Conditional efficient multiuser quantum cryptography network

Peng Xue,* Chuan-Feng Li, and Guang-Can Guo†
Laboratory of Quantum Communication and Quantum Computation and Department of Physics, University of Science and Technology of China, Hefei 230026, People's Republic of China
(Received 13 June 2001; published 15 January 2002)

We propose a conditional quantum key distribution scheme with three nonorthogonal states. Combined with the idea presented by Lo *et al.* (H.-K. Lo, H. F. Chau, and M. Ardehali, e-print arXiv: quant-ph/0011056), the efficiency of this scheme is increased to tend to 100%. Also, such a refined data analysis guarantees the security of our scheme against the most general eavesdropping strategy. Then, based on the scheme, we present a quantum cryptography network with the addition of a device called ''space optical switch.'' Moreover, we give out a realization of a quantum random number generator. Thus, a feasible experimental scheme of this efficient quantum cryptography network is completely given.

DOI: 10.1103/PhysRevA.65.022317 PACS number(s): 03.67.Dd, 03.65.Ud

I. INTRODUCTION

The desire and necessity to transmit secret messages from one person to another are probably as old as the ability of human beings to communicate. Cryptography is the art of encoding a text in such a way that an eavesdropper can get as little information as possible about it, and only the authorized users can decode it perfectly. To achieve this goal, an algorithm is used to combine a message with some additional information—known as the ''key''—to produce a cryptogram. For this reason, secure key distribution is a crucial problem in cryptography.

Since publication of the BB84 scheme proposed by Bennett and Brassard, there has been much interest in using quantum mechanics in cryptography [1–8]. To date, quantum cryptography is the most mature prospect of quantum information processing (QIP). The best-known quantum cryptographic application is quantum key distribution (QKD). Theoretical two-party QKD models based on the uncertainty principle have been analyzed by Bennett and Brassard (BB84) [1] and models based on quantum correlations have been proposed by Ekert (E91) [2], which are based on entangled pairs and use the generalized Bell's inequality [9] (Clauser-Horne-Shimony-Holt inequality [10]) to establish security. In these schemes, the sender Alice uses nonorthogonal quantum states (transmitted through a quantum channel) to transfer the key to the receiver Bob. Such states cannot be cloned [11,12], hence, any attempt by an eavesdropper Eve to get information on the key disturbs the transmitted signals and induces noise. This noise will be detected by the legal users during the second stage of the transmission, which includes discussion over a public channel.

The efficiencies of the schemes, which are based on nonorthogonal states are no more than 50%. In 1998, Ardehali *et al.* and Lo *et al.* devised a modification [13,14] that essentially doubles the efficiency of the BB84 scheme, where Alice and Bob choose between the two bases independently but with *substantially* different probabilities ϵ and $1-\epsilon$. They also prove the security of their scheme.

Furthermore, quantum cryptography is experimentally the most advanced subfield of QIP. The first QKD prototype, working over a distance of 30 cm in 1989, was implemented by means of laser transmitting in free space [5]. Soon, experimental demonstrations by optical fibers were set up. Now, the transmission distance is extended to more than 48 km in telecom fibers [15] and about 1 km in free space [16].

There are also theoretical proposals for QKD between more that two parties based on (GHZ) states [17,18], and an experiment has already been performed [19].

If some practical techniques were to become widespread, however, it would have to be effective over a quantum cryptography network. Biham *et al.* [20] proposed the time-reserved Einstein-Podolsky-Rosen (EPR) protocol, which combined with quantum memories to build a quantum cryptography network. In a series of publications, Townsend *et al.* [21] have shown how the properties of passive optical networks can be exploited to give *one-to-any* and *any-to-any* key distribution using quantum cryptography on branch- and loop-configuration networks.

In this paper, we present a QKD scheme with three nonorthogonal states. Combined with the idea presented by Lo *et al.* [14], the efficiency of this scheme is increased to tend to 100%. If it is combined with the use of a device called the ''space optical switch,'' QKD between any pair of parties can be realized. Therefore, we can establish a conditional multiuser quantum cryptography network. We choose a two-user scenario by way of example and it will become evident that there are many users that will work equally well. We shall explain the scheme using the language of polarization of photons, but clearly any two-level quantum system would do. The center Alice prepares pairs of photons in the known $|BC\rangle_1$, $|BC\rangle_2$, and $|BC\rangle_3$ states (see below) with probabilities $(1-\epsilon_1)/2$, $(1-\epsilon_1)/2$, and ϵ_1, respectively. She then sends a sequence of photons out of each pair to the two users Bob and Carol. The users choose their bases independently with different probabilities and perform measurements, and then broadcast their bases actually chosen via the classical channel to establish a common key between them. Since two parties are much more likely to be using the same basis, thus reducing the fraction of discarded data, a significant gain in

