SCIENTIFIC REPORTS

OPEN

Received: 25 July 2018
Accepted: 19 November 2018
Published online: 10 January 2019

Phase self-aligned continuous-variable measurement-device-independent quantum key distribution

Hua-Lei Yin, Wei Zhu & Yao Fu

Continuous-variable measurement-independent-device quantum key distribution (CV-MDI-QKD) can offer high secure key rate at metropolitan distance and remove all side channel loopholes of detection as well. However, there is no in-field experimental demonstration of CV-MDI-QKD due to the remote distance phase-locking techniques challenge. Here, we present a new optical scheme to overcome this difficulty and also removes the requirement of two identical independent lasers. Furthermore, we give an alternate but detailed proof of the minimized key rate condition to extract the secure key rate. We anticipate that our new scheme can be used to demonstrate the in-field CV-MDI-QKD experiment and build the CV-MDI-QKD network with untrusted source.

Quantum key distribution (QKD) allows remote parties (usually referred as Alice and Bob) to establish a string of secure key even at the presence of an eavesdropper (referred as Eve)[1–3]. Based on the laws of quantum mechanics, QKD achieves formidable task and opens a whole new area which is under rapid development and attracting lots of attentions[4]. Together with the well-known one time pad cryptosystem[5], QKD may provide information-theoretic security. In reality, the side-channel of the QKD system are the major security risks[6–10]. Fortunately, a novel protocol named measurement-device-independent QKD (MDI-QKD)[11–14] has been presented to remove all side channel attacks of detectors. In the MDI-QKD protocol, both Alice and Bob prepare perfect quantum states and then send them to the untrusted relay (referred as Charlie) through insecure quantum channels for Bell state measurement (BSM), the correlation between Alice and Bob can be built through the BSM results announced by Charlie. Together with the decoy-state theory[15,16], the qubit-based discrete-variable (DV) MDI-QKD has been successfully experimentally demonstrated[17–24]. Meanwhile, MDI-QKD also opens a new road to help building quantum communication network[25–28], even though, in the basic MDI-QKD protocols[11,12], the untrusted relay is a passive repeater which is not able to beat the point-to-point repeater-less bound[29] (see also a review[30]).

The experimental demonstration of DV-MDI-QKD has been successfully performed over 404 km optical fiber[23], while the secure key rate is relatively low even at metropolitan distance due to the single photon encoding. Continuous variable (CV) encoding scheme can also be used for QKD to share secret key[31–41]. The Gaussian-modulated coherent states CV-QKD has been successfully experimentally demonstrated through approximate 100 km optical fiber[42,43] under collective attack. Recently, the security of coherent states continuous-variable quantum key distribution against coherent attack in a realistic finite-size regime has been proved[44], which paves the way to information-theoretically secure CV-QKD. Due to its obvious advantages of high secure key rate, low cost and running in room-temperature, CV-QKD becomes a very active research area in quantum information[3]. Similar with the DV system, several practical attacks about detectors are also found in CV-QKD recently[45–48]. In order to be immune to all detector loopholes and achieve high secure key rate at metropolitan distance, the CV-MDI-QKD is proposed recently[49–52] with a proof-of-principle experimental demonstration performed on the free space optical platform by sharing a highly stable laser[49]. The CV-MDI-QKD has shown great potential for its high secret key rate and low commercial cost compared with the corresponding DV-MDI-QKD protocol[49,53,54]. However, a complete experimental demonstration of CV-MDI-QKD with distances of kilometers in optical fiber or free space is still not yet realized due to technical challenges. Thereinto,

Department of Physics, Zhejiang Institute of Modern Physics and ZJU-Phoenix Synergetic Innovation Center in Quantum Technology, Zhejiang University, Hangzhou, 310027, China. Correspondence and requests for materials should be addressed to H.-L.Y. (email: hlyin@zju.edu.cn) or Y.F. (email: yaofu@mail.ustc.edu.cn)

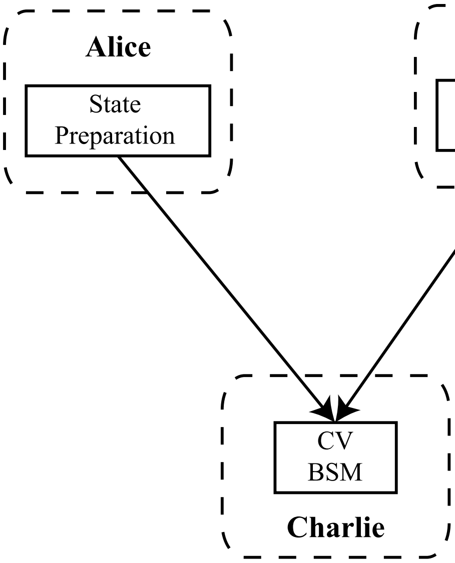

Figure 1. The general structure of the CV-MDI-QKD protocol.

the main challenge is that remote distance phase-locking technique is necessary to achieve correct CV BSM. However, this requirement is not needed in DV-MDI-QKD due to the fact that the two-photon Hong-Ou-Mandel interference is phase unrelated[55].

In this paper, we present a new optical scheme to solve the common phase-reference problem. The central idea of this new optical scheme is that reliable phase reference can be established by transmitting the two laser pulses quantum states through the same optical path, such as optical fiber or free space. Compared with the previous protocol[49], a pair of Faraday mirrors (FM) and several polarization beam splitters (PBS) are needed[56,57]. No complicated active or passive phase-locking or compensation technology is required in this new scheme, which greatly simplifies the experimental realization of CV-MDI-QKD. Similar structures has already been successfully used in a proof-of-principle experimental demonstration of quantum fingerprinting beating the classical limit[58]. Furthermore, we give an alternate but detailed proof of the minimized key rate condition to extract the secure key rate, which has been used and first proved in ref. [49].

Results

Phase self-aligned CV-MDI-QKD.

The basic idea of CV-MDI-QKD protocol is shown in Fig. 1. It includes the following major steps[49–51]: (1) Alice and Bob prepare the sequence of Gaussian-modulated coherent states $|x_A+ip_A\rangle$ and $|x_B+ip_B\rangle$, respectively. (2) The quantum states are transmitted through insecure quantum links to the untrusted relay for CV BSM. (3) The incoming quantum states from two parties are coupled to interfere through a balanced beam splitter. Two output quantum states are measured with homodyne in $\hat{x}$ and $\hat{p}$ quadrature, with $\hat{x}_- = (\hat{x}_A - \hat{x}_B)/\sqrt{2}$ and $\hat{p}_+ = (\hat{p}_A + \hat{p}_B)/\sqrt{2}$. The measurements together give $\gamma = (\hat{x}_- + i\hat{p}_+)/\sqrt{2}$ with the probability $p(\gamma)$, and the results γ are transmitted to both Alice and Bob through the public channel. (4) Based on the measurement results, Alice or Bob confirms the other's state value, then correlation is built. (5) Similar with the usual CV-QKD protocol, through error correction and privacy amplification, a secure key is acquired.

