Counterfactual quantum key distribution without polarization encoding

Akshata Shenoy H[1], R. Srikanth[2] and T. Srinivas[1]
[1]ECE Dept., IISc, Bangalore, India
[2]PPISR, Bangalore, India

Introduction. Quantum key distribution (QKD) is a method 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], and even commercially. 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], and, most recently, counterfactual QKD (CQKD) [9], which is based on the idea of interaction-free measurement [10]. CQKD involves secret information transmission not being mediated by a physical (i.e., non-vacuum) particle. The protocol has since been made more efficient [11] and its security investigated [12–14]. Recently, it was experimentally implemented [15]. 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.

Novelty. The presented CQKD involves "switch-encoded" secret bits, unlike the original Noh protocol, which uses polarization encoding. This simple modification gives new insight on the origin of security in counterfactual cryptography, as discussed below. One consequence of removing polarization-encoding is that, only one of the two bit values is counterfactually generated. If the vacuum state is treated at par with other dimensions, the present protocol can be described as an in deterministic, two-way, orthogonal-state based protocol, but differs fundamentally from all the *paradigmatic* QKD protocols.

Most importantly, unlike in the Noh protocol, the initial state here is a fixed path-entangled pulse and polarization encoding is not used. However, the following features are shared with the Noh protocol.

Unlike the two-way protocols of Ping-pong [7] and LM protocols [8], the present protocol is indeterministic. Unlike the LM and BB84 protocols, orthogonal states are used here for encoding. Unlike in the GV protocol [6], the communication is two-way. Finally, unlike in the Ping-pong protocol, where a local unitary is used for encoding, preserving the entanglement, here the encoding of secret bits involves measurement and disentangling the initial state.

A practical advantage of non-polarization encoding is that varying polarization allows a class of trojan horse attacks to be detected.

Counterfactual protocol. One of the two parties, sender Alice has a Michelson interferometer. A single photon enters an input port of the interferometer, hitting the beam-splitter, which splits the pulse into a reflected and transmitted component. The latter is directed to Bob, while the former remains within Alice's module. Each randomly applies a reflect or absorb operation, and Alice observes the pattern of outcomes in her interferometer. In a lossless situation, there are the following detection possibilities:

1. Detector (say) D2 clicks: This can arise from one of the parties reflecting their pulse, and necessarily if both reflect.
2. Detector D1: This can arise only if precisely one of them reflects the pulse. Ideally, this event gives rise to secret bits.

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. For the model of attack considered, which is photon-number preserving, the condition for security turns out to be:

$$1 - h\left(\frac{1 - V}{2 - V}\right) \geq \frac{1}{2}(1 - V)$$

where *V* is the visibility of the interference pattern observed by Alice and *h* is Shannon binary entropy. We deduce the largest tolerable error rate to be about 33%, where the above inequality fails, a rather large value, because we restrict ourselves to a restricted (photon-number preserving incoherent) attack by Eve.

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. However the particle (or the vacuum pulse corresponding to it) is re-exposed to Eve during the return phase of the pulse from Bob, and a proof of security must consider this, as in any other two-way QKD protocol.

By not using polarization encoding, our scheme shows that the origin of security in a CQKD is not the translated no-cloning theorem, invoked in Ref. [9]. This follows by noting that that the reduced density operator of the particle in our scheme is the same independent of encoding (similarly as in the Ping-pong protocol [7]).

We prove the security of the most general incoherent attack in an ideal setting. For a photon-number preserving incoherent attack, we derive conditions for tolerable error, given in the Equation above.

Directions for future work. We indicate below some ways in which this work can be furthered.

1. We have assumed zero transmission losses, so that every particle is accounted for by Alice's or Bob's detectors. Thus, this work may be generalized to allow for lossy channels.
2. Another direction is to study in a non-ideal situation, how much a coherent attack (photon-number preserving or otherwise), where Eve attacks individual particles but measures them jointly after Alice's classical announcement, helps her.
3. The inherent use of entanglement (in the state space spanned by a single-photon and vacuum) suggests that a device-independent version of the protocol may be developed.

References.

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev.Mod. Phys. 74, 145 (2002).

[2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. L□utkenhaus, and M. Peev, Rev. Mod. Phys.81, 1301 (2009).

[3] C. H. Bennett and G. Brassard, in Proc. IEEE Int. Conf.on Computers, Systems, and Signal Processing, Bangalore (1984), p. 175.

[4] A. K. Ekert, Phys. Rev. Lett. 67, 661 (1991).

[5] H. -K. Lo and H. F. Chau, Science 283, 2050 (1999).

[6] L. Goldenberg and L. Vaidman, Phys. Rev. Lett. 75, 1239 (1995).

[7] K. Bostrom and T. Felbinger, Phys. Rev. Lett. 89, 187902 (2002).

[8] M. Lucamarini and S. Mancini, Phys. Rev. Lett. 94, 140501 (2005).

[9] T.-G. Noh, Phys. Rev. Lett. 103, 230501 (2009).

[10] A. C. Elitzur and L. Vaidman, Found. of Phys. 23, 987 (1993).

[11] Y. Sun and Q.-Y. Wen, Phys. Rev. A 82, 052318 (2010).

[12] S. Zhang, J. Wang, and C. J. Tang, Europhys. Lett. 98, 30012 (2012).

[13] Z.-Q. Yin, H.-W. Li, W. Chen, Z.-F. Han and G.-C.Guo, Phys. Rev. A 82, 042335 (2010).

[14] S. Zhang, J. Wang, C. jing Tang, and Q. Zhang, Chin.Phys. B 21, 060303 (2012).

[15] G. Brida, A. Cavanna, I. P. Degiovanni, M. Genovese and P. Traina, Laser Phys. Lett. 3, 247 (2012).

[16] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Informatio*n (Cambridge, 2000).

[17] I. Csizár and J. Koerner, IEEE Trans. Inf. Theory 24, 339 (1978).