


## Examining the correctness of anonymity for practical quantum networks

Yu-Guang Yang <sup>1,2,3,\*</sup> Yong-Li Yang,<sup>1</sup> Xin-Long Lv,<sup>1</sup> Yi-Hua Zhou,<sup>1</sup> and Wei-Min Shi<sup>1</sup>

<sup>1</sup>Faculty of Information Technology, Beijing University of Technology, Beijing 100124, China

<sup>2</sup>State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

<sup>3</sup>Beijing Key Laboratory of Trusted Computing, Beijing 100124, China



(Received 5 October 2019; accepted 1 May 2020; published 4 June 2020)

In a recent paper [A. Unnikrishnan *et al.*, *Phys. Rev. Lett.* **122**, 240501 (2019)], a quantum anonymous communication protocol was proposed in the presence of malicious agents and an untrusted source. Here, we point out that malicious agents can change the generated anonymous entanglement between the sender and the receiver without being detected, which means that the correctness of the generated anonymous entanglement should be reexamined. The way to check the above correctness is discussed.

DOI: [10.1103/PhysRevA.101.062311](https://doi.org/10.1103/PhysRevA.101.062311)

### I. INTRODUCTION

Anonymity is defined as the secrecy of identity. Consider a quantum network with  $n$  nodes. If, for the sender, her identity remains unknown to all the other parties whereas, for the receiver, no one except the sender knows her identity, the sender and the receiver are both considered anonymous. In the future, the capability of anonymously transmitting quantum information is of vital importance to many potential applications on the quantum Internet [1–6].

In a recent paper, Unnikrishnan *et al.* [7] proposed a quantum anonymous communication protocol in the presence of malicious agents and an untrusted source. This protocol is subtly designed so that perfect anonymity is guaranteed. Here, from a different perspective of security, we consider a special threat which was not concerned in Ref. [7]. That is, after the anonymous communication, the correctness of the generated anonymous entanglement between the sender and the receiver is still not assured [7]. As the correctness of the generated anonymous entanglement is concerned, it has a vital effect on the correctness of transmitting quantum information from the sender to the receiver anonymously later. We will show that, by a special attack, malicious agents can destroy this correctness without introducing any detectable disturbance.

Let us first review the anonymous protocol in Ref. [7]. The agents first run a classical notification protocol [8] so that the sender can notify the receiver anonymously. Then, the source generates state  $|\psi\rangle$  and distributes it to the agents. Finally, the sender anonymously chooses verification or anonymous entanglement. If the verification mode is chosen, the agents use the verification protocol for verifying Greenberger-Horne-Zeilinger (GHZ) states [9,10]. More specifically, the verifier generates random angles  $\theta_j \in [0, \pi)$  for all agents including themselves ( $j \in [n]$ ) such that  $\sum_j \theta_j$  is a multiple of  $\pi$ . The angles are then sent out to all the agents in the network. Agent  $j$  measures in the basis  $\{|+\theta_j\rangle, |-\theta_j\rangle\} = \{(1/\sqrt{2})(|0\rangle + e^{i\theta_j}|1\rangle), (1/\sqrt{2})(|0\rangle - e^{i\theta_j}|1\rangle)\}$  and sends the outcome  $Y_j = \{0, 1\}$  to the verifier. It will show that state

$|\psi\rangle$  is a perfect GHZ state if the following condition is satisfied:  $\oplus_j Y_j = \frac{1}{\pi} \sum_j \theta_j \pmod{2}$ . If the anonymous entanglement mode is chosen, the agents run the anonymous entanglement protocol to generate the anonymous entanglement between the sender and the receiver [7]. More specifically, assume that there are  $n$  agents who share a generalized GHZ state. Each agent, apart from the sender and the receiver, applies a Hadamard transform to his qubit, measures it in the computational basis, and broadcasts his outcome. The sender first picks a random bit  $b$ , broadcasts it, and applies a phase flip  $\sigma_z$  only when  $b = 1$ . The receiver picks a random bit  $b'$ , broadcasts it, and applies a phase flip  $\sigma_z$  only when the parity of everyone else's broadcasted bits is 1.

