Quantum entanglement for secret sharing and secret splitting

Anders Karlsson,* Masato Koashi, and Nobuyuki Imoto
NTT Basic Research Laboratories, 3-1 Morinosato, Atsugi-shi, Kanagawa 243-0198, Japan

(Received 28 July 1998)

We show how a quantum secret sharing protocol, similar to that of Hillery, Buzek, and Berthiaume (Los Alamos e-print archive quant-ph/9806063), can be implemented using two-particle quantum entanglement, as available experimentally today. We also discuss in some detail how both two- and three-particle protocols must be carefully designed in order to detect eavesdropping or a dishonest participant. We also discuss the extension of a multiparticle entanglement secret sharing and splitting scheme toward a protocol so that m of n persons with $m \leqslant n$ can retrieve the secret. [S1050-2947(99)09301-4]

PACS number(s): 03.67.−a, 03.65.Bz, 42.50.Dv

I. INTRODUCTION

Quantum mechanics provides novel features to information processing, extending the capabilities beyond those possible using classical physics only. The most prominent examples to date have been quantum computation [1,2], quantum teleportation [3–5], and quantum cryptography [6], with the latter being most mature experimentally. For cryptographic applications, there has been much concern about whether quantum methods can be used only for secret key exchange, or if it is useful also for other purposes, such as authentication. However, recent proofs showing quantum bit commitment not to be unconditionally secure [7,8] have been somewhat of a setback for an extension of quantum cryptography toward such applications.

Recently, Hillery, Buzek, and Berthiaume [9] introduced a protocol of *quantum secret sharing*, which is a quantum-mechanical version of classical secret sharing schemes [10,11]. The basic idea of secret sharing in the simplest case is that a secret is shared between two persons, say Alice and Bob, in such a way that it can only be reconstructed if both collaborate. In a more general setting, notably for secure key management, an *m-out-of-n* protocol [or (m,n)-threshold scheme] with $1 \leqslant m \leqslant n$ spreads a secret to n participants in a way that any m participants can reconstruct it. The interesting aspect of exploring quantum mechanics for secret sharing is that it allows for the unconditionally secure distribution of the information to the participants. The scheme presented in Ref. [9] is based on a three-particle entangled Greenberger-Horne-Zeilinger state [12]. The main purpose of the present paper is to show that it is also possible to construct secret sharing protocol similar to that in Ref. [9] using two-particle quantum entanglement. We also present a detailed discussion of how to detect eavesdropping, or how to detect a dishonest party in the protocols. Specifically, we discuss the importance of the order in which the participants release the data to test for the presence of an eavesdropper. Furthermore, we discuss how a first step toward a possible *m-out-of-n* protocol for secret sharing and splitting can be realized by a combination of m-particle entanglement and entanglement swapping [13–15].

However, it should be remembered, as it was indeed stressed in Ref. [9], that for practical purposes conventional quantum cryptography followed by classical secret sharing can also be used to achieve secret sharing in a very simple manner. That is, the sender Trent sends one string R to Alice and a second string S to Bob, and then Trent encodes the secret message using a key K generated by the exclusive-OR (XOR), $K=R \oplus S$. Only if Alice and Bob collaborate can they find out the message. However, the principal advantage of the two-particle scheme is that for a given length of the secret key, fewer bits are needed to be sent in order to assure the nonpresence of the eavesdropper.

The paper is outlined as follows: First, in Sec. II, we review the preparation of two-particle maximally entangled states, the so-called Bell states. In Sec. III, we discuss secret sharing. In Sec. III A, we present the two-particle entanglement secret sharing protocol. In Sec. III B, we discuss the issue of eavesdropping. In Sec. IV, we discuss the extension of the splitting scheme of Ref. [9]. In Sec. IV A we briefly review their scheme for secret sharing, in Sec. IV B we briefly discuss eavesdropping considerations, in Sec. IV C we review their scheme for secret splitting, and in Sec. IV D we discuss a possible extension using entanglement swapping. Finally, in Sec. V, we discuss the obtained results.

II. TWO-PARTICLE ENTANGLEMENT AND BELL STATES

Let us begin with a brief review of two-particle polarization entanglement. The state generated from a type-II parametric down-conversion crystal can be written as [16]

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|z+\rangle_A|z-\rangle_B + e^{i\alpha}|z-\rangle_A|z+\rangle_B), \qquad (2.1)$$

where α is a birefringent phase shift of the crystal, and $|z+\rangle$ and $|z-\rangle$ denote the spin eigenstates, or equivalently the horizontal and vertical polarization eigenstates, and subscripts A and B denote the two particles (for Alice and Bob).

