ISSN 1674-1056
http://cpb.iphy.ac.cn
http://iopscience.iop.org/cpb
中国物理 B
Chinese Physics
中国物理
Chinese Physics B

Coherent attacks on a practical quantum oblivious transfer protocol

Guang-Ping He(何广平)

Citation: Chin. Phys. B . 2018, 27(10): 100308. **doi:** 10.1088/1674-1056/27/10/100308

Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

Two-step quantum secure direct communication scheme with frequency coding

Xue-Liang Zhao(赵学亮), Jun-Lin Li(李俊林), Peng-Hao Niu(牛鹏皓), Hong-Yang Ma(马鸿洋), Dong Ruan(阮东)

Chin. Phys. B . 2017, 26(3): 030302. **doi:** 10.1088/1674-1056/26/3/030302

Probabilistic direct counterfactual quantum communication

Sheng Zhang(张盛)

Chin. Phys. B . 2017, 26(2): 020304. **doi:** 10.1088/1674-1056/26/2/020304

Anonymous voting for multi-dimensional CV quantum system

Rong-Hua Shi(施荣华), Yi Xiao(肖伊), Jin-Jing Shi(石金晶), Ying Guo(郭迎), Moon-Ho Lee

Chin. Phys. B . 2016, 25(6): 060301. **doi:** 10.1088/1674-1056/25/6/060301

Controlled mutual quantum entity authentication using entanglement swapping

Min-Sung Kang, Chang-Ho Hong, Jino Heo, Jong-In Lim, Hyung-Jin Yang

Chin. Phys. B . 2015, 24(9): 090306. **doi:** 10.1088/1674-1056/24/9/090306

Multi-user quantum key distribution with collective eavesdropping detection over collective-noise channels

Huang Wei, Wen Qiao-Yan, Liu Bin, Gao Fei

Chin. Phys. B . 2015, 24(7): 070308. **doi:** 10.1088/1674-1056/24/7/070308

Coherent attacks on a practical quantum oblivious transfer protocol

Guang-Ping He(何广平)†

School of Physics, Sun Yat-sen University, Guangzhou 510275, *China*

(Received 27 April 2018; revised manuscript received 19 July 2018; published online 10 September 2018)

In a recent quantum oblivious transfer protocol proposed by Nagy *et al.*, it was proven that attacks based on individual measurements and 2-qubit entanglement can all be defeated. Later we found that 5-body entanglement-based attacks can break the protocol. Here we further tighten the security bound, by showing that the protocol is insecure against 4-body entanglement-based attacks, while being immune to 3-body entanglement-based attacks. Also, increasing the number of qubits in the protocol is useless for improving its security.

Keywords: quantum cryptography, quantum algorithm, quantum oblivious transfer, entanglement

PACS: 03.67.Dd, 03.67.Ac, 03.65.Ud, 03.67.Hk **DOI:** 10.1088/1674-1056/27/10/100308

1. Introduction

While quantum cryptography has achieved great success in many cryptographic tasks such as quantum key distribution,[1] there are also some tasks which are known to be hard. Oblivious transfer (OT),[2,3] being an essential primitive for building two-party and multi-party secure computation protocols,[4] is unfortunately covered. Because of the existence of the so-called honest-but-curious attack,[5–9] and also partly due to the lack of a self-consistent definition of OT specifically made for the quantum case (as elaborated near the end of Section 5 of Ref. [10]), unconditionally secure quantum OT was proven to be impossible.[11,12] Therefore, researchers sought for practically secure OT in recent years.[13–29]

Recently, Nagy *et al.*[30] proposed a very feasible quantum OT protocol, which does not require quantum storage when all participants are honest. The authors proved that the protocol is secure against individual measurements, as well as 2-qubit entanglement-based attacks. Later, however, we found that it is insecure against 5-body entanglement-based attacks.[31] More rigorously, the goal of OT is to provide a method for the sender Alice to transfer a secret bit b to the receiver Bob, and it is called secure if Bob can obtain b unambiguously with probability $1/2$ only, while Alice does not know whether Bob has learned b or not. We showed in Ref. [31] that if Bob has the technology to handle 5-body entangled states, then in the protocol of Ref. [30], he can learn b unambiguously with probability 62.5% using von Neumann measurements, or 64.6% using positive operator-valued measure (POVM).

These findings lead us to the question what is the exact security bound of the protocol between 2-qubit entanglement-based attacks and 5-body entanglement-based attacks. In the current paper, we will close the gap by showing that 4-body entangled states can still enable Bob to cheat, while 3-body entangled states are insufficient for him to learn b unambiguously with a probability higher than $1/2$.

The paper is organized as follows. We will first review the OT protocol of Ref. [30] in Section 2. Then in Section 3, we will use the $N = 1$ case of the protocol as an example, to elaborate the cheating strategy using 4-body entangled states. The cheating strategy on protocols with arbitrary N will be provided in Section 4. Finally, the cheating using 3-body entangled states will be analyzed in Section 5.

