Authority-based user authentication in quantum key distribution

Daniel Ljunggren, Mohamed Bourennane, and Anders Karlsson*
Laboratory of Quantum Electronics and Quantum Optics, Department of Electronics, Royal Institute of Technology, Electrum 229, SE-164 40 Kista, Sweden

(Received 19 November 1999; published 13 July 2000)

We propose secure protocols for user authenticated quantum key distribution on jammable public channels between two parties, Alice and Bob. Via an arbitrator, Trent, these protocols provide data integrity and mutual identification of the messenger and recipient. The first three are based on single-photon generation and detection. The first and second require (initially) an unjammable channel between the arbitrator and each party. The third requires one broadcast from the arbitrator, disclosing what type of deterministic modification of the states sent through the quantum channel was done by him. The fourth and fifth protocols are based on two-particle entanglement with a preselection of nonorthogonal superpositions of Bell states. These two protocols also require one broadcast from the arbitrator disclosing the type of entangled state in each sending.

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

I. INTRODUCTION

Secure electronic communication, as provided by cryptography, is one of the cornerstones of the emerging information society. The following are among the basic tasks of cryptography: authentication of users, integrity of data, and privacy of data [1,2]. By *user authentication* (also called user identification) we mean the way in which a user's identity is proved (i.e., the origin of data); by *data integrity* (also called data authentication) we mean the way that data sent by the true user over any channel have not been modified or replaced; and by *privacy of data*, we mean the prevention of data from being intercepted by an unauthorized eavesdropper. The latter is warranted by encrypting the plain text into a cipher text, and for this we need a key that is to become shared by both parties involved, and this requires secure key distribution.

Classically, cryptography is divided into two classes, namely, private (symmetric) key cryptography and public (asymmetric) key cryptography. In the former class, two users (conventionally denoted Alice and Bob) must share a key to protect the privacy of data. To some extent this method can also be used to provide data integrity once the users have been authenticated, but not for user authentication directly since this requires an encryption key that has not yet been authenticated.

In the latter class, a user can provide all other users with a public key for encryption, while he/she keeps a private key for decryption. The decryption key cannot easily be found knowing only the encryption key. This class of cryptosystems easily solves the problem of *key distribution*, and can also be used to provide user authentication and data integrity, although it has the disadvantage of relying heavily on computational assumptions [1–4], making it vulnerable to threats of powered computing. It is often used together with private key cryptography, and serves in this case only the need for key distribution.

Quantum key distribution (QKD) has been proposed as a way to solve the problem of key distribution using fundamental properties of quantum mechanics to establish an unconditionally secret shared key [5–7]. See [8,9] for a flavor of experimental QKD and [10–12] for discussions on the security of QKD.

Before addressing the issue of authentication, we will define two types of channels present in QKD: the quantum channel and the public channel.

(1) The quantum channel serves the need to be private in the sense that the quantum channel may be eavesdropped on or tampered with by no more than what is permissible by quantum mechanics. This can be done passively by Eve, or actively by Mallory. The essence of QKD is to provide a method of encoding bits onto quantum states in such a way that any measure taken by an eavesdropper can be discovered by the legitimate users.

(2) The public channel is used by involved parties to exchange classical information, required for basis encoding, error correction, check of eavesdropping, and privacy amplification. It can be divided into two classes: jammable and unjammable. The unjammable channel provides data integrity that can be classically realized through authentication techniques using hash functions [3]. The security of these functions, though, also relies on computational assumptions. The jammable channel can be actively tampered with in such a way as to insert or modify messages.

A crucial assumption in QKD has been that the public channel is unjammable. Indeed, if Mallory controls the classical public channel as well as being able to monitor the quantum channel, QKD will inevitably fail. In such a scenario, Mallory can always do a ''man-in-the-middle'' attack and impersonate Alice or Bob. For instance, separate keys could be established for Alice and Bob, and thus provide unlimited access to their information.

To guarantee that this does not happen, user authentication comes into play. The fundamental problem of authentication is how to check for a shared secret under the guarantee that it will stay known only to Alice and Bob. For mutual authentication, of course, it is inevitable that they share some initial secret. If this is not the case, one classical method is to use a trusted third party who can verify that a certain key

*Electronic address: andkar@ele.kth.se

belongs to whomever it is supposed to—like in public key cryptography. User authentication based on quantum cryptography using any kind of public channel has previously been studied. Most protocols use unjammable channels and are so-called self-enforcing; i.e., no parties other than Alice and Bob are involved. However, a realistic QKD environment instead suggests that a jammable public channel between Alice and Bob should be considered. Moreover, contrary to self-enforcing protocols, we believe it is desirable that Alice and Bob need not share an initial secret. Due to this, and to prevent ‘‘man-in-the-middle’’ attacks, the introduction of a trusted authority, Trent, becomes inevitable also for QKD. The authentication between Alice and Bob will instead pass via Trent, who can verify (necessarily over unjammable channels) to each user the identity of the other. This is partly addressed in Ref. [21].

