PHYSICAL REVIEW A, VOLUME 61, 022303

Identity verification in quantum key distribution

Guihua Zeng[1] and Weiping Zhang[2]
[1]National Key Laboratory on ISDN, XiDian University, Xi'an 710071, People's Republic of China
[2]Department of Physics, Macquarie University, New South Wales 2109, Australia

(Received 30 April 1999; published 6 January 2000)

The security of the previous quantum key distribution protocols, which is guaranteed by the laws of quantum physics, is based on legitimate users. However, impersonation of the legitimate communicators by eavesdroppers, in practice, will be inevitable. In this paper, we proposed a quantum key verification scheme, which can simultaneously distribute the quantum secret key and verify the communicators' identity. Investigation shows that this proposed identity verification scheme is secure.

PACS number(s): 03.67.Dd, 03.65.Bz

I. INTRODUCTION

Since the first finding that quantum effects may protect privacy information transmitted in an open quantum channel by Wiesner [1], and then by Bennett *et al.* [2], a remarkable surge of interest in the international scientific and industrial community has propelled quantum cryptography into mainstream computer science and physics. Furthermore, quantum cryptography is becoming increasingly practical at a fast pace. Quantum cryptography is a field which combines quantum theory with information theory. The goal of this field is to use the law of physics to provide secure information exchange, in contrast to classical methods based on a (unproven) complexity assumption. Current investigations of quantum cryptography involve three aspects: the quantum key distribution (QKD) [3–21], quantum secret sharing [22,23], and quantum bit commitment and its application [24–26]. In particular, the quantum key distribution became especially important due to technological advances which allow their implementation in the laboratory. Several quantum key distribution protocols have been proposed; three main protocols of these are the BB84 protocol [3], B92 protocol [4], and EPR protocol [5]. The first quantum key distribution prototype, working over a distance of 32 cm in 1989, was implemented by means of laser transmitting in free space [6]. Soon experimental demonstrations by optical fibers were set up [7]. After that, many works on the quantum key distribution have been presented, which cover three aspects: (a) theoretical and experimental investigation of QKD protocols [8–10], (2) security of QKD protocols and detection of eavesdroppers [11–16], and (3) investigations of QKD used in practical applications [17–20].

To obtain a secure key, classic cryptography provides a technology, called key management. It includes key generation, key distribution, key preservation, key verification, key copying, key destruct, etc. In a practical application any single process (for example, key distribution) cannot completely guarantee the security of the key. In contrast to classic key management, we propose the concept of quantum key management. Currently, quantum key management includes quantum key generation and distribution, quantum key preservation (QKP), and quantum key verification (QKV). To guarantee the security of the quantum key in practical applications, quantum key verification and quantum key preservation are important as well as the quantum key distribution. In the following we describe these procedures.

The quantum key distribution is defined as a procedure allowing two legitimate users of a communication channel to establish two exact copies, one copy for each user, of a random and secret sequence of bits. The quantum key distribution employs quantum phenomena such as the Heisenberg uncertainty principle and quantum corrections to protect distributions of cryptographic keys. QKD is a technique that permits two parties, who share no secret information initially, to communicate over an open channel and to establish between themselves a shared secret sequence of bits. The presented QKD protocols are provably secure against an eavesdropping attack, in that, as a matter of fundamental principle, the secret data cannot be compromised unknowingly to legitimate users of the channel. Three ingenious protocols in the quantum key distribution have been proposed, and their security was warranted by the corresponding law of quantum physics. The first, by Bennett and Brassard [3], relies on the uncertainty principle of quantum mechanics to provide key security. The security guarantee is derived from the fact that each bit of data is encoded at random on either one of a conjugate pair of observables of a quantum mechanical object. Because such a pair of observables is subjected to the Heisenberg uncertainty principle, measuring one of the observables necessarily randomizes the other. A further elegant technique has been proposed by Ekert [5], which relies on violation of the Bell inequalities to provide the secret security. And the third technique, devised by Bennett [4], is based on the transmission of nonorthogonal quantum states.

