Counterfactual Quantum Cryptography

Tae-Gon Noh (노태곤)*

Electronics and Telecommunications Research Institute, Daejeon 305-700, Korea

(Received 16 October 2008; published 1 December 2009)

Quantum cryptography allows one to distribute a secret key between two remote parties using the fundamental principles of quantum mechanics. The well-known established paradigm for the quantum key distribution relies on the actual transmission of signal particle through a quantum channel. In this Letter, we show that the task of a secret key distribution can be accomplished even though a particle carrying secret information is not in fact transmitted through the quantum channel. The proposed protocols can be implemented with current technologies and provide practical security advantages by eliminating the possibility that an eavesdropper can directly access the entire quantum system of each signal particle.

DOI: 10.1103/PhysRevLett.103.230501 PACS numbers: 03.67.Dd, 03.65.Ta, 03.67.Hk

According to quantum mechanics, events that might have occurred can have actual physical effects, even though they do not in fact occur. What has been termed as an interaction-free measurement [1–4] is a typical example of such striking counterfactual phenomena: the presence of an object can be determined without a photon being scattered by the object. It has also been shown that the outcome of a quantum computation can sometimes be inferred without the running of a computer [5–8]. This counterfactual computation exhibits a surprising counterintuitive quantum computational effect, but it seems that it does not have a practical advantage for a specific computational purpose in its present form. Here we apply the fundamental concept of quantum counterfactuality to a real-world communication task in what may be called a ''counterfactual communication.'' We present a novel class of counterfactual protocols of quantum cryptography [9–12] that relies on the ''nontransmission'' of a signal particle (the carrier of secret information): the mere possibility for signal particles to be transmitted is sufficient to create a secret key.

Quantum cryptography, also known as quantum key distribution (QKD), is considered to be a method of providing unconditional security in communications between two remote parties (''Alice'' and ''Bob'' in the example below). It allows, in principle, the seamless distribution of a secret key that can be used efficiently as a one-time pad. Any attempt by an eavesdropper (''Eve'') to gain information about the key can be not only protected against, but also discovered based on the laws of quantum mechanics.

The previous protocols of QKD require the transmission of signal particles through a quantum channel. For instance, Alice prepares a single photon in a quantum state and sends it to Bob. Bob performs a measurement on the received signal photon. Alice and Bob then obtain a perfectly correlated secret key by carrying out the subsequent classical procedures of basis reconciliation, error correction, and privacy amplification. Entanglement-based protocols [13–15] also require the transmission of signal particles. To date, all of the proposed and demonstrated QKD protocols of which we are aware fall into the paradigm of ''signal particle transmission.'' (All communication methods, either classical or quantum, proposed thus far may fall into this paradigm.)

We present an entirely different approach based on the quantum counterfactual effect. Figure 1 shows the typical architecture of the proposed QKD system. The protocol is initiated by triggering the single-photon source S, which emits a short optical pulse containing a single photon. The single-photon pulse passes through the optical circulator C and is then split by the beam splitter BS. The polarization state of the single-photon pulse is chosen at random to have either horizontal polarization $|H\rangle$ representing the bit value ''0'', or vertical polarization $|V\rangle$ representing ''1.'' According to the chosen bit value, the initial quantum state

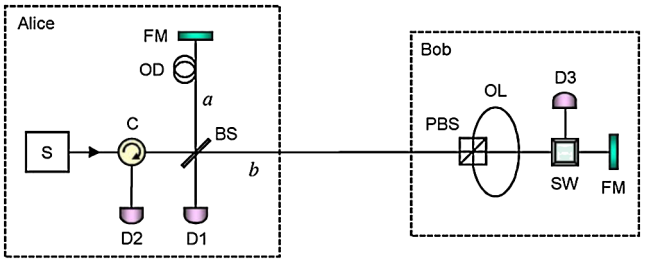

FIG. 1 (color online). Schematic of the proposed QKD system. A single-photon pulse entering a Michelson-type interferometer is split into two pulses by a beam splitter BS and travels through two paths a and b. The interferometer is adjusted using an optical delay OD. Therefore, if the bit values chosen at random by Alice and Bob are different, the two split pulses are recombined in the BS and the single photon is detected at detector $D2$ with certainty as a result of constructive interference. However, if the two bit values are equal, a split pulse going through path b is blocked by detector $D3$. Consequently, the interference is destroyed and the photon can be detected at detector $D1$ with a finite probability. In this case, the photon has been completely isolated from the outside of Alice's secure station, as it has traveled through only path a.

