Improving the performance of twin-field quantum key distribution with advantage distillation technology

Hong-Wei Li[1], Rui-Qiang Wang[2], Chun-Mei Zhang[3], and Qing-Yu Cai[4]

[1]Henan Key Laboratory of Quantum Information and Cryptography, SSF IEU, Zhengzhou 450000, China

[2]CAS Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei, Anhui 230026, China

[3]Institute of Quantum Information and Technology, Nanjing University of Posts and Telecommunications, Nanjing 210003, China

[4]School of Information and Communication Engineering, Hainan University, Haikou 570228, China

In this work, we apply the advantage distillation method to improve the performance of a practical twin-field quantum key distribution system under collective attack. Compared with the previous analysis result given by Maeda, Sasaki and Koashi [Nature Communication 10, 3140 (2019)], the maximal transmission distance obtained by our analysis method will be increased from 420 km to 470 km. By increasing the loss-independent misalignment error to 12%, the previous analysis method can not overcome the rate-distance bound. However, our analysis method can still overcome the rate-distance bound when the misalignment error is 16%. More surprisingly, we prove that twin-field quantum key distribution can generate positive secure key even if the misalignment error is close to 50%, thus our analysis method can significantly improve the performance of a practical twin-field quantum key distribution system.

1 Introduction

Quantum key distribution (QKD) [1] is the art of sharing information-theoretical secure key between two different remote parties Alice and Bob. Under the perfect quantum devices preparation, the eavesdropper Eve can not get the secure key information even if she has unlimited computation and storage power [2–4]. Unfortunately, a practical QKD system is usually composed of imperfect devices, and the practical QKD system may be attacked [5–8] by utilizing imperfect quantum state preparation and measurement devices. To avoid the detector side channel attack [6, 7], measurement-device-independent QKD (MDI-QKD) was proposed [9, 10]. In MDI-QKD, the ideal quantum states are randomly prepared by Alice and Bob, and then will be transmitted to untrusted Charlie to apply Bell state measurement [11]. To beat the Pirandola-Laurenza-Ottaviani-Banchi (PLOB) bound [12], twin-field QKD (TF-QKD) [13] was proposed which is a variant of the MDI-QKD protocol. TF-QKD can overcome the rate scaling from η to $\sqrt{\eta}$ with a relatively simple setup, where η is the single-photon transmissivity of the link from Alice to Bob. In the TF-QKD protocol, Charlie simply conducts an interference measurement to learn

Hong-Wei Li: lihow@ustc.edu.cn

Qing-Yu Cai: qycai@wipm.ac.cn

the relative phase between Alice and Bob, and the secure key can be generated with in-phase and anti-phase measurement outcomes respectively. More recently, many intensive studies have been devoted to achieving information theoretic proofs of variants of TF-QKD protocols [14–21], and several practical TF-QKD systems have been widely implemented in labs and field tests [22–28]. By applying the entanglement purification with two-way classical communication, the transmission distance of TF-QKD protocol can be improved [29].

To analyze the security of MDI-QKD protocols [9, 10], Alice and Bob should randomly prepare phase-randomized pulses in Z basis and X basis respectively, where Z basis consists of $|0\rangle$ and $|1\rangle$, and X basis consists of $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $|-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$. Note that the bit error rate in Z basis and X basis can also be applied to characterize the bit error rate and phase error rate about the quantum channel. Based on this quantum channel characterization, the upper bound of the secure key information leaked to Eve can be estimated. However, to estimate the bit error rate in X basis, TF-QKD needs to generate a non-classical optical state [19, 29], which is difficult to realize in current technology. Fortunately, Maeda, Sasaki and Koashi proposed the operator dominance method [19] to estimate the bit error rate in X basis by preparing phase-randomized weak coherent states. Combining the error rate in Z basis with the error rate in X basis, the practical quantum channel in TF-QKD can be characterized, and the secure key rate can be analyzed with the entanglement distillation and purification method [2, 3, 19]. The purpose of TF-QKD is to extend the transmission distance with current technology, but the final solution is to use quantum repeater in the future research [30–32].

In this work, we apply the error rate in X basis and Z basis to characterize the practical quantum channel. By applying the information-theoretical security analysis method, we apply the advantage distillation (AD) method to improve the secure key rate and transmission distance. The AD method was initially proposed in classical cryptography theory [33], then it has been widely used in different QKD protocols [34–37] to improve the error tolerance. More recently, we analyze the security of practical BB84-QKD [1], six-state-QKD [38] and MDI-QKD [9, 10] systems by combining the AD method [4] with the decoy-state method [39–41], and the analysis results demonstrate that the AD method can significantly improve the performance of different practical QKD systems [42]. Inspired by our previous work, we combine the AD method and the operator dominance method [19] to analyze the security of TF-QKD, and the analysis results demonstrate that both the transmission distance and the secure key rate can be sharply improved. More surprisingly, the analysis results also demonstrate that TF-QKD can generate positive secure key even if the loss-independent misalignment error is close to 50%, thus our analysis method can significantly improve the robustness of the practical TF-QKD system.

2 Security of QKD with AD

To prove the security of a QKD protocol, the bit error rate of different bases should be precisely estimated. It has been proved that the security of the state preparation and measurement based QKD protocol can be analyzed with the entanglement based QKD protocol [2, 4]. In the entanglement based protocol, Alice and Bob can take inputs from four-dimensional Hilbert spaces $H_A \otimes H_B$ to apply Z basis and X basis measurements. By considering BB84 [1] and six-state [38] QKD protocols, it has been proved that Eve's general attack can be reduced to the Pauli attack [4, 43], which can be described by the classical probability theory. Thus, the QKD protocol can be illustrated with the following

quantum state preparation,

$$\sigma_{AB} = \sum_{i=0}^{3} \lambda_i \left| \Phi_i \right\rangle \left\langle \Phi_i \right|, with \sum_{i=0}^{3} \lambda_i = 1, \tag{1}$$

where

$$\begin{aligned}
\left| \Phi_0 \right\rangle &= \frac{1}{\sqrt{2}} (\left| 00 \right\rangle + \left| 11 \right\rangle) \\
\left| \Phi_1 \right\rangle &= \frac{1}{\sqrt{2}} (\left| 00 \right\rangle - \left| 11 \right\rangle) \\
\left| \Phi_2 \right\rangle &= \frac{1}{\sqrt{2}} (\left| 01 \right\rangle + \left| 10 \right\rangle) \\
\left| \Phi_3 \right\rangle &= \frac{1}{\sqrt{2}} (\left| 01 \right\rangle - \left| 10 \right\rangle).
\end{aligned} \tag{2}$$