Indeed, the verification protocol is just useful to examine the correctness of the GHZ states. However, to verify the correctness of the generated anonymous entanglement between the sender and the receiver is not considered in the anonymous entanglement protocol. Given the perfect GHZ states, the malicious agents can take a special attack. That is, the malicious agents do not follow the anonymous entanglement protocol honestly, i.e., apply a Hadamard transform to their particles, measure them in the computational basis, and broadcast their outcomes, but just choose a random bit to publish without performing any operation on their particles. Obviously, the resultant two-qubit state shared between the sender and  $R$  is not the correct one, albeit, perfectly anonymous. Here, the purpose of the malicious agents is to destroy the anonymous communication instead of to extract the information on the identities of the sender and the receiver. Since the role of this attack is just to change the generated anonymous entanglement, the sender and the receiver will obtain the anonymous entanglement differently from what they intended. And more seriously, they cannot detect the presence of the malicious agents (obviously, the malicious agents can pass the verification protocol successfully).

It can be seen that this special attack causes a severe effect, that is, the anonymous entanglement cannot be successfully shared between the sender and the receiver as they intended. More seriously, at the end of the anonymous protocol, when the sender and the receiver are happy for the successful sharing of the anonymous entanglement, they even do not

\*yangyang7357@bjut.edu.cn

know they have been cheated by the malicious agents. When the sender utilizes the anonymous entanglement differently from what they intended to transmit quantum information to the receiver, remarkable errors would appear. But, at that time, they still do not know whether the malicious agents exist in the process of anonymous communication, which is a really intractable problem. Consequently, this problem must be overcome in a real implementation. In fact, the above attack is a special kind of denial-of-service attack, and it is forbidden in other quantum cryptographic protocols [11–13].

To realize the secure quantum communication, all thinkable attack strategies should be taken into consideration. Otherwise, the intended communications may be attacked successfully, for instance, see Refs. [11–26]. In Ref. [7], the main attention is paid to forbid the malicious agents from extracting the identity information of the sender and the receiver, whereas the correctness of the generated anonymous entanglement is overlooked.

## II. AN IMPROVED PROTOCOL FOR ANONYMITY FOR PRACTICAL QUANTUM NETWORKS

Now, consider how to detect this special attack. Obviously, before performing measurements, the malicious agents know if they will run the verification or anonymous entanglement mode. In the verification mode, the malicious agents run the protocol honestly, whereas, in the anonymous entanglement mode, they take the special attack. So, the special attack by the malicious agents will not introduce any detectable disturbance. In view of the above analysis, to expose the special attack, the agents should be required to perform measurements on their qubits and broadcast their results before they know the mode selection. Therefore, a possible way is to subtly adjust the order of the agents knowing the mode selection and performing measurements. That is, the agents are required to first perform measurements on their particles, broadcast their results, and finally perform the LOGICALOR protocol to know the mode selection. If the malicious agents act honestly, the verification should be deterministically successful. By this way, the verifier can assure the correctness of the anonymous entanglement except with a probability that vanishes exponentially with the number of rounds used to implement the subroutines. The improved version of the protocol in Ref. [7] is as follows.

### Protocol 1

*Step 1.* The sender notifies the receiver anonymously.

*Step 2.* GHZ state generation: The source generates state  $|\psi\rangle$  and distributes it to the agents ( $V$ ).

*Step 3.* Each node  $j \in V \setminus \{s, r\}$ , apart from the sender and the receiver

- (1) applies a Hadamard transform to her qubit.
- (2) Measures this qubit in the computational basis with outcome  $Y_j \in \{0, 1\}$ .
- (3) Broadcasts her measurement outcome  $Y_j$ .

*Step 4.* The receiver picks a random bit  $b' \in \{0, 1\}$  and broadcasts it.

*Step 5.* The sender picks a bit  $x$  to be 0 or 1 according to the following probability distribution: She flips  $S$  fair classical coins, and if all coins are heads, she gets 0, otherwise she gets 1. Let the outcome be  $x$ .