*Email address: xuepeng@mail.ustc.edu.cn
†Email address: gcguo@ustc.edu.cn

efficiency is achieved. To ensure our scheme is secure, we divide the accepted data into various subsets according to the bases employed and estimate an error rate for each subset *separately*. We then show that such a refined error analysis is sufficient in ensuring the security of our scheme against the most general eavesdropping strategy. The proof is based on the technique in Shor and Preskill's proof of the security of another scheme [22]. Particularly, it can decrease the proportion of the EPR state $|BC\rangle_3$ in the incident states to tune the value of ϵ_1. If the value is small enough, all the sifted key bits obtained as the EPR state are used as the incident state will be used to detect the eavesdropper and then abort. Henceforth, the secret key obtained as the product states $|BC\rangle_1$ and $|BC\rangle_2$ are used is also known to the center Alice who may be regarded as a *superuser*. Therefore, we can realize the efficient QKD among three users. Similarly, to realize the two-party protocol, we only need to increase ϵ_1.

In addition, we give a realization of a fast and compact quantum random number generator. Thus, a feasible experimental scenario of this efficient quantum cryptography network is completely shown.

This paper is organized as follows. In the next section, we present an efficient two-user QKD scheme with three nonorthogonal states. By considering a simple biased eavesdropping strategy by Eve, we note that our refined analysis is an essential feature of our scheme in Sec. III. We consider the most general type of eavesdropping strategy allowed by quantum mechanics and prove that our present scheme is unconditionally secure in Sec. IV. In Sec. V, the constraints on the probabilities are derived. In addition, in Sec. VI, we give a realization of a quantum random number generator. We then present a quantum cryptography network based on the QKD scheme, which is combined with a device called the ''space optical switch'' in Sec. VII. Finally, we conclude the scheme in Sec. VIII.

II. EFFICIENT TWO-USER QKD SCHEME

In our scheme, there are three parties: the center Alice and the users Bob and Carol. Alice prepares pairs of photons in the known nonorthogonal states

$$|BC\rangle_1=|0\rangle_B|0\rangle_C,$$

$$|BC\rangle_2=|1\rangle_B|1\rangle_C, \tag{1}$$

$$|BC\rangle_3=\frac{1}{\sqrt{2}}(|0\rangle_B|0\rangle_C+|1\rangle_B|1\rangle_C),$$

with probabilities $(1-\epsilon_1)2$, $(1-\epsilon_1)/2$, and ϵ_1, respectively. Photon B is sent to Bob and photon C is sent to Carol. There are two types of measurements that the receivers may perform: they may measure along the rectilinear basis, thus distinguishing between photons in the states $|0\rangle$ and $|1\rangle$ (i.e., horizontal and vertical photons). Alternatively, they may measure along the diagonal basis, thus distinguishing between the $+45$ and $-45\,^{\circ}$C photons.

The three parties are connected by a quantum channel and a classical public channel. The quantum channel consists usually of an optical fiber. The public channel, however, can be any communication link. The scheme works in the following way:

(1) Alice, Bob, and Carol pick two numbers ϵ_1 and ϵ_2, $0<\epsilon_1$, $\epsilon_2\leqslant 1$, and make their values public. The constraints on ϵ_1 and ϵ_2 will be discussed in Sec. V.

(2) Alice prepares a sequence of pairs of photons in one of the three states ($|BC\rangle_1$, $|BC\rangle_2$, and $|BC\rangle_3$) with probabilities $(1-\epsilon_1)/2$, $(1-\epsilon_1)/2$, and ϵ_1, respectively. Then, she sends photons B to Bob and photons C to Carol, and records her choices of the incident states.

(3) For each photon, Bob (Carol) has two types of measurements. One measurement is along the rectilinear basis (i.e., $\{|0\rangle,|1\rangle\}$), and the other is along the diagonal basis (i.e., $\{1/\sqrt{2}(|0\rangle+|1\rangle),1/\sqrt{2}(|0\rangle-|1\rangle)\}$). He chooses between the two types with probabilities $1-\epsilon_2$ and ϵ_2, respectively. If he detects photon $B(C)$ in the state $|0\rangle$ or $1/\sqrt{2}(|0\rangle+|1\rangle)$, the result is 0; otherwise, the measurement yields the result one, and potentially reveals one bit of information. He writes down his measurement bases and the results of the measurements. The ensemble of these bits registered by both Bob and Carol is the raw key.

