Quantum Cryptography Based on Split Transmission of One-Bit Information in Two Steps

Masato Koashi and Nobuyuki Imoto
NTT Basic Research Laboratories, 3-1 Morinosato Wakamiya, Atsugi, Kanagawa 243-01, Japan

(Received 5 March 1997)

We propose a simple quantum cryptographic scheme involving truly two orthogonal states. The security of the protocol is based on splitting the transfer of one-bit information into two steps, ensuring that only a fraction of the bit information is transmitted at a time. A particular implementation with an asymmetric interferometer is presented, which does not require the random timing of the packet sending as was used by Goldenberg and Vaidman [Phys. Rev. Lett. **75**, 1239 (1995)]. [S0031-9007(97)04075-1]

PACS numbers: 89.70.+c, 03.65.−w

One of the goals in cryptography is to allow two remote parties to share a random bit sequence ("key") without any leaks to the rest of the world. Once the sharing is attained, the two parties can secretly exchange a message over the public channel by encrypting them with a key with an equal length to the message. In the key distribution with classical transmission lines, an eavesdropper can freely sneak into the transmissions and monitor the information. Thus the role of cryptography is to provide some mathematical procedure that makes it computationally difficult for the eavesdropper to reproduce the key from the information sent through the transmission lines. However, no existing classical cryptosystems have been proven to present sufficient difficulty to an eavesdropper. In particular, it was shown that some of them can be broken in principle by quantum computation [1]. On the other hand, in quantum cryptography [2], the key is sent over a quantum channel in order to benefit from the laws of quantum mechanics. In this case the eavesdropper can also intervene and read the key, but this inevitably introduces transmission errors. For detecting these errors, the legal users verify a portion of the shared key over an unjammable classical channel. If too many errors are detected, they agree on discarding the key, and the key left to the eavesdropper turns out to be valueless. If the number of errors is tolerable the users can probably obtain a secure final key [3].

In recent years many schemes for quantum cryptography have been proposed [2,4–11] and experimentally demonstrated [12]. The first scheme, presented by Bennett and Brassard [2], uses four states of single photons polarized along different directions. In this scheme, in principle, the receiver (henceforth "Bob") can recognize every bit sent by the sender (henceforth "Alice"), if Bob delays his measurement. A simpler scheme was proposed by Bennett [6], which uses only two nonorthogonal states. In this method, nonorthogonal encoding of the bit information inevitably leads to the waste of a portion of photons. In contrast with these schemes that use nonorthogonal states, Goldenberg and Vaidman proposed [9] a scheme utilizing orthogonal encoding, which ideally wastes no photons. In this scheme, only watching out for errors in the regularly transmitted bits is not sufficient for the detection of an eavesdropper because it is possible for her to send a packet of a dummy photon beforehand. This loophole was covered by sending photons at random and secret intervals, and by confirming later that the photons were received at the proper timing. The random sending times can be replaced by random discrete sending times [9]. Noting that sending no photons is equivalent to sending the vacuum state, in this protocol the sender actually chooses among three states (two encoded and one the vacuum) at each discrete time. Thus, this scheme is made up of three orthogonal states. So far, therefore, more than three states were necessary in order to attain 100% use of photons, and waste of photons was inevitable with two-state cryptography because the two states are nonorthogonal.

In this Letter, we propose a quantum cryptography using two orthogonal states (hence with 100% use of photons in the ideal case) based on split transmission of one-bit information in two steps. The test for the presence of an eavesdropper requires only the verification of the part of the transmitted bits, and no auxiliary tests such as timing identification for the randomly generated photons are necessary. We present a particular implementation in which asymmetry is introduced in the interferometer used in Ref. [9] so that only a fraction of one-bit information is transmitted at a time. This allows us to avoid the random timing test. A protocol with the minimal number of states and no limitation on efficiency may also be important from the practical point of view.

