A Letters Journal Exploring the Frontiers of Physics

February 2022

EPL, **137** (2022) 38001
doi: 10.1209/0295-5075/ac4fd2

www.epljournal.org

Secure delegated quantum computation based on Z-rotation encryption

Shuquan Ma[1], Changhua Zhu[1,2,3(a)], Min Nie[3,4], Dongxiao Quan[1] and Changxing Pei[1]

[1] *State Key Laboratory of Integrated Services Networks, Xidian University - Xi'an, Shaanxi 710071, China*
[2] *Collaborative Innovation Center of Quantum Information of Shaanxi Province, Xidian University Xi'an, Shaanxi 710071, China*
[3] *Shaanxi Key Laboratory of Information Communication Network and Security, Xi'an University of Posts and Telecommunications - Xi'an, Shaanxi 710121, China*
[4] *School of Communications and Information Engineering, Xi'an University of Posts and Telecommunications Xi'an, Shaanxi 710121, China*

received 11 November 2021; accepted in final form 28 January 2022
published online 22 April 2022

Abstract – Quantum computing on encrypted data allows a client who has limited quantum capacity to delegate his or her private computation to an untrusted quantum server, while the input and output are encrypted by the quantum one-time pad and only the client can correctly decrypt them. Generally, the client is required to have ability to prepare some single qubits and perform some basic gates. In this work, we consider a further restricted situation where the client can only prepare one single qubit and perform one basic gate. Specifically, we show that as long as the client can prepare a fixed qubit $|+\rangle$ and perform a fixed phase gate P, then he or she can still achieve the secure delegated quantum computation. Besides, our protocol can provide a more rigorous security for any quantum computation. For example, even if some encryption keys about the computation are leaked, it can still guarantee the privacy of the input and output. Finally, our protocol experimentally has a great significance in reducing the device complexity of the client's side.

Introduction. – Secure delegated quantum computation (SDQC) achieves a basic functionality that a client can delegate his or her computation to an untrusted server while the server cannot obtain the information about the input and output of the client's computation. SDQC is thought of as one of important quantum computing patterns [1–3] in the future, since we know building and maintaining a quantum computer is extremely difficult, and ordinary clients cannot afford such a quantum computer in the near future.

Any delegated quantum computation protocol that achieves this functionality can be referred to as a SDQC protocol. There are two distinct ways to achieve SDQC [4–12]. One simple way is making use of the idea of *homomorphic encryption* [13] in classical cryptography, by which the client first prepares the input state and encrypts it by some quantum operations, then sends the encrypted input to the server, after receiving the client's input the server performs the delegated quantum circuit on this encrypted input, in the end of the computation the output state is still encrypted and only the client can correctly decrypt it. During the computation, it is allowed that the client and the server can exchange necessary information so that the computation can be performed correctly. The first SDQC protocol based on this method is put forward by Childs [4]. In Childs' protocol the client is required to be able to prepare some single qubits and perform two Pauli gates and a two-qubit swap gate. Besides that, it also requires a two-way quantum communication between client and server during the computation. Inspired by Childs' work, many related quantum computation protocols were subsequently proposed [7,14–18]. Another way to achieve the

(a) E-mail: chhzhu@xidian.edu.cn (corresponding author)

SDQC derives from the *measurement-based quantum computation* (MBQC) model [19]. The first prototype protocol of delegated quantum computation based on this model is proposed by Raussendorf and Briegel [20]. However, in their work they did not consider the privacy of computations. Then, Broadbent *et al.* developed their work by proposing a protocol named *universal blind quantum computation* (UBQC) [5]. In fact, the UBQC can be thought of as an enhanced SDQC, which achieves not only the basic functionality but also that the server can learn nothing about the computation itself (*i.e.*, algorithm). In [5], the client only needs to prepare eight possible single qubits and there is no need for a quantum communication during the computation. There are also some different schemes to implement a SDQC based on the MBQC model [8,21–23], for example in [8] the authors proposed a blind quantum computation protocol where the client only needs to perform some single-qubit measurements. Nevertheless, the MBQC model generally requires much more ancillary qubits. Typically, in the UBQC protocol, for each basic gate (even if a trivial gate I), the client needs to prepare eight ancillary qubits.

Considering the aforementioned facts, Broadbent then proposed an improved SDQC protocol, named *quantum computing on encrypted data* (QCED) [7], which reduces not only the quantum capacities of the client but also the consumption of ancillary qubits. Specifically, the client only needs to prepare some specified single qubits and perform some specified single-qubit operators. Meanwhile, no quantum communication is needed during the computation. Note that both UBQC and QCED protocols have been experimentally demonstrated using photons and linear optics [14,24].

In this letter, we further improve the QCED protocol from the following aspects: We simply optimize the QCED protocol so that the client only needs to prepare one fixed qubit and perform one fixed operator. We also improve the encryption scheme by introducing an extra basic operator so that the protocol can provide a more rigorous security for any quantum computation. We will discuss those detailed improvements in the rest of this letter.