(4) After exchanging enough photons, Alice broadcasts on the public channel the resulting ''product state'' (P) or ''EPR state'' (E) depending on the incident state in which she has sent the pair of photons.

(5) Now, Bob and Carol tell each other the sequence of bases they used, but not the results that they obtained, and according to the result ''P'' or ''E'' announced by Alice, they decide on the compatible bases.

There are three cases in which Alice chooses the states with certain probabilities, respectively. For each of these cases, both Bob and Carol are much more likely to choose the rectilinear basis and obtain correlated bits, thus achieving a significant gain in efficiency. If Alice prepares the photons in the product states $|BC\rangle_1$ or $|BC\rangle_2$, in order to generate a sifted key, both Bob and Carol should choose the rectilinear basis. Therefore, they can generate a key bit ''0'' or ''1'' with a probability $(1-\epsilon_1)/2\cdot(1-\epsilon_2)^2$. The sifted key is also known to the center Alice. Otherwise, if either of them uses the diagonal basis, he gets the outcomes ''0'' and ''1'' with an equal probability of $\frac{1}{2}$. Otherwise, if Alice sent the photons in the EPR state $|BC\rangle_3$, this would be a modified Ekert QKD scheme between Bob and Carol. Whenever they used the same basis, they would get a sifted key with a probability $\epsilon_1[(1-\epsilon_2)^2+\epsilon_2^2]$. And the key is secret to the center. In one word, the sifted key is generated with the total probability $(1-\epsilon_2)^2+\epsilon_1\epsilon_2^2$ which goes to 1 as ϵ_2 goes to *zero*. However, due to imperfections in the transmission, and to a potential eavesdropper, there will be some errors (see Table I).

(6) Bob and Carol throw away the useless cases when they have used incompatible bases. Since the total probabilities for the two users to obtain the results ''0'' and ''1'' are equal, the ensemble of these bits of the remaining four cases is a sifted key. Therefore, the remaining cases are kept for further analysis and to generate the secret key.

(7) Bob and Carol divide up the accepted data into two subsets according to the actual bases. In one subset where the

TABLE I. Example of the two-user QKD scheme. Alice prepares pairs of photons in the known states $|00\rangle$, $|11\rangle$, and $1/\sqrt{2}(|00\rangle+|11\rangle)$. The two users choose a basis with certain probability to measure their photons and register the bit value (0 or 1), respectively. The ensemble of these bits is the raw key. Alice broadcasts on the public channel the result "product state" or "EPR state," and according to these results, the two users decide on the useful bits. Then, they keep only the bits corresponding to the compatible bases. This is the sifted key. [Here, + and × represent the rectilinear and diagonal bases, respectively, and $\Phi^+=1/\sqrt{2}(|00\rangle+|11\rangle)$.]

A state	$\|00\rangle$	$\|00\rangle$	$\|00\rangle$	$\|00\rangle$	$\|11\rangle$	$\|11\rangle$	$\|11\rangle$	$\|11\rangle$	Φ^+	Φ^+	Φ^+	Φ^+	Φ^+	Φ^+	Φ^+	Φ^+
P or *E*?	*P*	*P*	*P*	*P*	*P*	*P*	*P*	*P*	*E*	*E*	*E*	*E*	*E*	*E*	*E*	*E*
B basis	+	+	×	×	+	+	×	×	+	+	+	+	×	×	×	×
B bit value	0	0	0/1	0/1	1	1	0/1	0/1	0	1	0	1	0	1	0	1
C basis	+	×	+	×	+	×	+	×	+	+	×	×	+	+	×	×
C bit value	0	0/1	0	0/1	1	0/1	1	0/1	0	1	0/1	0/1	0/1	0/1	0	1
Compatible?	y	n	n	n	y	n	n	n	y	y	n	n	n	n	y	y
Sifted key	0				1				0	1					0	1

two users both use the rectilinear basis, they randomly pick a fixed number, say m_1 photons, and publicly compare their measurement results. The number of mismatches r_1 (here, mismatch means that the bit values of measurements are not correlated) tells them the estimated error rate $e_1=r_1/m_1$. Similarly, in the other subset where they both use the diagonal basis, they pick a fixed number, say m_2 photons, and publicly compare their measurement results. The number of mismatches r_2 gives the estimated error rate $e_2=r_2/m_2$.