after the BS is given by one of the two orthogonal states

$$|\phi_0\rangle = \sqrt{T}|0\rangle_a|H\rangle_b + i\sqrt{R}|H\rangle_a|0\rangle_b, \quad (1)$$

$$|\phi_1\rangle = \sqrt{T}|0\rangle_a|V\rangle_b + i\sqrt{R}|V\rangle_a|0\rangle_b, \quad (2)$$

where a and b represent, respectively, the path toward Alice's Faraday mirror (FM) and the path toward Bob's site, and where $|0\rangle_k$ denotes the vacuum state in the mode $k = a, b$. R and $T = 1 - R$ are the reflectivity and transmissivity of the BS, respectively.

Bob also randomly chooses one of the two polarizations representing his bit value. Bob blocks the optical path b of the single-photon pulse if the polarization of the pulse is identical to his polarization. The blocking of optical path b in such a polarization-selective way can be suitably accomplished, for instance, using the setup depicted in Bob's site (Fig. 1). If an optical pulse incident on 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 polarization state to the detector $D3$.

On the other hand, if the single-photon pulse has a polarization orthogonal to Bob's, its optical path b is not affected by the SW. Hence, a split pulse travelling through path b may be reflected by the FM in Bob's site and is returned back to the BS. Here, when a split pulse is returned back to the BS, the total optical path length along path b is identical for the two orthogonal polarization states although the two states experience different paths in Bob's site. The function of the two FMs is to transform the polarization state into its orthogonal, to offset possible birefringence effects automatically in the optical paths of the interferometer. It is also assumed that the detectors shown in Fig. 1 can measure the polarization state of a detected photon. (This can be conducted simply by ensuring that each of the detectors has a polarizing beam splitter and two conventional single-photon detectors.)

The interferometer can be stabilized using feedback control; therefore, if Alice's and Bob's bit values differ, the photon leaves the interferometer going toward detector $D2$ with certainty owing to the interference effect (the phase difference is π radians between the two paths a and b). If, however, Alice's and Bob's bit values are equal, the split pulse in path b is blocked by detector $D3$ and the interference is destroyed. In this case, there are three possibilities for a single photon: (i) the photon travels through path a and is detected at detector $D1$ with probability RT; (ii) the photon travels through path a and is detected at detector $D2$ with probability R^2; (iii) the photon goes to Bob through path b and is detected at detector $D3$ with probability T. After the detection of a photon is completed, Alice and Bob tell each other whether or not each of the detectors clicked. If $D2$ or $D3$ clicks, they also announce both the detected polarization state and the initial polarization states that were chosen. This is intended to detect Eve's intervention by monitoring the correct operation of the interferometer. Additionally, if $D1$ clicks alone, Alice compares the detected polarization state to her initial polarization state: if they are consistent, she does not reveal any information about the polarization states; otherwise, she also announces her measurement results.

Alice and Bob can then establish an identical bit string (a "sifted key") by selecting only the events for which $D1$ alone detects a photon with a correct final polarization state. They disregard all other events, including events in which multiple detectors click or where no detector clicks (those events can be monitored to improve the security). The overall efficiency of creating a sifted key bit is $RT/2$. As Alice announces only the fact that a photon was detected at $D1$ with a correct polarization state, the bit information is not revealed to Eve. As in conventional QKD protocols, Alice and Bob can estimate an error rate using small portions of the sifted key obtained this way in order to detect Eve's intervention. A shorter key remaining after the error estimation step may undergo error correction and privacy amplification to become the secure final key.