By combining this state preparation with the Z basis and X basis measurement in Alice and Bob's side, the secure key rate can be given by [4]

$$\begin{aligned}
R \geq &min_{\lambda_0,\lambda_1,\lambda_2,\lambda_3}[S(A|E) - H(A|B)] \\
= &min_{\lambda_0,\lambda_1,\lambda_2,\lambda_3}[1 - (\lambda_0 + \lambda_1)H(\frac{\lambda_0}{\lambda_0 + \lambda_1}) \\
&- (\lambda_2 + \lambda_3)H(\frac{\lambda_2}{\lambda_2 + \lambda_3}) - H(\lambda_0 + \lambda_1)],
\end{aligned} \tag{3}$$

where E is Eve's ancillary state, $S(A|E) = S(A,E) - S(E)$, $H(A|B) = H(A,B) - H(B)$, $H(x) = -x\log x - (1 - x)\log(1 - x)$ and $S(\rho) = -\text{tr}(\rho\log\rho)$ are entropy functions. Since the quantum channel can be controlled by Eve, she can choose the optimal parameters $\lambda_i, \ i = \{0, 1, 2, 3\}$ to reduce the secure key rate, but λ_i should also be restricted by the quantum bit error rate in two different bases.

To improve the maximal tolerable error rate, the repetition code protocol based AD method has been proposed [4]. In the repetition code protocol, Alice and Bob split their raw key into blocks of b bits $x_0, x_1, ...x_{b-1}$ and $y_0, y_1, ...y_{b-1}$ respectively. Alice privately generates a random bit $c \in \{0, 1\}$, and sends the message $m = m_0, m_1, ..., m_{b-1} = x_0 \oplus c, x_1 \oplus c, ...x_{b-1} \oplus c$ to Bob through an authenticated classical channel. Bob accepts the block if and only if $m_0 \oplus y_0, m_1 \oplus y_1, ..., m_{b-1} \oplus y_{b-1} \in \{0, 0, ...0 \text{ or } 1, 1, ..., 1\}$. If Alice and Bob accept the block, they keep the first bit x_0 and y_0 as the raw key. Finally, Alice and Bob will apply the error correction and privacy amplification algorithms to generate the final secure key.

Based on the repetition code protocol, the secure key rate $\tilde{R}$ can be modified as the following inequality [4]

$$\begin{aligned}
\tilde{R} \geq &max_b \ min_{\lambda_0,\lambda_1,\lambda_2,\lambda_3} \frac{1}{b} p_{succ}[1 - (\tilde{\lambda}_0 + \tilde{\lambda}_1)H(\frac{\tilde{\lambda}_0}{\tilde{\lambda}_0 + \tilde{\lambda}_1}) \\
&- (\tilde{\lambda}_2 + \tilde{\lambda}_3)H(\frac{\tilde{\lambda}_2}{\tilde{\lambda}_2 + \tilde{\lambda}_3}) - H(\tilde{\lambda}_0 + \tilde{\lambda}_1)],
\end{aligned} \tag{4}$$

where

$$\begin{aligned}
\tilde{\lambda}_0 &= \frac{(\lambda_0 + \lambda_1)^b + (\lambda_0 - \lambda_1)^b}{2p_{succ}}, \\
\tilde{\lambda}_1 &= \frac{(\lambda_0 + \lambda_1)^b - (\lambda_0 - \lambda_1)^b}{2p_{succ}}, \\
\tilde{\lambda}_2 &= \frac{(\lambda_2 + \lambda_3)^b + (\lambda_2 - \lambda_3)^b}{2p_{succ}}, \\
\tilde{\lambda}_3 &= \frac{(\lambda_2 + \lambda_3)^b - (\lambda_2 - \lambda_3)^b}{2p_{succ}},
\end{aligned} \tag{5}$$

$p_{succ} = (\lambda_0 + \lambda_1)^b + (\lambda_2 + \lambda_3)^b$ is the successful probability of the AD method. Since the parameter b in the AD method can be controlled by Alice and Bob, they can choose the optimal b to improve the secure key rate. Note that this secure key rate is based on the single photon state preparation, which can also be applied in practical QKD systems with weak coherent pulse preparation [42].

3   The virtual protocol to analyze the quantum channel

Based on the TF-QKD protocol proposed by Maeda, Sasaki and Koashi [19], Alice and Bob generate four different pulses with the signal state modulation and the testing state modulation respectively. In the signal state modulation, Alice and Bob randomly prepare the weak coherent pulse with amplitude $\sqrt{\mu}$ or $-\sqrt{\mu}$. In the testing state modulation, Alice and Bob randomly prepare the phase-randomized weak coherent pulse with intensities ν_1, ν_2 and 0 respectively. For every pair of pulses received from Alice and Bob, Charlie announces whether the phase difference is successfully detected. When the phase difference is detected, Charlie further announces whether it is in-phase when detector D_1 clicks or anti-phase when detector D_2 clicks. After receiving Charlie's measurement outcomes, Alice and Bob will apply phase information on the signal state to generate the sifted key. More precisely, Charlie's measurement outcomes can be divided into two cases. In the in-phase measurement outcome case, Alice and Bob will respectively generate the random bit a with the signal state preparation $|(-1)^a\sqrt{\mu}\rangle$. In the anti-phase measurement outcome case, Alice and Bob will respectively generate the random bit a with the signal state preparation $|(-1)^a\sqrt{\mu}\rangle$ and $|(-1)^{a\oplus 1}\sqrt{\mu}\rangle$ respectively.

By applying the entanglement based protocol, the signal state preparation in Alice's side can be illustrated with the following quantum state

$$\frac{|0\rangle_A|\sqrt{\mu}\rangle_{C_A} + |1\rangle_A|-\sqrt{\mu}\rangle_{C_A}}{\sqrt{2}}. \tag{6}$$

After preparing the quantum states $|\psi\rangle_{AC_A}$, Alice will measure the first quantum state, and the second quantum state will be transmitted to the quantum channel. And the signal state preparation in Bob's side can be illustrated with the following quantum state.

$$\frac{|0\rangle_B|\sqrt{\mu}\rangle_{C_B} - |1\rangle_B|-\sqrt{\mu}\rangle_{C_B}}{\sqrt{2}}. \tag{7}$$

After preparing the quantum states $|\varphi\rangle_{BC_B}$, Bob will measure the first quantum state, and the second quantum state will be transmitted to the quantum channel.

