International Journal of Modern Physics B
Vol. 22, Nos. 1 & 2 (2008) 82–87

World Scientific
www.worldscientific.com

A NEW QUANTUM KEY DISTRIBUTION PROTOCOL BASED ON QUANTUM FARADAY ROTATION

TAESEUNG CHOI and MAHN-SOO CHOI*
Department of Physics, Korea University, Seoul 136-713, Korea
**choims@korea.ac.kr*

Received 3 December 2007

We propose a new quantum key distribution (QKD) protocol, which exploits the maximal entanglement between home qubits and flying qubits induced by means of quantum Faraday rotation (QFR). The entanglement between the flying and home qubits provides the essential part of the security of the protocol. We also discuss possible experimental implementations, the optical cavity QED and quantum dots in microcavity, which is feasible in current spintronics technology.

Keywords: Quantum cryptography; entanglement; quantum nonlocality.

1. Introduction

The purpose of QKD is to generate a private key between legitimate partners, say Alice and Bob, in the presence of an eavesdropper, Eve. The seminal works by Bennet, Brassard (BB84), and Eckert (E91)[1,2,3] stimulated numerous new QKD proposals to enhance the security and efficiency under non-idealistic situations and to incorporate new ideas [4].

Recently Boström and Felbinger proposed a so-called *ping-pong protocol*. Although the original protocol was proved to be insecure[6,7], Lucamarini and Mancini[8] have proposed a modified version to overcome the security issues. The interesting feature of this protocol is the round-trip journey of an information carrier (travel qubit), which enables a quantum communication without any public channel (except for checking eavesdropping). In this protocol, Alice performs one of two unitary transformations which result in orthogonal states, and Bob decodes the message from Alice directly by comparing two orthogonal states. The unitary transformation is performed conditioned on the classical bits, 0 or 1. Here, a natural question would be: What if the unitary transformation is conditioned on a quantum state? In this work, we address this question and show that it indeed provides a conceptually new protocol. Below we will analyze the security of the new protocol for a special type of attack by Eve; more general analyses will be discussed elsewhere.[19]

2. Quantum Faraday Rotation

When a linearly polarized light travels through a substance in a magnetic field, it experiences a rotation, known as the Faraday rotation. One can formulate the Faraday rotation as a unitary operator in two dimensional complex space. When the light is propagating along z-axis, the Faraday rotation can be represented by the following unitary transformation,

$$U(\beta) = e^{-i\sigma^z \beta/2}. \tag{1}$$

Here β is the Faraday rotation angle and proportional to the classical field. The Faraday rotation is thus "classical" in the sense that the rotation angle β is determined by the classical state of the substance.

Imagine a Fraraday rotation with the rotation angle determined by the quantum state of the substance that the light travels through. Later we will discuss possible experimental set-ups, where the Faraday rotation of the polarization of the light is determined by the quantum state of an electron spin that it interacts with. We will call as quantum Faraday rotation (QFR) such a Faraday rotation conditioned on the quantum state of a qubit (e.g., electron spin). We will consider the polarization state of the light as a flying qubit and the electron spin as a home qubit. We will denote the QFR of the flying qubit C *conditioned on* the quantum state of the qubit A by

$$U_{A;C} = e^{-i(\pi/4)\sigma_A^z \sigma_C^z}. \tag{2}$$

Here we particularly considered the QFR by angle $\pi/2$. The polarization state of the light (flying qubit) is represented by a point on the Poincaré sphere *conditioned on* the state of the home qubit A, while the spin state of the electron (home qubit) is represented by a point on the Bloch sphere. Then the same notation can be used for the basis of the eigenstates of σ^z, $|\uparrow\rangle$ (right-handed circular polarization) and $|\downarrow\rangle$ (left-handed circular polarization). The state along the azimuthal angle ϕ on the equator of the Poincaré (or Bloch) sphere is denoted by

$$|\phi\rangle = \frac{|\uparrow\rangle + e^{i\phi}|\downarrow\rangle}{\sqrt{2}}. \tag{3}$$

