Efficient multiparty quantum-secret-sharing schemes

Li Xiao,[1,2] Gui Lu Long,[1,2,3,4] Fu-Guo Deng,[1,2] and Jian-Wei Pan[5]
[1]*Department of Physics, Tsinghua University, Beijing 100084, China*
[2]*Key Laboratory for Quantum Information and Measurements, MOE, Beijing 100084, People's Republic of China*
[3]*Center of Atomic and Molecular NanoSciences, Tsinghua University, Beijing 100084, China*
[4]*Center for Quantum Information, Tsinghua University, Beijing 100084, China*
[5]*Institute for Experimental Physics University of Vienna, Boltzmanngasse 5, Vienna 9, Austria*

(Received 1 August 2003; published 11 May 2004)

In this work, we generalize the quantum-secret-sharing scheme of Hillery, Bužek, and Berthiaume [Phys. Rev. A **59**, 1829 (1999)] into arbitrary multiparties. Explicit expressions for the shared secret bit is given. It is shown that in the Hillery-Bužek-Berthiaume quantum-secret-sharing scheme the secret information is shared in the parity of binary strings formed by the measured outcomes of the participants. In addition, we have increased the efficiency of the quantum-secret-sharing scheme by generalizing two techniques from quantum key distribution. The favored-measuring-basis quantum-secret-sharing scheme is developed from the Lo-Chau-Ardehali technique [H. K. Lo, H. F. Chau, and M. Ardehali, e-print quant-ph/0011056] where all the participants choose their measuring-basis asymmetrically, and the measuring-basis-encrypted quantum-secret-sharing scheme is developed from the Hwang-Koh-Han technique [W. Y. Hwang, I. G. Koh, and Y. D. Han, Phys. Lett. A **244**, 489 (1998)] where all participants choose their measuring basis according to a control key. Both schemes are asymptotically 100% in efficiency, hence nearly all the Greenberger-Horne-Zeilinger states in a quantum-secret-sharing process are used to generate shared secret information.

DOI: 10.1103/PhysRevA.69.052307 PACS number(s): 03.67.Dd, 03.67.Hk, 89.70.+c

I. INTRODUCTION

The combination of quantum mechanics with information has produced many interesting and important developments. Quantum cryptography is one important application. Quantum key distribution (QKD) concerns the distribution of one-time-pad keys between distant two parties [1]. With quantum mechanics, other cryptographic task can be realized. Suppose Alice wants two parties Bob and Charlie who are at distant places to fulfill certain tasks. Alice knows that one of them may be dishonest, but she does not know who this dishonest guy is. To complete this task, classical cryptography uses the secret-sharing technique [2,3]. In quantum information, this task can be achieved by quantum secret sharing (QSS), and it is a fruitful area of research. Many researches have been carried out [4,5,7–9]. It has also been demonstrated in experiment recently [6]. With quantum mechanics, one can share both classical information and quantum information. In this paper, we consider the issue of sharing of classical secret information. We specifically consider the QSS scheme proposed by Hillery, Bužek, and Berthiaume (hereafter we refer to HBB protocol) [4]. In Ref. [4], secret sharing with three and four parties have been studied. In the HBB QSS scheme, the secret sharing is accomplished by using the Greenberger-Horne-Zeilinger (GHZ) state [10]. In this scheme, Alice, Bob, and Charlie need to choose randomly one measuring basis from either the σ_x measuring basis or the σ_y measuring basis, respectively, similar to the Bennett-Brassard 1984 (BB84) QKD scheme [1]. In half of the cases, nobody chooses the σ_y axis or two parties choose the σ_y axis, the measuring results of the three parties are correlated. In these cases, Bob and Charlie can combine their measuring-basis information and their measurement outcomes to determine the results of Alice's measurement. In this case, Alice's measurement result is used as the secret information that she wants Bob and Charlie to share. Generally in order to establish the secret-sharing scheme, a detailed table needs to be constructed to list all the possible combinations of the measuring basis and the possible outcomes of all parties. When the number of participating parties is large, the construction of such a table is very tedious and it is also inconvenient to use. In this paper, we reformulate the HBB scheme in simple mathematical terms, and the shared secret information becomes the parity of a binary string formed by the measured outcomes of the participating parties. From this formulation, the rules in the HBB QSS scheme are obtained. For instance for a round of communication to be a valid one, the number of parties choosing the σ_y basis has to be even, because when even number of parties choose the σ_y basis, the bit value of Alice has a one-to-one correspondence with the parity of the binary number formed by the measurement outcomes of the participating parties. From this mathematical formalism, we generalize the HBB scheme into arbitrary number parties cases. This is given in Sec. II.

