Side-Channel-Secure Quantum Key Distribution with Imperfect Vacuum Sources

Cong Jiang,[1,2] Zong-Wen Yu,[3] Xiao-Long Hu,[4] and Xiang-Bin Wang[1,2,5,6,7,*]

[1] *Jinan Institute of Quantum Technology, Jinan, Shandong 250101, People's Republic of China*

[2] *State Key Laboratory of Low Dimensional Quantum Physics, Department of Physics, Tsinghua University, Beijing 100084, People's Republic of China*

[3] *Data Communication Science and Technology Research Institute, Beijing 100191, People's Republic of China*

[4] *School of Physics, State Key Laboratory of Optoelectronic Materials and Technologies, Sun Yat-sen University, Guangzhou 510275, People's Republic of China*

[5] *Frontier Science Center for Quantum Information, Beijing, People's Republic of China*

[6] *Shanghai Branch, CAS Center for Excellence and Synergetic Innovation Center in Quantum Information and Quantum Physics, University of Science and Technology of China, Shanghai 201315, People's Republic of China*

[7] *Shenzhen Institute for Quantum Science and Engineering, and Physics Department, Southern University of Science and Technology, Shenzhen 518055, People's Republic of China*

(Received 17 May 2022; revised 13 December 2022; accepted 28 April 2023; published 1 June 2023)

The side-channel-secure (SCS) quantum key distribution (QKD), SCS QKD has attracted much attention due to its higher security compared to the measurement-device-independent protocols. It is not only measurement-device-independent secure, but also secure against source-state side channels provided that Eve has no access to Alice's or Bob's setups inside their labs. In the original protocol for SCS QKD, the side channels and the intensities of the coherent sources are allowed to be different in different time windows, but the vacuum sources of Alice and Bob have to be perfect, which is impossible in practice due to the finite extinction ratio of the intensity modulators. In this paper, we present a method that does not need the perfect vacuum source requested by the original protocol and assures the result as secure as the original protocol. With the upper bounds of the amplitudes of the nonvacuum part of the sources, the secure key rate of our SCS QKD protocol here with imperfect vacuum and unstable sources can be calculated. The numerical results show that, the secure distance of the SCS QKD protocol exceeds 150 km, provided that the intensity of the imperfect vacuum source is less than 10^{-8}, which can be achieved in the experiment by a two-stage intensity modulator, where we also show that the active odd-parity pairing method and standard pairing method using two-way classical communication can be applied to the SCS QKD protocol to improve the key rate. Given the side-channel security based on the existing technological level, this work makes it possible to realize side-channel-secure QKD with real devices.

DOI: 10.1103/PhysRevApplied.19.064003

I. INTRODUCTION

Quantum key distribution (QKD) can provide information-theoretical secure symmetric keys between two remote parties [1–5]. Since the BB84 protocol was proposed in 1984 [1], much progress has been made in eliminating the actual security threat with imperfect QKD devices [6–10]. In particular, the decoy-state method [11–13] can beat the possible photon-number-splitting attack to an imperfect single-photon source; the measurement-device-independent (MDI) QKD [14,15] and its practical optimization protocol [16], the twin-field (TF) QKD [17], which breaks the linear bound (PLOB bound) of secure key rate [18], and its variants [19–25] are immune to all attacks to measurement devices.

However, in the source side, there could be side channels, which might leak extra information to Eve, such as basis-dependent source flaws [3,26]. Aiming for security with side channel, the side-channel-secure (SCS) QKD, SCS QKD was studied recently. In the original SCS QKD protocol [26], there are only two source states: the vacuum state and the coherent state in Alice's (Bob's) side, and Alice (Bob) encodes the bit 0 and bit 1 (bit 1 and bit 0) into the choice of not sending, i.e., the vacuum state, and sending, i.e., the coherent state. Using the fact that there is no side channel in the vacuum state, the original SCS QKD protocol is proved to be secure against the source-state side channels, provided that Eve has no access to Alice's or Bob's setups inside their labs. And by introducing a third party as a measurement station, it is also immune to all attacks to the detectors [14,15]. Its secure distance can exceed 200 km even with 20%

*Corresponding author: xbwang@mail.tsinghua.edu.cn

misalignment error [26]. Recently, the SCS QKD protocol was experimentally demonstrated in 50-km fibers [27], which shows the potential of the SCS QKD protocol in practical applications.

In the original SCS QKD protocol [26], if Alice (Bob) decides not sending, a perfect vacuum pulse is assumed to send out to the measurement station. But due to the finite extinction ratio of the intensity modulators, the perfect vacuum pulse is impossible in practice. Although the recent experiment [27] has verified the most impressive advantage of the promised long distance by the SCS QKD protocol [26], the major problem in the original SCS QKD protocol requesting perfect vacuum source is still open. In this paper, we present a method that does not need the perfect vacuum source assumption and assures the result as secure as the original SCS QKD protocol, i.e., it is not only MDI secure, but also secure against to source state side-channels provided that Eve has no access to Alice's or Bob's setups inside their labs.

The paper is arranged as follows. We first introduce the procedure of the SCS QKD protocol with imperfect vacuum sources in Sec. II A. We then show how to estimate the phase-flip error rate of a certain time window in Sec. II B. With the conclusion in Sec. II B, we further generalize the estimation method of the phase-flip error rate to the whole protocol and get the key rate formula. The numerical simulation results are shown in Sec. III. The paper ends with some conclusion remarks.

II. METHODS

A. The protocol

For the time window i, Alice (Bob) randomly chooses the weak source, i.e., the imperfect vacuum source o_A (o_B), or the strong source x_A (x_B) with probabilities p_0 and $p_x = 1 - p_0$, respectively. If the weak source o_A (o_B) is chosen, a WCS pulse with intensity ν_A^i (ν_B^i) is prepared, and Alice (Bob) takes it as bit 0 (1). If the strong source x_A (x_B) is chosen, a WCS pulse with intensity μ_A^i (μ_B^i) is prepared, and Alice (Bob) takes it as bit 1 (0). Alice and Bob send the prepared pulses to a untrusted third party, Charlie, who is assumed to first compensate the phase difference of the received pulse pair and then perform the interference measurement. The model of Charlie's measurement equipment is shown in Fig. 1. Charlie would publicly announce the measurement results to Alice and Bob. If only one detector clicks, Alice and Bob would take the i-th window as an effective window, and this event is also called an effective event whose corresponding bit is called an effective bit.