Unjammable channels like those between Alice-Trent and Bob-Trent can be guaranteed by ‘‘personal’’ authentication of such a kind that you make when you visit your bank to get your personal identification number code, together with classical authentication techniques, e.g., authentication codes [2]. In principle, if necessary, arbitrarily long authentication seeds can be exchanged for this purpose.

As a first indication that quantum authentication could be possible we consider the method of Crépeau and Salvail [13]. It provides a simple solution without Trent: if there is a shared secret string between the true Alice and Bob, then use the secret string for the selection of the polarization basis in the Bennett-Brassard 1984 (BB84) four-state quantum cryptoprotocol [5] and send a known code word over the channel. Having no *a priori* information regarding the basis choice, the eavesdropper will inevitably make errors in his or her detection. Independently, Huttner, Imoto, and Barnett proposed a very similar idea in Ref. [14], again using the basis encoding to test the correspondence between two strings. The problem, however, as stressed in [13], is that in the authentication process a dishonest party or an eavesdropper should not be able to extract any information about the initial secret, even through repeated attempts. In [13], no solution to this strict requirement was found, although it was proposed that a protocol could be built on quantum-oblivious transfer. Later, however, it was shown that quantum-bit commitment and quantum-oblivious transfer are not unconditionally secure [15,16].

Similar ideas along these lines, without Trent, have also been presented by Dusek *et al.* in [17]. They propose one classical and one QKD-based solution for user authentication. To address the problem in [13] regarding repeated attempts by an eavesdropper, the bits used for authentication are thrown away after each interleaved comparison of their secretly shared string. New secret bits are then refueled using QKD.

Another recent paper [18] discusses self-enforced authentication based on entanglement catalysis. In a first simple protocol, Alice and Bob share an ensemble of two-particle entangled quantum states. The initial secret in this case is Alice and Bob’s unique knowledge of the particle states. To authenticate, Alice (Bob) sends over a number of states from her (his) ensemble and Bob (Alice) verifies that the states are the correct ones. In this process, a few of the initial states are consumed and thus the authentication secret is diminished. In an improved version of the protocol, the states initially shared by Alice and Bob are catalysis states [19]. Using these catalysis states as the shared secret only Alice and Bob will be able to make the correct local transformations [20,19] of another pair of states. The correctness of this transformation is verified between Alice and Bob and used as an authentication. What is interesting about this procedure is that the shared secret information, the catalysis states, is kept intact.

These protocols described above involve only Alice and Bob. Recently, Zeng and Zhang [21] studied the same basic idea as in [13] and [14]; however, their work was more in the context of user authenticated secret key distribution. Trent is introduced to generate the initial secret. In the protocol, Alice and Bob each have a two-particle entangled state [Einstein-Podolsky-Rosen (EPR) pairs] from which one particle each is sent to and measured by Trent. He uses the method of entanglement swapping [22] to generate a joint key to be used by Alice and Bob. Following this, the joint key should be used for user authentication in an EPR-type quantum cryptography [6] protocol with the basis choice made from the joint session key, similar to [13] and [14].

The main purpose of the present work is to address the issue of user authentication and data integrity by quantum methods. This also goes under the name of quantum authentication. As pointed out, in a realistic scenario we cannot justify self-enforcing protocols, and so therefore we feel the arbitrator unavoidable. With Trent’s help, and with a jammable channel at Alice and Bob’s disposal, we will provide means for Alice and Bob to agree upon a secret key using QKD. If we have a channel, or a combination of channels, that can provide us with data integrity, we can then use this to perform user authentication. Furthermore, we will show that the same objectives as in [21], using an arbitrator, can be achieved in a less complex fashion using either nonentanglement or entanglement-based protocols.

The paper is outlined as follows: In this introduction we gave a brief review of the recent work on quantum authentication. In Sec. II we will introduce and define the conditions for the third-party trusted authority, Trent. His role is to provide Alice and Bob with the seeding information that will increase security. In Sec. III, we present protocols for quantum key distribution based on conventional single-photon quantum cryptography, providing user authentication and data integrity. In Sec. IV, we present two simple entanglement-based quantum key distribution protocols, also with user authentication and data integrity. Finally, in Sec. V, our results are discussed and concluded.

