Quantum data hiding with spontaneous parameter down-conversion

Guang-Can Guo and Guo-Ping Guo*
Key Laboratory of Quantum Information, University of Science and Technology of China, Chinese Academy of Science, 230026 Hefei, Anhui, People's Republic of China

(Received 11 March 2003; published 23 October 2003)

Here we analyze the practical implications of using Bell states produced through optical down-conversion in a quantum-data-hiding protocol. We show that the uncertainty in the production of Bell states through spontaneous parametric down-conversion should be taken into account, because it will cause difficulties for the encoding procedure. A set of extended Bell states and a generalized Bell-state analyzer are proposed to describe and analyze the possible states of two photons distributed in two paths. Then we present a method to integrate the above uncertainty of Bell-state preparation into the data-hiding procedure, when we encode the secret with the set of extended Bell states. These modifications greatly simplify the hider's encoding operations, and thus pave the way for the implementation of quantum data hiding with present-day quantum optics.

DOI: 10.1103/PhysRevA.68.044303 PACS number(s): 03.67.Hk, 03.65.Ud

It is well known that quantum mechanics can keep classical and quantum bits secret in a number of different circumstances. In some scenarios, the bits are kept secret from eavesdropper, while in others they are kept secret from participants themselves.

Quantum key distribution [1–6] is the first such example, which keeps messages secret from any eavesdropper accessing the output of the quantum channel. As the quantum generalization of the one-time pad, it is also known as private quantum channel and is most near practical application. In this case, two parties make use of shared random bits to create a secure quantum channel between them. Then they can safely transmit messages with this secure quantum channel. A second example is quantum secret sharing [7,8], which aims to share a secret, in the form of classical or quantum bits, among many parties. Only certain prescribed combinations of the parties, known as authorized sets, are capable of fully reconstructing the secret with the assistance of local operations and classical communications. Nothing at all can any unauthorized combination learns about the secret, even though they can act jointly on their shares or have quantum communications. The third example is the quantum data hiding recently proposed by Terhal and her cooperators [9–11], which discusses a different security problem in the quantum information field and explores another application.

Although quantum data hiding also aims to share a secret between biparty or multiparty, it imposes a much stronger security criterion than quantum secret sharing. In the quantum-data-hiding protocols, quantum communications or channels are prerequisite, even for authorized sets, to reveal the secret. In Terhal's original protocol of hiding classical bits, n pairs of Bell states are shared between two parties, Alice and Bob. For each Bell state, the first qubit goes to Alice and the second to Bob. The secret is encoded in the number of the state $|\Psi\rangle^-$ among those n pairs of Bell states, whose even numbers represent 0 and odd numbers denote 1. The substantial information, which the two sharers could get about the secret through any sequence of local quantum operations supplemented by unlimited two-way classical communication (LOCC), is exponentially small in n, the number of Bell states used for encoding. Later, generalized schemes for hiding classical data in multipartite quantum states and hiding quantum data have also been proposed [10,11]. Furthermore, two significant conclusions have been made, which provide the basic descriptions for the problem of quantum data hiding. Perfect quantum data hiding is impossible and the quantum data hiding with pure states is impossible. In addition, Terhal *et al.* discussed the implementation of the Bell-states quantum-data-hiding protocol by virtue of current quantum optics setup, such as optical down-converter.

Here, we particularly analyze the experimental implications of this Bell-states quantum-data-hiding protocol with optical down-converter. We show that the uncertainty in producing of the Bell states with spontaneous parameter down-conversion should be taken into account, because it will cause serious trouble to the hider encoding procedure. Subsequently, we propose a set of extended Bell-states and a generalized Bell states analyzer to describe and analyze the possible states of two photons distributing along two paths. Then we present a method to elegantly integrate the above uncertainty of Bell states preparation into the data-hiding procedure and encode the secret in a set of the extended Bell states. Compared to the rigorous security proof for the original quantum data hiding protocol with Bell states, this modified quantum-data-hiding protocol can be straightforwardly argued to maintain similar security. It paves the way for the experimental implementation of the quantum data hiding with present-day quantum optics.

