Available online at www.sciencedirect.com
ScienceDirect
Physics Letters A 363 (2007) 361–368
PHYSICS LETTERS A
www.elsevier.com/locate/pla

Threshold quantum cryptograph based on Grover's algorithm

Jian-Zhong Du [a,b,*], Su-Juan Qin [a], Qiao-Yan Wen [a], Fu-Chen Zhu [c]

[a] *School of Science, Beijing University of Posts and Telecommunications, Beijing 100876, China*
[b] *State Key Laboratory of Integrated Services Network, Xidian University, Xi'an 710071, China*
[c] *National Laboratory for Modern Communications, P.O. Box 810, Chengdu 610041, China*

Received 24 June 2006; received in revised form 13 November 2006; accepted 14 November 2006

Available online 21 November 2006

Communicated by P.R. Holland

Abstract

We propose a threshold quantum protocol based on Grover's operator and permutation operator on one two-qubit signal. The protocol is secure because the dishonest parties can only extract 2 bits from 3 bits information of operation on one two-qubit signal while they have to introduce error probability 3/8. The protocol includes a detection scheme to resist Trojan horse attack. With probability 1/2, the detection scheme can detect a multi-qubit signal that is used to replace a single-qubit signal, while it makes every legitimate qubit invariant.

PACS: 03.67.Dd; 03.65.Ud

Keywords: Quantum cryptography; Grover search algorithm; Secure multi-party computation

1. Introduction

In a secure multi-party computation [1,2], n parties, $P_1, P_2, \ldots, P_n$, compute and reveal the result of the multi-variable function $f(x_1, x_2, \ldots, x_n)$, where x_i is a secret input provided by P_i. It is also necessary to protect the maximum privacy of each input x_i. The menace of input leakage comes from eavesdroppers outside and dishonest parties inside. In contrast to the eavesdroppers outside, the dishonest parties inside have many advantages to attack another's input. As pointed out in Ref. [3], if multi-party scheme is secure for the dishonest parties, it is secure for any eavesdropper.

Based on the operators $I = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $U = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, $H = \frac{1}{\sqrt{2}}\left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$ and $\bar{H} = \frac{1}{\sqrt{2}}\left(\begin{smallmatrix} -1 & 1 \\ 1 & 1 \end{smallmatrix}\right)$, two quantum versions of secure multi-party computation, multi-party quantum secret sharing (MQSS) protocol [4] and threshold quantum protocol [5], have been proposed, which are inspired by the work of Deng et al. in quantum secure direct communication (QSDC) protocols [6,7]. Lucamarini and Mancini [8] showed that these protocols [4–7] are quasisecure to eavesdropper outside. But a dishonest party inside can gain another's secret input in the two quantum multi-party protocols [4,5], using a multi-photon signal instead of a legitimate single-photon signal introduced by Deng et al. [9], or using the fake state introduced by Qin et al. [10]. To avoid these attacks to the MQSS protocol [4], all the parties have to pick out a subset of the photons as the sample for checking cheat. The sample schemes [9,10] can also revise the threshold quantum protocol [5] to improve the security. However the number of qubits of the quantum state generated by the threshold protocol revised must exceed that of the quantum state generated by the original (nonthreshold) protocol. We do not follow this line of argument. Instead we modify the protocol using two-qubit quantum operation.

In this Letter, instead of one-qubit operators, we show that two-qubit operators based on Grover's algorithm [11,12] can adapt to threshold quantum protocol. Each party does one of eight kinds of operations on every two-qubit signal as input. The dishonest

* Corresponding author.
E-mail address: ddddjjjjzzzz@tom.com (J.-Z. Du).

0375-9601/$ – see front matter
doi:10.1016/j.physleta.2006.11.024

parties can only extract 2 bits from 3 bits information of operation on one two-qubit signal while they have to introduce error probability 3/8. The property guarantees the threshold quantum protocol against an attack with a fake signal. Since three-qubit Grover's algorithm has been experimentally realized [13], the threshold quantum protocol becomes highly practical for experimental realization. Furthermore, we also propose a detection scheme to find Trojan horse attack [9,14]. The detection scheme can detect every multi-qubit signal with probability 1/2, while it makes every legitimate single-qubit signal invariant.

This Letter is organized as follows. Section 2 introduces two-qubit operators based on Grover's algorithm [11]. Section 3 proposes a t-out-of-n quantum cash threshold protocol followed the line sketched in Ref. [5] but with some relevant differences. Section 4 shows security of the threshold protocol. Section 5 proofs that Trojan horse attack can be detected. Section 6 then draws some conclusions.

2. Two-qubit operations based on Grover's algorithm

Grover's operator [11] on the two-qubit system case

$$V = \frac{1}{2}\begin{pmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix} \tag{1}$$

can transform the basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ to the basis $\{|\overline{00}\rangle = (1/2)(-|00\rangle + |01\rangle + |10\rangle + |11\rangle), |\overline{01}\rangle = (1/2)(|00\rangle - |01\rangle + |10\rangle + |11\rangle), |\overline{10}\rangle = (1/2)(|00\rangle + |01\rangle - |10\rangle + |11\rangle), |\overline{11}\rangle = (1/2)(|00\rangle + |01\rangle + |10\rangle - |11\rangle)\}$. V can also transform the basis $\{|\overline{00}\rangle, |\overline{01}\rangle, |\overline{10}\rangle, |\overline{11}\rangle\}$ to the basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$.

