Secure direct communication with a quantum one-time pad

Fu-Guo Deng[1,2] and Gui Lu Long[1,2,3,4]
[1]*Department of Physics, Tsinghua University, Beijing 100084, China*
[2]*Key Laboratory For Quantum Information and Measurements, Beijing 100084, China*
[3]*Center for Atomic and Molecular NanoSciences, Tsinghua University, Beijing 100084, China*
[4]*Center For Quantum Information, Tsinghua University, Beijing 100084, China*
(Received 31 October 2003; published 17 May 2004)

Quantum secure direct communication is the direct communication of secret messages without first producing a shared secret key. It may be used in some urgent circumstances. Here we propose a quantum secure direct communication protocol using single photons. The protocol uses batches of single photons prepared randomly in one of four different states. These single photons serve as a one-time pad which is used directly to encode the secret messages in one communication process. We also show that it is unconditionally secure. The protocol is feasible with present-day technique.

DOI: 10.1103/PhysRevA.69.052319 PACS number(s): 03.67.Hk, 03.65.Ud

Quantum key distribution (QKD) provides a novel way for two legitimate parties to establish a common secret key over a long distance. Its ultimate advantage is its unconditional security, the feat in cryptography. Combining with the one-time pad scheme in which the private key is as long as the messages, secret messages can be communicated safely from one place to another place. QKD has progressed quickly [1] since Bennett and Brassard designed the original QKD protocol (BB84) [2].

Recently, a novel concept, quantum secure direct communication (QSDC) was proposed and pursued [3–6]. Different from QKD whose object is to establish a common random key between the two remote parties of communication, QSDC is to transmit the secret message directly without first creating a key to encrypt them. In 2002, Beige *et al.* presented a QSDC scheme based on single-photon two-qubit states [3]. In this scheme the message can be read after a transmission of an additional classical information for each qubit, which is similar to a QKD scheme as each bit of key can represent one bit of secret message with an additional classical information, i.e., retaining or flipping the bit value in the key according to the secret message. Boström and Felbinger put forward a ping-pong QSDC scheme [4] using Einstein-Podolsky-Rosen (EPR) pairs [7] as quantum information carriers. It is secure for key distribution, but is only quasisecure for direct secret communication if perfect quantum channel is used. However it is insecure even for QKD if it is operated in a noisy quantum channel, as shown by Wójcik [8]. The ping-pong protocol can be modified for secure QKD by taking into account the procedures proposed by Wójcik [8]. Cai found that the ping-pong scheme can be attacked without eavesdropping [9]. Meanwhile, we proposed a two-step secure QSDC protocol with EPR pairs transmitted in block [5] by modifying a QKD protocol based on EPR pairs [10]. In Ref. [6], Cai modifies the ping-pong scheme by replacing the entangled photons with single photons in mixed state. However it is unsafe in a noisy channel, and is vulnerable to the opaque attack [11].

QSDC may be important in some applications. For instance when the transmission time is urgent, or the transmission may be subject to the danger of destruction. Furthermore, as the technologies for quantum information improves, the efficiency of quantum transmissions may be greatly increased compared to the low rate transition in present-day laboratories, then secure direct quantum communication may well become highly demanded and become an elegant means for secret communication.

In this paper, we propose a QSDC scheme that uses single photons in batches. The states of the single photons themselves serve as a one-time pad, and they are encoded with the secret message by two different unitary operations. The scheme may be viewed as a modification of the well-known BB84 QKD scheme. Comparing with protocols using EPR pairs, this scheme is practical and well within the present-day technology. All in all, it inherits the unconditional security merit of the BB84 QKD scheme, and renders it an attractive choice in practical applications. Here we first present our QSDC protocol, then we analyze its security by reducing it to the BB84 QKD protocol.

The security of QKD is the capability of the users to detect eavesdropping. If no eavesdropping is detected or the eavesdropping is negligible, the transmissions are retained, and after some treatment, a sequence of secret key is produced. Otherwise the transmissions are abandoned. However the requirement for secure direct quantum communication is even higher. In addition to the ability to detect eavesdropping, the users must ensure that the secret messages encoded do not leak to eavesdropper before she is detected. For instance in a noiseless channel, the ping-pong protocol is secure for quantum key distribution, but is insecure for direct communication as it does not satisfy the second requirement and some message has already leaked to Eve, the eavesdropper, before she is detected.

