Side-channel-free quantum key distribution with practical devices

Cong Jiang,1,2 Zong-Wen Yu,3 Xiao-Long Hu,4 and Xiang-Bin Wang1,2,5,6,7,*

1Jinan Institute of Quantum Technology, Jinan, Shandong 250101, P. R. China
2State Key Laboratory of Low Dimensional Quantum Physics, Department of Physics, Tsinghua University, Beijing 100084, P. R. China
3Data Communication Science and Technology Research Institute, Beijing 100084, P. R. China
4School of Physics, State Key Laboratory of Optoelectronic Materials and Technologies, Sun Yat-sen University, Guangzhou 510275, P. R. China
5Shanghai Branch, CAS Center for Excellence and Synergetic Innovation Center in Quantum Information and Quantum Physics, University of Science and Technology of China, Shanghai 201315, P. R. China
6Shenzhen Institute for Quantum Science and Engineering, and Physics Department, Southern University of Science and Technology, Shenzhen 518055, P. R. China
7Frontier Science Center for Quantum Information, Beijing, P. R. China

Based on the idea that there is no side channel in the vacuum state, the side-channel-free quantum key distribution (SCFQKD) protocol was proposed, which is immune to all attacks in the source side-channel space and all attacks in the detectors. In the original SCFQKD protocol, an important assumption is that Alice and Bob can produce the perfect vacuum pulses. But due to the finite extinction ratio of the intensity modulators, the perfect vacuum pulse is impossible in practice. In this paper, we solve this problem and make the quantum key distribution side-channel secure with real source device which does not emit perfect vacuum pulses. Our conclusion only depends on the upper bounds of the intensities of the sources. No other assumptions such as stable sources and stable side channels are needed. The numerical results show that, comparing with the results of SCFQKD protocol with perfect vacuum sources, the key rates and secure distance are only slightly decreased if the upper bound of the intensity of the imperfect vacuum source is less than $10^{-8}$ which can be achieved in experiment by two-stage intensity modulator. We also show that the two-way classical communication can be used to the data post-processing of SCFQKD protocol to improve the key rate. Specially, the active odd-parity pairing method can improve the key rates in all distances by about two times and the secure distance by about 40 km. Give that the side channel security based on imperfect vacuum, this work makes it possible to realize side channel secure QKD with real devices.

I. INTRODUCTION

Quantum key distribution can provide secure communication between two remote parties [3–11], no matter what the eavesdropper, Eve, does in the channel. However, the security of a practical QKD system can be broken due to the imperfection of the practical devices. In the source side, there could be side channels which might leak extra information to Eve, such as basis dependent synchronization errors in the pulse emitting time or the frequency-spectrum difference for different encoding states or bases in the source sides. Besides, the detectors can be controlled by the eavesdropper through strong light attacks [12–14]. Encoding the bits into sending or not-sending as used in the sending-or-not-sending (SNS) protocol [15] of twin-field QKD [16], using the fact that there is no side channel in the vacuum state, the side-channel-free (SCF)QKD protocol was proposed [11]. SCFQKD protocol [11] is immune to all attacks in the side-channel space of sources, and by introducing a third party as a measurement station, it is also measurement device independent [9, 10] immune to all attacks in the detectors. SCFQKD protocol only needs to know the upper bounds of the intensities of the non-vacuum sources and its secure distance can exceed 200 km even with 20% misalignment error. Recently, SCFQKD protocol was experimentally demonstrated in 50 km fibers [17], which shows the potential of SCFQKD protocol in practical applications.

Although the recent experiment [17] has verified the the most impressive advantage of the promised long distance by SCFQKD protocol proposed in Ref. [11], the major problem in the original SCFQKD protocol requesting perfect vacuum source is still open. In this paper, we solve this open problem and make the QKD side-channel secure with real source device which does not emit perfect vacuum pulses. Our conclusion only depends on the upper bounds of the intensities of the sources. No other assumptions such as stable sources and stable side channels are needed. The channel security of our protocol allows whatever imperfect detection loophole and whatever side channel imperfection.

* Corresponding author: xbwang@mail.tsinghua.edu.cn
of emitted photons, say, it guarantees a secure QKD provided that Eve has no access to devices inside Alice’s and Bob’s labs. Give that the side channel security based on imperfect vacuum, this work makes it possible to realize side channel secure QKD with real devices.