II. THIRD-PARTY TRUSTED ARBITRATOR FOR QKD-BASED USER AUTHENTICATION

Obviously, it would be nice if quantum methods could provide self-enforcing protocols. However, even if this would call for some kind of ‘‘asymmetric quantum key’’ cryptography (which remains to be invented), we would unfortunately still need a trusted authority to authenticate the public quantum key. What we are concerned with here is to reflect upon whether quantum mechanics with its inherent properties (unitarity, entanglement) can yield any advantage over classical methods providing authentication via an arbitrator.

For protocols designed with Trent, like those proposed here and in Ref. [21], we believe we cannot provide Alice and Bob with a key that can be unconditionally kept in secret from Trent, as it is actually he/she who directs the entire authentication process. In other words, if Alice and Bob's mutual authentication is guaranteed only by their individual and non-necessarily correlated secret with Trent, Trent will also have full control over their communication (regardless of what channels are used) and can always do a ''man-in-the-middle'' attack if he so chooses. We conclude that, in principle, no restrictions can be imposed on Trent.

What we gain though, and what our last four protocols show, is that we can make it necessary for Trent to actively have to eavesdrop on the communication between Alice and Bob in order to get the key. Also, for the authentication that enables the authenticated direct channel to be opened up between Alice and Bob, we can allow the channels Alice-Trent and Trent-Bob to be open only once initially. Note that Trent can succeed in his eventual attempt of finding the key only during its setup and that Mallory can never. The protocols we propose are quite simple, and can clearly be improved, but we hope they are in enough detail to illustrate a few points that presumably have not been pointed out before.

Suppose the protocol followed by Trent has the following properties:

(A) Alice and Trent know the identity of each other, and they share at some instant an unjammable public channel.

(B) Bob and Trent know the identity of each other, and they share at some instant an unjammable public channel.

If the channels are available at all times, we again have an unjammable and direct public channel between Alice and Bob, and conventional quantum cryptography can be used. What we would like to do is to set restrictions on the joint availability of the channel with Trent. We will present five schemes, starting from very simple schemes and moving toward more complex ones, where with given restrictions, and some additional ones, one will be able to authenticate Alice and Bob, while at the same time provide a secret key for encryption. By giving these examples, we try to address the essential classical and quantum ingredients in the protocols.

III. NONENTANGLEMENT-BASED QKD WITH USER AUTHENTICATION

A. Nonentanglement QKD protocol (i)

The additional restriction we set on the channels between Alice and Trent and Bob and Trent for the next two protocols is (C) the public channel between Alice and Trent is open only once, as is also the channel between Bob and Trent, and there is on no occasion a channel that is directly open between Alice, Trent, and Bob. This condition, as formulated, is needed for the scheme presented next.

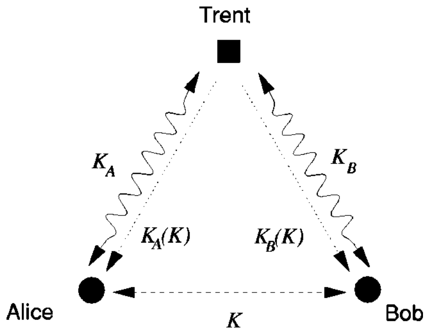

FIG. 1. Channel diagram for protocol (i). The wavy line shows the quantum channel, the dotted line shows the unjammable public channel, and the dashed line the encrypted channel. See text for details.

To set up the authentication between Alice and Bob, Trent does the following, as illustrated in Fig. 1:

(1) Trent sends Alice a long bit string encoded using the BB84 protocol (or another quantum key distribution protocol such as Ekert's protocol [6]) along with error correction and privacy amplification [5] to generate a secret key K_A. He then sends the ''session key'' K to Alice encrypted with the secret key K_A.

(2) Next, Trent sends the key K to Bob by the same method (using a different secret key K_B).

(3) Alice and Bob can send each other the secret message encrypted with the key K. It should be noted that in this trivial case, since Trent knows the key K, he can also listen to the encrypted communication. Furthermore, this protocol is obviously nothing other than a slight variation of the conventional quantum cryptographic protocol split up into two channels with Trent in the middle. Thus this protocol as such is not very interesting, but it serves as a prelude to the protocols that will follow.

B. Nonentanglement QKD protocol (ii)

The second protocol is also based on the scheme BB84 using either phase or polarization encoding. The basic idea of this protocol is to send an authentication string S to Alice and Bob, which is then sent from Alice to Bob interleaved with the other bits in the QKD protocol.

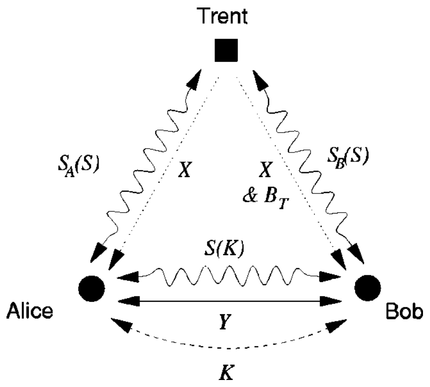

FIG. 2. Channel diagram for protocol (ii). The line types are defined as in Fig. 1, with the addition of the solid line showing the jammable public channel. See text for details.

