Twin-field quantum key distribution with discrete phase randomization

Rong Wang,1, 2 Zhen-Qiang Yin,1, 2 Feng-Yu Lu,1, 2 Shuang Wang,1, 2 Wei Chen,1, 2 Wei Huang,3 Bing-Jie Xu,3 Guang-Can Guo,1, 2 and Zheng-Fu Han1, 2

1CAS Key Laboratory of Quantum Information, CAS Center for Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei 230026, China
2State Key Laboratory of Cryptology, P. O. Box 5159, Beijing 100878, P. R. China
3Science and Technology on Communication Security Laboratory, Institute of Southwestern Communication, Chengdu, Sichuan 610041, China

Twin-field quantum key distribution (TF-QKD) and its variant protocols are highly attractive due to its advantage of overcoming the well-known rate-loss limit for QKD protocols, i.e. $R \leq \log_2(1-\eta)$, with $\eta$ standing for the channel transmittance. These protocols can be divided into two types, with phase randomization from $[0, \pi]$ and without phase randomization in code mode. Here, we generalize the two types into a unified protocol, where Alice and Bob prepare coherent states with $2M \ (M \in \{1, 2, 3, \ldots\})$ different phases. Moreover, our security proof indicates that the achievable distance becomes longer with $M$ exponentially increasing, as a trade-off, the secret key rate will be lowered at short distance due to phase postselection. Numerical simulations show that the protocol with $M = 2$ may be the best choice in experiment.

I. INTRODUCTION

Quantum key distribution (QKD) provides two distant parties (Alice and Bob) a secure random bit string against any eavesdropper (Eve) guaranteed by the law of quantum mechanics. During last three decades, QKD has been developed both in theory and experiment, it is on the way to a wide range of implementation. Among all QKD experiments before, there are some fundamental limits, e.g., linear bound or Pirandola-Laurenza-Ottaviani-Banchi (PLOB) bound on secret key rate versus channel transmittance without quantum repeater.

Remarkably, twin-field (TF) QKD protocol, proposed by Lucamarini et al., is capable of overcoming this limit. TF-QKD, known as a measurement device independent (MDI) QKD type protocol, uses single-photon click rather than two-photon click in previous MDI-QKD to beat the limit. Because of this dramatic breakthrough, a variant of TF-QKD protocols have been proposed consequentially. Among these TF type QKD, phase-matching (PM) QKD protocol requires Alice and Bob to do continuous phase randomization in code mode. In other three protocols, Alice and Bob are only required to modulate two opposite phase randomly in code mode. By a fair comparison through numerical simulation, it seems that PM QKD protocol generates lower secret key at short distance but has longer transmission distance than the other three protocols. Intuitively, there may exist a more general TF type QKD to cover these four protocols above.

In this paper, inspired by the idea of discrete phase randomization of BB84 QKD protocol, we introduce a more general TF-QKD, in which Alice and Bob are required to modulate $2M$ discrete phase randomly in code mode. In other word, Alice and Bob encode classical bit "0", "1" in to phase $0$, $\pi$ respectively, then, randomize them by randomly adding a phase from $0, \pi/2, \pi, \ldots, (M - 1)\pi/2$. Besides, our protocol is suitable with and without post-selection in decoy mode.

We present a security proof for TF-QKD protocol with discrete phase randomization against collective attack, which has been proven as the most powerful attack in asymptotic scenarios. The security proof indicates that the transmission distance becomes longer with $M$ exponentially increasing, as a trade-off, the secret key rate will be lower at short distance. When $M$ tends to infinity, our protocol is almost same with PM-QKD, and the transmission distance comes to a limitation. Besides, numerical simulations show that the transmission distance can be almost expanded to the limit with $M = 2$.

This paper is organized as follows. In Sec. II, we describe details of TF-QKD protocol with discrete phase randomization. In Sec. III, we present the security proof of this protocol as well as an explicit formula for secure key rate. In Sec. IV, we analyze the secret key rate when choosing different $M$ and do numerical simulation with infinite decoy states. In Sec. V, we analyze its performance when post-selection in decoy mode is removed, which is quite convenient in experiment. Finally, in Sec. VI, we come to a conclusion.

