Quantum cryptography using single-particle entanglement

Jae-Weon Lee and Eok Kyun Lee
Department of Chemistry, School of Molecular Science (BK 21), Korea Advanced Institute of Science and Technology, Taejon 305-701, Korea

Yong Wook Chung and Hai-Woong Lee
Department of Physics, Korea Advanced Institute of Science and Technology, Taejon 305-701, Korea

Jaewan Kim
School of Computational Sciences, Korea Institute for Advanced Study, 207-43 Cheongryangri-dong, Dongdaemun-gu Seoul 130-012, Korea

(Received 21 February 2003; published 23 July 2003)

A quantum cryptography scheme based on entanglement between a single-particle state and a vacuum state is proposed. The scheme utilizes linear optics devices to detect the superposition of the vacuum and single-particle states. Existence of an eavesdropper can be detected by using a variant of Bell's inequality.

DOI: 10.1103/PhysRevA.68.012324 PACS number(s): 03.67.−a, 03.67.Dd, 03.67.Lx

Entanglement could be exploited in many interesting applications, including quantum teleportation [1,2] and quantum cryptography [3]. Discussion on the nonlocal nature (entanglement) of quantum systems was initiated by Einstein, Podolsky, and Rosen (EPR) [4] and later extended by Bell [5–7]. Since then many authors have studied the physical meaning of the nonlocality of a single particle [8–15]. Generally, quantum cryptography schemes based on entanglement (EPR-based schemes) use two or more spatially separated particles possessing correlated properties as the source of entanglement. However, recent developments in experimental techniques [16–18] for generating and manipulating single photons have made quantum information processing utilizing single-particle entanglement feasible. Here, single-particle entanglement refers to entanglement of a single-particle state and the vacuum state [19].

In the present study, we have developed a quantum cryptography scheme based on single-particle entanglement. The proposed scheme utilizes linear optics to detect a superposition of the vacuum state and a single-photon state. A variant of Bell's inequality suggested by Peres [20] is used for the detection of eavesdropping. In fact, the idea of quantum cryptography using single-particle entanglement is not new. Examples of other approaches that can be considered as quantum cryptography schemes using single-particle entanglement are the phase coding scheme of Bennett [21] and Ardehali's scheme based on the delayed choice experiment [22], which uses interferometers. In these double-rail schemes, detection of a particle state is performed by a single observer at a given site. A characteristic feature of our single-rail scheme is that both of two spacelike separated parties, whom we call Alice and Bob, detect either a single particle or no particle at their respective sites. This characteristic makes our scheme more compatible with the original meaning of quantum nonlocality [23].

We begin with a description of our scheme, which is depicted in Fig. 1. The setup consists of a single-photon source (S) and a lossless 50/50 beam splitter (BS_0), which generate the single-particle entanglement state, and two identical non-deterministic projective measurement devices belonging to Alice and Bob, respectively. Each projective measurement device shown in detail in Fig. 2 itself consists of a lossless 50/50 beam splitter (BS_A or BS_B) with a probe state $\gamma|0\rangle + \delta|1\rangle$ and two photon detectors (D_{Aa}, D_{Ab} or D_{Ba}, D_{Bb}). We assume that every beam splitter induces a sign change in a transmitted beam incident on the black side (Eq. (2)).

The output state emerging from the beam splitter BS_0 is given by [see Eq. (4)]

$$|\phi\rangle = \frac{1}{\sqrt{2}}(|1\rangle_A|0\rangle_B - |0\rangle_A|1\rangle_B), \tag{1}$$

where subscripts A and B refer to the modes of the photons exiting the beam splitter through the output ports A (towards Alice) and B (towards Bob), respectively, and $|1\rangle$ and $|0\rangle$ are the single-photon state and the vacuum state, respectively.

The state given in Eq. (1) represents a single-photon entangled state. Following the argument of Peres [20] , Alice and Bob, who test a violation of Bell's inequality, measure the projection on the superposed state of a single particle and the vacuum $\alpha|0\rangle + \beta|1\rangle$. However, detection of the superposition of a particle state and the vacuum state is made diffi-

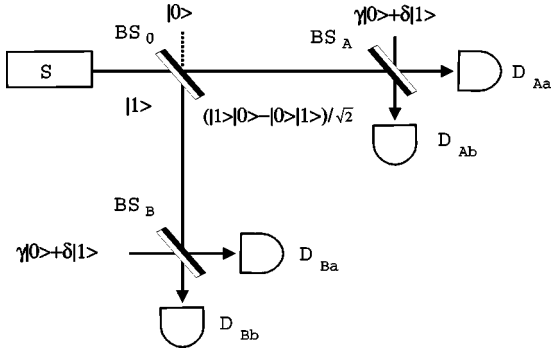

FIG. 1. Schematic of the experimental setup for quantum cryptography based on single-particle entanglement. See text for a detailed explanation.