A permutation operator

$$U = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{2}$$

has properties: $U|00\rangle = |01\rangle$, $U|01\rangle = |10\rangle$, $U|10\rangle = |11\rangle$, $U|11\rangle = |00\rangle$, $U|\overline{00}\rangle = |\overline{01}\rangle$, $U|\overline{01}\rangle = |\overline{10}\rangle$, $U|\overline{10}\rangle = |\overline{11}\rangle$, and $U|\overline{11}\rangle = |\overline{00}\rangle$.

V and U are commute operators. U encodes a classical quaterit on one non-orthogonal two-qubit signal and V changes the base of one two-qubit signal. A digit called "quaterit" for quaternary number system consisting of four digit (00, 01, 10, 11).

3. t-out-n threshold scheme

We propose the t-out-of-n threshold version of quantum cash protocol following the line sketched in Ref. [5]. There are three differences between our protocol and the protocol proposed by Tokunaga et al. [5] mainly: one is the assumption that some parties are dishonest instead of the assumption that all parties are honest, one is two-qubit operation instead of one-qubit operation to resist the attack proposed by Ref. [10], another is an additional detection to resist Trojan horse attack [9,14].

Each banknote with L_K contains a secret binary string K, where L_K is a kind of serial number. We use the same notations as in Ref. [5]. For simplicity of description, we do not distinguish between the element over $\mathbf{F}_{2^N}$ and its binary representation.

Distribute phase. In this phase, a dealer splits the secret K into n classical shared secrets and distributes the shared secrets to centers.

(i) A dealer uniformly chooses an original binary secret

$$K = (a_1, b_1, a_2, b_2, \ldots, a_m, b_m) \tag{3}$$

for each banknote with L_K, where $a_i \in \{00, 01, 10, 11\}$ and $b_i \in \{0, 1\}$.

(ii) The dealer then makes n shares $S_1, \ldots, S_n$ of K using Shamir's secret sharing scheme [15] over $\mathbf{F}_{2^N}$ as follows, where $N = 3m$. The dealer chooses x_j's for $j = 1, \ldots, n$ which are n distinct, nonzero elements in $\mathbf{F}_{2^N}$. The dealer randomly chooses a secret $(t-1)$th-degree polynomial $f(x)$ over $\mathbf{F}_{2^N}$, where $f(0) = K$. Then the dealer computes $S_j = f(x_j)$ for $j = 1, \ldots, n$ over $\mathbf{F}_{2^N}$.

(iii) For each $\{k_1, \ldots, k_t\} \subseteq \{1, \ldots, n\}$, the dealer calculates the following value

$$K^{[k_j]} = S_{k_j} \prod_{1 \leqslant l \leqslant t, l \neq j} \frac{x_{k_l}}{x_{k_l} - x_{k_j}}, \quad j = 1, \ldots, t \tag{4}$$

over $\mathbf{F}_{2^N}$. Let

$$K^{[k_j]} = \left(a_1^{[k_j]}, b_1^{[k_j]}, a_2^{[k_j]}, b_2^{[k_j]}, \ldots, a_m^{[k_j]}, b_m^{[k_j]}\right), \tag{5}$$

where $a_i^{[k_j]} \in \{00, 01, 10, 11\}$ and $b_i^{[k_j]} \in \{0, 1\}$. These values satisfy the equation $K = \bigoplus_{j=1}^{t} K^{[k_j]}$, where $\oplus$ represents bitwise addition, $0 \oplus 0 = 0$, $0 \oplus 1 = 1$, $1 \oplus 0 = 1$, and $1 \oplus 1 = 0$. The dealer computes $\boxplus_{j=1}^{t} a_i^{[k_j]}$, where $\boxplus$ represents quateritwise addition, namely binary addition module 100, for example, $00 \boxplus 01 = 01$, $01 \boxplus 01 = 10$, $01 \boxplus 10 = 11$, and $01 \boxplus 11 = 00$. If there exists an

$$a_i \neq \boxplus_{j=1}^{t} a_i^{[k_j]}, \tag{6}$$

the dealer returns to (ii), and chooses different x_j's for $j = 1, \ldots, n$, or different $f(x)$ in (ii).

(iv) The dealer secretly sends S_j with L_K to center P_j for each $j = 1, \ldots, n$. Each x_j with L_K, used as a corresponding value for the center P_j, is published.

Precomputation phase. In the phase, every collaborative center P_{k_j}, where $k_j \in \{1, \ldots, n\}$, computes the preliminary information $K^{[k_j]}$ using Eq. (4) with his shared secret S_{k_j} and t public elements x_{k_l}'s of t collaborative centers. The set of collaborative centers can be different in each issuing or checking. Note that even in the following collaboration procedure, $K^{[k_j]}$ is kept secretly at P_{k_j} and the original secret K is not recovered.

Issuing phase. In this phase, t centers collaborate to issue a banknote $(L_K, |\phi\rangle)$ implying the secret K. Here, we assume that the t centers are $P_1, \ldots, P_t$. Hereafter, we will describe a sequential protocol from P_1 to P_t, but the order is not essential, and any order is possible.

