Communication channels secured from eavesdropping via transmission of photonic Bell states

Kaoru Shimizu and Nobuyuki Imoto
NTT Basic Research Laboratories, 3-1 Morinosato Wakamiya, Atsugi, Kanagawa 243-0198, Japan
(Received 24 July 1998; revised manuscript received 13 November 1998)

This paper proposes a quantum communication scheme for sending a definite binary sequence while confirming the security of the transmission. The scheme is very suitable for sending a ciphertext in a secret-key cryptosystem so that we can detect any eavesdropper who attempts to decipher the key. Thus we can continue to use a secret key unless we detect eavesdropping and the security of a key that is used repeatedly can be enhanced to the level of one-time-pad cryptography. In our scheme, a pair of entangled photon twins is employed as a bit carrier which is encoded in a two-term superposition of four Bell states. Different bases are employed for encoding the binary sequence of a ciphertext and a random test bit. The photon twins are measured with a Bell state analyzer and any bit can be decoded from the resultant Bell state when the receiver is later notified of the coding basis through a classical channel. By opening the positions and the values of test bits, ciphertext can be read and eavesdropping is simultaneously detected. [S1050-2947(99)03107-8]

PACS number(s): 03.67.Lx, 03.65.Bz, 42.50.Ar, 42.79.Ta

I. INTRODUCTION

The security of any secret-key cryptosystem relies on the secrecy of the key. The key, therefore, must be distributed between legitimate users with complete conviction that no one else knows it. Quantum key distribution (QKD) is a methodology designed to meet this requirement [1–6]. Heisenberg's uncertainty principle assures security of the shared key in QKD.

Security can be guaranteed for one-time-pad use in a secret-key cryptosystem [7]. However, repeated use of the same key necessarily degrades the security. This is because Eve, an eavesdropper, can intercept and resend the ciphertext without being detected by the legitimate users. She may be able to decipher the key by comparing different ciphertexts ciphered by the same key and finally read all plaintexts and the key [7]. Thus repeated use of the key facilitates such kinds of attack and the security of the key is not guaranteed. In the same way, ciphering a lengthy plaintext by means of a short key is also insecure. Security degradation is a serious problem and is attributed to the use of classical communication channels for sending any ciphertext. This suggests the possibility of avoiding the problem by using a quantum channel instead of a classical one. Almost all protocols proposed to date for QKD, however, cannot be employed for sending any definite binary sequence which contains meaningful information.

For example, in QKD with the four polarization states of a single photon [the Bennett-Brassard 1984 (BB84) protocol] [2], Alice, the sender, encodes a bit of information by choosing a coding basis and Bob, the receiver, selects a measurement basis at random. If his measurement basis coincides with her coding basis, they pick up the corresponding photons. Then they check some test photons to see if they have any bit errors; if none are detected they can finally share random binary numbers as a secret key. This means they can detect eavesdropping without fail but Bob cannot receive a definite binary sequence prepared by Alice. This is because the received bit value is meaningless if the measurement basis selected by Bob is different from the coding basis and thus approximately half the received bit values are wrong [2,5,6].

Provided that the original BB84 protocol can be modified so that Bob can wait and delay his measurement of the polarization state until Alice unveils her polarization coding basis, he can always obtain the correct bit value and an error-free transmission of the bit value can be expected. This favorable theoretical assumption, however, cannot be applied to implementation in general and we should consider other methods of quantum communication based on one by one measurement of the transmitted carrier particles in the way used for conventional QKD schemes [1–6].

The use of orthogonal-state quantum cryptography, which has been proposed recently [8], appears to meet our requirements. However, bit information encoded by Alice is inevitably destroyed when Eve, an eavesdropper, intercepts and measures a photon. Bob, therefore, cannot expect to obtain the correct information even if he receives a photon at a designated time. In general, the security of any QKD scheme relies on the unavoidable bit error caused by eavesdropping. Therefore, it appears to be a contradiction to send a definite binary sequence while confirming transmission security by employing secure quantum channels which are based on Heisenberg's uncertainty principle.

This paper, however, shows theoretically that the use of polarization-entangled photon twins [9–12] instead of a single photon makes it possible to send a definite binary sequence, or intelligible information, while confirming the security of the transmission. Moreover, the receiver can expect to obtain the binary sequence without transmission error, despite it being intercepted and resent by an eavesdropper. Our proposed communication scheme, therefore, can cope with the problem of degradation in key security in a secret-key cryptosystem. As long as the legitimate users detect no evidence of eavesdropping in the ciphertexts, they can guarantee the secrecy of the plaintext with an arbitrary level of security and can use the key repeatedly. When they discover evidence of interception, they can change the key. An eavesdropper, therefore, cannot obtain two or more ciphertexts ciphered in the same key. In this way, the security

of a cryptosystem with a repeatedly used key is enhanced to the level of a one-time-pad system.

Section II explains some basic features of our proposed quantum channel which employs polarization-entangled photon twins as a bit carrier. In Sec. III we describe in detail how our proposed quantum channel can be applied to ciphertext transmission. We estimate the failure probability when detecting eavesdropping and discuss a method for reducing this probability. In Sec. IV, we describe a photonic implementation of our quantum channel. We also discuss the feasibility of an experimental demonstration which uses a Hong-Ou-Mandel two-photon interferometer.

II. COMMUNICATION VIA TRANSMISSION OF BELL STATES

In our proposed communication scheme, information transmission is separated into two steps. First, Alice encodes a bit of information on a quantum state of polarization-entangled photon twins and sends them to Bob. He measures them by using an appropriate basis and obtains partial information concerning the quantum state. Later Alice notifies Bob of the additional information which Bob needs to determine the quantum state.

A. Preparation of quantum states and information encoding

Alice encodes a bit of information on an entangled quantum state of photon twins. Here we should employ the set of four Bell states $\{|P\rangle,|Q\rangle,|R\rangle,|S\rangle\}$ [12–14] as a normalized orthonormal basis for expressing purely entangled quantum states of photon twins. The four Bell states are

$$|P\rangle\equiv\begin{bmatrix}1\\0\\0\\0\end{bmatrix}\equiv|\Psi^+\rangle=\frac{1}{\sqrt{2}}(|H\rangle_{\rm I}|V\rangle_{\rm II}+|V\rangle_{\rm I}|H\rangle_{\rm II}), \quad (2.1)$$

$$|Q\rangle\equiv\begin{bmatrix}0\\1\\0\\0\end{bmatrix}\equiv i|\Psi^-\rangle=i\frac{1}{\sqrt{2}}(|H\rangle_{\rm I}|V\rangle_{\rm II}-|V\rangle_{\rm I}|H\rangle_{\rm II}), \quad (2.2)$$

$$|R\rangle\equiv\begin{bmatrix}0\\0\\1\\0\end{bmatrix}\equiv i|\Phi^+\rangle=i\frac{1}{\sqrt{2}}(|H\rangle_{\rm I}|H\rangle_{\rm II}+|V\rangle_{\rm I}|V\rangle_{\rm II}), \quad (2.3)$$

and

$$|S\rangle\equiv\begin{bmatrix}0\\0\\0\\1\end{bmatrix}\equiv|\Phi^-\rangle=\frac{1}{\sqrt{2}}(|H\rangle_{\rm I}|H\rangle_{\rm II}-|V\rangle_{\rm I}|V\rangle_{\rm II}), \quad (2.4)$$

where H and V, respectively, mean the horizontal and vertical linear polarization states and the subscripts I and II mean entangled photons I and II. Additional $\pi/2$ phase shifts for the states $|\Psi^-\rangle$ and $|\Phi^+\rangle$ very conveniently explain the state transformations of the photon twins. We assign four-dimensional unit vectors for each of the four Bell states as shown in Eqs. (2.1)–(2.4). We can transform each state into another state by operating an appropriate spinor rotation on one photon as detailed in Sec. IV.