It should be pointed out that this analysis method has been given in Ref. [19]. Maeda, Sasaki and Koashi have proved that Alice and Bob's procedure in the signal mode can be equivalently executed by preparing the qubits AB and the optical pulses $C_A C_B$ in a joint quantum state $\frac{|0\rangle_A|\sqrt{\mu}\rangle_{C_A} + |1\rangle_A|-\sqrt{\mu}\rangle_{C_A}}{\sqrt{2}} \otimes \frac{|0\rangle_B|\sqrt{\mu}\rangle_{C_B} - |1\rangle_B|-\sqrt{\mu}\rangle_{C_B}}{\sqrt{2}}$. After preparing these quantum states, Alice and Bob will measure the first quantum state, and the second quantum state will be transmitted to Charlie. Thus the quantum state shared among Alice, Bob and Charlie can be given by

$$
\begin{aligned}
&\frac{|0\rangle_A|\sqrt{\mu}\rangle_{C_A} + |1\rangle_A|-\sqrt{\mu}\rangle_{C_A}}{\sqrt{2}} \otimes \frac{|0\rangle_B|\sqrt{\mu}\rangle_{C_B} - |1\rangle_B|-\sqrt{\mu}\rangle_{C_B}}{\sqrt{2}}\\
={}&\tfrac{1}{4}[(|0\rangle|0\rangle + |1\rangle|1\rangle)_{AB}(|\sqrt{\mu}\rangle|\sqrt{\mu}\rangle - |-\sqrt{\mu}\rangle|-\sqrt{\mu}\rangle)_{C_A,C_B}\\
&+ (|0\rangle|0\rangle - |1\rangle|1\rangle)_{AB}(|\sqrt{\mu}\rangle|\sqrt{\mu}\rangle + |-\sqrt{\mu}\rangle|-\sqrt{\mu}\rangle)_{C_A,C_B}\\
&+ (|0\rangle|1\rangle + |1\rangle|0\rangle)_{AB}(-|\sqrt{\mu}\rangle|-\sqrt{\mu}\rangle + |-\sqrt{\mu}\rangle|\sqrt{\mu}\rangle)_{C_A,C_B}\\
&+ (|0\rangle|1\rangle - |1\rangle|0\rangle)_{AB}(-|\sqrt{\mu}\rangle|-\sqrt{\mu}\rangle - |-\sqrt{\mu}\rangle|\sqrt{\mu}\rangle)_{C_A,C_B}].
\end{aligned} \tag{8}
$$

After measuring the received quantum states C_A and C_B with a 50 : 50 beam-splitter and a pair of photon detectors D_1 and D_2, Charlie announces whether the phase difference is successfully detected. Note that TF-QKD protocol is based on the first-order interference, while MDI-QKD is based on the second-order interference. Correspondingly, this quantum state will be transformed to

$$
\begin{aligned}
\frac{1}{4}[&(|0\rangle|0\rangle + |1\rangle|1\rangle)_{AB}(|\sqrt{2\mu}\rangle|0\rangle - |-\sqrt{2\mu}\rangle|0\rangle)_{D_1,D_2} + \\
&(|0\rangle|0\rangle - |1\rangle|1\rangle)_{AB}(|\sqrt{2\mu}\rangle|0\rangle + |-\sqrt{2\mu}\rangle|0\rangle)_{D_1,D_2} + \\
&(|0\rangle|1\rangle + |1\rangle|0\rangle)_{AB}(-|0\rangle|\sqrt{2\mu}\rangle + |0\rangle|-\sqrt{2\mu}\rangle)_{D_1,D_2} + \\
&(|0\rangle|1\rangle - |1\rangle|0\rangle)_{AB}(-|0\rangle|\sqrt{2\mu}\rangle - |0\rangle|-\sqrt{2\mu}\rangle)_{D_1,D_2}],
\end{aligned}
\tag{9}
$$

where the detection results that detector D_1 clicks and detector D_2 clicks respectively demonstrate the in-phase and anti-phase measurement outcomes in Charlie's side. Here, for the simplicity of the discussion, we assume that there are no channel losses. Correspondingly, the quantum states $(|\sqrt{2\mu}\rangle|0\rangle - |-\sqrt{2\mu}\rangle|0\rangle)_{D_1,D_2}$ and $(|\sqrt{2\mu}\rangle|0\rangle + |-\sqrt{2\mu}\rangle|0\rangle)_{D_1,D_2}$ demonstrate the in-phase measurement outcome, while quantum states $(-|0\rangle|\sqrt{2\mu}\rangle + |0\rangle|-\sqrt{2\mu}\rangle)_{D_1,D_2}$ and $(-|0\rangle|\sqrt{2\mu}\rangle - |0\rangle|-\sqrt{2\mu}\rangle)_{D_1,D_2}$ demonstrate the anti-phase measurement outcome. Note that TF-QKD protocol is a variant of the MDI-QKD protocol, thus the measurement outcomes can be assumed to be controlled by Eve. We can simply assume the click of detector D_1 demonstrates the Bell state $\frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)_{AB}$ preparation in Alice and Bob's side, while the click of detector D_2 demonstrates the Bell state $\frac{1}{\sqrt{2}}(|0\rangle|1\rangle + |1\rangle|0\rangle)_{AB}$ preparation in Alice and Bob's side. Since Charlie's measurement outcomes have no security requirement, this assumption is reasonable, and more detailed explanation has been given in Ref. [19].

By applying the time reversed entanglement technique, we can assume the Bell states $\frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)_{AB}$ and $\frac{1}{\sqrt{2}}(|0\rangle|1\rangle + |1\rangle|0\rangle)_{AB}$ is prepared in Charlie's side, then the two quantum states will be transmitted to Alice and Bob to perform Z basis or X basis measurement. Based on this analysis method, the in-phase measurement outcome demonstrates the Bell state preparation

$$
\frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)_{AB} = \frac{1}{\sqrt{2}}(|+\rangle|+\rangle + |-\rangle|-\rangle)_{AB}.
\tag{10}
$$

Suppose Alice and Bob apply Z basis measurement, Z basis error is defined to be an event where the pair is found in either state $|0\rangle|1\rangle_{AB}$ or $|1\rangle|0\rangle_{AB}$. Suppose Alice and Bob apply X basis measurement, X basis error is defined to be an event where the pair is found in either state $|+\rangle|-\rangle_{AB}$ or $|-\rangle|+\rangle_{AB}$.