Note that the test samples m_1 and m_2 are sufficiently large, the estimated error rates e_1 and e_2 should be rather accurate. Now they demand that e_1 and $e_2<e_{\max}$ where $e_{\max}$ is a prescribed maximal tolerable error rate. If these independent constraints are satisfied, they proceed to the next steps. Otherwise, they throw away the bit values of measurement and restart the whole procedure. Notice that the constraints e_1 and $e_2<e_{\max}$ are more stringent than the original naive prescription $\bar{e}<e_{\max}$ (here, $\bar{e}$ is the average error rate). We will discuss it in detail in Sec. III.

(8) If the error rates are not too high, they can use classical information processing techniques, such as error correlation and privacy amplification (see Ref. [22]), to reduce the error rates to zero, while reducing the information obtained by Eve to zero as well.

From the discussion in step (5), we know that the efficiency of the sifted key can tend to 100%. However, after some classical error correction and privacy amplification, the efficiency of the secret key cannot achieve 100%, and it depends on the error rate, which is generated by both eavesdropping and intrinsic noise due to experimental imperfections. Suppose we use a classical linear code $C(k,N,d)$ with N bits, having 2^k code words and minimum distance d as an error correction [23], and the code of minimum distance $d>2t$ is necessary if t errors are to be corrected. In what follows, we will make use of two simple bounds, the Hamming or sphere-packing bound introduced by Hamming in 1950 and the Gilbert-Varshamov bound. In the limit of large N, it takes the form

$$\left[1-H\left(\frac{d}{N}\right)\right](1-\zeta)\leqslant\frac{k}{N}\leqslant\left[1-H\left(\frac{d}{2N}\right)\right](1-\zeta), \qquad (2)$$

where $\zeta\to 0$ as $N\to\infty$, and $H(x)$ is the entropy function

$$H(x)\equiv x\log_2\frac{1}{x}+(1-x)\log_2\frac{1}{1-x}. \qquad (3)$$

So the secret key's rate approaches $k/N\times 100\%$, and is still more efficient than that of other schemes (for example, in Ref. [18], the efficiency after error correction tends to be $k/N\times 50\%$).

III. REFINED ERROR ANALYSIS

For each photon, as the choices of bases used by Bob and Carol are unknown to the eavesdropper Eve, any interaction by her will unavoidably modify the transmission and introduce some errors. She has an eavesdropping attack as below: (i) with a probability p_1 (p_2) she measures the state along the rectilinear (diagonal) basis and resends a photon according to the result of her measurement to the user; (ii) with a probability $1-p_1-p_2$ she does nothing.

Consider the error rate e_1 for the case where both Bob and Carol use the rectilinear basis. For the biased eavesdropping strategy under current consideration, errors occur only if Eve uses the diagonal basis. This happens with a *conditional* probability p_2. In this case, the polarization of the photon is randomized, thus giving an error rate

$$e_1=\frac{p_2}{2}. \qquad (4)$$

Similarly, errors for the case where both Bob and Carol use the diagonal basis happen with a *conditional* probability p_1. Thus, the error rate for this case is given,

$$e_2=\frac{p_1}{2}. \qquad (5)$$

Therefore, the users will find that, for the biased eavesdropping attack, the average error rate

$$\bar{e}=\frac{(1-\epsilon_2)^2e_1+\epsilon_1\epsilon_2^2e_2}{(1-\epsilon_2)^2+\epsilon_1\epsilon_2^2}=\frac{(1-\epsilon_2)^2p_2+\epsilon_1\epsilon_2^2p_1}{2[(1-\epsilon_2)^2+\epsilon_1\epsilon_2^2]}. \qquad (6)$$

Suppose Eve always eavesdrops only along a rectilinear basis (i.e., $p_1=1,\ p_2=0$), then

$$\overline{e}=\frac{\epsilon_1\epsilon_2^2}{2[(1-\epsilon_2)^2+\epsilon_1\epsilon_2^2]}\rightarrow 0 \tag{7}$$

as ϵ_1 or ϵ_2 tends to 0, which is similar with the result of Ref. [14]. This means that if Eve is always eavesdropping along the rectilinear basis, with a naive error analysis prescribed as $\overline{e}<e_{\max}$, Bob and Carol will fail to detect eavesdropping by Eve.