When the state of home qubit A is $|0\rangle_A$ and the state of travel qubit C is $|\phi\rangle_C$, the QFR generates the maximally entangled states of A and C as

$$U_{A;C}|0\rangle_A|\phi\rangle_C = \frac{e^{-i\pi/4}|\uparrow\rangle_A|\phi_+\rangle_C + e^{i\pi/4}|\downarrow\rangle_A|\phi_-\rangle_C}{\sqrt{2}}, \tag{4}$$

where $|\phi_\pm\rangle_C = |\phi \pm \pi/2\rangle_C$. This shows that $|\phi\rangle_C$ is rotated counterclockwise (clockwise) when A is in the state $|\uparrow\rangle_A$ ($|\downarrow\rangle_A$). In the quantum information theoretic terms, the QFR in Eq. (2) is a *conditional phase shift*. More generally, any state $|\psi\rangle_A$ on the equator of the Bloch sphere can generate a maximally entangled states with C under the QFR with just a phase change of $\pi/4 \to \pi/4+\psi$ in the clockwise rotation. Since the two qubits A and C becomes maximally entangled as a result of QFR, the

single photon C is not polarized at all. That is, C becomes a complete mixed state with a reduced density matrix $\rho_C = \mathrm{Tr}(U_{A;C}|0\rangle_A|\phi\rangle_{CC}\langle\phi|_A\langle 0|U^\dagger_{A;C}) = I/2$, where I is a 2×2 identity matrix. This means that a measurement on the polarization of one travel qubit C produces a completely random result. This property will be extensively used in our protocol to acquire the security.

3. QKD Protocol

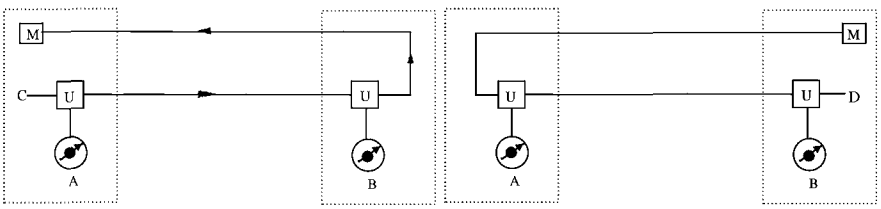

Fig. 1. (a) Travel qubit C of Alice takes a round-trip(ping-pong) under the action of QFR's. (b) Travel qubit D of Bob takes a round-trip(ping-pong) under the action of QFR's.

Our protocol consists of the following steps: (1) To start the nth iteration of the protocol, Alice and Bob first prepare their home qubits A and B, respectively, in the state $|0\rangle$ (Fig. 1 (a)). (2) Alice then takes a travel qubit C and prepares it in the state $|\phi\rangle$. The angle ϕ should be chosen randomly in the interval $0 \leq \phi < 2\pi$. (3) Alice performs (by interacting A and C) the QFR $U_{A;C}$ on C and send it to Bob. We note that on its way to Bob, the travel qubit C is maximally entangled with A (see Eq. (4)) (4) Bob receives C, performs $U_{B;C}$ on it, and send it back to Alice. The qubit C is again maximally entangled on its way back to Alice, now with both A and B :

$$(e^{-i\pi/2}|\uparrow\uparrow\rangle + e^{i\pi/2}|\downarrow\downarrow\rangle)_{AB}|\bar{\phi}\rangle_C + (|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle)_{AB}|\phi\rangle_C \tag{5}$$

(not normalized), where $|\bar{\phi}\rangle_C = |\phi + \pi\rangle_C$. (5) Now Bob takes his own travel qubit D and prepares it in the state $|\eta\rangle$. The angle η should be chosen randomly in the interval $0 \leq \eta < 2\pi$ (Fig. 1 (b)). (6) Bob performs the QFR $U_{B;D}$ on D and send it to Alice. (7) Alice receives D, performs $U_{A;D}$ on it, and send it back to Bob. The final state of all the qubits A, B, C, and D is given by a GHZ-like state

$$(|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle)_{AB}\,|\phi\eta\rangle_{CD} - (|\uparrow\uparrow\rangle + |\downarrow\downarrow\rangle)_{AB}\,|\bar{\phi}\bar{\eta}\rangle_{CD} \tag{6}$$

(8) Alice measures the observable $S_\phi = \cos\phi\sigma^x + \sin\phi\sigma^y$ on C. Likewise, Bob measures the observable $S_\eta = \cos\eta\sigma^x + \sin\eta\sigma^y$ on D. They will get (in the ideal case) the identical result $+1$ or -1, which enables Alice and Bob to share the the key $K_{2n-1} = 1$ or 0. (9) If $K_{2n-1} = 1$, Bob performs σ^x (the NOT gate), on his home qubit B. (10) Alice and Bob measures σ^z on their home qubits A and B, respectively. Depending on the measurement result, another bit of key $K_{2n} = 0$ ($\sigma^x = +1$) or 1 ($\sigma^x = -1$) is generated. (11) Repeat the steps 1 through 10 with n

Table 1. The probabilities for different measurement outcomes of Alice, Bob, and Eve.