The paper is arranged as follows. We first introduce the procedure of SCFQKD protocol with real devices in Sec. II. We then show how to estimate the phase-flip error rate of a certain time window in Sec. III. With the conclusion in Sec. IV, 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. V, where we also show that the two-way classical communication (TWCC) can be used to the data post-processing of SCFQKD protocol to improve the key rate. The article is ended with some conclusion remarks.

II. 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 \( p_s = 1 - p_0 \) respectively. If the weak source \( o_A \) (\( o_B \)) is chosen, a weak coherent state (WCS) pulse with intensity \( \nu_A^0 \) (\( \nu_B^0 \)) 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 \( \mu_A \) (\( \mu_B \)) is prepared, and Alice (Bob) takes it as bit 0 (1). 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. 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 used in each time windows. For the effective key generation windows, the corresponding bits are used to distil the final keys.

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 \( B \) (\( O \)) 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, \( \overline{\epsilon}^{ph} \). The key rate formula is

\[
R = \frac{1}{N} \left\{ n_u \left[ 1 - H(\overline{\epsilon}^{ph}) \right] - f n_t H(E_K) \right\},
\]

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.

In what follows we shall study how to calculate \( n_u \) and \( \overline{\epsilon}^{ph} \) by observed values and we result in Eqs. (18-22).

III. 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 only need to consider the side-channel space for the non vacuum parts. The states can be decomposed in two parts, vacuum and non vacuum. Explicitly, if Alice (Bob) chooses the weak source, she (he) actually prepares the state:

\[
\begin{align*}
|\alpha^0_A \rangle &= e^{-\nu_A^0/2}|0 \rangle + \sqrt{1 - e^{-\nu_A^0}}|\psi_A \rangle, \\
|\alpha^0_B \rangle &= e^{-\nu_B^0/2}|0 \rangle + \sqrt{1 - e^{-\nu_B^0}}|\psi_B \rangle.
\end{align*}
\]

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

\[
\begin{align*}
|\alpha_A \rangle &= e^{-\mu_A^0/2}|0 \rangle + \sqrt{1 - e^{-\mu_A^0}}|\phi_A \rangle, \\
|\alpha_B \rangle &= e^{-\mu_B^0/2}|0 \rangle + \sqrt{1 - e^{-\mu_B^0}}|\phi_B \rangle.
\end{align*}
\]
Here $|0\rangle$ is the vacuum state and $|\psi_A\rangle, |\psi_B\rangle, |\phi_A\rangle, |\phi_B\rangle$ are the corresponding non vacuum parts of each states. Obviously, we have

$$
(0|\psi_A) = (0|\psi_B) = (0|\phi_A) = (0|\phi_B) = 0,
$$

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

As shall be shown, our protocol does not request any specific photon number distribution of its sources, it only needs a linear superposition of vacuum and non vacuum 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

$$
|\Psi\rangle = \frac{1}{\sqrt{2}}((|\alpha_A, 0\rangle_A \otimes |0\rangle_Z + |\alpha_A, \alpha_B^0\rangle_A \otimes |10\rangle_Z)).
$$

(5)

Also, we have

$$
|\Psi\rangle = \frac{1}{2}(N_+|\tilde{\chi}^+\rangle \otimes |\Phi^0\rangle_Z + N_-|\tilde{\chi}^-\rangle \otimes |\Phi^1\rangle_Z),
$$

(6)

where

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

(7)

and

$$
|\tilde{\chi}^+\rangle = \frac{1}{N_+}(|\alpha_A^0, \alpha_B^0\rangle + |\alpha_A, \alpha_B^0\rangle), \quad |\tilde{\chi}^-\rangle = \frac{1}{N_-}(|\alpha_A^0, \alpha_B^0\rangle - |\alpha_A, \alpha_B^0\rangle),
$$

(8)

where $N_+$ and $N_-$ are normalization coefficients.