To ensure the security of our scheme, it is crucial to employ a refined data analysis: the accepted data are further divided into various subsets according to the actual bases, and the error rate of each subset is computed separately. From Eqs. (4) and (5), we can see that these error rates e_1 and e_2 depend on Eve's eavesdropping strategy, but not on the value of ϵ_1 or ϵ_2. So, the refined data analysis guarantees the security of the present scheme against the biased eavesdropping attack.

IV. PROOF OF SECURITY OF THIS QKD SCHEME

In this section, we provide a proof of security of our QKD scheme against the most general type of attack that is allowed by quantum mechanics, by generalizing the proof of the modified Lo-Chau EPR scheme proposed by Shor and Preskill [22], who related the security of the QKD to entanglement purification protocols [26] and Calderbank-Shor-Steane (CSS) codes [27] for privacy amplification and error correction.

In our scheme, EPR pairs of photons are used to ensure the security of the quantum channel between the two users. Please see Refs. [14,22,24,25] for details. The users demand that both bit- and phase-flip error rates e_1 and e_2 of the channel must be sufficiently small,

$$0\leqslant e_1,e_2\leqslant 11\%. \tag{8}$$

Then, it has been proved that both error rates of the signal are also small enough to allow the CSS code to correct.

Consider several types of attack which are probably adopted by the eavesdropper Eve. If Eve intercepts and resends the photons in one way, no matter along which basis she chooses, the measurement will unavoidably modify the transmission and introduce some errors. If Eve intercepts all pairs of photons in both ways and measures them, she might know what photons Alice sends. But when she resends the photons according to the result of her measurement to the users, she would be detected unavoidably, unless she only sends the EPR pairs of photons. However, according to the description of our scheme in Sec. II, Bob and Carol can distribute a secret key as well. That is, the quantum channel between Bob and Carol is unconditionally secure. But the channels between Alice and users are not secure, unless Alice participates in comparing the states actually sent [step (5) in Sec. II].

We remark that the proof of our scheme is based on the proof of the modified Lo-Chau EPR scheme [22], and the error correction and privacy amplification procedure that we use are exactly the same as in the Shor-Preskill proof. The point is the following: Once the error rate is shown to be correctable by a quantum (CSS) code, the procedure for error correction and privacy amplification in their proof can be carried over directly to our scheme.

V. THE CONSTRAINT ON ϵ_1 AND ϵ_2

From the above discussion, we remark that the Ekert QKD scheme is a special case of our scheme where $\epsilon_1=1$ and $\epsilon_2=\frac{1}{2}$. In a general case, however, the bases used by the two users are compatible with a probability $(1-\epsilon_2)^2+\epsilon_1\epsilon_2^2$, which goes to 1 as ϵ_2 goes to *zero*, either. Because of decoherence in the preparation, transmission, and storage, the EPR states unavoidably degenerate to mixed entangled states. So the value of ϵ_1 should be small enough to decrease the proportion of the EPR state in the incident states. But to guarantee the security of this scheme it cannot be *zero*.

From Sec. II, we know the value of ϵ_2 should be small but cannot be *zero*. The limit $\epsilon_2\rightarrow 0$ is singular, as the scheme is obviously insecure when $\epsilon_2=0$. The main constraint on ϵ_2 is that there should be enough photons for an accurate estimation of the error rates e_1 and e_2. We assume that N pairs of photons are chosen by Alice, i.e., N photons are transmitted from Alice to Bob and Carol, respectively. On average, for $|BC\rangle_3$ only $N\epsilon_1\epsilon_2^2/4$ photons belong to the case where both Bob and Carol use the diagonal basis. To estimate e_2 reasonably accurately, the number $N\epsilon_1\epsilon_2^2/4$ should be larger than some fixed number such as m_2. The key point to note is that this number m_2 depends on e_2 and the desired accuracy of the estimation but *not* on N. (Indeed, the number m_2 can be computed from classical statistical analysis.) So,

$$N\epsilon_1\epsilon_2^2/4\geqslant m_2,$$

$$\epsilon_1\epsilon_2^2\geqslant 4m_2/N. \tag{9}$$

As N tends to ∞, ϵ_2 can tend to *zero*, but never reach it, and the efficiency of this scheme is 100% asymptotic.

VI. THE GENERATION OF A QUANTUM RANDOM NUMBER

In our efficient QKD scheme, true quantum random numbers are required widely. We present a realization of a physical quantum random number generator based on the process of splitting a beam of photons on a polarizing beam splitter (PBS), a quantum mechanical source of true randomness. The device is similar to that proposed in Refs. [28,29]. Of course, there is some difference.

