IOP Publishing Physica Scripta

Phys. Scr. 95 (2020) 055106 (8pp) https://doi.org/10.1088/1402-4896/ab73d5

An attempt at universal quantum secure multi-party computation with graph state

Zhao Dou[1], Xiu-Bo Chen[1,2,5], Gang Xu[1,2], Wen Liu[3], Yi-Xian Yang[1,2] and Yu Yang[4]

[1] Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, People's Republic of China
[2] GuiZhou University, State Key Laboratory of Public Big Data, Guizhou, Guiyang 550025, People's Republic of China
[3] School of Computer Science and Cybersecurity, Communication University of China, Beijing 100024, People's Republic of China
[4] School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing 100876, People's Republic of China

E-mail: flyover100@163.com

Received 3 October 2019, revised 19 January 2020
Accepted for publication 5 February 2020
Published 3 March 2020

Abstract
Quantum secure multi-party computation (SMC) is a vital field in quantum cryptography. In this paper, we try to resolve SMC problems universally via graph states. Firstly, three kinds of quantum SMC protocols are investigated, which are quantum private comparison protocol, quantum millionaire protocol and quantum multi-party summation protocol. Secondly, three proposed protocols are reviewed, and then the core of them is summarized. We further find that the computation, deduced as modulo subtraction, can be resolved by using graph state. This implies that our protocols are universal in part and will be widely applicable. Thirdly, analyses show that the proposed protocols are correct and secure. Our research will promote the development of quantum secure multi-party computation.

Keywords: quantum secure multi-party computation, graph state, stabilizer formalism, security, universality

1. Introduction

In secure multi-party computation (SMC), each player has a private input. All the players want to compute and obtain an output cooperatively. SMC is widely used in distributed networks [1–4], such as secret sharing, electronic voting, secure sorting, data mining and so on [5]. Yao [6] firstly investigated the millionaire problem, which is a kind of SMC problems. In this problem, two millionaires want to compare their value of assets without the help of any others.

Quantum cryptography is a vital branch of cryptography. It is a possible approach to achieve the unconditional security of protocols. In 2008, Markham *et al* [7] presented a quantum secret sharing (QSS) protocol via two-dimensional graph state. Then, Keet *et al* [8] designed a QSS protocol with d-dimensional graph state. Graph states are a kind of quantum entangled states which are tractable and widely applied in quantum information processing [7–11].

Quantum private comparison (QPC) protocols are the quantum solutions of the socialist millionaire problem. In 2010, Chen *et al* [12] introduced the semi-honest third party (TP) into QPC protocol, and designed an efficient protocol. Here, semi-honest TP will not be corrupted by any player or adversary, but he may record all the intermediate computations and steal players' inputs from the record [12]. Recently, Liu *et al* [13] researched a QPC protocol via single-photon interference.

Considering millionaire problem, Jia *et al* [14] proposed a quantum millionaire (QM) protocol in 2011. The inputs are coded into phases of d-dimensional entangled states [15]. After that, Lin *et al* [16] also designed a QM protocol based on d-dimensional Bell states.

Another kind of quantum SMC protocol is quantum multi-party summation (QMS) protocol. In 2007, Du *et al* [17] investigated a novel QMS protocol based on non-orthogonal

[5] Author to whom any correspondence should be addressed.

states. Recently, Yang *et al* [18] proposed a QMS protocol, in which the traveling particles are transmitted in a tree-type mode.

In 2017, we proposed the concept of universality in a quantum communication protocol [19]. A feature of universality is that one protocol could be used to resolve another problem with a little modification. Up to now, most researches of different SMC problems are independent. The relationship among these problems and the universality of quantum SMC protocols remain vague. In this paper, we attempt to find a universal solution of SMC problems by employing the graph state and stabilizer formalism. Firstly, we propose a QPC protocol, a QM protocol and a QMS protocol. The procedures of protocols are simple and efficient. Secondly, we summarize these protocols and find that the difference between numbers of performing Pauli operators could also be computed in the same way. If inputs of players are represented by numbers of performing Pauli operators, we are able to obtain the difference between players' inputs. Therefore, if a problem can be deduced as subtraction module *dim*, it can be resolved by our protocol. From this point of view, our proposed protocols are partly universal. Thirdly, analyses indicate that our protocols are correct and secure. Our research will be helpful for the development of quantum SMC protocols.

The structure of this paper is organized as follows. Preliminaries are provided in section 2. Later, our proposed protocols and two examples are introduced in section 3. Then, we analyze the universality, correctness and security of our protocols in section 4. Finally, conclusions are given in section 5.

2. Preliminaries

2.1. Graph states

An undirected graph $G = (V,\ E)$ comprises n vertices. Here, $V = \{v_j\}$ is the set of vertices while $E = \{e_{jk} = (v_j,\ v_k)\}$ is the set of edges. A pure graph state is a state which could be represented by a graph.

A two-dimensional graph state is created from the n-qubit uniform superposition state

$$|+\rangle^{\otimes n} = \frac{1}{2^{n/2}}(|0\rangle + |1\rangle)^{\otimes n}. \tag{1}$$

Then, the two-qubit controlled phase operator $CZ_2|ab\rangle = (-1)^{ab}|ab\rangle$ is performed in the particles whose corresponding vertices on the graph are joined by an edge [7]. The state will be denoted as:

$$|G_2\rangle = \prod_{e\in E}(CZ_2)_e| + \rangle^{\otimes n}. \tag{2}$$

Similarly, in the *dim*-dimensional case, the graph state is created from the n-qudit uniform superposition state [8]

$$|\bar{0}\rangle^{\otimes n} = \frac{1}{dim^{n/2}}(|0\rangle + |1\rangle + \ldots + |dim - 1\rangle)^{\otimes n}. \tag{3}$$

Here, $|\bar{j}\rangle = F_{dim}|j\rangle = \frac{1}{dim^{n/2}}\sum_k \omega^{jk}|k\rangle$, $\omega = e^{2\pi i/dim}$. The two-qudit controlled phase operator is symbolled as $CZ_{dim}|jk\rangle = \omega^{jk}|jk\rangle$. Therefore, a *dim*-dimensional graph state will be denoted as:

$$|G_{dim}\rangle = \prod_{e\in E}(CZ_{dim})_e|\bar{0}\rangle^{\otimes n}. \tag{4}$$

2.2. Stabilizer formalism

The stabilizer formalism is a tool to describe the quantum state. Many states could be graphically described by working with the operators that stabilize them [20].