In the HBB QSS scheme, only half of the GHZ states can be used for secret sharing. This is the intrinsic limitation of this scheme. This is similar to the BB84 QKD scheme where only half of the photons transmitted can be used to generate useful keys. In QKD, Lo, Chau, and Ardehali [11] have proposed a scheme that increases the intrinsic efficiency to 100% asymptotically. In their scheme, they choose one preferred measuring basis most of the time, and choose the other measuring basis, the unfavored measuring basis, with a small probability. The events that Alice and Bob choose the unfavored measuring basis are used later for eavesdropping checking. This has greatly increased the intrinsic efficiency of the BB84 scheme. In the limiting case of large numbers, the efficiency approaches 100%. This has been shown to be unconditionally secure [11]. Hwang, Koh, and Han [12] have proposed another modification to the BB84 QKD scheme that also increases its efficiency to nearly 100% by letting Alice and Bob to choose identical measuring basis according to a common secret key. This control key is used repeatedly during a QKD transmission session. Controlled keys have also been used in QKD in the controlled-order-rearrangement-encryption scheme [13], where Alice takes one particle from each Einstein-Podolsky-Rosen (EPR) pair from a group of EPR pairs and mixes up their orders and sends them to Bob, and Bob recovers the orders of the particles to get the correct particle correlation of EPR pairs. Alice and Bob synchronize their action by using a control key repeatedly. The following example explains the Koh and Han technique: if the control key is 0101001110, then Alice and Bob choose their measuring basis in the following sequence "$+\times+\times++\times\times\times+$" where "+" represents the vertical-horizontal measuring basis, and "×" represents the diagonal-antidiagonal measuring basis. The control key is usually quite short, say 1000 bits long. It is repeated again and again until the QKD process ends. In this way, Alice and Bob can always choose the same measuring basis. The quantum-mechanical nature of the single photons renders eavesdropping detectable, and the random nature of the measured results keeps the information on the control key safe. It has been shown that the scheme is secure [14] for ideal single-photon sources. The essential ingredient in these improvements is to allow the two parties to use identical measuring basis as much as possible. Generalizing these two techniques, we have proposed two efficient QSS schemes that are asymptotically 100% in efficiency. This is given in Sec. III. A summary is given in Sec. IV.

II. MULTIPARTY HBB QUANTUM-SECRET-SHARING SCHEME

We present the n-party HBB QSS scheme first. Suppose there are n parties taking part in the secret-sharing process. It is done by using a sequence of GHZ multiplets

$$|\psi\rangle_{\mathrm{GHZ}}=\frac{1}{\sqrt{2}}(|000\cdots0\rangle+|111\cdots1\rangle), \tag{1}$$

where states $|0\rangle=|z+\rangle$ and $|1\rangle=|z-\rangle$ are eigenstates of the spin projection in the z direction, σ_z. Alice keeps one particle and sends the other two particles to Bob and Charlie each. Then Alice, Bob, Charlie randomly choose from the σ_x and the σ_y basis to measure their particles respectively. The eigenstates of the σ_x and the σ_y operators are

$$|0\rangle_x=|+x\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle),\quad |1\rangle_x=|-x\rangle=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle), \tag{2}$$

$$|0\rangle_y=|+y\rangle=\frac{1}{\sqrt{2}}(|0\rangle+i|1\rangle),\quad |1\rangle_y=|-y\rangle=\frac{1}{\sqrt{2}}(|0\rangle-i|1\rangle). \tag{3}$$

