Measurement-device-independent quantum key distribution with insecure sources

Hua-Jian Ding¹,²,³, Xing-Yu Zhou¹,²,³, Chun-Hui Zhang¹,²,³, Jian Li¹,²,³, and Qin Wang¹,²,³

¹Institute of quantum information and technology, Nanjing University of Posts and Telecommunications, Nanjing 210003, China. ²"Broadband Wireless Communication and Sensor Network Technology” Key Lab of Ministry of Education, NUPT, Nanjing 210003, China. and ³“Telecommunication and Networks” National Engineering Research Center, NUPT, Nanjing 210003, China.

Measurement-device-independent quantum key distribution (MDI-QKD) can eliminate all detector side-channel loopholes and has shown excellent performance in long-distance secret keys sharing. Conventional security proofs, however, require additional assumptions on sources and that can be compromised through uncharacterized side channels in practice. Here, we present a general formalism based on reference technique to prove the security of MDI-QKD against any possible sources’ imperfection and/or side channels. With this formalism, we investigate the asymptotic performance of single-photon sources without any extra assumptions on the state preparations. Our results highlight the importance of transmitters’ security.

INTRODUCTION

Quantum key distribution (QKD) can allow two legitimate users, Alice and Bob, to generate secret keys with information-theoretic security even in the presence of eavesdropper, Eve, who has unlimited computation powers. Since the first protocol, called BB84, is proposed by Bennett and Brassard in 1984 [1], QKD has achieved rapid developments theoretically and experimentally [2, 3]. In principle, QKD promises unconditional security based on quantum laws [4–6] and enables permanent protection of confidential data when combined with Vernam’s one-time pad cipher. In practice, however, realistic implementations would open security loopholes at the level of devices. These could be identified and exploited by Eve to enforce specific hacking and side-channel attacks [7–10].

One way that can resist all side-channel attacks is fully device-independent (DI) QKD. However, DI-QKD is greatly challenging to realize in that it requires perfectly efficient detection efficiency and no information leakage from the measurement units. As a compromise, a more practical strategy is proposed, namely measurement-device-independent (MDI) QKD [11, 12]. MDI-QKD is easy to implement with current technology and has been widely demonstrated [13–17]. In terms of security, MDI-QKD can remove all potential detector side channels, but still makes additional assumptions on transmitters. To be precise, in a typical MDI-QKD system, Alice and Bob prepare almost perfect states from their fully protected laboratory [11]. However, such premise on sources can be compromised through uncharacterized side channels, say, state preparation flaws (SPFs) [18], information leakage [19], and classical correlations between the generated pulses [20, 21], et al. At present, there exist solutions for some security vulnerabilities. For example, SPFs have been efficiently treated with the loss-tolerant (LT) method [22, 23] and the so-called uncharacterized qubit sources [24, 25]. Moreover, the issue of information leakage from users’ internal settings has also been studied in Refs. [26, 27, 30]. Lastly, the pulse correlations among emitted signals have been incorporated in recent works [20, 31]. Remarkably, the reference technique (RT) introduced in Ref. [31] is general to accommodate various other side channels. Inspired by the results of RT, we combine it with MDI-QKD to guarantee practical security against both sources and detection side channels. For this, we consider some reference states and bound the maximum deviation between the probabilities associated with them and those associated with the actual emitted states. In particular, we evaluate the performance of the protocol with single-photon sources.

PROTOCOL DESCRIPTION

For simplicity, we assume that there are no side channels in the following description. Figure 1 shows a typical MDI-QKD setup. 1. In each round, Alice (Bob) wants to generate the state $|\varphi_{js}\rangle_a$ ($|\varphi_{js}\rangle_b$), where $j, s \in \{0, 1\}$ and $\alpha, \beta \in \{Z, X\}$ are their bit value and basis choices, respectively. As in the LT analysis [22], they only select $j_\alpha, s_\beta \in \{0_Z, 1_Z, 0_X\}$. The states are then send out to an untrusted relay Eve via quantum channels.

2. If Eve is honest, he performs a Bell state measurement (BSM) that projects the incoming signals into Bell state. Next, he announces the results of BSM. For simplicity, the discussion below only considers one Bell state: $|\psi^\text{−}\rangle$.

3. Alice and Bob keep the data that corresponds to the successful instances and discard the rest, regardless of whether they employ the same or different bases. Next, say Bob flips his data to correctly correlate them with those of Alice.