Alice does not send a solitary Bell state directly but prepares a quantum state given by a two-term superposition of the four Bell states. These are expressed as follows:

$$|A^+\rangle\equiv\frac{1}{\sqrt{2}}(|P\rangle+|Q\rangle)=\frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\\0\\0\end{bmatrix}, \quad (2.5)$$

$$|B^+\rangle\equiv\frac{1}{\sqrt{2}}(|R\rangle+|S\rangle)=\frac{1}{\sqrt{2}}\begin{bmatrix}0\\0\\1\\1\end{bmatrix}, \quad (2.6)$$

$$|C^+\rangle\equiv\frac{1}{\sqrt{2}}(|P\rangle+|R\rangle)=\frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\\1\\0\end{bmatrix}, \quad (2.7)$$

and

$$|D^+\rangle\equiv\frac{1}{\sqrt{2}}(|Q\rangle+|S\rangle)=\frac{1}{\sqrt{2}}\begin{bmatrix}0\\1\\0\\1\end{bmatrix}. \quad (2.8)$$

The states $|A^+\rangle$ and $|B^+\rangle$ constitute a set of orthonormal quantum states as well as the states $|C^+\rangle$ and $|D^+\rangle$ making up another set. However, two quantum states belonging to the different sets are nonorthonormal. Therefore both of the two sets can be regarded as two different coding bases, which are analogous to the linear and circular polarization bases for a single photon. Here we define the two sets of $\{|A^+\rangle,|B^+\rangle\}$ and $\{|C^+\rangle,|D^+\rangle\}$ as the AB-coding set and CD-coding set, respectively.

Alice, the information sender, selects one of the two coding sets in accordance with the following rules when she encodes a bit of information on photon twins:

$$|A^+\rangle\equiv 0 \text{ and } |B^+\rangle\equiv 1 \quad \text{for } AB\text{-coding set}$$

and

$$|C^+\rangle\equiv 0 \text{ and } |D^+\rangle\equiv 1 \quad \text{for } CD\text{-coding set.}$$

Alice can prepare each state of $|A^+\rangle$, $|B^+\rangle$, $|C^+\rangle$, and $|D^+\rangle$ by operating an appropriate one-photon spinor rotation for any Bell state. These operations are detailed in Sec. IV.

The AB-coding set can be extended to a normalized orthonormal basis of a four-dimensional Hilbert space by introducing two additional quantum states:

$$|A^-\rangle\equiv\frac{1}{\sqrt{2}}(|P\rangle-|Q\rangle)=\frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\\0\\0\end{bmatrix} \quad (2.9)$$

and

$$|B^-\rangle \equiv \frac{1}{\sqrt{2}}(|R\rangle - |S\rangle) = \frac{1}{\sqrt{2}}\begin{bmatrix} 0 \\ 0 \\ 1 \\ -1 \end{bmatrix}. \tag{2.10}$$

Any two elements of $\{|A^+\rangle, |B^+\rangle, |A^-\rangle, |B^-\rangle\}$ are orthonormal to each other. In a similar manner, $\{|C^+\rangle, |D^+\rangle, |C^-\rangle, |D^-\rangle\}$ makes up another normalized orthonormal basis, where

$$|C^-\rangle \equiv \frac{1}{\sqrt{2}}(|P\rangle - |R\rangle) = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 0 \\ -1 \\ 0 \end{bmatrix} \tag{2.11}$$

and

$$|D^-\rangle \equiv \frac{1}{\sqrt{2}}(|Q\rangle - |S\rangle) = \frac{1}{\sqrt{2}}\begin{bmatrix} 0 \\ 1 \\ 0 \\ -1 \end{bmatrix}. \tag{2.12}$$

The inner product for any quantum states belonging to the two different bases is $\frac{1}{2}$ or $-\frac{1}{2}$. For example, $|C^+\rangle$ and $|D^+\rangle$ can be expanded as follows by using the $\{|A^+\rangle, |B^+\rangle, |A^-\rangle, |B^-\rangle\}$ basis:

$$|C^+\rangle = \tfrac{1}{2}(|A^+\rangle + |A^-\rangle + |B^+\rangle + |B^-\rangle) \tag{2.13}$$

and

$$|D^+\rangle = \tfrac{1}{2}(|A^+\rangle - |A^-\rangle + |B^+\rangle - |B^-\rangle). \tag{2.14}$$

Therefore Heisenberg's uncertainty principle ensures that there is a non-orthonormal relation between the *AB*- and *CD*-coding bases which are employed for encoding a bit of information. The use of the two different orthonormal bases $\{|A^+\rangle, |B^+\rangle, |A^-\rangle, |B^-\rangle\}$ and $\{|C^+\rangle, |D^+\rangle, |C^-\rangle, |D^-\rangle\}$ makes it possible for Alice to prepare quantum states which cannot be measured correctly without knowing the coding basis.

Although the photon twins generally have an information capacity of 2 bits, Alice intentionally does not employ $\{|A^-\rangle, |B^-\rangle\}$ or $\{|C^-\rangle, |D^-\rangle\}$ to encode a second bit of information. Encoding less information than the capacity allows Bob to perform a new kind of quantum measurement. He can obtain partial information concerning the quantum state sent by Alice even though he knows nothing about the coding basis. Such a possibility is ruled out for a single photon. In the next subsection, we describe the quantum measurement executed by Bob.

B. Quantum state measurement and information decoding

Bob, the information receiver, performs a joint measurement of the photon twins by using an appropriate measurement basis. As long as he selects either $\{|A^+\rangle, |B^+\rangle, |A^-\rangle, |B^-\rangle\}$ or $\{|C^+\rangle, |D^+\rangle, |C^-\rangle, |D^-\rangle\}$ as the basis, his measurement destroys the encoded information completely when his choice differs from that of Alice. As in the QKD with the four polarization states, he cannot obtain any information about the quantum state without knowing the coding basis and a received bit value is meaningless whenever his basis is wrong. Therefore it is impossible to transmit a definite binary sequence from Alice to Bob, though they can successfully share random numbers.

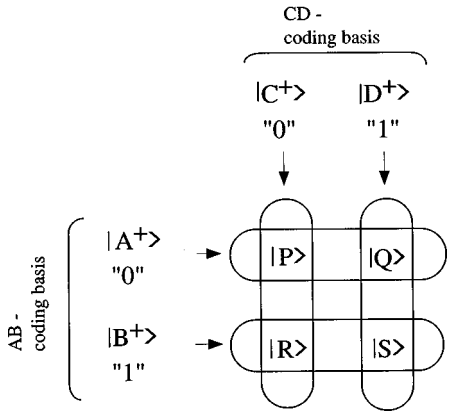

FIG. 1. Relationships between prepared quantum states and resultant Bell states.