(i) P_1 generates a quantum state

$$\left|\phi^{[1]}\right\rangle = |\psi_{a_1^{[1]}, b_1^{[1]}}\rangle \otimes |\psi_{a_2^{[1]}, b_2^{[1]}}\rangle \otimes \cdots \otimes |\psi_{a_m^{[1]}, b_m^{[1]}}\rangle, \tag{7}$$

and then sends the $(L_K, |\phi^{[1]}\rangle)$ to P_2, where $|\psi_{a_i^{[1]}, b_i^{[1]}}\rangle$ is defined as:

$$\begin{aligned} &|\psi_{00,0}\rangle = |00\rangle, \quad |\psi_{01,0}\rangle = |01\rangle, \quad |\psi_{10,0}\rangle = |10\rangle, \quad |\psi_{11,0}\rangle = |11\rangle, \\ &|\psi_{00,1}\rangle = |\overline{00}\rangle, \quad |\psi_{01,1}\rangle = |\overline{01}\rangle, \quad |\psi_{10,1}\rangle = |\overline{10}\rangle, \quad |\psi_{11,1}\rangle = |\overline{11}\rangle. \end{aligned} \tag{8}$$

The value of $b_i^{[1]}$ determines the kind of the basis. If $b_i^{[1]}$ is 0 then $a_i^{[1]}$ is encoded in the basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$; if $b_i^{[1]}$ is 1 then $a_i^{[1]}$ is encoded in the basis $\{|\overline{00}\rangle, |\overline{01}\rangle, |\overline{10}\rangle, |\overline{11}\rangle\}$.

(ii) For each $j = 2, \ldots, t$, when P_j receives $(L_K, |\phi^{[j-1]}\rangle)$ from P_{j-1}, he detects Trojan horse attack and encodes his secret input on $|\phi^{[j-1]}\rangle$.

Our detection scheme is depicted in Fig. 1. To every qubit $|d\rangle$ of $|\phi^{[j-1]}\rangle$, called data qubit, P_j randomly choices auxiliary qubit $|a\rangle = |0\rangle$ or $|a\rangle = |1\rangle$ with equal probability, and performs *Hadamard* gate on $|a\rangle$. He performs one *CNOT* gates on the auxiliary qubit and the data qubit (the former is the controller and the latter is the target). Then he performs the unitary transformation

$$T = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & -1 & 0 \end{pmatrix} \tag{9}$$

on the auxiliary qubit and the data qubit. After that, he measures the auxiliary qubit $|a\rangle$ in basis $\{|0\rangle, |1\rangle\}$. To legitimate single qubit $|d\rangle$, matrix multiplication $T_{ad} \cdot CNOT_{ad} \cdot (H_a \otimes I_d) = I_a \otimes I_d$, so both the data qubit and the auxiliary qubit are invariant. If the auxiliary qubit $|a\rangle$ flips, $|d\rangle$ must be replaced by a multi-qubit signal. To all the qubits of $|\phi^{[j-1]}\rangle$, even if just one multi-qubit

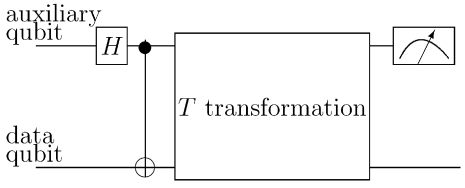

Fig. 1. Detection scheme of Trojan horse attack.

signal is detected, P_j rejects the banknote. In Section 5, we prove that the detection scheme can detect every multi-qubit signal with probability $1/2$.

After making sure that no Trojan horse attack is detected, P_j applies the following transformation $W^{[j]}$ to $|\phi^{[j-1]}\rangle$:

$$W^{[j]} = U_1^{[j]}V_1^{[j]} \otimes U_2^{[j]}V_2^{[j]} \otimes \cdots \otimes U_m^{[j]}V_m^{[j]}, \tag{10}$$

where

$$\begin{aligned} &U_i^{[j]} = U\big(a_i^{[j]}\big), \qquad V_i^{[j]} = V\big(b_i^{[j]}\big), \qquad U(00) = I, \qquad U(01) = U, \\ &U(10) = UU, \qquad U(11) = UUU, \qquad V(0) = I, \qquad V(1) = V. \end{aligned} \tag{11}$$

P_j then obtains $|\phi^{[j]}\rangle$ by the unitary transformation

$$W^{[j]}: \big|\phi^{[j-1]}\big\rangle \mapsto \big|\phi^{[j]}\big\rangle, \tag{12}$$

and sends $(L_K, |\phi^{[j]}\rangle)$ to P_{j+1} (P_{t+1} is the user whom the banknote is issued to).

Checking phase. In this phase, t centers collaborate to check the validity of quantum banknote $(L_K, |\phi'\rangle)$. A quantum banknote $(L_K, |\phi'\rangle)$ is valid if $|\phi'\rangle$ implies the secret K. Here, we assume that the t centers are $P'_1, \ldots, P'_t$. This set of t centers can be different from the set of centers who collaborate to issue the banknote. Each P'_j has calculated $K^{[j]\prime} = (a_1^{[j]\prime}, b_1^{[j]\prime}, a_2^{[j]\prime}, b_2^{[j]\prime}, \ldots, a_m^{[j]\prime}, b_m^{[j]\prime})$ in the precomputation phase. Let $|\phi^{[0]\prime}\rangle = |\phi'\rangle$, and P'_0 be the shop.