Using appropriate birefringent phase shifts and polarization conversion, one may easily convert the above state into any of the four Bell states [16]

*Permanent address: Department of Electronics, Royal Institute of Technology, Electrum 229, S 164 40 Kista, Sweden. Electronic address: andkar@ele.kth.se

$$|\phi^{\pm}\rangle=\frac{1}{\sqrt{2}}(|z+\rangle_A|z+\rangle_B\pm|z-\rangle_A|z-\rangle_B) \tag{2.2}$$

and

$$|\psi^{\pm}\rangle=\frac{1}{\sqrt{2}}(|z+\rangle_A|z-\rangle_B\pm|z-\rangle_A|z+\rangle_B). \tag{2.3}$$

Experimentally shifting between these states has been demonstrated in Bell-state analysis [17]. As written above, the states are expressed in a z direction base $\{|z+\rangle,|z-\rangle\}$. Defining the x-spin eigenstates as

$$|x+\rangle=\frac{1}{\sqrt{2}}(|z+\rangle+|z-\rangle),\quad |x-\rangle=\frac{1}{\sqrt{2}}(|z+\rangle-|z-\rangle), \tag{2.4}$$

we may rewrite the Bell states in this basis as

$$\begin{aligned}
|\phi^{+}\rangle&=\frac{1}{\sqrt{2}}(|x+\rangle_A|x+\rangle_B+|x-\rangle_A|x-\rangle_B),\\
|\phi^{-}\rangle&=\frac{1}{\sqrt{2}}(|x+\rangle_A|x-\rangle_B+|x-\rangle_A|x+\rangle_B),\\
|\psi^{+}\rangle&=\frac{1}{\sqrt{2}}(|x+\rangle_A|x+\rangle_B-|x-\rangle_A|x-\rangle_B),\\
|\psi^{-}\rangle&=\frac{1}{\sqrt{2}}(|x-\rangle_A|x+\rangle_B-|x+\rangle_A|x-\rangle_B).
\end{aligned} \tag{2.5}$$

As should be noted, for example, the $|\phi^{+}\rangle$ states give correlated results in both the z and x bases, however, the $|\phi^{-}\rangle$ states give correlated results in the z basis, but anticorrelated results in the x basis.

The feature we wish to explore in the quantum secret sharing protocol is the detection properties in two nonorthogonal basis sets. Let us therefore define a linear combination of Bell states as

$$\begin{aligned}
|\Psi^{+}\rangle&\equiv\frac{1}{\sqrt{2}}(|\phi^{-}\rangle+|\psi^{+}\rangle)\\
&=\frac{1}{\sqrt{2}}(|z+\rangle_A|x+\rangle_B+|z-\rangle_A|x-\rangle_A)\\
&=\frac{1}{\sqrt{2}}(|x+\rangle_A|z+\rangle_B+|x-\rangle_A|z-\rangle_B)
\end{aligned} \tag{2.6}$$

and

$$\begin{aligned}
|\Phi^{-}\rangle&\equiv\frac{1}{\sqrt{2}}(|\phi^{-}\rangle-|\psi^{+}\rangle)\\
&=\frac{1}{\sqrt{2}}(|z+\rangle_A|x-\rangle_B-|z-\rangle_A|x+\rangle_B)\\
&=\frac{1}{\sqrt{2}}(|x+\rangle_A|z-\rangle_B-|x-\rangle_A|z+\rangle_B).
\end{aligned} \tag{2.7}$$

Now, the set of states $\{\psi^{+},\phi^{-},\Psi^{+},\Phi^{-}\}$ has the desired feature that $\langle\psi^{+}|\phi^{-}\rangle=\langle\Psi^{+}|\Phi^{-}\rangle=0$, which, as we will see below, allows for a simple encoding of the information to be shared. Furthermore, the states from the two different sets are nonorthogonal, as $|\langle\psi^{+}|\Psi^{+}\rangle|^2=|\langle\psi^{+}|\Phi^{-}\rangle|^2=\frac{1}{2}$ and $|\langle\phi^{-}|\Psi^{+}\rangle|^2=|\langle\phi^{+}|\Phi^{-}\rangle|^2=\frac{1}{2}$. This is the crucial feature that enables the detection of an eavesdropper in the two-particle entanglement-based protocol presented below.

III. ONE- TO TWO-PARTY SECRET SHARING

As discussed in Sec. I, in secret sharing, information is sent from a sender Trent, to multiple participants (here two, Alice and Bob), so that both need to collaborate to have the information. In this section we present a two-particle quantum entanglement protocol for secret sharing.