The cryptography and the cryptoanalysis are always a pair contradiction. Once a cryptographic protocol is proposed, an eavesdropper (Eve) will try to break it. Quantum cryptography is also no exception. With the quantum key distribution protocols presented, several attack strategies have been proposed, such as an intercept and resend scheme [6], beamsplitting scheme [6], entanglement scheme [14], quantum copying [15,16], etc. Investigation show that the QKD protocols are secure under all presented attacks. It is appropriate to emphasize the limitation of the presented attack strategies which are restricted by quantum attack strategies.

Quantum key preservation is defined as a procedure of preserving quantum qubits which correspond the secret key

1050-2947/2000/61(2)/022303(5)/$15.00

between legitimate communicators. Ekert proposed a method of preservation quantum key using entanglement pairs, Biham *et al.* also proposed a method of preservation of the quantum key using quantum memory [21]. However, because the current technology cannot preserve the quantum states for long times, the proposed methods are not applicable. Currently, the quantum key is preserved by transferring the quantum states to a set of binary bits. This provides Eve a change to eavesdrop on the key, because the preservation of the classic key cannot prevent eavesdropping.

Quantum key verification is defined as a procedure of verifying the authenticity of the obtained key. The security of the previous QKD protocols, which is guaranteed by the law of quantum physics, is based on the legitimate users. In practice, the impersonation makes the communicators have to take action against eavesdroppers; an efficient way is to verify the communicators' identity. Unfortunately, there is no known way to initiate quantum identity verification in previous protocols. In addition, the presented QKD protocols are completely insecure under the men-in-middle attack: When the legitimate communicator Alice communicates with the legitimate communicator Bob, Eve intercepts all qubits sent by Alice, and communicates with Bob by impersonating Alice. Finally, Eve obtains two keys K_{AE},K_{EB}, where K_{AE} represents the secret key between Alice and Eve, and K_{AE} represents the secret key between Bob and Eve. As a result Eve can easily decrypt the ciphertext sent by Alice or Bob. Of course, communicators may use classic verification technologies to prove the legitimate communicators' identity. However, because Alice and Bob cannot simultaneously complete the identity verification and quantum key distribution, Eve may avoid the identity verification procedure. So, practically, quantum key verification is necessary in quantum key management.

In this paper, we propose a quantum key verification scheme to guarantee the security of quantum key obtained by the quantum key distribution. Our scheme uses a believable information center in the initial phase, because quantum key verification needs a sharing message between the legitimate users to confirm the communicators' identity. The information center is responsible neither for mutual verification nor for the generation and distribution of quantum keys. The role of this center is to simply help the legitimate users obtain the sharing message. Once the legitimate communicators obtain the sharing message, the information center does not need in any further communication. Of course, the information center is not necessary in the initial phase, because the communicators may use other methods to obtain a sharing message, e.g., the secure channel.

II. QUANTUM KEY VERIFICATION SCHEME

In what follows we propose a quantum key verification scheme which can implement quantum identity verification in a QKD protocol. It may be implemented by noncommute quantum states or nonorthogonal quantum states with the Heisenberg uncertainty principle. It also can be implemented by EPR pairs associated with Bell's theorem. In this paper, we use an EPR pair with Bell's theorem [27] to implement quantum identity verification. Both the identity verification and quantum key distribution are used in our secure verification protocol. There are two phases in the quantum identity verification protocol. The initial phase is completed at the key information center to set up the system, and the verification phase is executed between the two communication parties to achieve mutual verification and exchange the secure quantum key.

A. Initial phase

In this phase, we use the technology of Biham *et al.* [21], which uses quantum memory. For implementation of qubits in quantum memory the reader may refer to Ref. [21]. The communicators and the center are composed of a network. When the secure network system is set up, the information center and the communicators, Alice and Bob, will execute the following steps.