If  $x = 0$ , the sender chooses the anonymous entanglement mode:

Picks a random bit  $b \in \{0, 1\}$ .

Broadcasts  $b$ .

Applies a phase flip  $\sigma_z$  to her qubit if  $b = 1$ .

Otherwise, she chooses the verification mode:

(1) Applies a Hadamard transform to her qubit.

(2) Measures this qubit in the computational basis with outcome  $Y_s \in \{0, 1\}$ .

(3) Broadcasts  $Y_s$ .

*Step 6.* The agents perform the LOGICALOR protocol with input  $\{x_i\}_{i=1}^n$  and security parameter  $S$  and output its outcome where the sender inputs  $x$ ; all other agents pick  $x_i = 0$ . Let the outcome be  $y$ . Note that, in an honest run,  $y = x$  except with a probability that vanishes exponentially with the number of rounds, and so, if any agent behaves dishonestly, the sender will abort.

*Step 7.* According to outcome  $y$ , the agents perform the following operations:

If  $y = 0$ , the receiver applies a phase flip  $\sigma_z$  to her qubit if  $b \oplus (\bigoplus_{j \in V \setminus \{s, r\}} Y_j) = 1$ , otherwise if  $y = 1$ :

(i) The receiver applies a Hadamard transform to her particle and measures this particle in the computational basis with outcome  $Y_r \in \{0, 1\}$ .

(ii) The agents perform the LOGICALOR protocol with input  $\{y_i\}_{i=1}^n$  and output its outcome where the receiver inputs  $z' = b' \oplus Y_r$ ; all other agents pick  $y_i = 0$ . Let the outcome be  $z$ . Note that, in an honest run, if  $z' = 0$ , the correct probability of obtaining  $z = z'$  is 1. If  $z' = 1$ , the correct probability of obtaining  $z = z'$  is  $1 - 2^{-S}$  after  $S$  rounds.

(iii) The sender runs the verification test as the verifier. The verification test is passed when it satisfies the following condition:  $\bigoplus_{j \in V \setminus \{s, r\}} Y_j \oplus Y_s \oplus z \oplus b' = 0$ , i.e., there must be an even number of one outcome for  $Y_j (j \in V)$ . If she accepts the outcome of the test, they return to step 2, otherwise the protocol aborts.

If at any point in the protocol, the sender realizes someone does not follow the protocol, she stops behaving like the sender and behaves as any agent.

In contrast to the protocol [7] where the verifier is a randomly chosen agent  $j$  by the sender, the verifier is just the sender himself. Obviously, the probability of passing the GHZ test with state  $|\psi\rangle$  differently from the perfect GHZ state is  $P(|\psi\rangle)$ , which is lower than  $\frac{n-k}{n} + \frac{k}{n}P(|\psi\rangle)$  in the protocol in Ref. [7].

It is worth mentioning that the verification condition  $\bigoplus_{j \in V \setminus \{s, r\}} Y_j \oplus Y_s \oplus z \oplus b' = 0$  is, in fact, a special case of  $\bigoplus_{j \in V} V_j = \frac{1}{\pi} \sum_j \theta_j \pmod{2}$  where  $\theta_j = 0$ . The verification can achieve the two goals of checking the correctness of the GHZ state and the generated anonymous entanglement simultaneously, which is superior to that [7] which is just useful to examine whether the GHZ state is prepared correctly.

As in Refs. [7,9], we take the ideal  $n$ -party state to be  $|\Phi_0^n\rangle$ , given by

$$|\Phi_0^n\rangle = \frac{1}{\sqrt{2^{n-1}}} \left[ \sum_{\Delta(y)=0 \pmod{4}} |y\rangle - \sum_{\Delta(y)=2 \pmod{4}} |y\rangle \right], \quad (1)$$

which can be obtained from the GHZ state by applying a Hadamard and a phase shift  $\sqrt{Z}$  to each qubit and, thus, is equivalent to the GHZ state up to local unitaries. Here  $\Delta(y) = \sum_i y_i$  denotes the Hamming weight of the classical  $n$ -bit string  $y$ . Analogous to Refs [7,9,10], to measure the quality of state  $|\psi\rangle$  shared between the  $n$  agents, we take a fidelity measure given by  $F'(|\psi\rangle) = \max_U F(U|\psi, |\Phi_0^n\rangle) = \sqrt{1 - \varepsilon^2}$ , where  $U$  is a general operator in the space of the malicious agents.