A. Two-particle quantum entanglement secret sharing protocol

Let us now present our protocol for the secret sharing to two persons. In a naïve protocol Trent, the sender, encodes a random binary bit string S, selecting for instance the states $\{|0\rangle,|1\rangle\}\Leftrightarrow\{|\psi^{+}\rangle,|\phi^{-}\rangle\}$. Each of the participants Alice and Bob receives one of the particles (say photons), and then randomly makes a measurement either in the z or x basis. They then publicly discuss the results, with Trent listening, and keep only the results where their measurement bases (directions) coincided. When they later compare their data, they can use the correlation properties of the Bell states above as a lockup table to reconstruct from the correlation which one of the two states was sent. However, this naïve version can easily be cracked by a dishonest party. An eavesdropper Eve or dishonest receiver Bob*, who tries to find out the secret all by himself, may simply capture both particles, perform a measurement of the Bell states using a Bell state analyzer [17] and then regenerate the corresponding Bell state and send further to Alice and Bob. Let us emphasize that since only two Bell states are used in this naïve scheme, eavesdropping would be possible using interferometric Bell state analyzers [17], which can separate two Bell states with certainty, and give a different answer for the two other Bell states. The problem with the naïve scheme can be traced back to the fact that the Bell states are orthogonal, and hence can in principle be measured without disturbance.

Let us therefore present a more elaborate version, in which Trent switches randomly between two sets of states, similar to four-state quantum cryptography [6], also drawing ideas from quantum communication using Einstein-Podolsky-Rosen (EPR) pairs [18]. Now Trent proceeds in a

TABLE I. Correlation between outcomes for Alice and Bob, allowing them to decide jointly which state was sent by Trent, given that they know the choice of basis made by Trent.

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^+

fashion similar to the case of four-state quantum cryptography. To this end he makes use first of the set of states $\{|\psi^+\rangle,|\phi^-\rangle\}$, and also the states $|\Psi^+\rangle$ and $|\Phi^-\rangle$ defined above. In this case, as will be seen below, even a perfect Bell analyzer which can separate all four Bell states cannot be used for eavesdropping. The protocol goes as follows.

(1) Trent sends information as $\{|0\rangle,|1\rangle\}\Leftrightarrow\{|\psi^+\rangle,|\phi^-\rangle\}$ and $\{|0'\rangle,|1'\rangle\}\Leftrightarrow\{|\Psi^+\rangle,|\Phi^-\rangle\}$. Alice and Bob detect the states, either in the z or x basis. Note that these measurements are *local*, each made on one particle only.

(2) Alice and Bob then have a public discussion where they declare the measurement outcomes for a set of bits used for a test of the eavesdropping. After this has been done, they also declare the measurement bases that were used for the test bits and the secretly shared bits. This should be done in a way that, for the test bits, the person who declared the outcome first should be the last to declare the basis; the reason for this will be explained below. As we will show below, in order to stop an eavesdropper, or a dishonest party, it is essential that a set of bits are released for test *before* the bases are declared. Naturally, the set of bits used for the eavesdropping test should be decided by both parties, and not by one party alone.

(3) After some bits (measurement outcomes and bases) have been released, Trent reveals to them which of the two bases the state was sent, but not which state. Also, Trent tells which state was sent for the test bits. In half of all cases, Alice and Bob must discard their results, but in the other half they have useful results, as described in Table I, which shows the joint correlation properties of the outcomes for measurements made by Alice and Bob, given that a certain state was sent by Trent.

When this has been done, Alice and Bob can independently make a test for the presence of an eavesdropper, or test whether one of them is dishonest. As will be shown below, an eavesdropper, or a dishonest party (say Bob) trying to find out the shared key without Alice and Trent knowing it, will introduce a 25% error rate in the bits. If the test shows no errors, however, they can construct the secret sharing key from the rest of the bits where only Trent's basis was released, as can be inferred from Table I. However, neither of them alone may determine if $|\psi^+\rangle$ or $|\phi^-\rangle$ was sent in the first basis set, or if $|\Psi^+\rangle$ or $|\Phi^-\rangle$ was sent in a second basis set. Hence, in order to know which bit value was sent by Trent, they must collaborate.

B. Security against eavesdropping

The present secret sharing scheme is secure against eavesdropping in a manner similar to that in four-state quantum cryptography [6]. To see this in a sufficient way, we will consider two possible cases. The first involves an honest Alice and Bob, and a third eavesdropper. The second case concerns a situation in which one of the involved parties, say Bob (or Bob*), is dishonest and tries to find the secret key by himself, without collaborating with Alice in the final stage.

TABLE II. Eavesdropping attempt and the state sent further.

Trent sends	Eve observes	Eve sends
ψ^+	ψ^+	ψ^+
ϕ^-	ϕ^-	ϕ^-
Ψ^+	ψ^+ or ϕ^-	ψ^+ or ϕ^- ?
Φ^-	ψ^+ or ϕ^-	ψ^+ or ϕ^- ?