(1) Alice and Bob send the center their identifications $\mathrm{ID}_A,\mathrm{ID}_B$ to register this secure network. Then the center sets up a quantum channel between Alice and the center, and between Bob and the center.

(2) The center prepares two singlet EPR pairs. These EPR pairs may be expressed as

$$|\Phi_{ac}\rangle=\sqrt{\frac{1}{2}}(|\uparrow_a\downarrow_c\rangle-|\downarrow_a\uparrow_c\rangle), \tag{1}$$

$$|\Phi_{bc}\rangle=\sqrt{\frac{1}{2}}(|\uparrow_b\downarrow_c\rangle-|\downarrow_b\uparrow_c\rangle). \tag{2}$$

The state of the whole system is

$$|\Phi_{abc}\rangle=\frac{1}{2}(|\uparrow_a\downarrow_c\rangle-|\downarrow_a\uparrow_c\rangle)\otimes(|\uparrow_b\downarrow_c\rangle-|\downarrow_b\uparrow_c\rangle) \tag{3}$$

where the subscripts a,b,c denote the particles (for Alice, Bob, and the center). Equations (1)–(3) may be rewritten as

$$|\Phi_{ac}\rangle=\sqrt{\frac{1}{2}}(|\nearrow_a\searrow_c\rangle-|\searrow_a\nearrow_c\rangle), \tag{4}$$

$$|\Phi_{bc}\rangle=\sqrt{\frac{1}{2}}(|\nearrow_b\searrow_c\rangle-|\searrow_b\nearrow_c\rangle), \tag{5}$$

and

$$|\Phi_{abc}\rangle=\frac{1}{2}(|\nearrow_a\searrow_c\rangle-|\searrow_a\nearrow_c\rangle)\otimes(|\nearrow_b\searrow_c\rangle-|\searrow_b\nearrow_c\rangle), \tag{6}$$

where $|\uparrow\rangle,|\downarrow\rangle$ are the eigenstates of $\hat{S}_z$, and $|\nearrow\rangle,|\searrow\rangle$ are the eigenstates of $\hat{S}_x$. The first particle of each singlet pair is sent to Alice and to Bob, respectively, while the center keeps the second of each singlet EPR pair.

(3) Alice and Bob randomly and independently measure their particles along the $\hat{S}_z$ and $\hat{S}_x$ axes (Alice's and Bob's measurement are local), where $\hat{S}_z$ and $\hat{S}_x$ are noncommute,

$$[\hat{S}_z,\hat{S}_x]=i\hbar\hat{S}_y. \tag{7}$$

After finishing the measurement the corresponding state of Alice's and Bob's particles is in any of the four states $|\uparrow\rangle,|\downarrow\rangle,|\nearrow\rangle,|\searrow\rangle$.

(4) Check eavesdropping between Alice and the center, and between Bob and the center. Alice and Bob randomly choose some quantum states from the secquence of their quantum states, respectively, and check the correction of quantum states like in the EPR protocol.

(5) The center measures the eigenvalue of the total-spin operator ($\hat{S}$) of the first pair, the second pair, etc., except for the qubits for the detection of eavesdropping. The center must be able to keep the quantum states for a while (in case the states do not arrive at the same time from Alice and Bob).

(6) The center tells Alice and Bob the measurement results. If the result of the measurement is $s=1$, Alice and Bob discard the transmission, because Alice and Bob cannot infer anything about the value of each other's quantum states. Even if they have the same axis, it cannot give a perfect anticorrection along both $\hat{S}_z$ and $\hat{S}_x$ axes. If the result of the measurement is $s=0$, the two particles are projected onto the singlet state, Alice and Bob keep their quantum states. In that case Eqs. (4) and (5) ensures that, if the two spins were prepared along the same axis, they necessarily had opposite values (the projection of the states with identical spins on the singlet state is zero). As a result, Alice and Bob can know each other's quantum states.