Figure 2 shows the detailed structure of our new scheme with optical fiber. The laser pulse goes through a polarization maintaining fiber PBS (PMF-PBS) to filter out its horizonal (H) polarized component. Then after a polarization maintaining optical circulator, the laser pulse directly goes through a balanced PMF beam splitter (PMF-BS) and be splitted into two identical laser pulses that each will be finally transmitted to Alice and Bob for CV encoding. Meanwhile, this PMF-BS will be reused in the CV BSM later. For simplicity, we name the two identical laser pulses as the left and right pulse. Here, we take the optical transmission process of the left pulse as an example. The left pulse goes out of the PMF-BS and into a PMF-PBS, due to its H polarization, it transmits through the PMF-PBS. Through a long distance single mode optical fiber, the left pulse goes into Alice's port. All the modulators are not working at this moment. The left pulse is then reflected by the FM, changing its polarization to vertical (V) polarization. Once the left pulse is transmitted back to the PMF-PBS, due to the change of its polarization it is reflected this time and going to the right branch of this set. Then it meets another PMF-PBS and again reflected. The left pulse is transmitted to Bob's port through another long distance single mode optical fiber, then it is reflected by FM. Once reflected, the polarization is restored back to H, and Bob prepares his CV Gaussian-modulated quantum states. The modulated left pulse goes back to the PMF-PBS, due to its H polarization, it transmits through the PMF-PBS and back to the balanced PMF-BS of untrusted relay for CV BSM. As for the right pulse, the process is quite similar, except that the modulation process takes place at Alice's port. The CV quantum states prepared by Alice and Bob will stably interfere due to the two identical laser pulses go through the same optical path. In another word, the phase-reference is self-aligned. By the way, a $\pi/2$ phase modulation to the encoded pulse back from Bob's port is added for CV Bell detection purpose[49]. For simplified, the additional $\pi/2$ phase can be directly implemented in Bob's quantum states preparation stage. It's worth noting that the idea

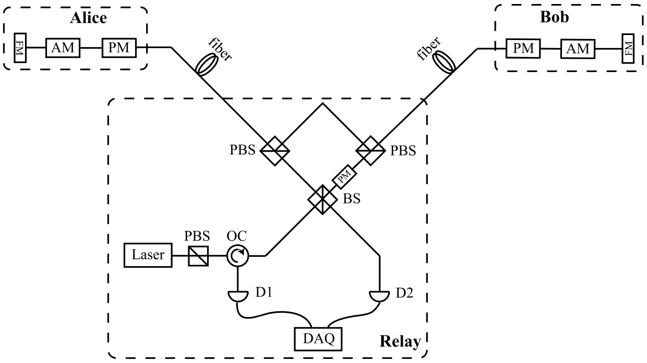

Figure 2. Schematic structure of the self-aligned CV-MDI-QKD protocol. PBS, polarization beam splitter; OC, optical circulator; BS, 50:50 beam splitter; AM, amplitude modulator; PM, phase modulator; FM, Farady mirror; D1, D2, detector; DAQ, data acquisition.

of our new optical scheme about self-aligned phase-reference can also be used in free space and satellite-based CV-MDI-QKD[59–62], especially for geostationary satellite[63].

The secure key rate and simulation result.

The security of general CV-MDI-QKD protocol has been analyzed under two kinds of quantum attack. One is using two independent entanglement cloners[50,51], each attacking the channel between the relay and Alice or Bob independently. This kind of attack just extends the one-channel entanglement cloner attack in CV-QKD protocol to two channels independently. The other kind of attack is more general[49], two ancillary modes from a reservoir of ancillas each attacks one of the two channels. These two ancillary modes may be correlated, which means the first kind of attack is nothing but a special condition of the second kind of attack. It has been proven that the most effective attack is when the two ancillary modes are entangled[49], and this is also the most powerful attack of Eve can launch in the CV-MDI-QKD protocol.

Here, we follow the security analysis in ref. [49]. For general two channel attack, the two Gaussian ancillas can be described by the following covariance matrix[49]

$$\sigma_{E_1E_2} = \begin{pmatrix} \omega_A \mathbf{I} & \mathbf{G} \\ \mathbf{G} & \omega_B \mathbf{I} \end{pmatrix}, \tag{1}$$

with $\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $\mathbf{G} = \begin{pmatrix} g & 0 \\ 0 & g' \end{pmatrix}$. Where ω_A and ω_B are the eigen-frequencies of these two ancillas, while G stands for the correlation between two ancillary modes with corresponding parameters g and g'.

Here we assume that Alice's raw key is the reference. For simplify, we ignore the Trojan-horse attack in the quantum states preparation. The Trojan-horse attack of untrusted source in plug-and-play structure will be discussed in discussion section later. With the ideal Gaussian modulation variance $\varphi \gg 1$, the secure key rate of CV-MDI-QKD protocol R can be given by[49]

$$\begin{aligned} R &= \xi I_{AB} - I_{EA}, \\ I_{AB} &= \log_2 \frac{\mu}{\chi}, \\ I_{EA} &= h\left(\frac{\sqrt{\lambda\lambda'}}{|\tau_A - \tau_B|}\right) + \log_2 \frac{e|\tau_A - \tau_B|\mu}{2(\tau_A + \tau_B)} - h(\nu), \end{aligned} \tag{2}$$

with I_{AB} representing the mutual information between Alice and Bob, while I_{EA} being Eve's information about the raw key of Alice. $\xi \le 1$ stands for the reconciliation efficiency, χ is the equivalent noise, τ_A and τ_B are Alice's and Bob's transmissivities, respectively. The h-function is defined as $h(x) = \frac{x+1}{2}\log_2\frac{x+1}{2} - \frac{x-1}{2}\log_2\frac{x-1}{2}$ and $\mu = \varphi + 1$. Some intermediate variables are introduced to simplify the above equations, their definitions are[49] $\nu = \sqrt{(\tau_A + \lambda)(\tau_A + \lambda')}/\tau_B$, $\lambda = \kappa - ug$, and $\lambda' = \kappa + ug'$, with $\kappa = (1 - \tau_A)\omega_A + (1 - \tau_B)\omega_B$, and $u = 2\sqrt{(1 - \tau_A)(1 - \tau_B)}$. In the proof-of-principle CV-MDI-QKD experiment[49], the modulation variance $\varphi = 60$ has been achieved, so the ideal modulation assumption is a good approximation. As for reconciliation efficiency $\xi = 0.97$ can be achieved[38], which is very close to 1. The difference seems minor but has a major impact on the rate, improving ξ is a major task in nowadays CV-QKD research. When the transmission efficiency $\tau_A = \tau_B = \tau$, i.e., the symmetric condition, the secure key rate of CV-MDI-QKD under the realistic condition can be given by

$$R = \log_2 \frac{8\tau\mu^{\xi-1}}{e^2\chi^{\xi}\sqrt{\lambda\lambda'}} + h(\nu_1), \tag{3}$$