Consider a protocol where Alice transmits one-bit information to Bob in two steps, by sending a packet in each step. After the two steps, Bob performs measurement on the two packets and obtains the full one bit. The amount of the information transfer just after the first step may be estimated from the bit-value dependence of the reduced density operator of the first packet. In an extreme case (case I) where Bob receives the full bit after the first step, an eavesdropper can freely obtain the bit value because it is encoded in orthogonal states. In the opposite case (case II) where no information is transferred by the first step, the eavesdropper can replace the first packet by a fake one because the first packet is independent of the bit value. Then, at the second step she obtains the bit value from the two original packets and inserts a second fake packet that is properly correlated to the first fake packet. The scheme in Ref. [9] belongs to case II and this is why the scheme needs the random timing. Our scheme lies in the intermediate between case I and II, where a fraction of one-bit information is transferred in the first step, and the rest of the information is transferred in the second step. Here the eavesdropper cannot extract the bit value without causing bit errors, as shown below.

Figure 1 shows a typical implementation of our scheme. It consists of a Mach-Zehnder interferometer similar to the setup in Ref. [9], except that the two beam splitters (BS1 and BS2) are identical beam splitters with transmissivity T and reflectivity $R = 1 - T$, where $R \neq T$. The phase difference between the two arms is adjusted to π. Beam splitter BS1 is located in Alice's site and BS2 is located in Bob's site. Two equal-time delay lines (D_a and D_b) are installed in both arms. The role of this delay is to prevent any eavesdropper (henceforth "Eve") from accessing the packet in arm a after she accesses that in arm b. This is one of the essential points in the scheme of orthogonal coding [9]. For the above requirement, the optical length of the delay lines needs not exceed the optical length L of the lines between Alice and Bob. They have only to be longer than the difference between L and the distance between Alice and Bob's sites. We assume that the transmission and the detection are ideal, i.e., lossless and error free.

For the transmission of one bit of the key, Alice randomly chooses the bit value "0" or "1," and injects a single photon into the port A0 or A1 of BS1, depending on the chosen bit value. The states $|\Phi_j\rangle$ for the bit value $j = 0, 1$ after passing BS1 is written as

$$|\Phi_0\rangle = \sqrt{T}\,|0\rangle_a|1\rangle_b - i\sqrt{R}\,|1\rangle_a|0\rangle_b\,, \qquad (1)$$

$$|\Phi_1\rangle = \sqrt{T}\,|1\rangle_a|0\rangle_b - i\sqrt{R}\,|0\rangle_a|1\rangle_b\,, \qquad (2)$$

where $|n\rangle_s$ is the n photon Fock state for the arm $s = a, b$. The two states $|\Phi_0\rangle$ and $|\Phi_1\rangle$ are orthogonal, and Bob can indeed distinguish between them by using the setup shown in Fig. 1, as follows. Assuming that the phase shift π is introduced just before BS2, the transformation of the states is written as

$$|1\rangle_a|0\rangle_b \rightarrow \sqrt{T}\,|0\rangle_0|1\rangle_1 - i\sqrt{R}\,|1\rangle_0|0\rangle_1\,, \qquad (3)$$

$$|0\rangle_a|1\rangle_b \rightarrow -(\sqrt{T}\,|1\rangle_0|0\rangle_1 - i\sqrt{R}\,|0\rangle_0|1\rangle_1)\,. \qquad (4)$$

Applying these rules to $|\Phi_j\rangle$, the states $|\Psi_j\rangle$ after BS2 for the bit values $j = 0, 1$ are

$$|\Psi_0\rangle = -|1\rangle_0|0\rangle_1\,, \qquad (5)$$

$$|\Psi_1\rangle = |0\rangle_0|1\rangle_1\,. \qquad (6)$$

This means that the initial state $|\Phi_0\rangle$ always triggers detector D0 and $|\Phi_1\rangle$ triggers the other detector D1. Therefore, Bob can receive every bit sent by Alice in the ideal case assumed here.