After Alice and Bob repeat the above process for N times and Charlie announces all the measurement results, *they* perform the data post-processing. For each time window, Alice randomly decides whether it is a test window, which is used for decoy analysis with probability r, or a key generation window, which is used for the final key distillation with probability $1 - r$. For the effective test windows, Alice and Bob publicly announce the sources they use in each time window. For the effective key generation windows, the corresponding bits are used to distil the final keys.

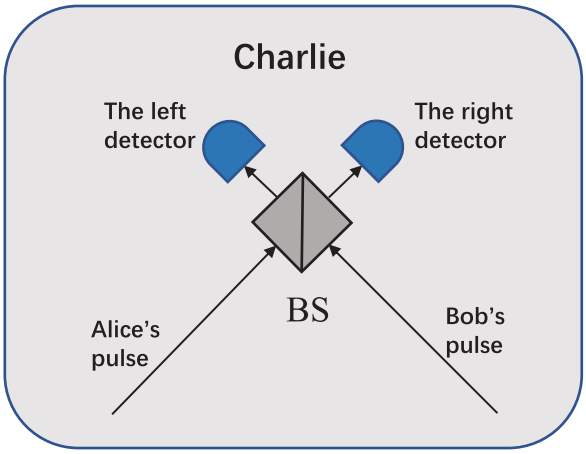

FIG. 1. Model of Charlie's measurement equipment. BS, the 50:50 beam splitter.

For a time window, if only one of Alice and Bob decides to send out a pulse from strong sources, it is a $\tilde{Z}$ window. For a time window, if both Alice and Bob decide to send out a pulse from strong sources (weak sources), it is a $\mathcal{B}$ ($\mathcal{O}$) window.

The corresponding effective bits of the effective events of $\tilde{Z}$ key generation windows are untagged bits. The $\tilde{Z}$ key generation window means it is a $\tilde{Z}$ window and chosen for key generation. Through decoy-state analysis, we can get the upper bound of the phase-flip error rate of those untagged bits, $\overline{e}^{\mathrm{ph}}$. The key rate formula is

$$R = \frac{1}{N}\{n_u[1 - H(\overline{e}^{\mathrm{ph}})] - f n_t H(E_K)\}, \tag{1}$$

where $H(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is the entropy function; n_u is the number of untagged bits; n_t is the number of corresponding bits of effective key generation windows; f is the correction efficiency factor; E_K is the bit-flip error rate of the effective bits from the key generation windows.

To calculate the secure key rate, we need to know the relationship between $n_u, \overline{e}^{\mathrm{ph}}$ and the observed values. With the methods presented in the following, we result in Eqs. (18)–(22).

B. The phase-flip error rate of a certain time window

We first consider the phase-flip error rate of a certain time window. For simplicity, we omit the superscript i of $\nu_A^i, \nu_B^i, \mu_A^i, \mu_B^i$ and all other physical quantities and states appeared in this section.

In a real experiment, instead of simply living in the operational space (Fock space), the sent out pulses actually live in the whole space including all side-channel spaces such as the frequency, the polarization, the spatial angular momentum, and so on. Yet the vacuum state has no side-channel space and therefore we need only to consider the side-channel space for the nonvacuum parts. The states can be decomposed in two parts, vacuum and nonvacuum. Explicitly, if Alice (Bob) chooses the weak source, she (he) actually prepares the state:

$$|\alpha_A^0\rangle = e^{-\nu_A/2}|0\rangle + \sqrt{1-e^{-\nu_A}}|\psi_A\rangle,$$
$$|\alpha_B^0\rangle = e^{-\nu_B/2}|0\rangle + \sqrt{1-e^{-\nu_B}}|\psi_B\rangle. \quad (2)$$

If Alice (Bob) chooses the strong source, she (he) actually prepares the state:

$$|\alpha_A\rangle = e^{-\mu_A/2}|0\rangle + \sqrt{1-e^{-\mu_A}}|\phi_A\rangle,$$
$$|\alpha_B\rangle = e^{-\mu_B/2}|0\rangle + \sqrt{1-e^{-\mu_B}}|\phi_B\rangle. \quad (3)$$

Here $|0\rangle$ is the vacuum state and $|\psi_A\rangle, |\psi_B\rangle, |\phi_A\rangle, |\phi_B\rangle$ are the corresponding nonvacuum parts of each states. Obviously, we have

$$\langle 0|\psi_A\rangle = \langle 0|\psi_B\rangle = \langle 0|\phi_A\rangle = \langle 0|\phi_B\rangle = 0, \quad (4)$$

which would be used in the calculation of phase-flip error rate.

As shown, our protocol does not request any specific photon-number distribution of its sources, it needs only a linear superposition of vacuum and nonvacuum for the source state in whole space.

In this certain time window, if only one of Alice and Bob chooses the strong source, it is a $\tilde{Z}$ window. To prove the security, we consider the virtual protocol where Alice and Bob preshare

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|\alpha_A^0, \alpha_B\rangle \otimes |01\rangle_{\mathcal{I}} + |\alpha_A, \alpha_B^0\rangle \otimes |10\rangle_{\mathcal{I}}). \quad (5)$$

Also, we have

$$|\Psi\rangle = \frac{1}{2}(\mathcal{N}_+|\chi^+\rangle \otimes |\Phi^0\rangle_{\mathcal{I}} + \mathcal{N}_-|\chi^-\rangle \otimes |\Phi^1\rangle_{\mathcal{I}}), \quad (6)$$

where

$$|\Phi^0\rangle_{\mathcal{I}} = \frac{1}{\sqrt{2}}(|01\rangle_{\mathcal{I}} + |10\rangle_{\mathcal{I}}),$$
$$|\Phi^1\rangle_{\mathcal{I}} = \frac{1}{\sqrt{2}}(|01\rangle_{\mathcal{I}} - |10\rangle_{\mathcal{I}}), \quad (7)$$

and

$$|\chi^+\rangle = \frac{1}{\mathcal{N}_+}(|\alpha_A^0, \alpha_B\rangle + |\alpha_A, \alpha_B^0\rangle),$$
$$|\chi^-\rangle = \frac{1}{\mathcal{N}_-}(|\alpha_A^0, \alpha_B\rangle - |\alpha_A, \alpha_B^0\rangle), \quad (8)$$

where $\mathcal{N}_+$ and $\mathcal{N}_-$ are normalization coefficients.