1. Intercept and resend by Eve

Suppose the eavesdropper, by convention denoted by Eve, is in possession of a Bell state analyzer for the Bell states as defined above. If so, she will be able to distinguish $|\psi^+\rangle$ or $|\phi^-\rangle$ when Trent sends either of the two. However, in the conjugate basis she has a random outcome. Suppose the eavesdropping strategy is to resend the Bell state according to the result of his Bell state analysis. In Table II, we summarize the outcomes using this strategy. In order to detect the eavesdropper, we should consider what happens if, for instance, the state $|\Psi^+\rangle$ is sent by Trent. In half the cases Eve chooses the right basis, and resends the Bell state perfectly. In the other half of the cases Eve chooses the wrong basis and either sends $|\psi^+\rangle$ or $|\phi^-\rangle$. These states will be correctly detected by Alice and Bob in half the cases. Adding up the probability of causing an error becomes $1/2\times(1/2\times1/2+1/2\times1/2)=1/4$, which is the same as for four-state cryptography. In a manner similar to the four-state cryptography, it is also possible to do a more complex eavesdropping using an ancilla, or measuring in an intermediate basis compared to the $\{0,1\}$ and $\{0',1'\}$ bases. However, the eavesdropper is still detectable, and the fundamental security remains.

2. A dishonest Bob when the bases are declared first*

A more serious threat is that of a dishonest Bob (Bob*), mentioned briefly earlier. Bob* seeks to learn the full information himself, while fooling Alice and Trent into believing that he is not in possession of the full information. In conventional quantum cryptography, the eavesdropper is outside the original protocol, and tries to monitor and learn the key without being detected. Here Bob* is an insider, who participates in the protocol, and who tries to use it to his own advantage. We show that this implies that one must design the protocol carefully, and choose the right order of releasing the public information. For instance, naïvely, if Bob* would be allowed to choose for himself which bits are used for the test of eavesdropping, then for those bits he may simply follow the original protocol, and introduce no error rate at all. If, however, he is not allowed to choose which bits Alice will disclose first, he must use a more sophisticated strategy.

Let us here first analyze the case for a ''careless'' protocol, which is different from the protocol in Sec. III A only in that the measurement bases are released first, followed by the measurement outcome of the bits used for the eavesdropping test. The strategy for Bob* is to capture the original state and send a fake state, say $|\phi^-\rangle$ to Alice. He then tries to reproduce the true correlations by using the information leaked in the public discussion. Let us go through Bobs*'s strategy in detail. When Trent sends the state, Bob* simply captures the original state and stores it. He then sends one particle from the fake state $|\phi^-\rangle$ to Alice. When Alice tells which basis she measured, he measures the other particle of $|\phi^-\rangle$ in the same basis, and from this he knows exactly the outcome of Alice's measurement. This is a crucial point. Next Bob* makes the measurement on the original state, choosing for Alice's original particle the same basis as Alice did. For his particle, he will follow the original protocol and measure in a randomly chosen basis. Now, for basis choices that will agree with that sent by Trent, Bob* can use the measurement outcomes from his measurements on the original state and his knowledge of Alice's outcome, to tell Alice and Trent a measurement outcome that agrees both with the state sent by Trent and with the outcome observed on the fake particle received by Alice. To illustrate, if Bob* makes measurements compatible with states from the set $\{|\phi^-\rangle,|\psi^+\rangle\}$, then infers that the state $|\phi^-\rangle$ was sent, he will tell Alice that he observed the same outcome as she did. If he infers that $|\psi^+\rangle$ was sent by Trent, he will reveal the opposite outcome to that observed by Alice. A similar argument holds for the $\{|\Psi^+\rangle,|\Phi^-\rangle\}$ basis. If Bob*'s basis choice does not agree with the basis chosen by Trent, the bit is discarded anyway. Using this strategy, Bob* is able to exactly reproduce the correlation that Alice and Trent expect. It does not matter if Alice or Bob* declare their test bits first.

3. A dishonest Bob when the measurement outcomes are declared first, followed by the measurement basis*

Let us now show that the procedure introduced in Sec. III A is indeed secure, namely, first releasing the measurement outcome, then the basis, in the order such that the person who declared the outcome first should be the last to declare the basis used for the measurement. The reason this works is that, in contrast to the case in Sec. III B 2, Bob* cannot exactly deduce Alice's basis from her declaration of her outcome, even if he uses an entangled fake state. As a result of this, he will then sometimes declare an outcome which is incompatible with the state prepared by Trent. Further, in order to ensure that this incompatibility is actually tested, the order of releasing information must be chosen carefully. There are four cases to be studied: (1) Alice reveals the outcome followed by Bob, then Alice reveals the basis followed by Bob; (2) Alice reveals the outcome followed by Bob, then Bob reveals the basis followed by Alice; (3) Bob reveals the outcome followed by Alice, then Alice reveals the basis followed by Bob; and finally (4) Bob reveals the outcome followed by Alice, then Bob reveals the basis followed by Alice. Let us now show why (2) and (3) are good procedures, but (1) and (4) are not.

Let us first see what will happen in case (1). Suppose that Bob* has intercepted the original particle. In this case, Bob* is not helped by sending the entangled fake state $|\phi^-\rangle$ used earlier. This is simply because he cannot tell from Alice's and his outcome alone which was the basis used by Alice. So, in principle, he can send an arbitrary ''dummy'' particle to Alice.