The principle of operation of the random generator is shown in Fig. 1. It works as follows: If each individual photon coming from the light source is polarized at 45° by a polarizer and then travels through the PBS, it has an equal probability of being detected in the H (horizontal) polarization or V (vertical) polarization. Quantum theory predicts that the individual ''decisions'' are truly random and independent of each other. In our device, this feature is imple-

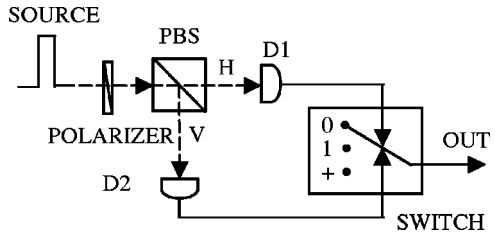

FIG. 1. The device of a quantum random number generator. The source of randomness in this device is the splitting of a weak coherent light pulse. It is realized by a 50:50 optical polarizing beam splitter (PBS). Before traveling into the PBS, the incoming light is polarized at 45° with the polarizer. There are two single-photon detectors $D1$ and $D2$, which toggle the switch among it three states.

mented by detecting the polarizations of photons in the two output beams with single-photon detectors and combining the detection pulse in a toggle switch, which has three states, 0, 1, +. If only the detector $D1$ fires, it means that there is one photon traveling through the PBS and it is in the H polarization. Then, the switch is flipped to state 0 and left in the state until the next detection in the other two states. If only the detector $D2$ fires, the photon traveling through the PBS is in the V polarization, and the switch will be flipped to the state 1 and left in the state till an event of the next different detection. Otherwise, if the two detectors both fire, it means that there are two photons with orthogonal polarizations traveling through the PBS simultaneously. Then, the switch is flipped to the state + and left until the next different detections. In practice, the several detections occur in a row in the same detector, then only the first detection will toggle the switch into the corresponding state, and the following detections leave the switch unaltered. Consequently, the toggling of the switch among the three states constitutes a ternary random signal with the randomness depending on the times of the transitions among the three states. If a binary random number is required, we only take the first two cases into account, i.e., the toggle switch only needs two states. Moreover, we can adjust the polarizer and let the photon in the state $\sqrt{1-\epsilon}|H\rangle+\sqrt{\epsilon}|V\rangle$. Thus, we can get a sequence of the binary random number with a different probability.

The light source can be an adjustable current coherent light pulse. We choose the random numbers which Alice used by way of example. She prepares the pairs of photons in the three states with probabilities $(1-\epsilon_1)/2$, $(1-\epsilon_1)/2$, and ϵ_1, respectively. Suppose that the light coming from the source is in the coherent state, which may be expanded in terms of the number states as

$$|\alpha\rangle=\exp\left(-\frac{1}{2}|\alpha|^2\right)\frac{\alpha^n}{\sqrt{n!}}|n\rangle, \tag{10}$$

where $|n\rangle$ is the Fock state. We note that the probability distribution of photons in this state is a Poisson distribution as

$$P(n)=|\langle n|\alpha\rangle|^2=\frac{|\alpha|^{2n}e^{-|\alpha|^2}}{n!}, \tag{11}$$

where $|\alpha|^2$ is the average number of the photons $\bar{n}$. Hence, in a pulse, the probability of the case where two photons are traveling through the PBS and incident to the same detector is given as $P(2)=(|\alpha|^4e^{-|\alpha|^2})/2$ (ignoring higher-order terms). Only if they have orthogonal polarizations, are they detected by both $D1$ and $D2$ with the probability $P(2)/2=|\alpha|^4e^{-|\alpha|^2}/4$. Similarly, if only one detector fires, the probability is shown as $P(1)+P(2)/2=|\alpha|^2e^{-|\alpha|^2}+|\alpha|^4e^{-|\alpha|^2}/4$, where the second term corresponds to the case where two photons have the same polarization. Hence, the ratio of the probabilities three states required in our QKD scheme is obtained as

$$\frac{\epsilon_1}{1-\epsilon_1}=\frac{P(2)/2}{P(1)+P(2)/2}=\frac{\bar{n}}{\bar{n}+4}. \tag{12}$$

Then, we gain the relationship between the average number of the photons and the probability ϵ_1:

$$\epsilon_1=\frac{\bar{n}}{2\bar{n}+4}. \tag{13}$$

By tuning the average number of the photons of the pulse, we can obtain the proper sequence of a ternary quantum random number. Since the random number generator is based on a basic quantum process, similar to Refs. [29,30], we also apply an autocorrelation test in order to check the randomness of the output. Apart from a small correlation between successive bits, which is explained and can be eliminated, the generator behaves like a perfect random source.