II. PROTOCOL DESCRIPTION

Twin-field quantum key distribution protocol with discrete phase randomization runs as follows.

**PROTOCOL I**

Step 1. Alice and Bob randomly choose code mode or decoy mode in each trial.

Step 2. If a code mode is selected, Alice (Bob) randomly generates a key bit $k_a$ ($k_b$) and a random number $x$ ($y$) and then prepares the coherent state $|\alpha e^{i(k_a + x)\pi/2}\rangle$.
can be written as \( \phi \) and Bob can be written as \( \beta \) the composite states shared by Alice and Bob when they with discrete phase randomization. Firstly, we analyze where the fock state is defined as \( |\phi_k\rangle \). For each trial, only three from a pre-decided set.

Step 3. Alice and Bob send their quantum states to the untrusted receiver Eve. For each trial, only three outcomes are legal, which are "Only detector L clicks", "Only detector R clicks" and "No detectors click", another outcome "Both detectors click" is considered as "No detectors click", consequently, Eve announces one of the four outcomes.

Step 4. Alice and Bob repeat the above steps many times. Alice and Bob publicly announce which trials are code modes and which trials are decoy mode. For each trial that both Alice and Bob select code mode, the raw key bit is generated only if \( x = y \) and Eve announces a successful detection. Alice and Bob keep \( k_a, k_b \) as their raw key if Eve announces "Only detector L clicks". Bob flips his bit if Eve announces "Only detector R clicks". For each trial that both Alice and Bob select decoy mode, Alice and Bob announce \( \beta_a \) with random phase \( \phi_a \) and \( \beta_b \) with random phase \( \phi_b \), and only keep the trial that \( \beta_a = \beta_b \) and \( \phi_a - \phi_b = 0 \) or \( \pi \).

Step 5. Alice and Bob perform information reconciliation and privacy amplification to extract the final secure key.

III. SECURITY PROOF

Here, we present security proof of twin field protocol with discrete phase randomization. Firstly, we analyze the composite states shared by Alice and Bob when they both select the decoy mode. In the case of \( \beta_a = \beta_b = \beta \) and \( \phi_a = \phi_b = \phi \), the composite state of Alice and Bob can be written as

\[
\rho_{AB} = \frac{1}{2\pi} \int_0^{2\pi} d\phi \left| \beta e^{i\phi} \right\rangle \left\langle \beta e^{i\phi} \right| = \sum_{n=0}^\infty P_n |n, +\rangle \langle n, +| \]

(1)

where the fock state is defined as

\[
|n, +\rangle = \frac{1}{\sqrt{2^n n!}} (a^\dagger b^\dagger)^n |00\rangle_{AB} \]

(2)

with probability \( P_n \). In the case of \( \beta_a = \beta_b = \beta \) and \( \phi_a = \phi_b = \phi + \pi (\text{mod} 2\pi) = \phi \), the composite state of Alice and Bob can be written as

\[
\rho_{AB} = \frac{1}{2\pi} \int_0^{2\pi} d\phi \left| \beta e^{i\phi} \right\rangle \left\langle -\beta e^{-i\phi} \right| = \sum_{n=0}^\infty P_n |n, -\rangle \langle n, -| \]

(3)

where the fock state is defined as

\[
|n, -\rangle = \frac{1}{\sqrt{2^n n!}} (a^\dagger - b^\dagger)^n |00\rangle_{AB} \]

(4)

with probability \( P_n \).

In what follows, we concentrate on bounding Eve’s Holevo information. Eve’s general collective attack can be given by

\[
U_{EVE} = \sqrt{Y_{N,\pm}^L |\gamma_{n, \pm}^L \rangle \langle L|} + \sqrt{Y_{N,\pm}^R |\gamma_{n, \pm}^R \rangle \langle R|} + \sqrt{Y_{N,\pm}^N |\gamma_{n, \pm}^N \rangle \langle N|} \]