Bob* then measures in the x basis on his original particle, and in the z basis on Alice's original particle. Suppose now that Trent sent a state from the $\{|\Psi^+\rangle,|\Phi^-\rangle\}$ set of states. If he obtains the outcomes corresponding to the $|\Psi^+\rangle$ state he declares the same outcome as Alice, but the opposite basis. If he obtains outcomes corresponding to the $|\Phi^-\rangle$ state, he declares the opposite outcome as Alice and the opposite basis (see Table I). A cheating Bob* can thus obtain information on the states sent in the $\{|\Psi^+\rangle,|\Phi^-\rangle\}$ basis without causing any errors. The cases when Trent sent in the $\{|\psi^+\rangle,|\phi^-\rangle\}$ basis are automatically discarded because Bob* always declares the basis opposite to Alice's.

It should be noted that this cheating strategy cannot be applied to steal information about states sent in the $\{|\psi^+\rangle,|\phi^-\rangle\}$ basis. This is because Bob* cannot determine whether the outcomes should be correlated or anticorrelated, even if he knows which one of the states $|\psi^+\rangle$ and $|\phi^-\rangle$ was sent by Trent (see Table I). This asymmetry means that too much use of the above strategy leads to a detectable correlation between Alice's and Bob's choice of basis. But a small number of bits can still be successfully cheated, so protocol (1) should be avoided.

Let us then consider case (2), where Bob releases his basis first. In this protocol, Bob* cannot use the above strategy. This is because he will sometimes release a basis which is the same as that of Alice, when Trent also sent a valid state for that basis (i.e., $|\psi^+\rangle$ or $|\phi^-\rangle$). In this case, the combination of outcomes released by Alice and Bob* does not necessarily correspond to the state sent by Trent, so that the cheating should be detected. It can be shown that this order of releasing the outcomes and the basis also prevents a cheating Alice (Alice*) from obtaining the state without introducing errors in the protocol. This is because Alice* must release her outcome first, so she cannot control whether the outcomes should be correlated or anticorrelated for the valid choice of measurement bases used. Hence the order of releasing information in (2) can be seen to be a good one.

Now, since we see that case (1) is vulnerable to Bob*, and case (2) is secure against Alice* and Bob*, the symmetry between Alice and Bob shows that case (3) is secure and case (4) is vulnerable to Alice*. It should now be clear why only orders (2) and (3) should be used.

To conclude this somewhat lengthy discussion of eavesdropping, we have shown the importance of choosing a correct order of releasing the bits used for the test for eavesdropping, or the test of a dishonest party in the protocol. As stated initially, we believe the root of this need to be careful stems from the fact that the cheating party is an insider to the protocol.

IV. QUANTUM SECRET SHARING AND SPLITTING WITH THREE-PARTICLE ENTANGLED STATES

In this section, we discuss how three-particle entanglement can be used for secret sharing, as was first shown in Ref. [9]. Next we introduce the concept of secret splitting of quantum information, first by briefly reviewing the scheme in Ref. [9], followed by some brief comments on the generation of the initial state for the secret splitting. Finally, we

TABLE III. Correlation between outcomes for Alice and Bob, allowing them to decide jointly which outcome was observed by Trent, given that they know the choice of measurement basis (x or y direction) made by Trent.

Alice/Bob	$x+$	$x-$	$y+$	$y-$
$x+$	$x+$	$x-$	$y-$	$y+$
$x-$	$x-$	$x+$	$y+$	$y-$
$y+$	$y-$	$y+$	$x-$	$x+$
$y-$	$y+$	$y-$	$x+$	$x-$

show how the secret splitting protocol of Ref. [9] can possibly be extended using entanglement swapping [13,14].

A. A brief review of secret sharing with GHZ states

Suppose Trent, Alice, and Bob share one particle each from a three-particle entangled Greenberger-Horne-Zeilinger (GHZ) state [12],

$$|\psi_{\mathrm{GHZ}}\rangle=\frac{1}{\sqrt{2}}(|z+\rangle_T|z+\rangle_A|z+\rangle_B+|z-\rangle_T|z-\rangle_A|z-\rangle_B),\tag{4.1}$$

where the first particle is that of Trent, the second that of Alice, and the third that of Bob [in Ref. [9] the parties (Trent, Alice, Bob) were denoted (Alice, Bob, Charlie), but here we stick to the common notation of denoting the sender in secret sharing by Trent]. Now they then make random measurements, either in the x or y direction, where the x eigenstates were defined above, and the y eigenstates are defined as

$$|y+\rangle=\frac{1}{\sqrt{2}}(|z+\rangle+i|z-\rangle),\quad |y-\rangle=\frac{1}{\sqrt{2}}(|z+\rangle-i|z-\rangle).\tag{4.2}$$

Now, by reexpressing the GHZ state in the x and y eigenstates, as shown in Ref. [9], Alice and Bob can construct a lock-up table that allows them jointly, but only jointly, to determine which was the measurement outcome of Trent. Table III is the analog of Table I introduced earlier for the two-particle entanglement. As seen from Table III, Alice or Bob alone cannot determine which measurement outcome was observed by Trent, even if they know in which basis (direction) he measured.