In order to understand the implication of the asymmetry, let us consider an example of Eve's intervention strategy (strategy I) depicted in Fig. 2(a). Using a beam splitter BS3 identical to BS1 and a delay D_a' identical to D_a, Eve copies the detection apparatus at Bob's site and learns the bits sent by Alice perfectly. Using an apparatus similar to Alice's, she would send Bob a fake photon according to the bit just learned, but a problem arises here. She has to send the packet into Bob's delay D_a before the packet running along arm b emerges from Alice's delay, namely, before she learns the bit value chosen by Alice. Thus, practically she has to inject a fake photon into one port of BS4 regardless of the bit value. If the beam splitters used by Alice and Bob have $T = R$, Eve can effectively make as if she injected the photon to the other port

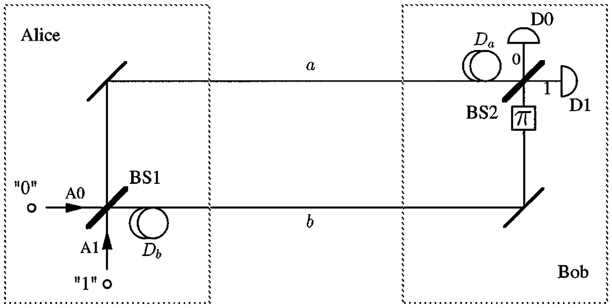

FIG. 1. Schematic representation of the proposed cryptographic scheme.

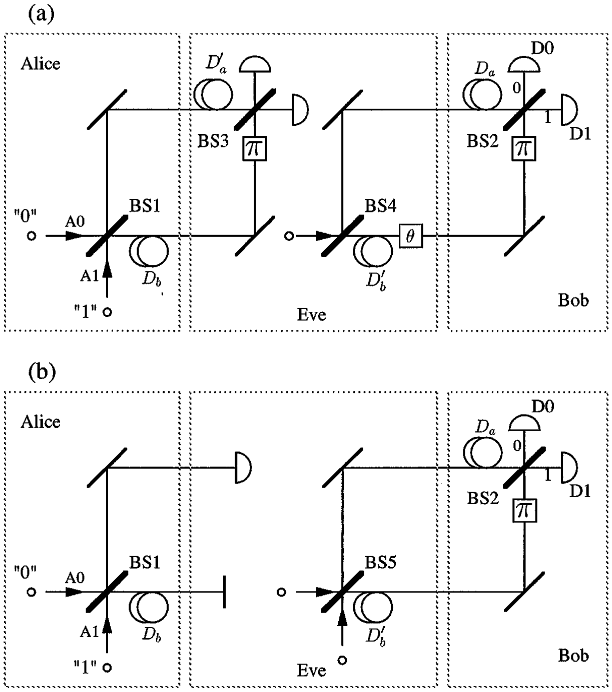

FIG. 2. Intervention strategies by an eavesdropper Eve: (a) strategy I and (b) strategy II.

by adjusting the phase shift θ introduced just after the delay D'_b, after she learns the bit value [9]. This is why the scheme in Ref. [9] requires the random sending time for security. In our scheme ($T \neq R$), the probability amplitudes of finding one photon in each arm are different depending on the bit value, and the compensation by the phase shift does not completely work. Assuming that Eve uses a 50%:50% beam splitter for BS4, the fake state $|\Psi_f\rangle$ received by Bob is

$$\begin{aligned} |\Psi_f\rangle = &-\frac{1}{\sqrt{2}}(\sqrt{T}e^{i\theta} + \sqrt{R})\,|1\rangle_0|0\rangle_1 \\ &+ \frac{i}{\sqrt{2}}(\sqrt{R}e^{i\theta} - \sqrt{T})\,|0\rangle_0|1\rangle_1 . \end{aligned} \tag{7}$$

Thus, even with the optimum compensation by the phase shift θ, there is still a nonzero probability P_{I} of introducing error in the bit value transmitted to Bob:

$$P_{\mathrm{I}} = \frac{1}{2}(\sqrt{T} - \sqrt{R})^2 = \frac{1}{2} - \sqrt{TR} . \tag{8}$$