Inversely we have the expansion of the eigenstates of the σ_z operator in terms of the σ_x and the σ_y eigenbasis as follows:

$$|0\rangle=\frac{1}{\sqrt{2}}(|0\rangle_x+|1\rangle_x),\quad |1\rangle=\frac{1}{\sqrt{2}}(|0\rangle_x-|1\rangle_x), \tag{4}$$

$$|0\rangle=\frac{1}{\sqrt{2}}(|0\rangle_y+|1\rangle_y),\quad |1\rangle=-\frac{i}{\sqrt{2}}(|0\rangle_y-|1\rangle_y). \tag{5}$$

We make the convention that the positive polarized states along x or y axis are taken as 0, and those along the negative direction are denoted as 1. In the HBB scheme, only half of the GHZ particles can be used for secret sharing. The choice of the measuring basis plays an important role in judging whether a round of measurement can be used for secret sharing.

We use a sequence $[b_1(j),b_2(j),\ldots,b_i(j),\ldots,b_n(j)]$ to denote the measuring basis information for Alice, Bob,… for the jth GHZ-state. The number in the bracket j refers to the jth GHZ state in a sequence of secret-sharing operations. The subscript refers to the order number of particles, 1 represents Alice's particle, 2 refers to Bob's particle, and so on. If $b_i(j)=0$, then the ith party uses the x basis, and $b_i(j)=1$ means that the ith party uses the y axis. To obtain the measuring result in such a case, we need to expand the GHZ state in the eigenbasis of $[b_i(j),i=1,\ldots,n]$. Using Eqs. (4) and (5), the $|00\cdots0\rangle$ component can be written as

$$|00\cdots0\rangle=\prod_{i=1}^{n}\left(\sqrt{\frac{1}{2}}(|0\rangle_{b_i}+|1\rangle_{b_i})\right), \tag{6}$$

and the $|11\cdots1\rangle$ component can be written as

$$|11\cdots1\rangle=\prod_{i=1}^{n}\left(\frac{-i}{\sqrt{2}}(|0\rangle_{b_i}-|1\rangle_{b_i})\right). \tag{7}$$

When the y basis are chosen by an odd number of participants, the expansion for $|11\cdots1\rangle$ has the following form:

$$|11\cdots1\rangle=\pm\frac{i}{(\sqrt{2})^n}\prod_{i=1}^{n}(|0\rangle_{b_i}-|1\rangle_{b_i}), \tag{8}$$

where the + sign is for $n=2k+1$ and − sign is for $n=4k+1$, where k is a positive integer.

Hence the GHZ state in Eq. (1) can be rewritten as

$$|\psi\rangle_{\mathrm{GHZ}}=\frac{1}{2^{(n+1)/2}}\left(\prod_{i=1}^{n}(|0\rangle_{b_i}+|1\rangle_{b_i})\pm i\prod_{i=1}^{n}(|0\rangle_{b_i}-|1\rangle_{b_i})\right), \tag{9}$$

for an odd number of participants choosing the y basis. There is no cancellation between the first product term and the second product term in Eq. (9), and terms such as $|0i_2i_3\cdots i_{n-1}\rangle_{b_1b_2\cdots b_n}$ and $|1i_2i_3\cdots i_{n-1}\rangle_{b_1b_2\cdots b_n}$ both present in the expansion in Eq. (9). In other words, for a set of measured values $i_2,\ldots,i_n$ measured in measuring basis $b_2,\ldots,b_n$ by the participants Bob, Charlie, and so on, Alice's measured result still has two possibilities. Even if the $n-1$ secret-sharing parties get together and disclose their measuring-basis information and their measuring outcomes, they still cannot obtain the result of Alice's measurement. For instance in a three-party QSS, if Alice chooses the y axis, Bob and Charlie choose the x axis, the expansion in the eigenbasis of σ_y, σ_x, and σ_x (for Alice, Bob, and Charlie, respectively) will be