The two-dimensional graph state could be defined by the stabilizers [7]

$$K_{2,j} = X_{2,j} \otimes_{e_{j,k}\in E} Z_{2,k}. \tag{5}$$

That is to say, $K_{2,j}|G_2\rangle = |G_2\rangle$. Here, $X_2 = |0\rangle\langle 1| + |1\rangle\langle 0|$ and $Z_2 = |0\rangle\langle 0| - |1\rangle\langle 1|$. For the *dim*-dimensional graph state, the stabilizers are [8]

$$K_{dim,j} = X_{dim,j} \otimes_{e_{j,k}\in E} Z_{dim,k}. \tag{6}$$

The state $|G_{dim}\rangle$ is stabilized by the operator $K_{dim,j}$. We also have $K_{dim,j}|G_{dim}\rangle = |G_{dim}\rangle$, $X_{dim} = \sum_l |l + 1\rangle\langle l|$ and $Z_{dim} = \sum_l \omega^l|l\rangle\langle l|$.

3. The proposed quantum multi-party computation protocol

Based on graph state, three quantum SMC protocols are designed. Concretely, a QPC protocol, a QM protocol and a QMS protocol are investigated in subsection 3.1, subsection 3.2 and subsection 3.3, respectively. After that, two examples of our QM protocol and QMS protocols are given in subsection 3.4 and 3.5 successively.

3.1. A new quantum private comparison protocol

A two-particle two-dimensional graph state could be prepared as follows:

$$|\phi_2\rangle = (CZ_2)_{12}|{+}{+}\rangle = \frac{1}{\sqrt{2}}(|0+\rangle + |1-\rangle). \tag{7}$$

It is the eigenstate of

$$K_{2,1} = X_{2,1} \otimes Z_{2,2};\quad K_{2,2} = Z_{2,1} \otimes X_{2,2} \tag{8}$$

with eigenvalues (1, 1).

Suppose that the player Alice and Bob has the secret XC and YC, respectively. Here, XC and YC could be represented by the n-bits string $(xc_{n-1}, xc_{n-2}, \ldots, xc_0)$ and $(yc_{n-1}, yc_{n-2}, \ldots, yc_0)$, severally. Players will determine whether $XC = YC$ or not with the help of semi-honest TP. The procedures of the QPC protocol are given as follows.

[C-1] TP prepares a sequence of $|\phi_2\rangle$. Then, he mixes all the first (second) particles of states $|\phi_2\rangle$ with a sequence of decoy states $\{|0\rangle,\ |1\rangle,\ |+\rangle,\ |-\rangle\}$, and sends the mixed sequence to Alice (Bob).

[C-2] After receiving the particles, players and TP check the eavesdropping. TP tells each player the exact position of each decoy state and the measurement basis in the mixed sequences.

If the decoy state is $|0\rangle$ or $|1\rangle$, players need to measure it in Z_2 basis $\{|0\rangle, |1\rangle\}$. Otherwise, X_2 basis $\{|+\rangle, |-\rangle\}$ will be employed. After that, TP analyzes the error rate of measurement result. If the rate is higher than the preset threshold, players and TP will deduce that eavesdropper has disturbed the transmission of mixed sequences. Players and TP will discard all the sequences and restart the step [C-1]. Otherwise, two players collaborate to verify the authority of state $|\phi_2\rangle$. Concretely, they measure some of states $|\phi_2\rangle$ in their hands with prearranged basis (Z_2 basis or X_2 basis), respectively. After that, they compare the relationship of their $|\phi_2\rangle$ measurement results. If the results of two players are relative, the authority of state is verified. Players will go to the step [C-3]. Otherwise, the carrier $|\phi_2\rangle$ is fake. Players will restart the step [C-1].

[C-3] Alice (Bob) will perform the Pauli operators on her (his) own particles. For Alice, if $xc_i = 0$, she will perform the operator I_2, otherwise the operator X_2. For Bob, if $yc_i = 0$, he will perform the operator I_2, otherwise the operator Z_2.

[C-4] Two players mix particles with new decoy states, send the sequences back, and check the eavesdropping with TP again. Later, TP measures the received particles. The measurement bases are $B_2 = \{(|0+\rangle + |1-\rangle)/\sqrt{2}, (|0-\rangle + |1+\rangle)/\sqrt{2}, (|0+\rangle - |1-\rangle)/\sqrt{2}, (|0-\rangle - |1+\rangle)/\sqrt{2}\}$, which are constructed by $I_2 \otimes H_2$ and Bell bases.

$$\begin{pmatrix} (|0+\rangle + |1-\rangle)/\sqrt{2} \\ (|0-\rangle + |1+\rangle)/\sqrt{2} \\ (|0+\rangle - |1-\rangle)/\sqrt{2} \\ (|0-\rangle - |1+\rangle)/\sqrt{2} \end{pmatrix} = \begin{pmatrix} I_2 \otimes H_2 & & & \\ & I_2 \otimes H_2 & & \\ & & I_2 \otimes H_2 & \\ & & & I_2 \otimes H_2 \end{pmatrix} \times \begin{pmatrix} (|00\rangle + |11\rangle)/\sqrt{2} \\ (|01\rangle + |10\rangle)/\sqrt{2} \\ (|00\rangle - |11\rangle)/\sqrt{2} \\ (|01\rangle - |10\rangle)/\sqrt{2} \end{pmatrix}. \tag{9}$$

Corresponding measurement results are encoded as $c_j = 0, 1, 2$ and 3, respectively.

[C-5] The bits xc_i and yc_i will be equal if $c_j = 0$, and not equal if $c_j = 1$. But if $c_j = 2$ or 3, some unexpected errors have happened. That is to say, secrets XC and YC will be equal if all the $c_j = 0$. They will be not equal if any $c_j = 1$. If any $c_j = 2$ or 3, some errors have happened, players and TP should restart the protocol.

3.2. A novel quantum millionaire protocol

A two-particle $2d$-dimensional graph state could be represented as follows:

$$|\phi_{2d}\rangle = (CZ_{2d})_{12}|\overline{0}\overline{0}\rangle = \frac{1}{\sqrt{2d}}(|0\overline{0}\rangle + |1\overline{1}\rangle + \ldots + |2d-1, \overline{2d-1}\rangle). \tag{10}$$

It is the eigenstate of

$$K_{2d,1} = X_{2d,1} \otimes Z_{2d,2}; \quad K_{2d,2} = Z_{2d,1} \otimes X_{2d,2} \tag{11}$$

with eigenvalues (1, 1).