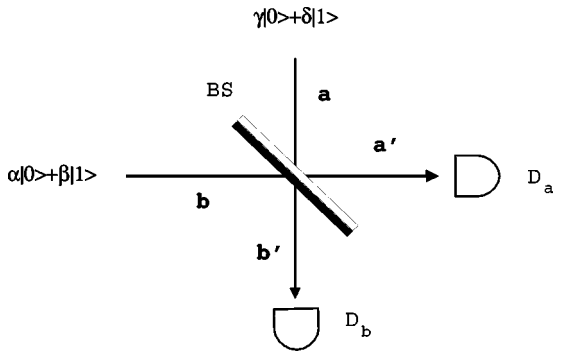

FIG. 2. Schematic of a device for performing a nondeterministic projective measurement of the superposition state of the vacuum and a single photon $\alpha|0\rangle+\beta|1\rangle$. $\gamma|0\rangle+\delta|1\rangle$ is a known probe state.

cult by the fact that the superposed state is not a particle number eigenstate. The experimental setup shown in Fig. 2, which is a generalization of the setup considered in Ref. [24], can be used to detect the superposed state. The beam splitter *BS* (corresponding to the beam splitter BS_A or BS_B in Fig. 1) performs the mode transformation

$$\begin{pmatrix} a' \\ b' \end{pmatrix} = \begin{pmatrix} \sqrt{R} & \sqrt{1-R} \\ -\sqrt{1-R} & \sqrt{R} \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}, \tag{2}$$

where R is the reflectivity of the beam splitter. Using the second-quantized notation, the general form of the input state shown in Fig. 2 can be written as

$$\psi = (\gamma+\delta a^\dagger)(\alpha+\beta b^\dagger)|0\rangle, \tag{3}$$

with normalization requirements $\gamma^2+\delta^2=1$ and $\alpha^2+\beta^2=1$. Here, $\gamma|0\rangle+\delta|1\rangle$ is a known probe state with fixed γ and δ, while $\alpha|0\rangle+\beta|1\rangle$ is an unknown state to be measured. The probe state can be prepared by linear optics with coherent light and a single-photon state [24] or by parametric down-conversions [10]. By replacing a and b in Eq. (3) with a' and b' obtained from transformation (2), we obtain the following output state:

$$\begin{aligned} \psi = [&\alpha\gamma+\sqrt{R(1-R)}\beta\delta(a'^{\dagger 2}-b'^{\dagger 2})-\beta\delta(1-2R)a'^\dagger b'^\dagger \\ &+(\sqrt{1-R}\beta\gamma+\sqrt{R}\alpha\delta)a'^\dagger \\ &+(\sqrt{R}\beta\gamma-\sqrt{1-R}\alpha\delta)b'^\dagger]|0\rangle. \end{aligned} \tag{4}$$

Hence, by setting $R=1/2$ and choosing γ and δ which satisfy

$$\alpha\delta=\beta\gamma, \tag{5}$$

one finds that the coefficient of the $b'^\dagger$ term vanishes while that of the $a'^\dagger$ term does not. In other words, there is a possibility that detector D_a detects a single photon, while D_b detects none. By noting this event, one can perform a nondeterministic projection on the superposition state $\alpha|0\rangle+\beta|1\rangle$. Using the parameters chosen above, the output state can be written as

$$\psi = \alpha\gamma|00\rangle+\sqrt{2}\beta\gamma|10\rangle+\frac{\beta\delta}{\sqrt{2}}(|20\rangle-|02\rangle), \tag{6}$$

where $|ij\rangle$ denotes the state with i particles in mode a' and j particles in mode b'. Thus, the probability of measuring $|10\rangle$ is $2|\beta\gamma|^2\leq 1/2$, because $|\gamma|=|\alpha|$ from Eq. (5). Similarly, if the input state is $\alpha|0\rangle-\beta|1\rangle$, the roles of the $a'^\dagger$ and $b'^\dagger$ terms are interchanged and we obtain the $|01\rangle$ term instead of the $|10\rangle$ term. In this way, the observers are able to measure a projection on a superposed state $\alpha|0\rangle\pm\beta|1\rangle$ [P'_A and P'_B in Eq. (7)] of a single photon and the vacuum. When we measure a projection on the input state $|1\rangle$ [P_A and P_B in Eq. (7)] which is not a superposed state, $\alpha=0$ and hence $\gamma=0$, so according to Eq. (6) we observe a two-photon event instead of the single-photon event. (Or, in this case we can simply remove the beam splitter in Fig. 2 and check whether the detector D_a fires or not.)

