Counterfactual quantum key distribution without polarization encoding

Akshata Shenoy H.[1] * R.Srikanth[2 3] † T.Srinivas[1] ‡

[1] *ECE Department,Indian Institute of Science,Bangalore,India.*
[2] *Poornaprajna Institute of Scientific Research,Bangalore,India.*
[3] *Raman Research Institute,Bangalore,India*

Abstract. In counterfactual quantum key distribution (QKD), two remote parties can share a secure secret random key even without transmission of a physical particle (a non-vacuum pulse) through the channel. A QKD scheme is proposed which is counterfactual in one of the bits, and in which the secret bits are not encoded in the polarization, but in the joint action of Alice and Bob. On the conceptual level, our scheme throws new light on the origin of security in counterfactual cryptography. On the practical side, non-polarization encoding makes it robust against certain trojan horse attacks. We study the the general photon-number preserving incoherent attack in detail.

Keywords: Quantum cryptography,Counterfactual quantum cryptography

1 Introduction

Quantum key distribution (QKD) allows two parties (Alice and Bob) to share a secret key, whose secrecy is protected by the laws of quantum mechanics (QM), such as no-cloning and the indistinguishability of non-orthogonal states [1]. It remains the most advanced application of quantum information theory experimentally [2]. Since the proposal of the first QKD protocol [3], various paradigms of QKD have been proposed such as use of entanglement [4, 5], orthogonal states [6], two-way communication [7, 8], secure direct communication [9, 10, 11] and, most recently, counterfactual QKD (CQKD) [12, 13], which is based on the idea of interaction-free measurement [14]. CQKD involves secret information transmission not being mediated by a physical (i.e., non-vacuum) particle. The protocol has since been made more efficient [15] and its security investigated [16, 17, 18]. Recently, it was experimentally implemented [19]. Here we propose a new CQKD scheme in which secret bits are generated indeterministically through the joint actions of Alice and Bob, independently of polarization.

2 New Protocol

We propose a new CQKD scheme which does not require polarization encoding but instead uses a switch state to generate secret bits. Alice's set up is a Michelson-type interferometer (Fig reference). The arm b of which acts as a channel between her and Bob. Single photons from source S hits the beamsplitter BS and splits along arms a and b respectively.The state of the particle after BS is

$$|\phi\rangle_{AB} = \sqrt{T}|00\rangle|\psi\rangle + i\sqrt{R}|\psi\rangle|00\rangle, \qquad (1)$$

where T and R represent the coefficients of transmittance and reflectance of the BS respectively, where $T = 1 - R$ and $|00\rangle$ represents the vacuum state in the two polarization modes H and V, while $|\psi\rangle$ represents an single photon state of arbitrary polarization, i.e., $|\psi\rangle = \alpha|10\rangle + \beta|01\rangle$ with $|\alpha|^2 + |\beta|^2 = 1$. The first (second) ket refers to the transmitted (reflected) or Alice (Bob) arm.

Alice and Bob each randomly apply a reflect F or an absorb A operation depending on their switch SW state (on or off) which are independently connected to a quantm random number generator. Alice observes the pattern of outcomes in her interferometer. The patterns of detection, and outcome probabilities, are given in Table 1. For a fraction of pulses, both settings and outcomes are announced to compute V, the visibility observed by Alice; e, the channel error; r, fraction of multiple counts; and λ, the transmission loss. If these experimental parameters are sufficiently close to their ideal values, the protocol run is deemed secure; else it is aborted.

Detection	Pattern (Alice, Bob)
D_1	$((F,A),\frac{1}{4})$, $((A,F),\frac{1}{4})$
D_2	$((F,F),1)$, $((F,A),\frac{1}{4})$, $((A,F),\frac{1}{4})$
Null	$((F,A),\frac{1}{2})$, $((A,F),\frac{1}{2})$, $((A,A),1)$

Table 1: The allowed pattern of Alice's and Bob's action along with the probability that a detector click was produced.

3 Security

Intuitively, security arises because Eve's attempt to ascertain Bob's choice tends to localize the particle in one of the arms, thereby reducing the coherence between the two paths and hence undermining the visibility in the interference in the case where Alice and Bob reflect their respective pulse. A detailed proof of security for a general incoherent attack, and an incoherent photon-number preserving attack are given in Ref. [20].

For the general incoherent number-preserving attack, Eve prepares an ancilla in the state $|0\rangle_E$, and on the joint system BE, applies the following operation during the onward transmission: $\mathcal{U} = |00\rangle_B\langle 00| \otimes U_0 + (|01\rangle_B\langle 01| + |10\rangle_B\langle 10|) \otimes U_1$, such that $\langle 0|U_1^\dagger U_0|0\rangle \equiv$

*akshataphy@gmail.com
†srik@poornaprajna.org
‡tsrinu.iisc@gmail.com

$\langle Y|N\rangle = \cos(\theta)$. This interaction produces the state: $\mathcal{U}|\phi\rangle_{AB}|0\rangle = \frac{1}{\sqrt{2}}(|\psi\rangle|00\rangle|N\rangle + |00\rangle|\psi\rangle|Y\rangle)$. She then measures her ancilla using the optimal POVM, conditioned on Alice announcing a D_1 detection.