1. A comment on eavesdropping in the GHZ-state secret sharing

As discussed in Ref. [9], this GHZ-state protocol is in principle secure against eavesdropping, and may also be generalized to involve more than two parties. Let us emphasize here that the order of declaring the test bit is also crucial in the GHZ-state secret sharing protocol. This was not explicitly stressed in Ref. [9], although it may have been implicitly assumed. To see why the order is important, suppose Bob* uses the following strategy for finding out what was the outcome of Trent (without letting Alice and Trent know that he is cheating). When Trent sends the two particles of the GHZ state to Alice and Bob*, he catches Alice's particle as well as his own. He then sends a fake state $|\phi^-\rangle$ to Alice. When Alice declares her measurement basis to Trent and Bob*, Bob* measures his particle from the fake state according to Alice's choice of basis. He then knows Alice's outcome as well. Next he follows the original protocol for the true state, measuring in the same basis as Alice on her original particle. Suppose Alice and Bob measured in the x direction, and that Alice obtained $x+$. Bob* hears from Alice that she used the x basis, and then measures on the fake state to find out Alice's outcome. If Bob* obtains a correlated result for the original particles, he will know that for the valid settings Trent obtained $x+$ as well; see Table III. He also declares to Trent and Alice that he obtained $x+$. If he instead obtained anticorrelated results, he would know that Trent observed $x-$, and that he should declare $x-$ as well. The remedy against this eavesdropping attack is that Alice and Bob release the outcomes for the test bits for eavesdropping before they release the directions of their measurements. It can then be shown in a similar manner to that of the two-particle entanglement scheme that a dishonest party will introduce errors in the data, allowing for his detection.

B. A brief review of secret splitting with GHZ states

In Ref. [9], quantum key sharing was also extended to quantum information splitting by teleportation, which one of us also recently studied in the context of teleportation to two parties [19]. The basic idea is as follows: Trent has a qubit $|Q\rangle=(a|z+\rangle+b|z-\rangle)$, which he wants to send to either Alice or Bob (both cannot generally have it as that would violate ''no-cloning'' theorems). This may be done using a teleportation procedure, whereby Trent, Alice, and Bob initially share a GHZ state. Next Trent makes a joint Bell-state measurement [17] on the state $|Q\rangle$ and his particle of the GHZ state. By communicating the outcome (two bits) to Alice and Bob, their joint state can be rotated to the split state $|Q\rangle_{s2}=a|z_1+,z_2+\rangle+b|z_1-,z_2-\rangle$; here the notation is that of Alice having the first particle and Bob the second particle. From this state, Alice may, for instance, retrieve $|Q\rangle$ if Bob does a measurement in the x basis, and communicates (one bit) which outcome ($x+$ or $x-$) he obtained. However, as stressed in Refs. [9,19], if both receivers do not collaborate, each one may still obtain the same amount of information as that of a single von Neumann measurement [20], i.e., the measurement will give that the state at least has a component along a given axis. This is different from the classical case, where no information should be available for the dishonest parties.

It should also be emphasized that the teleportation method is not the only way to achieve the quantum information splitting. By using quantum-controlled-NOT gates [21], the quantum information in a qubit can also trivially be split to several parties, e.g., for instance to three parties $|Q\rangle_{s3}=a|z_1+,z_2+,z_3+\rangle+b|z_1-,z_2-,z_3-\rangle$, by the successive operation of two quantum-controlled-NOT gates.

C. An *m-out-of-n* secret splitting protocol using entanglement swapping

Let us now show how the quantum splitting scheme can be extended to a initial version of an *m-out-of-n*-protocol, or a so-called (m,n) threshold scheme. The basic idea is that a secret is divided into n pieces or shares; though in such a way that any m group of shares can be used to reconstruct the secret. In the context of quantum secret splitting, that would correspond to spreading a quantum bit to n parties in such a way that any m parties could reconstruct it. If implementable, this feature probably could find some use for providing redundancy in quantum computation. The protocol may, also in analogy with Ref. [9], be used for the secret sharing of classical information.