Here $|01\rangle_Z$ and $|10\rangle_Z$ are local states that are stored in Alice’s and Bob’s labs. If Alice and Bob decide to measure their local states in $\tilde{Z}$ basis, i.e., $\{|01\rangle_Z, |10\rangle_Z\}$ 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 $|\alpha_A^0, \alpha_B^0\rangle$ 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., $\{|\Phi^0\rangle_Z, |\Phi^1\rangle_Z\}$ 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 $|\tilde{\chi}^+\rangle$ or $|\tilde{\chi}^-\rangle$ with probabilities $N_+^2/4$ and $N_-^2/4$ 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 $|\tilde{\chi}^+\rangle$, i.e., the measurement result of their local state is $|\Phi^0\rangle_Z$, and Charlie announces the right detector clicking; 2) the effective window while Alice and Bob send out a pulse pair in state $|\tilde{\chi}^-\rangle$, i.e., the measurement result of their local state is $|\Phi^1\rangle_Z$, and Charlie announces the left detector clicking.

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

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

$$
T_X = \frac{N_+^2}{4}S^R_{X_+} + \frac{N_-^2}{4}S^L_{X_-} = \frac{N_+^2}{4}(S^R_{X_+} - S^L_{X_-}) + S^L_{\tilde{Z}}.
$$

(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 $\frac{N_+^2}{4}S^R_{X_+} + \frac{N_-^2}{4}S^L_{X_-} = S^L_{\tilde{Z}}$.

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

$$
e^{ph} = \frac{T_X}{S^L_{\tilde{Z}}} = \frac{N_+^2}{4}(S^R_{X_+} - S^L_{X_-}) + S^L_{\tilde{Z}},
$$

(10)

where $S^L_{\tilde{Z}} = S^L_{\tilde{Z}} + S^R_{\tilde{Z}}$. 
As shown in the Appendix A, we have the upper bound of $S_{K+}^t$ and the lower bound of $S_{K-}^t$

\[
S_{K+}^t \leq \frac{1}{N^2} \left( c_0^2 S_{O}^t + c_1^2 S_{B}^t + c_2^2 + 2c_0 c_1 \sqrt{S_{O}^t S_{B}^t} + 2c_0 c_2 \sqrt{S_{O}^t} + 2c_1 c_2 \sqrt{S_{B}^t} \right),
\]

\[
S_{K-}^t \geq \frac{1}{N^2} \left( c_0^2 S_{O}^t + c_1^2 S_{B}^t - 2c_0 c_1 \sqrt{S_{O}^t S_{B}^t} - 2c_0 c_2 \sqrt{S_{O}^t} - 2c_1 c_2 \sqrt{S_{B}^t} \right),
\]

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

\[
c_2^2 \leq \left( c_0 + c_1 - 2e^{-\nu_A/2-\mu_A/2} + 2\sqrt{1 - e^{-\nu_A}} \sqrt{1 - e^{-\mu_A}} \right) \left( c_0 + c_1 - 2e^{-\nu_B/2-\mu_B/2} + 2\sqrt{1 - e^{-\nu_B}} \sqrt{1 - e^{-\mu_B}} \right).
\]

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

### IV. THE PHASE-FLIP ERROR RATE IN THE WHOLE PROTOCOL

In Sec. [11], 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 $\mu$, the probabilities $S_{O}^t$ and $T_X$, $c_0, c_1, c_2$ by the corresponding values in this certain $\tilde{Z}$ window.

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

\[
n^{ph} = \sum_{i=1}^{N} 2p_0 p_x (1-r) T_X^i,
\]

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

Eqs. (11)(13) always hold provided that $c_0 c_1 = 1$. Thus we take the same value of $c_0$ and $c_1$ for all time windows and denote by $c_0, c_1$ respectively. The value of $c_2$ is upper bounded by Eq. (13). Further more, we have

\[
(c_2^j)^2 \leq c_2^2 = \left( c_0 + c_1 - 2e^{-\nu_A^j/2-\mu_A^j/2} + 2\sqrt{1 - e^{-\nu_A^j}} \sqrt{1 - e^{-\mu_A^j}} \right) \left( c_0 + c_1 - 2e^{-\nu_B^j/2-\mu_B^j/2} + 2\sqrt{1 - e^{-\nu_B^j}} \sqrt{1 - e^{-\mu_B^j}} \right),
\]