$$\frac{(1-i)}{4}(|000\rangle+|011\rangle+|101\rangle+|110\rangle)+\frac{(1+i)}{4}(|001\rangle+|010\rangle + |100\rangle+|111\rangle), \tag{10}$$

where the basis orders $y-x-x$ in the subscript are omitted for brevity. When Bob and Charlie have definite measured results, Alice's result still has two possibilities. For instance, when Bob and Charlie's results are 0 and 0, respectively (along the positive-x axis), Alice's result may be 0 (along the positive-y axis) from component $|000\rangle$, or 1 (along the negative-y axis) from component $|100\rangle$. Thus it is not useful for quantum secret sharing.

When the number of parties choosing the y basis is even, we have

$$|\psi\rangle_{\text{GHZ}}=\frac{1}{2^{(n+1)/2}}\left(\prod_{i=1}^{n}(|0\rangle_{b_i}+|1\rangle_{b_i})\pm\prod_{i=1}^{n}(|0\rangle_{b_i}-|1\rangle_{b_i})\right). \tag{11}$$

Because some terms in the second product term in the expansion have negative sign, they cancel with relevant terms in the first product term, hence there are only 2^{n-1} terms left in Eq. (11). Among the 2^{n-1} terms, the value of the first bit, which is the result of Alice's measurement, is uniquely determined by the remaining $n-1$ bit values. In this case when the $n-1$ parties get together and reveal their measuring-basis information and the measured results, they can uniquely determine the bit value of Alice. Unless all $n-1$ participating parties present, the determination of Alice's bit value is impossible. For instance, if only $n-2$ parties are present, from their measured values and measuring-basis information, they can only narrow the state down to two possibilities in which Alice can have either 0 or 1. Thus it is only when all $n-1$ parties work collectively that they can get the bit value of Alice.

Summarizing the above observation, the general rule for multiparty secret sharing are as follows.

(1) The number of parties using the σ_y basis has to be even.

(2) When the number of parties using y basis is equal to $2(2k+1)$ where k is a non-negative integer, the bit value of Alice is simply the modulo 2 sum of the $n-1$ parties' bit value plus 1:

$$i_{\text{Alice}}=i_1=i_2\oplus i_3\oplus\cdots\oplus i_n\oplus 1. \tag{12}$$

For instance in a three-party QSS with two parties using y axis, there is a component $|100\rangle$ in the expansion (11), the modulo 2 sum of Bob and Charlie gives 0, then adding 1 gives 1.

(3) When the number of parties taking the y basis is $4k$, then the bit value of Alice is simply the modulo 2 sum of the $n-1$ parties' bit values.

$$i_{\text{Alice}}=i_1=i_2\oplus i_3\oplus\cdots\oplus i_n. \tag{13}$$

Hence the n party HBB QSS scheme can be given as follows: (1) Alice prepares an n particle GHZ state (1); (2) Alice keeps one particle at her own hand and sends the rest of particles to the $n-1$ participants, each party a particle; and (3) each party chooses randomly from the x or the y measuring basis to measure his/her particle. He/she keeps the measured result and the measuring-basis information for his/her particle. If the measured result is up (down) along the measuring basis, he/she records the result as 0 (1); (4) the above procedures (1)–(3) are repeated many times until sufficient number of measured results are produced. This should be at least twice as much as the number of desired shared bits; (5) after procedure (4), each participants sends the measuring-basis information to Alice through a classical channel and upon receiving all the measuring-basis information, Alice counts the number of parties choosing the y basis. Alice publicly announces the nature of this number for each round: odd, or an even number with the form of $2(2k+1)$, or an even number with the form of $4k$. The exact number of k need not be disclosed. If the number is odd, then that round of measurement result is dropped, and if the number is even, all the participants keep their measured values and the measuring-basis information for these events; (6) Alice selects a sufficiently large subset of events and asks the participants to disclose their measured values for these events. From this information, Alice can check if there exists eavesdropping in the quantum channel. For instance, if an eavesdropper tries to intercept the QSS scheme by measuring the state of the particle intended for a legitimate participant using randomly the x or the y basis, the error rate will be as high as 25%, just like the BB84 QKD case. If the error rate is high, then Alice concludes that there is eavesdropping and the QSS session is dropped. If the error rate is low, then the QSS session is concluded safe and after quantum error correction and privacy amplification, a final secret sharing bit string is produced. The $n-1$ participants can determine the shared secret bit using the QSS rules given in Eqs. (12) and (13) for each valid of transmission.

