Vol.2021-QS-2 No.16
2021/3/29

古典Quantum randomized encodingの不可能性

森前　智行[1,a)]

概要：Randomized encoding is a powerful cryptographic primitive with various applications such as secure multiparty computation, verifiable computation, parallel cryptography, and complexity lowerbounds. Intuitively, randomized encoding $\hat{f}$ of a function f is another function such that $f(x)$ can be recovered from $\hat{f}(x)$, and nothing except for $f(x)$ is leaked from $\hat{f}(x)$. Its quantum version, quantum randomized encoding, has been introduced recently [Brakerski and Yuen, arXiv:2006.01085]. Intuitively, quantum randomized encoding $\hat{F}$ of a quantum operation F is another quantum operation such that, for any quantum state ρ, $F(\rho)$ can be recovered from $\hat{F}(\rho)$, and nothing except for $F(\rho)$ is leaked from $\hat{F}(\rho)$. In this paper, we show that if quantum randomized encoding of BB84 state generations is possible with an encoding operation E, then a two-round verification of quantum computing is possible with a classical verifier who can additionally do the operation E. One of the most important goals in the field of the verification of quantum computing is to construct a verification protocol with a verifier as classical as possible. This result therefore demonstrates a potential application of quantum randomized encoding to the verification of quantum computing: if we can find a good quantum randomized encoding (in terms of the encoding complexity), then we can construct a good verification protocol of quantum computing. We, however, also show that too good quantum randomized encoding is impossible: if quantum randomized encoding with a classical encoding operation is possible, then the no-cloning is violated. We finally consider a natural modification of blind quantum computing protocols in such a way that the server gets the output like quantum randomized encoding. We show that the modified protocol is not secure.

Impossibility of classical quantum randomized encoding

1. Introduction

Randomized encoding [1], [2] is a powerful cryptographic primitive with various applications, such as secure multiparty computation, verifiable computation, parallel cryptography, and complexity lowerbounds. Intuitively, randomized encoding $\hat{f}$ of a function f is another function such that $f(x)$ can be recovered from $\hat{f}(x)$, and nothing except for $f(x)$ is leaked from $\hat{f}(x)$. More precisely, it is defined as follows.

Definition 1 (Randomized encoding [1]) Let $f : X \to Y$ be a function. We say that a function $\hat{f} : X \times R \to Z$ is a δ-correct and (t, ϵ)-private randomized encoding of f if there exist randomized algorithms, Dec (the decoder) and Sim (the simulator), with the following properties.

- (δ-correctness) For any input $x \in X$,

  $$\Pr_{r \leftarrow R}[\mathrm{Dec}(\hat{f}(x; r)) \neq f(x)] \leq \delta,$$

  where $r \leftarrow R$ means that r is sampled uniformly at random from R.
- ((t, ϵ)-privacy) For any $x \in X$ and any circuit A of size t,

  $$\left| \Pr\left[A(\mathrm{Sim}(f(x))) = 1\right] - \Pr_{r \leftarrow R}\left[A(\hat{f}(x; r)) = 1\right] \right| \leq \epsilon,$$

  where the first probability is over the randomness of the simulator Sim.

Intuitively, the correctness means that the value $f(x)$ is correctly decoded from $\hat{f}(x; r)$ for many r, and the privacy means that no information except for $f(x)$ is leaked from $\hat{f}(x; r)$: the distribution $\{\hat{f}(x; r)\}_{r \leftarrow R}$ can be approximately simulated by the simulator algorithm Sim

[1] 京都大学基礎物理学研究所
[a)] tomoyuki.morimae@yukawa.kyoto-u.ac.jp

that gets only $f(x)$ as the input.

The quantum version of randomized encoding, namely, quantum randomized encoding, has been introduced recently [3]. It is defined as follows.

Definition 2 (Quantum randomized encoding [3]) Let F be a quantum operation. We say that a quantum operation $\hat{F}$ is a δ-correct and ϵ-private quantum randomized encoding of F if there exist quantum operations, Dec (the decoder) and Sim (the simulator), with the following properties.

