Journal of Quantum Information Science, **2011, 1, 116-120**
doi:10.4236/jqis.2011.13016 Published Online December 2011 (http://www.SciRP.org/journal/jqis)

Practical Stabilization of Counterfactual Quantum Cryptography

Musheng Jiang, Shihai Sun, Linmei Liang*
Department of Physics, National University of Defense Technology, Changsha, China
E-mail: *nmliang@nudt.edu.cn*
Received August 14, 2011; *revised September* 23, 2011; *accepted September* 30, 2011

Abstract

A novel counterfactual quantum key distribution scheme was proposed by T.-G. Noh and a strict security analysis has been given by Z.-Q. Yin, in which two legitimate geographical separated couples may share secret keys even when the key carriers are not traveled in the quantum channel. However, there are still plenty of practical details in this protocol that haven't been discussed yet, which are of significant importance in physical implementation. In this paper, we will give a practical analysis on such kind of counterfactual quantum cryptography in the aspects of quantum bit error rate (QBER) and stabilization. Furthermore, modified schemes are proposed, which can obtain lower QBER and will be much more robust on stabilization in physical implementation.

Keywords: Counterfactual Quantum Cryptography, Quantum Bit Error Rate, Practical Stabilization

1. Introduction

Combining with one time pad, quantum key distribution (QKD) [1,2] based on the fundamental principles of quantum mechanics can in principle offer the unconditionally secure private communications between two users, Alice and Bob. Many successful QKD experiments [3-9] have been realized during the past decade, which must transmit key carriers in a public quantum channel. Besides, an entirely different scheme based on the quantum counterfactual effect was proposed recently, named as counterfactual quantum cryptography [10]. Since this counterfactual quantum cryptography is based on polarization-multiplexing, we call it polarization-multiplexed counterfactual quantum cryptography (PCQC) in this paper. In this scheme, the task of a secret key distribution can be accomplished without transmitting any particle carrying secret key information in the quantum channel. A photon that carries secret key information has been confined from its birth to death within Alice's secure zone, and Eve can never access the photon, but Bob still can extract a secret key from the nondetectable events, which is a surprising counterintuitive fact. Furthermore, the PCQC protocol provides clear security advantages when taking photon number splitting attack (PNS) [11] into account. More recently, a strict security analysis of the PCQC protocol has also been given in an ideal situation [12]. However, some practical factors are unconsidered. In this paper, we will give a practical analysis on the PCQC protocol in the aspects of quantum bit error rate (QBER) and stabilization. Furthermore, some modified schemes are proposed, which can obtain lower QBER and will be much more robust on stabilization in physical implementation.

2. Stabilization Analysis of Counterfactual Quantum Cryptography

To begin with, let us review the PCQC protocol briefly. As shown in **Figure 1** (cited from [10]), Alice randomly encodes a single photon in one of the two orthogonal

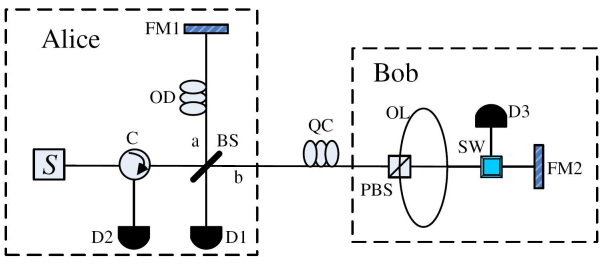

Figure 1. (Color online) Schematic diagram of the original polarization-multiplexed counterfactual quantum cryptography system (cited from Ref. [10]).