Similarly, the anti-phase measurement outcome demonstrates the Bell state preparation

$$
\frac{1}{\sqrt{2}}(|0\rangle|1\rangle + |1\rangle|0\rangle)_{AB} = \frac{1}{\sqrt{2}}(|+\rangle|+\rangle - |-\rangle|-\rangle)_{AB}.
\tag{11}
$$

Suppose Alice and Bob apply Z basis measurement, Z basis error is defined to be an event where the pair was found in either state $|0\rangle|0\rangle_{AB}$ or $|1\rangle|1\rangle_{AB}$. Suppose Alice and Bob apply X basis measurement, X basis error is defined to be an event where the pair is found in either state $|+\rangle|-\rangle_{AB}$ or $|-\rangle|+\rangle_{AB}$.

In a practical TF-QKD experiment, the bit error rate in Z basis can be directly tested, but the bit error rate in X basis can't be directly observed. To analyze the bit error rate in X basis, the quantum state shared among Alice, Bob and Charlie can be rewritten as

$$
\begin{aligned}
&\frac{|0\rangle_A|\sqrt{\mu}\rangle_{C_A} + |1\rangle_A|-\sqrt{\mu}\rangle_{C_A}}{\sqrt{2}} \otimes \frac{|0\rangle_B|\sqrt{\mu}\rangle_{C_B} - |1\rangle_B|-\sqrt{\mu}\rangle_{C_B}}{\sqrt{2}} \\
= \ &(\sqrt{c_+}|+\rangle_A|\sqrt{\mu_{even}}\rangle_{C_A} + \sqrt{c_-}|-\rangle_A|\sqrt{\mu_{odd}}\rangle_{C_A}) \\
&\otimes (\sqrt{c_-}|+\rangle_B|\sqrt{\mu_{odd}}\rangle_{C_B} + \sqrt{c_+}|-\rangle_B|\sqrt{\mu_{even}}\rangle_{C_B}),
\end{aligned}
\tag{12}
$$

where $c_+ := e^{-\mu}\cosh\mu$, $c_- := e^{-\mu}\sinh\mu$, $|\sqrt{\mu_{even}}\rangle = (|\sqrt{\mu}\rangle + |-\sqrt{\mu}\rangle)/(2\sqrt{c_+})$ and $|\sqrt{\mu_{odd}}\rangle = (|\sqrt{\mu}\rangle - |-\sqrt{\mu}\rangle)/(2\sqrt{c_-})$. Based on this state preparation, the X basis error occurs with probability $p_{even} = c_+^2 + c_-^2 = e^{-2\mu}\cosh 2\mu$, and the optical pulses are sent in the following quantum state

$$
\begin{aligned}
p_{even}\rho^{even} = \quad & c_+^2|\sqrt{\mu_{even}}\sqrt{\mu_{even}}\rangle\langle\sqrt{\mu_{even}}\sqrt{\mu_{even}}|_{C_A C_B} \\
& + c_-^2|\sqrt{\mu_{odd}}\sqrt{\mu_{odd}}\rangle\langle\sqrt{\mu_{odd}}\sqrt{\mu_{odd}}|_{C_A C_B}.
\end{aligned}
\tag{13}
$$

To analyze the error rate in X basis, the counting rate with this non-classical optical state preparation can be analyzed with the operator dominance method [19], where the detection frequency of ρ^{even} can be estimated from a combination of phase-randomized weak coherent states with intensities ν_1, ν_2 and 0. Combining this analysis result with the operator dominance method given by [19], we can estimate the quantum channel parameters λ_i, $i = \{0, 1, 2, 3\}$ in the following section.

4 Security of TF-QKD with AD

By applying the previous analysis result with the signal state modulation in Alice and Bob's side, we need to analyze the error rate E_{uu}^{ZZ} in Z basis and the error rate E_{uu}^{XX} in X basis respectively. In a practical TF-QKD experiment, E_{uu}^{ZZ} can be directly calculated by testing part of the in-phase and anti-phase measurement outcomes. However, the non-classical optical state ρ^{even} is hard to realize in current technology, the bit error rate E_{uu}^{XX} can not be directly estimated in a practical TF-QKD system. Fortunately, Maeda, Sasaki and Koashi proposed the operator dominance method to estimate E_{uu}^{XX} [19], where the linear combination of the testing states can be applied to approximate the non-classical optical state ρ^{even}. To analyze the security of the entanglement based TF-QKD protocol with the information-theoretical analysis method, the relationship among E_{uu}^{ZZ}, E_{uu}^{XX} and λ_i can be given with the following equations,

$$
\begin{aligned}
\lambda_1 + \lambda_3 &= E_{uu}^{XX}, \\
\lambda_2 + \lambda_3 &= E_{uu}^{ZZ},
\end{aligned}
\tag{14}
$$

where $\lambda_0 + \lambda_1 + \lambda_2 + \lambda_3 = 1$. In the TF-QKD protocol, only the signal state can be used to generate the final secure key. Since the quantum channel parameters λ_i, $i = \{0, 1, 2, 3\}$ can be estimated with Eq. (14), Eq. (4) can be modified with the following inequality by applying the AD method

$$
\begin{aligned}
R_{TF} \geq & \max_b \frac{1}{b} q_{succ}^{ZZ} Q_{uu}^{ZZ} [S(A|E) - H(A|B)] \\
= & \max_b \frac{1}{b} q_{succ}^{ZZ} Q_{uu}^{ZZ} [(1 - (\tilde{\lambda}_0 + \tilde{\lambda}_1) H(\frac{\tilde{\lambda}_0}{\tilde{\lambda}_0 + \tilde{\lambda}_1}) \\
& - (\tilde{\lambda}_2 + \tilde{\lambda}_3) H(\frac{\tilde{\lambda}_2}{\tilde{\lambda}_2 + \tilde{\lambda}_3})) - f h(\tilde{E}_{uu}^{ZZ})],
\end{aligned}
\tag{15}
$$

where Q_{uu}^{ZZ} is the counting rate by considering Alice and Bob prepare the signal states, $\tilde{E}_{uu}^{ZZ} = \frac{E_{uu}^{ZZ^b}}{E_{uu}^{ZZ^b} + (1 - E_{uu}^{ZZ})^b}$ is the error rate after the AD protocol, $f > 1$ is the error correction efficiency, $q_{succ}^{ZZ} = E_{uu}^{ZZ^b} + (1 - E_{uu}^{ZZ})^b$ is the successful probability of the AD method in the practical TF-QKD system.

