Improving the performance of Twin-Field Quantum Key Distribution

Feng-Yu Lu, Zhen-Qiang Yin, Chao-Han Cui, Guan-Jie Fan-Yuan, Rong Wang, Shuang Wang, Wei Chen, De-Yong He, Guang-Can Guo, and Zheng-Fu Han

CAS Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei 230026, P. R. China
Synergetic Innovation Center of Quantum Information & Quantum Physics, University of Science and Technology of China, Hefei, Anhui 230026, P. R. China and
State Key Laboratory of Cryptology, P. O. Box 5159, Beijing 100878, P. R. China

(Dated: February 13, 2019)

Twin-Field Quantum Key Distribution (TF-QKD) protocol and its variants, e.g., Phase-Matching QKD (PM-QKD), Sending-or-Not QKD and TF-QKD without phase post-selection, can overcome the rate-distance limit without the help of quantum repeaters. Among all of these protocols, the TF-QKD without phase post-selection enjoys higher key rate and simplicity in practice since the post-selection of global phases is removed. However, its achievable distance is shorter compared with the original PM-QKD. In this work, we propose to improve its performance by introducing an additional decoy mode. With the help of this, the upper bound of the information leakage can be estimated more tightly, and then both the key rate and achievable distance are significantly improved. Interestingly, the proposed additional decoy mode does not need phase randomization and work well in finite decoy-state cases, which is quite meaningful in practice.

I. INTRODUCTION

Quantum Key Distribution (QKD) [1] allows two remote users, called Alice and Bob, to share secret random keys with information-theoretic security [2-5] which is guaranteed by principles of quantum physics, even if there is an eavesdropper, Eve.

With the developments of QKD in both theory and experiment, QKD implementations with longer achievable distance [6, 7] and higher secret key rate (SKR) [8-10] were realized. However, all these implementations must obey some limits on SKR versus channel transmittance [11, 12]. Moreover, SKR of any “repeaterless” QKD system cannot overcome the linear bound (also called PLOB bound) [11]. Surprisingly, a recently proposed protocol called Twin-Field Quantum Key Distribution (TF-QKD) [13] and its variants, e.g., Phase-Matching QKD (PM-QKD) [14], Sending-or-Not QKD [15] and TF-QKD without phase post-selection (we will call it NPP-TFQKD in the following, which is the abbreviation of no phase post-selection TF-QKD) [16-18] can overcome this bound, which means the performance of QKD may be significantly improved without the need of quantum repeaters. What’s more, these protocols have been proved to be immune to all potential side-channel attacks to measurement device, just like the original measurement-device-independent protocol [19].

In the original TF-QKD and PM-QKD, Alice (Bob) encodes key bit as the 0 or \( \pi \) phase of weak coherent optical pulse, adds an additional random phase \( \alpha_A(\alpha_B) \), and send it to an untrusted middle station which interferes the incoming pulses. Upon receiving the message from middle station, Alice and Bob postselect the trials satisfying \( \alpha_A \approx \alpha_B \) to generate secret key bits. The post-selection of \( \alpha_A \approx \alpha_B \) inevitably degrades the SKR and make the postprocessing more complicated. To overcome this problem, Cui et al. proposed NPP-TFQKD [10].

Soon after, two other groups independently proposed similar schemes [17, 18]. In Ref. [16], the flow of NPP-TFQKD is divided into code mode and decoy mode. The first one which is run without adding random phase \( \alpha_A(\alpha_B) \), can be used to generate key bit. The latter one is just used to monitor the security. Since the phase randomization and post-selection are removed in the code mode, its SKR is significantly improved. However, its achievable distance is much shorter than PM-QKD. In the similar scheme proposed by Ref. [18], the achievable distance is increased by infinite decoy-states, which is not feasible in practice.

In this work, we propose a practical method to significantly improve the performance of NPP-TFQKD. Our work is mainly based on the Ref. [16]. The core of our method is introducing an additional decoy mode in NPP-TFQKD protocol. This new decoy mode is run with the same phase of code mode and can be used to estimate the information leakage \( I_{AE} \) tightly. As a result, the achievable distance is increased.