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

\[
n^{ph} = \sum_{i=1}^{N} 2p_0 p_x (1-r) T_X^i
\]

\[
\leq \sum_{i=1}^{N} \frac{1}{2} p_0 p_x (1-r) \left[ 2c_0 \left( S_{O}^i R - S_{O}^i L \right) + c_1 \left( S_{B}^i R - S_{B}^i L \right) + c_2^2 + 2c_0 c_1 \left( \sqrt{S_{O}^i R S_{B}^i R} + \sqrt{S_{O}^i L S_{B}^i L} \right) \right]
\]

\[
+ 2c_0 c_2 \left( \sqrt{S_{O}^i R} + \sqrt{S_{O}^i L} \right) + 2c_1 c_2 \left( \sqrt{S_{B}^i R} + \sqrt{S_{B}^i L} \right) + \sum_{i=1}^{N} 2p_0 p_x (1-r) S_{Z}^{i, L}
\]

\[
\leq \frac{1}{2} p_0 p_x (1-r) \left[ 2c_0 \sum_{i=1}^{N} \left( S_{O}^i R - S_{O}^i L \right) + c_1 \sum_{i=1}^{N} \left( S_{B}^i R - S_{B}^i L \right) + c_2^2 + 2c_0 c_1 \left( \sum_{i=1}^{N} S_{O}^i R \sum_{i=1}^{N} S_{B}^i R + \sum_{i=1}^{N} S_{O}^i L \sum_{i=1}^{N} S_{B}^i L \right) \right]
\]

\[
+ 2c_0 c_2 \left( \sum_{i=1}^{N} \sqrt{S_{O}^i R} + \sum_{i=1}^{N} \sqrt{S_{O}^i L} \right) + 2c_1 c_2 \left( \sum_{i=1}^{N} \sqrt{S_{B}^i R} + \sum_{i=1}^{N} \sqrt{S_{B}^i L} \right) + \sum_{i=1}^{N} 2p_0 p_x (1-r) S_{Z}^{i, L}.
\]

Here we have used the Cauchy inequality in the second inequality

\[
\left( \sum_{i=1}^{N} a_i b_i \right)^2 \leq \sum_{i=1}^{N} a_i^2 b_i^2 \quad a_i, b_i \in \mathbb{R}.
\]
Denote $n_d^2$ as the number of observed effective events caused by the detector $d$ in the ς-test-windows (those ς windows chosen for test) where $d \in \{L, R\}$ and ς \( \in \{O, B, Z\} \). We have

$$n_d^O = \sum_{i=1}^{N} n_{i}^{L} S_{O}^{i,d}, \quad n_d^B = \sum_{i=1}^{N} n_{i}^{L} S_{B}^{i,d}, \quad n_d^Z = \sum_{i=1}^{N} 2p_0 p_x S_{Z}^{i,d}. \quad (18)$$

We define

$$S_{O,A}^{d} = \frac{n_d^O}{N_{p_0}^{d}}, \quad S_{B,A}^{d} = \frac{n_d^B}{N_{p_0}^{d}}, \quad S_{Z,A}^{d} = \frac{n_d^Z}{2N_{p_0} p_x}. \quad (19)$$

With those observed values, we have

$$n_{ph}^{\mu} \leq \bar{\tau}_{ph}^{\mu} = \frac{1}{2} p_0 p_x (1 - r) N \left[ c_0^2 (S_{O,A}^{R} - S_{O,A}^{L}) + c_1^2 (S_{B,A}^{R} - S_{B,A}^{L}) + \bar{\tau}_{2}^{\mu} + 2c_0 c_1 \left( \sqrt{S_{O,A}^{R} S_{O,A}^{R}} + \sqrt{S_{O,A}^{L} S_{O,A}^{L}} \right) \right]$$

$$+ 2c_0 \bar{\tau}_{2}^{\mu} \left( \sqrt{S_{O,A}^{R}} + \sqrt{S_{O,A}^{L}} \right) + 2c_1 \bar{\tau}_{2}^{\mu} \left( \sqrt{S_{B,A}^{R}} + \sqrt{S_{B,A}^{L}} \right) + 4S_{Z,A}^{L}.$$

And the number of untagged bits $n_u$ satisfies

$$n_u = \sum_{i=1}^{N} 2p_0 p_x (1 - r) (S_{Z}^{i,L} + S_{Z}^{i,R}) = 2p_0 p_x (1 - r) N (S_{Z,A}^{L} + S_{Z,A}^{R}). \quad (21)$$