Here we first describe the details of our quantum-one-time pad QSDC scheme. Suppose Alice wants to transform a secret message to Bob. Similar to the BB84 QKD protocol [2], Alice and Bob use two measuring bases (MB), namely, the rectilinear basis, i.e., $\{|H\rangle=|0\rangle, |V\rangle=|1\rangle\}$ and the diagonal basis, i.e., $\{|u\rangle=1/\sqrt{2}(|0\rangle+|1\rangle), |d\rangle=1/\sqrt{2}(|0\rangle-|1\rangle)\}$ where $|H\rangle$ and $|V\rangle$ are the horizontal and vertical polarization states, respectively. As in the BB84 QKD protocol, the $|0\rangle$ and $|u\rangle$

states represent the binary value 0, and the $|1\rangle$ and $|d\rangle$ states represent binary value 1. For simplicity we call them the plus-measuring basis (plus-MB) and the cross-measuring basis (cross-MB), respectively. We assume ideal noiseless channel first. The case with a noisy channel will be discussed later. The quantum-one-time pad QSDC protocol contains two phases.

(1) The secure doves sending phase. Bob prepares a batch of polarized single photons and sends the photons to Alice. Each photon is randomly in one of the four polarization states: $|H\rangle$, $|V\rangle$, $|u\rangle$ and $|d\rangle$. We call this batch of photons at this stage, the *A*-batch photon as it goes toward Alice. After receiving the batch of photons, Alice and Bob check eavesdropping by the following procedure. Alice selects randomly a sufficiently large subset of photons from the *A* batch, which we call the *S* batch, and she measures each of them using one of the two measuring bases randomly. Alice tells Bob the positions, and the measuring basis and the result of the measurement for each of the sampled photons in the *S* batch. With this knowledge, Bob can determine, through the error rate, whether there is any eavesdropping. The photons leftover in the *A* batch after the eavesdropping are called the *B* batch. Apparently, the *B* batch is the difference set of the *A* batch and the *S* batch: $B=A-S$. If the error rate is high, Bob concludes that the channel is not secure, and the communication is halted. Otherwise, Alice and Bob continue to the next phase. This is just like that Bob sends a batch of doves to Alice for carrying the message back. This is similar to *ping* in the ping-pong protocol, but instead of a single ping, our protocol uses a batch of *pings*. In addition to operating in batches, another major difference between our protocol and the Cai protocol [6] is that we use four states, but only the $|H\rangle$ and $|u\rangle$ states are used in Cai's protocol at this phase, and this makes the Cai protocol insecure under an opaque attack [11].

(2) The message coding and doves returning phase. After the security of the *B* batch is completed, Alice encodes each of the photons in the *B* batch with one of the two unitary operations, $I=|0\rangle\langle 0|+|1\rangle\langle 1|$, and $U=i\sigma_y=|0\rangle\langle 1|-|1\rangle\langle 0|$, respectively, according to the secret message. If the secret message is 0, then operation *I* is performed, and if it is a 1 the $i\sigma_y$ operation is performed, the same as that in Ref. [6]. The nice feature of the *U* operation is that it flips the state in both measuring bases,

$$U|0\rangle = -|1\rangle, \quad U|1\rangle = |0\rangle, \tag{1}$$

$$U|u\rangle = |d\rangle, \quad U|d\rangle = -|u\rangle. \tag{2}$$

After encoding the photons in the *B* batch, Alice returns them to Bob. As the *A* batch is prepared by Bob, Bob knows the measuring basis, and the original state of each photon in the *B* batch. He uses the same measuring basis when he prepared the photon to measure the photon, and reads out the secret messages directly. To guarantee the security of the whole communication process, it is necessary for Alice to use randomly some of the *B*-batch photons as checking instances. She will announce publicly the positions and the coded bit values of these checking photons after the transmission of a batch is completed. This measure gives Alice and Bob an estimate whether there is an Eve in the line to intercept their communication. But Eve can only interrupt their transmission in this phase and could not get any useful information about the secret message since Eve cannot get any useful information during the *B*-batch transmission, in the same way as in the two-step protocol [5].