In the discussion above, a sifted key is created by selecting only the events during which a single photon is detected at $D1$. Thus, in ideal cases, the photons used to create a sifted key have not travelled through path b but only through path a (if the photons have traveled through the path b, they must have been detected at $D3$). The task of a secret key distribution, therefore, can be accomplished without any photon carrying secret information being sent through the quantum channel (path b). A photon that carries secret information has been confined from its birth to death within Alice's secure station, and Eve can never access the photon. Formally speaking, when Alice's and Bob's bit values are equal, the initial state $|\phi_0\rangle$ collapses to one of the two states, $|0\rangle_a|H\rangle_b$ or $|H\rangle_a|0\rangle_b$, and the initial state $|\phi_1\rangle$ collapses to $|0\rangle_a|V\rangle_b$ or $|V\rangle_a|0\rangle_b$, due to Bob's measurement. To create a sifted key bit, Alice and Bob use only two states, $|H\rangle_a|0\rangle_b$ and $|V\rangle_a|0\rangle_b$, among the four collapsed states. Hence, Bob in fact extracts a secret key from the nondetection events.

The security of the proposed protocol can be understood by a no-cloning principle of orthogonal states in a composite system which consists of two subsystems. It is known that there are cases in which orthogonal states cannot be cloned if the subsystems are only available one after the other [16–19]. However, an important point of the present protocol is that Eve can only access one subsystem (path b) while she can never access the other subsystem (the path a). Hence, we present here a new type of no-cloning principle for orthogonal states: if reduced density matrices of an available subsystem are nonorthogonal and if the other subsystem is not allowed access, it is impos-

sible to distinguish two orthogonal quantum states without disturbing them. Let $|\Psi_0\rangle$ and $|\Psi_1\rangle$ be two normalized pure states of a quantum system AB composed of two subsystems, A and B. According to the Schmidt decomposition,

$$|\Psi_0\rangle = \sum_i \lambda_i |i_A\rangle |i_B\rangle, \tag{3}$$

$$|\Psi_1\rangle = \sum_j \lambda_j |j_A\rangle |j_B\rangle, \tag{4}$$

where $|i_A\rangle$ ($|i_B\rangle$) and $|j_A\rangle$ ($|j_B\rangle$) are orthonormal states for the subsystem A (B), and where λ_i and λ_j are the Schmidt coefficients. We also suppose that a unitary operator U acts only on the product space of the subsystem B and Eve's measuring apparatus that is in an initial normalized state $|m\rangle$. To conceal Eve's intervention, the states $|\Psi_0\rangle$ and $|\Psi_1\rangle$ should be left undisturbed after the unitary evolution:

$$U(|\Psi_0\rangle|m\rangle) = |\Psi_0\rangle|m_0\rangle, \qquad U(|\Psi_1\rangle|m\rangle) = |\Psi_1\rangle|m_1\rangle. \tag{5}$$

Here, $|m_0\rangle$ and $|m_1\rangle$ are the final states of Eve's measuring apparatus. As U does not act on subsystem A, Eq. (5) becomes

$$U(|i_B\rangle|m\rangle) = |i_B\rangle|m_0\rangle, \qquad U(|j_B\rangle|m\rangle) = |j_B\rangle|m_1\rangle. \tag{6}$$