The rest of this paper is organized as follows. In Sec. II, we briefly introduce the flow of NPP-TFQKD and its method to calculate upper bound of \( I_{AE} \) in Ref. [16]. An intuitive explanation on why this upper bound is too loose is also given here. In Sec. III, we will detailly introduce our new method, which keeps the superiority of higher SKR, longer distance and practicability at same time.

II. TF-QKD WITHOUT PHASE POST SELECTION

The process of NPP-TFQKD is described as follows. [10]

Step1. Measurement: Alice and Bob randomly choose...
code mode or decay mode. When choosing code mode, Alice(Bob) prepare a initial phase locked WCS with intensity $\mu$, randomly modulate 0 or $\pi$ phase. We define $Q^c_\mu$ as gain of code mode. When choosing decay mode, they prepare phase randomized WCS and randomly choose an intensity from pre-decided set. Then they send the modulated quantum state to the untrusted party Charlie for interference measurement. Note that the randomized phase in the decay mode is not publicly announced, and Alice and Bob actually prepare mixed state in photon number space as Eq.4 there $\omega_1$ and $\omega_2$ denote, respectively, the intensity chose by Alice and Bob, respectively. The gain of $\rho_{\omega_1} \otimes \rho_{\omega_2}$ is denoted as $Q^d_{\omega_1\omega_2}$ and The yield of $(|m\rangle \otimes |n\rangle \langle n|)$ is denoted as $Y_{m,n}$. The relation between them is showed in Eq.2

$$\rho_{\omega_1} \otimes \rho_{\omega_2} = \sum_{m=0}^{\infty} \sum_{n=0}^{\infty} (p^{\omega_1}_m |m\rangle \langle m|) \otimes (p^{\omega_2}_n |n\rangle \langle n|)$$  

(1)

$$Q^d_{\omega_1\omega_2} = \sum_{m=0}^{\infty} \sum_{n=0}^{\infty} p^{\omega_1}_m p^{\omega_2}_n Y_{m,n}$$  

(2)

**Step 2.** Announcement: For each trail, Charlie must publicly announce the detector (L or R) that click or failure.

**Step 3.** Sifting: Alice and Bob repeat the above steps many times, then they publicly announce which trails are code mode and which are decay mode. For the trials they both choose code mode and Charlie announces success event(L or R clicked), the raw key bit are generated. They record $\kappa_a$ and $\kappa_b$ as their raw key. They keep their raw key bit only when both of them send code mode and Bob needs to flip his $\kappa_b$ when Charlie’s announcement is ‘R’ or $|\phi_a - \phi_b|$ = $\pi$. Then they get the sifted key.

**Step 4.** Parameters estimation: Alice and Bob estimate the gains $Q^c_\mu$ and quantum bit error rate(QBER) $E_p^c$ from sifted keys and they calculate the upper bound of mutual information of Alice and Eve $T_{AE}$. Then they can calculate lower bound of SKR by Eq.6 Where $H(p) = -p \log_2 p - (1-p) \log_2 (1-p)$ is shannon entropy.

**Step 5.** Key distillation: Alice and Bob generate their secure key by doing error correction and privacy amplification in the sifted key.

$$R = Q^c_\mu [1 - f H(E_p^c) - T_{AE}]$$  

(3)

In Ref.[10], the upper bound of information leakage $T_{AE}$ depends on $|\gamma_{n,m}|$, which is defined as the state of Eve’s ancilla in case of Alice and Bob sending Fock states $|n\rangle$ and $|m\rangle$ respectively. Then we define four intermediate states labeled by the photon-number’s parity of Alice and Bob’s output. The relation of $I_{AE}$ and these intermediates is showed in Eq.6

$$I_{AE} \leq h(\frac{||\psi_{ee}||^2}{Q_\mu}, \frac{||\psi_{oe}||^2}{Q_\mu}, \frac{||\psi_{oo}||^2}{Q_\mu}, \frac{||\psi_{eo}||^2}{Q_\mu})$$  

(5)

Where $h(x, y) = -x \log_2 x - y \log_2 y + (x + y) \log_2 (x + y)$ denotes the Von Neumann entropy.