This is plotted against T in Fig. 3(a). Note that choices of the transmissivity of BS4 other than 50% lead to larger error probabilities [13]. The mutual information $I_{\mathrm{AE}}^{(\mathrm{I})}$ between Alice and Eve is $\ln 2$ since Eve obtains the bit value sent by Alice perfectly. The mutual information $I_{\mathrm{EB}}^{(\mathrm{I})}$ between Eve and Bob is equal to that between Alice and Bob ($I_{\mathrm{AB}}^{(\mathrm{I})}$) and is calculated to be

$$\begin{aligned} I_{\mathrm{EB}}^{(\mathrm{I})} = I_{\mathrm{AB}}^{(\mathrm{I})} &= \ln 2 + \left(\frac{1}{2} + \sqrt{TR}\right)\ln\left(\frac{1}{2} + \sqrt{TR}\right) \\ &\quad + \left(\frac{1}{2} - \sqrt{TR}\right)\ln\left(\frac{1}{2} - \sqrt{TR}\right) \\ &= \ln 2 + P_{\mathrm{I}}\ln P_{\mathrm{I}} + (1 - P_{\mathrm{I}})\ln(1 - P_{\mathrm{I}}) . \end{aligned} \tag{9}$$

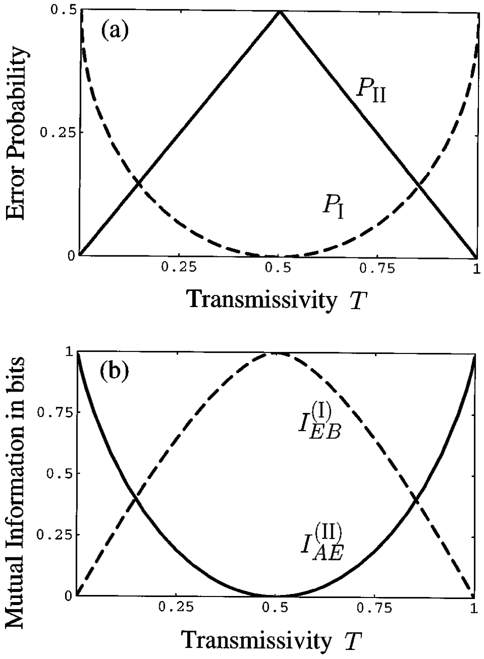

FIG. 3. Error probability (a) and mutual information (b) for the two eavesdropping strategies. The broken curves are for strategy I and the solid ones are for strategy II.

Figure 3(b) shows its dependence on T.

Next, consider another example of Eve's strategy (strategy II), shown in Fig. 2(b), which is complementary to strategy I. In this strategy, Eve exactly copies Alice's apparatus, and intends to completely control the bit values received by Bob. For that purpose, she determines the bit value by watching only arm a. When $T < R$, she assumes the bit value 0 if detector D3 is triggered, and the value 1 if not. The error probability P_{II} in this case is $P_{\mathrm{II}} = \min\{T, R\}$. This is also shown in Fig. 3(a). The mutual information in this case is $I_{\mathrm{EB}}^{(\mathrm{II})} = \ln 2$, and

$$\begin{aligned} I_{\mathrm{AE}}^{(\mathrm{II})} = I_{\mathrm{AB}}^{(\mathrm{II})} &= \ln 2 + T\ln T + R\ln R \\ &= \ln 2 + P_{\mathrm{II}}\ln P_{\mathrm{II}} + (1 - P_{\mathrm{II}})\ln(1 - P_{\mathrm{II}}) . \end{aligned} \tag{10}$$

The latter is plotted in Fig. 3(b). Together with the curves for strategy I, Fig. 3 suggests that some moderate asymmetry gives better redundancy in the security of the scheme. The crossing points of the two curves for both strategies are considered to be optimum at least against the two particular strategies considered here. The transmissivities for these points, which are the same for plots (a) and (b), are $T = (2 \pm \sqrt{2})/4 = 0.15, 0.85$.