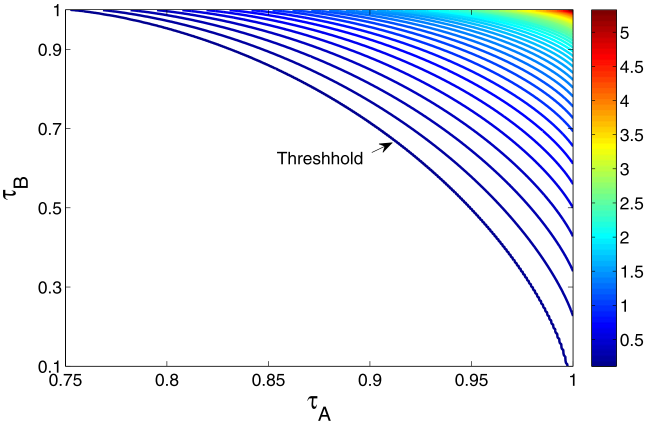

Figure 3. The secure key rate of CV-MDI-QKD varies with the transmissivities τ_A and τ_B. Here, we use the parameters $\xi = 0.97$, $\varphi = 60$ and $\varepsilon = 0.01$ for simulation. The unit of the secret key rate is bits per relay use.

with $\nu_1 = \sqrt{(\tau + \lambda)(\tau + \lambda')}/\tau$. When the transmission efficiency $\tau_A \neq \tau_B$, i.e., the asymmetric condition, the secure key rate of CV-MDI-QKD under the realistic condition can be given by

$$R = \log_2 \frac{2(\tau_A + \tau_B)\mu^{\xi-1}}{e|\tau_A - \tau_B|\chi^{\xi}} + h(\nu) - h\left(\frac{\sqrt{\lambda\lambda'}}{|\tau_A - \tau_B|}\right). \tag{4}$$

Follow the discussion in ref. [49], two situations need to be considered: one is that Alice and Bob know the transmissivities (τ_A and τ_B) and the thermal noise affecting each link (ω_A and ω_B). Then they must calculate the lower bound of the key rate for various g and g'. To determine Eve's best strategy and give a lower bound of the key rate is of central importance in any QKD protocol[1–3], since overestimate of the rate will harm the security of the final key. The minimized key rate of Eqs (3) and (4) in this situation can be written as

$$R(\tau, \omega_A, \omega_B) = h\left(\frac{\tau + \lambda_{opt}}{\tau}\right) + \log_2 \frac{8\tau\mu^{\xi-1}}{e^2\chi_{opt}^{\xi}\lambda_{opt}}, \tag{5}$$

and

$$R(\tau_A, \tau_B, \omega_A, \omega_B) = h\left(\frac{\tau_A + \lambda_{opt}}{\tau_B}\right) - h\left(\frac{\lambda_{opt}}{|\tau_A - \tau_B|}\right) + \log_2 \frac{2(\tau_A\tau_B)^{\xi}\mu^{\xi-1}}{e\,|\,\tau_A - \tau_B\,|\,(\tau_A + \tau_B + \lambda_{opt})^{\xi}}, \tag{6}$$

respectively, with $\lambda_{opt} = \kappa + u|g|_{max}$ and $\chi_{opt} = 2\,(2\tau + \lambda_{opt})/\tau$. The two expressions can be obtained by using the following two steps. First, by using the condition $g = -g'$, one can minimize the key rate. Second, by using the condition $g = |g|_{max}$, we can further minimize the key rate.

The second situation is that Alice and Bob know the transmissivities and the equivalent noise (χ). Actually, this is a more realistic situation since these parameters can be determined through data comparison in the classical post-process of the QKD protocol[49]. So the expression of the minimized key rate in symmetric condition is

$$R(\tau, \chi) = h\left(\frac{\chi - 2}{2}\right) + \log_2 \frac{16\mu^{\xi-1}}{e^2\chi^{\xi}(\chi - 4)}, \tag{7}$$

and in asymmetric condition is

$$R(\tau_A, \tau_B, \chi) = \log_2 \frac{2(\tau_A + \tau_B)\mu^{\xi-1}}{e\,|\,\tau_A - \tau_B\,|\,\chi^{\xi}} + h\left(\frac{\tau_A\chi}{\tau_A + \tau_B} - 1\right) - h\left[\frac{\tau_A\tau_B\chi - (\tau_A + \tau_B)^2}{|\tau_A - \tau_B\,|\,(\tau_A + \tau_B)}\right], \tag{8}$$

with $\chi = 2(\tau_A + \tau_B)/\tau_A\tau_B + \varepsilon$, and ε is the excess noise. The above two expressions can be achieved when $g = -g'$. So in the above two situations (thermal noise and equivalent noise), the condition $g = -g'$ can always minimize the key rate. Based on Eq. (8) and the experiment parameters of ref. [49], the secure key rate of CV-MDI-QKD for various transmissivities τ_A and τ_B is shown in Fig. 3. We can see the secure key rate is smaller when the untrusted relay is closer to the center between Alice and Bob. The ideal situation is that the untrusted relay is very close to Alice or even the CV BSM is performed by Alice. Once Bob's raw key is used as the reference, the conclusion is opposite due to the symmetry of CV-MDI-QKD protocol.

We remark that Eqs (3) to (8) are a natural generalization of the secure key rate formulas given in ref. [49] from $\xi = 1$ to a more general condition with $\xi \leq 1$. Here, we assume the condition that minimize the rate when $\xi = 1$ also holds for $\xi < 1$. In the next section, we will rigourously prove this assumption and shows the above generalization is valid.

Discussion

In this paper, a new optical kind of CV-MDI-QKD scheme has been proposed. Through delicately manipulating the polarization, two laser pulses quantum states transmitted through the same fibers before CV BSM in the relay, thus their relative phase fluctuation is negligible and the phase-reference is self-aligned without introducing any complicated technologies. Furthermore, we give an alternate proof of the minimized key rate condition to generate the secure key rate. We hope that our work can help the experimental study of the CV-MDI-QKD. One should note that the remote distance phase-locking technology may be achieved by the development of frequency combs or atom-clock synchronization.

We should point out that there are still some drawbacks in our scheme. Like all plug-and-play type QKD systems[56], there exists untrusted source problem in our scheme[64,65]. The most well-known threat for an untrusted source QKD protocol is the Trojan-horse attack[66,67]. Recently, a work shows Trojan-horse attack will greatly decrease the key rate along with the increasing of the mean photon number of the Trojan-horse mode[68]. The practical security bound against the Trojan-horse attack in DV-QKD has been shown[67]. The security of collective attack in plug-and-play CV-QKD system has also been given[69]. The wavelength filter and the intensity monitoring detector are the most suitable countermeasures for the Trojan-horse-type attack[64,65,67,69]. Note that these countermeasures will inevitably reduce the key rate. However, the unconditional security proof of CV-QKD with untrusted source is still an important open problem for future study. Similar with the plug-and-play QKD system[56], another drawback of our scheme is the strong Rayleigh scattering, which will effect the coherent detection at Charlie. This drawback has been studied in the work of the plug-and-play CV-QKD[69]. Several methods have been presented to solve this problem, such as using a wideband shot-noise-limited homodyne detector and preparing optical pulses with a narrow full width at half maximum[69]. At last, the repetition rate is limited in the plug-and-play QKD system.