Quantum computing on encrypted data. – Let $|in\rangle$ be the n-qubit input and U be the delegated circuit. The QCED protocol works as follows [7]:

First, the client prepares and encrypts each qubit of $|in\rangle$ by random Pauli operators X and Z, that is for qubit i the client uses $X_i^{a_i}Z_i^{b_i}$ to encrypt it, where $a_i, b_i \in \{0,1\}$ are called *encryption keys*. This encryption is formally called the *quantum one-time pad*, which can provide the information-theoretic security for any input state [25]. Second, the server performs a sequence of basic gates on the encrypted input state. The universal gate set used in the protocol is $\{X, Z, P, T, H, CX\}$. The following identities all hold up to an irrelevant global phase, which has no influence for quantum computing. For example, for any n-qubit state $|\psi\rangle$, applying an XZ on qubit i of $|\psi\rangle$ is equivalent to applying a ZX on this qubit, because two resulting states only differ by a global phase -1.

$$\begin{aligned}
X_i(X_i^{a_i}Z_i^{b_i}) &\equiv (X_i^{a_i}Z_i^{b_i})X_i,\\
Z_i(X_i^{a_i}Z_i^{b_i}) &\equiv (X_i^{a_i}Z_i^{b_i})Z_i,\\
H_i(X_i^{a_i}Z_i^{b_i}) &\equiv (X_i^{b_i}Z_i^{a_i})H_i,\\
P_i(X_i^{a_i}Z_i^{b_i}) &\equiv (X_i^{a_i}Z_i^{a_i\oplus b_i})P_i,\\
T_i(X_i^{a_i}Z_i^{b_i}) &\equiv (X_i^{a_i}Z_i^{a_i\oplus b_i}P_i^{a_i})T_i,\\
CX_{i,j}(X_i^{a_i}Z_i^{b_i}X_j^{a_j}Z_j^{b_j}) &\equiv (X_i^{a_i}Z_i^{b_i\oplus b_j}X_j^{a_i\oplus a_j}Z_j^{b_j})CX_{i,j}.
\end{aligned}$$

Note that there is an undesired term P^a arising in the T gate. To correct this deviation, Broadbent utilized the circuit shown in fig. 1 which she called *gadget*. By this circuit, with the aid of additional inputs of the client, the server can implement a secure T gate as follows:

$$X_i^{a_i}Z_i^{b_i} \xrightarrow{T_i} X_i^{a_i\oplus c_i}Z_i^{(a_ic_i)\oplus(a_iy_i)\oplus b_i\oplus d_i\oplus x_i}T_i, \qquad (1)$$

where $c_i \in \{0,1\}$ is the measurement outcome. The client needs to prepare $x_i = a_i \oplus y_i$ and $Z_i^{d_i}P_i^{y_i}|+\rangle$, where d_i, y_i are uniform in $\{0,1\}$, denoted by $d_i, y_i \in_R \{0,1\}$.

Secure delegated quantum computation. –

Encoding and encryption schemes. Note that in the QCED protocol the author did not specify the encoding basis of input states. By convention, both input and output are encoded in Z basis, *i.e.*, encoding $x \in \{0,1\}^n$ as $|x\rangle = |x_1, x_2, \ldots, x_n\rangle$. Without loss of generality, we can always assume that $|in\rangle = |x\rangle$. Thus, the complete requirement for the client is that he or she is able to prepare two single qubits $|0\rangle, |+\rangle$ and execute three basic gates X, Z, and P. (The qubit $|1\rangle$ can be obtained by $X|0\rangle$.)

There are several manifest redundancies in the QCED protocol. First, if the input is encoded in X basis, *i.e.*, encoding $x_i \in \{0,1\}$ as $|+_{x_i\pi}\rangle$, where $|+_{x_i\pi}\rangle \equiv (|0\rangle + e^{jx_i\pi}|1\rangle)/\sqrt{2}$, then the client does not need to prepare the qubit $|0\rangle$ anymore. Second, since $X_i^{a_i}|+_{x_i\pi}\rangle$ only differs $|+_{x_i\pi}\rangle$ by an unimportant global phase $e^{ja_ix_i\pi}$, thus the client does not need to perform the Pauli X gate once the input is encoded in X basis. Finally, the Pauli Z gate is apparently redundant because of $P^2 = Z$. So, it is sufficient that the client has only ability to prepare the qubit $|+\rangle$ and perform the phase gate P.

However, there also exist several subtle problems. First, although the quantum one-time pad can provide an information-theoretic security, it requires the server has not any *prior* information on the input state. This is an unrealistic requirement, since in a general quantum computation model the server inevitably acquires the encoding information. In this case, the server can completely determine the state of the encrypted input. For example, given any encrypted input qubit in Z basis, *e.g.*, $X_i^{a_i}Z_i^{b_i}|x_i\rangle \equiv |a_i \oplus x_i\rangle$, the server is able to obtain the classical encrypted input $a_i \oplus x_i$ by measuring this qubit in Z basis. Clearly, this encrypted input qubit is no longer a completely mixed state $I/2$ for the server. Second, this

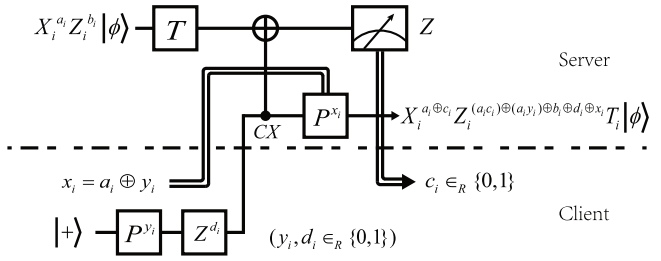

Fig. 1: The T-gadget in ref. [7], where $c_i \in_R \{0,1\}$ is the measurement outcome in Z basis. The double line denotes the classical information flow.

quantum one-time pad is not appropriate for some specific quantum computations. For example, if the quantum computation task delegated to the server is computing $U_f|x\rangle|00\ldots0\rangle = |x\rangle|f(x)\rangle$, where $x \in \{0,1\}^n$. Obviously, all encryption keys $\{a_i\}$ on these fixed qubits $|0\rangle$ will be exposed to the server completely! Finally, there exists a potential security issue in the updating rules of the encryption keys with respect to the T gate. Specifically, suppose that at some point the encryption keys on the qubit i are a_i, b_i and after executing a T gate on it, the keys are updated into a'_i, b'_i. From eq. (1) we know that (a'_i, b'_i) is related to (a_i, b_i). This is a hidden trouble: if the server somehow acquires a'_i, then it can infer a_i from $a'_i = a_i \oplus c_i$. Indeed, the server may infer even more encryption keys on this qubit during the computation. As a result, the server can successfully corrupt this qubit!