(i) For each $j = 1, \ldots, t$, after P'_j receives $(L_K, |\phi^{[j-1]\prime}\rangle)$ from P'_{j-1} and makes sure no Trojan horse attack, he applies the following transformation $W^{[j]\prime}$ to $|\phi^{[j-1]\prime}\rangle$:

$$W^{[j]\prime} = \underline{U_1^{[j]\prime}}V_1^{[j]\prime} \otimes \underline{U_2^{[j]\prime}}V_2^{[j]\prime} \otimes \cdots \otimes \underline{U_m^{[j]\prime}}V_m^{[j]\prime}, \tag{13}$$

where

$$V_i^{[j]\prime} = V\big(b_i^{[j]\prime}\big), \qquad \underline{U_i^{[j]\prime}} = U\big(\underline{a_i^{[j]\prime}}\big), \qquad \underline{00} = 00, \qquad \underline{01} = 11, \qquad \underline{10} = 10, \qquad \underline{11} = 01. \tag{14}$$

P_j then obtains $|\eta^{[j]\prime}\rangle$ by the unitary transformation

$$W^{[j]\prime}: \big|\phi^{[j-1]\prime}\big\rangle \mapsto \big|\eta^{[j]\prime}\big\rangle. \tag{15}$$

Additionally, P'_j chooses a secret

$$x^{[j]\prime} = \big(x_1^{[j]\prime}, x_2^{[j]\prime}, \ldots, x_m^{[j]\prime}\big), \tag{16}$$

where $x_i^{[j]\prime}$ is uniformly chosen from $\{0, 1\}$. P'_j then obtains $|\phi^{[j]\prime}\rangle$ by the unitary transformation

$$V\big(x_1^{[j]\prime}\big) \otimes \cdots \otimes V\big(x_m^{[j]\prime}\big): \big|\eta^{[j]\prime}\big\rangle \mapsto \big|\phi^{[j]\prime}\big\rangle. \tag{17}$$

P'_j sends $(L_K, |\phi^{[j]\prime}\rangle)$ to P'_{j+1} (P'_{t+1} is the trusted measurer).

(ii) Finally, the trusted measurer requires P'_j $(j = 1, \ldots, t)$ to send the $x^{[j]\prime}$ to him secretly, and then measures $|\phi^{[t]\prime}\rangle$ in bases $(\bigoplus_{j=1}^t x_1^{[j]\prime}, \ldots, \bigoplus_{j=1}^t x_m^{[j]\prime})$. The measurer gets and announces the string of measurement outcome

$$(c_1, \ldots, c_m). \tag{18}$$

The centers check whether $c_i = 00$ for all $i = 1, \ldots, m$. Even if just one result is not 00, the centers reject the banknote.

Necessity of the trusted measurer: If $(L_K, |\phi'\rangle)$ is an invalid quantum banknote, a dishonest measurer can always deceive the centers by announcing $(c_1, \ldots, c_m) = (00, \ldots, 00)$. So an honest measurer is necessary. It is also necessary that the trusted measurer receives the value $x^{[j]\prime}$ secretly, otherwise the center P'_t can always send the quantum states $|\phi^{[t]\prime}\rangle = |00\rangle \otimes \cdots \otimes |00\rangle$ to deceive the trusted measurer.

4. Security proof

The impossibility of Eve's eavesdropping outside in the threshold quantum protocol was shown using the quantum key distribution approach, following the line sketched in [16]. So we only need to consider the parties' cheat inside. Without loss of generality, assume that only one dishonest party is the cheater inside. A dishonest party, called Bob, is an evil quantum physicist able to build all devices that are allowed by the laws of quantum mechanics. Her aim is to elicit the input of another party, called Alice, and then

to reconstruct the quantum cash with $t-2$ other parties. For convenience of analysis, without loss of generality, we also assume that Alice does one of eight kinds of operations on every two-qubit signal with equal probability and that every two-qubit operation is independent. So it is sufficient to consider Bob's cheat on one two-qubit signal.

Let $|\phi_u\rangle$ be the two-qubit quantum state which Bob should send to Alice. Instead of $|\phi_u\rangle$, Bob prepares a fake signal $|\theta\rangle$ and sends it to Alice. Then from the fake signal operated by Alice, Bob tries to extract Alice's input information. Based on his extracted information, Bob reconstructs the quantum state $|\phi_v\rangle$ and resends it to Alice's next party.

Bob's fake signal can be presented as $|\theta\rangle = |00\rangle[(a_0+ia_1)|A\rangle + (b_0+ib_1)|B\rangle + (c_0+ic_1)|C\rangle + (d_0+id_1)|D\rangle] + |01\rangle[(e_0+ie_1)|A\rangle + (f_0+if_1)|B\rangle + (g_0+ig_1)|C\rangle + (h_0+ih_1)|D\rangle] + |10\rangle[(l_0+il_1)|A\rangle + (j_0+ij_1)|B\rangle + (k_0+ik_1)|C\rangle + (q_0+iq_1)|D\rangle] + |11\rangle[(m_0+im_1)|A\rangle + (n_0+in_1)|B\rangle + (r_0+ir_1)|C\rangle + (s_0+is_1)|D\rangle]$, where $|A\rangle$, $|B\rangle$, $|C\rangle$, and $|D\rangle$ are normalized orthogonal states, i is the imaginary unit, the rest of coefficients are real, and

$$\begin{aligned} &a_0^2+b_0^2+c_0^2+d_0^2+e_0^2+f_0^2+g_0^2+h_0^2+l_0^2+j_0^2+k_0^2+q_0^2+m_0^2+n_0^2+r_0^2+s_0^2+a_1^2+b_1^2+c_1^2+d_1^2+e_1^2+f_1^2+g_1^2\\ &\quad+h_1^2+l_1^2+j_1^2+k_1^2+q_1^2+m_1^2+n_1^2+r_1^2+s_1^2=1. \end{aligned} \tag{19}$$

Bob sends the former two-qubit signal to Alice and leaves the rest himself.