Surprisingly, one could use the new scheme to build a CV-MDI-QKD network with a single untrusted source by further security analysis, which is similar with the DV-MDI-QKD network with an untrusted source[65]. Recently, the composable security against coherent attacks of CV-MDI-QKD has been proven[70].

Methods

The detailed proof of the minimized key rate condition. Due to the fact that R is the same under the transformation $g \leftrightarrow -g'$, R is symmetric with respect to the bisector $g=-g'$[49]. It should to be noticed that the minimized key rate condition $g=-g'$ has been proven and used in ref. [49]. Here, we give an alternate proof of the minimized key rate condition by using the differential method. Our proof is quite straightforward. Under different situations, the key rate is a monotonic increasing function with the corresponding variable through the positivity of its first derivative. Then the minimum of R is achieved once the variable reaches its minimum.

Consider any accessible point (g_0, g'_0), the distance between this point and bisector $g=-g'$ is d and $(l, -l)$ is the projection point of (g_0, g'_0) on bisector $g=-g'$. With simple calculation, we have $d = |g_0 + g'_0|/\sqrt{2}$ and $l = (g_0 - g'_0)/2$. Due to the symmetry, we only need to consider the sector $g_0 + g'_0 \geq 0$, which leads to $g_0 = d' + l$ and $g'_0 = d' - l$ with $d = (g_0 + g'_0)/\sqrt{2}$ and $d' = \sqrt{2}\,d/2$. Therefore, we have obtained the parameter transformation from $\{g, g'\}$ to $\{d', l\}$.

Once ω_A and ω_B are fixed (κ is fixed), we let $\lambda = \kappa - u(d' + l)$, $\lambda' = \kappa + u(d' - l)$, we have $\lambda + \lambda' = 2\delta$ and $\lambda\lambda' = \delta^2 - u^2 d'^2$ with $\delta = \kappa - ul > 0$. The minimization procedure should be considered over two parameters d' and l. Once $\chi = \frac{\beta}{\alpha}\sqrt{(\beta + \lambda)(\beta + \lambda')}$ is fixed, the analytical expression of δ can be given by $\delta = \sqrt{\alpha^2\chi^2/\beta^2 + u^2 d'^2} - \beta$ with $\alpha = \tau_A \tau_B$ and $\beta = \tau_A + \tau_B$. Meanwhile, we have $\lambda + \lambda' = 2(\sqrt{\alpha^2\chi^2/\beta^2 + u^2 d'} - \beta)$ and $\lambda\lambda' = \alpha^2\chi^2/\beta^2 + \beta^2 - 2\beta\sqrt{\alpha^2\chi^2/\beta^2 + u^2 d'^2}$. So if χ is fixed, we only need to minimize the key rate over the parameter d'.

Here we show an alternate proof that $g=-g'$ minimize the key rate whenever the thermal noise or the equivalent noise is fixed for symmetric condition with $\tau_A = \tau_B$. First, we consider the case of the fixed thermal noise. Under the symmetric condition, the expression of the key rate in Eq. (3) can be written as

$$R(y) = h(\nu_1) - \log_2 \nu_2 - \log_2 \nu_3 + \log_2 \frac{8}{e^2}, \tag{9}$$

where $\nu_1 = \sqrt{(\tau + \delta)^2 - y}/\tau$, $\nu_2 = \mu^{1-\xi}(2\sqrt{(2\tau + \delta)^2 - y}/\tau)^{\xi}$ and $\nu_3 = \sqrt{\delta^2 - y}/\tau$ with $y = u^2 d'^2$ and $0 \leq y \leq \delta^2$. Obviously, $\nu_3 < \nu_1$.

Next, we prove that $R(y)$ is monotonic increase function, so it reaches its minimum once $y=0$. The first derivative of $R'(y)$ is

$$R'(y) = \frac{1}{2\tau^2}\left(\frac{\log_2 e}{\nu_3^2} - \frac{1}{2\nu_1} g(\nu_1)\right) - (\log_2 \nu_2)' > \frac{F(y)}{2\nu_3 \tau^2} - (\log_2 \nu_2)', \tag{10}$$

with $g(x) = \log_2 \frac{x+1}{x-1}$, $F(y) = \frac{\log_2 e}{\nu_3} - \frac{1}{2} g(\nu_1)$ and $F'(y) = \frac{\log_2 e}{2\tau^2}\left[\frac{1}{\nu_3^3} - \frac{1}{\nu_1(\nu_1^2 - 1)}\right]$. It's easy to verify that $g'(x) < 0$ and $(\log_2 \nu_2)' < 0$. Due to the fact that $\nu_1^2 - \nu_3^2 = \frac{(\tau + \delta)^2 - \delta^2}{\tau^2} = \frac{\tau^2 + 2\tau\delta}{\tau^2} > 1$, we get $\nu_1^2 - 1 > \nu_3^2$, which leads to $F'(y) > 0$ and $F(y) \geq L(0)$. Since $F(0) = F(0, \delta) = \frac{\tau \log_2 e}{\delta} - \frac{1}{2}\log_2 \frac{2\tau + \delta}{\delta}$, $F'(0, \delta) = -\tau \log_2 e\left[\frac{1}{\delta^2} - \frac{1}{\delta(\delta + 2\tau)}\right] < 0$ and together with the fact that $F(0, \delta \to +\infty) \to 0$, we have $F(y) \geq F(0, \delta) > 0$. Then $R'(y) > 0$, so $R(y)$ reaches its minimum when $y=0$, which means $d'=0$, i.e., $g=-g'$.

The second situation is that the equivalent noise χ is fixed. Under this situation, the key rate of Eq. (6) is simplified under the symmetric condition as

$$R = h(\nu_1) - \log_2\nu_2 + \log_2\frac{8\mu^{\xi-1}}{\chi^{\xi}e^2}, \tag{11}$$

where $\nu_1 = \sqrt{(\tau + \lambda)(\tau + \lambda')}/\tau = \sqrt{b_1 - a_1y}$, and $\nu_2 = \sqrt{\lambda\lambda'}/\tau = \sqrt{b_2 - a_2y}$, with $y = \sqrt{\tau^2\chi^2/4 + u^2d'^2}$, $b_1 = \frac{\chi^2}{4} + 1, a_1 = \frac{2}{\tau}, b_2 = \frac{\chi^2}{4} + 4$ and $a_2 = \frac{4}{\tau}$. It is easy to check that $\nu_1 > \nu_2$.

