University of Hong Kong start-up grant.

AUTHOR CONTRIBUTIONS

C.L., L.Q., and H.-K.L. developed the tagging idea in the CV QKD. C.L. performed the simulations and calculations of the secret key rate. All the authors contributed to the writing of the paper.

COMPETING INTERESTS

The authors declare no competing interests.

ADDITIONAL INFORMATION

Supplementary information The online version contains supplementary material available at https://doi.org/10.1038/s41534-021-00482-3.

Correspondence and requests for materials should be addressed to Chenyang Li.

Reprints and permission information is available at http://www.nature.com/reprints

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