- (δ-correctness) For any quantum state $\rho_{AB} \in H_A \otimes H_B$,
$$\frac{1}{2}\left\|\mathrm{Dec}_A(\hat{F}_A(\rho_{AB})) - F_A(\rho_{AB})\right\|_1 \leq \delta,$$
where H_A and H_B are Hilbert spaces, and the subscript A of an operation means that the operation acts only on H_A.
- (ϵ-privacy) For any quantum state $\rho \in H_A \otimes H_B$,
$$\hat{F}_A(\rho_{AB}) \approx_\epsilon \mathrm{Sim}_A(F_A(\rho_{AB})).$$
Here, $\approx_\epsilon$ means that the two states are ϵ-indistinguishable. Depending on the security requirement, the indistinguishability can be the statistical one, i.e.,
$$\frac{1}{2}\left\|\hat{F}_A(\rho_{AB}) - \mathrm{Sim}_A(F_A(\rho_{AB}))\right\|_1 \leq \epsilon,$$
or the computational one (i.e., no computationally bounded adversary can distinguish the two states with the advantage larger than ϵ.)

This is a quantum analogy of the definition, Definition 1, of classical randomized encoding. Intuitively, the correctness means that the state $F_A(\rho_{AB})$ is correctly recovered from the state $\hat{F}_A(\rho_{AB})$, and the privacy means that nothing except for $F_A(\rho_{AB})$ is leaked from $\hat{F}_A(\rho_{AB})$: the state $\hat{F}_A(\rho_{AB})$ is approximately generated by the simulator Sim that gets only $F_A(\rho_{AB})$ as the input. The reason why operations acting only on H_A is considered for bipartite states $\rho_{AB} \in H_A \otimes H_B$ is that the decoder and simulator should keep entanglement between the main system (H_A) and the ancillary system (H_B). In this paper, we consider the following restricted version of quantum randomized encoding, Definition 3, because it is simpler but enough for our purpose. (What we show in this paper are statements something like "if quantum randomized encoding is possible, then something happens". It is clear that if quantum randomized encoding of Definition 2 is possible, then quantum randomized encoding of Definition 3 is also possible, and therefore using Definition 3 is enough for our purpose.)

Definition 3 ((Restricted) quantum randomized encoding) Let S be a set of states. Let F be a quantum operation. We say that a quantum operation $\hat{F}$ is a δ-correct and ϵ-private quantum randomized encoding of F for S if there exist quantum operations, Dec (the decoder) and Sim (the simulator), with the following properties.

- (δ-correctness) For any quantum state $\rho \in S$,
$$\frac{1}{2}\left\|\mathrm{Dec}(\hat{F}(\rho)) - F(\rho)\right\|_1 \leq \delta.$$
- (ϵ-privacy) For any quantum state $\rho \in S$,
$$\hat{F}(\rho) \approx_\epsilon \mathrm{Sim}(F(\rho)).$$
Here, again, depending on the security requirement, the ϵ-indistinguishability, $\approx_\epsilon$, can be the statistical one, i.e.,
$$\frac{1}{2}\left\|\hat{F}(\rho) - \mathrm{Sim}(F(\rho))\right\|_1 \leq \epsilon,$$
or the computational one.

This restrictive definition, Definition 3, have two differences from Definition 2. First, Definition 3 does not care about entanglement between the main system and the ancillary system: the decoder and simulator do not need to keep entanglement between the main system and the ancillary system. Second, Definition 3 is restricted to a set S of states: in Definition 3, the correctness and the privacy are required to be satisfied only for states in S, while Definition 2 requires the correctness and the privacy for any state. It is clear that if quantum randomized encoding is possible in the sense of Definition 2, it is also possible in the sense of Definition 3. Hereafter, we consider only quantum randomized encoding in the sense of Definition 3.