2. The OT protocol of Nagy *et al.*

Let $\{|0\rangle, |1\rangle\}$ be the computational basis of a qubit. Denote the Hadamard basis as $\{|+\rangle, |-\rangle\}$, where $|\pm\rangle \equiv (|0\rangle \pm |1\rangle)/\sqrt{2}$. The OT protocol of Ref. [30] contains the following steps.

(i) Bob sends Alice M qubit sequences. Each sequence contains $4N$ qubits, where each of the states $|0\rangle$, $|1\rangle$, $|+\rangle$, and $|-\rangle$ appears N times, while the order is random. After receiving the qubits, Alice measures them all in one of the two bases (computational or Hadamard) and records the outcomes.

(ii) Alice verifies with Bob that the sequences received correspond to the agreed specifications. The details of this verification were provided in Section 3 of Ref. [30]. In brief, she picks a sequence and asks Bob to announce the state of each qubit, and checks whether the announced numbers of $|0\rangle$, $|1\rangle$, $|+\rangle$, and $|-\rangle$ in this sequence are equal. She also checks whether Bob has announced the states honestly using her own measurement outcomes on these qubits. All but one of the M sequences are checked and then discarded in this step. The sequence that is not verified is selected randomly among the M sequences received, and if the verification is successful, she assumes that the remaining unchecked sequence also contains equal numbers of $|0\rangle$, $|1\rangle$, $|+\rangle$, and $|-\rangle$.

(iii) Alice randomly chooses one qubit from the remain-

†Corresponding author. E-mail: hegp@mail.sysu.edu.cn

© 2018 Chinese Physical Society and IOP Publishing Ltd

ing sequence, and looks at the value measured in step (i). If the outcome of this measurement was $|0\rangle$ or $|+\rangle$, she sends the bit b she wants to transmit over to Bob through a classical channel. Or if the outcome of this measurement was $|1\rangle$ or $|-\rangle$, she sends $\bar{b}$ (i.e., the complement of her bit b) to Bob.

(iv) Now Alice tells Bob which qubit she chose in step (iii) and which basis she used for measuring this qubit. If her measurement basis is identical to the one in which Bob prepared that qubit in step (i), then Bob knows the value of b (note that if the outcome of Alice's measurement is $|1\rangle$ or $|-\rangle$, Bob has to complement the bit value received). Otherwise, Bob obtains no information on b.

3. Bob's cheating strategy for the protocol with $N = 1$

Now we will show that if Bob is dishonest and he has the technology to handle 4-body entangled states, then he can learn Alice's secret bit b unambiguously with a probability higher than $1/2$, making the protocol insecure.

For easy understanding, we first describe the cheating strategy in the protocol where M (the total number of qubit sequences) can be arbitrary, while each sequence merely contains four qubits, i.e., $N = 1$. According to the protocol, when Bob is honest, he should prepare the states of the four qubits as $|0\rangle$, $|1\rangle$, $|+\rangle$, and $|-\rangle$, respectively, with a random order. However, a dishonest Bob can cheat as follows.

In step (i) of the protocol, for the four qubits A_1, A_2, A_3, and A_4 in each of the M sequences, dishonest Bob introduces an additional 6-level quantum system B, and prepares their initial state as

$$\begin{aligned}|\Psi_{\text{init}}\rangle &= |0\rangle_{A_1} \otimes \frac{1}{\sqrt{6}} \sum_{i=1}^{6} P_i(|1\rangle|+\rangle|-\rangle)_{A_2A_3A_4}|l_i\rangle_B \\ &= |0\rangle_{A_1} \otimes \frac{1}{\sqrt{6}}(|1\rangle_{A_2}(|+\rangle_{A_3}|-\rangle_{A_4}|l_1\rangle_B \\ &\quad + |-\rangle_{A_3}|+\rangle_{A_4}|l_2\rangle_B) \\ &\quad + |+\rangle_{A_2}(|1\rangle_{A_3}|-\rangle_{A_4}|l_3\rangle_B \\ &\quad + |-\rangle_{A_3}|1\rangle_{A_4}|l_4\rangle_B) \\ &\quad + |-\rangle_{A_2}(|1\rangle_{A_3}|+\rangle_{A_4}|l_5\rangle_B \\ &\quad + |+\rangle_{A_3}|1\rangle_{A_4}|l_6\rangle_B)). \end{aligned} \tag{1}$$

Here each P_i denotes a permutation of the three states $|1\rangle$, $|+\rangle$, and $|-\rangle$, with $|l_i\rangle_B$ ($i = 1,\ldots,6$) being the states of system B, which are orthogonal to each other. We can see that qubit A_1 actually does not entangle with the others. Thus the state is a 4-body entangled state of qubits A_2, A_3, A_4, and system B, with qubit A_1 being prepared separately.