In the system described here, the transfer of bit information consists of two steps: sending the first packet through arm a and the second one through arm b. Since in strategy II Eve extracts the bit information only from the first packet, parameter $I_{\mathrm{AE}}^{(\mathrm{II})}$ is also a measure of how much information is transferred to Bob just after the first step. Figure 3(b) shows that the full one bit information is transmitted by the first step in the case $T = 0, 1$, and that no bit information is transferred by the first step for $T = 1/2$. We see that the split transmission of one-bit information in two steps favors the security against Eve.

Incidentally, since Eve manipulates the second packet in strategy I, parameter $I_{\mathrm{EB}}^{(\mathrm{I})}$ is considered to be a measure of how well the sender can still control the bit information in the second step. Figure 3(b) therefore suggests that there is a trade-off between this controllability and the amount of transferred information after the first step is finished. One constraint of the trade-off that both $I_{\mathrm{EB}}^{(\mathrm{I})}$ and $I_{\mathrm{AE}}^{(\mathrm{II})}$ cannot take large values at the same time means that the sender cannot control the bit already transferred to the receiver. This is a natural requirement of the local causality. The opposite case (both $I_{\mathrm{EB}}^{(\mathrm{I})}$ and $I_{\mathrm{AE}}^{(\mathrm{II})}$ taking small values) where the sender cannot control *and* the receiver cannot read out the bit value is just the situation pursued by bit commitment protocols. Figure 3(b) indicates that this case is also forbidden in our system. This is an example of the more generalized notion of the impossibility of secure quantum bit commitment [14].

Finally, we give a formal proof that any eavesdropping attempts change the state that Bob receives. Eve's intervention can generally be described by her measurement apparatus initially prepared in a state $|u\rangle_M$ and by a unitary transformation U acting on the product space of the transmission line and her apparatus. If we require that Eve's presence should be kept concealed from Alice and Bob, the unitary transformation must not alter the bit information transferred to Bob. This condition is written as follows [15]:

$$U|\Phi_0\rangle|u\rangle_M = |\Phi_0\rangle|u_0\rangle_M\,, \tag{11}$$

$$U|\Phi_1\rangle|u\rangle_M = |\Phi_1\rangle|u_1\rangle_M\,. \tag{12}$$

After this interaction, Eve can extract the bit information from her apparatus if $|u_0\rangle_M$ and $|u_1\rangle_M$ are different states. Unlike the protocol based on two nonorthogonal states [6], Eqs. (11) and (12) alone would still allow ${}_M\langle u_0\,|\,u_1\rangle_M \neq 1$ since here $|\Phi_0\rangle$ and $|\Phi_1\rangle$ are orthogonal. But here we have an additional restriction on U: the state in arm a must arrive at Bob's site before Eve poses any interaction on the state in arm b. This requirement together with Eqs. (11) and (12) ensures $|u_0\rangle_M = |u_1\rangle_M$.

To see this, suppose that instead of the states $|\Phi_0\rangle$ and $|\Phi_1\rangle$ actually used in our protocol, Alice sends one of the following states:

$$|\Phi_\alpha\rangle \equiv \frac{1}{\sqrt{2}}\,(|0\rangle_a|1\rangle_b - i|1\rangle_a|0\rangle_b)\,, \tag{13}$$

or

$$|\Phi_\beta\rangle \equiv \frac{1}{\sqrt{2}}\,(|1\rangle_a|0\rangle_b - i|0\rangle_a|1\rangle_b)\,. \tag{14}$$

Further suppose that Bob places a photodetector directly in arm a, and Eve conducts the same strategy described by U. Noting that $|\Phi_\alpha\rangle$ is written as

$$|\Phi_\alpha\rangle = \frac{1}{\sqrt{2}}\,(\sqrt{T} + \sqrt{R})\,|\Phi_0\rangle - \frac{i}{\sqrt{2}}\,(\sqrt{T} - \sqrt{R})\,|\Phi_1\rangle\,, \tag{15}$$

the probability p_α that Bob's detector registers a photon when Alice sends $|\Phi_\alpha\rangle$ is calculated as follows:

$$\begin{aligned} p_\alpha &= \mathrm{Tr}_{b,M}[{}_a\langle 1|U|\Phi_\alpha\rangle|u\rangle_{MM}\langle u|\langle\Phi_\alpha|U^\dagger|1\rangle_a] \\ &= \frac{1}{2} + \sqrt{TR}\,(T - R)\{\mathrm{Re}[{}_M\langle u_0\,|\,u_1\rangle_M] - 1\}. \end{aligned} \tag{16}$$

