Quantum Information Processing (2020) 19:293
https://doi.org/10.1007/s11128-020-02788-1

Quantum multiparty cryptosystems based on a homomorphic random basis encryption

Changbin Lu[1] · Fuyou Miao[1] · Junpeng Hou[2] · Zhaofeng Su[1] · Yan Xiong[1]

Received: 13 April 2020 / Accepted: 27 July 2020 / Published online: 24 August 2020

Abstract

Quantum information processing protocols have great advantages over their classical counterparts, especially on cryptography. Homomorphic encryption (HE) schemes enable processing encrypted data without decrypting them. In this paper, we study a quantum version of the HE scheme (iacr-ePrint/2019/1023) and improve it with flexible parties. Furthermore, we propose a threshold quantum secret scheme since multiparty cryptosystem is more practical due to its flexibility. These two schemes only require sequential decryption of quantum states. As a result, both schemes are information theoretically secure, perfectly correct and support homomorphism in a fully compact and non-interactive way. Finally, they are tested and verified on the IBM Q Experience platform.

Keywords Quantum cryptography · Homomorphic encryption · Multiparty cryptograph · Quantum secret sharing

✉ Fuyou Miao
mfy@ustc.edu.cn

Changbin Lu
lcb@mail.ustc.edu.cn

Junpeng Hou
Junpeng.Hou@utdallas.edu

Zhaofeng Su
zfsu@ustc.edu.cn

Yan Xiong
yxiong@ustc.edu.cn

[1] School of Computer Science and Technology, University of Science and Technology of China, Hefei, China

[2] Department of Physics, The University of Texas at Dallas, Richardson, 75080-3021 TX, USA

1 Introduction

It is well known that a fully quantum theory of information and information processing offers, among other benefits, a brand of cryptography with security based on fundamental physics, and a reasonable hope of implementing quantum computers that could speed up the solution of certain mathematical problems [1]. These benefits come from distinctive quantum properties such as superposition, entanglement, and nonlocality [2,3] which do not exist in classical mechanics. In the last four decades, many important quantum information processing protocols have been proposed, including quantum key distribution (QKD) [4], quantum teleportation [5], quantum factoring algorithm [6] and Grover search algorithm [7].

Quantum cryptography is one of the most successful applications in quantum information processing since physical laws ensure its inherent security. Contrarily, classical cryptography usually relies on the assumptions of computational complexity. The first quantum cryptosystem is quantum key distribution which is used to generate random secret keys that are only shared by two parties [4]. Later, quantum cryptography has been extensively studied and many protocols are proposed [8–15].

The homomorphic encryption (HE) scheme enables processing of encrypted data without decrypting them in advance. This useful feature was known for over 30 years. In 2009, Craig Gentry [16] introduced the first plausible and achievable fully homomorphic encryption (FHE) scheme , which supports processing of any function over the encrypted data (see the surveys [17,18]). But the scheme can only achieve computational security. It is natural to ask whether the physical principle of quantum mechanics can be applied to construct HE schemes so that better security/performance can be achieved. The answer is certain, and various quantum homomorphic encryption (QHE) schemes have been proposed. In summary, these schemes can be classified into two categories. One is efficient with information-theoretical security (ITS) that can only evaluate a subset of all possible functions [19–24]; the other can only achieve computational security [25–29]. Besides, it has been shown that it is impossible to construct an efficient quantum FHE with ITS [30,31]. Recently, Dor Bitan *et al.* proposed a quantum homomorphic encryption scheme [32] using a specific family of random bases. It can encrypt and outsource the storage of classical data while enabling quantum gate computations over the encrypted data with ITS.

In this work, we improve Dor Bitan's scheme with multiparty structure to achieve flexibility. After that, the scheme will be more practical in multiparty situation. Because after the dealer encrypts the data, more than one participant can cooperate to decrypt it sequentially with an appointed key. Furthermore, a (t, n) threshold quantum secret sharing scheme (QSS) (see basic definitions in [33]) is proposed so that no less than t participants can cooperate to recover the secret. In fact, the QSS scheme can be seen as a derivative of the QHE scheme [32]. Also, there is a QSS scheme [34] derived from the QHE scheme [22]. These two QSS schemes can evaluate the encoded quantum states without the need to decode the secret while having some differences, such as threshold ((t, n) or (n, n)), shared secrets (classical bits or quantum states), particle transmission mode (straight line type or tree type). As a result, both proposed schemes in this paper keep the same properties as the basic one [32] after analysis. Specifically, both schemes are information theoretically secure, perfectly correct and also support

homomorphic operations in a fully compact and non-interactive way. Finally, we carry out experiments on the IBM Q Experience platform and the statistical results confirm the feasibility of our schemes.

2 Preliminaries

2.1 The homomorphic random basis encryption scheme

Homomorphic encryption (HE) schemes can be described in a collection of four algorithms, which are key generation (Gen), encryption (Enc), evaluation (Eval), decryption (Dec). We give a brief review of the homomorphic random basis encryption scheme in the following.

- *Gen* Output a key that is a uniformly random pair (θ, ϕ) from $[0,2\pi]\times\{\frac{\pi}{2}, -\frac{\pi}{2}\}$.
- *Enc* Output a qubit $|q\rangle$ which is achieved from $|q\rangle = K|b\rangle$ with input message $b \in \{0, 1\}$ and a key $k = (\theta, \phi)$. Here the K is the encrypting operator in the form

$$K = \begin{bmatrix} \cos(\theta/2) & \sin(\theta/2) \\ e^{i\phi}\sin(\theta/2) & -e^{i\phi}\cos(\theta/2) \end{bmatrix}.$$

- *Dec* Output the plaintext of the input $|q\rangle$ with the key $k = (\theta, \phi)$. It can be achieved by applying $K^\dagger$ to $|q\rangle$ and outputting the measurement of $K^\dagger|q\rangle$ in the computational basis.