Bob then sends qubits A_1, A_2, A_3, and A_4 to Alice, while keeping system B privately at his side. In step (ii) of the protocol, once such a sequence is selected for verification, Bob uses $\{|l_1\rangle,\ldots,|l_6\rangle\}$ as the basis and measures B. If the measurement outcome is $|l_{i_0}\rangle$, he announces the state of the qubits A_1, A_2, A_3, and A_4 as $|0\rangle \otimes P_{i_0}(|1\rangle|+\rangle|-\rangle)$. It is trivial to show that he can always pass the verification in step (ii) successfully with this method. On the other hand, consider the case when such a sequence is not chosen for verification. Instead, it is picked for transferring Alice's secret bit b in steps (iii) and (iv). Since Alice randomly selects one of the qubits in this sequence to encode b, there can be four cases.

(I) Alice picks qubit A_1, which occurs with probability $p_1 = 1/4$.

Bob cannot cheat in this case since A_1 was actually prepared honestly following the protocol. Thus he can learn the value of Alice's b with probability $r_1 = 50\%$ only, as it is expected in the original protocol.

(II) Alice picks qubit A_2, which occurs with probability $p_2 = 1/4$. This case can be further broken down to two possibilities.

(II-1) Alice measures A_2 in the basis $\{|+\rangle,|-\rangle\}$, which occurs with probability $p_{2.1} = 1/2$ when case (II) indeed happens.

Bob keeps system B unmeasured until the end of step (IV). Then after Alice reveals to Bob that she has used $\{|+\rangle,|-\rangle\}$ as the basis for measuring system A_1, Bob measures system B in the basis $\{|l_1\rangle,\ldots,|l_6\rangle\}$. If the result belongs to the subset $\{|l_3\rangle,|l_4\rangle,|l_5\rangle,|l_6\rangle\}$ (which occurs with probability $p_{2.1.1} = 2/3$, as can be seen from Eq. (1)), he can deduce whether qubit A_2 has collapsed to the state $|+\rangle$ or $|-\rangle$, and learns Alice's secret bit b with probability $r_{2.1.1} = 100\%$.

On the contrary, there is the probability $p_{2.1.2} = 1/3$ that Bob's measurement result of B belongs to the subset $\{|l_1\rangle,|l_2\rangle\}$. It indicates that the state of A_2 has collapsed to $|1\rangle_{A_2}$. In this case, Bob cannot learn Alice's b at all, because either one of the two results $|+\rangle$ and $|-\rangle$ is possible when Alice measures $|1\rangle_{A_2}$ in the basis $\{|+\rangle,|-\rangle\}$.

(II-2) Alice measures A_2 in the basis $\{|0\rangle,|1\rangle\}$, which occurs with probability $p_{2.2} = 1/2$ when case (II) indeed happens.

In this case Bob tries to project system B into the subspace supported by $\{|l_1\rangle,|l_2\rangle\}$ using the projective operator

$$M_B = |l_1\rangle\langle l_1| + |l_2\rangle\langle l_2|. \tag{2}$$

Once the projection is successful (which occurs with probability $p_{2.2.1} = 1/3$, as can be seen from Eq. (1)), Bob obtains Alice's b value with probability $r_{2.2.1} = 100\%$.

On the contrary, there is the probability $p_{2.2.2} = 2/3$ that the above projection will fail. Then the state of $A_2 \otimes A_3 \otimes A_4 \otimes B$ will collapse from Eq. (1) into

$$\begin{aligned}|\Psi'\rangle = \frac{1}{2}&(|+\rangle_{A_2}(|1\rangle_{A_3}|-\rangle_{A_4}|l_3\rangle_B + |-\rangle_{A_3}|1\rangle_{A_4}|l_4\rangle_B) \\ &+ |-\rangle_{A_2}(|1\rangle_{A_3}|+\rangle_{A_4}|l_5\rangle_B + |+\rangle_{A_3}|1\rangle_{A_4}|l_6\rangle_B)). \end{aligned} \tag{3}$$

Under this circumstance, it will be unwise for Bob to complete the measurement on B in the basis $\{|l_3\rangle, |l_4\rangle, |l_5\rangle, |l_6\rangle\}$, because doing so cannot provide him any information on b at all. Instead, the best strategy for him to learn b is to measure system B in another basis, as constructed below. First, let us expand Eq. (3) as

$$\begin{aligned}|\Psi'\rangle = \frac{1}{4}(&|0\rangle_{A_2}(|1\rangle_{A_3}|0\rangle_{A_4}(|l_3\rangle_B + |l_5\rangle_B) - |1\rangle_{A_3}|1\rangle_{A_4}(|l_3\rangle_B - |l_5\rangle_B + |l_4\rangle_B - |l_6\rangle_B) + |0\rangle_{A_3}|1\rangle_{A_4}(|l_4\rangle_B + |l_6\rangle_B))\\ &+ |1\rangle_{A_2}(|1\rangle_{A_3}|0\rangle_{A_4}(|l_3\rangle_B - |l_5\rangle_B) - |1\rangle_{A_3}|1\rangle_{A_4}(|l_3\rangle_B + |l_5\rangle_B + |l_4\rangle_B + |l_6\rangle_B) + |0\rangle_{A_3}|1\rangle_{A_4}(|l_4\rangle_B - |l_6\rangle_B))).\end{aligned} \tag{4}$$