Noting that the values of inner product $(|\gamma_{n,m}| \langle \gamma_{n,m} |) (m, n \neq k, l)$ are unknow, we have to estimate the bound these $\psi_{xy} (x, y \in \{0, e\})$. The constraints are showed in Eq.6

**III. METHOD TO IMPROVE THE DISTANCE OF NPP-TFQKD**

By observing the constraints in Eq.7, we have an intuition that it estimate $I_{AE}$ excessively. Let’s take the upper bound of $||\psi_{ee}||^2$ as an example. The $||\psi_{ee}||^2$ can be regarded as two parts.
\[ \left| \langle \psi_{ee} \rangle \right|^2 = \Omega_{ee}^\mu + \Phi_{ee}^\mu \]  

(8)

The first part consists of those inner products whose subscript of bra and ket are same. We denote this part by \( \Omega_{ee}^\mu \) and call it non-cross term.

\[
\Omega_{ee}^\mu = \sum_{n,m=0}^{\infty} \sum_{k=0,\ell=0}^{m+1} \sqrt{p_{n2m}^\mu p_{2m}^\mu p_{2k}^\mu p_{2l}^\mu} \gamma_{2n,2m} \gamma_{2k,2l} \]

(9)

\[
\Phi_{ee}^\mu = \sum_{n,m=0}^{\infty} \sum_{k=0,\ell=0}^{m+1} \sqrt{p_{n2m}^\mu p_{2m}^\mu p_{2k}^\mu p_{2l}^\mu} \zeta_{2n,2m,2k,2l} \gamma_{2n,2m} \gamma_{2k,2l} \zeta_{2n,2m,2k,2l} \]

(10)

The symbol \( \zeta_{n,m,k,l} \) above is defined as \( \gamma_{n,m} \gamma_{k,l} + \gamma_{k,l} \gamma_{n,m} \). Noting that \( \zeta_{n,m,k,l} = 2Re(\gamma_{n,m} \gamma_{k,l}) \), \( \zeta \) must be a real number in range of \([-2,2]\). Compared with Eq(7) we can find the original upper bound replace all \( \zeta_{n,m,k,l} \) as 2, which is the worst situation. The influence of this replacement can be fatal when channel loss is large. It’s the main reason why the distance of NPP-TFQKD is shorter than PM-QKD. It’s naturally for us to consider if there is any method to estimate \( T_{AE} \) tighter and keep the practicability of the protocol at same time. Fortunately, the answer is yes. We will introduce our new method detailedly as following.

### A. Introduction of the new constraint conditions

By observing Eq(2) and the fifth constraint condition in Eq(7) we can find the gains \( Q \) is very different when Alice Bob both choose decoy mode or choose code mode since the phase randomize eliminate all cross terms.

\[
Q^d_{\omega_1 \omega_2} = \Omega_{ee}^\mu + \Omega_{cc}^\mu + \Omega_{cc}^\mu + \Omega_{cc}^\mu + \Phi_{ee}^\mu + \Phi_{ee}^\mu + \Phi_{ee}^\mu
\]

(11)

Define \( x_{n,m,k,l} = \zeta_{n,m,k,l} \sqrt{Y_{n,m} Y_{k,l}} \) as variables and let \( \delta_{\omega_1 \omega_2} = Q^d_{\omega_1 \omega_2} - Q^d_{\omega_1 \omega_2} \), we obtain a new linear equation.

\[
\delta_{\omega_1 \omega_2} = \Phi_{ee}^\mu + \Phi_{eo}^\mu + \Phi_{oe}^\mu + \Phi_{oo}^\mu
\]