The restriction we set on the channels between Alice and Trent and Bob and Trent is the same as in the previous example, i.e., (A–)C). The added feature in this protocol, and in the ones following, is that Trent does not directly possess the key *K*, but he has to actively eavesdrop on the information in *Y* to get it. On the contrary, Mallory can always be detected.

To set up the authentication between Alice and Bob, Trent does the following, as illustrated in Fig. 2:

(1) Trent sends Alice a long bit string encoded using the BB84 protocol with extra information *X* for error correction and privacy amplification. This will give Alice a bit string S_A of *N* bits, which is provably secure.

(2) Next, Trent sends an even longer bit sequence to Bob and establishes a secret bit string with Bob, S_B, again using the BB84 protocol with extra information *X*. From this string, Trent tells Bob a sequence $B_T=(b_1,b_2,\ldots,b_N)$, with the property that the bit sent to Bob at position b_i is exactly the same as the corresponding bit *i* in the string S_A established for Alice. Using this, Alice and Bob now share a common secret string $S=S_A=S_B$. Note that we rather not use *S* for the encryption itself, as Trent has direct knowledge of it. In practice we gain security if we can make Trent to actively have to eavesdrop on the information in *Y* to get the key. On the contrary, Mallory can always be detected.

(3) To use *S* for authentication, we partition *S* into blocks, $S=(S_1,S_2,\ldots,S_u,W,Z)$ where the length of $S_1,S_2,\ldots,S_u$ is $\log(M)$ bits (all log in base 2), *M* is the total number of bits sent for the key, and the length of *W* and *Z* is equal to *u*. We then let each block represent a position in the ensuing secret key transmission. The small chance that any $S_i=S_j$ for any *i* or *j* can be treated separately. Alternatively, we may divide *M* into separate blocks, with one S_i for each block. If so, the length of block S_i is $\log(M/u)$ bits.

(4) Now Alice and Bob establish a secret key *K* according to the BB84 protocol, sending a long bit string of *M* bits, however, interleaved at given bit slots S_i with a known outcome taken as the *i*th bit of *W* with polarizer settings from the *i*th bit of *Z*. This is similar to the hiding procedure used in [13]. With no *a priori* information on *S*, the photon sequence will then appear completely random for Mallory. In a simpler version, one could just use deterministic settings of the polarizers since Mallory will only get a few chances to extract the string.

(5) For Bob to authenticate Alice, he only checks that the outcome *Y* he receives corresponds to the correct ones he expects. This could be done using some coding procedure similar to that used in [13], or simply by checking the bit-error rate (BER) of the bits received. It should be noted that in practical cases where the transfer efficiency is low, the length of *Y* is much smaller than the length *u* of *W*.

(6) For Alice to authenticate Bob, she waits for Bob to send back over the public channel the result of Bob's measurement of *Y* together with the information of the timing slots indicating when he received each bit. The latter is needed when the transfer efficiency is below unity for Alice knowing which bit was received by Bob. If correct, she knows that Bob is the correct person receiving the secret key *K*. To succeed with eavesdropping, or impersonation, Mallory would have to succeed in evading detection. For the BB84 scheme using an intercept-and-resend strategy on all bits, Mallory will introduce a 25% BER [5]. Furthermore, he would have to guess which of the *M* bits constitutes *W*. The probability of succeeding in obtaining the authentication string correctly with no *a priori* information on *S* is $\Pr(S)=(3/4)^u\binom{u}{M}$, which is very small.

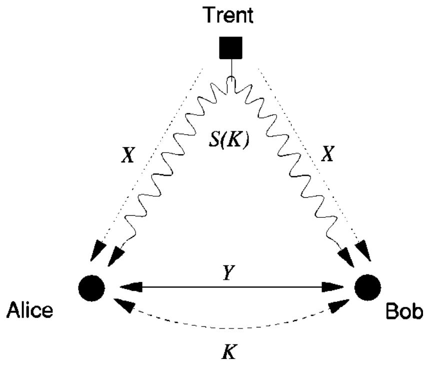

FIG. 3. Channel diagram for protocol (iii). The line types are defined as in the previous figures. In the quantum channel that goes between Alice and Bob (via Trent), Trent can only make changes in polarization. See text for details.

Another check of authentication is that Bob also knows that the sensible clear text he extracts must come from Alice, because if Mallory does not know *K* he cannot produce a cryptogram that when decrypted would produce anything readable.