(7) Alice and Bob tell each other the axis they used (but not the bit value). When they used different axes, they discard the transmission. Whenever they used the same axis they know if their qubits are correlated or anticorrelated, and they can judge the quantum states each other; e.g., if Alice and Bob measure their particles along $\hat{S}_z$, when Alice's state is $|\uparrow\rangle$, Bob's state is $|\downarrow\rangle$.

(8) Alice and Bob keep the qubits which correspond to $s=0$ with same axis as the raw sharing key K_1'. Proceeding with the key K_1' like the previous QKD protocol, e.g., the BB84 protocol, one obtains the sharing key K_1. Assuming the sharing key has n components, then K_1 may be expressed as

$$K_1=\{K_1^1,K_1^2,\ldots,K_1^n\}. \tag{8}$$

It is impossible for the center to know the sharing key K_1. Because if the center projects on the singlet state, he does not get any information on Alice's and Bob's bits; if the center projects onto a different state (possibly entangled with his own system), which cannot give perfect anticorrelation along both $\hat{S}_z$ and $\hat{S}_x$ axes, he will unavoidably introduce an error, which Alice and Bob shall identify during the discussion. However, a cheating center can use the middle-attack strategy described in the Introduction. So this proposed scheme needs a believable center. After the legitimate users obtain the sharing key K_1, the information center will not need further communication between Alice and Bob.

B. Verification phase

The verification phase performs the identity verification and the quantum key distribution; it executes the following steps.

Step 1. Alice and Bob transfer the sharing key K_1 into a sequence of measurement basis. While Alice and Bob need to verify their identification, or need to set up a new communication, they secretly transfer the preserved sharing key to a sequence of measurement bases according to the aforehand appointment. After being transferred, Alice and Bob obtain a sequence of sharing measurement bases M_{K_1}:

$$M_{K_1}=\{M^1_{K_1^1},M^2_{K_1^2},\ldots,M^n_{K_1^n}\}, \tag{9}$$

where $M^i_{K_1^i}$ depends on K_1^i, $i=1,2,\ldots,n$. For example, if Alice and Bob use the measurement basis of polarization photons which was used in the BB84 protocol, they may let the bit ''1'' correspond to the rectilinear measurement basis and ''0'' correspond to the diagonal measurement basis, or vice versa. Expressing the rectilinear measurement basis by the symbol $\oslash$ and the diagonal measurement basis by the symbol $\odot$, if the sharing key is $K_1=001101$, the sequence of measurement bases is $M_{K_1}=\odot\odot\oslash\oslash\odot\oslash$.

Step 2. Alice and Bob set up a quantum communication channel. When Alice wants to communicate with Bob, Alice and Bob need to set up a quantum channel. The transmitting quantum states in the quantum channel may be arbitrary, for example, the polarization photon state or the phase correction states. In this protocol, we use the two-particle polarization entanglement state. The state generated from a type-II parametric down-conversion crystal can be written as [28]

$$|\Psi_{ab}\rangle=\sqrt{\frac{1}{2}}(|\uparrow\rangle_a|\downarrow\rangle_b+e^{i\alpha}|\downarrow\rangle_a|\uparrow\rangle_b), \tag{10}$$

where α is a birefringent phase shift of the crystal, and $|\uparrow\rangle$ and $|\downarrow\rangle$ denote the horizontal and vertical polarization eigenstates. Using appropriate birefringent phase shifts and polarization conversion, one may easily convert the above state into any of the four Bell states

$$|\Psi^{\pm}_{Bell}\rangle=\sqrt{\frac{1}{2}}(|\uparrow_a\downarrow_b\rangle\pm|\downarrow_a\uparrow_b\rangle) \tag{11}$$

and

$$|\Phi^{\pm}_{Bell}\rangle=\sqrt{\frac{1}{2}}(|\uparrow_a\uparrow_b\rangle\pm|\downarrow_a\downarrow_b\rangle). \tag{12}$$