(12)

\[
= \sum_{n,m=0}^{\infty} \sum_{k=0}^{\infty} \{ \sqrt{p_{n2m}^\mu p_{2m}^\mu p_{2k}^\mu p_{2l}^\mu} X_{2n,2m,2k,2l} + \sqrt{p_{n2m}^\mu p_{2m}^\mu p_{2k}^\mu p_{2l}^\mu} X_{2n,2m,2k,2l} + \sqrt{p_{n2m}^\mu p_{2m}^\mu p_{2k}^\mu p_{2l}^\mu} X_{2n,2m,2k,2l} + \sqrt{p_{n2m}^\mu p_{2m}^\mu p_{2k}^\mu p_{2l}^\mu} X_{2n,2m,2k,2l} \}
\]

\[
x_{n,m,k,l} \in [ -2 \sqrt{Y_{n,m} Y_{k,l}}, 2 \sqrt{Y_{n,m} Y_{k,l}} ]
\]

Similar to the principle of infinity decoy state method \([20–22]\), we can get a linear equation set include infinite linear equations when using infinite intensities. By solving the linear equation set, all \( x_{n,m,k,l} \) can be known. Especially, in the ideal situation, there should be \( Q^d_{\omega_1 \omega_2} = Q^d_{\omega_1 \omega_2} \). i.e. all equations in Eq(12) is equal to zero. That is to say, the solution of Eq(12) is all \( x_{n,m,k,l} \) is zero. That is to say, the cross term \( \Phi_{ee}^\mu \) in Eq(7) is zeros. We simulate the performance of several kinds of TF-QKD with parameters showed in Tab.II the result is showed in Fig.I. In infinite decoy-state method, our new method contains the superiority of higher SKR belongs to original NPP-TFQKD and longer communication distance belongs to PM-QKD at the same time. In Tab.II

![Figure 1](https://via.placeholder.com/150)

**FIG. 1.** SKR versus communication distance, the blue, red and yellow solid line are, respectively, the performance of the original NPP-TFQKD, our improved NPP-TFQKD and PM-QKD. The purple dash line denotes linear bound

Avoiding causing ambiguity, we modify the Step.1 and Step.4 of NPP-TFQKD as follows.

**New Step.1.** Measurement: Alice and Bob randomly choose **decoy mode.1, decoy mode.2 or code mode**.When choosing **code mode**, Alice(Bob) prepare a initial phase locked WCS with intensity \( \mu \), randomly...
modulate 0 or $\pi$ phase. The gain in this mode is denoted by $Q_{\mu}^c$. When choosing **decoy mode.1**, they prepare phase randomized WCS and randomly choose a intensity from pre-decided set $I_1$. The gain in this mode is denoted by $Q_{\omega_1\omega_2}^{d1}$. The process of **decoy mode.2** is the same as **code mode**, except they should randomly choose an intensity from pre-decided set $I_2$ which is the subset of $I_1$. The gain in this mode is denoted by $Q_{\omega_1\omega_2}^{d2}$.

**New Step4.** Parameters estimation: Alice and Bob estimate the gains $Q_{\mu}^c$ and quantum bit error rate(QBER) $E_0^c$ from sifted keys and they calculate $T_{AE}$ by our new method. Then we can calculate a tighter lower bound of SKR.

### B. Improved NPP-TFQKD in practice

The infinite decoy-state method is not practically useful. In this subsection, we modify the infinite intensities method into 5-intensities in decoy mode.1 and 4-intensities in decoy mode.2. In order to facilitate the understanding, we will introduce the method in two steps. In first step, we use 4 intensities in decoy mode.2 but keep infinite intensities in decoy mode.1 to prove that we can still obtain a good upper bound of cross terms even if there is only a few equations in Eq.12. In second step we will analyze the problems and our solutions of using a few intensities in both decoy mode.1 and decoy mode.2.