Then by defining the new notations

$$|l'_3\rangle \equiv \frac{1}{\sqrt{2}}(|l_3\rangle + |l_5\rangle), \quad |l'_4\rangle \equiv \frac{1}{\sqrt{2}}(|l_4\rangle + |l_6\rangle), \quad |l'_5\rangle \equiv \frac{1}{\sqrt{2}}(|l_3\rangle - |l_5\rangle), \quad |l'_6\rangle \equiv \frac{1}{\sqrt{2}}(|l_4\rangle - |l_6\rangle), \tag{5}$$

as well as

$$\begin{aligned}|\Psi'_0\rangle_{A_3A_4B} &\equiv (|1\rangle_{A_3}|0\rangle_{A_4}|l'_3\rangle_B - |1\rangle_{A_3}|1\rangle_{A_4}(|l'_5\rangle_B + |l'_6\rangle_B) + |0\rangle_{A_3}|1\rangle_{A_4}|l'_4\rangle_B)/2,\\ |\Psi'_1\rangle_{A_3A_4B} &\equiv (|1\rangle_{A_3}|0\rangle_{A_4}|l'_5\rangle_B - |1\rangle_{A_3}|1\rangle_{A_4}(|l'_3\rangle_B + |l'_4\rangle_B) + |0\rangle_{A_3}|1\rangle_{A_4}|l'_6\rangle_B)/2,\end{aligned} \tag{6}$$

we can rewrite $|\Psi'\rangle$ as

$$|\Psi'\rangle = \frac{1}{\sqrt{2}}(|0\rangle_{A_2}|\Psi'_0\rangle_{A_3A_4B} + |1\rangle_{A_2}|\Psi'_1\rangle_{A_3A_4B}). \tag{7}$$

This equation implies that if Bob can discriminate the state $|\Psi'_0\rangle_{A_3A_4B}$ from the state $|\Psi'_1\rangle_{A_3A_4B}$, then he is able to deduce whether Alice's qubit A_2 has collapsed to $|0\rangle$ or $|1\rangle$, and therefore learn Alice's bit b. To study the probability for this state discrimination, let us find out the reduced density matrices ρ_j of Bob's system B corresponding to $|\Psi'_j\rangle_{A_3A_4B}$ $(j = 0, 1)$, which are defined as

$$\rho_j \equiv \mathrm{Tr}_{A_3A_4}(|\Psi'_j\rangle_{A_3A_4B}\langle\Psi'_j|), \tag{8}$$

where $\mathrm{Tr}_{A_3A_4}$ means tracing over the states of Alice's qubits A_3 and A_4. Substituting Eq. (6) into it and we yield

$$\begin{aligned}\rho_0 &= \frac{1}{4}(|l'_3\rangle_B\langle l'_3| + (|l'_5\rangle + |l'_6\rangle)_B(\langle l'_5| + \langle l'_6|) + |l'_4\rangle_B\langle l'_4|),\\ \rho_1 &= \frac{1}{4}(|l'_5\rangle_B\langle l'_5| + (|l'_3\rangle + |l'_4\rangle)_B(\langle l'_3| + \langle l'_4|) + |l'_6\rangle_B\langle l'_6|).\end{aligned} \tag{9}$$

We expanded the states of qubits A_3 and A_4 in the basis $\{|0\rangle, |1\rangle\}$ in Eq. (6) merely for the purpose of calculating ρ_j. Alice does not need to measure these qubits in this basis though. This is because ρ_j, being the reduced density matrix of Bob's local state only, has fixed values regardless of Alice's actual measurement bases.

The von Neumann projection operators for discriminating ρ_0 and ρ_1 can be constructed as

$$\begin{aligned}M_0 &= \frac{1}{2}(|l'_3\rangle - |l'_4\rangle)_B(\langle l'_3| - \langle l'_4|),\\ M_1 &= \frac{1}{2}(|l'_5\rangle - |l'_6\rangle)_B(\langle l'_5| - \langle l'_6|).\end{aligned} \tag{10}$$

This is because applying them to Eq. (9), we have

$$\mathrm{Tr}(M_j\rho_{\bar{j}}) = 0, \tag{11}$$

and

$$\mathrm{Tr}(M_j\rho_j) = 1/4 \tag{12}$$

for $j = 0, 1$, where $\bar{j} \equiv j \oplus 1$.

