

The phase matching quantum key distribution protocol with 3-state systems

Han Duo · Li Zhihui[✉] · Liu Chengji · Gao Feifei

Received: date / Accepted: date

Abstract Quantum Key Distribution, as a branch of quantum mechanics in cryptography, can distribute keys between legal communication parties in an unconditionally secure manner, thus can realize in transmitting confidential information with unconditional security. We consider a Phase-Matching Quantum Key Distribution protocol with 3-state systems for the first time, where the phase of the coherent state is 3, thus we propose three different ways to response to every successful detection and two parties gain their raw keys by “flip and flip”. The simulation results show that compared with Phase-Matching Quantum Key Distribution protocol where the phase equals 2, the proposed protocol breaks the limit of linear key generation rate in a shorter distance, and the longest practical transmission distance is about 470 *km*, whereas the ones of BB84 protocol is lower than 250 *km*.

Keywords Quantum Key Distribution · Phase · PM-QKD protocol

Han Duo
School of Mathematics and Information Science, Shaanxi Normal University, Xi'an, China, 710119.
Tel.: +18829287176
E-mail: handd@snnu.edu.cn

Li Zhihui[✉]
School of Mathematics and Information Science, Shaanxi Normal University, Xi'an, China, 710119.
Tel.: +13032989886
E-mail: lizhihui@snnu.edu.cn

Liu Chengji
State Key Laboratory of Integrated Services Networks, Xidian University, Xian, China, 710071.
Tel.: +15091056770
E-mail: 120148147@qq.com

Gao Feifei
School of Mathematics and Information Science, Shaanxi Normal University, Xi'an, China, 710119.
E-mail: 7920999462@qq.com

1 Introduction

Quantum cryptography [1] is an interdisciplinary subject combining cryptography and quantum mechanics [2]. It is an important research topic. Its security is based on the basic principles of quantum mechanics, such as quantum non-cloning theorem, uncertainty principle [3] et al., the quantum key distribution technology in quantum cryptography provides a means of communication for both parties to obtain unconditional security keys. Security and practical applications are the core of this research.

The first quantum cryptography protocol, the BB84 quantum key distribution protocol [1], was proposed by Bennett and Brassard in 1984, which introduced quantum mechanics into practical applications. However, until 1999, Lo and Chau proved the security of the BB84 protocol by equating the BB84 protocol with an entanglement and purification protocol [4]; but the quantum computer was needed in the proof process. Then in 2000, Shor and Preskill proposed a more concise proof method for CSS quantum error correction code for entanglement and purification [5]; which removed the dependence on quantum computers. Lo et al.'s research further proved bit error correction and phase error correction can be implemented separately [6].

Although the theoretical security of the BB84 protocol has been proved, its actual implementation still has a large security risk. Since there is no ideal single-photon source [7] in practice, a weak coherent pulse (Weak Coherent Pulse) [8] is commonly used to simulate a single-photon source, which leads to the generation of Photon Number Splitting [9]. In 2003, the problem was solved for the first time, since a decoy-state scheme [10] was proposed to defend against PNS attacks. Besides the hidden dangers of the light source, the detector side channel attack [11] also greatly threatened the security of the password. HK proposed decoy Measurement-Device-Independent Quantum Key Distribution (MDI-QKD) protocol [12] in 2012, which eliminates the detector side channel attack [13] without introducing more implementation equipment and double the transmission distance covered by the traditional QKD scheme at the same time.

However, these QKD protocols have same limitations—they never exceed the limit of the Secret Key Capacity (SKC) [14] of the lossy optical quantum channel. X.B.Wang et al. proposed the Twin-field Quantum Key Distribution (TF-QKD) protocol [15] in 2018, which broke the SKC bound of the previous QKD protocols under the condition of ensuring key security. The square root dependence of the key generation rate on the channel transmittance is obtained. However, the security of the agreement has not been proven. X.F.Ma et al. proposed the Phase-matching Quantum Key Distribution (PM-QKD) protocol in 2018 [16] which illustrated a security proof based on optical mode, and resisted all possible measuring attacks.