For the above attack, the condition for security turns out to be: $H\left(\frac{1-\cos\theta}{2-\cos\theta}\right) < \cos\theta$ where H is the Shannon binary entropy. We deduce the largest tolerable error rate to be about 20.9% (corresponding to $\theta \approx 0.74$). Eve could launch a Trojan horse attack by transmitting probes into Bob's apparatus and studying them upon return, using an Alice-like set-up. Alice may vary the polarization and cross-check polarization data as in BB84 to prevent this attack [20].

4 Discussion and conclusions

We have presented a protocol for QKD which is counterfactual on one of the generated secret bits in that the encoding corresponds to the blocking or the not blocking by Bob of a transmitted particle. Like the Noh, Pingpong, LM and Deng-Long [9] protocols, it may be thought of as a two-way QKD protocol, but differs from each of them in one or more key aspects. Our protocol has Alice sending a fixed state, unlike in the Noh and LM protocols. It involves single-particle nonlocality unlike in the LM protocol; finally, unlike in the Pingpong protocol, it does not involve two particle entanglement. A practical advantage of not using polarization encoding is that it makes the protocol secure against a kind of Trojan horse attack. We have assumed zero transmission losses, so that every particle is accounted for by Alice's or Bob's detectors. Thus, a direction for generalizing our work is to allow for lossy channels. Another direction is to study how much a more general incoherent and even coherent attack, helps Eve.

References

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden. Quantum Cryptography. *Rev. Mod. Phy*, 74, 145, 2002.

[2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkenhaus, and M. Peev. The security of practical Quantum key distribution. *Rev. Mod. Phy*, 74, 145, 2002.

[3] C. H. Bennett and G. Brassard. Quantum Cryptography: Public key distribution and Coin tossing. in *Proc. IEEE Int. Conf. on Computers, Systems, and Signal Processing*, Bangalore: p. 175, 1984.

[4] A. K. Ekert. Quantum Cryptography based on Bell's theorem. *Phys. Rev. Lett.*, 67, 661, 1991.

[5] H. K. Lo and H. F. Chau. Unconditional Security of Quantum key distribution over arbitrary long distances. *Science*, 283, 2050-2056, 1999.

[6] L. Goldenberg and L. Vaidman. Quantum Cryptography based on orthogonal states. *Phy. Rev. Lett.*, 75, 1239, 1995.

[7] Kim Boström and Timo Felbinger. Deterministic Secure Direct Communication Using Entanglement. *Phy. Rev. Lett.*, 89, 187902, 2002.

[8] Marco Lucamarini and Stefano Mancini. Secure Deterministic Communication without Entanglement. *Phy. Rev. Lett.*, 94, 140501, 2005.

[9] Fu-Guo Deng and Gui Lu Long. Secure direct communication with a quantum one-time pad *Phy. Rev. A.*, 69, 052319, 2004.

[10] Hua Lu, Chi-Hang Fred Fung, Xiongfeng Ma and Qing-yu Cai. Unconditional security proof of a deterministic quantum key distribution with a two-way quantum channel. *Phy. Rev. A.*, 84, 042344, 2011.

[11] C. Shukla, A. Pathak and R. Srikanth. Beyond the Goldenberg-Vaidman protocol: Secure and efficient quantum communication using arbitrary, orthogonal, multi-particle quantum states. *Int. J. Quantum Inf*, 10, 1241009, 2012.

[12] T. -G. Noh Counterfactual Quantum Cryptography. *Phy. Rev. Lett.*, 103, 230501, 2009.

[13] Hatim Salih, Zheng-Hong Li, M. Al-Amri and M. Suhail Zubairy. Protocol for Direct Counterfactual Quantum Communication. *Phy. Rev. Lett.*, 110, 170502, 2013.

[14] A. C. Elitzur and L. Vaidman. Quantum mechanical interaction-free measurements. *Found. of Phys.*, 23, 987, 1993.

[15] Ying Sun and Qiao-Yan Wen. Counterfactual quantum key distribution with high efficiency. *Phys. Rev. A*, 82, 052318, 2010.

[16] Zhen-Qiang Yin, Hong-Wei Li, Wei Chen, Zheng-Fu Han and Guang-Can Guo. Security of Counterfactual Quantum Cryptography. *Phys. Rev. A*, 82, 042335, 2010.

[17] Sheng Zhang, Jian Wang, Chao-jing Tang and Quan Zhang. Security proof of Counterfactual Quantum Cryptography against general intercept-resend attacks and its vulnerability. *Chin. Phys. B*, 21, 060303, 2012.

[18] Sheng Zhang, Jian Wang and Chao Jing Tang. Counterfactual attack on counterfactual quantum key distribution. *Euro. Phy. Lett.*, 98, 30012, 2012.

[19] Giorgio Brida, Andrea Cavanna, Ivo Pietro Degiovanni, Marco Genovese and Paolo Traina. Experimental realization of Counterfactual Quantum Cryptography. *Laser. Phy. Lett.*, 3, 247, 2012.

[20] Akshata Shenoy H., R. Srikanth and T. Srinivas Semi-counterfactual quantum cryptography. arXiv:1307.7551, 2013.