(5)

where state \( |e\rangle \) is Eve’s ancilla. Then, Eve is supposed to announce one of legal outcomes "Only detector L clicks" "Only detector R clicks" and "No detectors click" determined by her measurement results "\( |L|, |R|, |N| \)" respectively. In the case of \( \beta_a = \beta_b \) and \( \phi_a = \phi_b \), \( |\gamma_{n, \pm}^L \rangle, |\gamma_{n, +}^R \rangle \) and \( |\gamma_{n, -}^N \rangle \) are some arbitrary quantum states after Eve’s evolution, \( Y_{n,\pm}^L, Y_{n,\pm}^R, Y_{n,\pm}^N \) that satisfy the constraint \( Y_{n,\pm}^L + Y_{n,\pm}^R + Y_{n,\pm}^N = 1 \) are the yields, both of which are referred to Eve’s measurement results "\( |L|, |R|, |N| \)" respectively. Similarly in the case of \( \beta_a = \beta_b \) and \( \phi_a - \phi_b = \pi \), \( |\gamma_{n, \pm}^L \rangle, |\gamma_{n, \pm}^R \rangle \) and \( |\gamma_{n, \pm}^N \rangle \) are some arbitrary quantum states after Eve’s evolution, \( Y_{n,\pm}^L, Y_{n,\pm}^R, Y_{n,\pm}^N \) that satisfy the constraint \( Y_{n,\pm}^L + Y_{n,\pm}^R + Y_{n,\pm}^N = 1 \) are the yields, both of which are referred to Eve’s measurement results "\( |L|, |R|, |N| \)" respectively.

Without loss of generality, we firstly consider the secret key rate when her measurement result is "\( |L| \)". When Alice and Bob both select code mode, the initial prepared state \( |\alpha e^{i(k_a + \tilde{\pi})} \rangle \) and \( |\alpha e^{i(k_b + \tilde{\pi})} \rangle \), with keeping matched basis trials \( x = y \), can be given by

\[
|\alpha e^{i\tilde{\pi}} \rangle |\alpha e^{i\tilde{\pi}} \rangle = \sum_{n=0}^\infty \sqrt{P_n} e^{n(M+\tilde{\pi})} |n, +\rangle, k_a = k_b = 0
\]

\[
|\alpha e^{i\tilde{\pi}} \rangle |\alpha e^{i\tilde{\pi}} \rangle = \sum_{n=0}^\infty \sqrt{P_n} e^{n(M+\tilde{\pi})} |n, +\rangle, k_a = k_b = 1
\]

\[
|\alpha e^{i\tilde{\pi}} \rangle |\alpha e^{i\tilde{\pi}} \rangle = \sum_{n=0}^\infty \sqrt{P_n} e^{n(M+\tilde{\pi})} |n, -\rangle, k_a = 0, k_b = 1
\]

\[
|\alpha e^{i\tilde{\pi}} \rangle |\alpha e^{i\tilde{\pi}} \rangle = \sum_{n=0}^\infty \sqrt{P_n} e^{n(M+\tilde{\pi})} |n, -\rangle, k_a = 1, k_b = 0
\]

(6)

For the sake of simplicity, we define unnormalized states

\[
|\psi_{L/R,\pm}^{M+j,+} \rangle = \sum_{n=0}^\infty \sqrt{P_{2Mn+j} \sqrt{\frac{Y_{L/R,\pm}^{M+j}}{Y_{2Mn+j,\pm}}}} |L/R\rangle_{2Mn+j,\pm, \pm} \]

(7)

where \( j \in \{0, 1, 2, \ldots, 2M - 1\} \). We also define other unnormalized states composed by the states above

\[
|\psi_{L/R}^{\pm} \rangle = \sum_{j=0}^{M-1} e^{i(2j+1)x} |L/R\rangle_{2M+2j,\pm, \pm} \]

\[
|\psi_{L/R}^{\pm} \rangle = \sum_{j=0}^{M-1} e^{i(2j+1)x} |L/R\rangle_{2M+2j+1,\pm, \pm} \]

(8)

After Eve’s attack according to Eq.(5) and her announcing "\( |L| \)", Alice and Bob keep trials only if \( x = y \). Thus,
the state of Eve conditioned on Alice’s classical bit can be given by

$$\rho_{AE|x} = \frac{1}{2} |0\rangle_A \langle 0| \otimes (P(|\psi_{ex,+}^L\rangle + |\psi_{ox,+}^L\rangle)
+ P(|\psi_{ex,-}^L\rangle + |\psi_{ox,-}^L\rangle) + \frac{1}{2} |1\rangle_A \langle 1|
\otimes (P(|\psi_{ex,+}^L\rangle - |\psi_{ox,+}^L\rangle) + P(|\psi_{ex,-}^L\rangle - |\psi_{ox,-}^L\rangle))$$