Here $|01\rangle_{\mathcal{I}}$ and $|10\rangle_{\mathcal{I}}$ are local states that are stored in Alice's and Bob's labs. If Alice and Bob decide to measure their local states in Z basis, i.e., $\{|01\rangle_{\mathcal{I}}, |10\rangle_{\mathcal{I}}\}$ before *they* send out the pulse pair, it is equivalent to a protocol where Alice and Bob randomly send out a pulse pair in state $|\alpha_A^0, \alpha_B\rangle$ or $|\alpha_A, \alpha_B^0\rangle$ with 50% probability. If Alice and Bob decide to measure their local states in X basis, i.e., $\{|\Phi^0\rangle_{\mathcal{I}}, |\Phi^1\rangle_{\mathcal{I}}\}$ before *they* send out the pulse pair, it is equivalent to a protocol where Alice and Bob randomly send out a pulse pair in state $|\chi^+\rangle$ or $|\chi^-\rangle$ with probabilities $\mathcal{N}_+^2/4$ and $\mathcal{N}_-^2/4$, respectively.

In this protocol, a phase error occurs in either of the following two kinds of effective windows: (1) the effective window while Alice and Bob send out a pulse pair in state $|\chi^+\rangle$, i.e., the measurement result of *their* local state is $|\Phi^0\rangle_{\mathcal{I}}$, and Charlie announces the right detector clicking; (2) the effective window while Alice and Bob send out a pulse pair in state $|\chi^-\rangle$, i.e., the measurement result of *their* local state is $|\Phi^1\rangle_{\mathcal{I}}$, and Charlie announces the left detector clicking.

We denote S_ζ^d as the probability that Charlie announces an effective event with detector d clicking in a time window when *they* have sent out state from source ζ. Here $d \in \{L, R\}$ and $\zeta \in \{\mathcal{O}, \mathcal{B}, \tilde{Z}\}$; L represents the left detector and R represents the right detector. We denote $S_{X_+}^d$ ($S_{X_-}^d$) as the probability that Charlie announces an effective event with detector d clicking in a time window when *they* have sent out state $|\chi^+\rangle$ ($|\chi^-\rangle$).

With all those definitions, we can express the probability that Alice and Bob detect a phase error in the $\tilde{Z}$ window, T_X, as the following form:

$$T_X = \frac{\mathcal{N}_+^2}{4}S_{X_+}^R + \frac{\mathcal{N}_-^2}{4}S_{X_-}^L = \frac{\mathcal{N}_+^2}{4}(S_{X_+}^R - S_{X_+}^L) + S_{\tilde{Z}}^L. \quad (9)$$

Here we use the fact that density matrices of the sent out pulse pairs are the same when Alice and Bob measure their local states in X basis and Z basis, and thus $\mathcal{N}_+^2/4S_{X_+}^L + \mathcal{N}_-^2/4S_{X_-}^L = S_{\tilde{Z}}^L$.

We also have the phase-flip error rate in the $\tilde{Z}$ window

$$e^{\mathrm{ph}} = \frac{T_X}{S_{\tilde{Z}}} = \frac{\frac{\mathcal{N}_+^2}{4}(S_{X_+}^R - S_{X_+}^L) + S_{\tilde{Z}}^L}{S_{\tilde{Z}}}, \quad (10)$$

where $S_{\tilde{Z}} = S_{\tilde{Z}}^L + S_{\tilde{Z}}^R$.

As shown in Appendix A, we have the upper bound of $S^R_{X_+}$ and the lower bound of $S^L_{X_-}$

$$S^R_{X_+} \le \frac{1}{\mathcal{N}_+^2}\left(c_0^2 S^R_{\mathcal{O}} + c_1^2 S^R_{\mathcal{B}} + c_2^2 + 2c_0c_1\sqrt{S^R_{\mathcal{O}}S^R_{\mathcal{B}}} + 2c_0c_2\sqrt{S^R_{\mathcal{O}}} + 2c_1c_2\sqrt{S^R_{\mathcal{B}}}\right), \tag{11}$$

$$S^L_{X_+} \ge \frac{1}{\mathcal{N}_+^2}\left(c_0^2 S^L_{\mathcal{O}} + c_1^2 S^L_{\mathcal{B}} - 2c_0c_1\sqrt{S^L_{\mathcal{O}}S^L_{\mathcal{B}}} - 2c_0c_2\sqrt{S^L_{\mathcal{O}}} - 2c_1c_2\sqrt{S^L_{\mathcal{B}}}\right), \tag{12}$$

where c_0, c_1, c_2 are real positive values, $c_0c_1 = 1$ and

$$c_2^2 \le \left(c_0 + c_1 - 2e^{-\nu_A/2-\mu_A/2} + 2\sqrt{1-e^{-\nu_A}}\sqrt{1-e^{-\mu_A}}\right) \times \left(c_0 + c_1 - 2e^{-\nu_B/2-\mu_B/2} + 2\sqrt{1-e^{-\nu_B}}\sqrt{1-e^{-\mu_B}}\right). \tag{13}$$

With the above formulas, we can get the upper bound of T_X.

C. The phase-flip error rate in the whole protocol

In Sec. II B, we get the phase-error rate of a certain $\tilde{Z}$ window. But in practice, the sources are usually unstable in the whole spaces, which means the intensities of the sources and the actual states in different time windows might be different. Thus we cannot directly take Eq. (10) as the formula of the upper bound of the phase-flip error rate in the whole protocol. However, Eq. (10) holds for any certain $\tilde{Z}$ window, provided that we replace all values including the intensities μ, the probabilities S^d_ζ, and T_X, c_0, c_1, c_2 by the corresponding values in this certain $\tilde{Z}$ window.

Recall that T^i_X is the probability that a phase error occurs if the i-th window is a $\tilde{Z}$ window, we have

$$n^{\mathrm{ph}} = \sum_{i=1}^{N} 2p_0p_x(1-r)T^i_X, \tag{14}$$

where n^{ph} is the number of phase errors in the $\tilde{Z}$ key generation windows of the whole protocol.

Equations (11)–(13) always hold provided that $c_0^ic_1^i = 1$. Thus we take the same value of c_0^i and c_1^i for all time windows and denote by c_0, c_1, respectively. The valve of c_2^i is upper bounded by Eq. (13). Furthermore, we have

$$(c_2^i)^2 \le \bar{c}_2^2 = \left(c_0 + c_1 - 2e^{-\nu_A^U/2-\mu_A^U/2} + 2\sqrt{1-e^{-\nu_A^U}}\sqrt{1-e^{-\mu_A^U}}\right) \times \left(c_0 + c_1 - 2e^{-\nu_B^U/2-\mu_B^U/2} + 2\sqrt{1-e^{-\nu_B^U}}\sqrt{1-e^{-\mu_B^U}}\right), \tag{15}$$

where $\nu_A^U, \mu_A^U, \nu_B^U, \mu_B^U$ are the upper bounds of $\nu_A^i, \mu_A^i, \nu_B^i, \mu_B^i$, respectively, and we assume those bounds are known values in the protocol. $\bar{c}_2$ is the upper bound of c_2^i for all time windows. We have