**Infinite decoy mode.1 and four intensities decoy mode.2:**

Assume that we use infinite intensities in decoy mode.1, i.e. all yields $Y_{ij}$ are known value, and only use four intensities($\mu$, $\nu_1$, $\nu_2$) in decoy mode.2. The $\mu$ is intensity used in code mode here. There are totally 16 combinations and we can get an equation set includes 16 linear equations as Eq.12 we estimate totally 14 upper bound of cross terms, i.e. $\Phi_{ab}^\mu$, $\Phi_{cd}^\mu$, $\Phi_{-ab}^\mu$. Where $\Phi_{ab}^\mu$ denote the upper bound of $\Phi_{ab}^\mu$, $\Phi_{cd}^\mu$, $\Phi_{-ab}^\mu$ is the upper bound of $Q_{\mu}^d - Q_{\mu}^d - \Phi_{ab}^\mu$. a, b, c, d $\in \{e, o\}$. As showed in Fig.2 compared with the original infinite (blue solid line), the ‘infinite decoy mode.1 and 4-decoy mode.2’ method(red dash line) can’t improve the SKR in small channel loss, but can greatly improve the communication distance.

Then we obtain the $T_{AE}$ by more constraints as showed in Eq.13

$$
\begin{align*}
&\begin{cases}
\Omega_{ab}^\mu - |\Phi_{ab}^\mu| \leq x_{ab} \leq \Omega_{ab}^\mu + |\Phi_{ab}^\mu|, \\
x_{ab} + x_{cd} \leq \Omega_{ab}^\mu + \Omega_{cd}^\mu + |\Phi_{-ab}^\mu|, \\
Q_{\mu}^c - x_{ab} \leq Q_{\mu}^d - \Omega_{ab}^\mu + |\Phi_{ab}^\mu|, \\
x_{ee} + x_{oc} + x_{oo} + x_{eo} = Q_{\mu}^c.
\end{cases} \\
s.t. &
\begin{cases}
h(x_{ee} Q_{\mu}^d Q_{\mu}^c + h(x_{oc} Q_{\mu}^d Q_{\mu}^c)
\end{cases}
\end{align*}
$$

where $a, b, c, d \in \{e, o\}$; $ab \neq cd$

$T_{AE} = \max \{x_{ee} Q_{\mu}^d Q_{\mu}^c + h(x_{oc} Q_{\mu}^d Q_{\mu}^c)\}$

![Fig. 2. SKR versus communication distance, the orange and blue solid line denote, respectively, the performance of our improved NPP-TFQKD with infinite intensities in both decoy mode.1 and decoy mode.2, and the performance of original NPP-TFQKD with infinite decoy-state method. The red dash line is our method with infinite decoy mode.1 and infinite decoy mode.2. The yellow dot-dash line denotes the linear bound.](image)

**Five intensities decoy mode.1 and four intensities decoy mode.2:** Using infinite intensities in decoy mode.1 is still not practical. Here, we will give the method of using a few intensities in both decoy modes. Using finite decoy mode.1 means that we can’t obtain the true values of $Y_{m,n}$ and non-cross terms $\Omega_{ab}$ any more, where subscript $a, b \in \{e, o\}$. Using linear program to solve the linear equation set Eq.14 we can get the upper bound of $Y_{m,n}$ and $\Omega_{ab}$. There are $n^2$ linear equations in Eq.14 when using $n$ intensities in decoy mode.1, and $Y_{m,n}$ and $\Omega_{ab}$ denote the upper bound of $Y_{m,n}$ and $\Omega_{ab}$.

$$
\begin{align*}
&\begin{cases}
Q_{\omega_1\omega_2}^{d1} = \sum_{m=0}^{\infty} \sum_{n=0}^{\infty} P_m P_n Y_{m,n}; \\
Y_{m,n} \in [-1, 1]; \\
\omega_1, \omega_2 \in \{\mu, \nu_1, \nu_2, \nu_3, \ldots\}
\end{cases} \\
s.t. &
\begin{cases}
\omega_1, \omega_2 \in \{\mu, \nu_1, \nu_2, \nu_3, \ldots\}
\end{cases}
\end{align*}
$$