In this proposed scheme, we use the state

$$|\Psi_{ab}\rangle=|\Psi^{-}_{Bell}\rangle=\sqrt{\frac{1}{2}}(|\uparrow_a\downarrow_b\rangle-|\downarrow_a\uparrow_b\rangle). \tag{13}$$

Step 3. Alice chooses a random basis like in the EPR protocol for measuring one numbering of each EPR pair of particles. The other particle of each EPR pair is measured by

Bob in the next step. Alice's measurement results in effect determine, through the EPR corrections, a sequence of states for Bob's particles.

Step 4. Bob measures the received strings of quantum states. Bob randomly measures the sequence of quantum states by using two measurement bases M,M_{K_1}, where M is the measurement basis for the quantum key distribution and for obtaining a new identity sharing key, it is chosen randomly like that in the EPR protocol. M_{K_1} is the measurement basis for identity verification in the current communication.

Step 5. Alice and Bob check the eavesdropper. For secure communication, the legitimate communicators Alice and Bob need to first detect the eavesdroppers. Bob randomly chooses some measurement results measured by the basis M for checking the correction of the EPR pair. Then the communicators judge the eavesdropping according to Bell's theorem.

Step 6. Bob encrypts his results measured by M_{K_1}. Although Bob does not know the quantum states measured by Alice, it will not influence the identity verification. Expressing the substrings of quantum states for verification by

$$|\Psi\rangle=\{|\psi_1\rangle,|\psi_2\rangle,\dots,|\psi_n\rangle\}, \tag{14}$$

where $|\psi_i\rangle$ represents a quantum state received by Bob, it is determined by Alice's measurement. The corresponding sequence number of quantum states $|\psi_i\rangle$ is N_i in Alice's whole qubit strings. After finishing the measurement, Bob obtains

$$|\Phi\rangle=M_{K_1}|\Psi\rangle, \tag{15}$$

where $|\Phi\rangle=\{|\phi_1\rangle,|\phi_2\rangle,\dots,|\phi_n\rangle\}$ represents the measurement results under the measurement basis M_{K_1}, $|\phi_i\rangle=M^i_{K^i_1}|\psi_i\rangle$, $i=1,2,\dots,n$. Transferring $|\Phi_i\rangle$, $i=1,2,\dots,n$ into binary bit strings m according to the aforehand appointment, and then encrypting m and N_i by K_1, Bob obtains the ciphertext

$$y=E_{K_1}(m,N_i). \tag{16}$$

Bob sends Alice the ciphertext y.

Step 7. Verifying Bob's identity. Having received Bob's ciphertext y, Alice decrypts it,

$$m',N_i=E^{-1}_{K_1}(y). \tag{17}$$

Alice compares her results with m', then gets the measurement basis M_{K_t}. If $K_t=K_1$, Bob's identity is true.

Step 8. Verifying Alice's identity. After Alice decrypted the ciphertext, Alice sends Bob the result m'. If $m'=m$, Alice's identity is true.

Step 9. Alice and Bob distribute the quantum secret key. If the communicators are legitimate, Alice and Bob distribute the quantum secret key using the remainder qubits; the process is the same as the EPR protocol. Finally, the legitimate communications obtain a secure key K.

Step 10. Alice and Bob discard the sharing keys K_1, and set up a new sharing key K_2. After finishing the identity verification, the sharing key K_1 is no longer used. The legitimate users obtain a new sharing key from the qubits measured by M. The method is the same as that of obtaining the quantum key. Of course, one can directly take portion bits from the final quantum key as the sharing key. It is appropriate to stress that the generation of the new sharing key K_2 does not need the information center.

In practical communications, because the noise effects, errors are inevitable in the quantum channel. If the errors are produced by Bob's measurement, Bob tells Alice the error qubits to overcome the noise effects. If the errors are produced in transmission, Alice and Bob estimate the bound of errors e_t, and consider it in the identity verification. While the error is more than e_t, the communicators refuse each other; otherwise, the communicators are legitimate. This procedure may be finished in step 5.