In the PM-QKD protocol, the communication parties Alice and Bob each generate coherent state pulses independently. For a d -phase PM-QKD protocol, Alice and Bob encode their key information $\kappa_a, \kappa_b \in \{0, 1, \dots, d-1\}$ into the phase of the coherent state. Paper [16] mainly studied the the PM-QKD

in the case of phase $d=2$ (2-PM-QKD protocol) with phase randomization. In theory, the protocol is immune to all possible measurement attacks, and its key rate can even exceed the transmission probability η between two communicating parties; In practice, the protocol applies phase compensation to devise a practical version of the scheme without phase locking [17], which makes the proposed scheme feasible in current technology.

Inspired by the PM-QKD protocol in [18], this paper proposes a new PM-QKD whose phase $d=3$ with phase randomization (For simplicity, we use the name “3-PM-QKD protocol” in the text below).

In the 2-PM-QKD protocol, each transmitted 32-bit binary bit can encode the largest unsigned number, but if the 3-PM-QKD protocol is used, every 32-bit ternary trit can be successfully transmitted. In addition, in this protocol, the range of random phase matching is wider and the probability of successful matching is higher. Alice and Bob retain their key trits when their declared random phases difference is 0 , $\frac{2\pi}{3}$, or $\frac{4\pi}{3}$, which significantly improves the success rate of the phase sifting phase and also results in a higher final key rate.

The paper organized as follows. Following the 2-PM-QKD protocol, we propose the 3-PM-QKD protocol that can surpass the linear key-rate bound and make the key rate increase, whose details are given In Sec.2. Then, the security of 3-PM-QKD is proved in Sec.3, and in Sec.4, we consider all practical factors to simulate the 3-PM-QKD key rate and compare it to the previous QKD protocol. Finally, we summarize this work, put forward the the n -PM-QKD protocol and expound its some curious features in Sec.5.

2 3-PM-QKD protocol

This paper proposes a 3-PM-QKD protocol with phase randomization. That is, Alice and Bob add extra random phases on their coherent state pulses before sending these pulses to Eve. After Eve’s announcement, Alice and Bob announce the extra random phases and postselect the signals based on their random phases. The specific steps and related descriptions are as follows.

2.1 Specific steps

Step1 State Preparation - Alice randomly generates a key trit $\kappa_a \in \{0, 1, 2\}$ and a random phase $\phi_a \in [0, 2\pi)$, and then prepares a coherent state $\left| \sqrt{\mu_a} e^{i(\phi_a + \frac{2\pi}{3}\kappa_a)} \right\rangle_A$. Similarly, Bob generates $\kappa_b \in \{0, 1, 2\}$ and $\phi_b \in [0, 2\pi)$ then prepare $\left| \sqrt{\mu_b} e^{i(\phi_b + \frac{2\pi}{3}\kappa_b)} \right\rangle_B$.

Step2 Measurements - Alice and Bob send their light pulses A and B to an untrusted Eve, which needs to perform interferometry and record the response detector (D_0 , D_1 , or D_2). In particular, the detector response rules are as follows:

$$\Delta_\phi = \left| \phi_a + \frac{2\pi}{3}\kappa_a - \left(\phi_b + \frac{2\pi}{3}\kappa_b \right) \right| = \left| \frac{2\pi}{3}(\kappa_a - \kappa_b) + (\phi_a - \phi_b) \right|.$$

The way the detector responds in this protocol depends on the phase difference between Alice and Bob, The detector response mechanism is set to:

$$\begin{cases} D_0 \text{ response, when } \Delta\phi = 0 \pmod{2\pi}, \\ D_1 \text{ response, when } \Delta\phi = \frac{2\pi}{3} \pmod{2\pi}, \\ D_2 \text{ response, when } \Delta\phi = \frac{4\pi}{3} \pmod{2\pi}. \end{cases}$$

Step3 Statement - Eve announces his detection result. Then Alice and Bob announce random phase ϕ_a and ϕ_b , respectively.