Next, the proposed QM protocol will be described analogously. We also suppose that two players want to compare XM and YM with the help of semi-honest TP. XM and YM are two n-length sequences $(xm_{n-1}, xm_{n-2}, \ldots, xm_0)$ and $(ym_{n-1}, ym_{n-2}, \ldots, ym_0)$, where $0 \leqslant xm_j, ym_j \leqslant d-1$ for $0 \leqslant j \leqslant n-1$.

[M-1] TP prepares a sequence of $|\phi_{2d}\rangle$ and two sequences of decoy states $\{|0\rangle, |1\rangle, \ldots, |2d-1\rangle, |\overline{0}\rangle, |\overline{1}\rangle, \ldots, |\overline{2d-1}\rangle\}$. Then, he mixes the first (second) particles of all the $|\phi_{2d}\rangle$ with the first (second) decoy states sequence, and send the new sequence to Alice (Bob).

[M-2] After receiving the particles, two players ask TP to publish the position and measurement basis of each decoy state. If the decoy state is one of $|0\rangle, |1\rangle, \ldots, |2d-1\rangle$, the basis is Z_{2d} basis $\{|0\rangle, |1\rangle, \ldots, |2d-1\rangle\}$. Otherwise, the basis is F_{2d} basis $\{|\overline{0}\rangle, |\overline{1}\rangle, \ldots, |\overline{2d-1}\rangle\}$. Then, two players measure all decoy states, and tell results to TP. TP can analyze the error rate of measurements to judge the existence of eavesdropper. If the check is passed, two players will measure some $|\phi_{2d}\rangle$ particles in two sequences to verify whether the states are authentic or not. If the measurement results of two players are not relative, it can indicate that the state $|\phi_{2d}\rangle$ is not real. Players will restart the protocol. Otherwise, they go to the step [M-3].

[M-3] If the states are authentic, Alice (Bob) will perform the operator $X_{2d}^{xm_j}$ ($Z_{2d}^{ym_j}$) on the j-th particle. This means that X_{2d} (Z_{2d}) will be performed xm_j (ym_j) times.

[M-4] Then, two players send the particles with decoy states to TP. After the eavesdropping check, TP measures the state in the bases B_{2d}

$$\begin{aligned} &\{(|0\overline{0}\rangle + |1\overline{1}\rangle + \ldots + |2d-1, \overline{2d-1}\rangle)/\sqrt{2d}, \\ &(|0\overline{1}\rangle + |1\overline{2}\rangle + \ldots + |2d-1, \overline{0}\rangle)/\sqrt{2d}, \ldots, \\ &(|0, \overline{2d-1}\rangle + |1\overline{0}\rangle + \ldots + |2d-1, \overline{2d-2}\rangle)/\sqrt{2d}, \ldots, \\ &(|0\overline{0}\rangle + \omega^{2d-1}|1\overline{1}\rangle + \ldots + \omega^{(2d-1)^2}|2d-1, \overline{2d-1}\rangle)/\sqrt{2d}, \\ &(|0\overline{1}\rangle + \omega^{2d-1}|1\overline{2}\rangle + \ldots + \omega^{(2d-1)^2}|2d-1, \overline{0}\rangle)/\sqrt{2d}, \ldots, \\ &(|0, \overline{2d-1}\rangle + \omega^{2d-1}|1\overline{0}\rangle + \ldots + \omega^{(2d-1)^2}|2d-1, \overline{2d-2}\rangle)/\sqrt{2d}\}. \end{aligned} \tag{12}$$

Likewise, bases B_{2d} could be constructed by $I_{2d} \otimes F_{2d}$ and $2d$-dimensional Bell bases. The measurement results are denoted as $m_j = 0, 1, 2, \ldots, 4d^2 - 1$, respectively.

[M-5] If the result $m_j = 0$, TP will know that $xm_j = ym_j$. If $1 \leqslant m_j \leqslant d-1$, he will obtain that $xm_j < ym_j$. What's more, $xm_j > ym_j$ if $d+1 \leqslant m_j \leqslant 2d-1$. If any other results show up, some errors must have happened. Likewise, TP will further know that $XM = YM$ if all the $m_j = 0$, $XM < YM$ if $1 \leqslant m_{n-1} \leqslant d-1$ or if $1 \leqslant m_k \leqslant d-1$ when all the$m_j = 0 (j > k > 0)$, $XM > YM$ if $d+1 \leqslant m_{n-1} \leqslant 2d-1$ or if $d+1 \leqslant m_k \leqslant 2d-1$ when all the $m_j = 0 (j > k > 0)$.

3.3. A new quantum multi-party summation protocol

In this subsection, we design a quantum multi-party summation protocol based on graph states. The utilized two-particle d-dimensional graph state could be denoted in equation (13).

$$|\phi_d\rangle = (CZ_d)_{12}|\bar{0}\bar{0}\rangle = \frac{1}{\sqrt{d}}(|0\bar{0}\rangle + |1\bar{1}\rangle + \ldots + |d-1, \overline{d-1}\rangle). \quad (13)$$

Similarly, the state is the eigenstate of

$$K_{d,1} = X_{d,1} \otimes Z_{d,2}; \quad K_{d,2} = Z_{d,1} \otimes X_{d,2} \quad (14)$$

with eigenvalues (1, 1).

In this protocol, there are n players P_j $(1 \leqslant j \leqslant n)$ who want to compute the summation of their private inputs x_j $(1 \leqslant j \leqslant n)$. The steps are given below.

[S-1] Suppose that player P_1 prepares some states $|\phi_d\rangle$. Then he mixes the second particle of each state with some decoy states $\{|0\rangle, |1\rangle, \ldots, |d-1\rangle, |\bar{0}\rangle, |\bar{1}\rangle, \ldots, |\overline{d-1}\rangle\}$, and sends the mixed sequence to P_2.

[S-2] When P_2 receives the particle, P_2 and P_1 check the eavesdropping. P_1 publishes positions and measurement bases of decoy states, so P_2 can measure these states by using correct bases. To be specific, if the decoy state is one of $|0\rangle, |1\rangle, \ldots, |d-1\rangle$, the basis is Z_d basis $\{|0\rangle, |1\rangle, \ldots, |d-1\rangle\}$. Otherwise, the basis is F_d basis $\{|\bar{0}\rangle, |\bar{1}\rangle, \ldots, |\overline{d-1}\rangle\}$. Then, P_1 analyzes the error rate of decoy state measurements. If the rate is unexpectedly high, the transmission of mixed sequence is disturbed by eavesdropper. Players will restart the protocol. Otherwise, P_2 and P_1 further analyze whether the states $|\phi_d\rangle$ are real or not. Concretely, P_2 asks P_1 to measure the first particles of some $|\phi_d\rangle$ with specified bases (Z_d basis or F_d basis). After that, P_2 measures the second particles of the same states with the same bases, and analyzes the error rate. If the rate is acceptable, players go to the next step. Otherwise, the state $|\phi_d\rangle$ is fake, they restart the protocol.