Based on those observations, we come up with a simple method to solve those problems, meanwhile quantum capacities of the client do not increase. First, we use the X basis to encode the input. Second, we use random X, Z, and P to encrypt each input qubit. Specifically, for any input $x_i \in \{0,1\}$, the corresponding encrypted input qubit is $X_i^{a_i} Z_i^{b_i} P_i^{c_i} |+_{x_i\pi}\rangle$, where $a_i, b_i, c_i \in_R \{0,1\}$. Despite the Pauli $X_i^{a_i}$ gate, we can easily check that $X_i^{a_i} Z_i^{b_i} P_i^{c_i} |+_{x_i\pi}\rangle = |+_{\alpha_i}\rangle$, where $\alpha_i = (x_i \oplus b_i)\pi + (-1)^{a_i} c_i \pi/2 \in \{0, \pi/2, \pi, 3\pi/2\}$. Since $P \equiv R_z(\pi/2)$, to prepare such an encrypted qubit, the client in fact only needs to prepare the qubit $|+\rangle$ and perform the phase gate P 3 times at most. Furthermore, the new encryption scheme still guarantees an unconditional security. This is because for any qubit ρ, let $\rho' = \frac{1}{2}\sum_{c\in\{0,1\}} P^c \rho P^{\dagger c}$, then we obtain that

$$\sum_{a,b,c\in\{0,1\}} \frac{X^a Z^b P^c \rho P^{\dagger c} Z^b X^a}{8} = \sum_{a,b\in\{0,1\}} \frac{X^a Z^b \rho' Z^b X^a}{4}. \tag{2}$$

Clearly, for any single qubit ρ', the standard quantum one-time pad maps it to a totally mixed state, that is,

$$\frac{1}{2}\sum_{a,b\in\{0,1\}} X^a Z^b \rho' Z^b X^a = \frac{I}{2}. \tag{3}$$

Note also that the encrypted state will be one of X's eigenstates if the encryption key $c = 0$, otherwise it will be one of Y's eigenstates. Since these two bases are completely indistinguishable, the server can learn nothing about the classical encrypted input, *i.e.*, $x_i \oplus b_i$, as long as the server does not know the value of c, even if the input qubit is initialized as $|+\rangle$. More importantly, under this encryption scheme we can see that

$$T_i(X_i^{a_i} Z_i^{b_i} P_i^{c_i}) = (X_i^{a_i} Z_i^{a_i\oplus b_i\oplus(a_i c_i)} P_i^{a_i\oplus c_i}) T_i. \tag{4}$$

It follows from the above result that the T gate can be directly achieved in a non-interactive way. However, the price of this convenience is that the realization of the H gate will become somewhat complicated because $HP^c \neq P^{c'}H$. In this work, we mainly come up with a method to implement the H gate such that

$$X_i^{a_i} Z_i^{b_i} P_i^{c_i} \xrightarrow{H_i} X_i^{a'_i} Z_i^{b'_i} P_i^{c'_i} H_i, \tag{5}$$

where a'_i is irrelevant to a_i, even b_i, c_i, b'_i, c'_i. Thus, the server cannot gain any information about $a_i, b_i, c_i, b'_i, c'_i$ even if it acquires a'_i. And for each H_i gate, the client needs to prepare two classical bits and two ancillary qubits, where two ancillary qubits can be sent to the server before computing.

Generally, the output state of the computation is measured by the server. That is, the output is classical. But, it is possible that the output is a quantum state. For example, the computation task of the client is delegating the server to prepare some quantum system. Since we are considering the client who does not perform the Pauli X gate, therefore in this case each $X_i^{a_i}$ needs to be decrypted by the server. However, directly instructing the server to execute the decryption will result in information leakage about a_i. In order to avoid this problem, the client can instruct the server to execute two successive H gates on each output qubit, that is,

$$X_i^{a_i} Z_i^{b_i} P_i^{c_i} \xrightarrow{H_i} X_i^{a'_i} Z_i^{b'_i} P_i^{c'_i} H_i \xrightarrow{H_i} X_i^{a''_i} Z_i^{b''_i} P_i^{c''_i}, \tag{6}$$

in the end the client discloses a''_i so that the server can decrypt the Pauli X. This can be done since we have known that a''_i is irrelevant to $(a'_i, b'_i, c'_i, b''_i, c''_i)$. This procedure can be viewed as a part of computation, thus in the end the server simply sends the output state to the client.

Main protocol. Let $\mathcal{C}$ and $\mathcal{S}$ denote the client and the server, respectively. We choose $\{Z, P, T, H, CZ\}$ as the universal gate set. Note that some gates are redundant since $Z = P^2 = T^4$. Nevertheless, introducing additional basic gates can significantly improve the efficiency in quantum computing. And we will use the following identities (up to an irrelevant global phase), which can be easily verified:

$$Z_i(X_i^{a_i} Z_i^{b_i} P_i^{c_i}) \equiv (X_i^{a_i} Z_i^{b_i} P_i^{c_i}) Z_i, \tag{7a}$$

$$P_i(X_i^{a_i} Z_i^{b_i} P_i^{c_i}) \equiv (X_i^{a_i} Z_i^{a_i\oplus b_i} P_i^{c_i}) P_i, \tag{7b}$$

$$T_i(X_i^{a_i} Z_i^{b_i} P_i^{c_i}) \equiv (X_i^{a_i} Z_i^{a_i\oplus b_i\oplus(a_i c_i)} P_i^{a_i\oplus c_i}) T_i, \tag{7c}$$

$$CZ_{i,j}(X_i^{a_i} Z_i^{b_i} P_i^{c_i} X_j^{a_j} Z_j^{b_j} P_j^{c_j}) \equiv (X_i^{a_i} Z_i^{a_j\oplus b_i} P_i^{c_i} X_j^{a_j} Z_j^{a_i\oplus b_j} P_j^{c_j}) CZ_{i,j}. \tag{7d}$$