In Terhal's original quantum-data-hiding scheme [9], they proposed to hide bits in a series of Bell states produced with optical down-converter. The hider is assumed to have a supply of each of the four Bell states. When the one-bit secret $b=1$, the hider picks at random a set of n Bell states with uniform probability except that the number of singlets $|\Psi\rangle^-$ must be odd. The $b=0$ protocol is the same, except that the number of singlets must be even. It is well known that the

*Electronic address: harryguo@mail.ustc.edu.cn

state produced with the parameter down-conversion is not a Bell state, but a superposition of the vacuum, a two-photon Bell state, a four-photon state, etc. In fact, this state can be generally written as (unnormalized)

$$|\Sigma\rangle=\left[1+p^{1/2}a_{ij}^{\dagger}+\frac{(p^{1/2}a_{ij}^{\dagger})^2}{2}+o(p)\right]|\mathrm{vac}\rangle. \tag{1}$$

Here p is the probability of producing a pair of Bell state $|\Psi\rangle_{ij}^{-}=a_{ij}^{\dagger}|\mathrm{vac}\rangle=1/\sqrt{2}(h_i^{\dagger}v_j^{\dagger}-v_i^{\dagger}h_j^{\dagger})|\mathrm{vac}\rangle$, where h and v are the two polarization mode operators of photon, $o(p)$ represents the terms to produce more down-conversion photons, whose probabilities are smaller than p^2, and $|\mathrm{vac}\rangle$ is the vacuum state of the down-conversion photons. Obviously, the hider cannot exactly ascertain when the down-converter produce photons and whether these photons are in the Bell state $|\Psi\rangle^{-}$. As introducion of postselection measurements will make quantum-data-hiding meaningless, this uncertainty will cause serious problem for the encoding of the quantum-data-hiding scheme. It will be very difficult for the hider to pick out n pairs of Bell states and to ensure that there are exactly even or odd number of singlets among these states. Although a device of quantum nondemolition measurement for Bell states [12] can resolve this problem, the requirement for the uncommon individual photons CNOT gates or single-photon sources [13] renders it beyond the reach of the present experimental conditions.

To cope with this uncertainty in the generation of Bell states, we can modify the above quantum-data-hiding protocol in the following way. Consider an experimental optics setup as shown in Fig. 1. Generally, a pulse of ultraviolet (UV) light passing through a nonlinear crystal creates a pair of entangled photons in paths 1 and 2. After retroflection, the ultraviolet pulse creates another pair of photons in paths 3 and 4 during its second passage through the crystal. In view of the uncertainty for the parameter down-conversion, the total state of photons in paths 1, 2, 3, and 4 could be written in the following form (unnormalized):

$$\begin{aligned}|\Xi\rangle&=\left(1+p^{1/2}a_{12}^{\dagger}+\frac{(p^{1/2}a_{12}^{\dagger})^2}{2}+o(p)\right)\\&\quad\otimes\left(1+p^{1/2}a_{34}^{\dagger}+\frac{(p^{1/2}a_{34}^{\dagger})^2}{2}+o(p)\right)|\mathrm{vac}\rangle\\&=\left[1+p^{1/2}(a_{12}^{\dagger}+a_{34}^{\dagger})+p\left(a_{12}^{\dagger}a_{34}^{\dagger}+\frac{(a_{12}^{\dagger})^2}{2}+\frac{(a_{34}^{\dagger})^2}{2}\right)\right.\\&\quad\left.+o(p)\right]|\mathrm{vac}\rangle,\end{aligned} \tag{2}$$

where $a_{ij}^{\dagger}=1/\sqrt{2}(h_i^{\dagger}v_j^{\dagger}-v_i^{\dagger}h_j^{\dagger})$ is the creation operator for the singlet state $|\Psi\rangle^{-}$, and $|\mathrm{vac}\rangle$ is the vacuum state of the four paths. Obviously, we have a probability of the order of p^2 to have totally four photons in the four paths 1, 2, 3, and 4, which are in the state (unnormalized):

$$|\Theta\rangle=\left(a_{12}^{\dagger}a_{34}^{\dagger}+\frac{(a_{12}^{\dagger})^2}{2}+\frac{(a_{34}^{\dagger})^2}{2}\right)|\mathrm{vac}\rangle. \tag{3}$$