Bob, however, can adopt other kinds of measurement bases. We now show that the use of a Bell state analyzer makes it possible for Bob to read out partial information concerning the quantum state sent by Alice without knowing the coding basis. Bell state analysis is a quantum measurement which employs the $\{|P\rangle, |Q\rangle, |R\rangle, |S\rangle\}$ basis. Figure 1 summarizes the relationships between the quantum states prepared by Alice and the Bell states obtained by Bob. Whenever he obtains the Bell state $|P\rangle$, he has the partial information that Alice has sent either the $|A^+\rangle$ or $|C^+\rangle$ state. No further information is available at this stage. However, he will be able to decode all the information related to the quantum state when Alice eventually notifies him of the selected coding basis through a classical channel. Thus a bit of information can finally be transmitted from Alice to Bob without bit errors even if Bob knows nothing about the coding basis when he measures the photon twins.

As the Bell state analysis destroys any phase information between two Bell states, the two states $|A^+\rangle$ and $|A^-\rangle$ are indistinguishable. This means that the information capacity of the photon twins is limited to 1 bit provided Alice enables Bob to obtain the partial information concerning the quantum state. In other words, one of the two internal freedoms of the bispinor is devoted to constructing a new kind of communication scheme and the other is employed as a bit carrier.

From the viewpoint of information theory, one bit of classical information is transmitted by the photon twins through a quantum channel as a first step. Bob can reject two quantum states from the initial four candidates of $|A^+\rangle$, $|B^+\rangle$, $|C^+\rangle$, and $|D^+\rangle$ based on this information. Then another bit of classical information is transmitted later so that Bob can finally determine the quantum state sent by Alice. Eve, an eavesdropper, can also read the first bit of information by intercepting the photon twins and measuring them with a Bell state analyzer. However, she cannot resend the quantum state correctly because she cannot obtain the second bit of information until Alice opens it. If Eve tries to resend $|A^+\rangle$, $|B^+\rangle$, $|C^+\rangle$, or $|D^+\rangle$ to Bob, she has to guess but this results

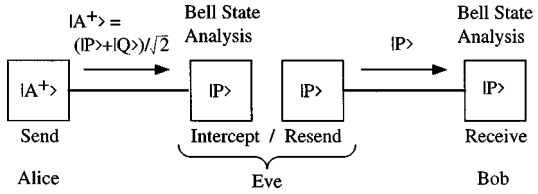

FIG. 2. Eavesdropping strategy of resending a resultant Bell state.

in a bit error with a finite probability if her guess is wrong. This is the basic device for detecting an eavesdropper in our proposed communication scheme. Eve can, however, resend her resultant Bell state directly to Bob and so can completely escape detection as illustrated in Fig. 2. Our communication scheme, therefore, must be improved to cope with this strategy of Eve's.

In the improved scheme, Bob operates an appropriate unitary transformation U at random, preceding the Bell state analysis. The U transformation is defined by

$$U=\frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & 1 \\ -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \end{bmatrix}. \tag{2.15}$$

The transformation does not change the quantum states $|A^+\rangle[=(1,1,0,0)/\sqrt{2}]$ and $|B^+\rangle[=(0,0,1,1)/\sqrt{2}]$:

$$U|A^+\rangle=|A^+\rangle \text{ and } U|B^+\rangle=|B^+\rangle. \tag{2.16}$$

The states $|C^+\rangle[=(1,0,1,0)/\sqrt{2}]$ and $|D^+\rangle[=(0,1,0,1)/\sqrt{2}]$ are transformed as follows:

$$U|C^+\rangle=\frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}=\frac{1}{\sqrt{2}}(|P\rangle+|S\rangle) \tag{2.17}$$

and

$$U|D^+\rangle=\frac{1}{\sqrt{2}}\begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}=\frac{1}{\sqrt{2}}(|Q\rangle+|R\rangle). \tag{2.18}$$

Figure 3 summarizes the relationships between the quantum states prepared by Alice and the resultant Bell states after operating the U transformation. Although the positions of $|R\rangle$ and $|S\rangle$ are the reverse of these in Fig. 1, Bob can read out the encoded information with additional information notifying him of the coding basis. Thus the transmission of the information suffers no disturbance from the random operation of the U transformation.

By contrast, the U transformation changes any solitary Bell state into a four-term superposition of the four Bell states with an equal probability amplitude of $\frac{1}{2}$ as follows:

$$U|P\rangle=\tfrac{1}{2}(|P\rangle+|Q\rangle-|R\rangle+|S\rangle), \tag{2.19}$$

$$U|Q\rangle=\tfrac{1}{2}(|P\rangle+|Q\rangle+|R\rangle-|S\rangle), \tag{2.20}$$

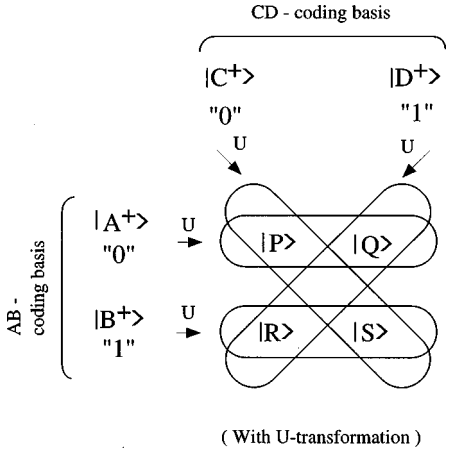

FIG. 3. Relationships between prepared quantum states and resultant Bell states (with U transformation).

$$U|R\rangle=\tfrac{1}{2}(|P\rangle-|Q\rangle+|R\rangle+|S\rangle), \tag{2.21}$$

and

$$U|S\rangle=\tfrac{1}{2}(-|P\rangle+|Q\rangle+|R\rangle+|S\rangle). \tag{2.22}$$

Therefore Eve must abandon her strategy of resending a resultant Bell state because it will lead to a bit error with a finite probability if Bob operates the U transformation. For example, the above procedure can be explained as follows: (i) Alice sends $|C^+\rangle$, (ii) Eve intercepts the photon twins and obtains the Bell state $|P\rangle$, (iii) Eve resends $|P\rangle$ to Bob, (iv) Bob operates the U transformation and obtains the Bell state $|Q\rangle$ or $|R\rangle$ with a probability of $\frac{1}{2}$, (v) Alice notifies Bob that she has sent $|C^+\rangle$, and (vi) Bob can detect eavesdropping because the transformed state $U|C^+\rangle$ does not contain the Bell states $|Q\rangle$ and $|R\rangle$. Thus our device for detecting an eavesdropper works well by introducing the random operation of U preceding the Bell state analysis. We will describe in detail how to discover eavesdropping in the next section.