Replacing $Y_{m,n}$ and $\Omega_{ab}$ by their upper bound $\bar{Y}_{m,n}$ and $\bar{\Omega}_{ab}$ in Eq.12 and Eq.13 These two equations are change to Eq.15 and Eq.16

| Parameter | Value | Description |
|-----------|-------|-------------|
| $P_{dc}$ | $8 \times 10^{-8}$ | Dark count rate |
| $\eta_d$ | 14.5% | Detection efficiency |
| $f_c$ | 1.15 | Correction efficiency |
| $M^c$ | 0.2dB/km | Fiber loss |
| $n^t$ | 16 | Phase post selection slice number in PM-QKD |
δ_{ω_1ω_2} = \Phi_{ee}^{\omega_1\omega_2} + \Phi_{eo}^{\omega_1\omega_2} + \Phi_{oc}^{\omega_1\omega_2} + \Phi_{oo}^{\omega_1\omega_2}

= \sum_{n,m=0}^{\infty} \sum_{k,l=0}^{\infty} \left\{ \sqrt{\sum_{l=0}^{2} P_{n}^{l} P_{2n/2+1}^{l} P_{2k/2+1}^{l} X_{2n,2m,2k,2l}^{l}} \right\} \quad (15)

+ \sqrt{\sum_{l=0}^{1} P_{n}^{l} P_{2n+1}^{l} P_{2k/2+1}^{l} X_{2n,2m+1,2k,2l+1}}

+ \sqrt{\sum_{l=0}^{1} P_{n}^{l} P_{2n+1}^{l} P_{2k}^{l} P_{2l}^{l} X_{2n,2m,2k+1,2l+1}}

\; ; \; \; x_{n,m,k,l} \in \{-2\sqrt{\frac{1}{n,m,n,k,l}}, 2\sqrt{\frac{1}{n,m,n,k,l}}\}

s.t.

\begin{align}
\|\bar{T}_{ab} - |\bar{T}_{ab}^{c}| \| & \leq x_{ab} \leq |\bar{T}_{ab}^{c}| + |\bar{T}_{ab}^{d}|, \\
\|\bar{T}_{ab}^{c} - x_{ab} - x_{cd} \| & \leq |\bar{T}_{ab}^{c}| + |\bar{T}_{ab}^{d}| + |\bar{T}_{ab}^{f}|, \\
\|\mu_{ab}^{d} - x_{ab} + x_{cd} \| & \leq |\bar{T}_{ab}^{c} - x_{ab} + x_{cd} + |\bar{T}_{ab}^{d} - x_{ab} + x_{cd}|, \\
\|x_{ee} + x_{oe} + x_{oc} + x_{oo} - Q_{\mu}\| & \leq |x_{ee} + x_{oe} + x_{oc} + x_{oo} - Q_{\mu}|.
\end{align}

(16)

where \(a, b, c, d \in \{e, o\}; ab \neq cd\)

\(T_{AE} = \max \left( h\left( \frac{x_{ee}}{Q_{\mu}}, \frac{x_{oe}}{Q_{\mu}} \right), h\left( \frac{x_{oo}}{Q_{\mu}}, \frac{x_{oe}}{Q_{\mu}} \right) \right)\)

We simulate the performance with the parameters in Tab.I and intensities in Tab.II. The performance is showed in Fig.3. Compared with the original four-intensity decoy state method, both SKR and communication distance are improved significantly. Especially, our distance is close to PM-QKD while the SKR is an order of magnitude larger.

It is worth noting that, the estimation of cross terms rely on the accuracy of \(Y_{n,m}\). To estimate the high-order \(Y_{n,m}(m+n \geq 4)\) tighter, we add an intensity larger than code mode in decoy mode.1.