Next, we prove that $R(y)$ is a monotonic increasing function. The first derivative of $R(y)$ is

$$R'(y) = \frac{a_2\log_2 e}{2\nu_2^2} - \frac{a_1}{4\nu_1}g(\nu_1) > \frac{L(y)}{2\nu_1}, \tag{12}$$

with $L(y) = \frac{a_2\log_2 e}{\nu_2} - \frac{a_1}{2}g(\nu_1)$ and $L'(y) = \left[\frac{a_2^2}{2\nu_2^3} - \frac{a_1^2}{2\nu_1(\nu_1^2 - 1)}\right]\log_2 e$. Due to $\chi \geq \beta^2/\alpha = 4$, one has $\upsilon_1^2 - \upsilon_2^2 = (a_2 - a_1)y - (b_2 - b_1) = \frac{2}{\tau}y - 3 \geq \frac{2}{\tau}\frac{\tau\chi}{2} - 3 = \chi - 3 \geq 1$. So $\nu_1^2 - 1 \geq \nu_2^2$ and along with the fact that $a_2 > a_1$, we have $L'(y) > 0$ which further indicates $L(y) \geq L\left(\frac{\tau\chi}{2}\right)$. $L'\left(\frac{\tau\chi}{2}\right) = -\frac{4\log_2 e}{\tau}\left[\frac{1}{(\chi - 4)^2} - \frac{1}{\chi(\chi - 4)}\right] < 0$ with χ being a variable, together with the fact that $L\left(\frac{\tau\chi}{2}\right) \to 0$ when $\chi \to +\infty$, we have $L\left(\frac{\tau\chi}{2}\right) > 0$. Finally, $R'(y) > L(y)/2\nu_1 \geq L\left(\frac{\tau\chi}{2}\right)/2\nu_1 > 0$. So $R(y)$ is a monotonic increasing function with its minimum obtained once y reaches its minimum. Due to the fact that y reaches its minimum when $d' = 0$, then $g = -g'$ minimize the key rate under the symmetric condition.

In the above discussion, we have provided an alternate proof that $g = -g'$ is Eve's best strategy in the symmetric condition no matter with the fixed thermal noise or equivalent noise. Next we analyze the general condition with $\tau_A \neq \tau_B$.

We first consider the situation with fixed equivalent noise. The key rate of Eq. (8) can be expressed as

$$R = h(\nu_1) - h(\nu_2) + \log_2\frac{2(\tau_A + \tau_B)\mu^{\xi-1}}{e|\tau_A - \tau_B|\chi^{\xi}}, \tag{13}$$

where $\nu_1 = \sqrt{b_1 - a_1y}$ and $\nu_2 = \sqrt{b_2 - a_2y}$ with $y = \sqrt{u^2d'^2 + \alpha^2\chi^2/\beta^2}$, $b_1 = 1 + \tau_A^2\chi^2/\beta^2$, $a_1 = \frac{2}{\tau_B}$, $b_2 = (\beta^2 + \alpha^2\chi^2/\beta^2)/(\beta^2 - 4\alpha)$ and $a_2 = 2\beta/(\beta^2 - 4\alpha)$. The domain of definition for variable y is $[y_{min}, y_{max}] = [\alpha\chi/\beta, (\alpha^2\chi^2/\beta^2 + \beta^2)/2\beta]$.

Next, we prove that $R(y)$ is a monotonic increasing function with y. Then its minimum can be achieved once y reaches its minimum ($d' = 0$ or equivalently $g = -g'$). The first derivative of $R(y)$ is

$$R'(y) = \frac{a_2}{4\nu_2}g(\nu_2) - \frac{a_1}{4\nu_1}g(\nu_1). \tag{14}$$

Introducing the variable transformations $q(y) = \frac{\nu_1 + \nu_2}{2}$ and $p(y) = \frac{\nu_1 - \nu_2}{2}$, rewrite the expression of $R'(y)$ as

$$R'(y) = \frac{p'(y)}{2}[g(\nu_1) + g(\nu_2)] + \frac{q'(y)}{2}[g(\nu_1) - g(\nu_2)], \tag{15}$$

with $p'(y) = \frac{a_2\nu_1 - a_1\nu_2}{4\nu_1\nu_2}$ and $q'(y) = -\frac{a_2\nu_1 + a_1\nu_2}{4\nu_1\nu_2} < 0$. The relationship between ν_1 and ν_2 can be summarized as

$$\begin{aligned} &\nu_1 > \nu_2 \quad (\tau_A \geq 2\tau_B), \\ &\nu_1 < \nu_2 \quad (\tau_A < 2\tau_B). \end{aligned} \tag{16}$$

While there is an extra restriction for χ when $\nu_1 < \nu_2$

$$\begin{aligned} &\chi \geq \frac{2\tau_B\beta}{\tau_A(2\tau_B - \tau_A)}(\tau_B < \tau_A \leq 2\tau_B), \\ &\chi \geq \frac{2\beta}{\tau_A}(\tau_A < \tau_B), \end{aligned} \tag{17}$$

otherwise $\nu_1 > \nu_2$. Meanwhile, $p'(y) > 0$ holds for any value of the parameters. For $\nu_1 > \nu_2$, since $g(x)$ is a monotonically decreasing function, we have $g(\nu_1) < g(\nu_2)$. Alongside with the fact that $q' < 0$ and $p' > 0$, it's easy to see that $R'(y) > 0$.

The remaining problem is to prove $R'(y) > 0$ also holds for $\nu_1 < \nu_2$. Introducing a new function $D(y) = d(\nu_1) - d(\nu_2)$ with $d(x) = (x - 1)g(x)$. The first and second derivatives of $d(x)$ are $d'(x) = g(x) - \frac{2\log_2 e}{x+1}$, and $d''(x) = \frac{2\log_2 e}{x+1}\left(\frac{1}{x+1} - \frac{1}{x-1}\right) < 0$, respectively. Since $d'(x) \to 0(x \to +\infty)$, we have $d'(x) > 0$. So $d(x)$ is a monotonically increasing function. Due to the fact that $\nu_1 < \nu_2$, i.e., $D(y) < 0$, the following inequation holds $\frac{g(\nu_1)}{g(\nu_2)} < \frac{\nu_2 - 1}{\nu_1 - 1}$. Thus, we have

$$R'(y) = \frac{a_2}{4\nu_2}g(\nu_2) - \frac{a_1}{4\nu_1}g(\nu_1) > \frac{a_1}{4\nu_2}g(\nu_2)\frac{A(y)}{a_1\nu_1(\nu_1 - 1)}, \tag{18}$$

where $A(y) = (a_2\nu_1^2 - a_1\nu_2^2) - (a_2\nu_1 - a_1\nu_2) = (a_2\nu_1^2 - a_1\nu_2^2) - k(y) \geq (a_2\nu_1^2 - a_1\nu_2^2) - k(y_{\min})$ with $k(y) = a_2\nu_1 - a_1\nu_2$. Here we use the fact that $k(y) \leq k(y_{\min})$ when $\nu_1 < \nu_2$. For $\tau_B < \tau_A \leq 2\tau_B$,

$$k(y_{\min}) = \frac{4\tau_A\tau_B\chi}{(\tau_A + \tau_B)(\tau_A - \tau_B)^2} - \frac{2(\tau_A + \tau_B)(2\tau_B - \tau_A)}{\tau_B(\tau_A - \tau_B)^2}, \tag{19}$$

which leads to

$$A(y) \geq \frac{2\tau_A^3[\chi^2 - 2\tau_B(\tau_A + \tau_B)\chi/\tau_A^2]}{(\tau_A^2 - \tau_B^2)^2} - \frac{2(\tau_A + \tau_B)}{\tau_B(\tau_A - \tau_B)}. \tag{20}$$