### III. SECURITY ANALYSIS OF THE IMPROVED PROTOCOL

Next, we present the security definitions and prove the security of Protocol 1 against active adversaries.

*Definition 1* (active adversary). We define the active adversary scenario as one in which the adversaries are active, i.e., can perform arbitrary joint operations on their state and even corrupt the source during the execution of the protocol.

We define security in terms of the probability of event  $C_\varepsilon$  that the protocol does not abort and the state used for the anonymous entanglement mode is such that the fidelity  $F'(|\psi\rangle) \leq \sqrt{1 - \varepsilon^2}$  [7,9,10]. We say that the protocol is secure when the probability of event  $C_\varepsilon$  is no larger than a significance level  $\delta$ , i.e., the maximum passing probability when the state satisfies  $F'(|\psi\rangle) \leq \sqrt{1 - \varepsilon^2}$ .

*Definition 2* (probability of event  $C_\varepsilon$ ). Let  $C_\varepsilon$  be the event that the protocol does not abort and the state used for the anonymous entanglement mode is such that  $F'(|\psi\rangle) \leq \sqrt{1 - \varepsilon^2}$  whatever the malicious agents perform to their particles.

*Theorem 1.* For the honest agents (only) for all  $\varepsilon > 0$ ,

$$\Pr[C_\varepsilon] \leq \frac{2^{2-S}}{1 - \sqrt{1 - \varepsilon^2}}. \quad (2)$$

*Proof.* Similar to Ref. [7], our aim is also to bound the probability that the protocol does not abort and the fidelity of the state satisfies  $F'(|\psi\rangle) \leq \sqrt{1 - \varepsilon^2}$ . As proved in Ref. [9], the optimal cheating strategy which maximizes the probability of passing the verification is to prepare some pure state  $|\psi\rangle$  in each round such that  $F'(|\psi\rangle) \leq \sqrt{1 - \varepsilon^2}$ .

First, we consider the probability that the state is used in round  $l$ . For this to happen, the sender must get all  $S$  coin flips to be heads ( $x = 0$ ), which happens with probability  $2^{-S}$ .

Second, we consider the probability that the state is tested in all  $(l - 1)$  previous rounds. More specifically, in step 5, the probability of the sender not getting all  $S$  coin flips to be 0 is given by  $1 - 2^{-S}$ . Then, in step 6, the agents perform the LOGICALOR protocol with input  $\{x_i\}_{i=1}^n$  and security parameter  $S$ . Then, they obtain the outcome of the LOGICALOR protocol  $y$  where the sender picks bit  $x = 1$  and other agents input 0. The correct probability of obtaining  $x = y$  is  $1 - 2^{-S}$ . In step 7(ii), the agents perform the LOGICALOR protocol with input  $\{y_i\}_{i=1}^n$  and security parameter  $S$ . Then, they obtain the outcome of the LOGICALOR protocol  $z$  where the receiver picks bit  $z'$  and other agents input 0. If  $z' = 0$  with probability  $1/2$ , the correct probability of obtaining  $z = z'$  is 1. If  $z' = 1$  with probability  $1/2$ , the correct probability of obtaining  $z = z'$  is  $1 - 2^{-S}$  after  $S$  rounds. Thus, the overall probability is given by  $(1 - 2^{-S})^{2(l-1)}(1 - 2^{-1-S})^{l-1}$ .