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

$$\bar{\tau}_{ph}^{\mu} = \frac{n_{ph}^{\mu}}{n_u}. \quad (22)$$

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

**Remark:** Although we have used model of WCS sources in the calculation above, it’s 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 vacuum part and non vacuum part:

$$|A\rangle = \sqrt{a_0} |0\rangle + \sqrt{1 - a_0} |\text{non - vacuum}\rangle,$$

where $a_0$ is the probability of vacuum part of the state and $|\text{non - vacuum}\rangle$ is a whole space non vacuum state. As shown in Eq. (15), our method only depends on $e^{-\nu^L_A}, e^{-\nu^R_A}, e^{-\mu^L_B}, e^{-\mu^R_B}$, 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 $\nu$ or $\mu$.

## V. NUMERICAL SIMULATION

We shall 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., $\nu^L_A = \nu^R_A = \nu$ and $\mu^L_B = \mu^R_B = \mu$. 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 parameters are listed in Table I. In the numerical simulation, $\nu$ is a fixed value and the other source parameters including $p_0, p_x, \mu$ are optimized. 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 I and II are the key rates of SCFQKD protocol under different $\nu$. The experiment parameters listed in Table I are used here, except for we set $E_d = 10\%$ in Figure II. By setting $\nu = 0$, the key rate formulas in Eqs. (1, 18, 22) are the same with those of the original SCFQKD protocol \[11\]. Thus lines ‘$\nu = 0$’ in Figures I and II are the results of SCFQKD protocol with perfect vacuum sources, i.e., the original SCFQKD protocol. Results in Figures I and II show that the imperfect vacuum sources, i.e., the weak sources have little affect on the key rates if the upper bound of the
TABLE I. List of experimental parameters used in numerical simulations. Here $p_d$ is the dark counting rate per pulse of Charlie’s detectors; $\eta_d$ is the detection efficiency of Charlie’s detectors; $E_d$ is the misalignment error; $f$ is the error correction inefficiency; $\alpha_f$ is the fiber loss coefficient (dB/km).

| $p_d$ | $E_d$ | $\eta_d$ | $f$ | $\alpha_f$ |
|-------|-------|----------|-----|------------|
| $1.0 \times 10^{-9}$ | 4% | 60.0% | 1.1 | 0.2 |

FIG. 1. The comparison of the key rates of SCFQKD protocol under different $\nu$. The experiment parameters here are listed in Table I.

intensities of the the imperfect vacuum sources are lower than $10^{-8}$. But when the upper bound of the intensities of the the imperfect vacuum sources is as large as $10^{-6}$, the key rates and secure distances are drastically decreased compared with those of the original SCFQKD protocol. In experiments, the intensity of the imperfect vacuum sources can be controlled in the level of $10^{-8}$ by two-stage intensity modulator \^[17\], thus we can expect little affect on the key rates in experiment due to the imperfect vacuum sources.

Since there are no errors in the untagged bits of SCFQKD protocol with or without perfect vacuum sources. We can directly applied the TWCC methods \^[18, 19\] including the standard TWCC method and the AOPP method to improve the key rates and secure distance of the SCFQKD protocol. The calculation methods are shown in Appendix C.

Figures 3 and 4 are the comparison of the key rates of SCFQKD 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 Figure 3 and $\nu = 10^{-8}$ in Figure 4. The other experiment parameters are listed in Table I. Results in Figures 3 and 4 show that both the standard 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 two times, while the standard TWCC method can only improve the key rates at long distance.

VI. CONCLUSION

In this paper, we make SCFQKD protocol side-channel secure with real source device which does not emit perfect vacuum pulses. Our conclusion only depends on the upper bounds of the intensities of the sources and no other assumptions are needed. 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 \^[17\]. We also show that the TWCC methods including the standard TWCC method and the AOPP method can be directly applied to SCFQKD protocol to improve the key rates and secure distance. Our numerical simulation results show that AOPP method can improve the key rates in all distances by about two times and improve the secure distance by about 40 km. Give that 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 post data processing method such as \^[20, 21\]. This will be reported elsewhere.
FIG. 2. The comparison of the key rates of SCFQKD protocol under different $\nu$. We set $E_d = 10\%$. The other experiment parameters are listed in Table I.