By applying the operator dominance method with asymptotic key length, the error rate in X basis $E_{\mu\mu}^{XX}$ can be given by [19]

$$
E_{\mu\mu}^{XX} = C_1(1 + \sqrt{(C_2 + C_4)C_3})^2,
\tag{16}
$$

where $C_1 = \frac{e^{-2\mu d}}{1-e^{-2\mu\eta}+e^{-2\mu\eta}d}$, $C_2 = \frac{e^{-2\nu_1(\nu_1-\nu_2)}}{\mu_2}$, $C_3 = \frac{1}{\nu_1 e^{-2\nu_1}}\sum_{k=1}^{\infty}\frac{\mu^{2k}(k+1)}{\nu_1^{2k-1}-\nu_2^{2k-1}}$, $C_4 = \frac{1}{d}(1-e^{-2\nu_1\eta}+e^{-2\nu_1\eta}d-\frac{\nu_1 e^{-2\nu_1}}{\nu_2 e^{-2\nu_2}}(1-e^{-2\nu_2\eta}+e^{-2\nu_2\eta}d))$, $max(\mu,\ \nu_2) < \nu_1$. Note that, we assume each detector has a dark count probability of p_d, which amounts to the effective probability $d = 2p_d - p_d{}^2$ from the two detectors. By considering the channel transmission efficiency, the overall transmissivity from Alice (Bob) to Charlie's detection is η.

Based on the simulation parameters given by [19], we calculate the secure key rate R_{TF} as a function of secure key rate transmission distance L between Alice and Bob with different loss-independent misalignment error. The loss-independent misalignment error is the probability that a photon hits the erroneous detector, which is independent of the transmission distance. In a practical experimental realization, the loss-independent misalignment error can be applied to characterize the alignment and stability of the optical system. We assume a fiber loss of 0.2 dB/km, a loss-independent misalignment error of $e_d = 0.03$, error correction efficiency $f = 1.1$, each detector has a detection efficiency $\eta_d = 0.3$ and dark count probability $p_d = 10^{-8}$. The overall transmissivity from Alice (Bob) to Charlie's detection is $\eta = \eta_d 10^{-0.01L}$. In the asymptotic limit, the counting rate of Alice and Bob's signal states Q_{uu}^{ZZ} can be given by

$$Q_{uu}^{ZZ} = 1 - e^{-2\mu\eta} + e^{-2\mu\eta}d, \tag{17}$$

Correspondingly, the error rate in Z basis $E_{\mu\mu}^{ZZ}$ can be given by

$$E_{\mu\mu}^{ZZ} = \frac{e_d(1-e^{-2\mu\eta})+\frac{e^{-2\mu\eta}d}{2}}{Q_{uu}^{ZZ}}. \tag{18}$$

Based on these simulation parameters and the optimal b values, we calculate the secure key rate R_{TF} as a function of transmission distance between Alice and Bob in Figure 1. Comparing with the previous analysis result given by [19], we find that both of the two analysis results can overcome the PLOB bound $-\log(1 - \eta_d 10^{-0.02L})$, but the maximal secure key transmission distance can be improved from 420 km to 470 km.

By increasing the loss-independent misalignment error to $e_d = 0.12$, we calculate the secure key rate in Figure 2. We find that our analysis result can overcome the PLOB bound and the maximal secure key transmission distance can be improved from 345 km to 443 km, but the previous analysis method can not overcome the PLOB bound at any transmission distance.

By increasing the loss-independent misalignment error to $e_d = 0.16$, we calculate the secure key rate in Figure 3. We find that our analysis result can still overcome the PLOB bound, and the maximal secure key transmission distance can be improved from 308 km to 428 km. From the calculation result, we find that the advantage distillation technology has a better effect on improving the secure key rate when the misalignment error rate is high.

By increasing the loss-independent misalignment error to $e_d = 0.48$, we calculate the secure key rate in Figure 4. More surprisingly, we find that our analysis method can still generate positive secure key, the reason for which is that $E_{\mu\mu}^{XX}$ has no correlation with e_d in the security analysis model. This is quite different from the BB84-QKD system or the original MDI-QKD system, where all of the error rate in different bases will be increased by increasing e_d. However, in a TF-QKD system, we can prove that the error rate $E_{\mu\mu}^{XX}$ will be unchanged. By applying the AD method with $b > 1$, the error rate $\tilde{E}_{uu}^{ZZ} = \frac{E_{uu}^{ZZ^b}}{E_{uu}^{ZZ^b}+(1-E_{uu}^{ZZ})^b}$ will be smaller than $E_{\mu\mu}^{ZZ}$ at the cost of increasing $\tilde{\lambda}_0$ and $\tilde{\lambda}_1$. Thus, if b is large enough, we can also generate positive secure key rate R_{TF} even if the error e_d is close to 0.5. From the calculation result, we find that the secure key rate is very low for high misalignment
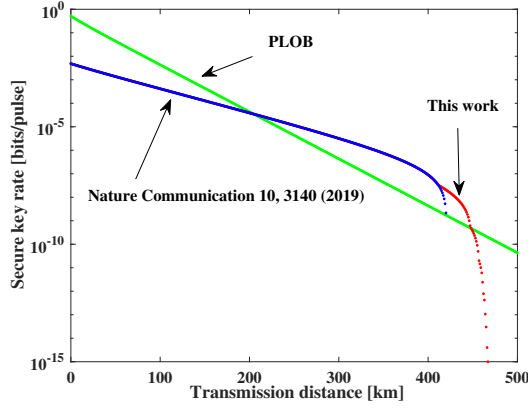
(a) The relationship between the transmission distance and the secure key rate, the blue line is the secure key rate given by [19], the red line is the secure key rate given by this work, and the green line is the PLOB bound.
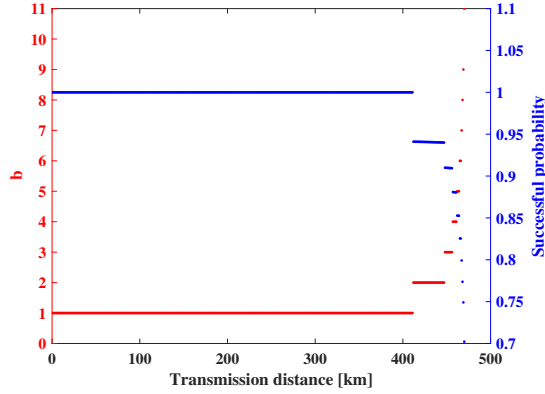
(b) The optimal b and success probability of advantage distillation with different transmission distances. From 0 km to 411 km, the optimal b value is 1 and the success probability of advantage distillation is 1, thus we do not need to utilize the AD method in these transmission distances.