We have reformulated the HBB QSS protocol in a concise mathematical form and generalized it into arbitrary multiparties. In these rules, the secret key can be simply calculated using the parity of the measurement outcomes of the participating parties together with the number of y basis used in the process. However only half of the GHZ states can be used for quantum secret sharing.

III. ASYMPTOTIC 100% EFFICIENT QSS SCHEMES

By 100% efficient, we mean that all the GHZ-state particles used in a QSS scheme can be used for sharing the secret information as compared with the original HBB-QSS scheme where half of the GHZ states have to be discarded, because half of the time the participants may choose an odd number of σ_y basis. Here we propose two efficient QSS schemes using techniques that were originally used for QKD to increase the efficiency. Full efficiency can be obtained if the participants can always choose the right combination of measuring basis so that there are always even number of participants choosing the σ_y-measuring basis. This can be achieved in two different ways. One is to use the method proposed by Lo, Chau, and Ardehali for QKD [11]. In this scheme the efficiency of the BB84 QKD scheme is asymptotically 100%. The other one is the one based on the method proposed by Hwang, Koh, and Han [12]. They have discovered that the efficiency of BB84 QKD scheme can be increased to 100% by letting Alice and Bob to choose identical measuring basis according to a common secret key repeatedly, say with a 1000 bit control key. For instance a 0 in the control key means Alice and Bob use the horizontal-vertical measuring basis and a 1 in the control key directs them to use the diagonal-antidiagonal measuring basis. These schemes have several advantages. First the efficiency is increased to 100% asymptotically. Second the public announcement of measuring basis can be omitted or almost omitted and this saves a lot of storage space, classical communication, and the comparison computation time. These techniques can be generalized with some modification for use in QSS. In the following, we present the results in details.

A. The favored-measuring-basis efficient QSS scheme

We call the efficient QSS scheme based on the Lo-Chau-Ardehali technique as the favored-measuring-basis efficient QSS scheme. It is noticed that if all the participants in a QSS round choose the σ_x basis, it is a valid QSS round, and the GHZ state in Eq. (1) can be written in the σ_x basis as

$$|\psi\rangle_{\mathrm{GHZ}} = \sqrt{\frac{1}{2^{n+1}}}\left(\prod_{i=1}^{n}(|0\rangle + |1\rangle) - \prod_{i=1}^{n}(|0\rangle - |1\rangle)\right)$$

$$= \sqrt{\frac{1}{2^{n-1}}}\sum_{i_1 i_2 \cdots i_n}{}' \, |i_1 i_2 \cdots i_n\rangle, \tag{14}$$

where the prime over the sum means a restricted sum for those running indices satisfying