FIG. 3. The comparison of the key rates of SCFQKD protocol with or without TWCC. Here we set $E_d = 10\%, \nu = 0$. The other experiment parameters are listed in Table I.

VII. ACKNOWLEDGEMENT

We acknowledge the financial support in part by Ministry 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 Grant Nos. 12174215, 12104184, 11974204 and 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.

Appendix A: The calculation method of the upper and lower bounds of $S_{X+}^R$ and $S_{X+}^L$

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

$$|\chi^+\rangle = \frac{c_0|\alpha_0^A, \alpha_0^B\rangle + c_1|\alpha_A, \alpha_B\rangle + c_2|\phi_2\rangle}{N_+},$$

where

$$c_2|\phi_2\rangle = |\alpha_0^A, \alpha_B\rangle + |\alpha_A, \alpha_0^B\rangle - c_0|\alpha_0^A, \alpha_0^B\rangle - c_1|\alpha_A, \alpha_B\rangle.$$
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 \( c_0 c_1 = 1 \).

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

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

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 \( c_0 c_1 = 1 \), 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 \( \beta_A = \beta_B = -1 \). And we have

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

Finally, apply the input-output theory proposed in Ref. [11], we can get the upper and lower bounds of \( S_{X+}^R \) and \( S_{X+}^L \) shown in Eqs. [12][13][18]. To ensure the completeness of the article, this theory is briefly introduced in Appendix [13]

### 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. [11], here we just simply introduce its content.

Suppose at the beginning of a certain time window, Alice and Bob send out a 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 \( L \) is included in the ancillary state \( |\kappa\rangle \). The initial state is

\[
|\Psi_{in}\rangle = |\psi\rangle \otimes |\kappa\rangle. \tag{B1}
\]

At time \( t \), Charlie observes his instrument \( L \) to see the result. His instrument \( L \) is observed by Alice and she can find 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 \( |\Psi_{in}\rangle = |\psi\rangle \otimes |\kappa\rangle \) will evolve with time under a quantum process. Here we assume a unitary quantum process \( \mathcal{U} \). Even though Charlie presents a non-unitary 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

\[
|\Psi(t)\rangle = U(t)|\Psi_{ini}\rangle = U(t)(|\psi\rangle \otimes |\kappa\rangle)
\]

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

\[
S_{l_1}^{(t)} = \langle l_1|\text{tr}_{\bar{\mathcal{L}}} (|\Psi(t)\rangle\langle\Psi(t)|)|l_1\rangle
\]

We will 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

\[
S_{l_1}^{(t)} = \sum_k |\langle \gamma_k^{(l_1)} |\Psi \rangle|^2
\]

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

Suppose state \( |\phi\rangle \) has the form of

\[
|\phi\rangle = \xi_0|\phi_0\rangle + \xi_1|\phi_1\rangle + \xi_2|\phi_2\rangle,
\]

Without loss of generality, we assume \( \xi_0, \xi_1, \xi_2 \) are real positive values. With Eq. (B4), we have

\[
\begin{align*}
S_{\phi}^{(l_1)} &= \sum_k |\langle \gamma_k^{(l_1)} |\phi \rangle|^2, \\
S_{\phi_0}^{(l_1)} &= \sum_k |\langle \gamma_k^{(l_1)} |\phi_0 \rangle|^2, \\
S_{\phi_1}^{(l_1)} &= \sum_k |\langle \gamma_k^{(l_1)} |\phi_1 \rangle|^2,
\end{align*}
\]

where \( S_{\tau}^{(l_1)} \) 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

\[
S_{\phi}^{(l_1)} \leq \xi_0^2 S_{\phi_0}^{(l_1)} + \xi_1^2 S_{\phi_1}^{(l_1)} + \xi_2^2 + 2\xi_0\xi_1\sqrt{S_{\phi_0}^{(l_1)} S_{\phi_1}^{(l_1)}} + 2\xi_0\xi_2\sqrt{S_{\phi_0}^{(l_1)} S_{\phi_2}^{(l_1)}} + 2\xi_1\xi_2\sqrt{S_{\phi_1}^{(l_1)} S_{\phi_2}^{(l_1)}}
\]

and

\[
S_{\phi}^{(l_1)} \geq \xi_0^2 S_{\phi_0}^{(l_1)} + \xi_1^2 S_{\phi_1}^{(l_1)} \left( 2\xi_0\xi_1\sqrt{S_{\phi_0}^{(l_1)} S_{\phi_1}^{(l_1)}} + 2\xi_0\xi_2\sqrt{S_{\phi_0}^{(l_1)} S_{\phi_2}^{(l_1)}} + 2\xi_1\xi_2\sqrt{S_{\phi_1}^{(l_1)} S_{\phi_2}^{(l_1)}} \right)
\]

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 SCFQKD protocol [18]. 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 [18].