$$\begin{aligned} n^{\mathrm{ph}} &= \sum_{i=1}^{N} 2p_0p_x(1-r)T^i_X \\ &\le \sum_{i=1}^{N} \frac{1}{2}p_0p_x(1-r)\left[c_0^2(S^{i,R}_{\mathcal{O}} - S^{i,L}_{\mathcal{O}}) + c_1^2(S^{i,R}_{\mathcal{B}} - S^{i,L}_{\mathcal{B}}) + \bar{c}_2^2 + 2c_0c_1\left(\sqrt{S^{i,R}_{\mathcal{O}}S^{i,R}_{\mathcal{B}}} + \sqrt{S^{i,L}_{\mathcal{O}}S^{i,L}_{\mathcal{B}}}\right)\right. \\ &\quad \left. + 2c_0\bar{c}_2\left(\sqrt{S^{i,R}_{\mathcal{O}}} + \sqrt{S^{i,L}_{\mathcal{O}}}\right) + 2c_1\bar{c}_2\left(\sqrt{S^{i,R}_{\mathcal{B}}} + \sqrt{S^{i,L}_{\mathcal{B}}}\right)\right] + \sum_{i=1}^{N} 2p_0p_x(1-r)S^{i,L}_{\tilde{Z}} \\ &\le \frac{1}{2}p_0p_x(1-r)\left[c_0^2\sum_{i=1}^{N}(S^{i,R}_{\mathcal{O}} - S^{i,L}_{\mathcal{O}}) + c_1^2\sum_{i=1}^{N}(S^{i,R}_{\mathcal{B}} - S^{i,L}_{\mathcal{B}}) + \bar{c}_2^2 + 2c_0c_1\left(\sqrt{\sum_{i=1}^{N}S^{i,R}_{\mathcal{O}}\sum_{i=1}^{N}S^{i,R}_{\mathcal{B}}} + \sqrt{\sum_{i=1}^{N}S^{i,L}_{\mathcal{O}}\sum_{i=1}^{N}S^{i,L}_{\mathcal{B}}}\right)\right. \\ &\quad \left. + 2c_0\bar{c}_2\left(\sqrt{N\sum_{i=1}^{N}S^{i,R}_{\mathcal{O}}} + \sqrt{N\sum_{i=1}^{N}S^{i,L}_{\mathcal{O}}}\right) + 2c_1\bar{c}_2\left(\sqrt{N\sum_{i=1}^{N}S^{i,R}_{\mathcal{B}}} + \sqrt{N\sum_{i=1}^{N}S^{i,L}_{\mathcal{B}}}\right)\right] + \sum_{i=1}^{N} 2p_0p_x(1-r)S^{i,L}_{\tilde{Z}}. \end{aligned} \tag{16}$$

Here we use the Cauchy inequality in the second inequality

$$\left(\sum_{i=1}^{N} a_i b_i\right)^2 \leq \sum_{i=1}^{N} a_i^2 \sum_{i=1}^{N} b_i^2 \quad a_i, b_i \in \mathbb{R}. \tag{17}$$

Denote n_ζ^d as the number of observed effective events caused by the detector d in the ζ-test-windows (those ζ windows chosen for test) where $d \in \{L, R\}$ and $\zeta \in \{\mathcal{O}, \mathcal{B}, \tilde{Z}\}$. We have

$$\begin{aligned} n_{\mathcal{O}}^d &= \sum_{i=1}^{N} p_0^2 r S_{\mathcal{O}}^{i,d}, \quad n_{\mathcal{B}}^d = \sum_{i=1}^{N} p_x^2 r S_{\mathcal{B}}^{i,d}, \quad n_{\tilde{Z}}^d \\ &= \sum_{i=1}^{N} 2 p_0 p_x r S_{\tilde{Z}}^{i,d}. \end{aligned} \tag{18}$$

We define

$$S_{\mathcal{O},A}^d = \frac{n_{\mathcal{O}}^d}{N p_0^2 r}, \quad S_{\mathcal{B},A}^d = \frac{n_{\mathcal{B}}^d}{N p_x^2 r}, \quad S_{\tilde{Z},A}^d = \frac{n_{\tilde{Z}}^d}{2 N p_0 p_x r}. \tag{19}$$

With those observed values, we have

$$\begin{aligned} n^{\mathrm{ph}} \leq \overline{n}^{\mathrm{ph}} = \frac{1}{2} p_0 p_x (1-r) N \Big[& c_0^2 (S_{\mathcal{O},A}^R - S_{\mathcal{O},A}^L) + c_1^2 (S_{\mathcal{B},A}^R - S_{\mathcal{B},A}^L) + \overline{c}_2^2 + 2 c_0 c_1 \left(\sqrt{S_{\mathcal{O},A}^R S_{\mathcal{B},A}^R} + \sqrt{S_{\mathcal{O},A}^L S_{\mathcal{B},A}^L} \right) \\ & + 2 c_0 \overline{c}_2 \left(\sqrt{S_{\mathcal{O},A}^R} + \sqrt{S_{\mathcal{O},A}^L} \right) + 2 c_1 \overline{c}_2 \left(\sqrt{S_{\mathcal{B},A}^R} + \sqrt{S_{\mathcal{B},A}^L} \right) + 4 S_{\tilde{Z},A}^L \Big]. \end{aligned} \tag{20}$$

And the number of untagged bits n_u satisfies

$$\begin{aligned} n_u &= \sum_{i=1}^{N} 2 p_0 p_x (1-r) (S_{\tilde{Z}}^{i,L} + S_{\tilde{Z}}^{i,R}) \\ &= 2 p_0 p_x (1-r) N (S_{\tilde{Z},A}^L + S_{\tilde{Z},A}^R). \end{aligned} \tag{21}$$

Then, we get the upper bound of the phase-flip error rate of the untagged bits in the key generation windows

$$\overline{e}^{\mathrm{ph}} = \frac{\overline{n}^{\mathrm{ph}}}{n_u}. \tag{22}$$

With Eqs. (18)–(22), we can calculate the key rate by Eq. (1).