4. Alice and Bob reveal part of their sifted keys to estimate both the bit and the phase error rates. Finally, they perform error correction and privacy amplification to extract secret key strings.
In fact, for each particular round of the protocol, the emitted joint states are actually in the form
\[ |\Phi_{j, s}\rangle_T = \sqrt{1 - \varepsilon_j} |\phi_{j, s}\rangle_T + \sqrt{\varepsilon_j} |\phi^+_{j, s}\rangle_T, \]
where \( T := aE \), which include Alice’s (Bob’s) transmitted system \( a \) (\( b \)) and Eve’s system \( E \). \( \varepsilon_j \), \( s \) is a non-negative real number that satisfies \( 0 \leq \varepsilon_j \leq 1 \). Notice in this state that does not contain any information about Alice’s and Bob’s current round selections, and \( |\phi^+_{j, s}\rangle_T \) is an unknown side-channels state orthogonal to \( |\phi_{j, s}\rangle_T \). Importantly, any potential side channels from transmitters can be characterized with Eq. (1), which thus represents the most general description of the emitted states. This have been detailedly substantiated in Ref. 32.

The asymptotic key rate for single-photon sources is given by
\[ R \geq Y_{ZZ} [1 - h(e_{XX})] - f_{EC} \cdot h(e_{ZZ}), \]
where \( Y_{ZZ} \) and \( e_{ZZ} \) are the yield and bit error rate in ZZ basis, respectively, and can be directly obtained from experiment. The function of \( h(\cdot) \) is the binary entropy function and \( f_{EC} (= 1.16) \) is the error correction efficiency. The term \( e_{XX} \) is the phase error rate, which is an essential parameter to be estimated. For this, we use the complementary augment introduced by Koashi [33], where an equivalent virtual protocol is created.

In the virtual protocol, from Eve’s perspective, Alice and Bob first prepare the following state in the ZZ basis:
\[ |\Phi^{vir}_{ABT}\rangle = \frac{1}{2} \sum_{j, s=0, 1} |j, s\rangle_{AB} |\Phi_{j, s}\rangle_T, \]
with \( |0_z, 1_z\rangle \) being the computational basis for ancillary systems \( A \) and \( B \), and subsequently they send the system \( T \) to Eve. We then define the bit error rate as
\[ e_{XX} = \frac{Y_{ZZ}^{(XX)} + Y_{ZZ}^{(XX)} + Y_{ZZ}^{(XX)} + Y_{ZZ}^{(XX)}}{Y_{ZZ}^{(XX)} + Y_{ZZ}^{(XX)} + Y_{ZZ}^{(XX)} + Y_{ZZ}^{(XX)}}, \]
where the yield \( Y_{ZZ}^{(XX)} \) is the joint probability that Eve declare a successful BSM when Alice and Bob first prepare the state \( |\Phi^{vir}_{ABT}\rangle \) and Alice (Bob) obtains the bit value \( j \) (\( s \)) by measuring the system \( A \) (\( B \)) in the ZZ basis. Note that the superscripts ZZ denote the bases employed in state preparation, while the subscripts represent the bases used in local measurement. For brevity of notation, we shall omit the bases superscript or mode subscript, unless otherwise needed. Similarly, the phase error rate is defined as
\[ e_{XX} = \frac{Y_{ZZ}^{(XX)} + Y_{ZZ}^{(XX)} + Y_{ZZ}^{(XX)} + Y_{ZZ}^{(XX)}}{Y_{ZZ}^{(XX)} + Y_{ZZ}^{(XX)} + Y_{ZZ}^{(XX)} + Y_{ZZ}^{(XX)}}, \]
where \( Y_{ZZ}^{(XX)} \) is the joint probability that Alice (Bob) obtains bit value \( s \) (\( j \)) in the virtual X-basis measurement on system \( A \) (\( B \)) given the state preparation \( |\Phi^{vir}_{ABT}\rangle \) and also Eve declares a successful BSM. The phase error rate corresponds to the bit error in the virtual protocol. In addition, we have that the denominator of \( e_{XX} \) in Eq. (16) is equal to \( \sum_{j, s=0, 1} Y_{j, s} = 1 \). Therefore, we only need to calculate the numerator \( \Omega := Y_{00, 00} + Y_{11, 11} \) for \( e_{XX} \). Note that after Alice and Bob complete the virtual X-basis measurement, they send Eve the unnormalized states:
\[ |\hat{\Theta}^{vir}_{j, s}\rangle = T_{\hat{\Theta}^{vir}_{j, s}} (|j, s\rangle \langle j, s|_{AB} \otimes |\epsilon\rangle_E |\Phi^{vir}_{ABT}\rangle \langle \Phi^{vir}_{ABT}|), \]
where \( T_{\hat{\Theta}^{vir}_{j, s}} \) is the partial trace over ancillary systems \( A, B \). We write the normalized version as \( \hat{\Theta}^{vir}_{j, s} = T_{\hat{\Theta}^{vir}_{j, s}} (|\hat{\Theta}^{vir}_{j, s}\rangle \langle \hat{\Theta}^{vir}_{j, s}|) \).