We have not yet realized this full goal of quantum secret splitting, namely, the splitting of a qubit to n participants in a symmetric quantum state so that any m participants together can retrieve the original qubit. However, let us here describe a partial goal. Suppose a qubit $|Q\rangle=(a|z+\rangle+b|z-\rangle)$ is split among m ''executives'' so they each possess one particle from the entangled state

$$|\mathrm{QSS}\rangle=a|z_1+,\ \dots\ ,z_m+\rangle+b|z_1-,\ \dots\ ,z_m-\rangle. \tag{4.3}$$

Now, as shown previously, all m persons are needed if the original quantum bit is to be reconstructed at (any) one of the locations. As discussed above, in the absence of any one of the persons, only the amplitude information of the state is available [9,19]. However, before leaving, the ''executive'' should be requested to transfer his entanglement to a ''subordinate'' using entanglement swapping [13,14], demonstrated experimentally recently [15]. Suppose the joint state of the executives $|\mathrm{QSS}\rangle$ and the subordinate $|\mathrm{SO}\rangle=|z+\rangle_{\mathrm{SO}}$ is

$$\begin{aligned}|\mathrm{QSS}\rangle\otimes|\mathrm{SO}\rangle=&(a|z_1+,\ \dots\ ,z_m+\rangle\\&+b|z_1-,\ \dots\ ,z_m-\rangle)\otimes|z+\rangle_{\mathrm{SO}}.\end{aligned} \tag{4.4}$$

Generally, the entanglement swapping between two particles from two maximally entangled states requires a Bell-state measurement, as implementable with a quantum-controlled-NOT gate $\hat{C}_{\mathrm{not}}$, a Hadamard transformation $\hat{H}_a$, and a two-particle measurement [14]. The operation of the quantum-controlled-NOT gate is that it takes a two qubit input and flips the second qubit ($|z+\rangle\rightarrow|z-\rangle$ and $|z-\rangle\rightarrow|z+\rangle$) only if the first qubit is $|z-\rangle$. The (one bit) Hadamard gate transforms the input as $|z+\rangle\rightarrow(|z+\rangle+|z-\rangle)/\sqrt{2}$ and $|z-\rangle\rightarrow(|z+\rangle-|z-\rangle)/\sqrt{2}$. Let us here, however, first show the simple swapping of the state of the last particle in the $|\mathrm{QSS}\rangle$ state, and the $|\mathrm{SO}\rangle$ state. Applying a quantum-controlled-NOT gate, followed by the Hadamard transformation, gives

$$\begin{aligned}\hat{H}_a\hat{C}_{\mathrm{not}}|\mathrm{QSS}\rangle\otimes|\mathrm{SO}\rangle=&\hat{H}_a(a|z_1+,\ \dots\ ,z_m+\rangle\otimes|z+\rangle_{\mathrm{SO}}\\&+b|z_1-,\ \dots\ ,z_m-\rangle\otimes|z-\rangle_{\mathrm{SO}})\\=&(a|z_1+,\ \dots\ ,z_m+\rangle\otimes|z+\rangle_{\mathrm{SO}}\\&+b|z_1-,\ \dots\ ,z_m+\rangle\otimes|z-\rangle_{\mathrm{SO}})/\sqrt{2}\\&+(a|z_1+,\ \dots\ ,z_m-\rangle\otimes|z+\rangle_{\mathrm{SO}}\\&-b|z_1-,\ \dots\ ,z_m-\rangle\otimes|z-\rangle_{\mathrm{SO}})/\sqrt{2}.\end{aligned} \tag{4.5}$$

If we now make a measurement of the state of the last particle in the z basis, we project the remaining m particles into the desired swapped state. Suppose we obtain $z+$, the remaining state becomes

$$\begin{aligned}|\mathrm{QSS}\rangle_{\mathrm{swap}}=&(a|z_1+,\ \dots\ ,z_{m-1}+\rangle\otimes|z+\rangle_{\mathrm{SO}}\\&+b|z_1-,\ \dots\ ,z_{m-1}+\rangle\otimes|z-\rangle_{\mathrm{SO}}).\end{aligned} \tag{4.6}$$

Now this procedure would require both the particle to disentangle (from the executive) and the subordinate to be input to the quantum gate network, so, in this case, one may simply relabel the particles instead. Let us therefore present a more useful scenario. In this case, each subordinate is in possession of a two-particle maximally entangled state $|\mathrm{SO2}\rangle=(|z_a+,z_b+\rangle_{\mathrm{SO}}+|z_a-,z_b-\rangle_{\mathrm{SO}})/\sqrt{2}$. From this state one particle is left at a ''swapping center,'' and the second particle is kept by the subordinate. With n-m subordinates having left one entangled particle, there are altogether n persons that may help in retrieving the qubit. Now, to make the swapping, the executive goes to the swapping center and makes a joint Bell measurement on his particle and the one particle left by the subordinate at the swapping center. The state following the controlled-NOT and Hadamard gates can be written