Step4 Sifting - Alice and Bob repeat the above steps multiple times. When Eve announces a successful response (just one detector response), Alice and Bob make the κ_a and κ_b the raw key trits.

According to Eve's statement, Bob flips his key trits κ_b accordingly. The flipped key trits are recorded as κ'_b . The flip rule is as follows:

$$\begin{cases} \kappa'_b = \kappa_b, \text{ if } D_0 \text{ response,} \\ \kappa'_b = \kappa_b + 1 \pmod{2\pi}, \text{ if } D_1 \text{ response,} \\ \kappa'_b = \kappa_b + 2 \pmod{2\pi}, \text{ if } D_2 \text{ response.} \end{cases}$$

When Alice and Bob respectively announce random phases, Bob flips his key trits κ'_b again according to their random phase difference $|\phi_a - \phi_b|$. The flipped key trits are recorded as κ''_b . The flipping rules are as follows:

$$\begin{cases} \kappa''_b = \kappa'_b \pmod{2\pi}, \text{ if } |\phi_a - \phi_b| = 0 \pmod{2\pi}, \\ \kappa''_b = \kappa'_b - 1 \pmod{2\pi}, \text{ if } |\phi_a - \phi_b| = \frac{2\pi}{3} \pmod{2\pi}, \\ \kappa''_b = \kappa'_b - 2 \pmod{2\pi}, \text{ if } |\phi_a - \phi_b| = \frac{4\pi}{3} \pmod{2\pi}. \end{cases}$$

Finally, Bob's key trits are κ''_b .

Step5 Parameter Estimation - Alice and Bob derive the gain Q_μ and quantum trit error rate E_μ^Z from all the retained raw data and then estimate E_μ^X .

Step6 Key Distillation - Alice and Bob perform error correction and privacy amplification on the sifted key trits to generate a private key (note that the error correction and privacy amplification of this protocol are the same as in all QKD protocols except that we must use trits Not bits, so the parity becomes a ternary test, ie the modulus is 3 [18]).

In the actual implementation of this protocol, Alice and Bob retain their signals only when their declared random phases difference is 0, $\frac{2\pi}{3}$, or $\frac{4\pi}{3}$. However, due to the announcement of phase continuity, the probability of successful sifting is 0. In addition, the phase locking technique required in actual implementation is very difficult. Therefore, we use the phase post compensation method [19] like paper.

The post-phase compensation method used here is similar to 2-PM-QKD protocol. Alice and Bob divide the phase interval $[0, 2\pi)$ into M slices first. When a random phase is declared, Alice and Bob only compare the slice indicators, not the exact phase. This makes the step of phase sifting practical, but introduces inherent bias errors. This bias error can compensate for the inherent bias error by sacrificing a portion of the data, minimizing the quiz error

rate QBER based on random sampling, and calculating the appropriate phase offset. In addition, Alice and Bob do not perform phase sifting immediately in each round, but perform this phase sifting in data post-processing. This makes the 3-PM-QKD protocol practical.

More importantly, in the 2-PM-QKD protocol, each successfully transmitted 32-bit binary bit can encode the largest unsigned number to $2^{32} - 1$, but if this protocol is used, every 32-trit ternary trit transmitted can be encoded to $3^{32} - 1$. When the transmission efficiency is the same, every coherent state can carry more information.

In this protocol, the range of random phase matching is wider and the probability of matching success is higher. Alice and Bob retain their signals when their declared random phases difference is 0, $\frac{2\pi}{3}$, or $\frac{4\pi}{3}$, which significantly improves the success rate of the phase screening phase and also results in a higher final key rate.

To illustrate the feasibility of this protocol, this paper presents a simple key correspondence table to illustrate how Alice and Bob match key information by “flip and flip” successfully.