polarization states to represent his bit value. The encoded single-photon pulse entering a Michelson-interferometer is split into two pulses by a beam splitter (BS) and travels through two modes a and b. In mode a, the pulse is reflected back by a Faraday mirror (FM), and always confined within Alice's secure zone. In mode b, the pulse travels from Alice's site to Bob's site. Bob also randomly chooses one of the two orthogonal polarizations representing his bit value by blocking the corresponding polarization state, named as polarization-selection. If an optical pulse incident to Bob's site is horizontally polarized, it passes through the polarizing beam splitter (PBS) and goes directly to the high-speed optical switch (SW). However, if the pulse is vertically polarized, it is first reflected by the PBS, passes through the optical loop (OL), and then goes to the SW. Therefore, through accurate control of the switch timing, Bob can effectively switch the selected polarization state to the detector D3, while the other was reflected back to Alice's BS. Thus, if the bit values chosen by Alice and Bob are different, the split pulse going through mode b is not blocked by Bob, and the two split pulses are recombined in the BS, and the single photon is detected at detector D2 certainly as a result of quantum interference. On the other hand, if the two bit values are equal, the split pulse going through mode b is blocked by detector D3. Then, the photon can be detected at detector D1 with a finite probability, which is caused by the breakage of the interference. In this case, the photon has been completely confined within Alice's secure zone, and Eve can never access the photon, as it has only traveled through mode a. Alice and Bob can then establish a sifted key by selecting only the events for which D1 clicks alone. In summary, the process can be described as follows: 1) when the bit values of Alice and Bob are different, D2 clicks with probability 1/2; 2) when the bit values of Alice and Bob are equal, D1 clicks with probability $RT/2$, D2 clicks with probability $R^2/2$, and D3 clicks with probability $T/2$. The events for which D1 clicks alone are used to extract a secret key, and the other events are used to detect the latent eavesdropper (Eve). Here R and $T=1-R$ are the reflectivity and transmissivity of the BS, respectively.

Now, we analyze the PCQC protocol in the aspects of QBER and stabilization. It is mentioned in [10] that it may be hard to stabilize a long-armed interferometer, which is related to QBER and stabilization. For a long-armed interferometer, the symmetry of the interferometer relies sensitively on the environmental disturbances such as temperature fluctuations. The breakage of this symmetry will cause a variation of the interference, for example, phase drift may even completely destroy the interference. Ideally, it is easily seen that the single photon is detected at detector D2 with certainty when the bit values of Alice and Bob are different, as a result of quantum interference. But in fact, we can never keep the interference perfect for a long-armed interferometer under environmental disturbances. The extreme result is that the optical path difference of the interferometer is larger than the coherence length of the light source because of fiber length drift. Consequently, the interference is completely destroyed, that is, mode a and mode b of a single photon are not coherent any more. In this case, a single photon can be detected at detector D1 with probability 1/2, which is an error event and adds an additional QBER in the raw keys. Generally speaking, the interferometer can be stabilized using feedback control. Here we assume that, once the bit values of Alice and Bob are different, mode a and mode b of a single photon are always coherent under feedback control. However, error events may still happen with some probability as a result of phase drift. Here we note this event as phase-crosstalk, and the corresponding probability as C_{phase}. Note that in PCQC protocol, the events for extracting a secret key have a probability of RT/2, and the probability of error events caused by phase-crosstalk is $C_{\text{phase}}/2$. Thus, the additional QBER caused by phase-crosstalk can be written as

$$\text{QBER}_{\text{phase}} = \frac{C_{\text{phase}}/2}{C_{\text{phase}}/2 + RT/2} \tag{1}$$

Furthermore, since Bob must perform polarization-selection through the PBS to represent his bit value, instability due to the polarization mode dispersion effects in long-distance single-mode fiber should also be considered. In fact, a long-distance single-mode fiber should be considered as a birefringent medium as a result of its intrinsic imperfection and environmental disturbances. When a single photon passes through such a birefringent medium, the polarization mode dispersion effect is visible, which will result in the instability of polarization. Therefore, well performed polarization compensation is needed to compensate for the instability of polarization; otherwise the polarization-selection will not perform well, resulting in another additional QBER in the raw keys. But in fact, the polarization of a single photon will of course drift away from its original state more or less after traveling from Alice's site to Bob's site, regardless of how well the polarization compensation is performed. In the process of polarization-selection, if a single photon enters Bob's PBS with horizontal polarization, it passes through the PBS and goes directly to the SW; and if the single photon is vertically polarized, it is firstly reflected by the PBS, passes through the OL, and then goes to the SW. However, polarization drift may sometimes bring in unexpected result. For example, when the bit values of

Alice and Bob are different, the split pulse going through mode b should not be blocked by Bob but was reflected back to Alice's BS, and the two split pulses interfere in the BS; unfortunately, the polarization of a single photon may drift away from its original state when the photon enters Bob's PBS and then lose its way. Therefore, the split pulse going through mode b may be blocked by Bob and D1 clicks with some probability, which is an error event too. Similarly, we note this event as polarization-crosstalk, and the corresponding probability as $C_{polarization}$. Then the additional QBER caused by polarization-crosstalk can be expressed as

$$QBER_{polarization} = \frac{RTC_{polarization}/2}{RTC_{polarization}/2 + RT/2} \quad (2)$$