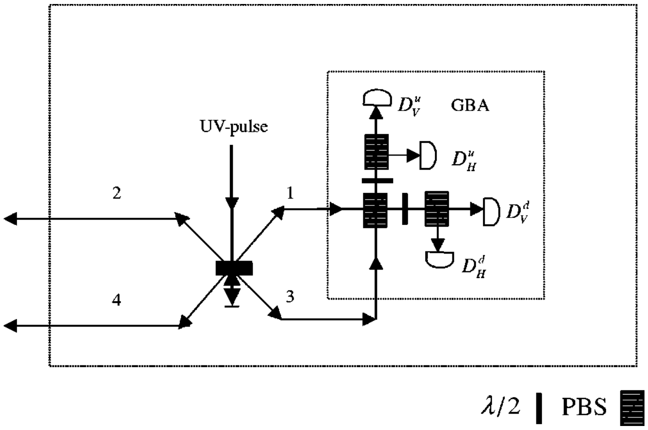

FIG. 1. The schematic setup for the modified quantum-data-hiding protocol with extended Bell states. A pulse of UV light passing through a nonlinear crystal creates the ancillary pair of entangled photons in paths 1 and 2. After retroflection during its second passage through the crystal, the ultraviolet pulse can create another pair of photons in paths 3 and 4. Then there is a probability of order of p^2 to have four photons in the four paths 1, 2, 3, and 4. The $\lambda/2$ plates are used to implement Hardmard operations, which transform h mode photon into $h-v$, and v mode into $h+v$. To encode secret, the hider measures the photons from the path 1 and 3 with the GBA and picks out n pairs of photons in paths 2 and 4, which are sent to the two sharers, Alice and Bob, respectively. In the secret decoding procedure, Alice and Bob cooperatively measure the photons from paths 2 and 4 with the same analyzer (GBA).

This state can also be written as (unnormalized)

$$\begin{aligned}|\Theta\rangle&=|\Phi\rangle_{13}^{\dagger}|\Phi\rangle_{24}^{\dagger}-|\Phi\rangle_{13}^{-}|\Phi\rangle_{24}^{-}-|\Psi\rangle_{13}^{\dagger}|\Psi\rangle_{24}^{\dagger}+|\Psi\rangle_{13}^{-}|\Psi\rangle_{24}^{-}\\&\quad+|\Gamma\rangle_{13}^{\dagger}|\Upsilon\rangle_{24}^{\dagger}+|\Gamma\rangle_{13}^{-}|\Upsilon\rangle_{24}^{-}+|\Upsilon\rangle_{13}^{\dagger}|\Gamma\rangle_{24}^{\dagger}+|\Upsilon\rangle_{13}^{-}|\Gamma\rangle_{24}^{-}\\&\quad-|\Omega\rangle_{13}^{\dagger}|\Omega\rangle_{24}^{\dagger}-|\Omega\rangle_{13}^{-}|\Omega\rangle_{24}^{-}.\end{aligned} \tag{4}$$

Here $|\Phi\rangle_{ij}^{\pm}=1/\sqrt{2}(h_i^{\dagger}h_j^{\dagger}\pm v_i^{\dagger}v_j^{\dagger})|\mathrm{vac}\rangle$ and $|\Psi\rangle_{ij}^{\pm}=1/\sqrt{2}(h_i^{\dagger}v_j^{\dagger}\pm v_i^{\dagger}h_j^{\dagger})|\mathrm{vac}\rangle$ are the four common Bell states, which constitute a set of complete bases in the Hilbert space H_1. This space represents the case that there is one and only one photon in each of two paths i and j. The states $|\Gamma\rangle_{ij}^{\pm}=\frac{1}{2}(h_i^{\dagger}h_i^{\dagger}\pm v_j^{\dagger}v_j^{\dagger})|\mathrm{vac}\rangle$, $|\Upsilon\rangle_{ij}^{\pm}=\frac{1}{2}(v_i^{\dagger}v_i^{\dagger}\pm h_j^{\dagger}h_j^{\dagger})|\mathrm{vac}\rangle$, and $|\Omega\rangle_{ij}^{\pm}=1/\sqrt{2}(h_i^{\dagger}v_i^{\dagger}\pm h_j^{\dagger}v_j^{\dagger})|\mathrm{vac}\rangle$ correspond to the case that there are two photons concentrating in one path and with no photon in the other path. These six states can also be regarded as a set of complete generalized Bell state bases in the Hilbert space H_2, where two photons concentrate in one certain path. Thus there are generally ten Bell-type states involving two photons and two paths, which belong to two sets of bases. Obviously, these two sets of bases lie in two different Hilbert spaces, H_1 and H_2.