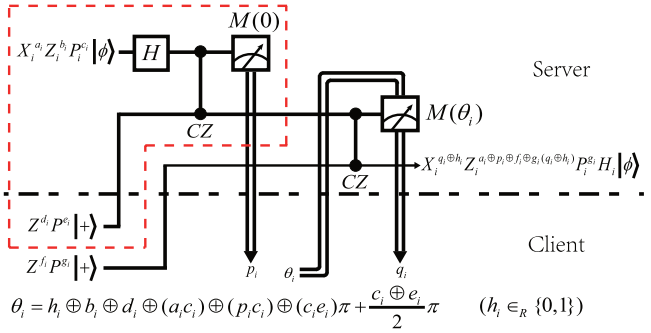

Fig. 2: The H-gadget in our protocol, where $p_i, q_i \in \{0,1\}$ are the measurement outcomes and $M(\theta_i)$ denotes the measurement basis $\{|+_{\theta_i}\rangle, |+_{\theta_i+\pi}\rangle\}$, and $|+_{\theta_i}\rangle = (|0\rangle + e^{j\theta_i}|1\rangle)/\sqrt{2}$.

Protocol: Secure Delegated Quantum Computation

Step 1: Preparation

First, $\mathcal{C}$ chooses randomly $a, b, c \in \{0,1\}^n$ and prepares n qubits $\{|+_{\alpha_i}\rangle\}_{i=1}^n$ as the encrypted $|in\rangle$, where $\alpha_i = (x_i \oplus b_i)\pi + (-1)^{a_i} c_i \pi/2$. Then, for each H_i gate, $\mathcal{C}$ prepares two random ancillary qubits $Z^{d_i}P^{e_i}|+\rangle$ and $Z^{f_i}P^{g_i}|+\rangle$, where $d_i, e_i, f_i, g_i \in_R \{0,1\}$. Finally, $\mathcal{C}$ sends all qubits to $\mathcal{S}$, and $\mathcal{S}$ labels them as $\mathcal{C}$ requests.

Step 2: Computation

According to the construction of U, $\mathcal{S}$ performs a sequence of basic gates on the encrypted qubits in sequence:

- If a Z_i, P_i, T_i, or $CZ_{i,j}$ gate happens, $\mathcal{S}$ just applies it on qubits i, j. Meanwhile, $\mathcal{C}$ updates the corresponding keys according to the rules in eqs. (7a)–(7d).
- If an H_i gate is required, then $\mathcal{S}$ performs the circuit described in fig. 2. After that, $\mathcal{C}$ updates the corresponding encryption keys by the following rule:

$$X_i^{a_i} Z_i^{b_i} P_i^{c_i} \xrightarrow{H_i} X_i^{q_i \oplus h_i} Z_i^{a_i \oplus p_i \oplus f_i \oplus g_i(q_i \oplus h_i)} P_i^{g_i} H_i, \quad (8)$$

where $h_i \in_R \{0,1\}$ is chosen by $\mathcal{C}$ and $p_i, q_i \in \{0,1\}$ are the measurement outcomes.

Step 3: Output

- For a classical output, $\mathcal{S}$ simply measures each output qubit in Z basis, then sends the measurement outcome, denoted by s, to $\mathcal{C}$. To obtain the correct result, $\mathcal{C}$ computes $y = s \oplus a$, where $s, a \in \{0,1\}^n$.
- For a quantum output, $\mathcal{S}$ simply sends it to $\mathcal{C}$, then $\mathcal{C}$ decrypts each qubit using the phase gate P. Specifically, for each qubit i, $\mathcal{C}$ performs the phase gate P with $2(b_i \oplus c_i) + c_i$ times.

Correctness of the protocol. – We first show the correctness of the Hadamard gate, then the correctness of the protocol almost follows.

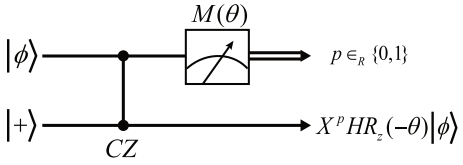

Fig. 3: A basic module in the MBQC model, where $R_z(\theta)$ denotes the z-rotation operator, $p \in_R \{0,1\}$ is the uniform measurement outcome. The correctness of this circuit can be directly verified, also see [19].

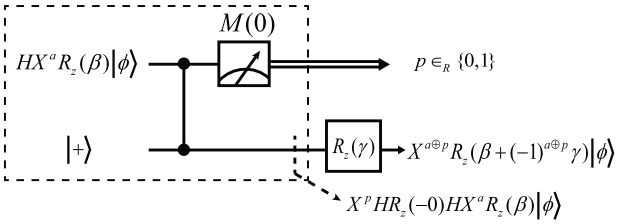

Fig. 4: The equivalent form for the part of circuit in fig. 2.

Correctness of the Hadamard gate. Our proof begins from a simple circuit as shown in fig. 3, which is a basic module in the MBQC model [19]. We will use this module to verify the correctness of the H-gadget in our protocol.

