Four-intensity decoy-state phase-matching quantum key distribution

Yang Yu[1] * Shengmei Zhao[1] † Le Wang[1] ‡ Qianping Mao[2] §

[1] *Institute of Signal Processing Transmission, Nanjing University of Posts and Telecommunications, Nanjing, 210003, China*

[2] *College of computer science and technology, Nanjing Tech University, Nanjing 211800, China*

Abstract. The phase-matching quantum key distribution (PM-QKD), one of the variants of Twin-Field (TF) QKD protocol, was recently proposed to overcome the rate-distance limits of point to point protocol without quantum repeaters. In this paper, we propose a more practical PM-QKD protocol version with four-intensity decoy states, named four-intensity decoy-state PM-QKD protocol, since the infinite decoy states are not available in practice. We present the formulation of the secure key rate of the proposed protocol and analyze the performances of it by numerical simulations to prove its validity.

Keywords: Quantum key distribution, PM-QKD, decoy state, secret key rate

1 Introduction

Under the circumstances that quantum repeaters are currently not feasible, the transmission distance will remain a major obstacle in actual implementation of all those existing protocols due to the rate-distance limit. In 2018, Lucamarini *et al.* did a marvelous work by proposing a so-called twin-field quantum key distribution(TF-QKD), which can break the limit without quantum repeaters [1]. Inspired by the amazing work, several variants of TF-QKD protocol turned out, such as the phase-matching quantum key distribution (PM-QKD) proposed by *Ma et al.* [2], the sending-or-not-sending quantum key distribution (SNS-QKD) presented by *Wang et al.* [3], and the twin-field quantum key distribution without phase post-selection by *Cui et al.* [4] and by *Curty et al.* [5].

In the PM-QKD protocol, Alice (Bob) prepares their weak coherent states randomly and adds a random phase $\phi(A)(\phi(B))$ to each of his weak coherent states. Afterwards, both of them send the states to an untrusted party (Charlie) located in the middle of the channel. Depending on the measurement performed by Charlie, Alice and Bob are able to generate the raw key after a post-selection of the case satisfying $\phi(A) \approx \phi(B)$. After a sifting, parameter estimation and key distillation are necessary to be used to generate a final private and secure key. The infinite decoy-state method was used to estimate the performance in the original PM-QKD [2]. But this method is not able to come true in practice. Thus, a more practical version with finite decoy states should be made. Also, BB84-QKD, MDI-QKD, RRDPS-QKD with finite decoy states have been proposed [6–9]. However, the PM-QKD with finite decoy states has been so far much less analyzed and reported.

*1018010520@njupt.edu.cn

†zhaosm@njupt.edu.cn

‡njwanglele@163.com

§maoqp@163.com

2 Four-intensity decoy-state PM-QKD

2.1 The protocol

Four-intensity decoy-state method is adopted to approach the performance of the PM-QKD protocol with infinite-intensity decoy-state method. The details of the protocol are listed below.

Step 1. Alice (Bob) first randomly generates a binary key k_a and chooses a random phase φ_a, $\varphi_a \in [0, 2\pi)$ and the intensity $\mu_A(\mu_B)$ from $\{\mu/2, v_1/2, v_2/2, v_3/2\}$. Here, $\mu/2$ represents the intensity of signal states, while $v_1/2$, $v_2/2$ and $v_3/2$ are intensities of decoy states, and they should satisfy the conditions: $\mu \geq v_1 \geq v_2 \geq v_3$ and $\mu > v_1 + v_2 + v_3$.

Then, Alice(Bob) prepares a coherent state $|\sqrt{\mu_A}e^{i(\varphi_A+\pi k_a)} >$ ($|\sqrt{\mu_A}e^{i(\varphi_B+\pi k_b)} >$) and sends it to a third party Charlie who can even be an eavesdropper.

Step 2. The third party, Charlie, is expected to carry out an interference measurements on the receiving pair of pulses with a beam splitter and record which detector clicks in each round.

Step 3. The authorized users Alice and Bob, along with the third party Charlie, repeat **Step 1.** to **Step 2.** N times.