To find the unknown quantity \( \Omega \), we employ the RT method [31], namely considering some reference states that close to their respective actual states. These reference states, in principle, can be chosen freely, but they should be selected in a way that it is easy to derive a relationship among the probabilities associated with them. For this, as an example, we select the reference states to be \( \{|\varphi_0\rangle, |\varphi_1\rangle, |\varphi_0\rangle\rangle \} \) for each user, which are defined as
\[ |\varphi_0\rangle = \cos \left( \frac{\delta_i}{4} \right) |0_z\rangle + \sin \left( \frac{\delta_i}{4} \right) |1_z\rangle, \]
\[ |\varphi_1\rangle = \sin \left( \frac{\delta_i}{4} \right) |0_z\rangle + \cos \left( \frac{\delta_i}{4} \right) |1_z\rangle, \]
\[ |\varphi_0\rangle = \sin \left( \frac{\delta_i}{4} \right) |0_z\rangle + \cos \left( \frac{\delta_i}{4} \right) |1_z\rangle, \]
where \( \delta_i (i = 1, 2, 3) \) denote the deviations of the phase modulation from the intended values due to encoding modulators. We emphasize that these reference states are never prepared in actual protocol but serve as mathematical tool for parameter estimation.

From the definitions of \( \hat{\Phi}^{vir}_{j, s} \), \( \hat{\Theta}^{vir}_{j, s} \) and \( Y_{s, X; j, X}^{vir} \), we can define analogous states and probabilities \( \hat{\Psi}^{vir}_{j, s} \), \( \hat{\Theta}^{vir}_{j, s} \) and \( Y_{s, X; j, X}^{vir} \) for reference states. In particular, the yields
\[ Y_{s, X; j, X}^{vir} = p_{s, j}^{vir} \cdot T_{\hat{\Theta}^{vir}_{j, s}} \left[ |\hat{\Psi}^{vir}_{j, s}\rangle \langle \hat{\Psi}^{vir}_{j, s}| \right], \]
where $\hat{M}_{\psi}$—corresponds to the successful announcement of Eve’s BSM, and $p^\text{vir}_{j,s} = Tr \left[ \Theta^\text{vir}_{j,s} \right]$. Again, we define an analogous quantity $\Omega^\text{ref} := Y^\text{vir}_{j,s} + Y^\text{vir}_{j,s}$ for the reference states, and then evaluate the deviation between the probabilities associated with the reference states and those associated with the actual states. Following the analysis of Ref. [31], this deviation is quantified by

$$G^L \left( \langle A | M | A \rangle, |\langle A | R \rangle| \right) \leq \langle R | \hat{M} | R \rangle \leq G^U \left( \langle A | M | A \rangle, |\langle A | R \rangle| \right)$$

(9)

where $|A\rangle$ and $|R\rangle$ are normalized pure state associated with the actual and reference states, respectively. $M$ is any non-negative bounded operator such that $0 \leq M \leq 1$, and we define $M = (|0_x, 0_z\rangle \langle 0_x, 0_z| + |1_x, 1_z\rangle \langle 1_x, 1_z|) \otimes M_{\psi}$. By applying Cauchy-Schwarz inequality to the vectors $\sqrt{N} |A\rangle$ and $\sqrt{N} |R\rangle$, with one $N = M$ and another $N = \hat{M}$, we can get the functions $G^L(x, y)$ and $G^U(x, y)$ as follows

$$G^L(x, y) = \left\{ \begin{array}{ll}
0 & x < 1 - y^2 \\
x + (1 - y^2)(1 - 2y) - 2y\sqrt{(1 - y^2)(1 - x)} & x \geq 1 - y^2
\end{array} \right.$$  