In this section, we temporarily drop the subscript i and define $R_z(\beta) = Z^b P^c$, $R_z(\gamma) = Z^d P^e$, and $R_z(\omega) = Z^f P^g$. That is, $\beta = (b + \frac{c}{2})\pi$, $\gamma = (d + \frac{e}{2})\pi$, and $\omega = (f + \frac{g}{2})\pi$. We first consider a part of this gadget, which is surrounded by red dashed lines in fig. 2. This part of circuit can be reorganized as follows. First, the H gate which is applied on the state $X^a R_z(\beta)|\phi\rangle$ now is absorbed into this qubit. Then, the ancillary qubit $R_z(\gamma)|+\rangle$ is viewed as a qubit $|+\rangle$ followed by a $R_z(\gamma)$, where we can put this $R_z(\gamma)$ behind the CZ. Finally, since local quantum operations on different qubits naturally commute with each other, therefore we can always think that the operator $R_z(\gamma)$ is deferred until the measurement $M(0)$ has been performed. We depict the reorganized circuit in fig. 4. From the picture, we can immediately see that the circuit in the black dashed box is exactly the same circuit described in fig. 3 except that the input state now is $HX^a R_z(\beta)|\phi\rangle$ and $\theta = 0$. Therefore, after the measurement the ancillary qubit will immediately collapse into $X^p H R_z(-0) H X^a R_z(\beta)|\phi\rangle = X^{a\oplus p} R_z(\beta)|\phi\rangle$. Finally, we apply the deferred $R_z(\gamma)$ on this state, obtaining that

$$R_z(\gamma) X^{a\oplus p} R_z(\beta)|\phi\rangle = X^{a\oplus p} R_z(\beta + (-1)^{a\oplus p}\gamma)|\phi\rangle, \quad (9)$$

where we use the following two simple equations:

$$\begin{cases} X^r R_z(\theta) X^r = R_z((-1)^r \theta), & r \in \{0,1\}, \\ R_z(\alpha) R_z(\beta) = R_z(\alpha + \beta), & \alpha, \beta \in [0, 2\pi). \end{cases} \quad (10)$$

A similar analysis can be applied into the rest part of this circuit. Here, we directly write down the output state

$$R_z(\omega)X^qHR_z(-\theta)X^{a\oplus p}R_z(\beta+(-1)^{a\oplus p}\gamma)\left|\phi\right\rangle = X^qR_z((-1)^q\omega+(a\oplus p)\pi)HR_z(\beta+(-1)^{a\oplus p}(\gamma-\theta))\left|\phi\right\rangle. \tag{11}$$

Let $\theta=(-1)^{a\oplus p}\beta+\gamma+h\pi$. Note that θ here is seemingly not the same as the one defined in fig. 2. Despite that, we will show they are exactly the same one. Substitute θ in the above equation, we can easily get the following result:

$$X^qR_z((-1)^q\omega+(a\oplus p)\pi)HR_z((-1)^{a\oplus p\oplus 1}h\pi)\left|\phi\right\rangle. \tag{12}$$

Since R_z is an operator with a period of 2π, which means $R_z(\pi)=R_z(-\pi)=Z$, thus the former result can be rewritten as follows:

$$X^qR_z((-1)^q\omega+(a\oplus p)\pi)HZ^h\left|\phi\right\rangle = X^{q\oplus h}R_z((-1)^{q\oplus h}\omega+(a\oplus p)\pi)H\left|\phi\right\rangle. \tag{13}$$

Substitute $\omega=f\pi+\frac{g}{2}\pi$ back in the above equation, for simplicity we omit the operators $X^{q\oplus h}, R_z, H$ and the state $\left|\phi\right\rangle$, then we can get that

$$\begin{aligned}
&(-1)^{q\oplus h}\left(f\pi+\frac{g}{2}\right)+(a\oplus p)\pi = \\
&(a\oplus p\oplus f)\pi+(-1)^{q\oplus h}\frac{g}{2}\pi \\
&=(a\oplus p\oplus f)\pi+2g(q\oplus h)\pi+(-1)^{q\oplus h}\frac{g}{2}\pi \\
&=(a\oplus p\oplus f)\pi+g(q\oplus h)\pi+\frac{2(q\oplus h)+(-1)^{q\oplus h}}{2}g\pi \\
&=a\oplus p\oplus f\oplus g(q\oplus h)\pi+\frac{g\pi}{2} \\
&\equiv X^{q\oplus h}Z^{a\oplus p\oplus f\oplus g(q\oplus h)}P^gH\left|\phi\right\rangle,
\end{aligned} \tag{14}$$

where we use a simple equality: for any $r\in\{0,1\}$, $2r+(-1)^r=1$. Similarly, substitute $\beta=b\pi+\frac{c}{2}\pi$ and $\gamma=d\pi+\frac{e}{2}\pi$ to θ, we can see that

$$\begin{aligned}
\theta &= (-1)^{a\oplus p}\left(b\pi+\frac{c}{2}\pi\right)+\left(d\pi+\frac{e}{2}\pi\right)+h\pi \\
&= b\pi+(-1)^{a\oplus p}\frac{c}{2}\pi+d\pi+\frac{e}{2}\pi+h\pi \\
&= b\pi+c(a\oplus p)\pi+\frac{c}{2}\pi+d\pi+\frac{e}{2}\pi+h\pi \\
&= h\oplus b\oplus d\oplus(ac)\oplus(pc)\pi+\frac{c+e}{2}\pi \\
&= h\oplus b\oplus d\oplus(ac)\oplus(pc)\oplus(ce)\pi+\frac{c\oplus e}{2}\pi,
\end{aligned} \tag{15}$$

where in the last term we use another simple equality: for any $c,e\in\{0,1\}$, $c+e=2ce+c\oplus e$. From the above results, the correctness of the Hadamard gate is obvious.