After Alice encoding, the fake signal $|\theta\rangle$ is converted into

$$\begin{aligned} &|\theta_{000}\rangle = \big(U(00)V(0)\otimes I\big)|\theta\rangle, \qquad |\theta_{010}\rangle = \big(U(01)V(0)\otimes I\big)|\theta\rangle,\\ &|\theta_{100}\rangle = \big(U(10)V(0)\otimes I\big)|\theta\rangle, \qquad |\theta_{110}\rangle = \big(U(11)V(0)\otimes I\big)|\theta\rangle,\\ &|\theta_{001}\rangle = \big(U(00)V(1)\otimes I\big)|\theta\rangle = \frac{1}{2}\big(-|\theta_{000}\rangle + |\theta_{010}\rangle + |\theta_{100}\rangle + |\theta_{110}\rangle\big),\\ &|\theta_{011}\rangle = \big(U(01)V(1)\otimes I\big)|\theta\rangle = \frac{1}{2}\big(|\theta_{000}\rangle - |\theta_{010}\rangle + |\theta_{100}\rangle + |\theta_{110}\rangle\big),\\ &|\theta_{101}\rangle = \big(U(10)V(1)\otimes I\big)|\theta\rangle = \frac{1}{2}\big(|\theta_{000}\rangle + |\theta_{010}\rangle - |\theta_{100}\rangle + |\theta_{110}\rangle\big),\\ &\text{or } |\theta_{111}\rangle = \big(U(11)V(1)\otimes I\big)|\theta\rangle = \frac{1}{2}\big(|\theta_{000}\rangle + |\theta_{010}\rangle + |\theta_{100}\rangle - |\theta_{110}\rangle\big). \end{aligned} \tag{20}$$

After Alice performs the eight kinds of operations on the fake signal with equal probability, the state reads

$$w = \frac{1}{8}\big(|\theta_{000}\rangle\langle\theta_{000}| + |\theta_{010}\rangle\langle\theta_{010}| + |\theta_{100}\rangle\langle\theta_{100}| + |\theta_{110}\rangle\langle\theta_{110}| + |\theta_{001}\rangle\langle\theta_{001}| + |\theta_{011}\rangle\langle\theta_{011}| + |\theta_{101}\rangle\langle\theta_{101}| + |\theta_{111}\rangle\langle\theta_{111}|\big), \tag{21}$$

which can be rewritten as the matrix form in the orthogonal basis $\{|00A\rangle, |00B\rangle, |00C\rangle, |00D\rangle, |01A\rangle, |01B\rangle, |01C\rangle, |01D\rangle, |10A\rangle, |10B\rangle, |10C\rangle, |10D\rangle, |11A\rangle, |11B\rangle, |11C\rangle, |11D\rangle\}$. We relabel w as the matrix form as following.

The mutual information of Bob and Alice, I(Alice, Bob), which can be extracted from the fake signal, is estimated by the Holevo bound [17], $I(\text{Alice, Bob}) \leqslant S(w) - \sum_{i,j,k=0}^{1} \frac{1}{8} S(|\theta_{ijk}\rangle\langle\theta_{ijk}|) = -\operatorname{tr}\{w\log_2 w\}$. In order to calculate the *von-Neumann* entropy, $-\operatorname{tr}\{w\log_2 w\}$, we need the eigenvalues λ of the matrix w. For simplicity of computation, we equivalently compute the eigenvalues of the matrix XwX^+, yielding the 16 eigenvalues

$$\begin{aligned} \lambda_{1,2} &= \frac{1}{4}\big[(a_0-l_0)^2+(a_1-l_1)^2+(b_0-j_0)^2+(b_1-j_1)^2+(c_0-k_0)^2+(c_1-k_1)^2+(e_0-m_0)^2+(e_1-m_1)^2\\ &\quad+(f_0-n_0)^2+(f_1-n_1)^2+(d_0-q_0)^2+(d_1-q_1)^2+(g_0-r_0)^2+(g_1-r_1)^2+(h_0-s_0)^2+(h_1-s_1)^2\big]\\ &\quad\pm\frac{1}{2}(b_1f_0-b_0f_1+c_1g_0-c_0g_1+d_1h_0-d_0h_1+e_1l_0-e_0l_1+f_1j_0-f_0j_1+g_1k_0-g_0k_1+a_1e_0-a_1m_0+l_1m_0\\ &\quad-l_0m_1-a_0e_1+a_0m_1-b_1n_0+j_1n_0+b_0n_1-j_0n_1+h_1q_0-h_0q_1-c_1r_0+k_1r_0+c_0r_1-k_0r_1-d_1s_0\\ &\quad+q_1s_0+d_0s_1-q_0s_1),\\ \lambda_3 &= \frac{1}{4}\big[(a_0-e_0+l_0-m_0)^2+(b_0-f_0+j_0-n_0)^2+(c_0-g_0+k_0-r_0)^2+(d_0-h_0+q_0-s_0)^2+(a_1-e_1+l_1-m_1)^2\\ &\quad+(b_1-f_1+j_1-n_1)^2+(c_1-g_1+k_1-r_1)^2+(d_1-h_1+q_1-s_1)^2\big],\\ \lambda_4 &= \frac{1}{4}\big[(a_0+e_0+l_0+m_0)^2+(b_0+f_0+j_0+n_0)^2+(c_0+g_0+k_0+r_0)^2+(d_0+h_0+q_0+s_0)^2+(a_1+e_1+l_1+m_1)^2\\ &\quad+(b_1+f_1+j_1+n_1)^2+(c_1+g_1+k_1+r_1)^2+(d_1+h_1+q_1+s_1)^2\big],\\ \lambda_{5-16} &= 0, \end{aligned} \tag{22}$$