IV. CONCLUSION

In summary, we proposed a practically useful method to overcome the disadvantages of NPP-TFQKD. By adding the decoy mode.2, we get more constraint condition and it helps us to estimate \(T_{AE}\) tighter. This work improves the communication distance significantly. According to the result of simulation, our method of 5-intensities in decoy mode.1 and 4-intensities in decoy mode.2 is close to infinite decoy-state PM-QKD in the same parameters while our SKR is larger. And it’s more than 50km longer than the original 4-intensities NPP-TFQKD.

In the experimental aspect, the manipulation of decoy mode.2 is the same as code mode and the random intensities is the subset of decoy mode.1. That’s to say, our modification doesn’t bring any extral difficulties in practical.

| TABLE II. Intensities we chose in simulation. |
|-----------------------------------------------|
| PROTOCOL | \(\mu^b\) | \(\nu_1\) | \(\nu_2\) | \(\nu_3\) | \(\nu^d\) |
|---------|---------|---------|---------|---------|---------|
| original | optimized | 0.005   | 0.002   | \(|\|\|\) | 0       |
| improved | optimized | 0.005   | 0.002   | 1.3     | 0       |
| improved | optimized | 0.005   | 0.002   | \(|\|\|\) | 0       |
| PM-QKD  | optimized | 0.005   | 0.002   | \(|\|\|\) | 0       |

\(|\|\|\) the same as the intensity used in code mode
\(|\|\|\) vacuum state
\(|\|\|\) optimized means the intensity of code mode is not fixed but change with the channel loss
\(|\|\|\) this intensity is not used
\(|\|\|\) intensities used in 4-intensities decoy state method of original
\(|\|\|\) No Phase Post-Selection proposed in Ref.10
\(|\|\|\) intensities used in decoy mode.1 of our improved method
\(|\|\|\) intensities used in decoy mode.2 of our improved method

FIG. 3. SKR versus communication distance, the blue and red dash line denote, respectively, infinite decoy-state method and 4-intensities decoy state method of original NPP-TFQKD. The purple and yellow solid line denote, respectively, our improved method with infinite and five intensities in decoy mode.1, four intensities in decoy mode.2. The green dot-dash line is infinite decoy-state method of PM-QKD and blue dot line is linear bound.
[1] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, 1984) pp. 175–179.

[2] H.-K. Lo and H. F. Chau, *science* **283**, 2050 (1999).

[3] P. W. Shor and J. Preskill, *Physical review letters* **85**, 441 (2000).

[4] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, *Rev. Mod. Phys.* **81**, 1301 (2009).

[5] R. Renner, *Int. J. Quantum Inf.* **6**, 1 (2008).

[6] A. Boaron, G. Bosco, D. Rusca, C. Valliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li, *et al.*, *Physical review letters* **121**, 190502 (2018).

[7] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, *et al.*, *Physical review letters* **117**, 100501 (2016).

[8] S. Wang, W. Chen, J.-F. Guo, Z.-Q. Yin, H.-W. Li, Z. Zhou, G.-C. Guo, and Z.-F. Han, *Optics letters* **37**, 1008 (2012).

[9] K. J. Gordon, V. Fernandez, G. S. Buller, I. Rech, S. D. Cova, and P. D. Townsend, *Optics Express* **13**, 3015 (2005).

[10] S. Wang, W. Chen, Z.-Q. Yin, D.-Y. He, C. Hui, P.-L. Hao, G.-J. Fan-Yuan, C. Wang, L.-J. Zhang, J. Kuang, *et al.*, *Optics letters* **43**, 2030 (2018).

[11] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, *Nat. Commun.* **5**, 15043 (2014).

[12] M. Takeoka, S. Guha, and M. M. Wilde, *Nat. Commun.* **5**, 5235 (2014).

[13] M. Lucamarini, Z. Yuan, J. Dynes, and A. Shields, *Nature* **557**, 400 (2018).

[14] X. Ma, P. Zeng, and H. Zhou, arXiv preprint arXiv:1805.05538 (2018).

[15] X.-B. Wang, Z.-W. Yu, and X.-L. Hu, *Physical Review A* **98**, 062323 (2018).