VII. A QUANTUM CRYPTOGRAPHY NETWORK

In this section, we combine the efficient QKD scheme and the use of a device called the ''space optical switch'' to present a *cascaded* quantum cryptography network. In the other schemes, an individual key can be established between a trusted center and each of the users. Our scheme can realize the QKD between arbitrary two users in the cascaded loop local networks. Unlike the scheme of Ref. [20], a quantum memory owned by the center is not needed in this scheme. What our scheme needs is shown as follows (see Fig. 2). (i) *Cascaded* loop local networks. Between two of these loops, there are two fibers linking them. (ii) A trusted center. In one of the loops (called loop 1), a trusted center Alice prepares pairs of photons in the three known nonorthogonal states with certain probabilities, respectively. (iii) Users. Linked via coupled fibers, the legitimate users are scattered around each loop. (iv) Switches. At each node, both among the loops and between the users and the loops, there are many ''space optical switches'' installed, which are often closed. Whenever a secret key is applied to be established, it causes the photons to be received by the proper users via fibers.

In a general case, suppose that the user $M(i)$ in loop M and the user $N(j)$ in loop N (suppose $M>N$) wish to agree on a secret key. After verifying the identification of the two users, the center Alice prepares and sends pairs of photons from contrary directions. After that, switches $A1$,

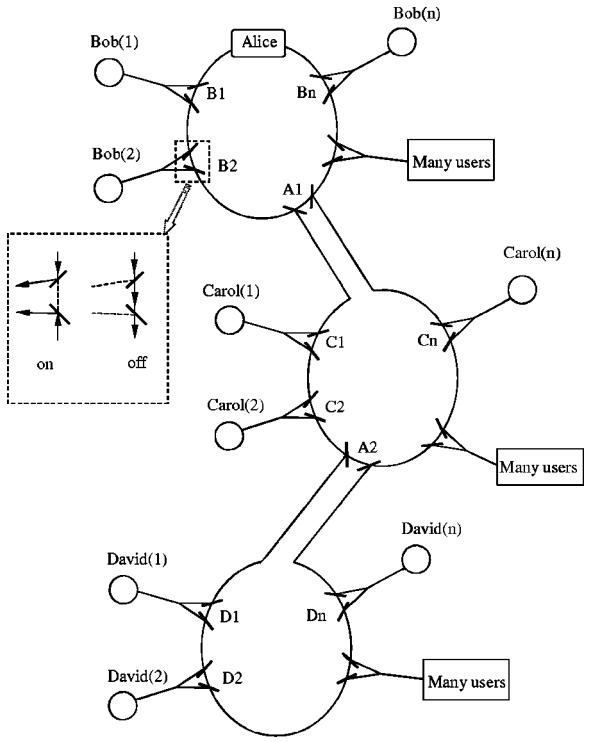

FIG. 2. A *cascaded* quantum cryptography network based on the efficient QKD scheme. There are many loop local networks. Alice plays the roles of the center and superuser in loop 1, the users of the network are linked with their loop by the coupling fibers. Between two loops, there are two fibers linking them. By the ''space optical switch,'' the photons can be received by the right users.

$A2\cdots A(m-1)$, and Mi, Nj open successively, the other switches are still closed. Then, they can establish the QKD.

The link of two consecutive loops needs two fibers; thus pairs of photons can be transmitted to the lower loop simultaneously, then received by the right users. Since the states will be measured directly when the photon is obtained by the user, the link of the user and loop needs only one coupled fiber. Yet, there are still two switches at the node between the user and its loop, which allows the user to be able to receive the photons from contrary directions.

VIII. CONCLUSION

In summary, we propose a QKD scheme with three nonorthogonal states. Combined with the idea presented by Lo *et al*. [14], the efficiency of this scheme is increased to tend to be 100% by the way in which the users choose the bases with the different probabilities, respectively. The security of the QKD scheme is based on the fundamental postulate of quantum physics that a ''nonorthogonal state cannot be cloned.''