Finally, we consider the probability that all the  $(l - 1)$  tests have passed. In our protocol, the sender runs the verification as the verifier. The probability that the test is passed with state  $|\psi\rangle$  is given by  $P(|\psi\rangle)$ . Then, the probability that all  $(l - 1)$  tests have passed is  $[P(|\psi\rangle)]^{l-1}$ . Note that, from Refs. [7,9,10], the probability that state  $|\psi\rangle$  with fidelity  $F'(|\psi\rangle)$  will pass the test is given by  $P(|\psi\rangle) \leq \frac{3+F'(|\psi\rangle)}{4}$ .

Thus, the total probability of event  $C_\varepsilon$  at the  $l$ th repetition of the protocol is as follows:

$$\begin{aligned} \Pr[C_\varepsilon^l] &= 2^{-S}(1 - 2^{-S})^{2(l-1)}(1 - 2^{-1-S})^{(l-1)}[P(|\psi\rangle)]^{l-1} \\ &\leq 2^{-S}(1 - 2^{-S})^{2(l-1)}(1 - 2^{-1-S})^{2(l-1)} \\ &\quad \times \left(\frac{3 + F'(|\psi\rangle)}{4}\right)^{l-1}. \end{aligned} \quad (3)$$

Since the summand is monotonously decreasing in the round number  $l$ , we then take the integral to upper bound this probability as follows:

$$\begin{aligned} \Pr[C_\varepsilon] &\leq \int_0^\infty 2^{-S}(1 - 2^{-S})^{2l}(1 - 2^{-1-S})^l \left(\frac{3 + F'(|\psi\rangle)}{4}\right)^l dl \\ &\leq 2^{-S} \int_0^\infty \left(\frac{3 + F'(|\psi\rangle)}{4}\right)^l dl = -\frac{2^{-S}}{\ln\left(\frac{3+F'(|\psi\rangle)}{4}\right)} \\ &\leq \frac{2^{-S}}{1 - \frac{3+F'(|\psi\rangle)}{4}} \leq \frac{2^{-S}}{1 - \frac{3+\sqrt{1-\varepsilon^2}}{4}} = \frac{2^{2-S}}{1 - \sqrt{1 - \varepsilon^2}}. \end{aligned} \quad (4)$$

We solve the equation  $\frac{2^{2-S}}{1 - \sqrt{1 - \varepsilon^2}} = \delta$  and obtain one solution as follows:

$$S = \log_2 \frac{4}{\delta(1 - \sqrt{1 - \varepsilon^2})} = 2 - \log_2[\delta(1 - \sqrt{1 - \varepsilon^2})], \quad (5)$$

By taking  $S = 2 - \log_2[\delta(1 - \sqrt{1 - \varepsilon^2})]$ , we have  $\Pr[C_\varepsilon] \leq \delta$ . The expected number of runs of the protocol is given by  $2^S = \frac{4}{\delta(1 - \sqrt{1 - \varepsilon^2})}$ . Thus, they can make this probability of failure negligible by performing a large number of runs.

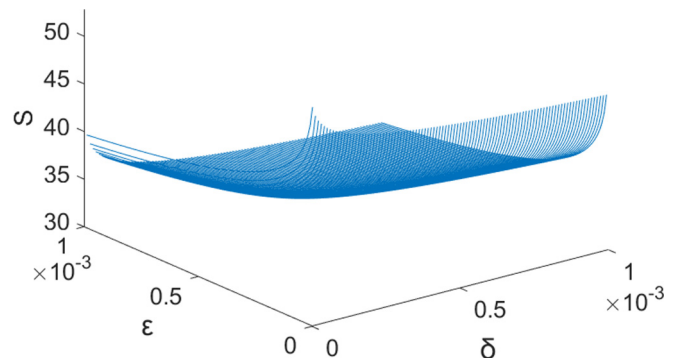


FIG. 1.  $S$  for different  $\varepsilon$ 's and  $\delta$ 's.  $S$  descends with  $\delta$  and  $\varepsilon$ . When  $S$  is very large, both  $\varepsilon$  and  $\delta$  approach zero.