It has been noted that the presented protocol cannot prevent voluntary attack. This is a drawback of quantum cryptography. How to prevent a voluntary attack needs further investigation.

III. SECURITY ANALYSIS

The proposed quantum key verification scheme can simultaneously distribute the quantum secret key and verify the communicators' identity. Because the proposed scheme includes two phases, we analyze the security of the initial phase and verification phase, respectively. It is noted that the security of the sharing key K_1 is very important, because the insecurity of K_1 results in the insecurity of quantum key verification.

In the initial phase, the security derives from the security of the EPR protocol, and relies on the fact that the singlet state is the only state for which the two spins are anticorrelated both in $\hat{S}_z$ and in the $\hat{S}_x$ basis. In fact, the security of this phase is the same as the ERP protocol. The reasons are the following: (1) the channels between Alice and the center, and between Bob and the center, are set up by EPR pairs. (2) Alice and Bob measure their particles randomly along the $\hat{S}_z$ and $\hat{S}_x$ axes (Alice's and Bob's measurements are local). Because $\hat{S}_z$ and $\hat{S}_x$ are noncommute, and Alice and Bob only show the measurement directions, Eve cannot obtain the sharing key. (3) The entanglement attack strategy is not succeed. It has been studied in Ref. [21]. So the sharing key K_1 is secure. It needs to be stressed that the center needs to be believable, because the center can use the men-in-middle attack strategy.

In the verification phase, the QKD is provably secure because we use the previous QKD protocol. So in the following, we mainly analyze the security of the verification procedure. We believe this scheme is secure for the following reasons. (1) Our protocol does not have the conspiracy problem of masquerading. If a forger wants to masquerade the user Alice or Bob to communicate with others, he must find the sharing key K_1. However, it is difficult to obtain the sharing secret because of the following two reasons. First, the sharing key is obtained by the quantum key distribution protocol which is provably secure. Second, the sharing key is used only one time; the eavesdropper does not know any information about the sharing key. In addition, Eve cannot get the ciphertext y described in Eq. (17) by any way, because one may use the one-time pad code, which was proved to be unconditionally secure by C.E. Shannon. (2) The quantum attacking strategy is invalid. The reason is the same as the analysis for previous QKD protocols, because our protocol uses the EPR pairs; the security relies on the correction of the EPR particle and Bell's theorem. So the security of our scheme equals the EPR protocol.

There is a weakness in our protocol. The weakness of our protocol is the preservation of the sharing key. Although the sharing key, obtained in the last time quantum communication, is provably secure, the preservation of the sharing key has not prevented the possibility of attacking by eavesdroppers like in classic cryptography, due to the fact that the sharing key is preserved by transferring the quantum states to a set of binary bits. In fact, this drawback exists in all symmetric cryptographic systems. Of course, we can use EPR effects or other quantum effects, e.g., quantum memory, to keep the common key, but the preservation time is very short according to current technology. A long time correction of quantum states is needed in the future.

IV. CONCLUSION

Quantum key management includes QKD, QKP, QKV, etc. Many works on QKD were presented. However, the previous QKD protocols are based on legitimate users. This means that legitimate communicators may be impersonated by an eavesdropper. Although one can use the classic verification protocol to verify the communicators' identity, because the verification procedure and the QKD procedure cannot be simultaneously implemented, Eve can escape the verification procedure. In addition, the quantum key distribution protocol is completely insecure under a men-in-middle attack.

For circumventing the above drawback, we proposed a quantum key verification scheme in this paper. Our scheme can simultaneously distribute the quantum secret key and verify the communicators' identity. The QKD is implemented by the previous EPR protocol; the verification procedure is implemented by the symmetric cryptographic scheme with quantum effects. The presented scheme is provably secure.