where

$$X = \begin{pmatrix}
\frac{1}{\sqrt{2}} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -\frac{1}{\sqrt{2}} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & \frac{1}{\sqrt{2}} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -\frac{1}{\sqrt{2}} & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & \frac{1}{\sqrt{2}} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -\frac{1}{\sqrt{2}} & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & \frac{1}{\sqrt{2}} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -\frac{1}{\sqrt{2}} & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & \frac{1}{\sqrt{2}} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -\frac{1}{\sqrt{2}} & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & \frac{1}{\sqrt{2}} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -\frac{1}{\sqrt{2}} & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{\sqrt{2}} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -\frac{1}{\sqrt{2}} & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{\sqrt{2}} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -\frac{1}{\sqrt{2}} \\
\frac{1}{2} & 0 & 0 & 0 & -\frac{1}{2} & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 & -\frac{1}{2} & 0 & 0 & 0 \\
0 & \frac{1}{2} & 0 & 0 & 0 & -\frac{1}{2} & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 & -\frac{1}{2} & 0 & 0 \\
0 & 0 & \frac{1}{2} & 0 & 0 & 0 & -\frac{1}{2} & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 & -\frac{1}{2} & 0 \\
0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 & -\frac{1}{2} & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 & -\frac{1}{2} \\
\frac{1}{2} & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 \\
0 & \frac{1}{2} & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 \\
0 & 0 & \frac{1}{2} & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 & \frac{1}{2} & 0 \\
0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 & \frac{1}{2}
\end{pmatrix}. \tag{23}$$

So we have

$$I(\text{Alice, Bob}) \leqslant -\lambda_1 \log_2 \lambda_1 - \lambda_2 \log_2 \lambda_2 - \lambda_3 \log_2 \lambda_3 - \lambda_4 \log_2 \lambda_4. \tag{24}$$

Only $\lambda_1 = \lambda_2 = \lambda_3 = \lambda_4 = 1/4$, $I(\text{Alice, Bob})$ reaches the maximal value 2 bits. We can deduce that $I(\text{Alice, Bob}) = 2$ if and only if $|\theta_{000}\rangle$, $|\theta_{010}\rangle$, $|\theta_{100}\rangle$, and $|\theta_{110}\rangle$ are the normalized orthogonal states.

Bob has to introduce 3/8 quaterit error rate when he gains the maximal value of $I(\text{Alice, Bob})$. Let $x = pqr$ be Alice's input and $y = ijk$ be Bob's extracted result when $I(\text{Alice, Bob}) = 2$, where $i, j, k, p, q, r = 0, 1$. In order to introduce the minimum error, basing on maximum-likelihood estimation, Bob has to resend the quantum state $|\phi_v\rangle = (U(ij)V(k))|\phi_u\rangle$ to Alice's next party. With probability $1 - |\langle\phi_v|(U(pq)V(r)\phi_u\rangle|^2$, the measurer's result is not 00. So the quaterit error rate is $1 - |\langle\phi_v|(U(pq)V(r))\phi_u\rangle|^2$. If Bob gains the extracted result $y = ijk$, the quaterit error rate is $1 - \sum_{p,q,r=0}^{1} P(x = pqr|y = ijk)|\langle\phi_u|(U(ij)V(k))^+(U(pq)V(r))|\phi_u\rangle|^2$. One gets $P(y = ijk|x = pqk) = |\langle\theta|(U(ij)V(k) \otimes I)^+(U(pq)V(k) \otimes I)|\theta\rangle|^2 = \delta_{ij,pq}$, $P(y = ijk|x = pq\bar{k}) = |\langle\theta|(U(ij)V(k) \otimes I)^+(U(pq)V(\bar{k}) \otimes I)|\theta\rangle|^2 = \frac{1}{4}$, and $P(x = pqk) = \frac{1}{8}$, where $\bar{0} = 1$, $\bar{1} = 0$ and $\delta_{ij,pq}$ is the Kronecker function. With Bayes's theorem:

$$P(x|y) = \frac{P(y|x)P(x)}{\sum_x P(y|x)P(x)}. \tag{25}$$

We get $P(x = pqk|y = ijk) = \frac{1}{2}\delta_{ij,pq}$ and $P(x = pq\bar{k}|y = ijk) = \frac{1}{8}$. The quaterit error rate is

$$1 - \sum_{p,q=0}^{1} P(x = pqk|y = ijk)\big|\langle\phi_u|\big(U(ij)V(k)\big)^+\big(U(pq)V(k)\big)|\phi_u\rangle\big|^2 - \sum_{p,q=0}^{1} P(x = pq\bar{k}|y = ijk)\big|\langle\phi_u|\big(U(ij)V(k)\big)^+\big(U(pq)V(\bar{k})\big)|\phi_u\rangle\big|^2 = \frac{3}{8}. \tag{26}$$

5. Trojan horse attack can be detected

Trojan horse attack bases on the idea that we can precisely know an unknown quantum state by measuring many copies of the state. Let Bob prepare the multi-qubit $\sum_{i_1 i_2 \ldots i_m} a_{i_1 i_2 \ldots i_m}|i_1 i_2 \ldots i_m\rangle_{1,2,\ldots m}$ $(m \geqslant 2)$ to replace one data qubit $|d\rangle$.