The Bell state analysis after the U transformation is equivalent to quantum measurement with the $\{|P'\rangle,|Q'\rangle,|R'\rangle,|S'\rangle\}$ basis. The basis is composed of

$$|P'\rangle=U^{-1}|P\rangle=\frac{1}{2}\begin{bmatrix} 1 \\ 1 \\ 1 \\ -1 \end{bmatrix}, \quad |Q'\rangle=U^{-1}|Q\rangle=\frac{1}{2}\begin{bmatrix} 1 \\ 1 \\ -1 \\ 1 \end{bmatrix}, \tag{2.23}$$

$$|R'\rangle=U^{-1}|R\rangle=\frac{1}{2}\begin{bmatrix} -1 \\ 1 \\ 1 \\ 1 \end{bmatrix}, \quad |S'\rangle=U^{-1}|S\rangle=\frac{1}{2}\begin{bmatrix} 1 \\ -1 \\ 1 \\ 1 \end{bmatrix}.$$

These are completely nonorthogonal with the $\{|P\rangle,|Q\rangle,|R\rangle,|S\rangle\}$ basis given by Eqs. (2.1)–(2.4). Any quantum state prepared by Alice can also be expressed as a two-term superposition by use of the $\{|P'\rangle,|Q'\rangle,|R'\rangle,|S'\rangle\}$ basis;

$$|A^+\rangle=\frac{1}{\sqrt{2}}(|P'\rangle+|Q'\rangle),\quad |B^+\rangle=\frac{1}{\sqrt{2}}(|R'\rangle+|S'\rangle),$$
$$|C^+\rangle=\frac{1}{\sqrt{2}}(|P'\rangle+|S'\rangle),\quad |D^+\rangle=\frac{1}{\sqrt{2}}(|Q'\rangle+|R'\rangle). \tag{2.24}$$

We can derive Eqs. (2.24) by operating U^{-1} on both sides of Eqs. (2.16)–(2.18) and Eq. (2.24) means that the U transformation does not disturb information transmission at all.

Alice adopts a pair of different orthonormal bases $\{|A^+\rangle,|B^+\rangle,|A^-\rangle,|B^-\rangle\}$ and $\{|C^+\rangle,|D^+\rangle,|C^-\rangle,|D^-\rangle\}$ for preparing quantum states which cannot be measured correctly without knowing the coding bases. By contrast, Bob employs another pair of orthonormal bases $\{|P\rangle,|Q\rangle,|R\rangle,|S\rangle\}$ and $\{|P'\rangle,|Q'\rangle,|R'\rangle,|S'\rangle\}$ for measuring them. This asymmetrical quantum state arrangement between the coding and measurement bases is a necessary condition for our communication scheme and we can satisfy this condition by using polarization-entangled photon twins as a bit carrier. Our proposed communication scheme is based on the two different kinds of uncertainty relation in the four-dimensional Hilbert space of the photon twins.

The use of the U transformation makes it impossible for Alice to prepare $|A^-\rangle$, $|B^-\rangle$, $|C^-\rangle$, and $|D^-\rangle$. If the U transformation is operated by Bob for these states, the resultant Bell states are indistinguishable from those for $|B^+\rangle$, $|A^+\rangle$, $U|D^+\rangle$, and $U|C^+\rangle$ as shown in the following:

$$U|A^-\rangle=-\frac{1}{\sqrt{2}}(|R\rangle-|S\rangle),\quad U|B^-\rangle=\frac{1}{\sqrt{2}}(|P\rangle-|Q\rangle),$$
$$U|C^-\rangle=\frac{1}{\sqrt{2}}(|Q\rangle-|R\rangle),\quad U|D^-\rangle=\frac{1}{\sqrt{2}}(|P\rangle-|S\rangle), \tag{2.25}$$

respectively. Bob cannot identify bit values.

III. COMMUNICATION PROTOCOL FOR SENDING A CIPHERTEXT

Here we describe how to use our quantum channel explained in the preceding section to send an intelligible binary sequence in a secure manner. In particular, we focus on an application to ciphertext transmission in a secret key cryptosystem to cope with the security degradation problem of the secret key. The degradation is caused by a series of undetectable interceptions by an eavesdropper who attempts to decipher the key. If the legitimate users can detect eavesdropping for a ciphertext, they can avoid any risk of key decipherment.

A. Basic protocol

A ciphertext is given by a lengthy definite binary sequence and we define each bit as an intelligible bit. By contrast, we introduce a test bit as a binary random number, which is employed for detecting eavesdroppers. Alice, the sender, inserts some test bits into the intelligible bit sequence at random and prepares a mixed sequence of intelligible and test bits.

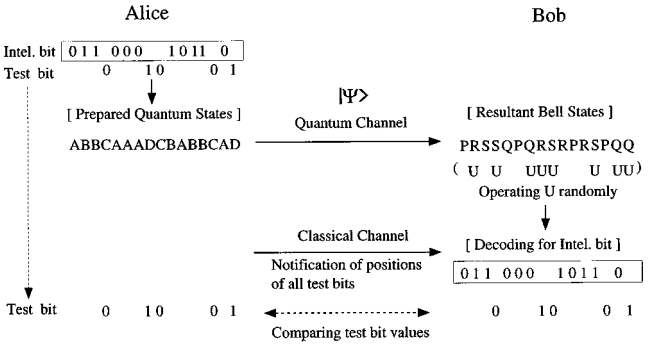

FIG. 4. Basic protocol for the secure transmission of ciphertext.

Before sending the mixed bit sequence, Alice and Bob make a decision (possibly in public) that *AB*- and *CD*-coding bases will be employed for encoding the intelligible bit and the test bit, respectively. The encoding scheme is as follows:

$$|A^+\rangle\equiv 0 \text{ and } |B^+\rangle\equiv 1 \quad \text{for an intelligible bit,}$$

and

$$|C^+\rangle\equiv 0 \text{ and } |D^+\rangle\equiv 1 \quad \text{for a test bit.}$$

As a bit of information is encoded in a quantum state unknown to anyone else, nobody can decode the information and distinguish the intelligible and test bits until Alice unveils the coding basis. The number of test bits depends on the degree of secrecy required [1] but it can be far smaller than the number of intelligible bits.

Bob, the receiver, measures photon twins by setting either the $\{|P\rangle,|Q\rangle,|R\rangle,|S\rangle\}$ or $\{|P'\rangle,|Q'\rangle,|R'\rangle,|S'\rangle\}$ basis, given by Eq. (2.23), at random. The latter arrangement is realized by operating the U transformation on the photon twins before Bell state analysis. Then Bob obtains a sequence of resultant Bell states but he cannot determine the quantum state prepared by Alice at this stage. Thus the first step via a quantum channel is accomplished.

After receiving all the photon twins, he asks Alice to unveil all the test bit positions and she does so. These are notified through a classical public channel and this makes it possible for Bob to distinguish intelligible bits from test bits. Then Bob can decode all the bit values by using the diagrams shown in Figs. 1 and 3. Thus he can read the definite binary sequence from his sequenced Bell states and the information transmission is completed. Alice and Bob compare the encoded and decoded bit values for all the test bits so that they can confirm security. If they detect no error in the test bits, they can guarantee that security has been maintained. The flow of our basic protocol is shown schematically in Fig. 4.