It supports homomorphic evaluation of the X gate, CNOT gate and D gate (used to create *Bell state*), where the control qubit is in the computational basis. Here, we focus on the X gate and CNOT gate, which appear in our paper. For the X gate, we can set $|\psi_0\rangle = K|0\rangle$, $|\psi_1\rangle = K|1\rangle$ and get

$$X|\psi_0\rangle = \pm i|\psi_1\rangle\,, X|\psi_1\rangle = \mp i|\psi_0\rangle\,. \tag{1}$$

For the CNOT gate with control qubit in the computational basis, we can verify that

$$\mathrm{CNOT}|1\rangle\otimes|\psi_0\rangle = \pm i|1\rangle\otimes|\psi_1\rangle\,, \mathrm{CNOT}|1\rangle\otimes|\psi_1\rangle = \mp i|1\rangle\otimes|\psi_0\rangle\,. \tag{2}$$

Since $\pm i$ $(\mp i)$ is an overall phase, we can drop it when measuring the quantum states.

2.2 The secret sharing scheme of Shamir

Here, we introduce the secret sharing scheme proposed by Shamir with (t, n) threshold [35]. In the scheme, it shows how to divide the secret s into n pieces in such a way that any t pieces can recover s easily, but never reveals any information about s even with complete knowledge of $t-1$ pieces. The scheme consists of two algorithms:

1. *Share generation* the dealer D picks a random polynomial $f(x)$ of degree $t-1$: $f(x) = a_0 + a_1x + \cdots + a_{t-1}x^{t-1} \bmod p$ with secret $s = a_0$ and all coefficients

$a_0, a_1, \ldots, a_{t-1}$ are in a finite field $\mathbb{F}_p$, p is a prime. Then D computes: $s_j = f(x_j)$, $j = 1, 2, \ldots, n$ with that x_j is the public information of party P_j. At last, the algorithm outputs a list of n shares $(s_1, s_2, \ldots, s_n)$ and allocates each share s_j to party P_j securely.

2. *Secret reconstruction* it takes any m ($m \geq t$) shares s_j, $j \in \mathcal{U} = \{i_1, i_2, \ldots, i_m\}$, $\mathcal{U} \subseteq \{1, 2, \ldots, n\}$ as inputs and outputs the secret s, which can be achieved from

$$s = \sum_{j \in \mathcal{U}} c_j = \sum_{j \in \mathcal{U}} f(x_j) \prod_{r \in \mathcal{U}, r \neq j} \frac{x_r}{x_r - x_j} \bmod p. \tag{3}$$

3 Multiparty decryption over the classical bit

Suppose the dealer Alice uses the random basis encryption scheme ($|0\rangle, |1\rangle$ represent classical bit 0,1 respectively) to encrypt her message among n participants Bob_j, $j = 1, 2 \ldots, n$. After receiving the encrypted quantum state, n participants Bob_j can collaborate to decrypt the message of Alice. The multiparty decryption (MD) scheme can be described as follows with a flowchart in Fig. 1a.

1: Alice generates n decryption keys θ_j, $j = 1, 2, \ldots, n$ from her key $\theta_0 \in [0, 2\pi]$ and sends each θ_j to the participant Bob_j using QKD, where the keys satisfy the condition $\theta_0 = \sum_{j=1}^{n} \theta_j \bmod 2\pi$.

2: Alice uses the random basis encryption scheme to encrypt her message b yielding the encrypted qubit in the form $|q\rangle = K_0|b\rangle$. Later, it is shared among n participants, here K_0 is the encrypting operator K with a key $(\theta_0, \phi = \frac{\pi}{2})$.

3: Participants Bob_j, $j = 1, 2 \ldots, n-1$, each performs $UK_j^{\dagger}$ on the received qubit sequentially and passes it to the next with $U = \begin{bmatrix} 0 & 1 \\ i & 0 \end{bmatrix}$.

4: Finally, the last participant Bob_n receives the resulted qubit and performs $V_n K_n^{\dagger}$ on it. The operators $K_j^{\dagger}$, $j = 1, 2 \ldots, n$ are the conjugate transpose of the encrypting operator K with a key $(\theta_j, \phi = \frac{\pi}{2})$, which are in the form $K_j^{\dagger} = \begin{bmatrix} \cos(\theta_j/2) & -i\sin(\theta_j/2) \\ \sin(\theta_j/2) & i\cos(\theta_j/2) \end{bmatrix}$, and

$$V_n = \begin{cases} \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = -I, n = 1 \bmod 4, \\ \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = -XZ, n = 2 \bmod 4, \\ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I, n = 3 \bmod 4, \\ \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = XZ, n = 0 \bmod 4. \end{cases}$$

After that, he measures the qubit in the computational basis and outputs the measurement result b as the message of Alice.

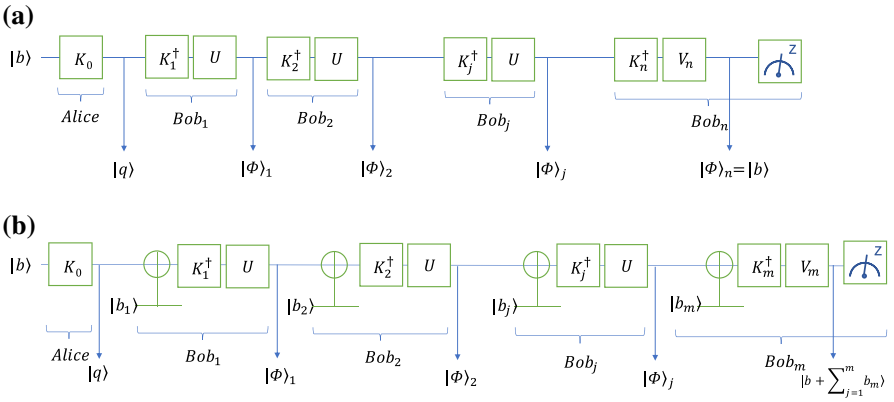

Fig. 1 The flow chart of the MD scheme (**a**) and QSS scheme (**b**)

4 Threshold quantum secret sharing scheme

Recently, a verifiable framework for quantum secret sharing was proposed [36]. Here, we propose a QSS under this framework which includes four algorithms (see the flowchart in Fig. 1b).