[S-3] If the state is real, P_2 will choose a random number r_2 $(0 \leqslant r_2 \leqslant d-1)$, and perform the operator $Z_d^{r_2}$ (i.e., perform Z_d for r_2 times) on the entire remaining particles. Later, P_2 will send all the particles to P_3.

[S-4] When P_j $(3 \leqslant j \leqslant n)$ obtains the particles, P_j and P_{j-1} will check the eavesdropping as P_2 and P_1. Subsequently, P_j and P_1 analyzes the authenticity of the states $|\phi_d\rangle$ as P_2 and P_1. If the state is real, P_j will select a random number r_j $(0 \leqslant r_j \leqslant d-1)$, and perform $Z_d^{r_j}$ on the remaining particles. Then, he will send all particles with decoy states to P_{j+1}.

[S-5] Afterwards, P_n sends the remaining particles with decoy states to P_1. They also check the eavesdropping at first. After that, P_1 measures the state in the bases B_d.

$$\begin{aligned}
&\{(|0\bar{0}\rangle + |1\bar{1}\rangle + \ldots + |d-1, \overline{d-1}\rangle)/\sqrt{d},\\
&(|0\bar{1}\rangle + |1\bar{2}\rangle + \ldots + |d-1, \bar{0}\rangle)/\sqrt{d}, \ldots,\\
&(|0, \overline{d-1}\rangle + |1\bar{0}\rangle + \ldots + |d-1, \overline{d-2}\rangle)/\sqrt{d}, \ldots,\\
&(|0\bar{0}\rangle + \omega^{d-1}|1\bar{1}\rangle + \ldots + \omega^{(d-1)^2}|d-1, \overline{d-1}\rangle)/\sqrt{d},\\
&(|0\bar{1}\rangle + \omega^{d-1}|1\bar{2}\rangle + \ldots + \omega^{(d-1)^2}|d-1, \bar{0}\rangle)/\sqrt{d}, \ldots,\\
&(|0, \overline{d-1}\rangle + \omega^{d-1}|1\bar{0}\rangle + \ldots + \omega^{(d-1)^2}|d-1, \overline{d-2}\rangle)/\sqrt{d}\}.
\end{aligned} \quad (15)$$

Bases B_d could be constructed by $I_d \otimes F_d$ and d-dimensional Bell bases. Subsequently, P_1 marks the results as $s = 0, 1, \ldots, d^2 - 1$, severally.

[S-6] If the result holds $0 \leqslant s \leqslant d-1$, P_1 will ask everyone else P_j $(2 \leqslant j \leqslant n)$ to publish the result $x_j - r_j$. Then, he computes $[\sum_j (x_j - r_j) + s + x_1] \bmod d$ and publishes it. Otherwise, the result satisfies $d \leqslant s \leqslant d^2 - 1$. It means that some errors have happened. All the players will restart the protocol soon.

3.4. An example of proposed quantum millionaire protocol

In this subsection, our QM protocol will be illustrated by narrating the case d=3. A two-particle six-dimensional graph state could be represented as follows:

$$|\phi_6\rangle = (CZ_6)_{12}|\bar{0}\bar{0}\rangle = \frac{1}{\sqrt{6}}(|0\bar{0}\rangle + |1\bar{1}\rangle + \ldots + |5\bar{5}\rangle). \quad (16)$$

It is the eigenstate of

$$K_{6,1} = X_{6,1} \otimes Z_{6,2}; \quad K_{6,2} = Z_{6,1} \otimes X_{6,2} \quad (17)$$

with eigenvalues (1, 1).

XM and YM are two n-length sequences, $(xm_{n-1}, xm_{n-2}, \ldots, xm_0)$ and $(ym_{n-1}, ym_{n-2}, \ldots, ym_0)$, where $0 \leqslant xm_j, ym_j \leqslant 2$ for $0 \leqslant j \leqslant n-1$. Brief steps of protocol are described below.

[M-1] TP prepares a sequence of $|\phi_6\rangle$, and send the first (second) particles of all the $|\phi_6\rangle$ with decoy states to Alice (Bob).

[M-2] After receiving the particles, two players and TP check the existence of eavesdropper. If the transmission is secure, two players will verify whether the states $|\phi_6\rangle$ are authentic or not.

[M-3] If the states are authentic, Alice (Bob) will perform the operator $X_6^{xm_j}$ $(Z_6^{ym_j})$ on the j-th particle. This means that $X_6 = \sum_{l=0}^{5}|l+1\rangle\langle l|$ $(Z_6 = \sum_{l=0}^{5}\omega^l|l\rangle\langle l|)$ will be performed xm_j (ym_j) times.

[M-4] Then, two players send these particles to TP. After the eavesdropping check, TP measures the state in the bases B_6

$$\begin{aligned}
&\{(|0\bar{0}\rangle + |1\bar{1}\rangle + \ldots + |5\bar{5}\rangle)/\sqrt{6},\\
&(|0\bar{1}\rangle + |1\bar{2}\rangle + \ldots + |5\bar{0}\rangle)/\sqrt{6}, \ldots,\\
&(|0\bar{5}\rangle + |1\bar{0}\rangle + \ldots + |5\bar{4}\rangle)/\sqrt{6}, \ldots,\\
&(|0\bar{0}\rangle + \omega^5|1\bar{1}\rangle + \ldots + \omega^{25}|5\bar{5}\rangle)/\sqrt{6},\\
&(|0\bar{1}\rangle + \omega^5|1\bar{2}\rangle + \ldots + \omega^{25}|5\bar{0}\rangle)/\sqrt{6}, \ldots,\\
&(|0\bar{5}\rangle + \omega^5|1\bar{0}\rangle + \ldots + \omega^{25}|5\bar{4}\rangle)/\sqrt{6}\}.
\end{aligned} \quad (18)$$

Likewise, bases B_6 could be constructed by $I_6 \otimes F_6$ and six-dimensional Bell bases. The measurement results are denoted as $m_j = 0, 1, 2, \ldots, 35$, respectively.

[M-5] If the result $m_j = 0$, TP will know that $xm_j = ym_j$. If $1 \leqslant m_j \leqslant 2$, he will obtain that $xm_j < ym_j$. And, $xm_j > ym_j$ if $4 \leqslant m_j \leqslant 5$. If any other results show up, some errors must have happened. Likewise, TP will further know that $XM = YM$ if all the $m_j = 0$, $XM < YM$ if $1 \leqslant m_{n-1} \leqslant 2$ or if $1 \leqslant m_k \leqslant 2$ when all the $m_j = 0 (j > k > 0)$, $XM > YM$ if $4 \leqslant m_{n-1} \leqslant 5$ or if $4 \leqslant m_k \leqslant 5$ when all the $m_j = 0 (j > k > 0)$.