We now discuss the unconditional security of this quantum-one-time pad QSDC scheme. First we notice that the encoding of secret messages in the second phase (doves returning phase) is identical to the process in a one-time pad encryption where the text is encrypted with a random key as the state of the photon in the *B* batch is completely random. In a one-time pad encryption, it is completely safe and no secret messages can be leaked even if the cipher text is intercepted by the eavesdropper. Here the quantum-one-time pad QSDC protocol is even more secure than the classical one-time pad in the sense that an eavesdropper cannot even intercept the whole cipher text as the photons' measuring basis is chosen randomly. Thus the security of this QSDC protocol depends entirely on the first step when Bob sends the *A* batch to Alice.

The process for ensuring a secure *A* batch of photons is similar to that in BB84 QKD protocol. The difference between this protocol and BB84 QKD is that the *B*-batch photons are stored, whereas all the photons are measured one by one in the BB84 QKD scheme. The security of BB84 QKD is assured by means that Alice and Bob choose randomly sufficient instances for checking eavesdropping. The process of the QSDC scheme before Alice encodes her message using the unitary operation is in fact identical to the BB84 QKD process. The BB84 QKD has been proven unconditionally secure by several groups [12]. The BB84 QKD protocol is secure even when the channel is noisy. In this way, the process for establishing a secure quantum channel in this QSDC scheme is proven unconditionally secure by this observation.

The Holevo bound states that the mutual information between Bob and Eve satisfies [13]

$$H(B{:}E) \leqslant S(\rho) - \sum_x P_x S(\rho_x), \tag{3}$$

where $\rho=\Sigma_x P_x \rho_x$ and ρ_x is a quantum state prepared by Bob with probability P_x, and is the Von Neumann entropy of state ρ_i [13]. If Bob prepares the four states, $|H\rangle$, $|V\rangle$, $|u\rangle$, and $|d\rangle$ symmetrically, then the binary entropy of states prepared by Bob is $H(B)=\Sigma_x - P_x \log_2 P_x = 2$. Thus we have

$$H(B{:}E) \leqslant S(\rho) - \sum_x P_x S(\rho_x) < H(B). \tag{4}$$

That is to say, Alice and Bob can share a sequence of quantum states securely [13].

The essential difference between this protocol and the ping-pong protocol [4] and its variant [6] is that the security of the quantum channel is analyzed first in a batch after batch manner and the encoding of the message is done only after the confirmation of the security of the quantum channel, while in the ping-pong protocols the security check and the encoding of messages are done concurrently. Since the security of the channel is insured first in this quantum one-time pad protocol, Eve can get nothing even though she monitors the rest of the process of communication. Another major difference between our protocol and the Cai protocol is the different sets of states in the doves sending phase. The asymmetry of the $|0\rangle$ and $|1\rangle$ components in Cai's protocol makes it insecure under the opaque attack.

In the implementation of this quantum-one-time pad QSDC protocol, single photon source and the technique for storing quantum states are required. These techniques are principally available, for instance, the single photon source [14], information storage through electromagnetic induced transparency [15]. Of course, they still need further improvement for perfection for realistic applications. At present, this protocol can be implemented with existing techniques. The storage of photons can be done by optical delays in a fibre as has been proposed in Ref. [5], shown in Fig. 1. In practice, there are also losses in the transmission lines, error correcting techniques are necessary. There have already been quite a few good correcting codes, for instance, in Refs. [16–18]. In fact, many of the state of art experimental QKD setups use the Faraday mirrors where the photons are sent to one party and then returned back to the sender. It is quite possible that these setups may be adapted to realize this QSDC protocol.

Before we conclude, it is worthwhile to inspect the basic requirements for quantum secure direct communication. First, eavesdropping check before the message being encoded must be performed first. This is necessary for secure communication. Secondly, since eavesdropping can only be performed through sampling, it is necessary to perform the communications in a batch after batch manner. A batch of single photons is transmitted first from one place to another place. Its security is assured by sampling a sufficiently large subset of instances from the batch. Then this secured batch is used to encode the secret message and transmitted to the other location.

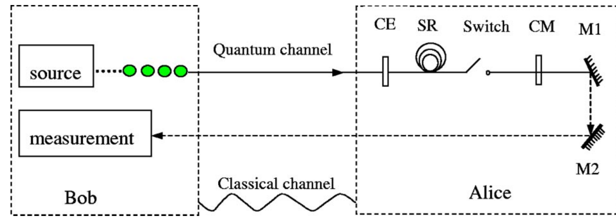

FIG. 1. Implementation of the QSDC with optical delays. CE is the eavesdropping check; SR represents an optical delay; switch is used to control the quantum communication process, if the batch of photons is safe, the switch is on and the message coding is performed; CM encodes the secret message, *M*1 and *M*2 are two mirrors in this simple illustrative setup.