Due to $\chi \geq \frac{2\tau_B(\tau_A + \tau_B)}{\tau_A(2\tau_B - \tau_A)} > \frac{\tau_B(\tau_A + \tau_B)}{\tau_A^2}$, we have $A(y) \geq \frac{4\tau_A^2(3\tau_B - \tau_A)}{\tau_B(\tau_A - \tau_B)(2\tau_B - \tau_A)^2} > 0$, thus $R'(y) > 0$. For $\tau_A < \tau_B$,

$$k(y_{\min}) = \frac{4\tau_A^2\chi}{(\tau_A + \tau_B)(\tau_A - \tau_B)^2} - \frac{2\tau_A(\tau_A + \tau_B)}{\tau_B(\tau_A - \tau_B)^2}, \tag{21}$$

which leads to

$$A(y) \geq \frac{2\tau_A^3\tau_B[\chi^2 - 2(\tau_A + \tau_B)\chi/\tau_A]}{\tau_B(\tau_A^2 - \tau_B^2)^2}. \tag{22}$$

Due to $\chi \geq \frac{2(\tau_A + \tau_B)}{\tau_A} > \frac{\tau_A + \tau_B}{\tau_A}$, we have $A(y) \geq 0$, thus $R'(y) > 0$. Therefore, $R'(y) > 0$ is a general result independent of the values of parameters. In conclusion, $g = -g'$ always minimized the key rate when χ is fixed. As for the condition with thermal noise ω_A and ω_B fixed, we can follow the above procedures to prove $g = -g'$ minimize the rate. For simplicity, we will not show the detailed calculations here. Follow the above discussion, in this situation the rate can be further minimized when $\lambda = \lambda_{opt}$, we also prove this conclusion.

The relationship between ν_1 and ν_2. Now we compare ν_1 and ν_2 through determining the sign of function

$$\nu_1 - \nu_2 = \frac{(b_1 - b_2) - (a_1 - a_2)y}{\upsilon_1 + \upsilon_2} = \frac{a_1 - a_2}{\upsilon_1 + \nu_2}(y_0 - y), \tag{23}$$

with $y_0 = \frac{b_1 - b_2}{a_1 - a_2}$. The above equation holds when $a_1 \neq a_2$.

For $a_1 = a_2$ ($\tau_A = 3\tau_B$), $\nu_1 - \nu_2 = \frac{b_1 - b_2}{\upsilon_1 + \upsilon_2}$. Based on the fact that $\chi > \frac{2\beta}{\tau_A}$, it's easy to verify $b_1 > b_2$ and $\nu_1 > \nu_2$.

For $a_1 < a_2$ ($\tau_A < 3\tau_B$), $y \geq y_0$ means $\nu_1 \geq \nu_2$ and $y < y_0$ means $\nu_1 < \nu_2$. Then, $y_{\max} - y_0 > 0$, here we use the fact that $\chi \geq \beta^2/\alpha$. If $3\tau_B > \tau_A > 2\tau_B$, and based on the fact that $\frac{\tau_A\chi}{\beta} > \frac{\beta}{\tau_B} > 2$, we have $y_{\min} > y_0$ which means $\nu_1 > \nu_2$. If $\tau_A < 2\tau_B$, $y_{\min} \leq y_0$ holds only if $\chi \geq \frac{\beta(3\tau_B - \tau_A + |\tau_A - \tau_B|)}{\tau_A(2\tau_B - \tau_A)}$. For $\tau_B < \tau_A < 2\tau_B$, we have $\chi \geq \frac{2\tau_B\beta}{\tau_A(2\tau_B - \tau_A)}$. For $\tau_A < \tau_B$, we have $\chi \geq \frac{2\beta}{\tau_A}$. So with the proper value of χ, $\nu_1 \leq \nu_2$ can be reached when $\tau_A < 2\tau_B$.

For $a_1 > a_2$ ($\tau_A > 3\tau_B$), $y \leq y_0$ leads to $\nu_1 \geq \nu_2$ while $y > y_0$ leads to $\nu_1 < \nu_2$. Following the same procedure, $y_{\max} - y_0 < 0$, so we have $\nu_1 > \nu_2$. In a word, once $\tau_A \geq 2\tau_B$, we have $\nu_1 > \nu_2$.

The Proof of $p'(y) > 0$. The expression of $p'(y)$ is $p'(y) = \frac{a_2\nu_1 - a_1\nu_2}{4\nu_1\nu_2}$. Here we introduce a new function $k(y) = a_2\nu_1 - a_1\nu_2$, $k'(y) = \frac{a_1a_2}{2}\left(\frac{1}{\nu_2} - \frac{1}{\nu_1}\right)$.

For $\tau_A \geq 2\tau_B$, we have $\nu_1 > \nu_2$. Then $k'(y) > 0$, so $k(y) \geq k(y_{\min}) > 0$, we have $p'(y) > 0$. Next, we consider the condition $\tau_A < 2\tau_B$. Based on Eq. (17), once $\chi < \frac{\beta(3\tau_B - \tau_A + |\tau_A - \tau_B|)}{\tau_A(2\tau_B - \tau_A)}$, $\nu_1 > \nu_2$ so we get $p'(y) > 0$. Once $\chi \geq \frac{\beta(3\tau_B - \tau_A + |\tau_A - \tau_B|)}{\tau_A(2\tau_B - \tau_A)}$, $y_{\min} \leq y_0 < y_{max}$. The region of y can be divided into three parts

$$\begin{aligned} &y_{\min} < y < y_0,\ k'(y) < 0(\nu_1 < \upsilon_2), \\ &y = y_0,\ k'(y) = 0(\nu_1 = \nu_2 = \nu), \\ &y_0 < y < y_{\max},\ k'(y) > 0(\nu_1 > \nu_2). \end{aligned} \tag{24}$$

It's easy to see that $k(y)$ reaches its minimum when $\nu_1 = \nu_2$, so $k(y) = a_2\nu_1 - a_1\nu_2 \geq (a_2 - a_1)\nu > 0$, we have $p'(y) > 0$. Therefore, $p'(y) > 0$ is always satisfied independent of the values of parameters.

Minimization over λ. Once the thermal noise is fixed, the minimization is actually a two-step procedure. We have already proved $g = -g'$ minimize the key rate, next is to prove $\lambda = \lambda_{opt}$ further minimize the key rate. The key rate can be divided into the following two parts

$$R = H(\tau_A, \tau_B, \lambda) + L(\tau_A, \tau_B, \lambda), \tag{25}$$

with $H(\tau_A, \tau_B, \lambda) = h\left(\frac{\tau_A + \lambda}{\tau_B}\right) - h\left(\frac{\lambda}{|\tau_A - \tau_B|}\right)$, and $L(\tau_A, \tau_B, \lambda) = \log_2 \frac{2(\tau_A\tau_B)^{\xi}\mu^{\xi-1}}{e|\tau_A - \tau_B|(\tau_A + \tau_B + \lambda)^{\xi}}$.