(9)

where we define $P(|x\rangle) = |x\rangle \langle x|$. The probability of Alice obtaining a shifted key ($x = y$) in a code mode when Eve announces "$|L\rangle$" is

$$Q^L_x = \frac{1}{2} (|\psi_{ex,+}^L\rangle^2 + |\psi_{ox,+}^L\rangle^2 + |\psi_{ex,-}^L\rangle^2 + |\psi_{ox,-}^L\rangle^2)$$

(10)

When Eve announces "$|L\rangle$", an error click occurs if $k_a \otimes k_b = 1$, thus, the error rate of shifted key ($x = y$) is given by

$$e^L_x = \sum_{j} |\psi_{ex,-}^j\rangle^2 + |\psi_{ox,-}^j\rangle^2
= \frac{1}{2Q^L_x}$$

(11)

Thanks to the strong subadditivity of von Neumann entropy, Eve’s Holevo information with her announcing "$|L\rangle$" is given by

$$I^L_{AE|x} \leq -(1 - e^L_x) H\left(\frac{|\psi_{ex,+}^L\rangle^2}{2(1 - e^L_x)Q^L_x}\right) + e^L_x H\left(\frac{|\psi_{ex,-}^L\rangle^2}{2e^L_xQ^L_x}\right)$$

(12)

where $H(x) = -x \log_2 x -(1-x) \log_2 (1-x)$ is binary Shannon entropy. The condition for equality of Eq.(12) is that $|\psi_{ex,+}^L\rangle$, $|\psi_{ox,+}^L\rangle$, $|\psi_{ex,-}^L\rangle$, $|\psi_{ox,-}^L\rangle$ are mutually orthogonal with each other. For each trial that $x = y$ and Eve announces "$|L\rangle$", the secret key rate is given by

$$R^L_x = Q^L_x (1 - fH(e^L_x) - I^L_{AE|x})$$

(13)

where $f$ is error correction efficiency. What we need to do next is to calculate the average secret key rate for different $x$ when Eve announces "$|L\rangle$". Without considering sifting factor, the average secret key rate when Eve announces "$|L\rangle$" is given by

$$R^L = \frac{1}{M} \sum_{x=0}^{M-1} R^L_x = \frac{1}{M} \sum_{x=0}^{M-1} Q^L_x (1 - fH(e^L_x) - I^L_{AE|x})$$

(14)

We define average gain $Q^L$ and average error rate $e^L$ of shifted key, which are given by

$$Q^L = \frac{1}{M} \sum_{x=0}^{M-1} Q^L_x$$

$$e^L = \frac{\sum_{x=0}^{M-1} Q^L_x e^L_x}{\sum_{x=0}^{M-1} Q^L_x}$$

(15)

Thanks to the concavity of binary Shannon entropy, we utilize Jensen’s inequality to minimize $R^L$. For the second term of Eq.(12) on the right, we have

$$\frac{1}{M} \sum_{x=0}^{M-1} Q^L_x e^L_x \leq Q^L H\left(\frac{1}{M} \sum_{x=0}^{M-1} Q^L_x e^L_x\right) = Q^L H(e^L)$$

(16)

The condition for equality of Eq.(16) is that $e^L_0 = e^L_1 = \ldots = e^L_{M-1}$. Similarly, for the third term of Eq.(12) on the right, we have

$$\frac{1}{M} \sum_{x=0}^{M-1} Q^L_x I^L_{AE|x} \leq 0$$

(17)

where $I^L_{AE}$ is defined by Eq.(17). Consequently, we have

$$R^L \geq Q^L (1 - fH(e^L) - I^L_{AE})$$

(18)