Figure 1: Results of TF-QKD protocol with $e_d = 0.03$.

errors close to 50%. In this situation, the advantage distillation is very interesting from a theoretical point of view, but it is not feasible in practice.

5 Discussion

In a practical TF-QKD system, by combining the AD method with the information-theoretical security analysis method, we prove that both the maximal transmission distance and the secure key rate can be sharply improved. More surprisingly, the numerical simulation results demonstrate that TF-QKD can generate positive secure key even if the loss-independent misalignment error is close to 50%, thus our analysis method can significantly improve the performance of a practical TF-QKD system. In the future research, it will be interesting to experimentally realize the AD method in a practical TF-QKD system, especially with a high loss-independent misalignment error.
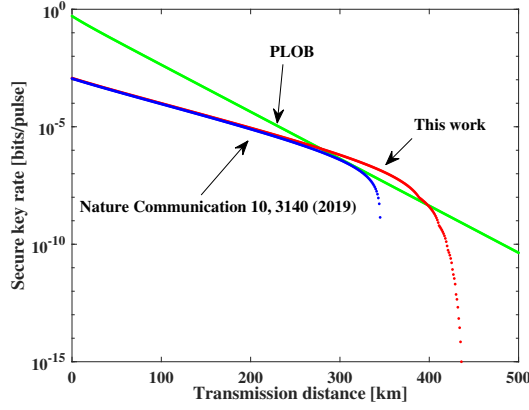
(a) The relationship between the transmission distance and the secure key rate, the blue line is the secret key rate given by [19], the red line is the secure key rate given by this work, and the green line is the PLOB bound.
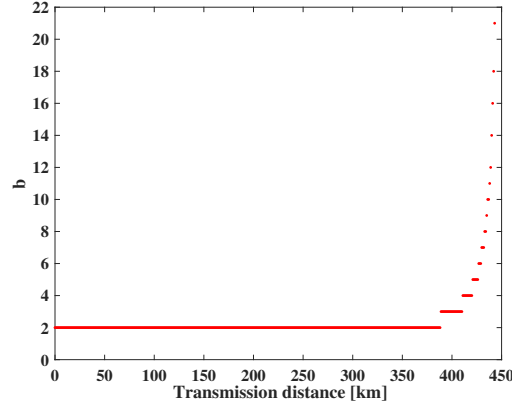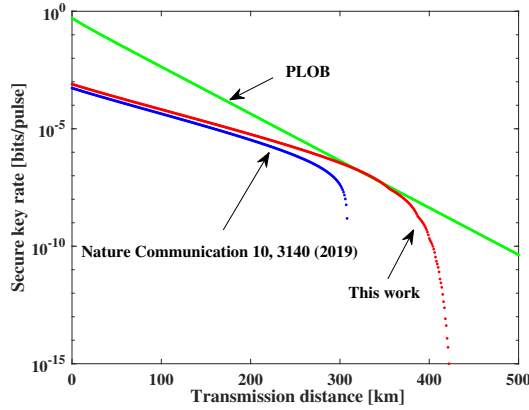

(b) The relationship between the transmission distance and the optimal b values. From 0 km to 388 km, the optimal b value is 2.

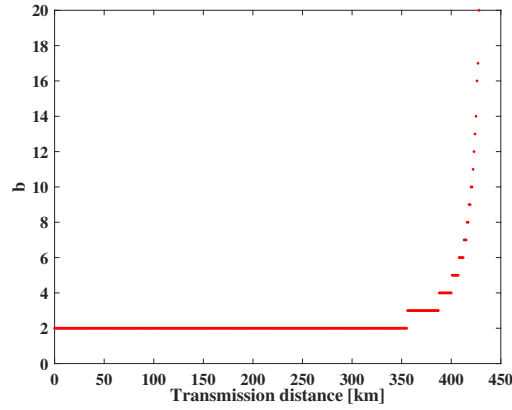Figure 2: Results of TF-QKD protocol with $e_d = 0.12$.

Since the AD method only modifies the classical post-processing step, the similar advantage distillation technology has been applied in the phase-matching quantum key distribution [44]. In the future research, it will be also interesting to analyze security of sending-not-sending TF QKD with advantage distillation technology [45–47]. More interestingly, based on the quantum asymptotic equipartition property [48], the leftover hash lemma [49] and the Chernoff bound [19, 50], the statistical fluctuation of the bit error rate and the secure key rate in finite-key length can be efficiently analyzed in the future research.

(a) The relationship between the transmission distance and the secure key rate, the blue line is the secret key rate given by [19], the red line is the secure key rate given by this work, and the green line is the PLOB bound.
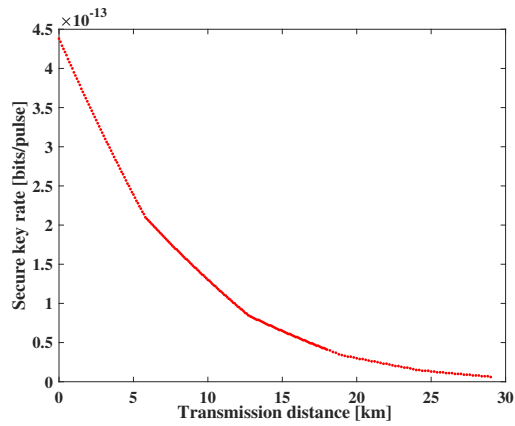

(b) The relationship between the transmission distance and the optimal b values. From 0 km to 355 km, the optimal b value is 2.
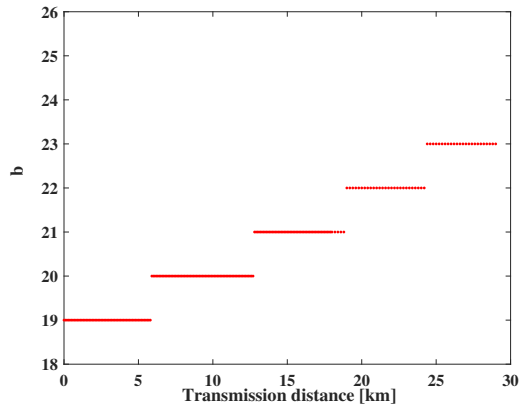
Figure 3: Results of TF-QKD protocol with $e_d = 0.16$.