We now discuss how to detect the presence of an eavesdropper using the projective measurement devices described above in conjunction with Bell's inequality. Choosing four projection operators

$$\begin{aligned} &P_A \equiv |1\rangle_A\langle 1|_A, \quad P_B \equiv |1\rangle_B\langle 1|_B, \\ &P'_A \equiv (\alpha|0\rangle_A+\beta|1\rangle_A)(\alpha^*\langle 0|_A+\beta^*\langle 1|_A), \\ &P'_B \equiv (\alpha|0\rangle_B-\beta|1\rangle_B)(\alpha^*\langle 0|_B-\beta^*\langle 1|_B), \end{aligned} \tag{7}$$

one can obtain expectation values of the operators

$$\begin{aligned} &\langle\phi|P'_A|\phi\rangle = \langle\phi|P'_B|\phi\rangle = \frac{1}{2}, \\ &\langle\phi|P'_AP_B|\phi\rangle = \langle\phi|P_AP'_B|\phi\rangle = \frac{|\beta|^2}{2}, \\ &\langle\phi|P_AP_B|\phi\rangle = 0, \quad \langle\phi|P'_AP'_B|\phi\rangle = 2|\alpha\beta|^2. \end{aligned} \tag{8}$$

From these expectation values, one can define a quantity

$$\begin{aligned} S \equiv &\langle\phi|P'_A+P'_B-P'_AP'_B-P'_AP_B-P_AP'_B+P_AP_B|\phi\rangle \\ = &|\alpha|^2(1-2|\beta|^2), \end{aligned} \tag{9}$$

which violates the following version of Bell's inequality, formulated by Peres:

$$0\leq S\leq 1 \tag{10}$$

when $|\beta|>1/\sqrt{2}$ and $\alpha\neq 0$. This inequality is obtained when we assume a local hidden variable. As usual, possible interception, detection, and substitution of the photons by an eavesdropper is equivalent to introducing a local hidden variable into the system. In this case, Alice and Bob obtain not S but

$$S_E = \int \rho(E_A,E_B)dE_A dE_B[p_A(E_A,A') + p_B(E_B,B') - p_A(E_A,A')p_B(E_B,B') - p_A(E_A,A')p_B(E_B,B) - p_A(E_A,A)p_B(E_B,B') + p_A(E_A,A)p_B(E_B,B)], \tag{11}$$

where $\rho(E_A,E_B)$ is the probability that Eve measures the projection on a state $|E_A\rangle$ at photon A ($P_{|E_A\rangle}$) and $|E_B\rangle$ at photon B ($P_{|E_B\rangle}$). This represents the strategy of the eavesdropper. $p_A(E_A,A')$ denotes the probability of a count from Alice's detector when she tests the projection operator P'_A after Eve has tested the projection operator $P_{|E_A\rangle}$ on the photon A. It is expressed by the quantum calculation

$$p_A(E_A,A') = \langle\phi|P'_A P_{|E_A\rangle}|\phi\rangle. \tag{12}$$

For example, setting $\alpha = 1/2$ and $\beta = \sqrt{3}/2$ and considering the special case in which the eavesdropper measures only photon A, we obtain from Eqs. (7) and (12)

$$S_E = \int \rho(E_A,E_B)dE_A dE_B[1 - p_A(E_A,A')] = \int \rho(E_A)dE_A\left[1 - \left|\alpha' + \frac{\sqrt{3}}{2}\beta'\right|^2\right], \tag{13}$$

where $|E_A\rangle \equiv \alpha'|0\rangle_A + \beta'|1\rangle_A$. With the triangle inequality, this implies $1/4 \leqslant S_E \leqslant 1$, which contradicts the quantum prediction of $S = -1/8$ obtained from Eq. (9) for the system with no eavesdropper. In this respect, one may say that our scheme represents another experimental method for examining the single-particle nonlocality.

We may now proceed to the discussion of a key distribution scheme going as follows.

(i) The photon source (S) and beam splitters (BS_0) periodically generate the single photon entangled state.

(ii) At a photon arrival time, Alice measures a projection operator randomly chosen between P_A and P'_A. Similarly, at the same time, Bob measures P_B or P'_B. This corresponds to the selection of the analyzer axis in ordinary two particle quantum cryptography schemes.