3.5. An example of proposed quantum multi-party summation protocol

In this subsection, our QMS protocol will be illustrated by narrating the case $d = 3$. The utilized two-particle three-dimensional graph state could be denoted in equation (19).

$$|\phi_3\rangle = (CZ_3)_{12}|\bar{0}\bar{0}\rangle = \frac{1}{\sqrt{3}}(|0\bar{0}\rangle + |1\bar{1}\rangle + |2\bar{2}\rangle). \quad (19)$$

Similarly, the state is the eigenstate of

$$K_{3,1} = X_{3,1} \otimes Z_{3,2}; \quad K_{3,2} = Z_{3,1} \otimes X_{3,2} \quad (20)$$

with eigenvalues (1, 1).

Brief steps of our protocol are given below.

[S-1] Suppose that player P_1 prepares some states $|\phi_3\rangle$ and sends the second particle of each state with decoy states to P_2.

[S-2] When P_2 receives the particle, P_2 and P_1 check the eavesdropping. Afterwards, they analyze whether the states $|\phi_3\rangle$ are real or not.

[S-3] If the state is real, P_2 will choose a random number r_2 $(0 \leqslant r_2 \leqslant 2)$, and perform the operator $Z_3^{r_2}$ (i.e., perform $Z_3 = \sum_{l=0}^{2} \omega^l |l\rangle\langle l|$ for r_2 times) on the entire remaining particles. Later, P_2 will send all the particles to P_3.

[S-4] When P_j $(3 \leqslant j \leqslant n)$ obtains the particles, P_j and P_{j-1} will check the security of transmission. Subsequently, P_j and P_1 analyzes the authenticity of the states $|\phi_3\rangle$. If the state is real, P_j will select a random number r_j $(0 \leqslant r_j \leqslant 2)$, and perform $Z_3^{r_j}$ on the remaining particles. Then, he will send all the particles to P_{j+1}.

[S-5] Afterwards, P_n sends the particle to P_1. They also check the eavesdropping at first. After that, P_1 measures the state in the bases B_3.

$$\begin{aligned}
&\{(|0\bar{0}\rangle + |1\bar{1}\rangle + |2\bar{2}\rangle)/\sqrt{3},\\
&(|0\bar{1}\rangle + |1\bar{2}\rangle + |2\bar{0}\rangle)/\sqrt{3},\\
&(|0\bar{2}\rangle + |1\bar{0}\rangle + |2\bar{1}\rangle)/\sqrt{3}, \ \ldots,\\
&(|0\bar{0}\rangle + \omega^2|1\bar{1}\rangle + \omega^4|2\bar{2}\rangle)/\sqrt{3},\\
&(|0\bar{1}\rangle + \omega^2|1\bar{2}\rangle + \omega^4|2\bar{0}\rangle)/\sqrt{3},\\
&(|0\bar{2}\rangle + \omega^2|1\bar{0}\rangle + \omega^4|2\bar{1}\rangle)/\sqrt{3}\}. \quad (21)
\end{aligned}$$

Bases B_3 could be constructed by $I_3 \otimes F_3$ and three-dimensional Bell bases. Subsequently, P_1 marks the results as $s = 0, \ 1, \ldots, 8$, severally.

[S-6] If the result holds $0 \leqslant s \leqslant 2$, P_1 will ask everyone else P_j $(2 \leqslant j \leqslant n)$ to publish the result $x_j - r_j$. Then, he computes $[\sum_j (x_j - r_j) + s + x_1] \bmod 3$ and publishes it. Otherwise, the result satisfies $3 \leqslant s \leqslant 8$. It means that some errors have happened. All the players will restart the protocol soon.

4. Analyses

Mathematics provides many tools [21, 22] to research practical problems. In this section, we analyze the core of our proposed protocols, and then discuss the universality of our protocols at first. After that, the correctness and security about the protocols are given one by one.

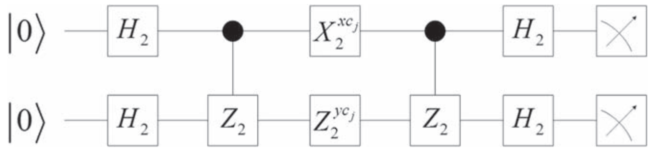

Figure 1. Circuit simulation of the proposed QPC protocol.

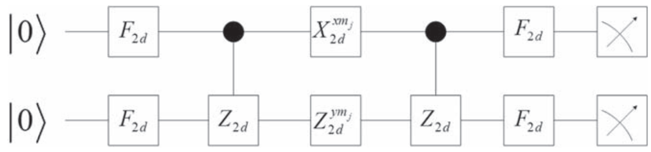

Figure 2. Circuit simulation of the proposed QM protocol.

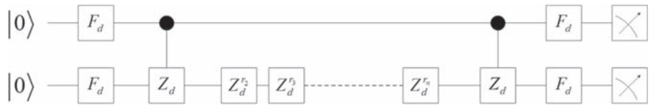

Figure 3. Circuit simulation of the proposed QMS protocol.

Table 1. Four quantum SMC protocols and their coefficients.

The protocol	DIMENSION	The computation
QPC	$dim = 2$	$(y - x) \bmod 2$
QM	$dim = 2d$	$(y - x) \bmod 2d$
QMS	$dim = d$	$(\sum y) \bmod d$, $x = 0$
QAR	$dim = d$	$(\sum y) \bmod d$, $x = 0$

4.1. The universality of our quantum multi-party computation protocol with graph state

In section 3, we proposed three protocols to resolve the QPC, QM and QMS problems, severally. Here, circuit simulations of them are illustrated by the figures 1–3.

From these figures, we can find that procedures of these protocols are similar. Then, a question comes naturally: is there any other problem could also be resolved by using graph state and stabilizer formalism? In this subsection, we will discuss this.