C. Nonentanglement QKD protocol (iii)

Let us now present an even simpler protocol, which to some extent resembles [21] in that Trent determines the correlations between the bits sent by Alice and received by Bob. Let us modify assumptions (A) and (B) and (C) to the following: (A′) Trent can publicly (unjammably) broadcast to Alice and Bob the results of his actions. There also exists a jammable public channel between Alice and Bob.

The protocol is as follows, illustrated by Fig. 3:

(1) Alice sends Bob a string *S* of qubits encoded according to the BB84 protocol, i.e., for each bit sending either a $|z+\rangle$, $|z-\rangle$, $|x+\rangle$, or $|x-\rangle$ polarized photon.

(2) Trent sits midway between, and choose randomly between five sets (shifts qubits $|z+\rangle\rightarrow|z-\rangle$, $|z-\rangle\rightarrow|z+\rangle$, $|x+\rangle\rightarrow|x-\rangle$, $|x-\rangle\rightarrow|x+\rangle$ or does nothing). This is possible both in theory and in practice (using a polarization shifter). Note that Trent does not know what the bit value is, as he does not measure the polarizations, he only shifts them. If he had measured them, his actions would have been the same as those of an eavesdropper.

(3) Bob tells Alice a different set of bits, their position in the transmission, and the settings of the polarizers. This classical information is denoted *Y* in Fig. 3.

(4) Bob and Alice randomly alternate telling the settings of the polarizers for all the states received. This classical information is denoted *Y* in Fig. 3.

(5) Trent broadcasts (unjammably) to Alice and Bob whether or not he shifted the bits. Alternatively, we may

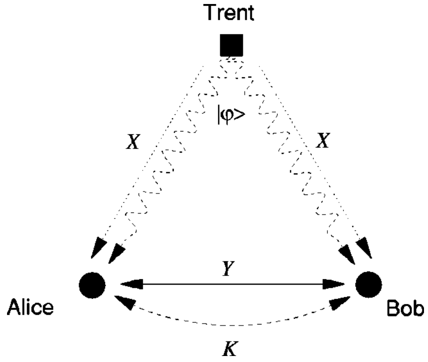

FIG. 4. Channel diagram for protocols (iv) and (v). The line types are defined as in the previous figures, with the addition of the entangled-state quantum channel illustrated with a wavy dashed line. See text for details.

suppose that the choice of states by Trent is secret information that the true Alice and Bob are given. This information is denoted X in Fig. 3.

(6) The above is done by first keeping only bits where the settings of the polarizers are correct.

If the data between Alice and Bob and the settings given from Trent agree, Bob and Alice have again authenticated each other via Trent. Let us stress the essential ingredient for authentication, namely, that Alice and Bob declare their bases and outcome for the test bits *before* Trent tells how the outcomes should be correlated. Note once again, that if Trent does not actively proceed with any eavesdropping on Alice and Bob's channel he will not know the authentication string, nor the key, K.

IV. ENTANGLEMENT-BASED QKD WITH USER AUTHENTICATION

Let us now show two protocols for authenticated key distribution based on entangled states. Whereas in [21], for each shared bit two entangled states are used, one for Alice and one for Bob, followed by an entanglement swapping measurement [22], in our protocol only one initial two-particle entangled state per shared bit is needed, which would make a substantial simplification in practice. In the present scheme, as illustrated in Fig. 4, Trent has a pool of entangled states. For each bit he wants to establish, he sends the first particle from the entangled state to Alice, and the other to Bob. Note that the present protocol uses some ideas from quantum secret sharing [27,28]. As in [21], using entanglement, Trent will only be required to broadcast extra information regarding which entangled states he sent in each case.

Before going into the protocols, let us reiterate some basic properties of entangled photon states. A two-photon entangled state, such as that generated from a type-II parametric down-conversion crystal [23], can be written as

$$|\psi\rangle=\frac{1}{\sqrt{2}}(|z+\rangle|z-\rangle+e^{i\alpha}|z-\rangle|z+\rangle), \tag{1}$$

where α is a birefringent phase shift of the crystal, and $|z+\rangle$ and $|z-\rangle$ denote the horizontal and vertical polarization eigenstates.

Using appropriate birefringent phase shifts and polarization conversions, one may easily convert the above state into any of the four Bell states;

$$|\phi^{\pm}\rangle=\frac{1}{\sqrt{2}}(|z+\rangle|z+\rangle\pm|z-\rangle|z-\rangle), \tag{2}$$

$$|\psi^{\pm}\rangle=\frac{1}{\sqrt{2}}(|z+\rangle|z-\rangle\pm|z-\rangle|z+\rangle). \tag{3}$$

Shifting between these states (actually among all four Bell states) has been demonstrated experimentally in Bell-state analysis [24]. (In the entanglement-based quantum cryptography scheme [6], however, one considers a passive version based on sending only one of the Bell states to Alice and Bob.)