(iii) After a series of measurements, Alice and Bob announce to each other which projection operator they chose. If Alice chose P_A and Bob chose P_B (probability 1/4), one of them will detect a photon and the other will not. Then they can share a random raw key 1 (say, for a photon) and 0 (for vacuum). With a probability of 3/4, either Alice chooses P'_A or Bob chooses P'_B. Since their results are not anticorrelated [see Eq. (8)] in these cases, they cannot extract keys. However, these discarded data together with the anticorrelated data from the previous step can be used to detect eavesdroppers, as shown in the next step.

(iv) Detection of eavesdroppers is possible by publicly comparing a subset of the results of Alice and Bob using Eqs. (9) and (10), as described above.

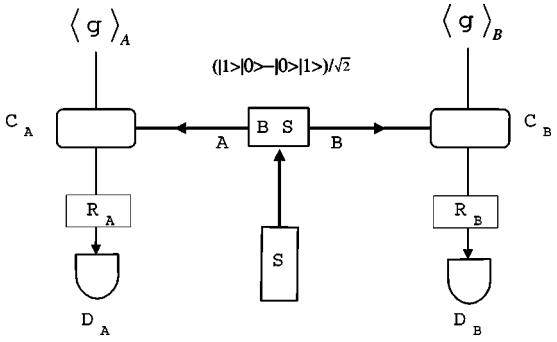

FIG. 3. Schematic of the apparatus for quantum cryptography with deterministic projective measurement using cavity QED.

We now briefly discuss another scheme that adopts deterministic projective measurement devices using cavity QED. The setup of this scheme, shown in Fig. 3, is similar to that considered by Davidovich *et al.*, Freyberger, Moussa, and Baseia [25–27], except that the single-particle entangled state $|\phi\rangle$ is generated not by an atom crossing the two cavities, but by the beam splitter and the single-photon source as in Fig. 1.

Assuming that at time $t=0$, two ground-state atoms $|g\rangle_A$ and $|g\rangle_B$ are injected into the cavities C_A and C_B, respectively, the total cavities-atom state is then $|\psi(0)\rangle = |\phi\rangle|g\rangle_A|g\rangle_B$. The interaction between atoms and photons in the cavity $C_k (k=A,B)$ is described by the Jaynes-Cummings Hamiltonian

$$H_I^k = \hbar\lambda(\sigma_{+,k}a_k + \sigma_{-,k}a_k^\dagger), \tag{14}$$

where λ is a coupling constant and $\sigma_{+,k}, \sigma_{-,k}$, and $a_k^\dagger, a_k$ are the raising and lowering operators for the atom and photon states, respectively. In the cavities, these atoms interact with the photons injected into the cavities. In Refs. [25–27], it was shown that by choosing the interaction time t to be $\lambda t = \pi/2$, one can replicate the information of the entanglement of the photon states $|\phi\rangle$ to that of the atoms. In other words, the state becomes

$$|\psi(t)\rangle = \exp[-i/\hbar(\Sigma_k H_I^k)t]|\psi(0)\rangle = \frac{1}{\sqrt{2}}(|e\rangle_A|g\rangle_B - |g\rangle_A|e\rangle_B)|0\rangle_A|0\rangle_B. \tag{15}$$

The projective measurement on $\alpha|0\rangle + \beta|1\rangle$ can be performed as follows. Microwave fields are appropriately adjusted in the Ramsey zones (R_k) such that a superposition of the ground state and the excited state of the atom, $\alpha|g\rangle_k + \beta|e\rangle_k$, with $|\alpha|^2 + |\beta|^2 = 1$, undergoes a unitary evolution to the excited state $|e\rangle_k$, which registers a click in the state-selective ionization detector D_k. Except for the measurement devices, the procedure followed in this scheme is the same as that with linear optics devices shown in Fig. 1.

Our scheme has the following merits compared to ordinary quantum cryptography schemes. First, compared to the ordinary two-particle EPR-based scheme, it is easier for our scheme to generate vacuum and single-particle entangle-

ments using beam splitters. Of course, our model entails the detection of a superposition of the vacuum and single-photon states, which is rather difficult to implement. However, the difficulty involved in detecting the superposed state will also be encountered by eavesdroppers. Second, compared to non-EPR based schemes such as the BB84 scheme, it is easier for the EPR-based schemes to use quantum repeaters [28] based on quantum teleportation [15] to send information to distant observers. One shortcoming of our scheme is that, due to low detection efficiency, Bob may sometimes confuse a loss of signal with the vacuum state. In this case, Alice and Bob need to distill a secret key from the series of keys using privacy amplification [29].