As a result, if Bob can apply von Neumann measurements only, once the operator M_B in Eq. (2) fails to project system B into the subspace supported by $\{|l_1\rangle, |l_2\rangle\}$, all Bob needs to do is to measure system B with either the operator M_0 or M_1 randomly. If what he applied is M_j $(j \in \{0, 1\})$ and Alice's qubit A_2 is in the state $|j\rangle$, the probability for his projection to be successful is $\mathrm{Tr}(M_j\rho_j)$. On the other hand, from Eq. (11) we know that if the state of Alice's qubit A_2 is $|\bar{j}\rangle$, then his projection can never be successful. As Bob picks M_0 or M_1 with the same probability, there is probability $1/2$ that he happens to pick M_j while qubit A_2 is in the state $|j\rangle$, so that he can discriminate the state of qubit A_2 unambiguously and deduce the value of Alice's b with probability $\mathrm{Tr}(M_j\rho_j)$. Namely, the probability for him to learn b unambiguously is

$$r_{\mathrm{von}} = \mathrm{Tr}(M_j\rho_j)/2 = (1/4)/2 = 12.5\%. \tag{13}$$

Moreover, if Bob owns the technology to perform a positive operator-valued measure (POVM), he can further increase this probability. As elaborated in Ref. [32], the POVM for optimum unambiguous discrimination of the density matrices ρ_0

and ρ_1 is $\{\Pi_0, \Pi_1, \Pi_2\}$, with

$$\begin{aligned}\Pi_0 &\equiv (2-\sqrt{2})M_0,\\ \Pi_1 &\equiv (2-\sqrt{2})M_1,\\ \Pi_2 &\equiv I-\Pi_0-\Pi_1.\end{aligned} \tag{14}$$

When Bob applies this POVM on system B and the result is Π_0 (Π_1), he will deduce with certainty that the density matrix of B was ρ_0 (ρ_1). Else if the result turns out to be Π_2, he knows that he fails to discriminate the state. Therefore, we can calculate the probability for Bob to discriminate the state unambiguously with this POVM, which is

$$\begin{aligned}r_{\text{POVM}} &= \text{Tr}(\Pi_j\rho_j) = (2-\sqrt{2})\,\text{Tr}\,(M_j\rho_j)\\ &= (2-\sqrt{2})/4 \simeq 14.6\%.\end{aligned} \tag{15}$$

As a brief summary of the above results, in case (II-2) Bob applies the operator M_B in Eq. (2) on system B first. With probability $p_{2.2.1} = 1/3$ the projection can be successful and he learns the value of b with probability $r_{2.2.1} = 100\%$. With the rest probability $p_{2.2.2} = 2/3$ the projection fails. In this case Bob continues by applying the von Neumann measurement in Eq. (10) or the POVM in Eq. (14), depending on what technology is available to him. Then he can learn the value of b with probability $r_{\text{von}} = 12.5\%$ or $r_{\text{POVM}} = 14.6\%$, respectively. Therefore, the average probability for him to learn b unambiguously in case (II-2) is $r_{2.2} = p_{2.2.1}r_{2.2.1} + p_{2.2.2}r_{\text{von}} = (1/3)\times 100\% + (2/3)\times 12.5\% = 41.6\%$ for von Neumann measurement or $r_{2.2} = p_{2.2.1}r_{2.2.1} + p_{2.2.2}r_{\text{POVM}} = (1/3)\times 100\% + (2/3)\times 14.6\% = 43.1\%$ for POVM.

Consequently, the total probability for Bob to learn b unambiguously in case (II) is

$$\begin{aligned}r_2 &= p_{2.1}p_{2.1.1}r_{2.1.1} + p_{2.2}r_{2.2}\\ &= \frac{1}{2}\times\frac{2}{3}\times 100\% + \frac{1}{2}\times r_{2.2}.\end{aligned} \tag{16}$$

That is, $r_2 = 54.1\%$ for von Neumann measurement or $r_2 = 54.9\%$ for POVM.

(III) Alice picks qubit A_3, which occurs with probability $p_3 = 1/4$.

From the symmetric form of qubits A_2, A_3, and A_4 in Eq. (1), we can see that the above analysis on case (II) also applies here. Thus, in the current case Bob can learn b unambiguously with probability $r_3 = r_2$.

(IV) Alice picks qubit A_4, which occurs with probability $p_4 = 1/4$.

For the same reason in case (III), the probability for Bob to learn b unambiguously in this case also satisfies $r_4 = r_2$.

As a result, the overall probability for Bob to learn b unambiguously in all the four cases is

$$\begin{aligned}r &= p_1r_1 + p_2r_2 + p_3r_3 + p_4r_4\\ &= \frac{1}{4}\times 50\% + 3\times\frac{1}{4}\times r_2,\end{aligned} \tag{17}$$

which is $r = (1/4)\times 50\% + (3/4)\times 54.1\% = 53.1\%$ for von Neumann measurement or $r = (1/4)\times 50\% + (3/4)\times 54.9\% = 53.7\%$ for POVM. As they all exceed 50%, which is the probability that a secure OT protocol should allow, the protocol cannot be regarded as secure against this cheating.