Finally, it is seen here that quantum secure direct communication does not necessarily need EPR pairs as the information carrier, therefore quantum entanglement and nonlocality are not the necessary requirements for QSDC.

This work is supported by the National Fundamental Research Program Grant No. 001CB309308, China National Natural Science Foundation Grant Nos. 60073009, 10325521, 10244003, the Hang-Tian Science Fund and the SRFDP program of Education Ministry of China.

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[2] C. H. Bennett, and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–179
[3] A. Beige, B.-G. Englert, Ch. Kurtsiefer, and H. Weinfurter, Acta Phys. Pol. A **101**, 357 (2002).
[4] K. Boström and T. Felbinger, Phys. Rev. Lett. **89**, 187902 (2002).
[5] F. G. Deng, G. L. Long, and X. S. Liu, Phys. Rev. A **68**, 042317 (2003).
[6] Q. Y. Cai, e-print quant-ph/0304033.
[7] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).
[8] A. Wójcik, Phys. Rev. Lett. **90**, 157901 (2003).
[9] Q. Y. Cai, Phys. Rev. Lett. **91**, 109801 (2003).
[10] G. L. Long and X. S. Liu, Phys. Rev. A **65**, 032302 (2002).
[11] The details will be published elsewhere. The opaque attack was discussed by C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992). In short, Eve uses the following attack: she intercepts every photon and measures them with an unorthogonal basis. If she obtains a result, she prepares a fake photon and sends it to Bob. If she does not get a result for her measurement, she simply blocks the photon. This of course results in an increase in loss, and Eve can compensate the loss by replacing the noisy channel with a noiseless channel.
[12] D. Mayers, e-print quant-ph/9802025; H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999); P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 411 (2000); D. Mayers, Eur. Phys. J. D **18**, 161 (2002); E. Biham, M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury, e-print quant-ph/9912053; N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000); M. Koashi and J. Preskill, e-print quant-ph/0208155; D. Gottesman, H. K Lo, N. Lütkenhaus, and J. Preskill, e-print quant-ph/0212066.
[13] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, UK, 2000).
[14] For a review, see C. Brunel, B. Lounis, P. Tamarat, and M. Orrit, Phys. Rev. Lett. **83**, 2722 (1999); P. Michler, A. Kiraz, C. Becher, W. V. Schoenfeld, P. M. Petroff, L. Zhang, E. Hu, and A. Imamoğlu, Science **290**, 2282 (2000); Z. Yuan, B. E. Kardynal, R. M. Stevenson, A. J. Shields, C. J. Lobo, K. Cooper, N. S. Beattie, D. A. Ritchie, and M. Pepper, *ibid.* **295**, 102 (2002); A. Kuhn, M. Hennrich, and G. Rempe, Phys. Rev. Lett. **89**, 067901 (2002); A. L. Migdall, D. Branning, and S. Castelletto, Phys. Rev. A **66**, 053805 (2002); W. Nakwaski, R. P. Sarzała, M. Wasiak, T. Czyszanowski, and P. Maćkowiak,

Opto-Electron. Rev. **11**, 127 (2003).
[15] C. Liu, Z. Dutton, C. H. Behroozi, and L. V. Hau, Nature (London) **409**, 490 (2001); D. F. Phillips, A. Fleischhauer, A. Mair, R. L. Walsworth, and M. D. Lukin, Phys. Rev. Lett. **86**, 783 (2001).
[16] G. Brassard and L. Salrail, *Euro-crypt 193*, Lectures Notes in Computer Sciences Vol. 765 (Springer-Verlag, New York, 1994), pp. 410–423
[17] A. R. Calderbank and P. W. Shor, Phys. Rev. A **54**, 1098 (1996); P. W. Shor, *ibid.* **52**, R2493 (1995); A. M. Steane, Phys. Rev. Lett. **77**, 793 (1996); A. M. Steane, Proc. R. Soc. London, Ser. A **452**, 2551 (1996); A. M. Steane, Phys. Rev. A **54**, 4741 (1996).
[18] K. Q. Feng, IEEE Trans. Inf. Theory **48**, 2384 (2002).