Finally, the total QBER of the system can be deduced when we consider all the potential factors: phase-crosstalk, polarization-crosstalk and the dark-counts of detector D1 η_{D1}.

$$QBER_{total} = \frac{RT\left(C_{polarization}/2 + \eta_{D1}\right) + C_{phase}/2}{\left(C_{phase} + RTC_{polarization} + RT\right)/2} \quad (3)$$

Besides, phase-crosstalk and polarization-crosstalk also bring in other problems. On the one hand, to detect Eve's intervention in PCQC protocol, Alice and Bob monitor the operation of the interferometer. They tell each other whether or not each of the detectors clicked for a photon, and obtain the probability for each event over a period of time. If D2 or D3 clicks, they also announce both the detected polarization state and the initial polarization states that were chosen. However, the operation of the interferometer may also be affected by phase-crosstalk and polarization-crosstalk: 1) the probability for each event may be changed by both the phase-crosstalk and the polarization-crosstalk; 2) when D3 clicks, the detected polarization state and the initial polarization states may be different as the result of polarization-crosstalk. Therefore, Alice and Bob may be hard to detect Eve's intervention in a way. And the following process of quantum cryptography such as privacy amplification should be based on the worst condition to guarantee the security. In other words, phase-crosstalk and polarization-crosstalk impair the security of the protocol. On the other hand, the control of stabilization is crucial to compensate for both the phase-crosstalk and the polarization-crosstalk. However, since it is a multivariable feedback control problem, it is hard to operate continuously alongside key distribution, which will result in key rate reduction. And in practical implementation, the complexity may be terrible while the precision of stabilization control may be limited, compared to single-variable feedback control.

3. Improvement on Stabilization

If we can avoid the phase-crosstalk or polarization-crosstalk, the system can obtain lower QBER and will be much more robust on stabilization in physical implementation, and the advantage of counterfactual quantum cryptography will attract more attention in physical implementation. Here we present a modified scheme of PCQC protocol, in which we have eliminated the polarization-crosstalk simply by moving the PBS from Bob's site to Alice's site. **Figure 2** shows the schematic of our PCQC system. In fact, our modified scheme of PCQC protocol is similar to the original one and we focus on the differences here. Within Alice's secure zone, the polarization-encoded single-photon pulse will choose a path according to its polarization state before entering the Michelson-interferometer. If an optical pulse is encoded horizontally polarized, it passes through the PBS and goes directly into the interferometer. However, if the pulse is encoded vertically polarized, it is first reflected by the PBS, passes through the OL, and then enters the interferometer. Therefore, the encoded single-photon pulses with different polarization enter the interferometer with different time nodes, and arrive at Bob's SW with different time nodes in mode b. Thus, Bob can directly switch the selected polarization state to the detector D3 while the other was reflected back to Alice's BS.

It is worthwhile to point out here that this modified PCQC protocol provides equivalent function as the original one in an ideal situation. Evidently, all the processes of PCQC can be implemented by the modified scheme. And since Eve can only access one subsystem (path b) while she can never access the other subsystem (path a), the security of the modified scheme is also guaranteed by no-cloning principle for orthogonal states: if reduced density matrices of an available subsystem are nonorthogonal and the other subsystem is not allowed access, it is impossible to distinguish two orthogonal quantum states without disturbing them [10]. Moreover, in physical implementation, the modified PCQC not only inherits all the advantages of the original one, but also has a sig-

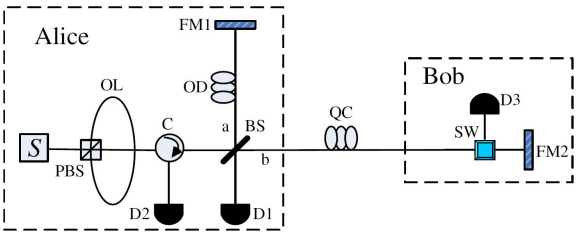

Figure 2. (Color online) Schematic diagram of the modified polarization-multiplexed counterfactual quantum cryptography system.

nificant improvement on QBER and stabilization. Since the encoded single-photon pulses with different polarization are separated just after their emission, the polarization-crosstalk due to polarization mode dispersion effects in long-distance single-mode fiber is eliminated. Then the polarization-selection can be performed without error through accurate control of the switch timing in Bob's site. That is to say, all the error events caused by the polarization-crosstalk do not exist in our modified PCQC. Therefore, the additional QBER due to polarization-crosstalk is discarded. And the total QBER of the system can be expressed as

$$\mathrm{QBER}_{\mathrm{total}} = \frac{\mathrm{RT}\,\eta_{\mathrm{D1}} + \mathrm{C}_{\mathrm{phase}}/2}{\left(\mathrm{C}_{\mathrm{phase}} + \mathrm{RT}\right)/2} \tag{4}$$

which is smaller than that in Equation (3). Moreover, the security and the stabilization are also improved because of the elimination of the polarization-crosstalk. And single-variable feedback control can meet the requirement of stabilization control, which is much simpler and more precise.