For a set of two-particle *dim*-dimensional orthogonal graph states $|\varphi^{(0)}\rangle$, $|\varphi^{(1)}\rangle$, … and $|\varphi^{(dim-1)}\rangle$, each of these states is the eigenstate of the operator $X_{dim} \otimes Z_{dim}$. In other words, $X_{dim} \otimes Z_{dim}|\varphi^{(j)}\rangle = |\varphi^{(j)}\rangle$. We know that $X_{dim}^{dim} = Z_{dim}^{dim} = I$, and can further deduce that

$$X_{dim}^{x} \otimes Z_{dim}^{y}|\varphi^{(0)}\rangle = X_{dim}^{0} \otimes Z_{dim}^{y-x}|\varphi^{(0)}\rangle = |\varphi^{(y-x)}\rangle. \quad (22)$$

From equation (22), we know that players can obtain the value of $(y - x) \bmod dim$ naturally by measuring the final state. Therefore, the graph state and stabilizer can be utilized to resolve any computation problem which can be reduced as the equation $(y - x) \bmod dim$. Our proposed QPC, QM, QMS protocols are three examples. Besides, the quantum anonymous ranking (QAR) [23, 24] is another one.

In table 1, we list dimensions of graph states and the computation that needs to be performed for these four protocols. These problems can all be resolved by using

Table 2. Values of coefficients in our QPC protocol.

xc_j	yc_j	Operator	Final state	c_j
0	0	$I_2 \otimes I_2$	$\|\phi_2\rangle$	0
0	1	$I_2 \otimes Z_2$	$\|\phi_2\rangle'$	1
1	0	$X_2 \otimes I_2$	$\|\phi_2\rangle'$	1
1	1	$X_2 \otimes Z_2$	$\|\phi_2\rangle$	0

graph state and stabilizer formalism. Procedures of these protocols are much the same. In other words, our protocols are partly universal [19].

4.2. Correctness

4.2.1. Correctness of quantum private comparison protocol. In our QPC protocol, only stabilizer $K_{2,1}$ is utilized. All the possible operators that players perform are: $I_2 \otimes I_2$, $I_2 \otimes Z_2$, $X_2 \otimes I_2$ and $X_2 \otimes Z_2$. Values of xc_j and yc_j, operators, final states, and encoding results c_j are listed in table 2.

Here, $|\phi_2\rangle' = (|0-\rangle + |1+\rangle)/\sqrt{2}$. From this table, the equation $c_j = (yc_j - xc_j) \bmod 2$ could be verified. TP can obtain that whether $xc_j = yc_j$ or not. He could further know that whether $XC = YC$ or not. That is the correctness of this QPC protocol.

4.2.2. Correctness of quantum millionaire protocol. Just like the proposed QPC protocol, correctness of our QM protocol could also be shown in the table 3.

Here, it is obvious that

$$\begin{aligned} |\phi_{2d}\rangle' &= X_{2d}^{xm_j} \otimes Z_{2d}^{ym_j} |\phi_{2d}\rangle \\ &= (|xm_j, \overline{ym_j}\rangle + |xm_j + 1, \overline{ym_j + 1}\rangle + \ldots \\ &\quad + |xm_j - 1, \overline{ym_j - 1}\rangle)/\sqrt{2d} \\ &= (|0, \overline{ym_j - xm_j}\rangle + |1, \overline{ym_j - xm_j + 1}\rangle + \ldots \\ &\quad + |2d - 1, \overline{ym_j - xm_j - 1}\rangle)/\sqrt{2d}. \end{aligned} \tag{23}$$

Then, $m_j = (ym_j - xm_j) \bmod 2d$ could be obtained. Since $0 \leqslant xm_j,\ ym_j \leqslant d - 1$, we will know that $m_j = 0$ if $xm_j = ym_j$, $1 < m_j < d - 1$ if $xm_j < ym_j$, and $d + 1 < m_j < 2d - 1$ if $xm_j > ym_j$. That is the correctness of this QM protocol.

4.2.3. Correctness of quantum multi-party summation protocol. In the QMS protocol, each player P_j ($2 \leqslant j \leqslant n$) performs the operator $X_d^{r_j}$ on the second particle. The final state will be

$$\begin{aligned} I \otimes Z_d^{r_n} \ldots Z_d^{r_2} |\phi_d\rangle &= \frac{1}{\sqrt{d}} (|0, \overline{r_2 + \ldots + r_n}\rangle \\ &+ |1, \overline{r_2 + \ldots + r_n + 1}\rangle + \ldots + |d - 1, \overline{r_2 + \ldots + r_n - 1}\rangle). \end{aligned} \tag{24}$$

Then, we can calculate that the result $s = (r_2 + \ldots + r_n) \bmod d$. Furthermore, the summation of all the players' inputs can be obtained by following equation.

$$\begin{aligned} &\left[\sum\nolimits_j (x_j - r_j) + s + x_1\right] \bmod d \\ &= (x_2 - r_2 + \ldots + x_n - r_n + r_2 + \ldots + r_n + x_1) \bmod d \\ &= (x_1 + x_2 + \ldots + x_n) \bmod d. \end{aligned} \tag{25}$$

That is the correctness of this QMS protocol.

4.3. Security

In this subsection, we analyze two kinds of outside attacks and three kinds of inside attacks for our protocols minutely.

4.3.1. Outside attacks. There are two types of general outside attacks. The first one contains the faked states attack, the time-shift attack, the detector blinding attack and the Trojan horse attacks [25–32]. For the faked states attack and the time-shift attack, an extra detector could be utilized to monitor the time when the state arrives at the sides of receiver Alice/ Bob/ TP/ player P_j [25, 26]. As far as the detector blinding attack, light intensity monitor will play a vital role [27]. Trojan horse attacks, such as the invisible photons eavesdropping (IPE) Trojan horse attack and the delay-photon Trojan horse attack could be resisted by using multi-photon detection [30].

The second type of attacks includes the intercept-resend attack, measurement-resend attack, entanglement-measure attack and correlation-elicitation attack [33]. Decoy state is an effective tool to resist these attacks. Since eavesdropper doesn't know the position of each decoy state, he cannot distinguish the carrier states and decoy states. His eavesdropping (the second kind of outside attacks) will disturb decoy states. In this situation, the second kind of outside attacks will be detected in the step [C-2]/ [M-2]/ [S-2]. The idea of this tool is learned from the famous BB84 protocol [34] which is already proved to be unconditionally secure [35].

Take our QPC protocol as an example. Utilized decoy states are $\{|0\rangle,\ |1\rangle,\ |+\rangle,\ |-\rangle\}$. Here, $\langle 0|+\rangle = \langle 0|-\rangle = \langle 1|+\rangle = \langle 1|-\rangle = 1/\sqrt{2}$. Some of these states are not orthogonal. What's more, eavesdropper doesn't know the position and the measurement basis of each decoy state. Therefore, he cannot perform eavesdropping without disturb any decoy state. With the help of the decoy states and security check in step [C-2], the proposed protocols are also immune to these attacks. Attacks will be detected by legal participants with a non-zero probability [36]. Similarly, these attacks are invalid for our QM and QMS protocol.