To make the scheme secure against the dominant basis eavesdropping attack, it is crucial to have a refined error analysis in place of a naive error analysis. We separate the accepted data into various subsets according to the basis employed and estimate an error rate for each subset separately. It is only when all error rates are small enough that the security of transmission is accepted. Then we provide a proof of security of our QKD scheme against the most general type of attack by generalizing Shor and Preskill's proof of security of the other schemes [22]. In addition, we present a realization of a quantum random number generator.

Then, based on the scheme, we present a *cascaded* quantum cryptography network with the addition of a device ''space optical switch.'' Furthermore, since the proportion of EPR states in the incident states would be so small that all the key bits can be used to detect the eavesdropper, we will not worry about the increasing of the error rate brought by the preparation, transmission, and storage of the EPR states, whereas the techniques needed by our scheme, such as the ''space optical switch,'' the quantum random number generator, the preparation and measurement of the photons are easy to be realized experimentally. So, our scheme may be implemented in practice.

ACKNOWLEDGMENT

This work was supported by the National Natural Science Foundation of China.

[1] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175.
[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1992).
[3] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
[4] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[5] C. H. Bennett, F. Bessette, G. Brassard, L. Savail, and J. Smolin, J. Cryptology **5**, 3 (1992).
[6] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **84**, 4729 (2000).
[7] D. S. Naik, C. G. Peterson, A. G. White, A. J. Berglund, and P. G. Kwiat, Phys. Rev. Lett. **84**, 4733 (2000).
[8] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, Phys. Rev. Lett. **84**, 4737 (2000).
[9] J. S. Bell, Physics (Long Island City, N.Y.) **1**, 195 (1965).
[10] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).
[11] D. Dieks, Phys. Lett. A **92**, 271 (1982).
[12] W. K. Wootters and W. Zurek, Nature (London) **299**, 802 (1982).
[13] M. Ardehali, H.-F. Chau, and H.-K. Lo, e-print arXiv: quant-ph/9803007.
[14] H.-K. Lo, H.-F. Chau, and M. Ardehali, e-print arXiv: quant-ph/0011056.
[15] R. J. Hughes, G. L. Morgan, and C. G. Peterson, J. Mod. Opt. **47**, 533 (2000); P. Townsend, Opt. Fiber Technol.: Mater., Devices Syst. **4**, 345 (1998), and references therein.
[16] W. T. Buttler *et al.*, Phys. Rev. Lett. **84**, 5652 (2000); B. C. Jacobs and J. D. Franson, Opt. Lett. **21**, 1854 (1996).
[17] M. Zuckowski, A. Zeilinger, M. Horne, and H. Weifurter, Acta Phys. Pol. A **93**, 187 (1998).

[18] M. Hillery, V. Buzek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).
[19] W. Tittel, H. Zbinden, and N. Gisin, Phys. Rev. A **63**, 042301 (2001).
[20] E. Biham, B. Huttner, and T. Mor, Phys. Rev. A **54**, 2651 (1996).
[21] P. D. Townsend, S.J. D. Phoenix, K. J. Blow, and S. M. Barnett, Electron. Lett. **30**, 1875 (1994); P. D. Townsend and K. J. Blow, European Patent Application EP93307121.9, September 1993; P. D. Townsend and D. W. Smith, European Patent Application EP93307121.0, September 1993; P. D. Townsend, Electron. Lett. **33**, 188 (1997); S. J. D. Phoenix, S. M. Barnett, P. D. Townsend, and K. J. Blow, J. Mod. Opt. **42**, 1155 (1995).
[22] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[23] D. Gottesman, Phys. Rev. A **54**, 1862 (1996).
[24] H.-K. Lo and H.-F. Chau, Science **283**, 2050 (1999).
[25] D. Mayers, J. Assoc. Comput. Mach. (to be published), e-print arXiv: quant-ph/9802025; preliminary version in *Advances in Cryptology—Proceedings of Crypto '96* (Springer-Verlag, New York, 2000), p. 715.
[26] C. H. Bennett, D. P. Di Vincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
[27] A. R. Calderbank and P. Shor, Phys. Rev. A **54**, 1098 (1996); A. M. Steane, Proc. R. Soc. London, Ser. A **452**, 2551 (1996).
[28] T. Jennewein, U. Achleitner, and G. Weihs, H. Weinfurter, and A. Zeilinger, e-print arXiv: quant-ph/9912118.
[29] A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, J. Mod. Opt. **47**, 595 (2000).
[30] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, Phys. Rev. A **53**, 2046 (1996).