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 same parities and discard the rest. The survived bits form a new bit string and would be performed the error correction and privacy amplification to distil the final keys according to the following key rate formulas

\[
R' = \frac{1}{N} \{n_u^{twcc}[1 - H(E_1) - f] + n_d H(E_1) + n_d H(E_2) + n_d H(E_3)\}.
\]
Here \( n_{tu}^{twcc} \) is the number of untagged bits after TWCC and

\[
n_u^{twcc} = \frac{n_u^2}{2n_t}.
\]  

(C2)

\( \tau_{ph}^{twcc} \) is the upper bound of the phase-flip error rate after standard TWCC and

\[
\tau_{ph}^{twcc} = 2\tau_{ph}(1 - \tau_{ph}).
\]  

(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 get \( n_g = min(n_{b0}, n_{b1}) \) 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 only keeps one bits from those announced pairs. The survived bits form a new bit string and would be performed the error correction and privacy amplification to distil the final keys according to the following key rate formulas

\[
R'' = \frac{1}{N} \{ n_u^{aopp} [1 - H(\tau_{ph}^{aopp})] - f n_t^{aopp} H(E_{aopp}) \}.
\]  

(C4)

Here \( n_u^{aopp} \) is the untagged bits after AOPP and

\[
n_u^{aopp} = \frac{n_{u0} n_{u1} n_g}{n_{b0} n_{b1}}.
\]  

(C5)

\( n_t^{aopp} \) is the number of survived bits after AOPP and \( E_{aopp} \) is the corresponding bit-flip error rate.

[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, Reviews of Modern Physics 74, 145 (2002).
[3] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Secure quantum key distribution with realistic devices, Reviews of Modern Physics 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. Shara, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, Advances in quantum cryptography, Advances in Optics and Photonics 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, Reviews of Modern Physics 81, 1301 (2009).
[6] W.-Y. Hwang, Quantum key distribution with high loss: toward global secure communication, Physical Review Letters 91, 057901 (2003).
[7] X.-B. Wang, Beating the photon-number-splitting attack in practical quantum cryptography, Physical Review Letters 94, 230503 (2005).
[8] H.-K. Lo, X. Ma, and K. Chen, Decoy state quantum key distribution, Physical Review Letters 94, 230504 (2005).
[9] H.-K. Lo, M. Curty, and B. Qi, Measurement-device-independent quantum key distribution, Physical Review Letters 108, 130503 (2012).
[10] S. L. Braunstein and S. Pirandola, Side-channel-free quantum key distribution, Physical Review Letters 108, 130502 (2012).
[11] X.-B. Wang, X.-L. Hu, and Z.-W. Yu, Practical long-distance side-channel-free quantum key distribution, Physical Review Applied 12, 054034 (2019).
[12] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Hacking commercial quantum cryptography systems by tailored bright illumination, Nature Photonics 4, 686 (2010).
[13] 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, Nature Communications 2, 1 (2011).
[14] 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 Journal of Physics 13, 073024 (2011).
[15] X.-B. Wang, Z.-W. Yu, and X.-L. Hu, Twin-field quantum key distribution with large misalignment error, Physical Review A 98, 062323 (2018).
[16] 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).
[17] 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, Physical Review Letter 128, 190503 (2022).

[18] 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, Physical Review A 101, 042330 (2020).

[19] 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 Journal of Physics 23, 063038 (2021).

[20] R. Amiri, P. Wallden, A. Kent, and E. Andersson, Secure quantum signatures using insecure quantum channels, Physical Review A 93, 032325 (2016).

[21] J.-Q. Qin, C. Jiang, Y.-L. Yu, and X.-B. Wang, Quantum digital signatures with random pairing, Physical Review Applied 17, 044047 (2022).