Here it should be noted that the linear and circular polarization bases for a single photon can be assigned to the intelligible and test bits, respectively, if we are allowed to employ the delayed and correctly measured BB84 protocol [2] as a quantum channel.

B. Eavesdropping and bit error per test bit

Intercept/resend strategy is a standard scheme for eavesdropping classical information. Hence we assume that Eve also employs this strategy for eavesdropping information

TABLE I. Bit error in a test bit; $|C^+\rangle=(|P\rangle+|R\rangle)/\sqrt{2}$. The states with an asterisk represent the bit errors.

	Intercept			Resultant Bell states	
Send	Measurement basis	Result	Resend	Without U	With U
(i) $\|C^+\rangle$	$\{\|P\rangle,\|Q\rangle,\|R\rangle,\|S\rangle\}$	$\|P\rangle$	$\|A^+\rangle$	$\|P\rangle\ \|Q\rangle^*$	$\|P\rangle\ \|Q\rangle^*$
		$\|R\rangle$	$\|B^+\rangle$	$\|R\rangle\ \|S\rangle^*$	$\|R\rangle^*\ \|S\rangle$
(ii) $\|C^+\rangle$	$\{\|A^+\rangle,\|B^+\rangle,\|A^-\rangle,\|B^-\rangle\}$	$\|A^+\rangle$	$\|A^+\rangle$	$\|P\rangle\ \|Q\rangle^*$	$\|P\rangle\ \|Q\rangle^*$
		$\|B^+\rangle$	$\|B^+\rangle$	$\|R\rangle\ \|S\rangle^*$	$\|R\rangle^*\ \|S\rangle$
		$\|A^-\rangle$	$\|C^+\rangle$	$\|P\rangle\ \|R\rangle$	$\|P\rangle\ \|S\rangle$
		$\|B^-\rangle$	$\|D^+\rangle$	$\|Q\rangle^*\ \|S\rangle^*$	$\|Q\rangle^*\ \|R\rangle^*$

from the photon twins. Any strategy which employs cloning is prohibited by the quantum no-cloning theorem [15,16]. As a transmission bit error is regarded as evidence of eavesdropping, Eve must attempt to minimize the total frequency of bit errors which may appear in the whole transmitted bit sequence. In particular, errors must be avoided in intelligible bits because this would give rise to an unavoidable disturbance in a deciphered plaintext and Bob necessarily regards any such disturbance as explicit evidence of eavesdropping.

Here Eve should also be assumed to know that (i) AB- and CD-coding bases are employed for intelligible and test bits, respectively, and (ii) the number of intelligible bits is relatively larger than that of test bits. With these assumptions, she can successfully behave so as not to leave any evidence in an intelligible bit provided she exploits the AB-coding basis when she resends the photon twins after interception. Thus she can greatly reduce the total number of bit errors. Nevertheless, she cannot escape detection because she necessarily resends $|A^+\rangle$ or $|B^+\rangle$ even though $|C^+\rangle$ or $|D^+\rangle$ is prepared by Alice as a test bit. Therefore there is a finite probability that Eve will leave evidence in a test.

There are two possible ways for Eve to carry out her interception/resend strategy, i.e., interception with either the $\{|P\rangle,|Q\rangle,|R\rangle,|S\rangle\}$ or $\{|A^+\rangle,|B^+\rangle,|A^-\rangle,|B^-\rangle\}$ measurement basis. With the first interception method, Alice and Bob can detect Eve as follows: (i) Alice is assumed to send $|C^+\rangle$, test bit 0, (ii) Eve intercepts the photon twins and obtains the Bell state $|P\rangle$, (iii) Eve resends $|A^+\rangle$ to Bob in accordance with the resend strategy, (iv) Bob obtains the Bell state $|Q\rangle$ with a probability of $\frac{1}{2}$, (v) Alice notifies Bob that she has sent a test bit, (vi) Bob considers $|Q\rangle$ to result from test bit 1, and (vii) they finally detect the bit error by comparing the encoded and decoded bit values. The error probability per test bit is $\frac{1}{2}$. If Eve obtains the Bell state $|R\rangle$ and then resends $|B^+\rangle$, Bob regards the resultant Bell state $|R\rangle$ or $|S\rangle$ as a bit error, depending on whether he operates the U transformation or not. The flows of the resultant and resent states are summarized in Table I.

With the second interception method, Alice and Bob can detect Eve as follows: quantum states $|C^+\rangle$ and $|D^+\rangle$ is completely destroyed by the interception with the $\{|A^+\rangle,|A^-\rangle,|B^+\rangle,|B^-\rangle\}$ measurement basis, as suggested by Eqs. (2.13) and (2.14). Whenever Eve obtains $|A^+\rangle$ or $|B^+\rangle$, she resends the resultant state and this results in an error with a probability of $\frac{1}{2}$ per test bit. By contrast, if Eve obtains $|A^-\rangle$ or $|B^-\rangle$ through the measurement, she knows that Alice prepared $|C^+\rangle$ or $|D^+\rangle$. This is because Alice never prepares $|A^-\rangle$ and $|B^-\rangle$, as mentioned in Sec. II. Eve, however, cannot determine the test bit value and has to guess when she resends the photon twins. For example, this can be explained as follows: (i) Alice sent $|C^+\rangle$, test bit 0, (ii) Eve obtains $|A^-\rangle$ and resends $|D^+\rangle$ by guessing, (iii) Bob obtains the Bell state $|Q\rangle$, (iv) Alice notifies Bob that she has sent a test bit, (v) Bob considers $|Q\rangle$ to result from test bit 1, and (vi) they finally detect the bit error after comparing the test bits. Thus the error probability per test bit is $\frac{1}{2}$. Table I also summarizes several sequences of the measurement results for the second interception method.

Eve, however, may be able to reduce the error probability per test bit by employing some other sophisticated eavesdropping strategy [17–20]. Provided that she can only access one photon pair at a time, the usual assumption in any QKD scheme, the nonorthonormal relation between the AB- and CD-coding bases ensures a finite error probability regardless of her eavesdropping strategies and the legitimate users can cope with the reduction by increasing the number ratio of test bits to intelligible bits. By contrast, if Eve is allowed to measure more than two carriers jointly (joint attack or coherent attack), the security issue of our current scheme needs further clarification in general and should be the subject of a future investigation [19,20]. As two serious proofs have recently been proposed for the security of conventional QKD schemes [21], it is necessary for us to reexamine the security of our current scheme on the basis of these proofs.

C. Ciphertext transmission in secret-key cryptography

Alice and Bob can expect the error-free transmission of a ciphertext provided that Eve adopts the intercept/resend strategy described in the preceding subsection. In this sense, Eve does not destroy bit information in any intelligible bit and our communication channel is equivalent to a classical channel as regards the transmission of intelligible bits. This requirement cannot be satisfied in quantum channels by means of orthogonal-state quantum cryptography [8] as already mentioned in Sec. I. The use of quantum states unknown to anyone else, however, makes it impossible for Eve to distinguish test bits from large numbers of intelligible bits and she necessarily fails to resend test bits. As the error probability per test bit is $\frac{1}{2}$, Alice and Bob can detect Eve with a whole probability of $1-(\frac{1}{2})^M$ by inserting M test bits. When Alice unveils all the test bit positions, Eve can also decode all the bit values and obtain the definite binary sequence prepared by Alice. Thus mutual information between

Alice and Eve becomes unity. It is for this reason that Alice and Bob employ our communication scheme for sending not plaintext but ciphertext.