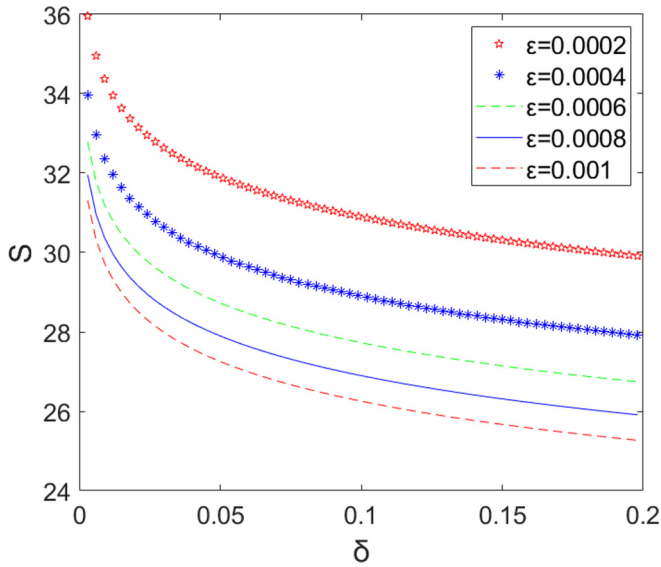


FIG. 2. Relations between  $S$  and  $\delta$  for different values of  $\varepsilon$ . When  $S = 38$  and  $\varepsilon = 0.0002$ ,  $\delta$  is about 0.0007. Use the case that  $\varepsilon = 0.0002$ . With the increase in  $S$ ,  $\delta$  approaches zero, and, thus,  $\text{Pr}[C_e]$  approaches zero.

We take the partial derivative of  $S$  with respect to  $\varepsilon$  and  $\delta$ , respectively,

$$\frac{\partial S}{\partial \delta} = -\frac{1}{\delta \ln 2}, \tag{6}$$

$$\frac{\partial S}{\partial \varepsilon} = -\frac{1}{\sqrt{1 - \varepsilon^2}(1 - \sqrt{1 - \varepsilon^2}) \ln 2}. \tag{7}$$

Obviously,  $\frac{\partial S}{\partial \delta}$  and  $\frac{\partial S}{\partial \varepsilon}$  are both negative which means that  $S$  descends with  $\delta$  and  $\varepsilon$ , respectively. Moreover, the graphs corresponding to the above two formulas are given to make it more visible (see Figs. 1 and 2).

One may argue that the special attack occurs in many other situations, for example, one-time pad, quantum key distribution, and quantum secure direct communication and, consequently, it is meaningless to discuss this problem here. However, it is not the fact for the case of anonymous communication. As we know, the malicious agents exist inevitably in anonymous communication. They may take various attack strategies to extract the information on the identities of the sender and the receiver or destroy the anonymous communication. Therefore, it is necessary to check the correctness of the product of anonymous communication, i.e., the correctness of the generated anonymous communication instead of only assuring the anonymity.

#### IV. CONCLUSIONS

In conclusion, we have presented a special attack on the anonymous protocol [7] by which the malicious agents can change the generated anonymous entanglement without being detected. It means that the generated anonymous entanglement should be reexamined. Furthermore, the way to check the correctness of the generated anonymous entanglement is discussed. Note that the special attack, i.e., the denial-of-service attack, is common in classical cryptography. Moreover, such an attack was effectively applied in breaking some quantum cryptographic protocols [11–13]. We hope that the special attack should be taken into account in the design of anonymous quantum protocols and other quantum cryptographic protocols [27].

#### ACKNOWLEDGMENTS

This work was supported by the Beijing Municipal Science & Technology Commission (Project No. Z191100007119004), the Beijing Natural Science Foundation (Grant No. 4182006), and the Guangxi Key Laboratory of Cryptography and Information Security (Grant No. GCIS201810).

[1] F. Stajano and R. Anderson, *The Cocaine Auction Protocol: On the Power of Anonymous Broadcast. Information Hiding*, edited by A. Pfitzmann, Lecture Notes in Computer Science Vol. 1768 (Springer, Berlin/Heidelberg, 2000), pp. 434–447.