Remark: Although we use the model of WCS sources in the calculation above, it is quite obvious that our method here can apply to any type of source since we can always express the states of any sources into the linear superposition of the vacuum part and the nonvacuum part:

$$|\mathcal{A}\rangle = \sqrt{a_0}|0\rangle + \sqrt{1-a_0}|\mathrm{nonvacuum}\rangle, \tag{23}$$

where a_0 is the probability of the vacuum part of the state and $|\mathrm{nonvacuum}\rangle$ is a whole-space nonvacuum state. As shown in Eq. (15), our method depends only on $e^{-\nu_A^U}, e^{-\nu_B^U}, e^{-\mu_A^U}, e^{-\mu_B^U}$, i.e., the lower bounds of the probabilities of vacuum state, thus Eq. (15) holds for any sources provided that we replace those lower bounds by the corresponding lower bound of a_0. We can get the lower bound of a_0 by partially characterizing states in Fock space. Specially, for the WCS sources, we can get the lower bound of a_0 by measuring the upper bound of the intensities ν or μ.

III. RESULTS AND DISCUSSION

We consider the symmetry case here. In the symmetry case, the distance from Alice to Charlie is the same as the distance from Bob to Charlie. And Charlie's two detectors are assumed to have the same properties such as the dark counting rate and the detection efficiency. Without loss of generality, we assume the source parameters of Alice and Bob are the same, i.e., $\nu_A^U = \nu_B^U = \nu$ and $\mu_A^U = \mu_B^U = \mu$. In the calculation of key rate, c_0, c_1 can be taken as any positive real values provided that $c_0 c_1 = 1$, and we can optimize c_0, c_1 to achieve the highest key rate. For simplicity, we set $c_0 = e^{\nu/2-\mu/2}, c_1 = e^{\mu/2-\nu/2}$. The experiment

TABLE I. List of experimental parameters used in numerical simulations. Here p_d is the dark counting rate per pulse of Charlie's detectors; η_d is the detection efficiency of Charlie's detectors; E_d is the misalignment error; f is the error correction inefficiency; α_f is the fiber loss coefficient (dB/km).

p_d	E_d	η_d	f	α_f
1.0×10^{-9}	4%	60.0%	1.1	0.2

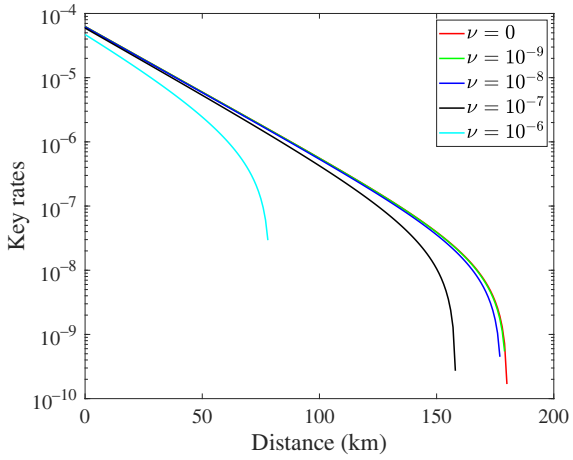

FIG. 2. Comparison of the key rates of the SCS-QKD protocol under different ν. The experiment parameters here are listed in Table I.

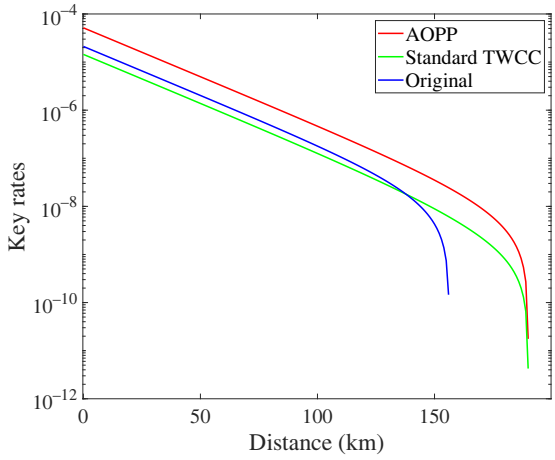

FIG. 4. The comparison of the key rates of the SCS-QKD protocol with or without TWCC. Here we set $E_d = 10\%, \nu = 0$. The other experiment parameters are listed in Table I.

parameters are listed in Table I. While the intensity of strong source can be controlled by the intensity modulator, the intensity of the weak source is due to the finite extinction ratio of the intensity modulators, i.e., generally uncontrollable. Thus in the numerical simulation, ν is a fixed value and the other source parameters, including p_0, p_x, μ are optimized. Different values of ν represent the maximum extinction ratio of different systems. Since the asymptotic case is considered here, we ignore the influence to the key rate of r, i.e., we take $r \sim 0$.

Figures 2 and 3 are the key rates of the SCS QKD protocol under different ν. The experiment parameters listed in Table I are used here, except for we set $E_d = 10\%$ in Fig. 3. By setting $\nu = 0$, the key rate formulas in Eqs. (1) and (18)–(22) are the same with those of the original SCS QKD protocol [26]. Thus lines "$\nu = 0$" in Figs. 2 and 3 are the results of the SCS QKD protocol with perfect vacuum sources, i.e., the original SCS QKD protocol. Results in Figs. 2 and 3 show that the imperfect vacuum sources, i.e., the weak sources have little affect on the key rates if the upper bound of the intensities of the imperfect vacuum sources are lower than 10^{-8}. But when the upper bound of the intensities of the imperfect vacuum sources is as large as 10^{-6}, the key rates and secure distances are drastically decreased compare with those of the original SCS QKD protocol. In experiments, the intensity of the imperfect vacuum sources can be controlled in the level of 10^{-8} by two-stage intensity modulator [27], thus we can expect little affect on the key rates in experiment due to the imperfect vacuum sources.

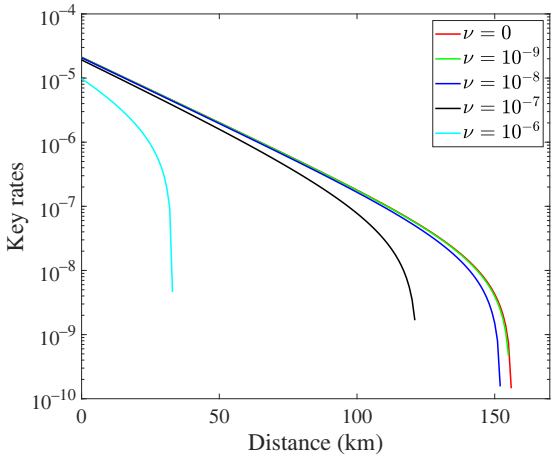

FIG. 3. The comparison of the key rates of the SCS QKD protocol under different ν. We set $E_d = 10\%$. The other experiment parameters are listed in Table I.

The active odd-parity pairing (AOPP) method [25,28] can greatly improve the key rate and secure distance of the sending-or-not-sending (SNS) protocol [19]. Since the encoding method of the SCS QKD protocol is similar to that of the SNS protocol and there are no errors in the untagged bits of the SCS QKD protocol with or without perfect vacuum sources, we can directly apply the AOPP method to the SCS QKD protocol and expect a great improvement in the key rate and secure distance. Besides,the standard two-way classical communication (TWCC) methods [25,28] can also be applied to the SCS QKD protocol. The calculation methods are shown in Appendix C.