$$i_1 \oplus i_2 \oplus \cdots \oplus i_n = 0. \tag{15}$$

Terms like $|10\cdots0\rangle$ are absent from the GHZ-state expression because a part from the second product cancels with that from the first product term in Eq. (14). Hence a high-efficiency QSS scheme based on the Lo-Chau-Ardehali technique [11] can be designed as follows: (1) Alice prepares a sequence of n-particle GHZ state in state (1); (2) for each GHZ state, Alice keeps one particle at her own site and sends the rest $n-1$ particles to other participants, each particle to a participant; (3) each participant chooses with a large probability to measure his/her particle in the σ_x basis, and with a small probability to measure in the σ_y basis. They records the basis they use and the outcome of the measurement for each particle; (4) after a large number of GHZ-state particles have been distributed and measured, they publish their measuring basis for each GHZ state; and (5) for those rounds of communication where at least one of the participants chooses the σ_y basis, all the participants publish also the outcomes of their measurements. In approximate half of these events, an even number of participants choose the σ_y basis, and the outcomes of the measurements of all the participants are correlated, and they will be used to check eavesdropping. We can modify the refined data analysis method proposed in Ref. [11] to catch Eve. In the refined data analysis, one only checks those cases that an even number of participants choose the σ_y basis(excluding the case when no participants choose the σ_y basis). Eve's interception will cause significant errors. Eve needs to intercept all the $n-1$ particles sent by Alice to the other $n-1$ participants. Suppose Eve always uses the σ_x basis to intercept for those events that two participants choose the σ_y basis, Eve will introduce an error rate as high as 50%. If we just look at the events where two participants choose the σ_y basis, this case can be seen as an variant of the efficient QKD scheme between these two participants where they use the σ_x basis most of the time and the σ_y basis only a small number of times in Ref. [11]. By examining the error rate, the participants can determine whether the QSS communication is secure. For noiseless channels and ideal photon sources, if no errors exist one can conclude the QSS operations as safe. If there are errors then one concludes that the QSS operations are insecure and discards the result. For noisy channels and imperfect photon sources, one has to use quantum error correction and privacy amplification method to get secure shared secret information. A more rigorous security analysis for this scheme, and the details of the postprocessing is needed, and this work is under way. We will not touch this issue in this paper.

TABLE I. An example of valid control keys for a three-party measuring-basis-encrypted QSS scheme.

Round No.	1	2	3	4	5	6	7	8	9	10
Alice	x	y	x	y	x	x	y	x	x	y
Bob	x	x	y	y	x	x	y	y	x	x
Charlie	x	y	y	x	x	x	x	y	x	y

B. The measuring-basis-encrypted efficient QSS scheme

We call the efficient QSS scheme based on the Hwang-Koh-Han QKD technique as the measuring-basis-encrypted QSS scheme, because the measuring basis of the participants are controlled by a secret key and this information is encrypted. In the Hwang-Koh-Han QKD scheme, the measuring basis of Alice and Bob in a QKD process is synchronized by a control key. Different from QKD where Alice and Bob use the same secret key to synchronize their measuring basis, we need n-control keys to control the valid choices of measuring basis for the n participants. Furthermore, the control key sequence is different for different participant. In Table I, we give an example of control keys for a three party QSS scheme. Here only the first 10 bits of the control keys are shown. In practice, the control keys are about 1000 bits long.

The essential part is to generate a control key for each participant so that the set of measuring basis in a QSS transmission always has an even number of σ_y basis. Now we introduce a method for establishing the control key sequences for each party on-site using the original HBB QSS scheme. First we run the HBB QSS scheme in its original form, that is, all parties choose their measuring basis randomly. They record their results and also the measuring-basis information. They then send the measuring-basis information to Alice, but the measured results are kept secret. Upon receiving the measuring-basis information from all parties, Alice can decide which GHZ-multiplets are valid QSS operation, that is, she knows that in these operations there are an even number of parties having chosen the σ_y basis. She then tells all the $n-1$ parties to retain the results in these rounds. Then each of the party will have a sequence of random numbers which is known only to himself/herself. It is noted that each party's control key is different from others. These numbers are used to determine each party's measuring-basis choice. Except Alice, each party will use the $\sigma_x(\sigma_y)$ basis, if the bit value in her/his sequence is 0 (1). Alice's control sequence is slightly different from the others in the following way: if the number of σ_y basis in the measurement is $4k$, she simply choose $\sigma_x(\sigma_y)$ basis if her measured result is 0 (1), and if the number of σ_y-basis measurement is $2(2k+1)$, then she will choose $\sigma_y(\sigma_x)$ basis if her measured result is 0 (1). This is because when the number of σ_y basis is $4k$, the measured result's parity is even, and it is odd when it is $2(2k+1)$. As in the QKD case, this control key can be used repeatedly. The control sequence needs not be long, a few hundreds of bit, the order of a thousand is sufficient.