Furthermore, let us define a new linear combination of Bell states as

$$\begin{aligned}|\Psi^{+}\rangle&\equiv\frac{1}{\sqrt{2}}(|\phi^{-}\rangle+|\psi^{+}\rangle)=\frac{1}{\sqrt{2}}(|z+\rangle|x+\rangle+|z-\rangle|x-\rangle)\\&=\frac{1}{\sqrt{2}}(|x+\rangle|z+\rangle+|x-\rangle|z-\rangle),\end{aligned} \tag{4}$$

$$\begin{aligned}|\Phi^{-}\rangle&\equiv\frac{1}{\sqrt{2}}(|\phi^{-}\rangle-|\psi^{+}\rangle)=\frac{1}{\sqrt{2}}(|z+\rangle|x-\rangle-|z-\rangle|x+\rangle)\\&=\frac{1}{\sqrt{2}}(|x+\rangle|z-\rangle-|x-\rangle|z+\rangle).\end{aligned} \tag{5}$$

Now the set of states $|\varphi\rangle\in\{|\psi^{+}\rangle,|\phi^{-}\rangle,|\Psi^{+}\rangle,|\Phi^{-}\rangle\}$ has the feature that $\langle\psi^{+}|\phi^{-}\rangle=\langle\Psi^{+}|\Phi^{-}\rangle=0$.

Furthermore, all states are not orthogonal, as $|\langle\psi^{+}|\Psi^{+}\rangle|^{2}=|\langle\psi^{+}|\Phi^{-}\rangle|^{2}=1/2$ and $|\langle\phi^{-}|\Psi^{+}\rangle|^{2}=|\langle\phi^{+}|\Phi^{-}\rangle|^{2}=1/2$. We will use this feature in the protocols below. The main idea is for Trent to pick states from a set of nonorthogonal base states and send them to Alice and Bob. Since the states are nonorthogonal, Mallory cannot intercept them and reliably measure their properties. A second feature we will use in the protocol is that Alice and Bob will first declare their information for authentication based on their respective measurements. After this, Trent will release which quantum state was sent, allowing Alice and Bob to cross check independently to see if the information released was correct. An impersonator like Mallory will not be able to release the correct information, and Alice and Bob will know that the public and/or quantum channel has been tampered with.

A. Four-state entanglement-based QKD with user authentication (iv)

Using two-particle quantum entanglement with Trent providing the states, we keep assumption (A′) on Trent. Let us

TABLE I. Correlation of measurement outcomes given that Trent has sent a certain two-particle entangled state.

Alice \ Bob	$z+$	$z-$	$x+$	$x-$
$z+$	ϕ^-	ψ^+	Ψ^+	Φ^-
$z-$	ψ^+	ϕ^-	Φ^-	Ψ^+
$x+$	Ψ^+	Φ^-	ψ^+	ϕ^-
$x-$	Φ^-	Ψ^+	ϕ^-	ψ^+

as starting states pick $|\phi^-\rangle$ and $|\psi^+\rangle$ as one base, and $|\Phi^-\rangle$ and $|\Psi^+\rangle$ as the other. The user authentication and key distribution scheme illustrated with Fig. 4 is as follows:

(1) Trent sends one of the entangled states $|\varphi\rangle \in \{|\psi^+\rangle, |\phi^-\rangle, |\Psi^+\rangle, |\Phi^-\rangle\}$, each with a probability of $\frac{1}{4}$. One photon from the entangled state is sent to Alice, and the other photon is sent to Bob. Alice and Bob measure the polarization of the incoming photon by switching randomly between the z base and the x base.

(2) Alice tells Bob a set of bits, their positions in the transmission, and the corresponding settings of the polarizers.

(3) Bob tells Alice a different set of bits, their positions in the transmission, and the corresponding settings of the polarizers.

(4) Bob and Alice randomly alternate telling the settings of the polarizers for all the states received.

(5) Trent broadcasts (unjammably) to Alice and Bob which of the entangled states he sent for all of the bits. Alternatively, we may suppose that the choice of states by Trent is secret information that the true Alice and Bob are given. This information is denoted by X.