[2] M. Naseri, *Opt. Commun.* **282**, 1939 (2009).

[3] M. Hillery, M. Ziman, V. Buzek, and M. Bielikova, *Phys. Lett. A* **349**, 75 (2006).

[4] L. Jiang, G. Q. He, D. Nie, J. Xiong, and G. H. Zeng, *Phys. Rev. A* **85**, 042309 (2012).

[5] W. Huang, Q.-Y. Wen, B. Liu, Q. Su, S.-J. Qin, and F. Gao, *Phys. Rev. A* **89**, 032325 (2014).

[6] D. Chaum, *Commun. ACM* **24**, 84 (1981).

[7] A. Unnikrishnan, I. J. MacFarlane, R. Yi, E. Diamanti, D. Markham, and I. Kerenidis, *Phys. Rev. Lett.* **122**, 240501 (2019).

[8] A. Broadbent and A. Tapp, *Advances in Cryptology-ASIACRYPT 2007*, edited by K. Kurosawa, Lecture Notes in Computer Science Vol. 4833 (Springer, Berlin/Heidelberg, 2007), pp. 410–426.

[9] A. Pappa, A. Chailloux, S. Wehner, E. Diamanti, and I. Kerenidis, *Phys. Rev. Lett.* **108**, 260502 (2012).

[10] W. McCutcheon, A. Pappa, B. A. Bell, A. McMillan, A. Chailloux, T. Lawson, M. Mafu, D. Markham, E. Diamanti, I. Kerenidis *et al.*, *Nat. Commun.* **7**, 13251 (2016).

[11] K. Boström and T. Felbinger, *Phys. Rev. Lett.* **89**, 187902 (2002).

[12] Q. Y. Cai, *Phys. Rev. Lett.* **91**, 109801 (2003).

[13] F. Gao, F.-Z. Guo, Q.-Y. Wen, and F.-C. Zhu, *Phys. Rev. A* **77**, 014302 (2008).

[14] Y. S. Zhang, C. F. Li, and G. C. Guo, *Phys. Rev. A* **63**, 036301 (2001).

[15] A. Wójcik, *Phys. Rev. A* **71**, 016301 (2005).

[16] F. Gao, F. Guo, Q. Wen, and F. Zhu, *Phys. Rev. A* **72**, 036302 (2005).

[17] F. Gao, F. Guo, Q. Wen, and F. Zhu, *Phys. Rev. A* **72**, 066301 (2005).

[18] F. G. Deng, X. H. Li, H. Y. Zhou, and Z. J. Zhang, *Phys. Rev. A* **72**, 044302 (2005).

- [19] F. Gao, Q. Y. Wen, and F. C. Zhu, *Phys. Lett. A* **360**, 748 (2007).
- [20] F. Gao, F. Z. Guo, Q. Y. Wen, and F. C. Zhu, *Phys. Rev. Lett.* **101**, 208901 (2008).
- [21] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, *Phys. Rev. A* **73**, 022320 (2006).
- [22] Y.-G. Yang, M. Naseri, and Q.-Y. Wen, *Opt. Commun.* **282**, 4167 (2009).
- [23] Y.-G. Yang, Y.-W. Teng, H.-P. Chai, and Q.-Y. Wen, *Quantum Inf. Process.* **10**, 317 (2011).
- [24] Y.-G. Yang, H.-P. Chai, Y.-W. Teng, and Q.-Y. Wen, *Int. J. Theor. Phys.* **50**, 395 (2011).
- [25] Y.-G. Yang, S.-J. Sun, and Q.-Q. Zhao, *Int. J. Theor. Phys.* **14**, 681 (2015).
- [26] Y.-G. Yang, J. Xia, X. Jia, and H. Zhang, *Quantum Inf. Process.* **12**, 877 (2013).
- [27] D.-H. Jiang, J. Wang, X.-Q. Liang, G.-B. Xu, and H.-F. Qi, *Int. J. Theor. Phys.* **59**, 436 (2020).