(10)

and

$$G^U(x, y) = \left\{ \begin{array}{ll}
0 & x < 1 - y^2 \\
x + (1 - y^2)(1 - 2y) + 2y\sqrt{(1 - y^2)(1 - x)} & x \geq 1 - y^2
\end{array} \right.$$  

(11)

Note that $-G^L(x, y)$ and $G^U(x, y)$ are concave with respect to $0 \leq x \leq 1$ for any fixed $0 \leq y \leq 1$, and $\partial_y G^L(x, y) \geq 0$ and $\partial_y G^U(x, y) \leq 0$ hold. And then, since $\Omega = \langle \Phi^\text{vir} | M | \Phi^\text{vir} \rangle$ and $\Omega^\text{ref} = \langle \Psi^\text{vir} | M | \Psi^\text{vir} \rangle$, we can employ Eq. (10) to get an upper bound on $\Omega$:

$$\Omega \leq G^U(\Omega^\text{ref}, \delta^\text{vir}) \leq \Omega^\text{ref} + \delta^\text{vir} = : \Omega^\text{ref},$$

(12)

where $\Omega^\text{ref}$ is an upper bound on $\Omega^\text{ref}$, and $\delta^\text{vir}$ is $\frac{1}{4} \sum_{j,s} \sqrt{1 - e_{j,s}}$ a lower bound on $\delta^\text{vir} := \langle \Psi^\text{vir} | M | \Phi^\text{vir} \rangle$. Importantly, $\Omega^\text{ref}$ can be bounded from all observables $Y_{j,s}$ of the actual states and from the square root fidelities of $\langle \Psi_{j,s} | \Phi_{j,s} \rangle$, with $\langle \Psi_{j,s} | \Phi_{j,s} \rangle = |\varphi_{j,s}(x) | \varphi_{j,s}(y) \rangle E$.

Below, we show how to obtain $\Omega^\text{ref}$ in detail. According to the LT method [22], the virtual states $\Theta^\text{vir}_{j,s}$ can be expressed as a linear combination of the Pauli operators $\{\sigma_1, \sigma_X, \sigma_Z\}$:

$$\Theta^\text{vir}_{j,s} = \frac{1}{4} \sum_{l,l'} S^l_{j,s} |l \rangle \langle l'\rangle \sigma_l \otimes \sigma_{l'},$$

(13)

where $S^l_{j,s}$ with $l, l' \in \{I, X, Z\}$ are the coefficients of the Bloch vector. Define the transmission rate of $\sigma_l \otimes \sigma_{l'}$ as

$$q_{l,l'} = \frac{1}{4} Tr \left[ \hat{M}_{\psi} - \sigma_l \otimes \sigma_{l'} \right],$$

(14)

and then combine it with Eqs. (8) and (13), the transmission rate $Y^\text{vir}_{j,s}$ can be rewritten as

$$Y^\text{vir}_{j,s} = p^\text{vir}_{j,s} \sum_{l,l'} S^l_{j,s} |l \rangle \langle l'\rangle q_{l,l'}.$$  

(15)

With this notation, we can concisely write the matrix equation

$$\Omega^\text{ref} = P^\text{vir} S^\text{vir} q,$$

(16)

where $P^\text{vir} = \left[ p^\text{vir}_{l,l'} \right]$, $S^\text{vir}$ is a $2 \times 9$ matrix containing the coefficients $s^l_{l,l'}$ in its first (second) row, and $q$ is a column vector containing the quantities $q_{l,l'}$. Similarly, we have

$$Y^\text{ref} = S q.$$  

(17)

Note that once the reference states are selected, these associated matrices $P^\text{vir}$, $S^\text{vir}$ and $S$ are determined. If we further define $f_{j,s} = : P^\text{vir} S^\text{vir} S^{-1} Y^\text{ref}$, we can conveniently get

$$\Omega^\text{ref} = \sum_{j,s} f_{j,s} Y^\text{ref}_{j,s} \leq \sum_{j,s} f_{j,s} Y^\text{ref}_{j,s} G^U \left( Y^\text{ref}_{j,s}, \delta^L_{j,s} \right) + \sum_{j,s} f_{j,s} G^L \left( Y^\text{ref}_{j,s}, \delta^L_{j,s} \right) = : \Omega^\text{ref},$$