In the first step of the present modified quantum-data-hiding protocol, the hider measures the photons from the paths 1 and 3 with an optical setup as shown in Fig. 1 [14,15]. When there are coincidence clicks between two same polarization mode detectors D_V^u and D_V^d (or D_H^u and D_H^d), the two photons in paths 1 and 3 are measured in either the state $|\Phi\rangle_{13}^{\dagger}$ or the state $|\Omega\rangle_{13}^{\dagger}$. And then the two photons in paths 2 and 4 are, obviously, collapsed into the state $|\Phi\rangle^{\dagger}_{24}$ or the state $|\Omega\rangle^{\dagger}_{24}$. Similarly, when there are coincidence clicks between two different polarization mode detectors D^{u}_{H} and D^{d}_{V} (or D^{u}_{V} and D^{d}_{H}), two photons in paths 1 and 3 are measured in either the state $|\Phi\rangle^{-}_{13}$ or the state $|\Omega\rangle^{-}_{13}$. And thus the two photons in paths 2 and 4 are collapsed into the state $|\Phi\rangle^{-}_{24}$ or the state $|\Omega\rangle^{-}_{24}$. Analogous to the existing Bell-states analyzer with linear optics, this optical setup as shown in Fig. 1 can be regarded as a general Bell analyzer (GBA). The GBA can divide the ten general Bell states into three classes: $|\Phi\rangle^{\dagger}_{ij}$ and $|\Omega\rangle^{\dagger}_{ij}$ as the first class, $|\Phi\rangle^{-}_{ij}$ and $|\Omega\rangle^{-}_{ij}$ as the second class, and the others as the third class.

According to the measurement results of the photons in path 1 and 3, the hider can conveniently pick out n pairs of photons in paths 2 and 4, which are randomly in the above three classes general Bell states. When the one-bit secret $b=1$, the hider picks out odd number of the first class states (can be either $|\Phi\rangle^{\dagger}_{ij}$ or $|\Omega\rangle^{\dagger}_{ij}$) among these n pairs of states chosen at random. For the case $b=0$, the hider chooses even number of the first class states in those n pairs of general Bell states. This encoding procedure is straightforward and effortless. The uncertainty caused by the parameter down-conversion is ingeniously integrated into the encoding states.

To hide the secret b, the n pairs of photons in paths 2 and 4 are sent to the sharers, with the photons in path 2 to Alice and path 4 to Bob, respectively. To completely decode the secret, a quantum channel between Alice's and Bob's is opened up and one sharer's photons, say Alice, are sent to the other sharer, as Bob. Then Bob can measure these photons with the same GBA as the hider has used. Simply count the number of the first class states measured (the number of the coincidence clicks between two same mode detectors), the sharers can easily figure out the parity and then the secret.

The rigorous proof for the security of the present quantum-data-hiding protocol with ten generalized Bell states is involuted and will be presented in other place [16]. Here we propose a simple but suggestive argument, which states that the present modified quantum-data-hiding protocol can be at least 2/5 times as secured as Terhal's original scheme.

The secret b is encoded in the parity of the total number of the states $|\Phi\rangle^{\dagger}$ and $|\Omega\rangle^{\dagger}$ in the tensor product of n general Bell states of the above two sets. We can then assume that among these n pairs of encoded states, there are m pairs of states of the set $S1=\{|\Phi\rangle^{\pm},|\Psi\rangle^{\pm}\}$ and $(n-m)$ pairs of states of the set $S2=\{|\Gamma\rangle^{\pm},|\Upsilon\rangle^{\pm},|\Omega\rangle^{\pm}\}$. The security analyze for quantum data hiding is equal to bounding the mutual information $I(b:M)$ the sharers can get about the secret b with LOCC operations M. Generally, there are two manners for the sharers to decode the secret b. In the first method, the two sharers do not try to separate the two sets of states, and directly act on the tensor product state of all these n pairs of states. Any sequence of LOCC operations is allowed for the sharers. In the second method, the two sharers first divide those n pairs of states into two sets $S1$ and $S2$ with some LOCC operations. Afterward, they separately decode the number n_1 of the state $|\Phi\rangle^{\dagger}$ from the m pairs of $S1$-set states and the number n_2 of the state $|\Omega\rangle^{\dagger}$ from the $(n-m)$ pairs of $S2$-set states. By combining the parity b_1 of the number n_1 and the parity b_2 of the number n_2, the two sharers can learn the secret $b=b_1\oplus b_2$, with $\oplus$ being the addition modulo 2.

As the sharers can do any sequence of LOCC operations in decode procedure, the second method is in fact a particular example contained in the first general method. Obviously, the states of the two sets $S1$ and $S2$ lie in two different Hilbert spaces H_1 and H_2, respectively and represent the case in which the two photons distribute in two paths or concentrate in one path. Thus we argue that the sharers cannot lose any advantage for decoding by first separating the two sets of different Hilbert space states. The mutual information $I(b:M)$ the two sharers can get about the secret b with the second particular method will not be less than that by the first general method. We can then prove the security of the present quantum-data-hiding protocol by analyzing the second particular decoding method.