1. *Classical private share distribution* in this algorithm, the dealer Alice uses Shamir's scheme to produce n shares s_j, $j = 1, 2, \ldots, n$ from the private value s with threshold $t (t \leq n)$ and prime p. She sends these shares s_j to each participants Bob_j using QKD.
2. *Secret encoding* assume Alice's secret is a classical bit b, then she uses the random basis encryption scheme to encrypt it with a key $(\theta_0 = \frac{2\pi s}{p}, \phi = \frac{\pi}{2})$ and the resulted qubit is $|q\rangle = K_0|b\rangle$. After that, the qubit is shared among participants.
3. *Sequential operation on single quantum system* after receiving the qubit, arbitrary m participants can recover the secret of Alice, here we assume these m participants are Bob_j, $j = 1, 2 \ldots, m$. To recover the secret, each except Bob_m first prepares a random bit $b_j \in \{0, 1\}$, $j = 1, 2, \ldots, m-1$ as the control qubit, then performs the CNOT gate with the received qubit as the target qubit. Later, each continues to perform $UK_j^{\dagger}$ on the received qubit sequentially with $\theta_j = \frac{2\pi c_j}{p}$ (c_j can be computed in Eq. 3).
4. *Secret reconstruction* the last participant Bob_m also prepares the random bit b_m and performs the CNOT gate, however, followed with the decryption $V_m K_m^{\dagger}$. Finally, he measures the qubit in the computational basis and outputs the measurement result $b + \sum_{j=1}^{m} b_m \bmod 2$. By exchanging the random numbers b_j, each of m participants can recover the value b as Alice's secret.

5 Analysis of the two schemes

5.1 Correctness

We will prove that both schemes generate expected outputs in the following.

In both schemes, if all the operations on the qubit do not transform the state (or with an overall phase), then the measurement result of the qubit equals to the original classical bit. Here, we first prove the following Theorem 1, which can show the correctness of the MD scheme.

Theorem 1 *If* $V_1 K_1^\dagger K_0 = I$ *and* $V_n K_n^\dagger \left[\prod_{j=n-1}^{1} (U K_j^\dagger)\right] K_0 = I, n \geq 2$ *hold with the condition* $\theta_0 = \sum_{j=1}^{n} \theta_j mod 2\pi$, *then the MD scheme can achieve the perfect correctness.*

Proof For the first case, it has the form

$$\begin{aligned} V_1 K_1^\dagger K_0 &= \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} \cos\frac{\theta_1}{2} & -i\sin\frac{\theta_1}{2} \\ \sin\frac{\theta_1}{2} & i\cos\frac{\theta_1}{2} \end{bmatrix} \begin{bmatrix} \cos\frac{\theta_0}{2} & \sin\frac{\theta_0}{2} \\ i\sin\frac{\theta_0}{2} & -i\cos\frac{\theta_0}{2} \end{bmatrix} \\ &= \begin{bmatrix} -\cos\frac{\sigma_1}{2} & -\sin\frac{\sigma_1}{2} \\ \sin\frac{\sigma_1}{2} & -\cos\frac{\sigma_1}{2} \end{bmatrix} = I, (\sigma_1 = \theta_0 - \theta_1). \end{aligned} \tag{4}$$

Then, it is the same for $n = 2, 3, 4$,

$$\begin{aligned} V_2 K_2^\dagger U K_1^\dagger K_0 &= V_2 K_2^\dagger \begin{bmatrix} 0 & 1 \\ i & 0 \end{bmatrix} \begin{bmatrix} \cos\frac{\sigma_1}{2} & \sin\frac{\sigma_1}{2} \\ -\sin\frac{\sigma_1}{2} & \cos\frac{\sigma_1}{2} \end{bmatrix} \\ &= \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} \cos\frac{\theta_2}{2} & -i\sin\frac{\theta_2}{2} \\ \sin\frac{\theta_2}{2} & i\cos\frac{\theta_2}{2} \end{bmatrix} \begin{bmatrix} -\sin\frac{\sigma_1}{2} & \cos\frac{\sigma_1}{2} \\ i\cos\frac{\sigma_1}{2} & i\sin\frac{\sigma_1}{2} \end{bmatrix} \\ &= \begin{bmatrix} -\cos\frac{\sigma_2}{2} & -\sin\frac{\sigma_2}{2} \\ \sin\frac{\sigma_2}{2} & -\cos\frac{\sigma_2}{2} \end{bmatrix} = I, (\sigma_2 = \theta_0 - \theta_1 - \theta_2). \end{aligned} \tag{5}$$