Figures 4 and 5 are the comparison of the key rates of the SCS QKD protocol with or without TWCC. The "Original" lines are the results calculated by Eq. (1). The "Standard TWCC" lines are the results calculated by Eq. (C1). The "AOPP" lines are the results calculated by Eq. (C4). We set $E_d = 10\%, \nu = 0$ in Fig. 4, and $\nu = 10^{-8}$ in Fig. 5. The other experiment parameters are listed in Table I. Results in Figs. 4 and 5 show that both the standard

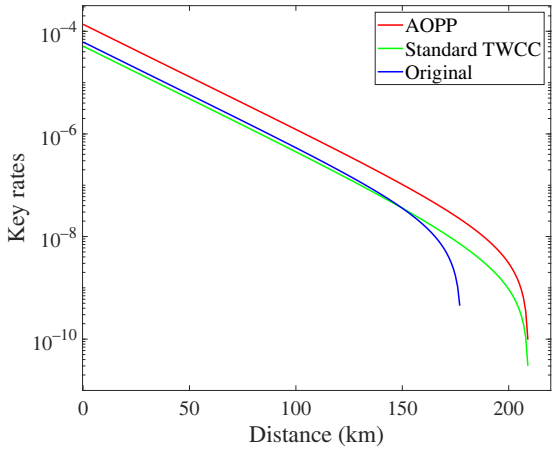

FIG. 5. Comparison of the key rates of the SCS QKD protocol with or without TWCC. Here we set $\nu = 10^{-8}$. The other experiment parameters are listed in Table I.

TWCC method and the AOPP method can improve the secure distance by about 40 km. The AOPP method can improve the key rates in all distances by about 2 times, while the standard TWCC method can improve only the key rates at long distance.

IV. CONCLUSION

In this paper, we make the SCS QKD protocol side-channel secure with real source device, which does not emit perfect vacuum pulses. The numerical simulation shows that the key rates and secure distance are only slightly decreased if the upper bound of the intensities of the imperfect vacuum sources are less than 10^{-8}, which can be achieved in experiment by two-stage intensity modulator [27]. As noted in the end of Sec. II, the sources of the protocol does not have to be WCS. What we only need is the bound values on some of the the photon number distribution coefficients. We also show that the TWCC methods including the standard TWCC method and the AOPP method can be directly applied to the SCS QKD protocol to improve the key rates and secure distance. Our numerical simulation results show that the AOPP method can improve the key rates in all distances by about 2 times and improve the secure distance by about 40 km. Given the side-channel security based on imperfect vacuum, this work makes it possible to realize side-channel-secure QKD with real devices. Our protocol can also apply to efficient quantum digital signature by taking the data post-processing method such as Refs. [29,30]. This will be reported elsewhere.

FUNDING

Ministration of Science and Technology of China through The National Key Research and Development Program of China Grant No. 2020YFA0309701; National Natural Science Foundation of China Grants No. 12174215, No. 12104184, No. 11974204, and No. 12147107; Shandong Provincial Natural Science Foundation Grant No. ZR2021LLZ007; Key R&D Plan of Shandong Province Grant Nos. 2021ZDPT01; Open Research Fund Program of the State Key Laboratory of Low-Dimensional Quantum Physics Grant No. KF202110; Leading talents of Quancheng industry.

APPENDIX A: THE CALCULATION METHOD OF THE UPPER AND LOWER BOUNDS OF $S^R_{X_+}$ AND $S^L_{X_+}$

For a certain $\tilde{Z}$ window, we have

$$|\chi^+\rangle = \frac{c_0|\alpha_A^0,\alpha_B^0\rangle + c_1|\alpha_A,\alpha_B\rangle + c_2|\phi_2\rangle}{\mathcal{N}_+}, \tag{A1}$$

where

$$c_2|\phi_2\rangle = |\alpha_A^0,\alpha_B\rangle + |\alpha_A,\alpha_B^0\rangle - c_0|\alpha_A^0,\alpha_B^0\rangle - c_1|\alpha_A,\alpha_B\rangle. \tag{A2}$$

Without loss of generality, we assume c_0, c_1, c_2 are real positive values. In principle, we can determine the values of c_0 and c_1 as we want and $c_2, |\phi_2\rangle$ are determined by c_0, c_1. For the convenience of the later calculation, we take $c_0c_1 = 1$.

Denote $\langle\psi_A|\phi_A\rangle = \beta_A$ and $\langle\psi_B|\phi_B\rangle = \beta_B$. Using the normalization condition, we have

$$c_2^2 = 2 + c_0^2 + c_1^2 + (\gamma_A\gamma_B^* + \gamma_A^*\gamma_B) - (c_0 + c_1)(\gamma_A^* + \gamma_B^* + \gamma_A + \gamma_B) + c_0c_1(\gamma_A^*\gamma_B^* + \gamma_A\gamma_B), \tag{A3}$$

where

$$\gamma_A = e^{-\nu_A/2-\mu_A/2} + \sqrt{1-e^{-\nu_A}}\sqrt{1-e^{-\mu_A}}\beta_A, \tag{A4}$$

$$\gamma_B = e^{-\nu_B/2-\mu_B/2} + \sqrt{1-e^{-\nu_B}}\sqrt{1-e^{-\mu_B}}\beta_B. \tag{A5}$$

With the condition $c_0c_1 = 1$, we have

$$c_2^2 = (c_0 + c_1 - \gamma_A - \gamma_A^*)(c_0 + c_1 - \gamma_B - \gamma_B^*). \tag{A6}$$

It is easy to check that the worst case of the phase-flip error rate is achieved when $\beta_A = \beta_B = -1$, while the condition $\nu_A, \mu_A, \nu_B, \mu_B \leq 0.7$ holds for any time window. Note that the optimized intensities of the strong sources are usually weaker than 0.02, thus this condition can always hold. And

we have

$$c_2^2 \le \left(c_0 + c_1 - 2e^{-\nu_A/2-\mu_A/2} + 2\sqrt{1-e^{-\nu_A}}\sqrt{1-e^{-\mu_A}}\right) \times \left(c_0 + c_1 - 2e^{-\nu_B/2-\mu_B/2} + 2\sqrt{1-e^{-\nu_B}}\sqrt{1-e^{-\mu_B}}\right). \tag{A7}$$

Finally, applying the input-output theory proposed in Ref. [26], we can get the upper and lower bounds of $S^R_{X_+}$ and $S^L_{X_+}$ shown in Eqs. (11) and (12). To ensure the completeness of the paper, this theory is briefly introduced in Appendix B.