(19)

with $f_{j,s}$ being the elements of the vector $f_{j,s}$. The terms $\delta^L_{j,s}$ are lower bound on $\langle \Psi_{j,s} | \Phi_{j,s} \rangle$, and roughly set as $\delta^L_{j,s} = \sqrt{1 - e_{j,s}}$. Notably, in the absence of observed statistics $Y_{j,s}$, we instead use the $Y^\text{ref}_{j,s}$ according to a typical channel model [34] for numerical simulation. Finally, the phase error rate can be estimated by $e_{xx} = \Omega^U / \Omega^L$. To show the performance of MDI-QKD in the presence of side channels, we now present the simulation results. The experimental parameters used are as follows: detection efficiency $\eta_d = 14.5\%$ and dark-count probability $p_d = 6.02 \times 10^{-6}$ of Eve’s detectors, the intrinsic error rate $e_d = 1.5\%$ [11], and the probabilities for Alice and Bob select $Z$ basis are, for simplicity, $p_{Z_A} = p_{Z_B} = \frac{3}{5}$. According to the experimental data [22, 33], we choose $\delta_i = \delta = 0 (0.126)$ for Eq. (7). Note that these SPFs
from modulation require a characterization. Regarding side channels $\varepsilon_{j_0,s_0}$, unfortunately, there are no studies founded to fully describe it. Therefore, we select some values to evaluate this imperfection and, for simplicity, we set $\varepsilon_{j_0,s_0} = \varepsilon$ for all $j_0, s_0 \in \{0,1,2,0\times\}$. The main results are illustrated in Fig. 2.

As expected, the secret key rate sharply decreases when the side channels characterized by $\varepsilon$ increases. We note, however, that a positive key is still available when considering a large $\varepsilon$. For instance, when $\varepsilon = 10^{-6}$, Alice and Bob could generate a secret key over about 8-dB transmission loss. In addition, comparing panels (A) and (B) of Fig. 2, the secret key rate corresponding to the case $\delta = 0$ and $\delta = 0.126$ are almost overlap, which fully demonstrates the high tolerance against SPFs with channel loss of the LT method.

Furthermore, comparing the purple and the black line of Fig. 2, the secret key rates are quite different, which indicates that the side channels have a great influence on the key rate. The side channels, especially mode dependences and pulse correlations, mostly occur in high-speed systems [20, 21]. If we ignore them in security analysis, the achieved keys may not be secure. As shown in Fig. 3, where we simply assume that $\lg(\varepsilon)$ is proportional to system frequency $f$, the key rate reaches its maximum at some point, rather than increasing all the way as we would expect. Therefore, in the development of high-speed QKD systems, we need to strictly analyze the possible side channels to guarantee the security of shared keys.

To conclude, we have introduced an MDI-QKD protocol that can accommodate any side channels in transmitters, thus closing the gap between theory and reality. The security analysis is achieved by introducing reference states and then bounding the maximum deviation between the probabilities associated with them and those of the actual states. Our results show that secret keys can be surely distributed with any side channel. In this regard, we believe that our work represents an important step towards constructing a truly secure QKD with realistic devices. The next steps for our protocol would be to incorporate coherent secure and decoy-state methods and complete the experimental characterization of $\varepsilon$ in practice.

**Funding.** National Key Research and Development Program of China (2018YFA0306400 and 2017YFA0304100); National Natural Science Foundation of China (NSFC) (12074194, 11774180 and U19A2075); Leading-edge Technology Program of Jiangsu Natural Science Foundation (BK20192001); Postgraduate Research & Practice Innovation Program of Jiangsu Province (KYCX20_0726).

---

**FIG. 2.** Secret key rate versus transmission loss (dB) in the presence of side channels. (A) There are no SPFs. (B) When there exits small SPFs, the secret key rate is only slightly worse.

**FIG. 3.** Secret key rate versus side channels. Here we assume that the side channels $\varepsilon$ in $\lg$ is proportional to system frequency $f$, with $\varepsilon \in [10^{-9},10^{-6}]$ and $f \in [0.1GHz,4GHz]$. 

---

*qiw@njupt.edu.cn*

[1] C. H. Bennett, and G. Brassard, in Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India (1984), pp. 175-179.

[2] F. H. Xu, X. F. Ma, Q. Zhang, H. K. Lo and J. W. Pan, “Secure quantum key distribution with realistic devices”, Rev. Mod. Phys. 92, 025002 (2020).

[3] S. Pirandola, U. L. Andersen et al., "Advances in quantum cryptography", Adv. Opt. Photon. 12, 1012 (2020).
[4] H. K. Lo and H. F. Chau, "Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances", Science 283, 2050 (1999).