When Eve’s measurement result is "$|R\rangle$", the analysis of secret key rate is almost same with the ones when she announces "$|L\rangle$". Thus, the secret key rate when Eve announces "$|R\rangle$" is given by

$$R^R \geq Q^R (1 - fH(e^R) - I^R_{AE})$$

(19)

where $I^R_{AE}$ is given by

$$I^R_{AE} = (1 - e^R) H\left(\frac{\sum_{j=0}^{M-1} |\psi_{2M+2j,-}^R\rangle^2}{2(1 - e^R)Q^R}\right)
+ e^R H\left(\frac{\sum_{j=0}^{M-1} |\psi_{2M+2j,-}^R\rangle^2}{2e^RQ^R}\right)$$

(20)

The trials when Eve’s measurement result is "$|N\rangle$" will not contribute to the secret key. Thus, the total secret key rate is $R = R^L + R^R$. The total gain and total error rate of shifted key are given by

$$Q = Q^L + Q^R$$

$$e = \frac{Q^L e^L + Q^R e^R}{Q}$$

(21)
In order to find the lower bound of the total secret key rate $R$, we utilize the technique as well as Eq.(16) and Eq.(17). Thus, we have

$$Q^L H(e^L) + Q^R H(e^R) \leq Q H\left(\frac{Q^L e^L + Q^R e^R}{Q}\right) = Q H(e)$$

The condition for equality of Eq.(22) is that $e^L = e^R = e$. Similarly, we have

$$Q^L I_{AE}^L + Q^R I_{AE}^R \leq Q[(1-e)H\left(\sum_{j=0}^{M-1} \left|\psi_{2M+2j,-}^L\right|^2 + \left|\psi_{2M+2j,0}^R\right|^2\right)$$

$$2(1-e)Q + eH\left(\sum_{j=0}^{M-1} \left|\psi_{2M+2j,-}^R\right|^2 + \left|\psi_{2M+2j,0}^R\right|^2\right)\right]$$

$$= Q I_{AE}$$

Consequently, the total secret key rate formula can be expressed by

$$R \geq \frac{1}{M} Q(1 - fH(e) - I_{AE})$$

where $I_{AE}$ is defined by Eq.(23), $1/M$ is the shifting factor.

The problem finding the lower bound of the total secret key rate can be converted into finding the upper bound of $I_{AE}$.

$$I_{AE} = (1-e)H\left(\sum_{j=0}^{M-1} \left|\psi_{2M+2j,-}^L\right|^2 + \left|\psi_{2M+2j,0}^R\right|^2\right)$$

$$2(1-e)Q + eH\left(\sum_{j=0}^{M-1} \left|\psi_{2M+2j,-}^R\right|^2 + \left|\psi_{2M+2j,0}^R\right|^2\right)\right]$$

$$\leq \sum_{n=0}^{\infty} \sqrt{P_{2Mn+j}} Y_{2Mn+j,\pm}^{L/R} \leq \sum_{n=0}^{\infty} \sqrt{P_{2Mn+j}}$$

$$\sum_{j=0}^{M-1} \left|\psi_{2M+2j,-}^L\right|^2 + \left|\psi_{2M+2j,0}^L\right|^2 = 2(1-e^L)Q^L$$

$$\sum_{j=0}^{M-1} \left|\psi_{2M+2j,0}^L\right|^2 + \left|\psi_{2M+2j,1}^L\right|^2 = 2e^L Q^L$$

$$\sum_{j=0}^{M-1} \left|\psi_{2M+2j,-}^R\right|^2 + \left|\psi_{2M+2j,0}^R\right|^2 = 2(1-e^R)Q^R$$

$$\sum_{j=0}^{M-1} \left|\psi_{2M+2j,0}^R\right|^2 + \left|\psi_{2M+2j,1}^R\right|^2 = 2e^R Q^R$$

With another constraint given by Eq.(21), we can finally find the maximum of $I_{AE}$.

### IV. SIMULATION

In this section, we simulate the performance of TF-QKD with discrete phase modulation. The simulation parameters are given in Table I. In ideal case, Alice and Bob can estimate $Y_{n,\pm}^{L/R}$ precisely by infinite decoy-state method.