We also present another modified counterfactual quantum cryptography based on wavelength-multiplexing, named as wavelength-multiplexed counterfactual quantum cryptography (WCQC). **Figure 3** shows the schematic of our WCQC system. Alice randomly sends out a single photon of wavelength λ_1 or λ_2 to represent his bit value. The photons of different wavelengths are coupled to the Michelson-interferometer via wavelength-division multiplexing WDM. In mode b, the pulses travel from Alice's site to Bob's site and will be separated in time by group velocity dispersion, then transmitted to SW with different time nodes. For example, the group velocity dispersion of single-mode fiber is $D = 17$ ps/nm·km, supposed $\Delta\lambda = \lambda_1 - \lambda_2 = 20$ nm, and the fiber length between Alice and Bob is $L = 30$ km, then the group delay in optical transmission is $\tau = D \cdot \Delta\lambda \cdot L = 10.2$ ns. Therefore, Bob can also randomly choose one of the two wavelengths representing his bit value by accurate control of the switching time, blocking the single photon with corresponding wavelength. Similar to PCQC protocol, all the processes of counterfactual quantum cryptography can be implemented effectively.

In fact, Alice can even randomly encode the single photon pulses in different time nodes to represent his bit value, by random control of SW1 shown in **Figure 4**. Similarly in mode b, single-photon pulses encoded in different time nodes will be transmitted to SW2 in Bob's site with different time nodes. And counterfactual quantum cryptography can be carried out similarly. Since time-multiplexing is used, this modified scheme is named as time-multiplexed counterfactual quantum cryptography (TCQC).

It is easily seen that both the TCQC protocol and the WCQC protocol are not involved in the polarization of the single-photons, so does the polarization-crosstalk. The total QBER of these systems can also be expressed by Equation (4). Therefore, they are much more robust on QBER, security and stabilization in physical implementation.

4. Discussion and Conclusions

We have given a practical analysis on counterfactual quantum cryptography, and have proposed some kinds of modified schemes, in which the single-photons are encoded in orthogonal states of different degrees of freedom. Here we can characterize the counterfactual quantum cryptography as follows: key carriers can be encoded into either orthogonal states or nonorthogonal states in any degrees of freedom; Alice and Bob extract secret keys in the encoded degrees of freedom (such as polarization, time and wavelength), while another degrees of freedom (usually the phase) is used to detect the disturbance of Eve; Alice and Bob can extract secret keys without transmitting any particle carrying secret key information in the quantum channel. The key point is that these two kinds of freedom are encoded in one physical carrier. These characteristics make the counterfactual quantum cryptography completely different from the previous protocols of QKD, BB84 protocol for example, in which nonorthogonal states must be used with

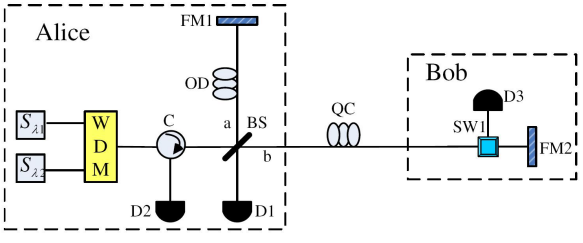

Figure 3. (Color online) Schematic diagram of the Wavelength-multiplexed counterfactual quantum cryptography system.

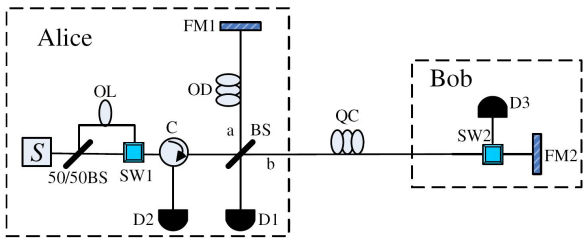

Figure 4. (Color online) Schematic diagram of the time-multiplexed counterfactual quantum cryptography system.

basis reconciliation, signal particle transmission is needed, and both the extract of secret keys and the detection of the latent Eve are operated in the same degree of freedom. Furthermore, these characteristics have provided security advantages, especially when considering the PNS attack.