[5] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol", Phys. Rev. Lett. 85, 441 (2000).

[6] D. Mayers, "Unconditional Security in Quantum Mechanics", J. ACM 48, 351 (2001).

[7] V. Makarov, A. Anisimov, and J. Skaar, "Effects of detector efficiency mismatch on security of quantum cryptosystems", Phys. Rev. A 74, 022313 (2006).

[8] B. Qi, C.-H.-F. Fung, H.-K. Lo, and X. Ma, "Time-shift attack in practical quantum cryptosystems", Quantum Inf. Comput. 7, 73 (2007).

[9] C.-H. F. Fung, B. Qi, K. Tamaki, and H.-K. Lo, "Phase-remapping attack in practical quantum-key-distribution systems", Phys. Rev. A 75, 032314 (2007).

[10] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Hacking commercial quantum cryptography systems by tailored bright illumination", Nat. Photonics. 4, 686 (2010).

[11] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution", Phys. Rev. Lett. 108, 130503 (2012).

[12] S. L. Braunstein and S. Pirandola, "Side-channel-free quantum key distribution", Phys. Rev. Lett. 108, 130502 (2012).

[13] C. Wang, X. T. Song, Z. Q. Yin, S. Wang, W. Chen, C. M. Zhang, G. C. Guo, and Z. F. Han, "Phase-reference-free experiment of measurement-device-independent quantum key distribution", Phys. Rev. Lett. 115, 160502 (2015).

[14] L. C. Comandar, M. Lucamarini, B. Frhlich, J. F. Dynes, A.W. Sharpe, S.W. B. Tam, Z. L. Yuan, R. V. Penty, and A. J. Shields, "Quantum key distribution without detector vulnerabilities using optically seeded lasers", Nat. Photonics. 10, 312 (2016).

[15] X. Y. Zhou, H. J. Ding, C. H. Zhang, J. Li, C. M. Zhang and Q. Wang, "Experimental three-state measurement-device-independent quantum key distribution with uncharacterized sources", Opt. Lett. 45, 4176 (2020).

[16] R. I. Woodward, Y. S. Lo, M. Pittaluga M. Minden, T. K. Paraíso, M. Lucamarini, Z. L. Yuan and A. J. Shields, "Gigahertz measurement-device-independent quantum key distribution using directly modulated lasers", Npj Quantum Inf. 7, 58 (2021).

[17] Y. P. Chen, J. Y. Liu, M. S. Sun, X. Y. Zhou, C. H. Zhang, J. Li, and Q. Wang, "Experimental measurement-device-independent quantum key distribution with the double-scanningmethod", arXiv:2105.09587 (2021).

[18] D. Gottesman, H.-K. Lo, N. Lütkenhaus, J. Preskill, "Security of quantum key distribution with imperfect devices", Quantum Inf. Comput. 4, 325–360 (2004).

[19] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, G. Ribordy, "Trojan-horse attacks on quantum-key-distribution systems", Phys. Rev. A 73, 022320 (2006).

[20] K.-i. Yoshino, M. Fujiwara, K. Nakata, T. Sumiya, T. Sasaki, M. Takeoka, M. Sasaki, A. Tajima, M. Koashi, A. Tomita, "Quantum key distribution with an efficient countermeasure against correlated intensity fluctuations in optical pulses", Npj Quantum Inf. 4, 8 (2018).

[21] F. Grünenfelder, F., Boaron, A., Rusca, D., Martin, A. and Zbinden, H. "Performance and security of 5 GHz repetition rate polarization-based quantum key distribution", Appl. Phys. Lett. 117, 140003 (2020).

[22] K. Tamaki, M. Curty, G. Kato, H.-K. Lo, and K. Azuma, "Loss-tolerant quantum cryptography with imperfect sources", Phys. Rev. A 90, 052314 (2014).

[23] X. F. Ma, K. Chen, "Decoy state quantum key distribution", Phys. Rev. Lett. 94, 230503 (2005).

[24] H. K. Lo, X. F. Ma, K. Chen, "Decoy state quantum key distribution", Phys. Rev. Lett. 94, 230504 (2005).

[25] Y. Zapatero1, Á. Navarrete, K. Tamaki and M. Curty, "Security of quantum key distribution with intensity correlations", preprint arXiv:2105.11165v1 (2021).