$$\begin{aligned} V_3 K_3^\dagger \prod_{j=2}^{1} (U K_j^\dagger) K_0 &= V_3 K_3^\dagger \begin{bmatrix} 0 & 1 \\ i & 0 \end{bmatrix} \begin{bmatrix} -\sin\frac{\sigma_2}{2} & \cos\frac{\sigma_2}{2} \\ -\cos\frac{\sigma_2}{2} & -\sin\frac{\sigma_2}{2} \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \cos\frac{\theta_3}{2} & -i\sin\frac{\theta_3}{2} \\ \sin\frac{\theta_3}{2} & i\cos\frac{\theta_3}{2} \end{bmatrix} \begin{bmatrix} -\cos\frac{\sigma_2}{2} & -\sin\frac{\sigma_2}{2} \\ -i\sin\frac{\sigma_2}{2} & i\cos\frac{\sigma_2}{2} \end{bmatrix} \\ &= \begin{bmatrix} -\cos\frac{\sigma_3}{2} & -\sin\frac{\sigma_3}{2} \\ \sin\frac{\sigma_3}{2} & -\cos\frac{\sigma_3}{2} \end{bmatrix} = I, (\sigma_3 = \theta_0 - \sum_{j=1}^{3} \theta_j). \end{aligned} \tag{6}$$

$$
\begin{aligned}
V_4 K_4^{\dagger} \prod_{j=3}^{1} (U K_j^{\dagger}) K_0 &= V_4 K_4^{\dagger} \begin{bmatrix} 0 & 1 \\ i & 0 \end{bmatrix} \begin{bmatrix} -\cos\frac{\sigma_2}{2} & -\sin\frac{\sigma_2}{2} \\ \sin\frac{\sigma_2}{2} & -\cos\frac{\sigma_2}{2} \end{bmatrix} \\
&= \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \cos\frac{\theta_4}{2} & -i\sin\frac{\theta_4}{2} \\ \sin\frac{\theta_4}{2} & i\cos\frac{\theta_4}{2} \end{bmatrix} \begin{bmatrix} \sin\frac{\sigma_3}{2} & -\cos\frac{\sigma_3}{2} \\ -i\cos\frac{\sigma_3}{2} & -i\sin\frac{\sigma_3}{2} \end{bmatrix} \\
&= \begin{bmatrix} -\cos\frac{\sigma_4}{2} & -\sin\frac{\sigma_4}{2} \\ \sin\frac{\sigma_4}{2} & -\cos\frac{\sigma_4}{2} \end{bmatrix} = I, (\sigma_4 = \theta_0 - \sum\nolimits_{j=1}^{4} \theta_j).
\end{aligned} \tag{7}
$$

Until now, we can summarize it for the general case $n = 4m + 1, 4m + 2, 4m + 3, 4m + 4, m \in \{1, 2, \ldots\}$. For $n = 4m + 1$, it has the form

$$
\begin{aligned}
& V_n K_n^{\dagger} \left[\prod_{j=m-1}^{0} \left(\prod_{l=4}^{1} U K_{4j+l}^{\dagger} \right) \right] K_0 \\
&= V_n K_n^{\dagger} \left[\prod_{j=m-1}^{1} \left(\prod_{l=4}^{1} U K_{4j+l}^{\dagger} \right) \right] \begin{bmatrix} \cos\frac{\sigma_4}{2} & \sin\frac{\sigma_4}{2} \\ i\sin\frac{\sigma_4}{2} & -i\cos\frac{\sigma_4}{2} \end{bmatrix} \\
&= V_n K_n^{\dagger} \left[\prod_{j=m-1}^{2} \left(\prod_{l=4}^{1} U K_{4j+l}^{\dagger} \right) \right] \begin{bmatrix} \cos\frac{\sigma_8}{2} & \sin\frac{\sigma_8}{2} \\ i\sin\frac{\sigma_8}{2} & -i\cos\frac{\sigma_8}{2} \end{bmatrix} \\
&= V_n K_n^{\dagger} \begin{bmatrix} \cos\frac{\sigma_4 m}{2} & \sin\frac{\sigma_4 m}{2} \\ i\sin\frac{\sigma_4 m}{2} & -i\cos\frac{\sigma_4 m}{2} \end{bmatrix} \\
&= I, (\sigma_{4m+1} = \theta_0 - \sum\nolimits_{j=1}^{4m+1} \theta_j).
\end{aligned} \tag{8}
$$

Later, it is easy to verify the equation when $n = 4m + 2, 4m + 3, 4m + 4$ just like the method to verify $n = 2, 3, 4$. At last, we can get $V_1 K_1^{\dagger} K_0 = I$ and $V_n K_n^{\dagger} \left[\prod_{j=n-1}^{1} (U K_j^{\dagger}) \right] K_0 = I, n \geq 2$, and this completes the proof. □

Since the QSS scheme is derived from the MD scheme and we use Theorem 1 to show the correctness of the MD scheme; thus, we can use a new theorem derived from Theorem 1 to show the correctness of the QSS scheme. In the QSS scheme, we can easily verify that $\theta_0 = \frac{2\pi s}{p}, \theta_j = \frac{2\pi c_j}{p}$, $j = 1, 2, \ldots, m$ satisfy $\theta_0 = \sum_{j=1}^{m} \theta_j \bmod 2\pi$ using Eq. 3. Therefore proving Theorem 2 is enough to show the correctness.

Theorem 2 *If the following equation*

$$
V_m K_m^{\dagger} \left[\prod_{j=m-1}^{1} (U K_j^{\dagger} X^{b_j}) \right] K_0 = \begin{cases} I, \oplus_{j=1}^{m} b_j = 0, \\ Y, \oplus_{j=1}^{m} b_j = 1, \end{cases} \tag{9}
$$

$m \geq 2$, holds for the condition $\theta_0 = \sum_{j=1}^{m} \theta_j mod 2\pi$, it can be concluded that the QSS scheme is perfectly correct.

Proof Using Theorem 1, we can know that sequential operations can complete the decryption successfully. So Eq. 9 can be rewritten as

$$V_m K_m^{\dagger} \left[\prod_{j=m-1}^{1} (U K_j^{\dagger}) \right] X^{\oplus_{j=1}^{m} b_j} K_0 = \begin{cases} I, \oplus_{j=1}^{m} b_j = 0, \\ Y, \oplus_{j=1}^{m} b_j = 1. \end{cases} \tag{10}$$

If $\oplus_{j=1}^{m} b_j = 0$, it is the same as Theorem 1 and if $\oplus_{j=1}^{m} b_j = 1$, we can simplify it as $K_0^{\dagger} X K_0 = Y$.