In the detection scheme of Trojan horse arrack (Fig. 1), Alice randomly prepares an auxiliary qubit $|a\rangle = |0\rangle$ or $|a\rangle = |1\rangle$ with equal probability.

After the operation $H|a\rangle$, the system state is

$$\big|\eta_1^0\big\rangle = \frac{1}{\sqrt{2}} \sum_{i_1 i_2 \ldots i_m} a_{i_1 i_2 \ldots i_m}\big(|0\rangle + |1\rangle\big)|i_1 i_2 \ldots i_m\rangle_{1,2,\ldots,m} \quad \big(|a\rangle = |0\rangle\big) \quad \text{or}$$

$$\left|\eta_1^1\right\rangle = \frac{1}{\sqrt{2}} \sum_{i_1 i_2 \ldots i_m} a_{i_1 i_2 \ldots i_m} \big(|0\rangle - |1\rangle\big)|i_1 i_2 \ldots i_m\rangle_{1,2,\ldots,m} \quad \big(|a\rangle = |1\rangle\big). \tag{27}$$

Here we use superscripts 0 and 1 to denote the states corresponding to $a = 0$ and $a = 1$, respectively. This notation also applies to the following equations and we will, for simplicity, suppress the word "or" later.

Instead of the operator $CNOT_{ad}$, the operators $CNOT_{a1}, CNOT_{a2}, \ldots, CNOT_{am}$ are performed. The system state is

$$\begin{aligned}
\left|\eta_2^0\right\rangle &= \frac{1}{\sqrt{2}} \sum_{i_1 i_2 \ldots i_m} a_{i_1 i_2 \ldots i_m} \big(|0\rangle|i_1 i_2 \ldots i_m\rangle_{1,2,\ldots,m} + |1\rangle|\overline{i_1} i_2 \ldots \overline{i_m}\,\rangle_{1,2,\ldots,m}\big), \\
\left|\eta_2^1\right\rangle &= \frac{1}{\sqrt{2}} \sum_{i_1 i_2 \ldots i_m} a_{i_1 i_2 \ldots i_m} \big(|0\rangle|i_1 i_2 \ldots i_m\rangle_{1,2,\ldots,m} - |1\rangle|\overline{i_1} i_2 \ldots \overline{i_m}\,\rangle_{1,2,\ldots,m}\big).
\end{aligned} \tag{28}$$

Instead of the operator T_{ad}, the operators $T_{a1}, T_{a2}, \ldots, T_{am}$ are performed. The system state is

$$\begin{aligned}
\left|\eta_3^0\right\rangle &= \frac{1}{\sqrt{2^{m+1}}} \sum_{i_1 i_2 \ldots i_m} |0\rangle|i_1 i_2 \ldots i_m\rangle_{1,2,\ldots,m} \Bigg\{ \sum_{x_2 \ldots x_m} \big[(-1)^{\tau(i_1 x_2 \ldots x_m \oplus i_1 i_2 \ldots i_m)} + (-1)^{\tau(i_1 x_2 \ldots x_m \oplus \overline{i_1} \overline{i_2} \ldots \overline{i_m})}\big] a_{i_1 x_2 \ldots x_m} \Bigg\} \\
&\quad + \frac{1}{\sqrt{2^{m+1}}} \sum_{i_1 i_2 \ldots i_m} |1\rangle|i_1 i_2 \ldots i_m\rangle_{1,2,\ldots,m} \Bigg\{ \sum_{x_2 \ldots x_m} \big[(-1)^{\tau(i_1 x_2 \ldots x_m 1 \oplus i_1 i_2 \ldots i_m 0)} + (-1)^{\tau(i_1 x_2 \ldots x_m 1 \oplus \overline{i_1} \overline{i_2} \ldots \overline{i_m} 0)}\big] a_{i_1 x_2 \ldots x_m} \Bigg\}, \\
\left|\eta_3^1\right\rangle &= \frac{1}{\sqrt{2^{m+1}}} \sum_{i_1 i_2 \ldots i_m} |0\rangle|i_1 i_2 \ldots i_m\rangle_{1,2,\ldots,m} \Bigg\{ \sum_{x_2 \ldots x_m} \big[(-1)^{\tau(i_1 x_2 \ldots x_m \oplus i_1 i_2 \ldots i_m)} + (-1)^{\tau(i_1 x_2 \ldots x_m \oplus \overline{i_1} \overline{i_2} \ldots \overline{i_m}) + 1}\big] a_{i_1 x_2 \ldots x_m} \Bigg\} \\
&\quad + \frac{1}{\sqrt{2^{m+1}}} \sum_{i_1 i_2 \ldots i_m} |1\rangle|i_1 i_2 \ldots i_m\rangle_{1,2,\ldots,m} \Bigg\{ \sum_{x_2 \ldots x_m} \big[(-1)^{\tau(i_1 x_2 \ldots x_m 1 \oplus i_1 i_2 \ldots i_m 0)} + (-1)^{\tau(i_1 x_2 \ldots x_m 1 \oplus \overline{i_1} \overline{i_2} \ldots \overline{i_m} 0) + 1}\big] a_{i_1 x_2 \ldots x_m} \Bigg\},
\end{aligned} \tag{29}$$

where $\bar{0} = 1$, $\bar{1} = 0$, and $\tau(x_1 x_2 \ldots x_n)$ represents the number of $x_k x_{k+1} = 11$ $(k = 1, 2, \ldots, n-1)$, for example, $\tau(1100111) = 3$, $\tau(1011011) = 2$.