2.2 Key-correspondence table of this protocol

In the 3-PM-QKD protocol, the key information $\kappa_{a(b)} \in \{0, 1, 2\}$, so a successful key is generated if and only if the random phase difference is an integer multiple of $\frac{2\pi}{3}$ (less than a non-negative integer multiple of 3). There are 27 cases, and we list the situation when ϕ_a and ϕ_b satisfy with $|\phi_a - \phi_b| = \frac{4\pi}{3} \pmod{2\pi}$ in this section, and other cases are equally available.

Table 1 Key-correspondence table with $|\phi_a - \phi_b| = \frac{4\pi}{3} \pmod{2\pi}$

κ_a	κ_b	$ \phi_a - \phi_b $	Δ_ϕ	Response	κ'_b	κ''_b
0	0	$4\pi/3$	$4\pi/3$	D_2	2	0
0	1	$4\pi/3$	$2\pi/3$	D_1	2	0
0	2	$4\pi/3$	0	D_1	2	0
1	0	$4\pi/3$	0	D_1	0	1
1	1	$4\pi/3$	$4\pi/3$	D_1	0	1
1	2	$4\pi/3$	$2\pi/3$	D_1	0	1
2	0	$4\pi/3$	$2\pi/3$	D_1	1	2
2	1	$4\pi/3$	0	D_1	1	2
2	2	$4\pi/3$	$4\pi/3$	D_1	1	2

The Table I shows that accurate detection response and key sifting can guarantee a successful key match with a probability close to 1, and the probability of successful match is higher than that of 2-PM-QKD protocol.

3 Security of 3-PM-QKD protocol

Unlike the general QKD protocol security proof, the commonly used photon number channel model [20] and the “tagging” method used in the security proof by Gottesman et al. (GLLP security proofs) [21] are no longer applicable here. This is because the random phases of Alice and Bob are announced in this protocol, and the quantum source can no longer be regarded as a mixture of photon number states. But as mentioned in [16], we can directly analyze the optical mode by applying Lo-Chau entangled distillation theory to demonstrate the security of PM-QKD with coherent pulses.

The proof of the security of this protocol is followed by the analysis of distillable entanglement based on the equivalent entanglement protocol, and transforms it into 3-PM-QKD protocol gradually. The security performance is proved in each operation. The proof process is similar to the 2-PM-QKD protocol, except we must use trits instead of bits, so we will not repeat them here.

4 Simulation Results

Since our solution is generalized from 2-PM-QKD, the simulation in this section is mainly compared with the 2-PM-QKD protocol. According to [16], when $l > 120km$, the key rate of 2-PM-QKD exceeded the key rate of traditional BB84 protocol; when transmitting distance $l > 250km$, 2-PM-QKD could exceed the limit of linear key rate; Compared with MDI-QKD, 2-PM-QKD can achieve a longer transmission distance of $l = 450km$, and at the time $l > 300km$, the key rate increased by about 4-6 orders of magnitude. This section will prove that the 3-PM-QKD protocol is better than the 2-PM-QKD protocol, and thus better than the traditional BB84 protocol and the MDI-QKD protocol.

Applying the key rate formula in Shor-Preskill’s security proof [5]

$$r = 1 - H(E^Z) - H(E^X). \quad (1)$$

And the key rate formula in [16]

$$R_{2-PM} \geq \frac{2}{M} Q_\mu [1 - fH(E_\mu^z) - H(E_\mu^X)]. \quad (2)$$

Where E^Z and E^X are the Z error rate and the X error rate, respectively. $H(x) = -x \log_2 x - (1-x) \log_2 (1-x)$ are the binary Shannon entropy function, Q_μ is the phase error rate, and f is the error correction efficiency.