	Alice	Bob	Eve	Probabilities[a]
Outcomes	+	+	+	9
	+	−	+	3
	−	+	+	3
	−	−	+	1
	−	−	−	9
	−	+	−	3
	+	−	−	3
	+	+	−	1

[a] This is normalized by 1/32.

increased by 1 until n becomes N. (12) Alice and Bob takes randomly M bits out of $\{K_{2k-1}|k=1,\cdots,N\}$, and test possible eavesdropping (or any other attack) by comparing the values through a classical communication channel.

To demonstrate the security of the protocol, we will consider the intercept-and-resend attack by Eve. The security analyses against general attacks will be published elsewhere.[19]. Since Eve does not know the polarization direction of the travel qubit, Eve has to make a random guess about the direction of observables to measure the polarization of the travel qubit. For convenience we denote the difference between the true polarization direction and the guessed direction by λ for C and by δ for D. Then,

$$|\phi_+\rangle_C = \cos\frac{\lambda}{2}|e\rangle + i\sin\frac{\lambda}{2}|\bar{e}\rangle\,, \quad |\eta_+\rangle_D = \cos\frac{\delta}{2}|e'\rangle + i\sin\frac{\delta}{2}|\bar{e'}\rangle\,, \tag{7}$$

where $\{|e\rangle, |\bar{e}\rangle\}$ or $\{|e'\rangle, |\bar{e'}\rangle\}$ are Eve's measurement bases at an intercept-and-resend attack. In these bases the probability for measurement outcome +1 becomes $\cos^2\frac{\lambda}{2}$ and $\cos^2\frac{\delta}{2}$, respectively. Table 1 shows the probabilities for different outcomes of Alice, Bob, and Eve under Eve's attack. Here the measurement outcome of Eve is given by the product of four outcomes on coming and going (returned) paths of C and D. This shows that the attack inevitably makes the outcomes of Alice's and Bob's measurement, which enables Alice and Bob to detect Eve by comparing their outcomes. The detection probability becomes 3/8. This is the same as that of Lucamarini *et al.*[8] under the "double" control mode, which is greater than 1/4 of BB84.

3.1. *Experimental implementation*

The key element which enables the QFR to establish the entanglement between the flying qubit and the home qubit is the interaction of the form

$$H_I = g\sigma_z^1\sigma_z^2, \tag{8}$$

where g is the coupling constant. We consider two experimental setups which can realize the interaction of the form in Eq. (8).

First, we consider the photons interacting with atomic spin in cavity. The interaction in Eq. (8) was realized between a collective spin operator (σ_z^1) of atoms and the Stokes operators (σ_z^2) of the photons[9]. By means of this entanglement mechanism quantum non-demolition (QND) measurements and spin squeezing have been investigated theoretically and experimentally [9,10]. The experimentally long-lived entanglement of two macroscopic objects was demonstrated by Julsgaard *et al.* [11]. However the Faraday rotation angle was very small in these cases. The entanglement of two separate macroscopic objects has not been a maximally entangled one which is suitable for a particular purpose, for example, quantum teleportation. Moreover these implementations have a crucial defect to be used in quantum cryptology, which is the usage of the semiclassical light (polarized pulse of light) vulnerable to Eve's attack. To cure the defect, a single atom and a single photon must be used. However, the interaction strength between a single atom and a photon is very weak, so it has to be strengthened by high-finesse optical cavity. The first experimental measurement of the birefringence of a single atom strongly coupled to high-finesse ($\mathcal{F} = 18000$) cavity was reported by Turchette *et al.*[12]. The conditional phase shift was approximately 16° per intracavity photon. However, their system was proposed as a candidate quantum phase gate. In this proposal, single photon pulses propagating in two frequency-offset channels, with internal states specified by $\sigma_\pm$ polarization are "flying qubits" and no entanglement between an atomic state and a photon state was investigated. Recently Duan *et al.* have proposed a scheme to achieve conditional quantum gate on remote atoms whose interactions are catalyzed by single photons [13]. In this sense, the maximal entanglement between a single atom and a photon is still challenging in cavity QED.