[16] C. Cui, Z.-Q. Yin, R. Wang, W. Chen, S. Wang, G.-C. Guo, and Z.-F. Han, arXiv preprint arXiv:1807.02334 (2018).

[17] M. Curty, K. Azuma, and H.-K. Lo, arXiv preprint arXiv:1807.07667 (2018).

[18] J. Lin and N. Lütkenhaus, *Physical Review A* **98**, 042332 (2018).

[19] H.-K. Lo, M. Curty, and B. Qi, *Physical review letters* **108**, 130503 (2012).

[20] X.-B. Wang, *Phys. Rev. A* **72**, 012322 (2005).

[21] H.-K. Lo, X. Ma, and K. Chen, *Phys. Rev. Lett.* **94**, 230504 (2005).

[22] W.-Y. Hwang, *Phys. Rev. Lett.* **91**, 057901 (2003).

[23] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, *Quantum Inf. Comput.* **4**, 325 (2004).

[24] P. W. Shor and J. Preskill, *Phys. Rev. Lett.* **85**, 441 (2000).

[25] S. L. Braunstein and S. Pirandola, *Phys. Rev. Lett.* **108**, 130502 (2012).

[26] N. Lütkenhaus, *Physical Review A* **61**, 052304 (2000).

[27] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, *Physical Review Letters* **85**, 1330 (2000).

[28] C.-H. F. Fung, B. Qi, K. Tamaki, and H.-K. Lo, *Physical Review A* **75**, 032314 (2007).

[29] F. Xu, B. Qi, and H.-K. Lo, *New Journal of Physics* **12**, 113026 (2010).

[30] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, *Physical Review A* **78**, 042333 (2008).

[31] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurt-siefer, and V. Makarov, *Nature communications* **2**, 349 (2011).

[32] V. Makarov, *New Journal of Physics* **11**, 065003 (2009).

[33] X. Ma and M. Razavi, *Physical Review A* **86**, 062319 (2012).

[34] Y. Liu, T.-Y. Chen, L.-J. Wang, H. Liang, G.-L. Shentu, J. Wang, K. Cui, H.-L. Yin, N.-L. Liu, L. Li, *et al.*, *Physical review letters* **111**, 130502 (2013).

[35] Y.-L. Tang, H.-L. Yin, S.-J. Chen, Y. Liu, W.-J. Zhang, X. Jiang, L. Zhang, J. Wang, L.-X. You, J.-Y. Guan, *et al.*, *Physical review letters* **113**, 190501 (2014).

[36] C. Wang, X.-T. Song, Z.-Q. Yin, S. Wang, W. Chen, C.-M. Zhang, G.-C. Guo, and Z.-F. Han, *Physical review letters* **115**, 160502 (2015).

[37] C. Wang, Z.-Q. Yin, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, *Optica* **4**, 1016 (2017).

[38] X.-B. Wang, *Phys. Rev. Lett.* **94**, 230503 (2005).

[39] X.-B. Wang, *Physical Review A* **87**, 032320 (2013).

[40] Z.-W. Yu, Y.-H. Zhou, and X.-B. Wang, *Physical Review A* **91**, 032318 (2015).

[41] Y.-H. Zhou, Z.-W. Yu, and X.-B. Wang, *Physical Review A* **93**, 042324 (2016).

[42] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, *Nature communications* **5**, 3732 (2014).

[43] X. Ma, C.-H. F. Fung, and M. Razavi, *Physical Review A* **86**, 052305 (2012).

[44] Z.-W. Yu, X.-L. Hu, C. Jiang, H. Xu, and X.-B. Wang, arXiv preprint arXiv:1807.09891 (2018).

[45] K. Tamaki, H.-K. Lo, W. Wang, and M. Lucamarini, arXiv preprint arXiv:1805.05511 (2018).

[46] M. M. Wilde, M. Tomamichel, and M. Berta, *IEEE Transactions on Information Theory* **63**, 1792 (2017).