$$\begin{aligned}\hat{H}_a\hat{C}_{\mathrm{not}}|\mathrm{QSS}\rangle\otimes|\mathrm{SO2}\rangle=\cdots&(a|z_1+,\ \dots\ ,z_m+\rangle\otimes|z_a+,z_b+\rangle_{\mathrm{SO}}+b|z_1-,\ \dots\ ,z_m+\rangle\otimes|z_a+,z_b-\rangle_{\mathrm{SO}})/2\\&+(a|z_1+,\ \dots\ ,z_m-\rangle\otimes|z_a+,z_b+\rangle_{\mathrm{SO}}-b|z_1-,\ \dots\ ,z_m-\rangle\otimes|z_a+,z_b-\rangle_{\mathrm{SO}})/2\\&+(a|z_1+,\ \dots\ ,z_m+\rangle\otimes|z_a-,z_b-\rangle_{\mathrm{SO}}+b|z_1-,\ \dots\ ,z_m+\rangle\otimes|z_a-,z_b+\rangle_{\mathrm{SO}})/2\\&+(a|z_1+,\ \dots\ ,z_m-\rangle\otimes|z_a-,z_b-\rangle_{\mathrm{SO}}-b|z_1-,\ \dots\ ,z_m-\rangle\otimes|z_a-,z_b+\rangle_{\mathrm{SO}})/2.\end{aligned} \tag{4.7}$$

Now, for instance, the measurement result (z_m+,z_a+), directly projects the remaining state into the desired state. However, generally, the subordinate must be told the result of the measurement (a two-bit message), and by a simple bit flip or sign change he may reconstruct the initial m-particle entangled state. Effectively this procedure ''teleports'' the entanglement to the subordinate. It should be kept in mind that strictly speaking this protocol is not a (m,n)-threshold protocol. This is because of the asymmetry between the executives and the subordinates, not allowing m subordinates by themselves to share the split state. However, the protocol still gives some added flexibility as a possible way to transfer a split qubit between various parties.

V. DISCUSSIONS

We have shown a simple two-particle quantum-entanglement-based protocol for quantum secret sharing, which is implementable by parametric down-conversion and interferometric Bell state analysis. The interest in using entanglement-based protocols is initially more of a ‘‘proof-of-principle’’ nature, as in some cases even simpler nonentanglement quantum cryptographic protocols may be used. We have also shown the extension of a quantum secret splitting scheme based on multiparticle entangled states toward a *m-out-of-n* protocol, where a qubit split to *m* participants can be shifted to other participants using entanglement swapping. A very interesting question remains concerning quantum secret sharing and splitting: What would be the protocol for secret splitting for quantum registers? We believe this would be of even more interest for quantum computation and communication than if it is only single quantum bits that are split. One of the most interesting questions in this respect is the amount of entanglement needed to construct a secure protocol.

ACKNOWLEDGMENTS

A.K. would like to thank NTT Basic Research Laboratories for generous support, and for having provided an excellent working atmosphere during his stay in Japan. This work was also supported by the Swedish Natural Science Research Council (NFR).

[1] P. W. Shor, in *Proceedings of the Symposium on the Foundation of Computer Science, 1994, Los Alamonitos, California* (IEEE Computer Society, New York, 1994), pp. 124–134.

[2] L. K. Grover, Phys. Rev. Lett. **79**, 325 (1997).

[3] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wooters, Phys. Rev. Lett. **70**, 1895 (1993).

[4] D. Bouwmeister, J. W. Pan, K. Mattle, M. Eible, H. Weinfurther, and A. Zeilinger, Nature (London) **390**, 575 (1997).

[5] D. Boschi, S. Branca, F. De Martini, L. Hardy, and S. Popescu, Phys. Rev. Lett. **80**, 1121 (1998).

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

[7] H. K. Loo and H. F. Chau, Phys. Rev. Lett. **78**, 3410 (1997).

[8] D. Mayers, Phys. Rev. Lett. **78**, 3414 (1997).

[9] M. Hillery, V. Buzek, and A. Bertaiume, Los Alamos e-print archive, quant-ph/9806063.

[10] G. R. Blakley, in *Proceedings of the American Federation of Information Processing 1979 National Computer Conference* (American Federation of Information Processing, Arlington, VA, 1979), pp. 313–317.

[11] A. Shamir, Commun. ACM **22**, 612 (1979).

[12] D. M. Greenberger, M. A. Horne, A. Shimony, and A. Zeilinger, Am. J. Phys. **58**, 1131 (1990).

[13] M. Zukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, Phys. Rev. Lett. **71**, 3031 (1993).

[14] S. Bose, V. Vedral, and P. L. Knight, Phys. Rev. A **57**, 822 (1998).

[15] J-W. Pan, D. Bouwmeester, H. Weinfurther, and A. Zeilinger, Phys. Rev. Lett. **80**, 3891 (1998).

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

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

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

[19] A. Karlsson and M. Bourennane, Phys. Rev. A **58**, 4394 (1998).

[20] S. Massar and S. Popescu, Phys. Rev. Lett. **74**, 1259 (1994).

[21] A. Barenco, D. Deutsch, A. K. Ekert, and R. Jozsa, Phys. Rev. Lett. **74**, 4083 (1995).