Once they have shared a secret key, they must continue to employ our communication scheme whenever they send any ciphertext. As long as they detect no evidence of eavesdropping, they can guarantee the security of the key and the plaintext with a high level of confidence and use the key repeatedly. In contrast, if they detect eavesdropping, they discard the key. Although Eve can intercept all the ciphertext, she can no longer expect to obtain any other ciphertexts ciphered in the same key and cannot decipher the key at all. This means that the security required for a key that is used repeatedly can be enhanced to the level of one-time-pad cryptography. This greatly reduces the size of the key stock.

In terms of the security of our proposed scheme, we must find a way to design our system so that we can detect an eavesdropper without fail whenever the ciphertext, or any portion of it, is intercepted. Here we introduce three parameters L, Γ, and η to discuss this security issue. L is the length of the secret key to be protected. We define Γ as the number ratio of test bits to intelligible bits. Parameter η is the fraction of the photon pairs assumed to be intercepted. Eve, who desires to intercept the ciphertext completely, necessarily fixes the parameter η value at unity. In this case, Alice, who sets the parameter Γ value at $\frac{1}{100}$, can detect Eve with a probability of $1-10^{-9}$ provided that Alice sends approximately 3000 photon pairs per one-time use of the secret key ($L \sim 3000$). Although such a lengthy key appears inconvenient or less realistic in comparison with 56 bits in data encryption standard (DES), it seems necessary in principle to increase the key length so that we can assure security in our proposed scheme.

If Eve unwillingly reduces the η parameter to $\frac{1}{10}$ to escape detection, she can still successfully intercept approximately 300 bits of intelligible information with a probability of $\frac{1}{8}$, without being detected. To prevent this not insignificant amount of information from being intercepted easily, Alice must improve the parameter Γ value to, for example, $\frac{1}{10}$. Then the probability of Eve secretly obtaining the 300 bits of information can be reduced exponentially to 10^{-9}.

Thus the probability of detecting an eavesdropper can be close to unity asymptotically by increasing the key length L for a given parameter Γ value. As Γ is necessarily smaller than the order of unity to ensure the error-free transmission of intelligible bits, it is preferable to lengthen the key. If Alice and Bob still desire to protect the secrecy of intelligible bit values as a precaution against an improbable but nonzero probability failure in the eavesdropping detection, they must further encrypt the ciphertext. Such anxiety, however, should generally be dispelled by increasing the parameter Γ value and the key length L.

In the above discussion, we assume the ideal conditions of a zero-loss transmission line, a unity photodetection efficiency, and a noiseless transmission system. These assumptions, however, are invalid for any actual transmission system and we must at least establish an error correction code for intelligible bits to cope with transmission and detection noise. The structure of the error correction code, however, helps Eve guess some possible candidates for the test bit positions in the mixed bit sequence prepared by Alice.

For example, we assume that Alice employs a parity code with a block length of $N=3$ for intelligible bits and prepares the bit string 1100 with the parity encoded in the last bit. She then inserts the test bit $0_t\,(=|C^+\rangle)$ between 110 and 0 and sends 1100_t0 to Bob. We express this mixed bit sequence as $(a,b,c,d,e)=(1,1,0,0_t,0)$. Here Eve should be assumed to know that Alice employs the error correction code with $N=3$ and that one of the five bits is a test bit. If Eve obtains the Bell state, for example, $|R\rangle$ for the fourth position d, she necessarily regards the bit sequence as $(a,b,c,d,e)=(1,1,0,1,0)$ and considers a, b, or d to be a possible test bit candidate.

Thus Eve can guess some possible candidates for the test bit positions by using the structure of the error correction code. Nevertheless, her guessing depends on some ambiguities and she cannot always locate the correct positions of the test bits. Moreover, if Eve wrongly locates the test bit and resends it, bit error may occur not only in the correct test bit but also in the intelligible bit picked up wrongly by her. Eve, therefore, must resend any intercepted bit as an intelligible bit to minimize the probability of detection whenever she cannot specify the correct position of the test bit. This suggests that it is practically impossible for Eve to escape detection provided that a sufficiently large number of test bits are inserted in a lengthy bit sequence. This issue deserves future quantitative analysis and will be presented elsewhere.

D. Comparison with usual QKD schemes

From the general viewpoint of secret-key cryptography, our proposed scheme is an alternative to the one-time-pad use of a secret key shared by quantum key distribution. The latter, however, has the disadvantage that a lengthy secret key, which has the same length as the ciphertext, must be generated every time. A very large number of quantum and classical information transfers are necessary when sharing such a lengthy key, preceding the classical transmission of each ciphertext. In contrast, once a key is shared in a secure manner, our proposed scheme requires a smaller number of classical information transfers to notify publicly Bob of all the positions and values of the test bits.

It should be noted that at this stage the practical advantage of the present proposal to usual QKD plus one-time-pad schemes is still not clear. As a quantum channel is needed for transmitting the ciphertext, our scheme may offer no saving in the amount of quantum information transmission as compared to the usual schemes. Moreover, the ciphertext may be lost due to photon loss of the quantum channel, leading to the necessity of a retransmission. Also, one cannot restrict the use of the quantum channel to off-peak hours, which is possible in the usual QKD. It is also unclear either how privacy amplification [22], which is effective in QKD, can be applied to the present scheme. All these should be sorted out for practical consideration in the future investigation. In this paper, however, we concentrate on showing that, in principle, the security of the repeated use of a key can be enhanced to the level of one-time pad by directly sending a ciphertext over the quantum channel.

IV. PHOTONIC IMPLEMENTATION OF A QUANTUM CHANNEL

This section describes the photonic implementation of our quantum channel. We also discuss a feasible experimental

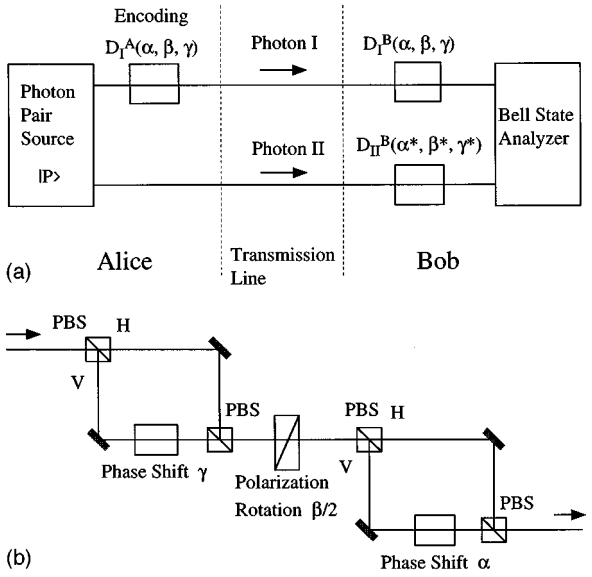

FIG. 5. (a) The schematic configuration of our quantum communication system by means of polarization-entangled photon twins: $D(\alpha,\beta,\gamma)$ indicates a one-photon spinor rotator. (b) The schematic configuration of a one-photon spinor rotator.

setup which employs a Hong-Ou-Mandel two-photon interferometer.