Step 4. Charlie announces the results of all the measurements, and Alice(Bob) announces all the intensities and random phases she(he) chooses. When the result of the ith measurement is that only one detector clicks, Alice(Bob) will keep the result as the raw bit if

$$|\varphi_A - \varphi_B - k\pi| \leq \frac{2\pi}{M}(k = 0, 1), \tag{1}$$

where M denotes the number of slices that Alice and Bob choose to divide $[0, 2\pi)$ to the phase interval. And the ith measurement result will be called as a success measurement event. Note that, the raw bit is obtained in Z-basis if $\mu_A = \mu_B = \mu/2$, or X-basis if $\mu_A = \mu_B \neq \mu/2$.

Step 5. Raw bits in X-basis are used for parameter estimations. A certain amount of bits in Z-basis are chosen for error evaluation and the others are used for key distillation.

2.2 Secure key rate

After the protocol is executed, some measured values can be obtained, including the overall gain $Q_x(x = \mu, v_1, v_2, v_3)$ and the bit error rate E_μ^Z. According to the original PM-QKD protocol [2], the secure key rate is given by

$$R = \frac{2}{M} Q_\mu [1 - fH(E_\mu^Z) - H(E_\mu^X)], \tag{2}$$

where f denotes the efficiency of the error correction, $H(x) = -xlog_2(x) - (1-x)log_2(1-x)$ is the binary Shannon information function. E_μ^X denotes the phase error rate, which can be calculated by

$$\begin{aligned} E_\mu^X &= \sum_{k=0}^{\infty} q_{2k+1} e_{2k+1}^Z + \sum_{k=0}^{\infty} q_{2k}(1 - e_{2k}^Z) \\ &\leq q_0 e_0^Z + (q_1 e_1^Z + q_3 e_3^Z + q_5 e_5^Z) \\ &+ (1 - q_0 - q_1 - q_3 - q_5), \end{aligned} \tag{3}$$

In Eq.(3), $q_k = \frac{Q_{k,\mu}}{Q_\mu}$ and e_k^Z respectively represent the fractions and the bit error rate of different photon components k, and $e_0^Z = 0.5$.According to the inequality above, q_k and e_k^Z can be calculated for $0 \leq k \leq 5$.

As for our four-intensity decoy-state PM-QKD protocol, the key rate formula is modified to

$$R = \frac{2}{M} \{ \sum_{k=0}^{2} Q_{k,\mu} [1 - H(E_\mu^X)] - f Q_\mu H(E_\mu^Z) \}, \tag{4}$$

where $Q_{k,\mu} = p_\mu(k) Y_k$ denotes the gain of the k-photon state for the signal state. The yield of k-photon state Y_k cannot be measured directly, but by applying decoy-state method, it can be estimated as well as the bit error rate of k-photon state e_k^Z.

The phase error rate E_μ^X is then rewritten as

$$\begin{aligned} E_\mu^X &= \sum_{k=0}^{\infty} q_{2k+1} e_{2k+1}^Z + q_0 e_0^Z + q_2(1 - e_2^Z) \\ &+ \sum_{k=2}^{\infty} q_{2k} - \sum_{k=2}^{\infty} q_{2k} e_{2k} \\ &\leq \sum_{k=0}^{\infty} q_{2k+1} e_{2k+1}^Z + q_0 e_0^Z + q_2(1 - e_2^Z) \\ &+ (1 - q_0 - q_2 - q_{odd}) \\ &= \sum_{k=0}^{\infty} q_{2k+1} e_{2k+1}^Z + q_0 e_0^Z - q_2 e_2^Z \\ &+ (1 - q_0 - q_{odd}). \end{aligned} \tag{5}$$

And with one signal state and three decoy states, q_k and e_k^Z can only be estimated for $0 \leq k \leq 2$, the overall bit error rate can be calculated as

$$E_\mu^X = q_0 e_0^Z + q_1 e_1^Z - q_2 e_2^Z + (1 - q_0 - q_1). \tag{6}$$

2.2.1 Estimation of the parameters

From earlier work [9], the lower bounds of Y_0, Y_1, Y_2 and the upper bounds of e_1, e_2 can be obtained using the decoy-state method.