We assume that the transmission efficiency of channel losses and detection efficiencies is $\eta$ and dark counting rate of single photon detectors (SPD) is $d$ per trial. Assuming the mean photon number of each pulse emitted by Alice and Bob is $\mu$, the counting rate is given by

$$Q = (1-d)(1-e^{-2\eta \mu}) + 2d(1-d)e^{-2\eta \mu}$$

$$= (1-d)(1-e^{-2\eta \mu} + 2de^{-2\eta \mu})$$

We assume that the optical misalignment is $e_{mis}$, the error rate should be

$$e = \frac{(1-d)[e_{mis} - (e_{mis} - d)e^{-2\eta \mu}]}{Q}$$

Applying infinite decoy states, $Y_{n,\pm}^{L/R}$ can be given by

$$Y_{n,+}^{L} = Y_{n,-}^{R} = (1-d)[1 - e_{mis} - (1 - e_{mis} - d)(1 - \eta)^n]$$

$$Y_{n,-}^{L} = Y_{n,+}^{R} = (1-d)[e_{mis} - (e_{mis} - d)(1 - \eta)^n]$$

With Eq.(28), we can reconstruct Eve’s Holevo information $I_{AE}$ and its constraint. We define

$$Y_{n,+}^{c} = Y_{n,-}^{c} = \frac{1}{2} \left|\psi_{2M+2j,0}^L\right|^2 + \left|\psi_{2M+2j,1}^L\right|^2$$

$$X_{2M+j}^{c} = \frac{1}{2} \left|\psi_{2M+2j,-}^L\right|^2 + \left|\psi_{2M+2j,0}^L\right|^2$$

$$X_{2M+j}^{c} = \frac{1}{2} \left|\psi_{2M+2j,-}^R\right|^2 + \left|\psi_{2M+2j,0}^R\right|^2$$

Thus, we have an equivalent expression of $I_{AE}$ and its

| TABLE I. Parameters | Values |
|---------------------|-------|
| Dark count rate $d$ | $8 \times 10^{-8}$ |
| Error correction efficiency $f$ | 1.15 |
| Detector efficiency $\eta_d$ | 14.5% |
| Misalignment error $e_{mis}$ | 1.5% |
constraint.

\[ I_{AE} = (1 - e)H\left(\sum_{j=0}^{M-1} \frac{X_j^e}{(1 - e)Q}\right) + eH\left(\sum_{j=0}^{M-1} \frac{X_j^e}{eQ}\right) \]

\[ 0 \leq X_j^e \leq \left| \sum_{n=0}^{\infty} \sqrt{P_{2Mn+j}^e Y_{2Mn+j}^e}\right|^2 \]

\[ 0 \leq X_j^e \leq \left| \sum_{n=0}^{\infty} \sqrt{P_{2Mn+j}^e Y_{2Mn+j}^e}\right|^2 \]

\[ \sum_{j=0}^{M-1} X_j^e + X_{j+1}^e = (1 - e)Q \]

\[ \sum_{j=0}^{M-1} X_j^e + X_{j+1}^e = eQ \]

For the sake of analyzing \( I_{AE} \), we define the upper bound of \( \sum_{j=0}^{M-1} X_j^e \) as a function for positive integer \( M \), which is given by

\[ F^{c/e}(M) = \sum_{j=0}^{M-1} \sum_{n=0}^{\infty} \sqrt{P_{2Mn+j}^e Y_{2Mn+j}^e}\]  \( \) (31)

As binary Shannon entropy \( H(x) \) increases when \( 0 \leq x \leq 1/2 \) and decreases when \( 1/2 < x < 1 \), it’s sufficient to consider the case of \( F^c(M) \leq (1 - e)Q/2 \) and \( F^c(M) \leq eQ/2 \) when finding the upper bound of \( I_{AE} \). It’s easy to prove that

\[ F^{c/e}(1) \geq F^{c/e}(M) \geq F^{c/e}(NM) \geq F^{c/e}(\infty) \]  \( \) (32)

where \( N \) is a positive integer. With \( M \) exponentially increasing, the upper bound of \( I_{AE} \) decreases to the extend that the transmission distance become longer, as a trade-off, the sifting cost grows so that secret key rate decreases at short distance. When \( M \) tends to infinity, the transmission distance come to a limitation. With several special \( M \), we present the numerical simulations of secret key rate in Fig.1 and the maximal channel loss in Table II.