It is easy to see that $L(\tau_A, \tau_B, \lambda)$ is minimized when maximizing λ, so the remaining part is to prove that $H(\tau_A, \tau_B, \lambda)$ is also minimized under this same condition. To find the minimum of $H(\tau_A, \tau_B, \lambda)$, we give its first and second derivatives $H'(\tau_A, \tau_B, \lambda) = \frac{1}{2\tau_B} g\left(\frac{\tau_A + \lambda}{\tau_B}\right) - \frac{1}{2\,|\,\tau_A - \tau_B|} g\left(\frac{\lambda}{|\tau_A - \tau_B|}\right)$, and $H''(\tau_A, \tau_B, \lambda) = \frac{1}{\lambda^2 - |\,\tau_A - \tau_B|^2} - \frac{1}{(\lambda + \tau_A)^2 - {\tau_B}^2}$, respectively. Then the sign of $H''(\tau_A, \tau_B, \lambda)$ is determined by the sign of the following term $(\lambda^2 - |\tau_A - \tau_B|^2) - [(\lambda + \tau_A)^2 - {\tau_B}^2] = -2\tau_A(\lambda + \tau_A - \tau_B) \leq -2\tau_A(\lambda - |\tau_A - \tau_B|) < 0$. Here, we use the fact that $\lambda > |\tau_A - \tau_B|$. If λ satisfies $\lambda \leq |\tau_A - \tau_B|$, a clear consequence is that $\frac{\lambda}{|\tau_A - \tau_B|} \leq 1$ is existing. So $h\left(\frac{\lambda}{|\tau_A - \tau_B|}\right)$ will give complex value which is certainly non-physical. So to overcome this problem, we have to set $\lambda > |\tau_A - \tau_B|$, and this further confirms $\frac{\tau_A + \lambda}{\tau_B} > 1$ to make the term $h\left(\frac{\tau_A + \lambda}{\tau_B}\right)$ physical. So $H''(\tau_A, \tau_B, \lambda) > 0$, makes $H'(\tau_A, \tau_B, \lambda)$ monotonically increasing in the region. For $\lambda \rightarrow +\infty$, $H'(\tau_A, \tau_B, \lambda) \rightarrow 0$, combined with the fact that it increases monotonically, we obtain $H'(\tau_A, \tau_B, \lambda) < 0$. So $H(\tau_A, \tau_B, \lambda)$ monotonically decreases in the region, and it reaches its minimum when maximizing λ, which equals $\lambda_{opt} = \lambda + u|g|_{max}$. Based on the deduction above, we prove that R reaches its minimum when λ reaches its maximum. For simplicity, we only give the proof for asymmetric condition above. It's easy to prove the conclusion also holds for the symmetric condition.

References

1. Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **74**, 145–195 (2002).
2. Scarani, V. *et al.* The security of practical quantum key distribution. *Rev. Mod. Phys.* **81**, 1301–1350 (2009).
3. Weedbrook, C. *et al.* Gaussian quantum information. *Rev. Mod. Phys.* **84**, 621–669 (2012).
4. Qiu, J. Quantum communications leap out of the lab. *Nature* **508**, 441 (2014).
5. Shannon, C. E. Communication theory of secrecy systems. *Bell System Tech. J* **28**, 656–715 (1949).
6. Fung, C.-H. F., Qi, B., Tamaki, K. & Lo, H.-K. Phase-remapping attack in practical quantum-key-distribution systems. *Phys. Rev. A* **75**, 032314 (2007).
7. Zhao, Y., Fung, C.-H. F., Qi, B., Chen, C. & Lo, H.-K. Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems. *Phys. Rev. A* **78**, 042333 (2008).
8. Lydersen, L. *et al.* Hacking commercial quantum cryptography systems by tailored bright illumination. *Nat. Photonics* **4**, 686–689 (2010).
9. Weier, H. *et al.* Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors. *New J. Phys.* **13**, 073024 (2011).
10. Tang, Y.-L. *et al.* Source attack of decoy-state quantum key distribution using phase information. *Phys. Rev. A* **88**, 022308 (2013).
11. Braunstein, S. L. & Pirandola, S. Side-channel-free quantum key distribution. *Phys. Rev. Lett.* **108**, 130502 (2012).
12. Lo, H.-K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **108**, 130503 (2012).
13. Zhou, Y.-H., Yu, Z.-W. & Wang, X.-B. Making the decoy-state measurement-device-independent quantum key distribution practically useful. *Phys. Rev. A* **93**, 042324 (2016).
14. Lo, H.-K., Curty, M. & Tamaki, K. Secure quantum key distribution. *Nat. Photonics* **8**, 595–604 (2014).
15. Wang, X.-B. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.* **94**, 230503 (2005).
16. Lo, H.-K., Ma, X. & Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **94**, 230504 (2005).
17. Rubenok, A., Slater, J. A., Chan, P., Lucio-Martinez, I. & Tittel, W. Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks. *Phys. Rev. Lett.* **111**, 130501 (2013).
18. Liu, Y. *et al.* Experimental measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **111**, 130502 (2013).
19. Ferreira da Silva, T. *et al.* Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits. *Phys. Rev. A* **88**, 052303 (2013).
20. Tang, Z. *et al.* Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **112**, 190503 (2014).
21. Tang, Y.-L. *et al.* Measurement-device-independent quantum key distribution over 200 km. *Phys. Rev. Lett.* **113**, 190501 (2014).
22. Wang, C. *et al.* Phase-reference-free experiment of measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **115**, 160502 (2015).
23. Yin, H.-L. *et al.* Measurement-device-independent quantum key distribution over a 404 km optical fiber. *Phys. Rev. Lett.* **117**, 190501 (2016).
24. Comandar, L. *et al.* Quantum key distribution without detector vulnerabilities using optically seeded lasers. *Nat. Photonics* **10**, 312–315 (2016).
25. Fu, Y., Yin, H.-L., Chen, T.-Y. & Chen, Z.-B. Long-distance measurement-device-independent multiparty quantum communication. *Phys. Rev. Lett.* **114**, 090501 (2015).
26. Tang, Y.-L. *et al.* Measurement-device-independent quantum key distribution over untrustful metropolitan network. *Phys. Rev. X* **6**, 011024 (2016).
27. Yin, H.-L. *et al.* Experimental measurement-device-independent quantum digital signatures over a metropolitan network. *Phys. Rev. A* **95**, 042338 (2017).
28. Roberts, G. *et al.* Experimental measurement-device-independent quantum digital signatures. *Nat. Commun.* **8**, 1098 (2017).
29. Pirandola, S., Laurenza, R., Ottaviani, C. & Banchi, L. Fundamental limits of repeaterless quantum communications. *Nature communications* **8**, 15043 (2017).
30. Pirandola, S. *et al.* Theory of channel simulation and bounds for private communication. *Quantum Science and Technology* **3**, 035009 (2018).
31. Cerf, N. J., Lévy, M. & Assche, G. V. Quantum distribution of gaussian keys using squeezed states. *Phys. Rev. A* **63**, 052311 (2001).
32. Grosshans, F. & Grangier, P. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.* **88**, 057902 (2002).
33. Grosshans, F. *et al.* Quantum key distribution using gaussian-modulated coherent states. *Nature* **421**, 238–241 (2003).
34. Grosshans, F. & Cerf, N. J. Continuous-variable quantum cryptography is secure against non-gaussian attacks. *Phys. Rev. Lett.* **92**, 047905 (2004).
35. Weedbrook, C. *et al.* Quantum cryptography without switching. *Phys. Rev. Lett.* **93**, 170504 (2004).
36. Pirandola, S., Mancini, S., Lloyd, S. & Braunstein, S. L. Continuous-variable quantum cryptography using two-way quantum communication. *Nat. Physics* **4**, 726–730 (2008).
37. 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).
38. Jouguet, P., Kunz-Jacques, S. & Leverrier, A. Long-distance continuous-variable quantum key distribution with a gaussian modulation. *Phys. Rev. A* **84**, 062317 (2011).
39. Leverrier, A. Composable security proof for continuous-variable quantum key distribution with coherent states. *Phys. Rev. Lett.* **114**, 070501 (2015).
40. Qi, B., Lougovski, P., Pooser, R., Grice, W. & Bobrek, M. Generating the local oscillator "locally" in continuous-variable quantum key distribution based on coherent detection. *Phys. Rev. X* **5**, 041009 (2015).
41. Soh, D. B. S. *et al.* Self-referenced continuous-variable quantum key distribution protocol. *Phys. Rev. X* **5**, 041010 (2015).