Also, instead of Eq. (1), it is not hard to see that Bob can cheat by preparing the initial state as either

$$|\Psi_{\text{init}}\rangle = |1\rangle_{A_1}\otimes\frac{1}{\sqrt{6}}\sum_{i=1}^{6}P_i(|0\rangle|+\rangle|-\rangle)_{A_2A_3A_4}|l_i\rangle_B \tag{18}$$

or

$$|\Psi_{\text{init}}\rangle = |+\rangle_{A_1}\otimes\frac{1}{\sqrt{6}}\sum_{i=1}^{6}P_i(|-\rangle|0\rangle|1\rangle)_{A_2A_3A_4}|l_i\rangle_B \tag{19}$$

or

$$|\Psi_{\text{init}}\rangle = |-\rangle_{A_1}\otimes\frac{1}{\sqrt{6}}\sum_{i=1}^{6}P_i(|+\rangle|0\rangle|1\rangle)_{A_2A_3A_4}|l_i\rangle_B, \tag{20}$$

with exactly the same probability r to learn Alice's b unambiguously.

4. Bob's cheating strategy for the protocol with $N > 1$

Now we proceed to show that even if we increase the value of the security parameter N in the protocol of Ref. [30], the probability of catching Bob's attack cannot be raised.

The cheating strategy is not much different from the one in the $N = 1$ case. For any $N > 1$, in step 1 of the protocol dishonest Bob simply prepares MN copies of 4-body entangled states. Each copy still takes the form of Eq. (1). Again, he sends the first four qubits of each copy to Alice, so that these qubits in all copies form the M sequences required in the protocol. The order of the qubits in each sequence can even be randomized too, as long as Bob himself remembered which qubits are the ones that belong to the same copy of the 4-body entangled states.

The remaining steps of the attack are exactly the same as that of the $N = 1$ case. Namely, in step (II) of the protocol, once a sequence of qubits is selected for verification, Bob measures system B in each copy of the 4-body entangled states in the basis $\{|l_1\rangle, \ldots, |l_6\rangle\}$. As mentioned above, with this method he can always know what can be disclosed as the states of the qubits A_2, A_3, and A_4 without causing any conflict with Alice's own measurement results.

Later in steps (III) and (IV) of the protocol, Bob waits until Alice discloses the position and her measurement basis on the qubit that she eventually selected for encoding the secret bit b. Then he finds out the copy of the 4-body entangled states which contained this qubit, and measures the corresponding system B with the operators that we presented in Eq. (10) or Eq. (14).

It is not hard to see that finally, Bob is still able to obtain the value of Alice's secret bit b unambiguously with probability 53.1% when using von Neumann measurement, or 53.7% when using POVM, as he did in the protocol with $N = 1$. That is, by increasing the value of N, dishonest Bob merely needs to raise the total number of the copies of the 4-body entangled states. He can achieve the same probability for successful cheating, without the need to entangle the quantum systems from different copies together. In short, increasing N will not make it harder for Bob to cheat. Also, as our above analysis on the $N = 1$ case does not put any restriction on the value of M, we arrive at the conclusion that both the security parameters N and M have little to do with the difficulty of the practical implementation of Bob's cheating, and they are completely unhelpful for reducing Bob's probability of successfully cheating. Simply put, even if we merely choose $N = M = 1$, the security level of the resultant protocol is exactly the same as the protocols with higher N, M values.

5. Impossibility of attack using 3-body entangled states

Here we will show that Bob cannot cheat if he can handle 3-body entanglement only. Again, taking the $N = 1$ case as an example, as he needs to keep one of the quantum system at his side, a 3-body entangled state used for his cheating can contain two of Alice's qubits at the most. In each of the M sequences sent to Alice which contain four qubits A_1, A_2, A_3, and A_4, once the sequence is chosen in step 2 for verification, Bob needs to show that all the four states $|0\rangle$, $|1\rangle$, $|+\rangle$, and $|-\rangle$ are presented. Without loss of generality, suppose that qubits A_1 and A_2 already took over the states $|1\rangle$ and $|-\rangle$ (or $|+\rangle$ and $|-\rangle$), respectively (regardless whether Bob prepared A_1 and A_2 in these states using entanglement or not). Then the states of A_3, A_4 can only be chosen among $\{|0\rangle, |+\rangle\}$ (or $\{|0\rangle, |1\rangle\}$). Thus, in place of the 4-body entangled state Eq. (1), Bob has to prepare the initial state of the 3-body entangled system as either

$$|\Psi'_{\text{init}}\rangle = \frac{1}{\sqrt{2}}(|0\rangle_{A_3}|+\rangle_{A_4}|l_1\rangle_B + |+\rangle_{A_3}|0\rangle_{A_4}|l_2\rangle_B) \quad (21)$$

or

$$|\Psi''_{\text{init}}\rangle = \frac{1}{\sqrt{2}}(|0\rangle_{A_3}|1\rangle_{A_4}|l_1\rangle_B + |1\rangle_{A_3}|0\rangle_{A_4}|l_2\rangle_B). \quad (22)$$

Obviously, with these states he can always pass the verification. Now consider the case that such a sequence is not selected for the verification. Instead, Alice picks qubit A_3 for encoding her secret bit b in steps (III) and (IV) (the case that she picks A_1, A_2, or A_4 can be analyzed similarly). Let us study the performance of the above two states one by one.

i) Suppose that Bob prepares the initial state as $|\Psi'_{\text{init}}\rangle$.