If we remove the sifting efficiency, the limitary channel loss with \( M \to \infty \) is 81.5 dB as it’s showed in Table II. As we can see in Fig.1, it’s sufficient to apply TF-QKD with \( M = 2 \) that it almost reaches the liminary transmission distance at the cost of about half of secret key rate at short distance.

Here, we consider the relationship with several varietal TF-QKD protocol \( [12, 14–16] \). When \( M \to \infty \), our protocol is exactly the PM-QKD \( [12] \) if we relax the post-selection condition \( |\phi_a - \phi| = 0 \) or \( \pi \) and add a corresponding sifting factor. When \( M = 1 \), our protocol is same with \( [14, 15] \) in code mode, the difference is the way to estimate the information leakage or the ”phase error”. To some extent, TF-QKD protocol with discrete phase randomization cover the four varietal TF-QKD protocol above.

### TABLE II. The maximal channel loss with different \( M \).

| \( M \) | The maximal channel loss (dB) |
|-------|-----------------------------|
| 1     | 72.3                        |
| 2     | 80.8                        |
| 4     | 81.3                        |
| \( \infty \) | 81.5                        |

![FIG. 1. Secret key rate R versus channel loss: The curves represent the secure key rate of TF-QKD protocol for \( M = 1, M = 2, M = 4 \) and the PLOB bound respectively. We do not show the case of \( M \to \infty \) because the key rate tends to 0](image)

V. REMOVING POST-SELECTION IN DECOY MODE

For the simplicity in experiments, we can remove post-selection in decoy mode in our protocol. Secutity proof shows that the simplified protocol resrve the capability of overcoming PLOB bound. Raw key generation in simplified protocol runs as follows.

**PROTOCOL II**

Step 1. Same as Protocol I

Step 2. Same as Protocol I

Step 3. Alice and Bob send their quantum states to the untrusted receiver Eve. For each trial, only three outcomes are legal in code mode, which are ”Only detector \( L \) clicks”, ”Only detector \( R \) clicks” and ”No detectors click”, another outcome ”Both detectors click” is considered as ”No detectors click”, consequently, Eve announces one of the four outcomes. For each trial that both Alice and Bob select decoy mode, the outcome ”Both detectors click” is considered as an legal outcome.

Step 4. Alice and Bob repeat the above steps many times. Alice and Bob publicly announce which trials are code modes and which trials are decoy mode. For each trial that both Alice and Bob select code mode, the raw key bit is generated only if \( x = y \) and Eve announces a successful detection. Alice and Bob keep \( k_a, k_b \) as their raw key if Eve announces ”Only detector \( L \) clicks”. Bob filps his bit if Eve announces ”Only detector \( R \) clicks”. 
For each trial that both Alice and Bob select decoy mode, the yield $Y'_{n,m}$, probability of Eve announcing the outcome "Detectors click" provided Alice emits $n$-photon state and Bob emits $m$-photon state, can be estimated. The outcome "Detectors click" includes "Only detector $L$ clicks" "Only detector $R$ clicks" and "Both detectors click".

Step 5. Same as Protocol I

The security proof of this simplified protocol is same as the one with post-selection in decoy mode. In simplified protocol, however, we can get a upper bound of $Y_{c/e}^n$ by infinite decoy states rather than estimate it exactly, which is given by

$$\sqrt{Y_{L/R}^{n/2}} \leq \sum_{k=0}^{n} \sqrt{\frac{C^k}{2^n}} Y'_{k,n-k}$$

$$\text{(33)}$$

Similarly, with Eq.(30), we present the numerical simulations of secret key rate in Fig.2 and the maximal channel loss in Table III for the simplified protocol. We get an analogous result compared to the protocol with post-selection in decoy mode. In simplified protocol, the limital channel loss with $M \to \infty$ is 75.8 dB showed in Table III when removing the sifting efficiency. As we can see in Fig.2, it’s sufficient to apply this simplified TF-QKD with $M = 2$ that it almost reaches the limital transmission distance at the cost of about half of secret key rate at short distance. When we compare our protocol with and without post-selection in decoy mode, the latter one does not require post-selection in decoy mode, as a trade-off, the maximal channel loss will be lower.