Thus, by unitarity,

$$\langle i_B|j_B\rangle = \langle i_B|j_B\rangle\langle m_0|m_1\rangle \tag{7}$$

from which it follows that either $|m_0\rangle = |m_1\rangle$, or $\langle i_B|j_B\rangle = 0$ for all i and j. The condition $\langle i_B|j_B\rangle = 0$ for all i and j implies that reduced density matrices of the subsystem B, $\rho_s(B) = \mathrm{Tr}_A[|\Psi_s\rangle\langle\Psi_s|]$, are orthogonal ($\mathrm{Tr}[\rho_0(B)\rho_1(B)] = 0$). Therefore, provided that the reduced density matrices of the available subsystem B are nonorthogonal, Eve cannot gain any information without disturbing the states $|\Psi_0\rangle$ or $|\Psi_1\rangle$, even when the states are orthogonal. It can be verified from Eqs. (1) and (2) that the reduced density matrices of the available subsystem (the path b) are nonorthogonal. That is, $\mathrm{Tr}[\rho_0(\text{path } b)\rho_1(\text{path } b)] = R^2 \neq 0$, where $\rho_s(\text{path } b) = \mathrm{Tr}_{\text{path } a}[|\phi_s\rangle\langle\phi_s|]$. For $R = 0$, however, the states $|\phi_0\rangle$ and $|\phi_1\rangle$ can be distinguished without disturbance, which is consistent with our intuition.

In conventional QKD protocols relying on the transmission of a signal particle, Eve can fully access, individually or coherently, signal particles sent through the quantum channel. In the present protocol, however, Eve cannot access the entire quantum system of each signal particle, but only part of the quantum system [20]. This distinctive property naturally leads to practical security advantages in various situations (see Appendix in Ref. [21] for detailed analysis of several eavesdropping strategies).

A complete analysis of the QKD security, including various experimental imperfections, is left for future study [22–26]. However, it is worthwhile to point out here that the present protocol provides clear security advantages for cases in which weak coherent pulses with nonzero multiphoton probabilities are used for practical implementation in place of single-photon pulses. First, Eve cannot determine the number of photons in each pulse because she is not allowed to access path a. Furthermore, it is impossible for Eve to measure even the number of photons travelling through the quantum channel (path b), provided that she does not disturb the states. Eve obtains ''which-path'' information through the photon number measurement in path b, and she destroys the interference. Hence, Eve may cause detection errors, and she may be detected due to the photon number measurement itself. Thus, the present protocol is inherently robust against the so-called ''photon-number-splitting'' attack [27,28]. Second, Eve cannot split a photon when all of the photons in the pulse travel through path a. That is, if all of the photons are detected at $D1$ after traveling through path a, the bit information is not revealed to Eve, even when a multiphoton pulse is used. Finally, Eve cannot obtain a copy of the initial quantum state even when she succeeds in splitting a photon. That is, Eve only obtains a ''collapsed'' state whenever she knows that she has a photon, and she remains limited by the no-cloning theorem.

Every component and device needed for the proposed QKD system is currently available. Therefore, actual implementation of the present protocol is expected to appear soon for short-range applications [29]. For long-distance implementations, however, it seems that there are two technical difficulties. One is the high channel loss due to the round-trip path. This channel loss problem may be overcome if the security advantages of the present protocol could allow the use of higher light intensity than previous protocols. The second difficulty is that it may be hard to stabilize a long-armed interferometer. However, considering recent experimental developments related to this problem [30], it seems that the present protocol may eventually operate over (at least) several tens of kilometers.

We have considered a Michelson-type interferometer using two orthogonal states merely because it is simple and feasible for practical applications. It is clear that the present protocol can be modified to incorporate the features of other QKD protocols. For instance, instead of using two orthogonal polarization states, it is possible to use either four polarization states as in the BB84 protocol [10] or two nonorthogonal states as in the B92 protocol [11]. When two nonorthogonal states are used, the proposed protocol becomes more robust, at the expense of key rate, against a passive beam-splitting attack in which Eve can insert a beam splitter and replace the quantum channel by an ideal lossless channel without inducing any error. If there is some loss in the quantum channel and if weak coherent pulses are used, Eve can sometimes obtain information about the bit value using the passive beam-splitting

attack. However, if two nonorthogonal polarization states are used, Eve cannot learn about the bit value even when she succeeds in splitting a photon. In addition, it is noteworthy that these protocols can also be correctly implemented using a Mach-Zehnder type interferometer [31]. It seems that various protocols and implementation schemes will appear within the counterfactual paradigm, where the central concept is the nontransmission of a signal particle.