The detection scheme can detect a multi-qubit signal instead of a single-qubit signal with probability $1/2$. When $m \geqslant 4$, the probability amplitude of $|0\rangle|i_1 \ldots i_{m-3} i_{m-2} i_{m-1} i_m\rangle$ in $|\eta_3^0\rangle$ and that of $|0\rangle|i_1 \ldots i_{m-3} \overline{i_{m-2}} i_{m-1} \overline{i_m}\,\rangle$ in $|\eta_3^1\rangle$ are same or opposite, so the probability of $|a\rangle = |0\rangle$ in the $|\eta_3^0\rangle$ equals to the probability of $|a\rangle = |0\rangle$ in the $|\eta_3^1\rangle$. Additionally verifying the cases of $m = 2, 3$, we can conclude that if we gain the measurement outcome $|a\rangle = |1\rangle$ in the $|\eta_3^0\rangle$ with probability α, we must gain the measurement outcome $|a\rangle = |0\rangle$ in the $|\eta_3^1\rangle$ with probability $1 - \alpha$. Because $|\eta_3^0\rangle$ and $|\eta_3^1\rangle$ are chosen with equal probability, so the auxiliary qubit flips with probability $1/2$.

Since the detection is a linear operation applied to quantum state, it will work not only with pure states, but also with mixed states. To the legitimate two qubits $|\overline{00}\rangle$, $|\overline{01}\rangle$, $|\overline{10}\rangle$, or $|\overline{11}\rangle$, the mixed state of every single qubit respectively inputs the detection, and two auxiliary qubits are invariant. When Bob sends m $(m \geqslant 2)$ copies of two-qubit signal, Alice can find Trojan attack with probability $1 - (1/2)^2 = 3/4$ by detecting whether or not two auxiliary qubits flip.

6. Conclusion

In this Letter, we have presented a threshold quantum protocol based on two-qubit operation. The number of qubits of the generated quantum state by the threshold protocol equals to that of the quantum state generated by the original (nonthreshold) protocol. The threshold protocol prevents the legitimate parties from fake signal attack and Trojan horse attack of a dishonest party.

The proposed two-qubit operation based on Grover's algorithm can also be included in QSDC protocols and MQSS protocols. The proposed detection scheme of Trojan horse attack can also be included in the quantum cryptography protocols else.

Acknowledgements

This work is supported by the National Natural Science Foundation of China, Grants No. 60373059; the National Laboratory for Modern Communications Science Foundation of China; the National Research Foundation for the Doctoral Program of Higher Education of China, Grants No. 20040013007; the Major Research plan of the National Natural Science Foundation of China (90604023); and the ISN Open Foundation.

References

[1] A. Yao, in: Proceedings of the 23rd IEEE Symposium on Foundations of Computer Science (FOCS), IEEE, Chicago, 1982, p. 160.
[2] D. Chaum, C. Crepeau, I. Damgard, in: Proceedings of the 20th Annual ACM Symposium on the Theory of Computing (STOC), ACM, New York, 1988, p. 11.

[3] A. Karlsson, M. Koashi, N. Imoto, Phys. Rev. A 59 (1999) 162.
[4] Z.J. Zhang, Y. Li, Z.X. Man, Phys. Rev. A 71 (2005) 044301.
[5] Y. Tokunaga, T. Okamoto, N. Imoto, Phys. Rev. A 71 (2005) 012314.
[6] Q.-Y. Cai, B.-W. Li, Chin. Phys. Lett. 21 (2004) 601.
[7] F.G. Deng, G.L. Long, Phys. Rev. A 69 (2004) 052319.
[8] M. Lucamarini, S. Mancini, Phys. Rev. Lett. 94 (2005) 140501.
[9] F.G. Deng, X.H. Li, H.Y. Zhou, Z.J. Zhang, Phys. Rev. A 72 (2005) 044302.
[10] S.J. Qin, F. Gao, Q.Y. Wen, F.C. Zhu, Phys. Lett. A 357 (2006) 101.
[11] L.K. Grover, Phys. Rev. Lett. 79 (1997) 325.
[12] G.L. Long, Phys. Rev. A 64 (2001) 022307.
[13] L.M.K. Vandersypen, M. Steffen, M.H. Sherwood, C.S. Yannoni, G. Breyta, I.L. Chuang, Appl. Phys. Lett. 76 (2000) 646.
[14] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, Rev. Mod. Phys. 74 (2002) 145.
[15] A. Shamir, Commun. ACM 22 (1979) 612.
[16] P.W. Shor, J. Preskill, Phys. Rev. Lett. 85 (2000) 441.
[17] M.A. Nielsen, I.L. Chuang, Quantum Computation and Quantum Information, Cambridge Univ. Press, Cambridge, 2000, pp. 531–534.