Since the sharers can theoretically do any sequence of LOCC operations on the photons, Alice and Bob can easily separate the states of the two sets $S1$ and $S2$ with some quantum nondemolition devices as photon-Fock-state-filter. Then the two sharers separately decode the parity b_1 and b_2 from the n pairs of $S1$-set states and the $(n-m)$ pair of $S2$-set states. It can be proved that the sharers can exactly decode the parity b_2 from the $(n-m)$ pair of $S2$-set states. With the result from the original quantum-data-hiding protocol with $S1$-set Bell states, the mutual information $I(b1:M)$ [17] the sharers can get about the parity b_1 with LOCC operation is bounded by $\delta H(b_1)$ [9], where $\delta=1/2^{m-1}$ and $H(B_1)$ is the Shannon information of the hidden bit. Thus the mutual information $I(b:M)$ the sharers can get about the secret $b=b_1\oplus b_2$ with the second method by separately acting on the two sets is only bounded by $\delta H(b_1) =H(B_1)/2^{m-1}$.

We have argued that this mutual information getting from the second method is also the bound of that which the two sharers can get with any sequence of LOCC operations. It is easy to see that the two photons in path 2 and 4 has a probability of 2/5 to be prepared in the $S1$-set states in the present quantum-data-hiding scheme with spontaneous parameter down-conversion. Thus, to achieve the same level of security, the present protocol needs 5/2 times as many pairs of states as the original quantum data hiding with $S1$-set Bell states.

In conclusion, we have analyzed the practical implication of the existing quantum-data-hiding protocol with Bell states produced with optical down-converter. We showed that the uncertainty for producing of the Bell states with spontaneous parameter down-conversion should be taken into account, because it will cause serious trouble to the hider encoding procedure. A set of extended Bell states and a generalized Bell-states analyzer are proposed to describe and analyze the possible states of two photons distributing in the two paths. Then we presented a method to integrate the above uncertainty of Bell-states preparation into the dating hiding procedure, when we encode the secret with a set of extended Bell-states. These modifications greatly simplify the hider's encoding operations. With the result from the origin protocol, the present modified quantum-data-hiding scheme is argued to have similar security. It paves the way for the experimental implementation of the quantum data hiding with present-day quantum optics.

We thank Barbara Terhal for the discussion on the security proof of the present protocol. This work was funded by the National Fundamental Research Program (Grant No. 2001CB309300), the National Natural Science Foundation of China, and the Innovation funds from Chinese Academy of Sciences.

[1] C.H. Bennett and G. Brassard, in *Proceedings of Ctypto84* (Springer-Verlag, Berlin, 1984), p. 475.
[2] C.H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[3] A. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[4] L. Goldenberg and L. Vaidman, Phys. Rev. Lett. **75**, 1239 (1995).
[5] G.P. Guo, C.F. Li, B.S. Shi, J. Li, and G.C. Guo, Phys. Rev. A **64**, 042301 (2001).
[6] A. Ambainis, M. Mosca, A. Tapp, and R. de Wolf, e-print quant-ph/0003101.
[7] R. Cleve, D. Gottesman, and H.K. Lo, Phys. Rev. Lett. **83**, 648 (1999).
[8] G.P. Guo and G.C. Guo, Phys. Lett. A **310**, 247 (2003).
[9] B.M. Terhal, D.P. Divincenzo, and D.W. Leung, Phys. Rev. Lett. **86**, 5807 (2001).
[10] D.P. Divincenzo, P. Hayden, and B.M. Terhal, IEEE Trans. Inf. Theory **48**, 580 (2002).
[11] D.P. Divincenzo, D.W. Leung, and B.M. Terhal, e-print quant-ph/0103098.
[12] G.P. Guo, C.F. Li, and G.C. Guo, Phys. Lett. A **286**, 401 (2001).
[13] E. Knill, R. Laflamme, and G. Milburn, Nature (London) **409**, 46 (2001).
[14] G.P. Guo and G.C. Guo, e-print quant-ph/0208071.
[15] G.P. Guo and G.C. Guo, e-print quant-ph/0301009.
[16] G.P. Guo, and G.C. Guo (unpublished).
[17] T.M. Cover and J.A. Thomas, *Elements of Information Theory* (Wiley, New York, 1991).