Because we have only expanded the value range of the key bits in this paper, other parts of the key rate formula are still similar to the 2-PM-QKD protocol, but the phase sifting factor in this article is $3/M$, Shannon’s entropy function becomes $H(x) = -x \log_3 x - (1-x) \log_3 (1-x)$ for the three-state system. Finally, our key rate formula is

$$R_{3-PM} \geq \frac{3}{M} Q_{\mu} [1 - fH(E_{\mu}^z) - H(E_{\mu}^X)]. \quad (3)$$

We use the parameters given in the Table 2 below to simulate the performance of 3-PM-QKD. Assuming that the lossy channels of Alice and Bob are symmetrical; the dark count rate is from Ref. [22], and other parameters are set to classic values. (Note that in order to identify the effect of the key rate is on the protocol itself rather than other parameters, the actual setting parameters used in this article are completely consistent with the 2-PM-QKD protocol).

Table 2 Parameters used for simulation in 3-PM-QKD protocol

Parameters	Values
Dark count rate p_d	8×10^{-8}
Error correction efficiency f	1.15
Detector efficiency η_d	14.5%
Number of phase slices M	16
Misalignment error e_d	1.5%

The simulation results are shown in the following figure.

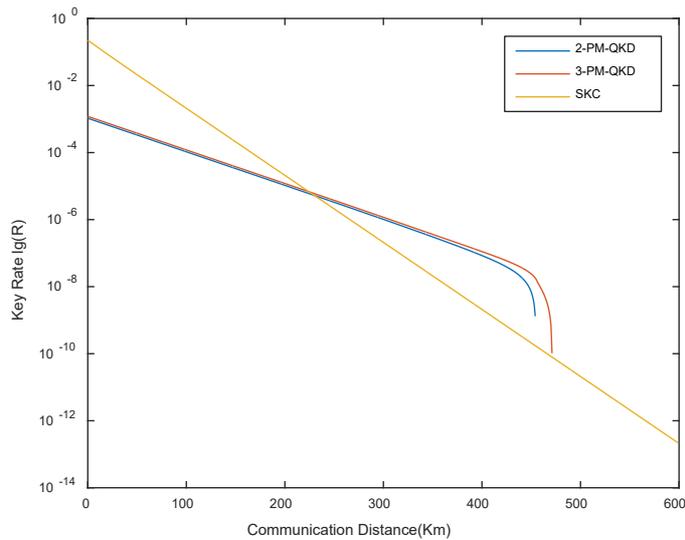


Fig. 1 Simulation of our protocol. For the considered simulation parameters, the key rate is similar to 2-PM-QKD protocol, but it breaks the SKC bound in a shorter distance and the effective transmission distance has increased by about 20 kilometers.

As can be seen, our protocol has a small increase on key rate compared with the 2-PM-QKD protocol, but the effective transmission distance has increased

by about 20 kilometers, and it has broken through SKC bound in a shorter distance.

5 Summary and Outlook

This paper proposes the 3-PM-QKD protocol and proves its security. The 3-PM-QKD protocol not only breaks the boundaries of SKC, but also reduces the distance to break the boundaries of SKC, meanwhile, the proposed protocol increases the key rate and effective transmission distance.

Also, the higher-dimensional promotion of the 3-PM-QKD protocol in this paper will be an interesting direction, such as the n -PM-QKD protocol with phase randomization. This is a very difficult problem, because when space is extended to any dimension, it is difficult to express all its properties strictly, but this attempt is very interesting. At the time $\kappa_{a(b)} \in \{0, 1, 2, \dots, n\}$, although the selection interval of the random phase was still the same, the probability of successful screening could approach 100%. This is an interesting change, which is because there is always a exact detector response for the specific value of any phase difference, but this requires extremely accurate detector standards. In any case, this will be one of the efforts of QKD protocol in practice. The specific steps of n -PM-QKD is similar to 2-PM-QKD, which will not be described in detail here.

However, the n -PM-QKD protocol is currently only possible theoretically, but if it can be successfully implemented, that will greatly increase the key rate of the QKD protocol and guarantee a 100% probability of successful phase matching, in which the corresponding parameter estimation and security proof will be the largest challenge. Once the phase of the coherent state is extended to infinite dimensions, it may have some distinctive properties, which is a subject worthy of study.