In conclusion, Eq. 9 holds for $\theta_0 = \sum_{j=1}^{m} \theta_j \mathrm{mod} 2\pi$ yielding the correctness of the Theorem 2. □

5.2 Security

In the paper [37], the authors first sketch a scenario for private quantum channels. Assume Alice wants to send a pure state $|\phi\rangle$ to Bob from the set $\mathcal{S}$, she appends ancilla qubits ρ_a to $|\phi\rangle\langle\phi|$ and then applies unitary transformation U_i to $|\phi\rangle\langle\phi| \otimes \rho_a$, where i is the key with probability p_i. Bob (shares the key i with Alice) receives the resulted state and performs U_i^{-1} to get $|\phi\rangle\langle\phi| \otimes \rho_a$. After that, he removes the ancilla ρ_a and achieves Alice's information $|\phi\rangle\langle\phi|$. Then they formalize this scenario so that Bob can recover the state perfectly with security against an eavesdropper in their definition. Following this idea, we adapt the definition to continuous setting for random basis encryption [32] and multiparty decryption.

Definition 1 Let $\mathcal{S} \subseteq \mathcal{H}_2$ be a set of qubits, $Q = \{U_i, i \in I\}$ be a superoperator where each U_i is a unitary mapping on $\mathcal{H}_2$, and ρ_0 be some density matrix. Then $[\mathcal{S}, \mathcal{E}, \rho_0]$ is called perfect masking of a given element $|\phi\rangle$ if and only if for all $|\phi\rangle \in \mathcal{S}$ we have

$$\int_I U_i \, |\phi\rangle \, \langle\phi| \, U_i^{\dagger} = \rho_0. \tag{11}$$

In the proposed MD scheme, for the dealer's encryption, we have $\mathcal{S} = \{|0\rangle, |1\rangle\}$, $Q = \{K_0, \theta_0 \in I\}$ and $I = [0, 2\pi]$ is a set of real numbers. According to Definition 1, the dealer's encryption is perfectly secure if and only if for all $|\phi\rangle \in \mathcal{S}$,

$$\int_I K_0 \, |0\rangle \, \langle 0| \, K_0^{\dagger} = \int_I K_0 \, |1\rangle \, \langle 1| \, K_0^{\dagger}, \tag{12}$$

is satisfied. A routine computation in the following can show the left and right sides of Eq. 12 are equal.

Proof

$$\int_I K_0|0\rangle\langle 0|K_0^\dagger = \int_{\theta_0=0}^{2\pi} \begin{bmatrix} \frac{1+\cos\theta_0}{2} & -\frac{i\sin\theta_0}{2} \\ \frac{i\sin\theta_0}{2} & \frac{1-\cos\theta_0}{2} \end{bmatrix} = \begin{bmatrix} \pi & 0 \\ 0 & \pi \end{bmatrix},$$
$$\int_I K_0|1\rangle\langle 1|)K_0^\dagger = \int_{\theta_0=0}^{2\pi} \begin{bmatrix} \frac{1-\cos\theta_0}{2} & \frac{i\sin\theta_0}{2} \\ -\frac{i\sin\theta_0}{2} & \frac{1+\cos\theta_0}{2} \end{bmatrix} = \begin{bmatrix} \pi & 0 \\ 0 & \pi \end{bmatrix}.$$

□

So for other participants' local operations $Q = \{UK_j^\dagger, \theta_j \in I\}$, $j = 1, 2, \ldots, n-1$, $\mathcal{S} = \left\{ \left|\varphi_{j-1}\right\rangle_b = \left[\prod_{r=j-1}^{1} (UK_r^\dagger)\right] K_0 |b\rangle, b = 0, 1 \right\}$ for $j = 2, 3, \ldots, n-1$ and $\mathcal{S} = \left\{ |\varphi_0\rangle_b = K_0 |b\rangle, b = 0, 1 \right\}$ for $j = 1$, we need to show

$$\int_I UK_j^\dagger \left|\varphi_{j-1}\right\rangle_{0\,0} \left\langle\varphi_{j-1}\right| K_j U^\dagger = \int_I UK_j^\dagger \left|\varphi_{j-1}\right\rangle_{1\,1} \left\langle\varphi_{j-1}\right| K_j U^\dagger. \tag{13}$$

Fortunately, after computation, we can achieve that the both sides of Eq. 13 are equal as well. To conclude, after the dealer's encryption, the density matrix that an adversary sees is equal and it is the same for participants' partial decryption, regardless of the input. *Therefore, the adversary cannot gain any information about the encrypted message and our MD scheme is secure.*

To show the security of the QSS, the method of proof is the same as the MD scheme. After the dealer's operation, we have $Q = \{K_0, \theta_0 \in I\}$, here $I = [0, 2\pi]$ is a set of real numbers, so the condition is Eq. 12. For other participants's operations, we have $Q = \{UK_j^\dagger X^{b_j}, \theta_j \in I\}$, $b_j \in \{0, 1\}$, $j = 1, 2, \ldots, m-1$, $\mathcal{S} = \left\{ \left|\varphi_{j-1}\right\rangle_b = \left[\prod_{r=j-1}^{1} (UK_r^\dagger X^{b_r})\right] K_0 |b\rangle, b = 0, 1 \right\}$ for $j = 2, 3, \ldots, m-1$ and $\mathcal{S} = \left\{ |\varphi_0\rangle_b = K_0 |b\rangle, b = 0, 1 \right\}$ for $j = 1$, so the condition is

$$\int_I UK_j^\dagger X^{b_j} \left|\varphi_{j-1}\right\rangle_{0\,0} \left\langle\varphi_{j-1}\right| X^{b_j} K_j U^\dagger = \int_I UK_j^\dagger X^{b_j} \left|\varphi_{j-1}\right\rangle_{1\,1} \left\langle\varphi_{j-1}\right| X^{b_j} K_j U^\dagger, \tag{14}$$

with $X^\dagger = X$. The correctness of Eq. 14 can also be verified after computation. Finally, we can conclude the QSS scheme is also secure.