In summary, our protocols are immune to outside attacks.

4.3.2. Inside attacks. Here, we analyze the inside attacks, which contains the single player attack, collusion attack of some players and the attack of TP/P_1. Since there only exist two players in QPC protocol and QM protocol, collusion attack is only involved in QMS protocol.

(1) Single player attack

As a player, Alice/ Bob/ P_j ($2 \leqslant j \leqslant n$) may want to steal the private information of Bob/ Alice/ P_k

Table 3. Values of coefficients in our QM protocol.

xm_j	ym_j	Operator	Final state	m_j
$0 \leqslant xm_j < ym_j \leqslant d-1$		$X_{2d}^{xm_j} \otimes Z_{2d}^{ym_j}$	$\|\phi_{2d}\rangle'$	$1 \leqslant m_j \leqslant d-1$
$0 \leqslant xm_j = ym_j \leqslant d-1$		$X_{2d}^{xm_j} \otimes Z_{2d}^{ym_j}$	$\|\phi_{2d}\rangle$	$m_j = 0$
$0 \leqslant ym_j < xm_j \leqslant d-1$		$X_{2d}^{xm_j} \otimes Z_{2d}^{ym_j}$	$\|\phi_{2d}\rangle'$	$d+1 \leqslant m_j \leqslant 2d-1$

$(2 \leqslant k \leqslant n,\ \ k \neq j)$. The most common way to deduce the information is the reduced density matrix. Here, we suppose the whole system is the state $|\varphi^{(s)}\rangle\langle\varphi^{(s)}|$, and the reduced matrix of Alice's /Bob's /P_j's particle is $\rho_1/\ \rho_2/\ \rho_2$.

$$\begin{aligned}\rho_1 &= tr_2|\varphi^{(s)}\rangle\langle\varphi^{(s)}| \\ &= \frac{1}{dim}tr_2[(|0,\bar{s}\rangle + |1,\overline{s+1}\rangle + ... + |dim-1,\overline{s-1}\rangle) \\ &\otimes(\langle 0,\bar{s}| + \langle 1,\overline{s+1}| + ... + \langle dim-1,\overline{s-1}|)] \\ &= \frac{1}{dim}(|0\rangle\langle 0|\langle\bar{s}|\bar{s}\rangle + |1\rangle\langle 1|\langle\overline{s+1}|\overline{s+1}\rangle + ... \\ &+ |dim-1\rangle\langle dim-1|\langle\overline{s-1}|\overline{s-1}\rangle) \\ &= \frac{1}{dim}(|0\rangle\langle 0| + |1\rangle\langle 1| + ... + |dim-1\rangle\langle dim-1|) \\ &= I_{dim}/dim.\end{aligned} \tag{26}$$

Similarly, we also can obtain that

$$\rho_2 = tr_1|\varphi^{(s)}\rangle\langle\varphi^{(s)}| = I_{dim}/dim. \tag{27}$$

Since $\rho_1 = \rho_2 = I_{dim}/dim$, the value of s will not be revealed to any player. No player has access to any other player's information. Hence, the reduced density matrix is useless for vicious players.

(2) Collusion attack

In our proposed QMS protocol, there are n players who participate the computation. Therefore, some players may cooperate to steal the information of the others.

One of the most possible collusion attacks is that players P_{j-1} and P_{j+1} $(3 \leqslant j \leqslant n-1)$ try to cooperate to obtain P_j's input x_j. To be specific, P_{j-1} sends some fake particles to P_j. If P_j performs some operators on these fake particles and sends them to P_{j+1}, his private information will be stolen by P_{j+1}. Fortunately, this attack can also be resisted since P_j checks the security of transmission and the authenticity of state $|\phi_d\rangle$ with P_1 in step [S-2]. If P_{j-1} sends a fake particle to P_j, this eavesdropping will be detected. As a result, players P_{j-1} and P_{j+1} cannot collude to obtain any extra information.

Another similar attack is that players P_2 and P_n cooperate to steal private information. Steps of this attack are briefly introduced here. Firstly, when P_2 obtains authentic particles from P_1, he tries to prepare some fake particles and sends them to P_3. Secondly, players transmit fake particles as real ones. Thirdly, when P_n receives these particles, he may compute $x_3 + x_4 + ... + x_{n-1}$. Finally, P_2 and P_n could deduce x_1 after they know the summation of all the inputs. Luckily, this attack are also invalid since P_j $(3 \leqslant j \leqslant n-1)$ can check the security of transmission and the authenticity of state $|\phi_d\rangle$ with P_1.

(3) TP's and P_1's attack

On one hand, in our QPC and QM protocols, TP is supposed to be semi-honest. That is to say, he may analyze the intermediate results to steal the private inputs of players. However, he cannot disturb the execution of protocol. The only messages he can obtain are measurement results of the final state. As we all know, he cannot know anything about players' inputs from the measurement results. Besides that, preparing fake states will also be found in steps [C-2] and [M-2]. In other words, TP's attacks are invalid in our QPC and QM protocols.

On the other hand, in our QMS protocol, P_1 is a player which also has the responsibility as the semi-honest TP. Firstly, intermediate results are not helpful for him to obtain the private input of any other player. Secondly, if he wants to prepare some fake states, this attack will be found out by performing check in step [S-2]. In other words, P_1's attacks are also fruitless in our QMS protocol.

In short, inside attacks are ineffective for our protocols.

5. Conclusion

In this paper, quantum SMC protocols were investigated by using graph state from the perspective of universality. A QPC protocol, a QM protocol and a QMS protocol were designed, respectively. On this basis, we discussed the core of these protocols, and found that modulo subtraction can be calculated certainly by using graph state. If a SMC problem could be deduced as modulo subtraction, it will also be resolved. Our protocols are partly universal. Moreover, the correctness and security of our protocols were ensured. Our research is valuable for the development of quantum SMC protocols.

Acknowledgments

This work is supported by the National Key R&D Program of China (2017YFB0802703), NSFC (Grant Nos. 61671087, 61272514, 61170272, 61003287, U1836205), the Fok Ying

Tong Education Foundation (Grant No. 131067), the Major Scientific and Technological Special Project of Guizhou Province (Grant No. 20183001), the Foundation of Guizhou Provincial Key Laboratory of Public Big Data (Grant No. 2018BDKFJJ016), the Foundation of State Key Laboratory of Public Big Data (Grant No. 2018BDKFJJ018) and sponsored by CCF-Tencent Open Fund WeBank Special Funding (CCF-WebankRAGR20180104).