(6) Alice and Bob sort their released data into four bins N_1 to N_4. In bin N_1, they place the states pertaining to if Trent sent a $|\psi^+\rangle$ state. In this case they know that their results should be anticorrelated in the z base and correlated in the x base. In bin N_2, they place the states pertaining to if Trent sent a $|\phi^-\rangle$ state. Their results should then be perfectly correlated when both are measured in the z base and anticorrelated when both are measured in the x base. In bin N_3 they place the results if Trent sent a $|\Psi^+\rangle$ state. In this case, if Bob and Alice measure in different bases, the results are correlated. Finally, in bin N_4, they place the results if Trent sent a $|\Phi^-\rangle$ state. For this state they know that the bits should be anticorrelated when Alice and Bob measure in different bases. All other cases they discard. In Table I we have summarized the correlation relations for different settings of Alice and Bob polarizers. This departure from correlation to anticorrelation gives Alice and Bob the unique signature from Trent, which allows them user authentication.

(7) Alice and Bob then check their bits according to the bins N_1 to N_4.

(8) The final step is to distribute the cryptokey K, which is done using the remaining secret bits from the bins N_1 to N_4 as before. This is done by first keeping only bits where the settings of the polarizers were the same. This exchanged information Y is shown in Fig. 4.

If the data between Alice and Bob and the settings given from Trent agree, Bob and Alice have again authenticated each other via Trent. Let us stress the two essential ingredients for authentication: first, the control of the sign of the correlation between the bits done by Trent, and second the fact that Alice and Bob declare their bases and outcome for the the test bits *before* Trent tells how the outcomes should be correlated. Note that, since we do the eavesdropping test using data from Trent, it is not necessary to use the encoding procedure in [6], where a test of the violation of a Bell inequality [26] is used to detect the eavesdropper. Consider the eavesdropper using a Bell analyzer to perform eavesdropping. If so, in half the cases he will make the right choice; in the other half he will not. On average, the eavesdropper will impair a 25% BER, as well as induce the same BER in the channel. To check the agreement with the data one may simply check that the BER is not above a critical value. Let us furthermore stress that, as Trent does not know the outcome of Alice and Bob's measurements, he knows neither the authentication string nor the secret key K established by Alice and Bob.

The data-sorting procedure used in the protocol is similar to the ''entangled entanglement'' studied by Krenn and Zeilinger [25] for three-particle entangled states (GHZ-states [29]), albeit here Trent does classical random selection of the states. One can also easily construct (on paper) a three-particle entangled version of the above protocol, in which the selection of the state sent by Trent is made purely random, contingent upon the outcome of the measurement of his particle from the three-particle entangled states.

B. Two-state entanglement-based QKD with user authentication (v)

Finally, let us show a simplified version of the four-state scheme, using only two nonorthogonal states. This scheme is in some respects, very similar to the two-state scheme Bennet 1992 (B92) [7]. In this case, Trent will again not know which is the authentication string, nor will he know the secret key bits.

The user authentication and key distribution scheme, as illustrated with Fig. 4, is as follows:

(1) Trent sends the entangled states $|\psi^+\rangle$ or $|\Psi^+\rangle$, each with the probability $\frac{1}{2}$ (remember these states are not orthogonal). Alice and Bob do measurements in the polarization by randomly switching between the z base and the x base.

(2) Alice tells Bob a set of bits, their position in the transmission, and the settings of the polarizers.

(3) Bob tells Alice a different set of bits, their position in the transmission, and the settings of the polarizers.

(4) Bob and Alice randomly alternate telling the settings of the polarizers for all the states received.

(5) Trent broadcasts which of the entangled states he sent for all of the bits.

(6) Alice and Bob sort their released data into two bins N_1 and N_2. In bin N_1, they place the states if Trent sent a $|\psi^+\rangle$ state. In this case they know that their results should be an-

ticorrelated in the z base and correlated in the x base. In bin N_2 they place the states if Trent sent $|\Psi^+\rangle$ state. In this case, if Bob and Alice measure in incompatible bases, the results are correlated.

(7) Alice and Bob then check their bits according to the bins N_1 and N_2.

(8) The final step is the distribution of the cryptokey itself, which is done using the remaining secret bits from the bins N_1 and N_2 as before. This is done by first keeping only bits where the settings of the polarizers were the same.

If the data between Alice and Bob and the settings given from Trent agree, Bob and Alice have again authenticated each other via Trent. If an eavesdropper listens in or is not in possession of any of the entangled states, he cannot reproduce the statistical correlations between the three persons. Furthermore, an eavesdropper cannot successfully (using a Bell-state measurement) distinguish the two states without ambiguity. If there are losses in the system, he may, however, succeed in eavesdropping as is the case for two-state quantum cryptography [7].