A. Bell state operation via spinor rotation

The schematic configuration of our quantum channel is shown in Fig. 5(a), where $D(\alpha,\beta,\gamma)$ indicates a one-photon spinor rotation [23]. Photon twins are emitted from an optical source and identified by two different optical paths I and II [12,14]. The initial state of the photon twins is assumed to be $|P\rangle(=|\Psi^+\rangle)$, given by Eq. (2.1). Alice can prepare each of $|A^+\rangle$, $|B^+\rangle$, $|C^+\rangle$, and $|D^+\rangle$ by operating $D(\alpha,\beta,\gamma)$ on photon I; $D_I^A(\alpha,\beta,\gamma)$. Bob can perform the U transformation by operating an appropriate one-photon spinor rotation on each photon such as $D_I^B(\alpha,\beta,\gamma)\otimes D_{II}^B(\alpha^*,\beta^*,\gamma^*)$. Then Bell state analysis is performed for the photon twins.

The one-photon spinor rotation $D(\alpha,\beta,\gamma)$ can be expressed as

$$D(\alpha,\beta,\gamma)=\begin{bmatrix} e^{-i\alpha/2} & 0 \\ 0 & e^{i\alpha/2}\end{bmatrix}\begin{bmatrix} \cos\beta/2 & -\sin\beta/2 \\ \sin\beta/2 & \cos\beta/2\end{bmatrix}\times\begin{bmatrix} e^{-i\gamma/2} & 0 \\ 0 & e^{i\gamma/2}\end{bmatrix} \tag{4.1}$$

by use of Euler angles (α,β,γ). Here the linear polarization states H and V are regarded as spin up (1,0) and down (0,1), respectively [22]. The configuration of the one-photon spinor operator is shown in Fig. 5(b). The initial state $|P\rangle$ is transformed as

$$D_I(\alpha,\beta,\gamma)|P\rangle=\cos\frac{\beta}{2}\cos\frac{\alpha+\gamma}{2}|P\rangle-\cos\frac{\beta}{2}\sin\frac{\alpha+\gamma}{2}|Q\rangle+\sin\frac{\beta}{2}\sin\frac{\alpha-\gamma}{2}|R\rangle-\sin\frac{\beta}{2}\cos\frac{\alpha-\gamma}{2}|S\rangle \tag{4.2}$$

by operating $D_I^A(\alpha,\beta,\gamma)$. Therefore $|A^+\rangle$, $|B^+\rangle$, $|C^+\rangle$, and $|D^+\rangle$ can be generated from $|P\rangle$ as follows:

$$D_I^A(-\pi/2,0,0)|P\rangle=\frac{1}{\sqrt{2}}(|P\rangle+|Q\rangle)=|A^+\rangle, \tag{4.3}$$

$$D_I^A(\pi,\pi,-\pi/2)|P\rangle=\frac{1}{\sqrt{2}}(|R\rangle+|S\rangle)=|B^+\rangle, \tag{4.4}$$

$$D_I^A(\pi/2,\pi/2,-\pi/2)|P\rangle=\frac{1}{\sqrt{2}}(|P\rangle+|R\rangle)=|C^+\rangle, \tag{4.5}$$

and

$$D_I^A(\pi/2,\pi/2,-3\pi/2)|P\rangle=\frac{1}{\sqrt{2}}(|Q\rangle+|S\rangle)=|D^+\rangle. \tag{4.6}$$

To derive a two-photon spinor rotation corresponding to the U transformation

$$U=\frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & 1 \\ -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1\end{bmatrix},$$

a four-dimensional representation using the $\{|P\rangle,|Q\rangle,|R\rangle,|S\rangle\}$ basis should be employed. The effects of $D_I(\alpha,\beta,\gamma)$ on entangled quantum states can be represented by

$$D_I^B(\alpha,\beta,\gamma)=\begin{bmatrix} \cos(\beta/2)\cos\phi & \cos(\beta/2)\sin\phi & -\sin(\beta/2)\sin\theta & \sin(\beta/2)\cos\theta \\ -\cos(\beta/2)\sin\phi & \cos(\beta/2)\cos\phi & -\sin(\beta/2)\cos\theta & -\sin(\beta/2)\sin\theta \\ \sin(\beta/2)\sin\theta & \sin(\beta/2)\cos\theta & \cos(\beta/2)\cos\phi & -\cos(\beta/2)\sin\phi \\ -\sin(\beta/2)\cos\theta & \sin(\beta/2)\sin\theta & \cos(\beta/2)\sin\phi & \cos(\beta/2)\cos\phi\end{bmatrix}, \tag{4.7}$$

where

$$\phi=(\alpha+\gamma)/2 \quad \text{and} \quad \theta=(\alpha-\gamma)/2.$$

In the same manner, $D_{\mathrm{II}}(\alpha^*,\beta^*,\gamma^*)$ can be expressed as

$$D_{\mathrm{II}}^{B}(\alpha^*,\beta^*,\gamma^*)=\begin{bmatrix} \cos(\beta^*/2)\cos\phi^* & -\cos(\beta^*/2)\sin\phi^* & -\sin(\beta^*/2)\sin\theta^* & \sin(\beta^*/2)\cos\theta^* \\ \cos(\beta^*/2)\sin\phi^* & \cos(\beta^*/2)\cos\phi^* & \sin(\beta^*/2)\cos\theta^* & \sin(\beta^*/2)\sin\theta^* \\ \sin(\beta^*/2)\sin\theta^* & -\sin(\beta^*/2)\cos\theta^* & \cos(\beta^*/2)\cos\phi^* & -\cos(\beta^*/2)\sin\phi^* \\ -\sin(\beta^*/2)\cos\theta^* & -\sin(\beta^*/2)\sin\theta & \cos(\beta^*/2)\sin\phi^* & \cos(\beta^*/2)\cos\phi^* \end{bmatrix}, \tag{4.8}$$

where

$$\phi^*=(\alpha^*+\gamma^*)/2 \quad \text{and} \quad \theta^*=(\alpha^*-\gamma^*)/2.$$

The U transformation can be realized by the two-photon spinor rotation given by $D_{\mathrm{I}}^{B}(\pi/2,-\pi/2,-\pi/2)\otimes D_{\mathrm{II}}^{B}(0,-\pi/2,0)$, where

$$D_{\mathrm{I}}^{B}(\pi/2,-\pi/2,-\pi/2)=\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{bmatrix} \tag{4.9}$$

and

$$D_{\mathrm{II}}^{B}(0,-\pi/2,0)=\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 0 & 0 & -1 \\ 0 & 1 & -1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}. \tag{4.10}$$