VI. CONCLUSION

In summary, we have introduced a TF type QKD with discrete phase randomization and proven its security in asymptotic scenarios. Our protocol can be viewed as a generalization of the four varietal TF-QKD protocol to some extent. The security proof discloses that the transmission distance become longer with $M$ exponentially increasing, as a trade-off, the secret key rate will be lower at short distance. When $M$ tends to infinity, the transmission distance come to a limitation. Numerical simulations show that it’s sufficient to apply TF-QKD with $M = 2$, for it almost reaches the limital transmission distance at the cost of about half of secret key rate, compared with the case of $M = 1$, at short distance. Post-selection in decoy mode is not convenient in experiment, thus, we remove it to make experiments more simpler in a modified protocol. We find that the removal of post-selection in decoy mode has very limited influence on the secret key rate and achievable distance. Our findings expect TF-QKD can be run with optimal phase randomization actively, i.e. at short distance one can simply bypass phase randomization while a phase randomization of 0 or $\pi/2$ is sufficient at long distance case.

VII. NOTE ADDED

During the preparation of this paper, we find that Pri-

maatmaja et al. proposed an open question that if coding phase in TF-QKD under different bases can improve secret key rate significantly. Their idea is similar with our proposal of discrete phase randomization in some sense.

ACKNOWLEDGMENTS

This work has been supported by the National Key Research and Development Program of China (Grant No. 2016YFA0302600), the National Natural Science Foundation of China (Grant Nos. 61822115, 61775207, 61702469, 61771439, 61622506, 61627820, 61575183), National Cryptography Development Fund (Grant No. MMJJ20170120) and Anhui Initiative in Quantum Information Technologies.
[1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, Bangalore, India (IEEE, New York, 1984) pp. 175–179.
[2] A. K. Ekert, Phys. Rev. Lett. 67, 661 (1991).
[3] K. Inoue, E. Waks, and Y. Yamamoto, Phys. Rev. Lett. 89, 037902 (2002).
[4] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. 108, 130503 (2012).
[5] C. Gobby, Z. L. Yuan, and A. J. Shields, Appl. Phys. Lett. 108, 3762 (2004).
[6] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, Phys. Rev. Lett. 96, 070502 (2006).
[7] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, Nat. Photonics. 115, 160502 (2013).
[8] C. Wang, X.-T. Song, Z. Q. Yin, S. Wang, W. Chen, C.-M. Zhang, G.-C. Guo, and Z.-F. Han, Phys. Rev. Lett. 115, 160502 (2015).
[9] M. Takeoka, S. Guha, and M. M. Wilde, Nat. Commu. 8, 5235 (2014).
[10] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Nat. Commu. 8, 15043 (2017).
[11] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Nature. 557, 400 (2018).
[12] X. Ma, P. Zeng, and H. Zhou, Phys. Rev. X. 8, 031043 (2018).
[13] X.-B. Wang, Z.-W. Yu, and X.-L. Hu, Phys. Rev. A. 98, 062323 (2018).
[14] C. Cui, Z. Q. Yin, R. Wang, W. Chen, S. Wang, G. C. Guo, and Z. H. Han, Phys. Rev. Applied. 11, 034053 (2019).
[15] M. Curty, K. Azuma, and H.-K. Lo, arXiv preprint arXiv:1807.07667 (2018).
[16] J. Lin and N. Lütkenhaus, Phys. Rev. A. 98, 042332 (2018).
[17] H. L. Yin and Z. B. Chen, arXiv preprint arXiv:1901.05009 (2019).
[18] Z. Cao, Z. Zhang, H.-K. Lo, and X. Ma, New J. Phys 17, 053014 (2015).
[19] W. Y. Hwang, Phys. Rev. Lett. 91, 057901 (2003).
[20] H.-K. Lo, X. F. Ma, and K. Chen, Phys. Rev. Lett. 94, 230504 (2005).
[21] X.-B. Wang, Phys. Rev. Lett. 94, 230503 (2005).
[22] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Phys. Rev. A. 72, 012326 (2005).
[23] R. Renner, *Security of Quantum Key Distribution*, Ph.D. thesis, SWISS FEDERAL INSTITUTE OF TECHNOLOGY ZURICH (2005).
[24] I. W. Primaatmaja, E. Lavie, K. T. Goh, C. Wang, and C. C. W. Lim, arXiv preprint arXiv:1901.01942 (2019).