Correctness of the protocol. According to the aforementioned argument, we know that if the protocol is performed honestly, then the output state after Step 2 will be $X^aZ^bP^c\left|out\right\rangle$, where $\left|out\right\rangle=U\left|in\right\rangle$ denotes the correct output state of the computation and X^a, Z^b, P^c are the n-fold encryption operators on the output state defined as $X^a=X_1^{a_1}\dots X_n^{a_n}, Z^b=Z_1^{b_1}\dots Z_n^{b_n}, P^c=P_1^{c_1}\dots P_n^{c_n}$. Generally, the output state $\left|out\right\rangle$ is an n-qubit superposition state, that is

$$\left|out\right\rangle=\sum_{y\in\{0,1\}^n}c_y\left|y\right\rangle. \tag{16}$$

Note that we have expressed the output state in Z basis, since we only consider the input is encoded in X basis. Indeed, for security reasons, the output state can be only measured in Z basis, otherwise there will be information leakages about encryption keys. It is not hard to verify that for any $y_i,a_i,b_i,c_i\in\{0,1\}$, $X_i^{a_i}Z_i^{b_i}P_i^{c_i}\left|y_i\right\rangle=e^{j(b_i+\frac{c_i}{2})y_i\pi}\left|y_i\oplus a_i\right\rangle$, thus substituting this result to $X^aZ^bP^c\left|out\right\rangle$, we finally get that

$$X^aZ^bP^c\left|out\right\rangle=\sum_{y\in\{0,1\}^n}e^{j(b+\frac{c}{2})y\pi}c_y\left|y\oplus a\right\rangle, \tag{17}$$

where $\left|y\oplus a\right\rangle=\left|y_1\oplus a_1,y_2\oplus a_2,...,y_n\oplus a_n\right\rangle$ and $(b+\frac{c}{2})y$ denotes $\sum_{i=1}^n(b_i+c_i/2)y_i$. It follows from eqs. (16) and (17) that

$$\Pr[y\left|Z\right\rangle,\left|out\right\rangle]=\Pr[y\oplus a\left|Z\right\rangle,X^aZ^bP^c\left|out\right\rangle], \tag{18}$$

where $\Pr[y\left|Z\right\rangle,\left|\phi\right\rangle]$ denotes the probability of obtaining y when measuring $\left|\phi\right\rangle$ in Z basis. Thus, in order to obtain the correct distribution of the computation outcomes, the client needs to compute $y=s\oplus a$, where $s,a\in\{0,1\}^n$ and s is the measurement outcome. Finally, for a quantum output $Z^bP^c\left|out\right\rangle$, the client can decrypt it by the operator $Z^bP^{c\dagger}$. Note that $Z^bP^{c\dagger}=Z^bP^{3c}=Z^bZ^cP^c=Z^{b\oplus c}P^c=P^{2(b\oplus c)+c}$, thus for each qubit i the client only needs to perform the phase gate P with $2(b_i\oplus c_i)+c_i$ times. To sum up the above arguments, we complete the proof of the correctness of our protocol.

Security of the protocol. – We show that our protocol can guarantee the privacy of the input and output of the computation. For the input, this conclusion is obvious. Thus, to complete the proof, we need to prove that the output state of the computation is also encrypted by a *sound* quantum one-time pad. In other words, there is no information leakage about the encryption keys during the computation.

Let us first consider an extreme case: the quantum circuit U delegated to the server contains no H gates. In this case, the client can achieve a non-interactive delegated quantum computation. Client and server do not need to exchange classical informations during the computation. Thus, there is completely no information leakage about the encryption keys as long as the initial keys are

secure. Based on this observation, we infer that to prove the privacy we only need to analyze the part that implements the H gates. From fig. 2, we can see that given the qubits $X_i^{a_i} Z_i^{b_i} P_i^{c_i} |\phi\rangle$, $Z^{d_i} P^{e_i} |+\rangle$, and $Z^{f_i} P^{g_i} |+\rangle$, all classical information accessible to the server are two measurement outcomes $p_i, q_i \in \{0,1\}$ and a measurement angle $\theta_i \in \{0, \pi/2, \pi, 3\pi/2\}$. Clearly, the measurement outcomes p_i, q_i are uniformly random, thus we only need to consider the measurement angle θ_i.

Now denote θ_i by $u_i\pi + \frac{v_i\pi}{2}$, where $u_i, v_i \in \{0,1\}$, then according to eq. (15) we know that u_i and v_i can be expressed as follows:

$$u_i = h_i \oplus b_i \oplus d_i \oplus (a_i c_i) \oplus (p_i c_i) \oplus (c_i e_i), \quad (19a)$$

$$v_i = c_i \oplus e_i, \quad (19b)$$

where both u_i and v_i are known to the server. Intuitively, given u_i and v_i the server cannot determine the correct values of $a_i, b_i, c_i, d_i, e_i, h_i$, since there are 6 variables in two equations. However, the server may gain some information according to u_i and v_i. Suppose, for example, $v_i = 1$, then the server can determine that $c_i e_i = 0$. Substitute this to eq. (19a), the server can obtain a simplified equality $u_i = h_i \oplus b_i \oplus d_i \oplus (a_i \oplus p_i)c_i$. Despite this fact, we can show that there is no information leakage about all variables from a_i to h_i. That is, we prove the following equality holds true:

$$\Pr[r_i \,|\, u_i, v_i] = \Pr[r_i] = \frac{1}{2}, \quad (20)$$

where the random variable $r_i \in \{a_i, b_i, c_i, d_i, e_i, f_i, g_i, h_i\}$. To see that, we need to know the following simple facts.