Next, we consider photons interacting with spins of electrons confined in quantum dots. Leuenberger *et al.*[14] have proposed a teleportation scheme for teleportation of many-qubit entangled states stored in the electron spins of a quantum dot system [14]. They have demonstrated theoretically that the GHZ-type entanglement can be established in the spin-photon-spin through the interaction between a photon and the two electron spins, via conditional Faraday rotation in microcavities. This interaction is also the right one to implement our protocol. The selection rules for a photon and an excess spin in the dot lead to Faraday rotation. This spin-selective coupling between the electron spins and photons gives the desired interaction (8) and can be enhanced by surrounding each of the dots by its own high-Q microcavity [15]. The experimental parameters have been estimated to reach the maximal entanglement between an excess spin and a photon polarization and their implementations are feasible in current technology [14]. The interaction time required for a maximal entanglement between the photon polarization and the electron spin is much smaller than the spin decoherence time in semiconductor nanostructures [16,17] and can be controlled by active Q switching of the microcavity [18]. After $T = 1$ ns in the small cavity before Q switching, the entangled state can be produced with high fidelity. The transmission distance is limited mainly by the coherence time of the electron spin in the quantum dot. The maximum transmission distance (given

by the speed of light) would be 10 m and 1×10^6 m for coherence times of 100 ns [16] and for 10 ms [17] in one-way transmission.

4. Conclusion

We have proposed a new QKD protocol based on the QFR. The proposed QKD proposal is a variation of the ping-pong protocol. Because of the quantum nature of the QFR, two round trips are required to finish one iteration of the key generation. Note that two keys are generated out of each iteration, and hence the efficiency of the key generation is the same as other ping-pong protocols. The preparation of an arbitrary polarization direction of the travel qubit may give stronger security than BB84 and Lucamarini *et al.* For an intercept-and-resend attack, the detection probability becomes 3/8 the same as Lucamarini *et al.*[8] The experimental implementation of our protocol is feasible in current spintronics technology.

Acknowledgments

This work was supported by the SRC/ERC program of MOST/KOSEF (R11-2000-071), the Korea Research Foundation Grant (KRF-2005-070-C00055), the SK Fund, and the KIAS.

References

1. C. H. Bennett and G. Brassard (IEEE Press, New York, 1984), pp. 175–179.
2. A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
3. C. H. Bennett, G. Brassard, and A. Ekert, Sci. Am. **267**, 50 (1992).
4. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinde, Rev. Mod. Phys. **74**, 145 (2002).
5. K. Boström and T. Felbinger, Phys. Rev. Lett. **89**, 187 902 (2002).
6. Q.-Y. Cai, Phys. Rev. Lett. **91**, 109801 (2003).
7. A. Wójcik, Phys. Rev. Lett. **90**, 157901 (2003).
8. M. Lucamarini and S. Mancini, Phys. Rev. Lett. **94**, 140501 (2005).
9. A. Kuzmich *et al.*, Europhys. Lett. **42**, 481 (1998); Phys. Rev. Lett. **85**, 1594 (2000).
10. Y. Takahashi *et al.*, Phys. Re. A **60**, 4974 (1999); M. Takeuchi *et al.*, Phys. Rev. Lett. **94** 023003 (2005); C. Genes and P.R. Berman, Phys. Rev. A **73**, 013801 (2006).
11. B. Julsgaard, A. Kozhekin, and E.S. Polzik, Nature **413**, 400 (2001).
12. Q.A. Turchette *et al.*, Phys. Rev. Lett. **75**, 4710 (1995).
13. L.-M. Duan, B. Wang, and H.J. Kimble, Phys. Rev. A **72**, 032333 (2005).
14. M.N. Leuenberger, M.E. Flatté, and D.D. Awschalom, Phys. Rev. Lett. **94**, 107401 (2005).
15. M. Gurioli, G. Khitrova, and H.M. Gibbs, Physica E (Amsterdam) **17**, 463 (2003).
16. J.M. Kikkawa and D.D. Awschalom, Phys. Rev. Lett. **80**, 4313 (1998).
17. M. Kroutvar *et al.*, Nature (London) **432**, 81 (2004).
18. D.H. Auston and M.C. Nuss, IEEE J. Quantum Electron. **24**, 184 (1988).
19. T. Choi and M.-S. Choi, preprint (unpublished).