In summary, we have proposed a quantum cryptography technique based on single-particle entanglement using linear optics devices and Bell's inequality to detect the presence of eavesdroppers.

We acknowledge support by the Korea Research Foundation Grant No. KRF-2002-070-C00048. H. Lee and J. Kim were supported by the Korea Research Foundation (Grant No. KRF-2002-070-C00029).

[1] C.H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W.K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[2] D. Bouwmeester, J.W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, Nature (London) **390**, 575 (1997); D. Boschi, S. Branca, F. De Martini, L. Hardy, and S. Popescu, Phys. Rev. Lett. **80**, 1121 (1998); A. Furusawa, J.L. Sorensen, S.L. Braunstein, C.A. Fuchs, H.J. Kimble, and E.S. Polzik, Science **282**, 706 (1998).
[3] A.K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[4] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).
[5] J.S. Bell, Physics (Long Island City, N.Y.) **1**, 195 (1964).
[6] S.J. Freeman and J.F. Clauser, Phys. Rev. Lett. **28**, 938 (1972); J.F. Clauser and A. Shimony, Rep. Prog. Phys. **41**, 1881 (1978).
[7] A. Aspect, P. Grangier, and G. Roger, Phys. Rev. Lett. **47**, 460 (1981); **49**, 91 (1982); A. Aspect, J. Dalibard, and G. Roger, *ibid.* **49**, 1804 (1982).
[8] G. Björk, P. Jonsson, and L.L. Sánchez-Soto, Phys. Rev. A **64**, 042106 (2001).
[9] S.M. Tan, D.F. Walls, and M.J. Collet, Phys. Rev. Lett. **66**, 252 (1991); S.M. Tan, M.J. Holland, and D.F. Walls, Opt. Commun. **77**, 285 (1990).
[10] L. Hardy, Phys. Rev. Lett. **73**, 2279 (1994); L. Vaidman, *ibid.* **75**, 2063 (1995); D.M. Greenberger, M.A. Horne, and A. Zeilinger, *ibid.* **75**, 2064 (1995); L. Hardy, *ibid.* **75**, 2065 (1995).
[11] E. Santos, Phys. Rev. Lett. **68**, 894 (1992); S.M. Tan, D.F. Walls, and M.J. Collet, *ibid.* **68**, 895 (1992).
[12] M. Revzen and A. Mann, Found. Phys. **26**, 847 (1996).
[13] C.C. Gerry, Phys. Rev. A **53**, 4583 (1996).
[14] M. Michler, H. Weinfurter, and M. Zukowski, Phys. Rev. Lett. **84**, 5457 (2000).
[15] H.W. Lee and J.K. Kim, Phys. Rev. A **63**, 012305 (2001).
[16] G.J. Milburn, Phys. Rev. Lett. **62**, 2124 (1989).
[17] J.C. Howell and J.A. Yeazell, Phys. Rev. A **62**, 012102 (2000).
[18] C.K. Hong and L. Mandel, Phys. Rev. Lett. **56**, 58 (1986); J. Kim, O. Benson, H. Kan, and Y. Yamamoto, Nature (London) **397**, 500 (1999); C. Brunel, B. Lounis, P. Tamarat, and M. Orrit, Phys. Rev. Lett. **83**, 2722 (1999).
[19] M. Czachor, Phys. Rev. A **49**, 2231 (1994); D. Home and G.S. Agarwal, Phys. Lett. A **209**, 1 (1995).
[20] A. Peres, Phys. Rev. Lett. **74**, 4571 (1992); **76**, 2205 (1996).
[21] C.H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[22] M. Ardehali, Phys. Lett. A **217**, 301 (1996).
[23] E. Knill, R. Laflamme, and G.J. Milburn, Nature (London) **409**, 46 (2001).
[24] A.P. Lund and T.C. Ralph, Phys. Rev. A **66**, 032307 (2002); D.T. Pegg *et al.*, Phys. Rev. Lett. **81**, 1604 (1604).
[25] L. Davidovich *et al.*, Phys. Rev. A **50**, R895 (1994).
[26] M.H.Y. Moussa and B. Baseia, Phys. Lett. A **245**, 335 (1998).
[27] M. Freyberger, Phys. Rev. A **51**, 3347 (1995).
[28] M. Zukowski *et al.*, Phys. Rev. Lett. **71**, 4287 (1993); H.-J. Briegel *et al.*, *ibid.* **81**, 5932 (1998).
[29] C.H. Bennett *et al.*, SIAM J. Comput. **17**, 210 (1998).