With the same method, the upper bounds of Y_1, Y_2 and the lower bounds of e_1, e_2 can be estimated as follows.

$$Y_1^U = \frac{Q_{v_1} e^{v_1} - Q_{v_2} e^{v_2}}{v_1 - v_2}, \tag{7}$$

$$Y_2^U = \frac{2[(v_2 - v_3) Q_{v_1} e^{v_1} - (v_1 - v_3) Q_{v_2} e^{v_2} + (v_1 - v_2) Q_{v_3} e^{v_3}]}{(v_1 - v_2)(v_1 - v_3)(v_2 - v_3)}, \tag{8}$$

$$\begin{aligned} (e_1^Z)^L = &\frac{\mu(E_{v_1} Q_{v_1} e^{v_1} - E_{v_2} Q_{v_2} e^{v_2})}{(v_1 - v_2)(\mu - v_1 - v_2) Y_1^U} \\ &- \frac{v_1 + v_2}{\mu(\mu - v_1 - v_2) Y_1^U} (E_\mu Q_\mu e^\mu - e_0^Z Y_0^L), \end{aligned} \tag{9}$$

$$\begin{aligned} (e_2^Z)^L = &\frac{2\mu}{Y_2^U (v_1 - v_2)(v_1 - v_3)(v_2 - v_3)(\mu - v_1 - v_2 - v_3)} \\ &\cdot [(v_2 - v_3)(E_{v_1} Q_{v_1} e^{v_1} - E_{v_2} Q_{v_2} e^{v_2}) - (v_1 - v_2) \\ &\cdot (E_{v_2} Q_{v_2} e^{v_2} - E_{v_3} Q_{v_3} e^{v_3})] - \frac{2(v_1 + v_2 + v_3)}{Y_2^U \mu^2 (\mu - v_1 - v_2 - v_3)} \\ &\cdot [E_\mu Q_\mu e^\mu - e_0^Z Y_0^L - (e_1^Z)^L Y_1^L \mu]. \end{aligned} \tag{10}$$

2.2.2 Numerical simulation

We simulate the performance of four-intensity decoy-state PM-QKD protocol with the parameters given in Table.1.

Table 1: Parameters of the simulation

Parameters	*pd*	e_0	η_d	α	f
Values	8×10^{-8}	0.5	14.5%	0.2	1.15

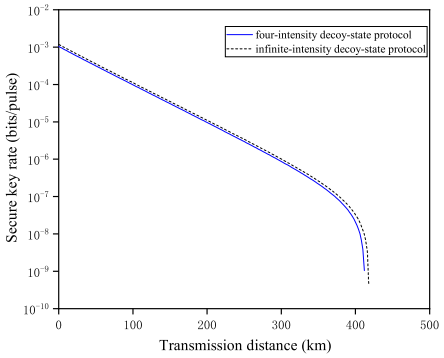

Figure 1: Key generation rate of the the PM-QKD protocol with three decoy states and with infinite decoy states.

Fig.1 shows the performance of the proposed four-intensity decoy-state PM-QKD protocol and the protocol with infinite decoy states. The result shows that, both the key rates decrease with the increasing transmission

distance, and the performance of the proposed protocol is always close to that one with infinite decoy states. Due to the unreality of the infinite-decoy protocol, the four-intensity decoy-state protocol can replace it in actual implementation.

3 Conclusions

In this paper, We have proposed the four-intensity decoy-state PM-QKD protocol. We also have derived the formulations of the secure key rate of the proposed protocol as well as the estimation of the parameters. Simulation results have shown that the proposed protocol's key generation rate is slightly smaller than the original PM-QKD protocol, proving the proposed protocol will suffice and be able to replace the original one in practice.

References

[1] Lucamarini M, Yuan Z L, Dynes J F, and Shields A J, Overcoming the rate-distance barrier of quantum key distribution without using quantum repeaters, *Nature*, 557, 400-403 (2018)

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

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

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

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

[6] Wang X-B, Decoy-state protocol for quantum cryptography with four different intensities of coherent light, *Phys. Rev. A*, 72, 012322 (2005)

[7] Yu Z-W, Zhou Y-H, and Wang X-B, Three-intensity decoy-state method for measurement-device-independent quantum key distribution, *Phys. Rev. A*, 88, 062339 (2013)

[8] Wang L, and Zhao S-M, Free-space measurement-device-independent quantum-key-distribution protocol using decoy states with orbital angular momentum, *Chin. Phys. B*, 24(12):242-249 (2015)

[9] Zhang Y-Y, Bao W-S, Zhou C, Li H-W, Wang Y, and Jiang M-S, Practical round-robin differential phase-shift quantum key distribution, *Opt. Express*, 24(18): 20763-20773 (2016)