APPENDIX B: THE INPUT-OUTPUT THEORY

The key idea of the input-output theory is that in a certain time window, we can regard Charlie uses the same measurement process to measure the received quantum state no matter what the quantum state is. This theory is proposed in Ref. [26], here we just simply introduce its content.

Suppose at the beginning of a certain time window, Alice and Bob send out pulse pairs in state $|\psi\rangle$. Charlie, who is assumed to control the channel and measurement station, then combines this state with his ancillary state $|\kappa\rangle$. Charlie's instrument state $\mathcal{L}$ is included in the ancillary state $|\kappa\rangle$. The initial state is

$$|\Psi_{\text{ini}}\rangle = |\psi\rangle \otimes |\kappa\rangle. \tag{B1}$$

At time t, Charlie observes his instrument $\mathcal{L}$ to see the result. His instrument $\mathcal{L}$ is observed by Alice and she can find the result from $\{l_i\}$ accompanied with its eigenstate $|l_i\rangle$ then. Most generally, after state $|\psi\rangle$ is sent to Charlie, Charlie's initial state $|\Psi_{\text{ini}}\rangle = |\psi\rangle \otimes |\kappa\rangle$ will evolve with time under a quantum process. Here we assume a unitary quantum process $\mathcal{U}$. Even though Charlie presents a nonunitary quantum process, it can be represented by a unitary process through adding more ancillary states. So, given the general ancillary state $|\kappa\rangle$, we can simply assume a unitary quantum process for Charlie. At time t, the state is now

$$|\Psi(t)\rangle = \mathcal{U}(t)|\Psi_{\text{ini}}\rangle = \mathcal{U}(t)(|\psi\rangle \otimes |\kappa\rangle). \tag{B2}$$

In general, the state at time t can be written in a bipartite form of another two subspaces, one is the instrument space $\mathcal{L}$ and the other is the remaining part of the space, subspace $\bar{\mathcal{L}}$. Given the initial input state $|\psi\rangle$ to Charlie, the probability that he observes the result l_1 at time t is

$$S^{l_1}_{|\psi\rangle} = \langle l_1|\,\text{tr}_{\bar{\mathcal{L}}}\left(|\Psi(t)\rangle\langle\Psi(t)|\right)|l_1\rangle. \tag{B3}$$

We omit (t) in the following formulas. Suppose the space $\bar{\mathcal{L}}$ is spanned by basis states $\{g_k\}$, we can rewrite Eq. (B3) by

$$S^{l_1}_{|\psi\rangle} = \sum_k |\langle\gamma_k^{(l_1)}|\Psi\rangle|^2, \tag{B4}$$

where $|\gamma_k^{(l_1)}\rangle = |g_k\rangle|l_1\rangle$.

Suppose state $|\phi\rangle$ has the form of

$$|\phi\rangle = \xi_0|\phi_0\rangle + \xi_1|\phi_1\rangle + \xi_2|\phi_2\rangle. \tag{B5}$$

Without loss of generality, we assume ξ_0, ξ_1, ξ_2 are real positive values. With Eq. (B4), we have

$$S^{l_1}_{|\phi\rangle} = \sum_k |\langle\gamma_k^{(l_1)}|\phi\rangle|^2, \tag{B6}$$

$$S^{l_1}_{|\phi_0\rangle} = \sum_k |\langle\gamma_k^{(l_1)}|\phi_0\rangle|^2, \tag{B7}$$

$$S^{l_1}_{|\phi_1\rangle} = \sum_k |\langle\gamma_k^{(l_1)}|\phi_1\rangle|^2, \tag{B8}$$

where $S^{l_1}_{|\tau\rangle}$ is the probability that Charlie observes the result l_1 at time t if Alice and Bob send out a pulse in state $|\tau\rangle$ in a certain time window for $\tau = \phi, \phi_0, \phi_1$.

With Eqs. (B5)–(B8), we have

$$S^{l_1}_{|\phi\rangle} \le \xi_0^2 S^{l_1}_{|\phi_0\rangle} + \xi_1^2 S^{l_1}_{|\phi_1\rangle} + \xi_2^2 + 2\xi_0\xi_1\sqrt{S^{l_1}_{|\phi_0\rangle}S^{l_1}_{|\phi_1\rangle}} + 2\xi_0\xi_2\sqrt{S^{l_1}_{|\phi_0\rangle}} + 2\xi_1\xi_2\sqrt{S^{l_1}_{|\phi_1\rangle}} \tag{B9}$$

and

$$S^{l_1}_{|\phi\rangle} \ge \xi_0^2 S^{l_1}_{|\phi_0\rangle} + \xi_1^2 S^{l_1}_{|\phi_1\rangle} - \left(2\xi_0\xi_1\sqrt{S^{l_1}_{|\phi_0\rangle}S^{l_1}_{|\phi_1\rangle}} + +2\xi_0\xi_2\sqrt{S^{l_1}_{|\phi_0\rangle}} + 2\xi_1\xi_2\sqrt{S^{l_1}_{|\phi_1\rangle}}\right). \tag{B10}$$

APPENDIX C: THE TWCC METHODS

Before Alice and Bob perform the error correction, *they* can first perform the TWCC methods to reduce the bit-flip error rate in the raw keys. Both the standard TWCC method and the AOPP method can be applied to the SCS QKD protocol [25]. And the iteration formulas of the lower bound of the untagged bits and the upper bound of the phase-flip error rate after TWCC are also holds here [25].

To perform the standard TWCC, Bob first randomly pairs his bits two by two and then announces all the paired sequences to Alice through the public channel. Then Alice and Bob compare the parity of these bit pairs, *they* keep one bit from the bit pairs with the same parities and discard the rest. The survived bits form an alternative bit string and would perform the error correction and privacy

amplification to distil the final keys according to the following key rate formulas:

$$R' = \frac{1}{N}\{n_u^{\mathrm{TWCC}}[1 - H(\bar{e}_{\mathrm{ph}}^{\mathrm{TWCC}})] - f\,[n_{t1}H(E_1) + n_{t2}H(E_2) + n_{t3}H(E_3)]\}. \tag{C1}$$

Here n_u^{TWCC} is the number of untagged bits after TWCC and

$$n_u^{\mathrm{TWCC}} = \frac{n_u^2}{2n_t}. \tag{C2}$$

$\bar{e}_{\mathrm{ph}}^{\mathrm{TWCC}}$ is the upper bound of the phase-flip error rate after standard TWCC and

$$\bar{e}_{\mathrm{ph}}^{\mathrm{TWCC}} = 2\bar{e}_{\mathrm{ph}}(1 - \bar{e}_{\mathrm{ph}}). \tag{C3}$$

n_{t1}, n_{t2} are the number of survived bits from the bit pairs containing two 0 bits, two 1 bits after standard TWCC, and n_{t3} is the number of survived bits from odd-parity bit pairs. E_1, E_2, E_3 are the corresponding bit-flip error rates. Those values can be directly observed in the experiment.