We use EPR effects with Bell's theorem to implement quantum identity verification. It can prevent impersonation and middle attack. Of course, it can also be implemented by noncommute quantum states or nonorthogonal quantum states with the Heisenberg uncertainty principle. So identity verification in the BB84 protocol and in the B92 protocol may be done by using a similar procedure.

ACKNOWLEDGMENT

This project was supported by the Natural Science Foundation of China, Grant No. 69803008.

[1] S. Wiesner, SIGACT News **15**, 78 (1983); original manuscript written ca. 1970.
[2] C.H. Bennett, G. Brassard, S. Breidbart, and S. Wiesner, *Advances in Cryptology: Proceedings of Crypto 82, 1982*, edited by D. Chaum, R.L. Rivest, and A.T. Sherman (Plenum Press, New York, 1982), p. 267.
[3] C.H. Bennett and G. Brassard, SIGACT News **20**, 78 (1989).
[4] C.H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[5] A.K. Ekert, Phys. Rev. Lett. **67**, 661 (1991); A.K. Ekert, J.G. Rarity, P.R. Tapster, and G.M. Palma, *ibid.* **69**, 1293 (1992).
[6] C.H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, J. Cryptology **5**, 3 (1992).
[7] J. Breguet, A. Muller, and N. Gisin, J. Mod. Opt. **41**, 2405 (1994).
[8] S. Phoenix, S. Barnett, P. Townsend, and K. Blow, J. Mod. Opt. **42**, 1155 (1995).
[9] S.M. Barnett and S.J.D. Phoenix, J. Mod. Opt. **40**, 1443 (1993).
[10] C.H. Bennett, G. Brassard, and N.D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
[11] B. Hutter and A. Ekert, J. Mod. Opt. **41**, 2455 (1994).
[12] C.A. Fuchs, N. Gisin, R.B. Griffiths, C.S. Niu, and A. Peres, Phys. Rev. A **56**, 1163 (1997).
[13] B.A. Slutsky, R. Rao, P.C. Sun, and Y. Fainman, Phys. Rev. A **57**, 2383 (1998).
[14] H.E. Brandt, John M. Meyers, and S.J. Lomonaco, Jr., Phys. Rev. A **56**, 4456 (1997).
[15] C.S. Niu, and R.B. Griffiths, Phys. Rev. A **58**, 4377 (1998).
[16] L.M. Duan and G.C. Guo, Phys. Rev. Lett. **80**, 4999 (1998).
[17] J.G. Rarity, P.C.M. Owens, and P.R. Tapster, J. Mod. Opt. **41**, 2435 (1994).
[18] P.D. Townsend, J.G. Rarity, and P.R. Tapster, Electron. Lett. **29**, 634 (1993).
[19] P.D. Townsend, J.G. Rarity, and P.R. Tapster, Electron. Lett. **29**, 1291 (1993).
[20] C. Marand and P.D. Townsend, Opt. Lett. **20**, 1695 (1995).
[21] E. Biham, B. Huttner, and T. Mor, Phys. Rev. A **54**, 2651 (1996).
[22] M. Hillery, V. Buzek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).
[23] A. Karlsson, M. Koashi, and N. Imoto, Phys. Rev. A **59**, 162 (1999).
[24] D. Mayers, Phys. Rev. Lett. **78**, 3414 (1997).
[25] H.K. Lo and H.F. Chau, Phys. Rev. Lett. **78**, 3410 (1997).
[26] L. Goldenberg, L. Vaidman, and S. Wiesner, Phys. Rev. Lett. **82**, 3356 (1999).
[27] J.S. Bell, Physics (Long Island City, N.Y.) **1**, 195 (1965).
[28] P.G. Kwiat, K. Mattle, H. Weinfurther, and A. Zeilinger, A.V. Serglenko, and Y. Shih, Phys. Rev. Lett. **75**, 4337 (1995).