6 Experiments on IBM Q experience

In the paper, the used unitary operations are most single-qubit operations. Therefore, to show the feasibility of our schemes, we run them in a superconducting qubit platform, provided by the IBM Q Experience.

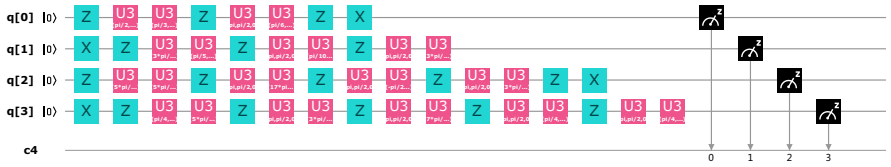

Fig. 2 The designed quantum circuit for testing the MD scheme. Here, "Z","X","U3" and panel gates represent the Pauli Z gate, Pauli X gate, $U_3(\theta, \phi, \lambda)$ gate and measurement in the computational basis, respectively

In Sect. 5.1, we have shown the correctness of our schemes in theory. Here, we first design four cases for the MD scheme with

$$\begin{aligned}
&n = 2, \theta_0 = \frac{\pi}{2}, \theta_1 = \frac{\pi}{3}, \theta_2 = \frac{\pi}{6},\\
&n = 3, \theta_0 = \frac{3\pi}{5}, \theta_1 = \frac{\pi}{5}, \theta_2 = \frac{\pi}{10}, \theta_3 = \frac{3\pi}{10},\\
&n = 4, \theta_0 = \frac{5\pi}{9}, \theta_1 = \frac{5\pi}{3}, \theta_2 = \frac{17\pi}{9}, \theta_3 = \frac{-\pi}{2}, \theta_4 = \frac{3\pi}{2},\\
&n = 5, \theta_0 = \frac{\pi}{4}, \theta_1 = \frac{5\pi}{4}, \theta_2 = \frac{3\pi}{4}, \theta_3 = \frac{7\pi}{4}, \theta_4 = \frac{\pi}{4}, \theta_5 = \frac{\pi}{4}.
\end{aligned} \tag{15}$$

In each case, the dealer first uses θ_0 to encrypt her bit b ($b = n \bmod 2$), then n participants sequentially decrypt the resulted qubit using θ_j. At last, they can get dealer's bit by measuring in the computational basis.

To perform the experiments, we can design the corresponding quantum circuit following Fig. 1a and it is illustrated in Fig. 2. Thanks to the U_3 operation offered by IBM Q Experience, which is in the form

$$U_3(\theta, \phi, \lambda) = \begin{bmatrix} \cos(\theta/2) & -e^{i\lambda}\sin(\theta/2) \\ e^{i\phi}\sin(\theta/2) & e^{i\lambda+i\phi}\cos(\theta/2) \end{bmatrix}. \tag{16}$$

Therefore, the operations used in the MD scheme can be represented as

$$\begin{aligned}
&K_0 = U_3(\theta_0, \pi/2, 0)Z, U = U_3(\pi, \pi/2, 0)Z,\\
&K_j^{\dagger} = U_3(\theta_j, 0, \pi/2), j = 1, 2, \ldots, n.
\end{aligned} \tag{17}$$

At last, we first run the circuit for three rounds with each round containing 8192 shots for simulation. However, for experiment, we run each line in the circuit independently. We show the statistical results for both simulation and experiment in Fig. 4.

It is the same for testing the QSS scheme. Assume the following (4,5)-QSS case, the selected random function is $f(x) = 2x^3+4x^2+9x+12 \bmod 13$ ($s = 12, p = 13$), the public information of participants P_j are $x_j = 1, 2, 3, 4, 5$, respectively. Considering Bob_j, $j \in \mathcal{U} = \{1, 2, 3, 5\}$ want to cooperate to recover the secret $S = b \in \{0, 1\}$,

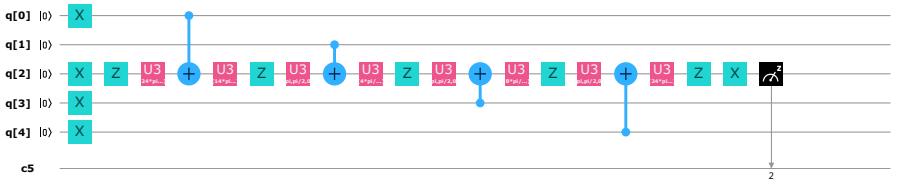

Fig. 3 The designed quantum circuit for QSS scheme with "+" represents the CNOT gate and others are the same in Fig. 2