The on-site generation of the control keys can be spared if the participating parties keep part of the random numbers left over from a previous QSS operation.

The security of the QSS has been discussed in Ref. [4], and the discussion there also applies here. The security of the repeated use of a control sequence is discussed in Refs. [12,14], and they can be adapted here with some minor modification. The QSS scheme can be viewed as a two "party" quantum key distribution scheme if one views the $n-1$ parties as whole as a single participant. These $n-1$ participants as a whole share a common secret key with Alice. However inside these $n-1$ parties, they have to act collectively to work out the secret key of Alice. Any eavesdropping will cause significant errors to the random key. Similarly, if one of the party is dishonest, significant error will occur. For instance if Eve uses randomly the σ_x basis and the σ_y basis to measure $n-1$ particles Alice sends to the $n-1$ participants, then Eve will have $(1/2)^{n-1}$ probability to choose the right measuring basis. For those that Eve has chosen the wrong measuring basis, there is 50% of probability to make error in the parity of the string, which is the shared secret information. Hence the error rate introduced by Eve is

$$e=[1-(1/2)^{n-1}]1/2. \tag{16}$$

For $n=3$, this amounts to $3/8=37.5\%$. As the number of participants increase, the error rate approaches 50%.

IV. SUMMARY

We have generalized the HBB QSS scheme into arbitrary number of parties, and given explicit expressions for the shared secret information in terms of the parity of strings formed by the measured results of the $n-1$ participants. By generalizing the Lo-Chau-Ardehali QKD scheme [11] and the Hwang-Koh-Han QKD scheme [12], we have developed two efficient QSS schemes: the favored-measuring-basis scheme and the measuring-basis-encrypted QSS schemes. The efficiency of these QSS schemes are asymptotically 100%. We have also qualitatively showed the security of the QSS scheme. It remains to be shown the security of these QSS schemes in noisy channels and with imperfect single-photon sources, in a way similar to what have been done for the security of QKD [15–17]. Work is under way and the result will be published elsewhere.

ACKNOWLEDGMENTS

This work was supported by the National Fundamental Research Program Grant No. 001CB309308, the China National Natural Science Foundation Grant Nos. 60073009 and 10325521, the Hang-Tian Science Fund, and the SRFDP program of the Education Ministry of China.

[1] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore* (IEEE, New York, 1984), pp. 175–179.

[2] B. Schneier, *Applied Cryptography* (Wiley, New York, 1996), p. 70.

[3] J. Gruska, *Foundations of Computing* (Thomson Computer Press, London, 1997), p. 504.

[4] M. Hillery, V. Bužek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).

[5] R. Cleve, D. Gottesman, and H. K. Lo, Phys. Rev. Lett. **83**, 648 (1999).

[6] W. Tittel, H. Zbinden, and N. Gisin, Phys. Rev. A **63**, 042301 (2001).

[7] S. Bandyopadhyay, Phys. Rev. A **62**, 012308 (2000).

[8] D. Gottesman, Phys. Rev. A **61**, 042311 (2000).

[9] A. Karlsson, M. Koashi, and N. Imoto, Phys. Rev. A **59**, 162 (1999).

[10] D. Greenberger, M. Horne, and A. Zeilinger, in *Bell's Theorem, Quantum Theory, and Conceptions of the Universe*, edited by M. Kaftos (Kluwer Academic, Dordrecht, 1989).

[11] H. K. Lo, H. F. Chau, and M. Ardehali, e-print quant-ph/0011056.

[12] W. Y. Hwang, I. G. Koh, and Y. D. Han, Phys. Lett. A **244**, 489 (1998).

[13] F. G. Deng and G. L. Long, Phys. Rev. A **68**, 042315 (2003).

[14] W. Y. Hwang, X. B. Wang, K. Matsumoto, J. Kim, and H. W. Lee, Phys. Rev. A **67**, 012302 (2003).

[15] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).

[16] D. Mayers, e-print quant-ph/9802025.

[17] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).