First, if $x, y \in \{0,1\}$ and x is uniform, then $x \oplus y \in_R \{0,1\}$. Second, if $x, y \in_R \{0,1\}$ and we define $z = x \oplus y$, then $\Pr[x \,|\, z] = \Pr[x] = 1/2$. Finally, if $x, y_1, y_2 \in \{0,1\}$ and x is uniform, let $z = x \oplus (y_1 y_2)$, then $\Pr[y_1 \,|\, z] = \Pr[y_1]$. These three basic facts can be easily verified. With these facts, we can complete our proof. Define $\xi_i = b_i \oplus d_i \oplus (a_i c_i) \oplus (p_i c_i) \oplus (c_i e_i)$ so that $u_i = h_i \oplus \xi_i$. Since $b_i, d_i \in_R \{0,1\}$, we first know that $\xi_i \in_R \{0,1\}$. Furthermore, since $h_i, \xi_i \in_R \{0,1\}$, we can get that $\Pr[h_i \,|\, u_i] = \Pr[h_i] = 1/2$. Likewise, we can also get $\Pr[b_i \,|\, u_i] = \Pr[b_i] = 1/2$ and $\Pr[d_i \,|\, u_i] = \Pr[d_i] = 1/2$. For $a_i \in_R \{0,1\}$, define $\xi_i = h_i \oplus b_i \oplus d_i \oplus (p_i c_i) \oplus (c_i e_i)$ so that $u_i = \xi_i \oplus (a_i c_i)$, from which we infer that $\Pr[a_i \,|\, u_i] = \Pr[a_i] = 1/2$. Note that h_i, b_i, d_i and a_i are irrelevant to v_i, which means $\Pr[r_i \,|\, u_i, v_i] = \Pr[r_i \,|\, u_i]$ for any $r_i \in \{h_i, b_i, d_i, a_i\}$. As for $c_i, e_i \in_R \{0,1\}$, since they are related to both u_i and v_i, in order to simplify our analysis, we define $h_i' = h_i \oplus (a_i c_i)$, $b_i' = b_i \oplus (p_i c_i)$, and $d_i' = d_i \oplus (c_i e_i)$, then obtain that $u_i = h_i' \oplus b_i' \oplus d_i'$. Clearly, $h_i', b_i', d_i' \in_R \{0,1\}$, so c_i and e_i are only related to v_i. By this way, we can easily get that $\Pr[c_i \,|\, u_i, v_i] = \Pr[c_i \,|\, v_i] = \Pr[c_i] = 1/2$ and $\Pr[e_i \,|\, u_i, v_i] = \Pr[e_i \,|\, v_i] = \Pr[e_i] = 1/2$. Finally, f_i and $g_i \in_R \{0,1\}$ are obviously irrelevant to u_i and v_i (see eqs. (19a) and (19b)), which means $\Pr[f_i \,|\, u_i, v_i] = \Pr[f_i] = 1/2$ and $\Pr[g_i \,|\, u_i, v_i] = \Pr[g_i] = 1/2$. So far, we have proved the statement in eq. (20), from which we know that the server can learn nothing about $a_i, b_i, c_i, d_i, e_i, f_i, g_i, h_i$ from the θ_i. Thus, from the perspective of the server, the output state of the computation is still encrypted by a sound quantum one-time pad.

Discussions. – We have proposed a secure delegated quantum computation protocol which can guarantee the unconditional security of the input and output. Indeed, it is easy to compile our protocol into a blind protocol, where the *blind* means the server can learn nothing about the computation except the upper bound of the size of the quantum circuit [5]. According to the quantum computation theory [26], there exists a universal quantum circuit $\mathcal{U}$ such that

$$\mathcal{U} |C(U)\rangle |in\rangle = |C(U)\rangle U |in\rangle, \quad (21)$$

where the input of the circuit $\mathcal{U}$ consists of two parts: $|in\rangle$ is the input of the circuit U while $C(U)$ is the canonical and classical description of the circuit U. Performing this universal circuit $\mathcal{U}$ in our protocol, we can apparently achieve a blind quantum computation, see [16] for a detailed discussion.

We should mention that in the case of a quantum output, the output state is not encrypted by a standard quantum one-time pad, since the server has decrypted the encryption operator X^a. Nevertheless, it is not hard to verify that, for any n-qubit state ρ,

$$\sum_{b,c \in \{0,1\}^n} \frac{Z^b P^c \rho P^{\dagger c} Z^b}{4^n} = \mathrm{diag}(\rho_{1,1}, \rho_{2,2}, \ldots, \rho_{2^n,2^n}) \triangleq \tilde{\rho}, \quad (22)$$

where $\mathrm{diag}(\rho_{1,1}, \rho_{2,2}, ..., \rho_{2^n,2^n})$ denotes the diagonal matrix whose diagonal elements are $\rho_{1,1}, \rho_{2,2}, ..., \rho_{2^n,2^n}$, and $\rho_{i,i}$ denotes the element of the i-th row and the i-th column of ρ. Clearly, the server generally cannot infer the correct ρ from $\tilde{\rho}$, since the encryption eliminates all non-diagonal elements of ρ. Indeed, the server even cannot determine the exact state of $\tilde{\rho}$, since the input of the computation is unknown to it. To determine the $\tilde{\rho}$, the server needs to perform a quantum state tomography procedure, which is obviously impossible since the server cannot prepare a large number of identical duplicates for $\tilde{\rho}$. However, if ρ happens to be a diagonal matrix, then $\tilde{\rho} = \rho$. In this case, we can see that $\rho = |y\rangle \langle y|$, where $y \in \{0,1\}^n$. There is an easy way to avoid this problem, we just need to encode the output state in X basis.

Besides that, it should also be mentioned that the present protocol can only work well in a noise-free environment. However, in practice, there are two kinds of errors which are worthy of attention. One is caused by the channel noise, the other generates from the server's operation including basic gates and measurement. Fortunately, in our protocol those two errors can be, in principle,

corrected using the technique of quantum error-correct code (QECC). As for the channel noise, since the clients only need to sent single qubits, they can protect each qubit using a QECC, *e.g.*, *the surface code* [27]. As for the computation error caused by the server, since the server is a general quantum computer, we can always assume that the server performs a *fault-tolerant quantum computation* [28], which includes the fault-tolerant basic gates and the fault-tolerant measurement.