42. Jouguet, P., Kunz-Jacques, S., Leverrier, A., Grangier, P. & Diamanti, E. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nat. Photonics* **7**, 378–381 (2013).
43. Huang, D., Huang, P., Lin, D. & Zeng, G. Long-distance continuous-variable quantum key distribution by controlling excess noise. *Sci. Rep.* **6**, 19201 (2016).
44. Leverrier, A. Security of continuous-variable quantum key distribution via a gaussian de finetti reduction. *Phys. Rev. Lett.* **118**, 200501 (2017).
45. Jouguet, P., Kunz-Jacques, S. & Diamanti, E. Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution. *Phys. Rev. A* **87**, 062313 (2013).
46. Ma, X.-C., Sun, S.-H., Jiang, M.-S. & Liang, L.-M. Local oscillator fluctuation opens a loophole for eve in practical continuous-variable quantum-key-distribution systems. *Phys. Rev. A* **88**, 022339 (2013).
47. Huang, J.-Z. *et al.* Quantum hacking on quantum key distribution using homodyne detection. *Phys. Rev. A* **89**, 032304 (2014).
48. Qin, H., Kumar, R. & Alléaume, R. Quantum hacking: Saturation attack on practical continuous-variable quantum key distribution. *Phys. Rev. A* **94**, 012325 (2016).
49. Pirandola, S. *et al.* High-rate measurement-device-independent quantum cryptography. *Nat. Photonics* **9**, 397–402 (2015).
50. Ma, X.-C., Sun, S.-H., Jiang, M.-S., Gui, M. & Liang, L.-M. Gaussian-modulated coherent-state measurement-device-independent quantum key distribution. *Phys. Rev. A* **89**, 042335 (2014).
51. Li, Z., Zhang, Y.-C., Xu, F., Peng, X. & Guo, H. Continuous-variable measurement-device-independent quantum key distribution. *Phys. Rev. A* **89**, 052301 (2014).
52. Ottaviani, C., Spedalieri, G., Braunstein, S. L. & Pirandola, S. Continuous-variable quantum cryptography with an untrusted relay: Detailed security analysis of the symmetric configuration. *Phys. Rev. A* **91**, 022320 (2015).
53. Xu, F., Curty, M., Qi, B., Qian, L. & Lo, H.-K. Discrete and continuous variables for measurement-device-independent quantum cryptography. *Nat. Photonics* **9**, 772–773 (2015).
54. Pirandola, S. *et al.* Reply to'discrete and continuous variables for measurement-device-independent quantum cryptography'. *Nat. Photonics* **9**, 773–775 (2015).
55. Zhao, B., Chen, Z.-B., Chen, Y.-A., Schmiedmayer, J. & Pan, J.-W. Robust creation of entanglement between remote memory qubits. *Phys. Rev. Lett.* **98**, 240502 (2007).
56. Muller, A. *et al.* plug and play systems for quantum cryptography. *Appl. Phys. Lett.* **70**, 793–795 (1997).
57. Choi, Y. *et al.* Plug-and-play measurement-device-independent quantum key distribution. *Phys. Rev. A* **93**, 032319 (2016).
58. Guan, J.-Y. *et al.* Observation of quantum fingerprinting beating the classical limit. *Phys. Rev. Lett.* **116**, 240502 (2016).
59. Hosseinidehaj, N. & Malaney, R. Cv-mdi quantum key distribution via satellite. *Quantum Inf. Comput.* **16**, 361–379 (2017).
60. Bedington, R., Arrazola, J. M. & Ling, A. Progress in satellite quantum key distribution. *npj Quantum Information* **3**, 30 (2017).
61. Liao, S.-K. *et al.* Satellite-to-ground quantum key distribution. *Nature* **549**, 43 (2017).
62. Liao, S.-K. *et al.* Satellite-relayed intercontinental quantum network. *Phys. Rev. Lett.* **120**, 030501 (2018).
63. Günthner, K. *et al.* Quantum-limited measurements of optical signals from a geostationary satellite. *Optica* **4**, 611–616 (2017).
64. Zhao, Y., Qi, B. & Lo, H.-K. Quantum key distribution with an unknown and untrusted source. *Phys. Rev. A* **77**, 052327 (2008).
65. Xu, F. Measurement-device-independent quantum communication with an untrusted source. *Phys. Rev. A* **92**, 012333 (2015).
66. Jain, N. *et al.* Trojan-horse attacks threaten the security of practical quantum cryptography. *New J. Phys.* **16**, 123030 (2014).
67. Lucamarini, M. *et al.* Practical security bounds against the trojan-horse attack in quantum key distribution. *Phys. Rev. X* **5**, 031030 (2015).
68. Pereira, J. & Pirandola, S. Hacking alice's box in cv-qkd. *arXiv:1807.04287* (2018).
69. Huang, D. *et al.* Continuous-variable quantum key distribution based on a plug-and-play dual-phase-modulated coherent-states protocol. *Phys. Rev. A* **94**, 032305 (2016).
70. Lupo, C., Ottaviani, C., Papanastasiou, P. & Pirandola, S. Continuous-variable measurement-device-independent quantum key distribution: Composable security against coherent attacks. *Phys. Rev. A* **97**, 052327 (2018).

Acknowledgements

H.-L. Yin gratefully acknowledges support from the Fundamental Research Funds for the Central Universities.

Author Contributions

H.-L.Y. and Y.F. have the main idea. All results are acquired through the discussion among all authors. All authors contribute to the writing and reviewing of the manuscript.

Additional Information

Competing Interests: The authors declare no competing interests.

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