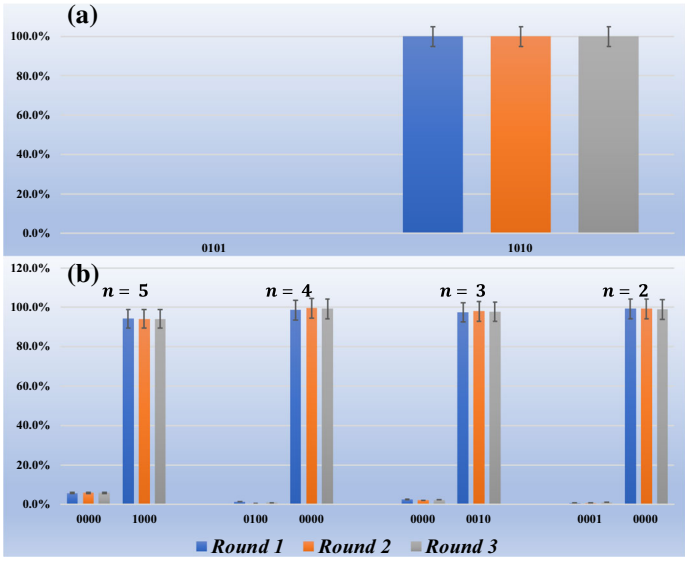

Fig. 4 Measurement results of quantum circuit in Fig. 2. The simulation results (**a**) and experimental results (**b**) are performed on the "ibmq_qasm_simulator" simulator and "ibmqx2" superconducting quantum systems. The error bar denotes the standard deviation

they each can compute the θ_j:

$$\theta_0 = \frac{24\pi}{13}, \theta_1 = \frac{14\pi}{13}, \theta_2 = \frac{4\pi}{13}, \theta_3 = \frac{8\pi}{13}, \theta_5 = \frac{24\pi}{13}. \tag{18}$$

Besides, the random selected numbers b_j are 1, 0, 1, 1.

Following Fig. 1b, a corresponding quantum circuit for this QSS case is designed as Fig. 3.

We also run the circuit for three rounds with each round containing 8192 shots for simulation and experiment, and we show the results in Fig. 5.

In Figs. 4a and 5a, we can see the results of simulation are 100% correct, which confirm the correctness of our schemes. However, when it comes to the experimental implementations, the MD scheme can achieve the correctness with 98% on average and the QSS scheme can only get the correct answer with 91% on average (see Figs. 4b and 5b). We would like to remark the wrong results come from the gate errors, which

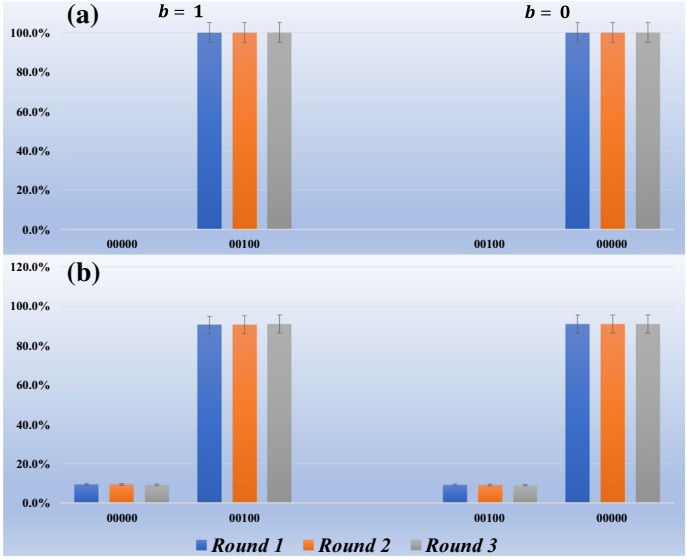

Fig. 5 Measurement results of quantum circuit in Fig. 3 with the same setup in Fig. 4. Here, b is the secret with the measurement result r satisfying $r = b + \sum_{j\in\mathcal{U}} b_j \bmod 2$

could be complemented by error corrections. Moreover, the error rate of the two qubits gate CNOT is larger than a single-qubit gate, which results the lower accuracy of the QSS scheme.

7 Conclusion

The homomorphic encryption scheme enables processing of encrypted data without decrypting them in advance which will be a useful solution for the delegation of computation [38]. In this paper, we first study a QHE scheme using a random base. It can encrypt and outsource the storage of classical data while enabling quantum gate computations over the encrypted data with ITS. Then, we improve it to achieve the multiparty structure which is flexible with the number of parties and further propose a threshold QSS scheme. As a result, we analyze the correctness and security of both schemes yielding they still keep the same properties as the basic one. Also, we test and verify them on the IBM Q Experience and the statistical results confirm their feasibility successfully.

Acknowledgements We would like to thank the anonymous reviewers for helpful suggestions. This work is supported by Key Research and Development Program of China 2018YFB0803400, National Natural Science Foundation of China 61572454, 61572453, 61520106007 and Anhui Initiative in Quantum Information Technologies AHY150100.