Finally, in this work we only consider an honest server who performs the protocol as the client desires. However, a real server may not follow the protocol honestly. To detect such a malicious server, generally we need to introduce a verification mechanics in the protocol. Indeed, this is an important topic in the delegated quantum computation theory, see [29,30]. There is an easy way to achieve the verification in our protocol using the universal quantum circuit $\mathcal{U}$, for example see [31].

* * *

This work is supported by the National Natural Science Foundation of China (Grant Nos. 62001351, 61372076, 61971348); Natural Science Basic Research Program of Shaanxi, China (Grant No. 2021JM-142); Foundation of Shaanxi Key Laboratory of Information Communication Network and Security (ICNS201802); Key Research and Development Program of Shaanxi Province (2019ZDLGY09-02).

Data availability statement: No new data were created or analysed in this study.

REFERENCES

[1] Knill Emanuel, Laflamme Raymond and Milburn Gerald J., *Nature*, **409** (2001) 46.
[2] Long Gui Lu, *Int. J. Theor. Phys.*, **50** (2011) 1305.
[3] Long Gui Lu and Xiao L., *Phys. Rev. A*, **69** (2004) 052303.
[4] Childs Andrew M., *Quantum Inf. Comput.*, **5** (2005) 456.
[5] Broadbent Anne, Fitzsimons Joseph and Kashefi Elham, *Universal blind quantum computation,* in *Proceedings of the 50th Annual Symposium on Foundations of Computer Science (FOCS 2009)* (IEEE) 2009, pp. 517–527.
[6] Sueki Takahiro, Koshiba Takeshi and Morimae Tomoyuki, *Phys. Rev. A*, **87** (2013) 060301.
[7] Broadbent Anne, *Can. J. Phys.*, **93** (2015) 941.
[8] Hayashi Masahito and Morimae Tomoyuki, *Phys. Rev. Lett.*, **115** (2015) 220502.
[9] Li Q., Li Z., Chan W. H., Zhang S. and Liu C., *Phys. Lett. A*, **382** (2018) 938.
[10] Sheng Yu Bo and Zhou L., *Phys. Rev. A*, **98** (2018) 052343.
[11] Xu Qingshan, Tan Xiaoqing, Huang Rui and Zeng Xiaodan, *Quantum Eng.*, **2** (2020) e51.
[12] Li Q., Liu C., Peng Y., Yu F. and Zhang C., *Opt. Laser Technol.*, **142** (2021) 107190.
[13] Gentry Craig, *Fully homomorphic encryption using ideal lattices,* in *Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing* (Association for Computing Machinery) 2009, pp. 169–178.
[14] Fisher Kent A. G., Broadbent Anne, Shalm L. K., Yan Z., Lavoie Jonathan, Prevedel Robert, Jennewein Thomas and Resch Kevin J., *Nat. Commun.*, **5** (2014) 1.
[15] Broadbent Anne and Jeffery Stacey, *Quantum homomorphic encryption for circuits of low t-gate complexity,* in *Annual Cryptology Conference* (Springer) 2015, pp. 609–629.
[16] Aharonov Dorit, Ben-Or Michael, Eban Elad and Mahadev Urmila, *Interactive proofs for quantum computations*, arXiv preprint, arXiv:1704.04487 (2017).
[17] Tan Xiaoqing and Zhou Xu, *Ann. Telecommun.*, **72** (2017) 589.
[18] Sano Yuichi, *J. Phys. Soc. Jpn.*, **90** (2021) 124001.
[19] Jozsa Richard, *An introduction to measurement based quantum computation, NATO Science Series, III: Computer and Systems Sciences, Quantum Information Processing-From Theory to Experiment*, Vol. **199**, 2006, pp. 137–158 (arXiv:quant-ph/0508124).
[20] Raussendorf Robert and Briegel Hans J., *Phys. Rev. Lett.*, **86** (2001) 5188.
[21] McKague Matthew, *Theory Comput.*, **12** (2016) 1.
[22] Zhang Xiaoqian, Luo Weiqi, Zeng Guoqiang, Weng Jian, Yang Yaxi, Chen Minrong Minrong and Tan Xiaoqing, *Inf. Sci.*, **498** (2019) 135.
[23] Xu Qingshan, Tan Xiaoqing, Huang Rui and Li Meiqi, *Phys. Rev. A*, **104** (2021) 042412.
[24] Barz Stefanie, Kashefi Elham, Broadbent Anne, Fitzsimons Joseph F., Zeilinger Anton and Walther Philip, *Science*, **335** (2012) 303.
[25] Ambainis A., Mosca M., Tapp A. and De Wolf R., *Private quantum channels,* in *Proceedings 41st Annual Symposium on Foundations of Computer Science* (IEEE) 2000, pp. 547–553.
[26] Bernstein Ethan and Vazirani Umesh, *SIAM J. Comput.*, **26** (1997) 1411.
[27] Fowler Austin G., Mariantoni Matteo, Martinis John M. and Cleland Andrew N., *Phys. Rev. A*, **86** (2012) 032324.
[28] Gottesman Daniel, *Phys. Rev. A*, **57** (1998) 127.
[29] Fitzsimons Joseph F., *Npj Quantum Inf.* **3** (2017) 23.
[30] Gheorghiu Alexandru, Kapourniotis Theodoros and Kashefi Elham, *Theory Comput. Syst.*, **63** (2019) 715.
[31] Ma Shuquan, Zhu Changhua, Nie Min and Quan Dongxiao, *Chin. Phys. B*, **30** (2021) 040305.