B. Implementation with a two-photon interferometer

Perfect Bell state analysis is regarded as experimentally unfeasible at this stage [11]. Three of the four Bell states, however, have been distinguished experimentally by using a Hong-Ou-Mandel two-photon interferometer [14]. Our proposed scheme is valid for such an imperfect but experimentally feasible Bell state analyzer. We assume that $|P\rangle$ $(\equiv|\Psi^+\rangle)$ or $|Q\rangle$ $(\equiv i|\Psi^-\rangle)$ can be distinguished from the other three while $|R\rangle$ $(\equiv i|\Phi^+\rangle)$ and $|S\rangle$ $(\equiv|\Phi^-\rangle)$ result in the same output $|R\vee S\rangle$. Therefore $|A^+\rangle$ and $|B^+\rangle$ can be completely distinguished with the imperfect analyzer but $|C^+\rangle$ and $|D^+\rangle$ are indistinguishable whenever $|R\vee S\rangle$ is the result. As shown in Figs. 1 and 3, however, Bob can detect a bit error with a finite probability if he obtains $|P\rangle$ or $|Q\rangle$. This can be explained as follows. Case I: (i) Alice sends $|C^+\rangle$, (ii) Eve obtains $|P\rangle$ and resends $|A^+\rangle$, (iii) Bob obtains $|Q\rangle$ with a probability of $\frac{1}{2}$ and they can successfully detect Eve. Case II: (ii) Eve obtains $|R\vee S\rangle$ and resends $|B^+\rangle$ and (iii) Bob obtains $|R\vee S\rangle$. In this case, he cannot detect Eve. Therefore the error probability is reduced to $\frac{1}{4}$ per test bit but the probability reduction can be compensated for by inserting more test bits.

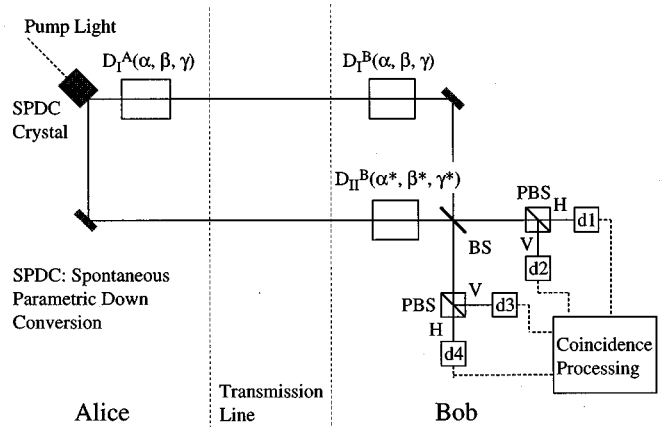

FIG. 6. The schematic configuration of our quantum channel with a two-photon interferometer.

Figure 6 shows the schematic configuration of our quantum channel based on two-photon interference [14]. Polarization-entangled photon twins can be generated through spontaneous parametric down conversion in a nonlinear optical crystal [12]. The signal and idler photons are superposed by a 50:50 beam splitter (BS). A linear polarization beam splitter (PBS) is inserted in either output direction of the BS. Output photons are counted by single-photon detectors numbered d1–d4 and coincidental registration makes it possible for Bob to distinguish $|P\rangle$, $|Q\rangle$, and $|R\vee S\rangle$ as summarized in Table II.

V. CONCLUSION

We propose a kind of secure quantum communication scheme for transmitting a definite binary sequence while confirming the security of the transmission against an eavesdropper. Our proposed communication scheme is very suitable for sending ciphertext in a secret-key cryptosystem because it enables us to detect an eavesdropper who attempts to decipher the key. In our proposed scheme, information transmission is separated into two steps. Alice, the sender, encodes a bit of quantum information on a quantum state of photon twins. Any quantum state is given by a two-term superposition of the four Bell states $|\Psi^+\rangle$, $i|\Psi^-\rangle$, $i|\Phi^+\rangle$, and $|\Phi^-\rangle$. Bob, the receiver, measures the photon twins with a Bell state analyzer and obtains partial information concerning the quantum state. Then Alice notifies Bob of the selected coding basis via a classical channel and Bob can de-

TABLE II. Imperfect Bell state analyzer.

Four Bell states	Registration results
$\lvert P\rangle$	(d1,d2),(d3,d4)
$\lvert Q\rangle$	(d1,d3),(d2,d4)
$\left.\begin{matrix}\lvert R\rangle \\ \lvert S\rangle\end{matrix}\right\}\ \lvert R\vee S\rangle$	Two photons are routed to the same detectors

termine the quantum state sent by Alice. A random operation of an appropriate unitary transformation before Bell state analysis makes it impossible for an eavesdropper to escape detection by Alice and Bob.

ACKNOWLEDGMENTS

The authors thank Dr. M. Koashi for valuable discussions, and Dr. T. Mukai and Dr. N. Uesugi for their encouragement during this research.

[1] G. Brassard, *Modern Cryptology: A Tutorial*, edited by G. Goos and J. Hartmanis, Lecture Notes in Computer Science Vol. 325 (Springer, Berlin, 1988).

[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] C. H. Bennett, G. Brassard, and A. K. Ekert, Sci. Am. (Int. Ed.) **267**, 50 (1992).

[4] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, J. Cryptology **5**, 3 (1992).

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

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

[7] B. Schneier, *Applied Cryptography* (Wiley, New York, 1993).

[8] Recently, QKD protocols have been proposed which do not discard any photon; L. Goldenberg and L. Vaidman, Phys. Rev. Lett. **75**, 1239 (1995); M. Koashi and N. Imoto, *ibid.* **79**, 2383 (1997); M. Ardehali, G. Brassard, H. F. Chau, and H. K. Lo, e-print quant-ph/9803007.

[9] A. Aspect, P. Grangier, and G. Roger, Phys. Rev. Lett. **47**, 460 (1981); **49**, 91 (1981); **49**, 1804 (1982).

[10] J. J. Sakurai, *Modern Quantum Mechanics, Revised Edition* (Addison-Wesley, New York, 1994), p. 323.

[11] P. G. Kwiat, K. Mattle, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **75**, 4337 (1995).

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

[13] M. Michler, K. Mattle, H. Weinfurter, and A. Zeilinger, Phys. Rev. A **53**, R1209 (1996).

[14] K. Mattle, H. Weinfurter, P. G. Kwiat, and A. Zeilinger, Phys. Rev. Lett. **76**, 4656 (1996).

[15] W. K. Wootters and W. H. Zurek, Nature (London) **299**, 802 (1982).

[16] D. Dieks, Phys. Lett. **92A**, 271 (1982).

[17] A. K. Ekert, B. Huttner, G. M. Palma, and A. Peres, Phys. Rev. A **50**, 1047 (1994).

[18] N. Gisin and B. Huttner, Phys. Lett. A **228**, 13 (1997).

[19] J. I. Cirac and N. Gisin, Phys. Lett. A **229**, 1 (1997).

[20] E. Biham and T. Mor, Phys. Rev. Lett. **79**, 4034 (1997).

[21] H. K. Lo and H. F. Chau, e-print quant-ph/9803006; D. Mayer, e-print quant-ph/9802025; C. H. Bennett and P. Shor, IEEE Trans. Inf. Theory **44**, 2724 (1998), and references therein.

[22] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996).

[23] In J. J. Sakurai, Ref. [10], p. 221.