References

[1] Charles H. Bennett and Gilles Brassard. "Quantum cryptography: Public key distribution and coin tossing". Theoretical Computer Science **560**, 7–11 (2014).

[2] Hoi-Kwong Lo and Hoi Fung Chau. "Unconditional security of quantum key distribution over arbitrarily long distances". Science **283**, 2050–2056 (1999).

[3] Peter W Shor and John Preskill. "Simple proof of security of the bb84 quantum key distribution protocol". Physical Review Letters **85**, 441 (2000).

[4] Renato Renner. "Security of quantum key distribution". International Journal of Quantum Information **6**, 1–127 (2008).

[5] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. "The security of practical quantum key distribution". Reviews of Modern Physics **81**, 1301 (2009).

[6] Hong-Wei Li, Shuang Wang, Jing-Zheng Huang, Wei Chen, Zhen-Qiang Yin, Fang-Yi Li, Zheng Zhou, Dong Liu, Yang Zhang, Guang-Can Guo, et al. "Attacking a

(a) The relationship between the transmission distance and the secure key rate.

(b) The relationship between the transmission distance and the optimal b values.

Figure 4: Results of TF-QKD protocol with $e_d = 0.48$.

practical quantum-key-distribution system with wavelength-dependent beam-splitter and multiwavelength sources". Physical Review A **84**, 062308 (2011).

[7] Lars Lydersen, Carlos Wiechers, Christoffer Wittmann, Dominique Elser, Johannes Skaar, and Vadim Makarov. "Hacking commercial quantum cryptography systems by tailored bright illumination". Nature Photonics **4**, 686–689 (2010).

[8] Hong-Wei Li, Zheng-Mao Xu, and Qing-Yu Cai. "Small imperfect randomness restricts security of quantum key distribution". Physical Review A **98**, 062325 (2018).

[9] Samuel L Braunstein and Stefano Pirandola. "Side-channel-free quantum key distribution". Physical Review Letters **108**, 130502 (2012).

[10] Hoi-Kwong Lo, Marcos Curty, and Bing Qi. "Measurement-device-independent quantum key distribution". Physical Review Letters **108**, 130503 (2012).

[11] Leong-Chuan Kwek, Lin Cao, Wei Luo, Yunxiang Wang, Shihai Sun, Xiangbin Wang, and Ai Qun Liu. "Chip-based quantum key distribution". AAPPS Bulletin**31** (2021).

[12] Stefano Pirandola, Riccardo Laurenza, Carlo Ottaviani, and Leonardo Banchi. "Fundamental limits of repeaterless quantum communications". Nature Communications **8**, 15043 (2017).

[13] Marco Lucamarini, Zhiliang L Yuan, James F Dynes, and Andrew J Shields. "Over-

coming the rate–distance limit of quantum key distribution without quantum repeaters". Nature **557**, 400–403 (2018).

[14] Xiongfeng Ma, Pei Zeng, and Hongyi Zhou. "Phase-matching quantum key distribution". Physical Review X **8**, 031043 (2018).

[15] Xiang-Bin Wang, Zong-Wen Yu, and Xiao-Long Hu. "Twin-field quantum key distribution with large misalignment error". Physical Review A **98**, 062323 (2018).

[16] Chaohan Cui, Zhen-Qiang Yin, Rong Wang, Wei Chen, Shuang Wang, Guang-Can Guo, and Zheng-Fu Han. "Twin-field quantum key distribution without phase postselection". Physical Review Applied **11**, 034053 (2019).

[17] Marcos Curty, Koji Azuma, and Hoi-Kwong Lo. "Simple security proof of twin-field type quantum key distribution protocol". npj Quantum Information **5**, 64 (2019).

[18] Jie Lin and Norbert Lütkenhaus. "Simple security analysis of phase-matching measurement-device-independent quantum key distribution". Physical Review A **98**, 042332 (2018).

[19] Kento Maeda, Toshihiko Sasaki, and Masato Koashi. "Repeaterless quantum key distribution with efficient finite-key analysis overcoming the rate-distance limit". Nature Communications **10**, 3140 (2019).

[20] Guillermo Currás-Lorenzo, Álvaro Navarrete, Koji Azuma, Go Kato, Marcos Curty, and Mohsen Razavi. "Tight finite-key security for twin-field quantum key distribution". npj Quantum Information **7**, 22 (2021).

[21] Guillermo Currás-Lorenzo, Lewis Wooltorton, and Mohsen Razavi. "Twin-field quantum key distribution with fully discrete phase randomization". Physical Review Applied **15**, 014016 (2021).

[22] M Minder, M Pittaluga, GL Roberts, M Lucamarini, JF Dynes, ZL Yuan, and AJ Shields. "Experimental quantum key distribution beyond the repeaterless secret key capacity". Nature Photonics **13**, 334–338 (2019).

[23] Xiaoqing Zhong, Jianyong Hu, Marcos Curty, Li Qian, and Hoi-Kwong Lo. "Proof-of-principle experimental demonstration of twin-field type quantum key distribution". Physical Review Letters **123**, 100506 (2019).

[24] Yang Liu, Zong-Wen Yu, Weijun Zhang, Jian-Yu Guan, Jiu-Peng Chen, Chi Zhang, Xiao-Long Hu, Hao Li, Cong Jiang, Jin Lin, et al. "Experimental twin-field quantum key distribution through sending or not sending". Physical Review Letters **123**, 100505 (2019).

[25] Shuang Wang, De-Yong He, Zhen-Qiang Yin, Feng-Yu Lu, Chao-Han Cui, Wei Chen, Zheng Zhou, Guang-Can Guo, and Zheng-Fu Han. "Beating the fundamental rate-distance limit in a proof-of-principle quantum key distribution system". Physical Review X **9**, 021046 (2019).