We thank Hoi-Kwong Lo for helpful comments on the manuscript. This work was partially supported by the IT R&D program of MKE/IITA (2005-Y-001-05 and 2008-F-035-02).

*tgnoh@etri.re.kr

[1] A. C. Elitzur and L. Vaidman, Found. Phys. **23**, 987 (1993).
[2] P. G. Kwiat *et al.*, Phys. Rev. Lett. **83**, 4725 (1999).
[3] T.-G. Noh and C. K. Hong, Quantum Semiclass. Opt. **10**, 637 (1998).
[4] R. Penrose, *Shadows of the Mind* (Oxford Univ. Press, New York, 1994), p. 240.
[5] R. Jozsa, in *Lecture Notes in Computer Science*, edited by C. P. Williams (Springer-Verlag, Berlin, 1999), Vol. 1509, p. 103.
[6] G. Mitchison and R. Jozsa, Proc. R. Soc. A **457**, 1175 (2001).
[7] O. Hosten, M. T. Rakher, J. T. Barreiro, N. A. Peters, and P. G. Kwiat, Nature (London) **439**, 949 (2006).
[8] L. Vaidman, Phys. Rev. Lett. **98**, 160403 (2007).
[9] S. Wiesner, SIGACT News **15**, 78 (1983).
[10] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE press, New York, 1984), p. 175.
[11] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[12] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[13] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[14] C. H. Bennett, G. Brassard, and N. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
[15] K. Boström and T. Felbinger, Phys. Rev. Lett. **89**, 187902 (2002); A. Wójcik, Phys. Rev. Lett. **90**, 157901 (2003); Q.-Y. Cai, Phys. Rev. Lett. **91**, 109801 (2003).
[16] W. K. Wootters and W. H. Zurek, Nature (London) **299**, 802 (1982).
[17] T. Mor, Phys. Rev. Lett. **80**, 3137 (1998).
[18] M. Koashi and N. Imoto, Phys. Rev. Lett. **79**, 2383 (1997).
[19] L. Goldenberg and L. Vaidman, Phys. Rev. Lett. **75**, 1239 (1995).
[20] The protocols proposed in Ref. [15] have an analogous feature where an eavesdropper has access to only one of two photons prepared in the Bell states; they are called two-way protocols in the sense that a signal photon actually travels forward and backward on the quantum channel. In our protocol, however, there is only a ''possibility'' for a photon to travel forth and back. Hence, our protocol is not a two-way scheme in the usual sense, but rather a counterfactual scheme.
[21] T.-G. Noh, arXiv:0809.3979v2.
[22] D. Mayers, in *Lecture Notes in Computer Science*, edited by N. Koblitz (Springer-Verlag, Berlin, 1996), Vol. 1109, p. 343.
[23] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).
[24] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[25] H. Inamori, N. Lütkenhaus, and D. Mayers, Eur. Phys. J. D **41**, 599 (2007).
[26] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **4**, 325 (2004).
[27] N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000).
[28] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).
[29] J. L. Duligall, M. S. Godfrey, K. A. Harrison, W. J. Munro, and J. G. Rarity, New J. Phys. **8**, 249 (2006).
[30] M. Musha *et al.*, Appl. Phys. B **82**, 555 (2006); S. M. Foreman *et al.*, Phys. Rev. Lett. **99**, 153601 (2007); J. Minář, H. de Riedmatten, C. Simon, H. Zbinden, and N. Gisin, Phys. Rev. A **77**, 052325 (2008).
[31] From a conceptual viewpoint, the present protocol might be simpler to understand if one considers two independent Elitzur-Vaidman's Mach-Zehnder type interferometers, each lying mostly in Alice's station, but with a portion of one arm in Bob's station. In this version, Alice launches a single photon into an interferometer chosen at random among the two interferometers. Bob also randomly chooses one of the two interferometers to block the arm with a detector.