To perform AOPP, Bob actively random pairs the bits 0 with bits 1, and Bob gets $n_g = \min(n_{b0}, n_{b1})$ pairs where n_{b0}, n_{b1} are the number of bits 0 and bits 1 in the raw keys before AOPP. Then Bob announces all the paired sequences to Alice through the public channel. Alice would announce all the positions of the pairs with odd parities and Alice and Bob keep only one bit from those announced pairs. The survived bits form another bit string and would perform the error correction and privacy amplification to distil the final keys according to the following key rate formulas:

$$R'' = \frac{1}{N}\{n_u^{\mathrm{AOPP}}[1 - H(\bar{e}_{\mathrm{ph}}^{\mathrm{AOPP}})] - f n_t^{\mathrm{AOPP}} H(E_{\mathrm{AOPP}})\}. \tag{C4}$$

Here n_u^{AOPP} is the untagged bits after AOPP and

$$n_u^{\mathrm{AOPP}} = \frac{n_{u0}}{n_{b0}}\frac{n_{u1}}{n_{b1}}n_g. \tag{C5}$$

n_t^{AOPP} is the number of survived bits after AOPP and E_{AOPP} is the corresponding bit-flip error rate. In the asymptotic case, we have [25]

$$\bar{e}_{\mathrm{ph}}^{\mathrm{AOPP}} = \bar{e}_{\mathrm{ph}}^{\mathrm{TWCC}} \tag{C6}$$

[1] C. H. Bennett and G. Brassard: Quantum cryptography: Public key distribution and coin tossing, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing* (1984) pp. 175–179

[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, Rev. Mod. Phys. **74**, 145 (2002).

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

[4] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, Advances in quantum cryptography, Adv. Opt. Photon. **12**, 1012 (2020).

[5] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution, Rev. Mod. Phys. **81**, 1301 (2009).

[6] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Quantum cryptography with coherent states, Phys. Rev. A **51**, 1863 (1995).

[7] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Limitations on Practical Quantum Cryptography, Phys. Rev. Lett. **85**, 1330 (2000).

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

[9] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, Full-field implementation of a perfect eavesdropper on a quantum cryptography system, Nat. Commun. **2**, 1 (2011).

[10] H. Weier, H. Krauss, M. Rau, M. Fürst, S. Nauerth, and H. Weinfurter, Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors, New J. Phys. **13**, 073024 (2011).

[11] W.-Y. Hwang, Quantum Key Distribution with High Loss: Toward Global Secure Communication, Phys. Rev. Lett. **91**, 057901 (2003).

[12] X.-B. Wang, Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography, Phys. Rev. Lett. **94**, 230503 (2005).

[13] H.-K. Lo, X. Ma, and K. Chen, Decoy State Quantum Key Distribution, Phys. Rev. Lett. **94**, 230504 (2005).

[14] H.-K. Lo, M. Curty, and B. Qi, Measurement-Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **108**, 130503 (2012).

[15] S. L. Braunstein and S. Pirandola, Side-Channel-Free Quantum Key Distribution, Phys. Rev. Lett. **108**, 130502 (2012).

[16] Y.-H. Zhou, Z.-W. Yu, and X.-B. Wang, Making the decoy-state measurement-device-independent quantum key distribution practically useful, Phys. Rev. A **93**, 042324 (2016).

[17] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Overcoming the rate–distance limit of quantum key distribution without quantum repeaters, Nature **557**, 400 (2018).

[18] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Fundamental limits of repeaterless quantum communications, Nat. Commun. **8**, 15043 (2017).

[19] X.-B. Wang, Z.-W. Yu, and X.-L. Hu, Twin-field quantum key distribution with large misalignment error, Phys. Rev. A **98**, 062323 (2018).

[20] K. Tamaki, H.-K. Lo, W. Wang, and M. Lucamarini, Information theoretic security of quantum key distribution overcoming the repeaterless secret key capacity bound, (2018), arXiv preprint ArXiv:1805.05511.

[21] X. Ma, P. Zeng, and H. Zhou, Phase-Matching Quantum Key Distribution, Phys. Rev. X **8**, 031043 (2018).

[22] J. Lin and N. Lütkenhaus, Simple security analysis of phase-matching measurement-device-independent quantum key distribution, Phys. Rev. A **98**, 042332 (2018).

[23] C. Cui, Z.-Q. Yin, R. Wang, W. Chen, S. Wang, G.-C. Guo, and Z.-F. Han, Twin-Field Quantum Key Distribution Without Phase Postselection, Phys. Rev. Appl. **11**, 034053 (2019).

[24] M. Curty, K. Azuma, and H.-K. Lo, Simple security proof of twin-field type quantum key distribution protocol, NPJ Quantum Inf. **5**, 64 (2019).

[25] H. Xu, Z.-W. Yu, C. Jiang, X.-L. Hu, and X.-B. Wang, Sending-or-not-sending twin-field quantum key distribution: Breaking the direct transmission key rate, Phys. Rev. A **101**, 042330 (2020).

[26] X.-B. Wang, X.-L. Hu, and Z.-W. Yu, Practical Long-Distance Side-Channel-Free Quantum Key Distribution, Phys. Rev. Appl. **12**, 054034 (2019).

[27] C. Zhang, X.-L. Hu, C. Jiang, J.-P. Chen, Y. Liu, W. Zhang, Z.-W. Yu, H. Li, L. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, Experimental Side-Channel-Secure Quantum Key Distribution, Phys. Rev. Lett. **128**, 190503 (2022).

[28] C. Jiang, X.-L. Hu, Z.-W. Yu, and X.-B. Wang, Composable security for practical quantum key distribution with two way classical communication, New J. Phys. **23**, 063038 (2021).

[29] R. Amiri, P. Wallden, A. Kent, and E. Andersson, Secure quantum signatures using insecure quantum channels, Phys. Rev. A **93**, 032325 (2016).

[30] J.-Q. Qin, C. Jiang, Y.-L. Yu, and X.-B. Wang, Quantum Digital Signatures with Random Pairing, Phys. Rev. Appl. **17**, 044047 (2022).