If Alice announces in step 4 that her measurement basis on A_3 is $\{|0\rangle, |1\rangle\}$, Bob can expand $|\Psi'_{\text{init}}\rangle$ as

$$|\Psi'_{\text{init}}\rangle = \frac{1}{\sqrt{2}}\left(\sqrt{\frac{3}{2}}|0\rangle_{A_3}\left(|0\rangle_{A_4}\sqrt{\frac{2}{3}}\frac{1}{\sqrt{2}}(|l_1\rangle_B + |l_2\rangle_B) + |1\rangle_{A_4}\sqrt{\frac{1}{3}}|l_1\rangle_B\right) + \frac{1}{\sqrt{2}}|1\rangle_{A_3}|0\rangle_{A_4}|l_2\rangle_B\right). \quad (23)$$

The reduced density matrices ρ_0, ρ_1 of Bob's system B when Alice found A_3 as $|0\rangle$, $|1\rangle$, respectively, are

$$\rho_0 = \frac{2}{3}\frac{1}{\sqrt{2}}((|l_1\rangle + |l_2\rangle)_B\frac{1}{\sqrt{2}}(\langle l_1| + \langle l_2|) + \frac{1}{3}|l_1\rangle_B\langle l_1|,$$
$$\rho_1 = |l_2\rangle_B\langle l_2|. \quad (24)$$

We can see that if Bob measures system B in the basis $\{|l_1\rangle, |l_2\rangle\}$ and the result is $|l_1\rangle$, he knows with certainty that Alice's measurement result on A_3 must be $|0\rangle$. On the other hand, if Alice's measurement result on A_3 is $|1\rangle$, there is no measurement for Bob to distinguish it unambiguously. As equation (21) shows that system B can be projected to $|l_1\rangle$ with probability $1/2$, we know that when Alice encoded her secret bit b with qubit A_3 using the measurement basis $\{|0\rangle, |1\rangle\}$, the probability for Bob to learn b unambiguously is $1/2$.

Similarly, from the symmetry of $|0\rangle_{A_3}$ and $|+\rangle_{A_3}$ in Eq. (21), it can be shown that if Alice's measurement basis on A_3 is $\{|+\rangle, |-\rangle\}$, Bob also stands a probability $1/2$ to learn b unambiguously. That is, preparing the initial state in the 3-body entangled form of equation (21) does not bring an extra advantage for Bob than following the original protocol honestly.

ii) Suppose that Bob prepares the initial state as $|\Psi''_{\text{init}}\rangle$.

If Alice announces in step 4 that her measurement basis on A_3 is $\{|0\rangle, |1\rangle\}$, Bob can simply measure system B in the basis $\{|l_1\rangle, |l_2\rangle\}$. From Eq. (22) we immediately know that Bob can learn Alice's measurement result and deduce her secret bit b with probability 100%.

However, if Alice announced the measurement basis on A_3 is $\{|+\rangle, |-\rangle\}$, equation (22) can be written as

$$|\Psi''_{\text{init}}\rangle = \frac{1}{\sqrt{2}}|+\rangle_{A_3}\frac{1}{\sqrt{2}}(|1\rangle_{A_4}|l_1\rangle_B + |0\rangle_{A_4}|l_2\rangle_B) + |-\rangle_{A_3}\frac{1}{\sqrt{2}}(|1\rangle_{A_4}|l_1\rangle_B - |0\rangle_{A_4}|l_2\rangle_B). \quad (25)$$

The reduced density matrices ρ_+, ρ_- of Bob's system B when Alice found A_3 as $|+\rangle$, $|-\rangle$, respectively, are both

$$\rho_+ = \rho_- = \frac{1}{2}(|l_1\rangle_B\langle l_1| + |l_2\rangle_B\langle l_2|). \quad (26)$$

Therefore, it is completely impossible for Bob to discriminate ρ_+ from ρ_- and deduce Alice's secret bit b in this case.

Since the probabilities for Alice to choose the basis $\{|0\rangle, |1\rangle\}$, or $\{|+\rangle, |-\rangle\}$ are both $1/2$, we can see that the

average probability for Bob to learn b unambiguously using Eq. (22) is $100\% \times (1/2) + 0\% \times (1/2) = 1/2$, which is the same as that in the honest case too.

Thus it is shown that both the 3-body entangled states equations (21) and (22) cannot increase dishonest Bob's probability for learning Alice's b unambiguously.

6. Summary

So we see that if Bob is limited to the technology to prepare 3-body (or less) entangled states, the probability for him to learn Alice's b unambiguously will remain to be $1/2$, which is the same as that in the honest case where he does not apply the entanglement-based attacks.