Acknowledgements We would like to thank anonymous reviewer for valuable comments. This work is supported by the National Natural Science Foundation of China under Grant No.11671244.

References

1. C.H.Bennett, G.Brassard, Quantum Cryptography:Public key distribution and coin tossing, (Proceedings of the IEEE international conference on computers, systems and signal processing, Bangalore (1984)
2. A.K.Ekert, Quantum Cryptography Based on Bell's Theorem, Phys. Rev. Lett., 67, 661(1991)
3. M.A.Nielsen, I.Chuang, Quantum Computation and Quantum Information(Cambridge University Press(2000)
4. H.K.Lo and H.F.Chau, Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances, Science, 283, 5410(1999)
5. P.W.Shor, J.Preskill, Simple Proof of Security of the BB84 Quantum Key Distribution Protocol, Phys. Rev. Lett., 85,441(2000)
6. H.K.Lo, Method for decoupling error correction from privacy amplification, New Journal of Physics,5(2003)

7. M.Curty, M.Lewenstein, and N.Gütkenhaus, Entanglement as a Precondition for Secure Quantum Key Distribution, *Phys. Rev. Lett.*, 92, 217903(2004)
8. B.Hutter, N.Imoto, N.Gisin, and T.Mor, Quantum cryptography with coherent states,*Phys. Rev. A*, 51,1863(1995)
9. X.B.Wang, Beating the photon-number-splitting attack in practical quantum cryptography, *Phys. Rev. Lett.*, 94,230503(2005)
10. W.Y.Hwang, Quantum Key Distribution with High Loss: Toward Global Secure Communication, *Phys. Rev. Lett.*, 91, 057901(2003)
11. Z.Q.Yin, S.Wang, W.Chen, H.W.Li, G.C.Guo, and Z.F.Han, Reference-free-independent quantum key distribution immune to detector side channel attacks, *Quantum Information Processing*, 13, 1237(2014)
12. H.K.Lo, M.Curty, Measurement-device-independent quantum key distribution, *Phys. Rev. Lett.*, 108, 130503(2012)
13. Y.Zhao, C.H.Fung, C.Chen, and H.K.Lo, Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems, *Phys. Rev. A*, 78, 042333(2008)
14. S.Pirandola, R.Laurenza, C.Ottaviani, and L.Banchi, Fundamental limits of repeaterless quantum communications, *Nature Communications*, 8,15043(2017)
15. Twin-field quantum key distribution with large misalignment error,*Phys. Rev. A*, 98, 062323(2018)
16. X.F.Ma, P Zeng, and H.Y. Zhou, Phase-matching quantum key distribution, *Phys. Rev. X*, 8,031043(2018)
17. G.Santarelli, A.Clairon, S.N.Lea, and G.M.Tino, Heterodyne optical phase-locking of extended-cavity semiconductor lasers at 9 GHz, *Opt.Common*, 104, 339(1994)
18. H.B.Pasquinucci and A.Peres, Quantum Cryptography with 3-State Systems, *Phys. Rev. Lett.*,85, 3313(2000)
19. X.F.Ma and M.Razavi, Alternative schemes for measurement-device-independent quantum key distribution, *Phys. Rev. A*,86, 062319(2012)
20. X.F.Ma, Quantum Cryptography:From Theory to Practice, Ph.D. thesis, University of Toronto(2008)
21. D.Gottesman,H.K.Lo, N. Lutkenhaus, and J.Preskill, Security of quantum key distribution with imperfect devices, *Quantum Inf. Comput.*, 4, 325(2004)
22. Y.Lin.Tang, H.L.Yin, S.J.Chen, Y.Liu, W.J.Zhang, X.Jiang, L.Zhang, J.Wang, L.X.You, J.Y.Guan, D.X.Yang, Z.Wang, H.Liang, Z.Zhang, N.Zhou, X.F.Ma, T.Y.Chen, Q.Zhang, and J.W.Pan, Measurement-Device-Independent Quantum Key Distribution over 200 km, *Phys. Rev. Lett.*,113, 190501(2014)