Similarly, the probability p_β for the state $|\Phi_\beta\rangle$ is

$$p_\beta = \frac{1}{2} - \sqrt{TR}\,(T - R)\{\mathrm{Re}[{}_M\langle u_0\,|\,u_1\rangle_M] - 1\}. \tag{17}$$

The states $|\Phi_\alpha\rangle$ and $|\Phi_\beta\rangle$ are connected by the unitary operator $i|0\rangle_{bb}\langle 0| - i|1\rangle_{bb}\langle 1|$, which acts only on arm b. This means that Alice can determine which of the states $|\Phi_\alpha\rangle$ and $|\Phi_\beta\rangle$ she sends *after* Bob makes the measurement on arm a. Thus, causality requires $p_\alpha = p_\beta$, namely,

$$\sqrt{TR}\,(T - R)\{\mathrm{Re}[{}_M\langle u_0\,|\,u_1\rangle_M] - 1\} = 0\,. \tag{18}$$

Since we have assumed $T \neq 0, 1/2, 1$ in our protocol, we obtain $|u_0\rangle_M = |u_1\rangle_M$. Therefore, Eve is ignorant of the bit value if she is not to change the state received by Bob.

So far, to clarify the basic idea, we have assumed that the transmission and the detection are ideal. The security of quantum cryptography under the realistic losses and errors is a subject of continuing discussion [3], and we leave the problem to future study. We only note that in the above implementation the transmission loss has the same effect as some of the eavesdropping attempts [13], as in the scheme with two nonorthogonal states [6].

In summary, by using an asymmetric interferometer we have shown that it is possible to construct a secure quantum cryptosystem with only two orthogonal states that has no fundamental limitation on the efficiency and no need for the random timing tests. The degree of the asymmetry of the interferometer determines how one-bit information is split and transferred in two steps. When the information is wholly transmitted in either one of the two steps, the protocol is vulnerable to an eavesdropper. Security is attained when only a fraction is transmitted at a time.

[1] P. W. Shor, in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (IEEE Computer Society Press, New York, 1994), p. 124.

[2] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175.

[3] E. Biham and T. Mor, Phys. Rev. Lett. **78**, 2256 (1997), and references therein.

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

[5] A. K. Ekert, J. G. Rarity, P. R. Tapster, and G. M. Palma, Phys. Rev. Lett. **69**, 1293 (1992).

[6] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).

[7] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).

[8] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A **51**, 1863 (1995).

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

[10] M. Koashi and N. Imoto, Phys. Rev. Lett. **77**, 2137 (1996).

[11] E. Biham, B. Huttner, and T. Mor, Phys. Rev. A **54**, 2651 (1996).

[12] C. H. Bennett, F. Bessette, G. Brassard, and L. Salvail, J. Cryptol. **5**, 3 (1992); A. Muller, J. Breguet, and N. Gisin, Europhys. Lett. **23**, 383 (1993); P. D. Townsend, Electron. Lett. **30**, 809 (1994); J. D. Franson and H. Ilves, Appl. Opt. **33**, 2949 (1994); but see also a criticism by H. P. Yuen, Quantum Semiclass. Opt. **8**, 939 (1996).

[13] Other types of strategy, such as using the same asymmetry as Alice and use of an additional attenuator on the second packet in half cases to change the bit value without degradation of visibility, also have larger error probabilities if Bob registers the events where he does not receive one photon as errors.

[14] H.-K. Lo and H. F. Chau, Phys. Rev. Lett. **78**, 3410 (1997); D. Mayers, Phys. Rev. Lett. **78**, 3414 (1997).

[15] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).