ORCID iDs

Zhao Dou https://orcid.org/0000-0002-2995-7186

References

[1] Guo R, Zhang Z, Liu X and Lin C 2017 Existence, uniqueness, and exponential stability analysis for complex-valued memristor-based BAM neural networks with time delays *Appl. Math. Comput.* **311** 100–17

[2] Pang Z H, Liu G P, Zhou D and Sun D 2017 Data-based predictive control for networked nonlinear systems with packet dropout and measurement noise *J. Syst. Sci. Complex* **30** 1072–83

[3] Li L, Wang Z, Li Y, Shen H and Lu J 2018 Hopf bifurcation analysis of a complex-valued neural network model with discrete and distributed delays *Appl. Math. Comput.* **330** 152–69

[4] Li Y, Zhang W and Liu X 2013 Stability of nonlinear stochastic discrete-time systems *J. Appl. Math.* **2013** 356746

[5] Shi R H, Mu Y, Zhong H, Cui J and Zhang S 2016 Secure multiparty quantum computation for summation and multiplication *Sci. Rep-UK* **6** 19655

[6] Yao A C 1982 Protocols for secure computations SFCS'08 *23rd Annual Symposium on Foundations of Computer Science* 160–4

[7] Markham D and Sanders B C 2008 Graph states for quantum secret sharing *Phys. Rev. A* **78** 042309

[8] Keet A, Fortescue B, Markham D and Sanders B C 2010 Quantum secret sharing with qudit graph states *Phys. Rev. A* **82** 062315

[9] Schlingemann D and Werner R F 2001 Quantum error-correcting codes associated with graphs *Phys. Rev. A* **65** 012308

[10] Benjamin S C, Browne D E, Fitzsimons J and Morton J J 2006 Brokered graph-state quantum computation *New J. Phys.* **8** 141

[11] Markham D and Krause A 2020 A simple protocol for certifying graph states and applications in quantum networks *Cryptography* **4** 3

[12] Chen X B, Xu G, Niu X X, Wen Q Y and Yang Y X 2010 An efficient protocol for the private comparison of equal information based on the triplet entangled state and single-particle measurement *Opt. Commun.* **283** 1561–5

[13] Liu B, Xiao D, Huang W, Jia H Y and Song T T 2017 Quantum private comparison employing single-photon interference *Quantum Inf. Process.* **16** 180

[14] Jia H Y, Wen Q Y, Song T T and Gao F 2011 Quantum protocol for millionaire problem *Opt. Commun.* **284** 545–9

[15] Cozzolino D, Da Lio B, Bacco D and Oxenløwe L K 2019 High-dimensional quantum communication: benefits, progress, and future challenges *Advanced Quantum Technologies.* **2** 1900038

[16] Lin S, Sun Y, Liu X F and Yao Z Q 2013 Quantum private comparison protocol with d-dimensional Bell states *Quantum Inf. Process.* **12** 559–68

[17] Du J Z, Chen X B, Wen Q Y and Zhu F C 2007 Secure multiparty quantum summation *Acta. Phys. Sin-Ch. Ed.* **56** 6214–9

[18] Yang H Y and Ye T Y 2018 Secure multi-party quantum summation based on quantum Fourier transform *Quantum Inf. Process.* **17** 129

[19] Chen X B, Dou Z, Xu G, He X Y and Yang Y X 2017 A kind of universal quantum secret sharing protocol *Sci. Rep-UK* **7** 39845

[20] Nielsen M A and Chuang I 2015 *Quantum Computation and Quantum Information* 70 (Cambridge: Cambridge University Press) pp 558 10th Anniversary ed

[21] Dong H, Zhang Y, Zhang Y and Yin B 2014 Generalized bilinear differential operators, binary bell polynomials, and exact periodic wave solution of boiti-leon-manna-pempinelli equation *Abstr. Appl. Anal.* **2014** 738609

[22] Jiang T, Jiang Z and Lin S 2014 An algebraic method for quaternion and complex least squares coneigen-problem in quantum mechanics *Appl. Math. Comput.* **249** 222–8

[23] Huang W, Wen Q Y, Liu B, Su Q, Qin S J and Gao F 2014 Quantum anonymous ranking *Phys. Rev.* A **89** 032325

[24] Lin S, Guo G D, Huang F and Liu X F 2016 Quantum anonymous ranking based on the Chinese remainder theorem *Phys. Rev.* A **93** 012318

[25] Makarov V, Anisimov A and Skaar J 2006 Effects of detector efficiency mismatch on security of quantum cryptosystems *Phys. Rev.* A **74** 022313

[26] Jain N, Stiller B, Khan I, Elser D, Marquardt C and Leuchs G 2016 Attacks on practical quantum key distribution systems (and how to prevent them) *Contemp. Phys.* **57** 366–87

[27] Qi B, Fung C H F, Lo H K and Ma X 2007 Time-shift attack in practical quantum cryptosystems *Quantum Inf. Comput.* **7** 73–82 arXiv:quant-ph/0512080

[28] Liu W, Wang Y B and Jiang Z T 2011 An efficient protocol for the quantum private comparison of equality with W state *Opt. Commun.* **284** 3160–3

[29] Liu B, Gao F, Jia H Y, Huang W, Zhang W W and Wen Q Y 2013 Efficient quantum private comparison employing single photons and collective detection *Quantum Inf. Process.* **12** 887–97

[30] Li Y B, Qin S J, Yuan Z, Huang W and Sun Y 2013 Quantum private comparison against decoherence noise *Quantum Inf. Process.* **12** 2191–205

[31] Zhang W W and Zhang K J 2013 Cryptanalysis and improvement of the quantum private comparison protocol with semi-honest third party *Quantum Inf. Process.* **12** 1981–90

[32] Chen X B, Su Y, Niu X X and Yang Y X 2014 Efficient and feasible quantum private comparison of equality against the collective amplitude damping noise *Quantum Inf. Process.* **13** 101–12

[33] Xu G, Chen X B, Dou Z, Yang Y X and Li Z 2015 A novel protocol for multiparty quantum key management *Quantum Inf. Process.* **14** 2959–80

[34] Bennett C and Brassard G 1984 Quantum cryptography: public key distribution and coin tossing *Conf. on Computers, Systems and Signal Processing* (https://doi.org/10.1016/j.tcs.2014.05.025)

[35] Lo H K and Chau H F 1999 Unconditional security of quantum key distribution over arbitrarily long distances *Science* **283** 2050–6

[36] Shor P W and Preskill J 2000 Simple proof of security of the BB84 quantum key distribution protocol *Phys. Rev. Lett.* **85** 441