References

1. Bennett, C.H., DiVincenzo, D.P.: Quantum information and computation. Nature **404**(6775), 247 (2000)
2. Einstein, A., Podolsky, B., Rosen, N.: Can quantum-mechanical description of physical reality be considered complete? Phys. Rev. **47**, 777–780 (1935)
3. Bell, J.S.: On the einstein podolsky rosen paradox. Physics **1**(3), 195–200 (1964)
4. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In: Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Systems and Signal Processing, pp. 175–179, New York, USA (1984)
5. Bennett, C.H., Brassard, G., Crépeau, C., Jozsa, R., Peresand, A., Wootters, W.K.: Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels. Phys. Rev. Lett. **70**(13), 1895–1899 (1993)
6. Shor, P.W.: Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings 35th Annual Symposium on Foundations of Computer Science, pp. 124–134. IEEE (1994)
7. Grover, L.K.: Quantum mechanics helps in searching for a needle in a haystack. Phys. Rev. Lett. **79**(2), 325 (1997)
8. Hillery, M., Bužek, V., Berthiaume, A.: Quantum secret sharing. Phys. Rev. A **59**(3), 1829 (1999)
9. Crépeau, C., Gottesman, D., Smith, A.: Secure multi-party quantum computation. In: Proceedings of the Thiry-fourth Annual ACM Symposium on Theory of Computing, pp. 643–652. ACM (2002)
10. Zeng, G., Keitel, C.H.: Arbitrated quantum-signature scheme. Phys. Rev. A **65**(4), 042312 (2002)
11. Deng, F.-G., Long, G.L., Liu, X.-S.: Two-step quantum direct communication protocol using the Einstein–Podolsky–Rosen pair block. Phys. Rev. A **68**(4), 042317 (2003)
12. Zhang, K.J., Zhang, L., Song, T.T., Yang, Y.H.: A potential application in quantum networks-deterministic quantum operation sharing schemes with bell states. Scie. China Phys. Mech. Astron. **59**(6), 660302 (2016)
13. Zhang, K., Zhang, X., Jia, H., Zhang, L.: A new n-party quantum secret sharing model based on multiparty entangled states. Quantum Inf. Process. **18**(3), 81 (2019)
14. Zhang, C., Razavi, M., Sun, Z., Situ, H.: Improvements on secure multi-party quantum summation based on quantum fourier transform. Quantum Inf. Process. **18**(11), 336 (2019)
15. Zhang, C., Razavi, M., Sun, Z., Huang, Q., Situ, H.: Multi-party quantum summation based on quantum teleportation. Entropy **21**(7), 719 (2019)
16. Gentry, C., Boneh, D.: A Fully Homomorphic Encryption Scheme. Stanford University, Stanford (2009)
17. Acar, A., Aksu, H., Uluagac, A.S., Conti, M.: A survey on homomorphic encryption schemes: theory and implementation. ACM Comput. Surv. (CSUR) **51**(4), 79 (2018)
18. Martins, P., Sousa, L., Mariano, A.: A survey on fully homomorphic encryption: an engineering perspective. ACM Comput. Surv. (CSUR) **50**(6), 83 (2018)
19. Rohde, P.P., Fitzsimons, J.F., Gilchrist, A.: Quantum walks with encrypted data. Phys. Rev. Lett. **109**(15), 150501 (2012)
20. Liang, M.: Symmetric quantum fully homomorphic encryption with perfect security. Quantum Inf. Process. **12**(12), 3675–3687 (2013)
21. Tan, S.-H., Kettlewell, J.A., Ouyang, Y., Chen, L., Fitzsimons, J.F.: A quantum approach to homomorphic encryption. Sci. Rep. **6**, 33467 (2016)
22. Ouyang, Y., Tan, S.-H., Fitzsimons, J.F.: Quantum homomorphic encryption from quantum codes. Phys. Rev. A **98**(4), 042334 (2018)
23. Tan, S.-H., Ouyang, Y., Rohde, P.P.: Practical somewhat-secure quantum somewhat-homomorphic encryption with coherent states. Phys. Rev. A **97**(4), 042308 (2018)
24. Ouyang, Y., Tan, S.-H., Fitzsimons, J., Rohde, P.P.: Homomorphic encryption of linear optics quantum computation on almost arbitrary states of light with asymptotically perfect security. Phys. Rev. Res. **2**(1), 013332 (2020)
25. Broadbent, A., Jeffery, S.: Quantum homomorphic encryption for circuits of low t-gate complexity. In: Annual Cryptology Conference, pp. 609–629. Springer, Berlin (2015)
26. Dulek, Y., Schaffner, C., Speelman, F.: Quantum homomorphic encryption for polynomial-sized circuits. In: Annual International Cryptology Conference, pp. 3–32. Springer, Berlin (2016)

27. Alagic, G., Dulek, Y., Schaffner, C., Speelman, F.: Quantum fully homomorphic encryption with verification. In: International Conference on the Theory and Application of Cryptology and Information Security, pp. 438–467. Springer, Berlin (2017)
28. Mahadev, U.: Classical homomorphic encryption for quantum circuits. In: 2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS), pp. 332–338. IEEE (2018)
29. Brakerski, Z.: Quantum FHE (almost) as secure as classical. In: Annual International Cryptology Conference, pp. 67–95. Springer, Berlin (2018)
30. Yu, L., Pérez-Delgado, C.A., Fitzsimons, J.F.: Limitations on information-theoretically-secure quantum homomorphic encryption. Phys. Rev. A **90**(5), 050303 (2014)
31. Aharonov, D., Brakerski, Z., Chung, K.-M., Green, A., Lai, C.-Y., Sattath, O.: On quantum advantage in information theoretic single-server PIR. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 219–246. Springer, Berlin (2019)
32. Bitan, D., Dolev, S.: Randomly rotate qubits compute and reverse—it-secure non-interactive fully-compact homomorphic quantum computations over classical data using random bases. Cryptology ePrint Archive, Report 2019/1023 (2019). https://eprint.iacr.org/2019/1023
33. Cleve, R., Gottesman, D., Lo, H.-K.: How to share a quantum secret. Phys. Rev. Lett. **83**(3), 648 (1999)
34. Ouyang, Y., Tan, S.-H., Zhao, L., Fitzsimons, J.F.: Computing on quantum shared secrets. Phys. Rev. A **96**(5), 052333 (2017)
35. Shamir, A.: How to share a secret. Commun. ACM **22**(11), 612–613 (1979)
36. Changbin, L., Miao, F., Hou, J., Huang, W., Xiong, Y.: A verifiable framework of entanglement-free quantum secret sharing with information-theoretical security. Quantum Inf. Process. **19**(1), 24 (2020)
37. Ambainis, A., Mosca, M., Tapp, A., De Wolf, R.: Private quantum channels. In: Proceedings 41st Annual Symposium on Foundations of Computer Science, pp. 547–553. IEEE (2000)
38. Rivest, R.L., Adleman, L., Dertouzos, M.L.: On data banks and privacy homomorphisms. Founda. Sec. Comput. **4**(11), 169–180 (1978)