In summary, we have analyzed the phase-crosstalk and the polarization-crosstalk of PCQC protocol in the aspects of QBER and stabilization. We find that the phase-crosstalk and the polarization-crosstalk not only bring in QBER but also impair the security and stabilization of the protocol. And a modified scheme of PCQC protocol without polarization-crosstalk has been proposed in this paper. Moreover, another two protocols of counterfactual quantum cryptography, TCQC and WCQC, were proposed. Time-multiplexed and Wavelength-multiplexed are used in these protocols, which are independent of the polarization of the single-photons. Since we have avoided the polarization-crosstalk in all of these modified schemes, they have a significant improvement on QBER, security and stabilization. However, the phase-crosstalk is a remained problem and single-variable feedback control is still needed to guarantee the stabilization of these modified protocols of counterfactual quantum cryptography. Further study on counterfactual quantum cryptography may find out another practical choice of QKD.

5. Acknowledgements

This work is supported by National Natural Science Foundation of China Grants No.61072071. Shi-Hai Sun is supported by Hunan Provincial Innovation Foundation for Postgraduate No.CX2010B007, and Fund of Innovation, Graduate School of NUDT No.B100203.

6. References

[1] C. H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, 9-12 December 1984, pp. 175-179.

[2] A. K. Ekert, "Quantum Cryptography Based on Bell's Theorem," *Physical Review Letters*, Vol. 67, No. 6, 1991, pp. 661-663. doi:10.1103/PhysRevLett.67.661

[3] A. Muller, H. Zbinden and N. Gisin, "Quantum Cryptography over 23 km in Installed Under-Lake Telecom Fiber," *Europhysics Letters*, Vol. 33, No. 5, 1996, pp. 335-339. doi:10.1209/epl/i1996-00343-4

[4] C.-Z. Peng, J. Zhang, D. Yang, W.-B. Gao, H.-X. Ma, H. Yin, H.-P. Zeng, T. Yang, X.-B. Wang and J.-W. Pan, "Experimental Long-Distance Decoy-State Quantum Key Distribution Based on Polarization Encoding," *Physical Review Letters*, Vol. 98, No. 1, 2007, pp. 010505.1-010505.4.

[5] C. H. Bennett, "Quantum Cryptography Using Any Two Nonorthogonal States," *Physical Review Letters*, Vol. 68, No. 21, 1992, pp. 3121-3124. doi:10.1103/PhysRevLett.68.3121

[6] X.-F. Mo, B. Zhu, Z.-F. Han, Y.-Z. Gui and G.-C. Guo, "Faraday-Michelson System for Quantum Cryptography," *Optics Letters*, Vol. 30, No. 19, 2005, pp. 2632-2634. doi:10.1364/OL.30.002632

[7] H.-Q. Ma, J.-L. Zhao and L.-A. Wu, "Quantum Key Distribution Based on Phase Encoding and Polarization Measurement," *Optics Letters*, Vol. 32, No. 6, 2007, pp. 698-700. doi:10.1364/OL.32.000698

[8] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden and N. Gisin, "'Plug and Play' Systems for Quantum Cryptography," *Applied Physics Letters*, Vol. 70, No. 7, 1997, pp. 793-795. doi:10.1063/1.118224

[9] S.-H. Sun, H.-Q. Ma, J.-J. Han, L.-M. Liang and C.-Z. Li, "Quantum Key Distribution Based on Phase Encoding in Long-Distance Communication Fiber," *Optics Letters*, Vol. 35, No. 8, 2010, pp. 1203-1205. doi:10.1364/OL.35.001203

[10] T.-G. Noh, "Counterfactual Quantum Cryptography," *Physical Review Letters*, Vol. 103, No. 23, 2009, pp. 230501.1-230501.4.

[11] G. Brassard, N. Lütkenhaus, T. Mor and B. C. Sanders, "Limitations on Practical Quantum Cryptography," *Physical Review Letters*, Vol. 85, No. 6, 2000, pp. 1330-1333. doi:10.1103/PhysRevLett.85.1330

[12] Z.-Q. Yin, H.-W. Li, W. Chen, Z.-F. Han and G.-C. Guo, "Security of Counterfactual Quantum Cryptography," *Physical Review A*, Vol. 82, No. 4, 2010, pp. 042335.1-042335.6.