To increase this probability, dishonest Bob should at least use 4-body entangled states. Then he can learn b unambiguously with probability 53.1% (using von Neumann measurement) or 53.7% (using POVM). It is lower than the values 62.5% (von Neumann measurement) or 64.6% (POVM) achieved by the cheating strategy proposed in Ref. [31] based on 5-body entangled states, and is merely a little higher than the value $1/2$ in the honest case. However, it remain nontrivial, and like the strategy in Ref. [31], raising the number of qubits used in the protocol of Ref. [30] (i.e., the values of N and M) cannot lower this probability nor make it harder to cheat.

From a practical point of view, to implement the attack, Bob needs the capacity to prepare 4-body entangled states, and delay the measurement while keeping the entanglement from decoherence. At the end of the process, however, he merely needs to perform measurements on his system B alone. No need for collective measurements on the multi-system. Nevertheless, B is a 6-level system as shown in Eq. (1). If such a system is implemented with qubits, then it takes 3 qubits so that there cannot be less than 6 orthogonal states. The 4-body entangled state will actually take 6 qubits to implement, and the measurement on system B will become a collective one on 3 qubits. Thus the protocol of Ref. [30] remains secure until this technology becomes available in the future. More interestingly, as increasing N and M is useless, the honest participants can simply run the protocol with $N = M = 1$, i.e., only 4 qubits are needed for implementing the protocol, which saves a lot of quantum resources.

References

[1] Bennett C H and Brassard G 1984 in *Proceedings of IEEE Int. Conf. Computers, Systems, and Signal Processing*, Bangalore, India (IEEE, New York) p. 175
[2] Rabin M O 1981 *technical report TR-81* (Aiken Computation Laboratory, Harvard University) Available online at http://eprint.iacr.org/2005/187.pdf
[3] Even S, Goldreich O and Lempel A 1982 *Advances in Cryptology: Proc. Crypto* '82 (Plenum) p. 205
[4] Kilian J 1988 *Proc.* 1988 *ACM Annual Symposium on Theory of Computing* (ACM, New York) p. 20
[5] Colbeck R 2007 *Phys. Rev. A* **76** 062308
[6] Salvail L, Schaffner C and Sotakova M 2008 arXiv: 0902.4036
[7] Salvail L and Sotakova M 2009 arXiv: 0906.1671
[8] Colbeck R 2009 arXiv: 0911.3814
[9] Chailloux A, Kerenidis I and Sikora J 2013 *Quantum Inform. Comput.* **13** 158
[10] He G P 2011 *J. Phys. A: Math. Theor.* **44** 445305
[11] He G P 2015 *Phys. Rev. A* **92** 046301
[12] He G P 2018 *J. Phys. A: Math. Theor.* **51** 155301
[13] Wehner S, Schaffner C and Terhal B 2008 *Phys. Rev. Lett.* **100** 220502
[14] Schaffner C 2010 *Phys. Rev. A* **82** 032308
[15] Wei C Y, Cai X Q, Liu B, Wang T Y and Gao F 2018 *IEEE Trans. Comput.* **67** 2
[16] Guo X Q, Luo C L and Yan Y 2013 *J. Theor. Appl. Inform. Technol.* **47** 277
[17] Erven C, Ng N, Gigov N, Laflamme R, Wehner S and Weihs G 2014 *Nat. Commun.* **5** 3418
[18] Li Y B, Wen Q Y, Qin S J, Guo F Z and Sun Y 2014 *Quantum Inform. Process.* **13** 131
[19] Yang Y G, Xu P, Tian J and Zhang H 2014 *Optik* **125** 5409
[20] Yang Y G, Sun S and Wang Y 2014 *Int. J. Theor. Phys.* **54** 910
[21] He G P 2015 *Quantum Inform. Process.* **14** 2153
[22] Yang Y G, Yang R, Lei H, Shi W M and Zhou Y H 2015 *Quantum Inform. Process.* **14** 3031
[23] Yang Y G, Sun S J, Pan Q X and Xu P 2015 *Optik* **126** 3206
[24] Yang Y G, Sun S J, Pan Q X and Xu P 2015 *Optik* **126** 3838
[25] Pitalúa-García D 2016 *Phys. Rev. A* **93** 062346
[26] Plesch M, Pawłowski M and Pivoluska M 2017 *Phys. Rev. A* **95** 042324
[27] Yang Y G, Yang R, Cao W F, Chen X B, Zhou Y H and Shi W M 2017 *Int. J. Theor. Phys.* **56** 1286
[28] Furrer F, Gehring T, Schaffner C, Pacher C, Schnabel R and Wehner S 2018 *Nat. Commun.* **9** 1450
[29] Cheng X G, Guo R and Chen Y H 2018 *Int. J. Quantum Inform.* **16** 1850039
[30] Nagy M and Nagy N 2016 *Quantum Inform. Process.* **15** 5037
[31] He G P 2017 *Quantum Inform. Process.* **16** 96
[32] Herzog U and Bergou J A 2005 *Phys. Rev. A* **71** 050301