[26] Hui Liu, Cong Jiang, Hao-Tao Zhu, Mi Zou, Zong-Wen Yu, Xiao-Long Hu, Hai Xu, Shizhao Ma, Zhiyong Han, Jiu-Peng Chen, Yunqi Dai, Shi-Biao Tang, Weijun Zhang, Hao Li, Lixing You, Zhen Wang, Yong Hua, Hongkun Hu, Hongbo Zhang, Fei Zhou, Qiang Zhang, Xiang-Bin Wang, Teng-Yun Chen, and Jian-Wei Pan. "Field test of twin-field quantum key distribution through sending-or-not-sending over 428 km". Physical Review Letters **126**, 250502 (2021).

[27] Jiu-Peng Chen, Chi Zhang, Yang Liu, Cong Jiang, Wei-Jun Zhang, Zhi-Yong Han, Shi-Zhao Ma, Xiao-Long Hu, Yu-Huai Li, Hui Liu, Fei Zhou, Hai-Feng Jiang, Teng-Yun Chen, Hao Li, Li-Xing You, Zhen Wang, Xiang-Bin Wang, Qiang Zhang, and Jian-Wei Pan. "Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas". Nature Photonics **15**, 570–575 (2021).

[28] Shuang Wang, Zhen-Qiang Yin, De-Yong He, Wei Chen, Rui-Qiang Wang, Peng Ye, Yao Zhou, Guan-Jie Fan-Yuan, Fang-Xiang Wang, Yong-Gang Zhu, Pavel V Morozov, Alexander V Divochiy, Zheng Zhou, Guang-Can Guo, and Zheng-Fu Han. "Twin-field quantum key distribution over 830-km fibre". Nature Photonics **16**, 154–161 (2022).

[29] Hua-Lei Yin and Zeng-Bing Chen. "Coherent-state-based twin-field quantum key distribution". Scientific Reports **9**, 14918 (2019).

[30] Mario Mastriani and Sundaraja Sitharama Iyengar. "Satellite quantum repeaters for a quantum internet". Quantum Engineering **2**, e55 (2020).

[31] Xiao-Min Hu, Cen-Xiao Huang, Yu-Bo Sheng, Lan Zhou, Bi-Heng Liu, Yu Guo, Chao Zhang, Wen-Bo Xing, Yun-Feng Huang, Chuan-Feng Li, and Guang-Can Guo. "Long-distance entanglement purification for quantum communication". Physical Review Letters **126**, 010503 (2021).

[32] Gui-Lu Long, Dong Pan, Yu-Bo Sheng, Qikun Xue, Jianhua Lu, and Lajos Hanzo. "An evolutionary pathway for the quantum internet relying on secure classical repeaters". IEEE Network **36**, 82–88 (2022).

[33] Ueli M Maurer. "Secret key agreement by public discussion from common information". IEEE Transactions on Information Theory **39**, 733–742 (1993).

[34] Barbara Kraus, Cyril Branciard, and Renato Renner. "Security of quantum-key-distribution protocols using two-way classical communication or weak coherent pulses". Physical Review A **75**, 012316 (2007).

[35] Joonwoo Bae and Antonio Acín. "Key distillation from quantum channels using two-way communication protocols". Physical Review A **75**, 012334 (2007).

[36] Gláucia Murta, Filip Rozpędek, Jérémy Ribeiro, David Elkouss, and Stephanie Wehner. "Key rates for quantum key distribution protocols with asymmetric noise". Physical Review A **101**, 062321 (2020).

[37] Ernest Y.-Z. Tan, Charles C.-W. Lim, and Renato Renner. "Advantage distillation for device-independent quantum key distribution". Physical Review Letters **124**, 020502 (2020).

[38] Dagmar Bruß. "Optimal eavesdropping in quantum cryptography with six states". Physical Review Letters **81**, 3018 (1998).

[39] Won-Young Hwang. "Quantum key distribution with high loss: toward global secure communication". Physical Review Letters **91**, 057901 (2003).

[40] Xiang-Bin Wang. "Beating the photon-number-splitting attack in practical quantum cryptography". Physical Review Letters **94**, 230503 (2005).

[41] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. "Decoy state quantum key distribution". Physical Review Letters **94**, 230504 (2005).

[42] Hong-Wei Li, Chun-Mei Zhang, Mu-Sheng Jiang, and Qing-Yu Cai. "Improving the performance of practical decoy-state quantum key distribution with advantage distillation technology". Communications Physics **5**, 53 (2022).

[43] Daniel Gottesman and Hoi-Kwong Lo. "Proof of security of quantum key distribution with two-way classical communications". IEEE Transactions on Information Theory **49**, 457–475 (2003).

[44] Rui-Qiang Wang, Chun-Mei Zhang, Zhen-Qiang Yin, Hong-Wei Li, Shuang Wang, Wei Chen, Guang-Can Guo, and Zheng-Fu Han. "Phase-matching quantum key distribution with advantage distillation". New Journal of Physics **24**, 073049 (2022).

[45] Zong-Wen Yu, Xiao-Long Hu, Cong Jiang, Hai Xu, and Xiang-Bin Wang. "Sending-or-not-sending twin-field quantum key distribution in practice". Scientific Reports **9**, 3080 (2019).

[46] Hai Xu, Zong-Wen Yu, Cong Jiang, Xiao-Long Hu, and Xiang-Bin Wang. "Sending-or-not-sending twin-field quantum key distribution: Breaking the direct transmission key rate". Physical Review A **101**, 042330 (2020).

[47] Xiao-Long Hu, Cong Jiang, Zong-Wen Yu, and Xiang-Bin Wang. "Sending-or-not-sending twin-field protocol for quantum key distribution with asymmetric source parameters". Physical Review A **100**, 062337 (2019).

[48] Marco Tomamichel. "A framework for non-asymptotic quantum information theory". Doctoral thesis. ETH Zürich. Zürich (2012).

[49] Jaikumar Radhakrishnan and Amnon Ta-Shma. "Bounds for dispersers, extractors, and depth-two superconcentrators". SIAM Journal on Discrete Mathematics **13**, 2–24 (2000).

[50] Wassily Hoeffding. "Probability inequalities for sums of bounded random variables". Journal of the American Statistical Association **58**, 13–30 (1963).