V. DISCUSSION

As for the general applicability of these schemes, they still assume the existence of an unjammable public channel at some instance (one way in some protocols, two ways in other). Alternatively, the protocols assume that some initial piece of secret information is available. Also with Trent this is inevitable. However, they do allow quantum key distribution on a jammable public channel between Alice and Bob, and they do increase the overall security by giving ''an extra handle'' in the correlations. We believe that the three main results–to send authentication information interleaved with the quantum key, to manipulate the Bell states used for the key generation, and to use a nonorthogonal state base similar to what is done in single-photon quantum cryptography—are all of interest for applications of user authentication in quantum cryptography. Entangled-state manipulation also has use in quantum secret sharing protocols [27,28]. An interesting question, that we just commented on briefly, is to what extent three-particle entangled states can be used for authentication, similar to the case of secret sharing [27]. As for the experimental feasibility of the above protocols, they would all be possible using present-day technology; optical Bell-state generation has been done by several groups, Bell-state manipulation has been demonstrated, and on the receiver side only single-photon detection will be required. Of course, the feasibility does not imply that the added technical complexity compared to attenuated coherent-state quantum cryptography using unjammable public channels will necessarily be justified.

ACKNOWLEDGMENTS

A. Karlsson would like to acknowledge Nobuyuki Imoto and Masato Koashi of NTT Basic Research Laboratories and Soken University for Graduate Studies, and Artur Ekert of Oxford University for useful discussions during the initial part of the work. This work was supported by the European IST FET QuComm project, the Swedish Natural Science Research Council (NFR), and the Swedish Technical Science Research Council (TFR).

[1] B. Schneier, *Applied Cryptography, Protocols, Algorithms and Source Code in C* (John Wiley and Sons, New York, 1996).
[2] D. R. Stinson, *Cryptography, Theory and Practice* (CRC, New York, 1995).
[3] M. N. Wegman and J. L. Carter, J. Comput. Syst. Sci. **22**, 265 (1981).
[4] A. Fiat and A. Shamir, in *Advances in Cryptology: Proceedings of Crypto 86*, edited by A. M. Odlyzko (Springer-Verlag, New York, 1987), pp. 186–194.
[5] C. H. Bennett, G. Brassard, and J. Smolin, J. Cryptology **5**, 3 (1992).
[6] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[7] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[8] H. Zbinden, H. Bechmann-Pasquinucci, N. Gisin, and G. Ribordy, Appl. Phys. B: Lasers Opt. **67**, 743 (1998).
[9] M. Bourennane, D. Ljunggren, A. Karlsson, Per Jonsson, A. Hening, and J. P. Ciscar, J. Mod. Opt. **47**, 563 (2000).
[10] N. Lütkenhaus, Phys. Rev. A **54**, 97 (1996).
[11] N. Lütkenhaus, Phys. Rev. A **59**, 3301 (1999).
[12] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Los Alamos e-print quant-ph/9911054.
[13] C. Crépeau and L. Salvail in *Advances in Cryptology: Proceedings of Eurocrypt '95*, edited by L. C. Guillon and J. J. Quisquater (Springer-Verlag, New York, 1995), p. 133–14.
[14] B. Huttner, N. Imoto, and S. Barnett, J. Nonlinear Opt. Phys. Mater. **5**, 823 (1996).
[15] H. K. Lo and H. F. Chau, Phys. Rev. Lett. **78**, 3410 (1997).
[16] D. Mayers, Phys. Rev. Lett. **78**, 3414 (1997).
[17] M. Dusek, O. Haderka, M. Henrych, and R. Myska, Phys. Rev. A **60**, 149 (1999).
[18] H. Barnum, Los Alamos e-print quant-ph/9910072.
[19] D. Jonathan and M. Plenio, Phys. Rev. Lett. **83**, 3566 (1999).
[20] M. Nielsen, Phys. Rev. Lett. **83**, 436 (1999).
[21] G. Zeng and W. Zhang, Phys. Rev. A **61**, 022303 (2000).
[22] J. W. Pan, D. Bouwmeester, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **80**, 3891 (1998).
[23] P. G. Kwiat, K. Mattle, H. Weinfurther, and A. Zeilinger, Phys. Rev. Lett. **75**, 4337 (1995).
[24] M. Michler, K. Mattle, M. Eible, H. Weinfurther, and A. Zeilinger, Phys. Rev. A **53**, R1209 (1996).
[25] G. Krenn and A. Zeilinger, Phys. Rev. A **54**, 1793 (1996).
[26] J. S. Bell, Physics (Long Island City, N.Y.) **1**, 195 (1964).
[27] M. Hillary, V. Buzek, and A. Bertaiume, Phys. Rev. A **59**, 1829 (1999).
[28] A. Karlsson, M. Koashi, and N. Imoto, Phys. Rev. A **59**, 162 (1999).
[29] D. M. Greenberger, M. A. Horne, A. Shimony, and A. Zeilinger, Am. J. Phys. **58**, 1131 (1990).