Ref. [3] constructed a concrete quantum randomized encoding scheme from a classical randomized encoding by using the gate-teleportation technique. Although the research of classical randomized encoding has a long history and there are plenty of results, the research of quantum randomized encoding has just started, and we do not know anything about it. In particular, we do not know any useful application of quantum randomized encoding [21].

1.1 First result: application to verification of quantum computing

One of the most important applications of (classical) randomized encoding is the delegation of computing. If

computing $\hat{f}(x;r)$ is much easier than computing $f(x)$, a computationally weak client can delegate her computing to a powerful server by sending $\hat{f}(x;r)$ to the server and asking the server to decode it to get $\mathrm{Dec}(\hat{f}(x;r)) = f(x)$. This delegation protocol can also be made verifiable, i.e., the client can check the integrity of the server, by using a message authentication code (MAC) [4]: the client sends the server a randomized encoding of $\mathrm{MAC}_k(f(x))$ and x, where MAC is a message authentication code and k is a key. The server returns the decoded value and $y = f(x)$ to the client.

For the quantum case, on the other hand, no relation is known between quantum randomized encoding and verification of quantum computing [21]. Our first result is to demonstrate a possible application of quantum randomized encoding to the verification of quantum computing. We show that if quantum randomized encoding is possible for BB84 state generations with an encoding operation E, then a two-round verification of quantum computing is possible for a classical verifier who can additionally do the operation E. One of the most important goals in the field of the verification of quantum computing is to construct a verification protocol with a verifier as classical as possible. Our first result suggests that if a good quantum randomized encoding is possible (in terms of the encoding complexity), then we can construct a good verification protocol of quantum computing.

The verification of quantum computing [5], [6] is defined as follows.

Definition 4 (Verification of quantum computing) An interactive protocol between a verifier and a prover is called a verification of quantum computing if for any promise problem $A = (A_{yes}, A_{no}) \in \mathrm{BQP}$ both of the following are satisfied with some c and s such that $c - s \geq \frac{1}{poly(|x|)}$:

- If $x \in A_{yes}$, there exists a quantum polynomial-time prover's strategy such that the verifier accepts with probability at least c.
- If $x \in A_{no}$, the verifier accepts with probability at most s for any (even computationally-unbounded) prover's strategy.

It is known that if the verifier is "almost classical" (i.e., the verifier can only generate or measure single-qubit states), a verification of quantum computing is possible [7], [8]. It is an open problem whether a verification of quantum computing is possible for a completely classical verifier. (A verification of quantum computing is possible for a completely classical verifier if more than two provers who are entangled but non-communicating are available [9], [10], [11], [12], [13], or if the soundness is relaxed to be the computational one [14].)

Our first result is stated as follows. (Its proof is given in Sec. 3.)

Theorem 1 Let F be a quantum operation and $\sigma_{h,m}$ be a quantum state such that

$$F(\sigma_{h,m}) = \Big(\bigotimes_{j=1}^{N} H^h |m_j\rangle\langle m_j| H^h \Big) \otimes \eta_{junk}$$

for all $h \in \{0,1\}$ and all $m = (m_1, ..., m_N) \in \{0,1\}^N$, where H is the Hadamard gate, η_{junk} is any state that is independent of (h,m), and F does not depend on (h,m). Assume that δ-correct statistical-ϵ-private (restricted) quantum randomized encoding $\hat{F}$ of F for $\{\sigma_{h,m}\}_{(h,m)\in\{0,1\}\times\{0,1\}^N}$ exists with negligible δ and ϵ (i.e., $\lim_{N\to\infty} \delta(N)p(N) = 0$ and $\lim_{N\to\infty} \epsilon(N)p(N) = 0$ for every polynomial p). Furthermore, assume that the decoder, Dec, can be implemented in quantum polynomial-time (in terms of the number of qubits of $\hat{F}(\sigma_{h,m})$). Let E be an operation that is required to generate $\hat{F}(\sigma_{h,m})$ for any $(h,m) \in \{0,1\} \times \{0,1\}^N$. Then, a two-round verification of quantum computing is possible with a classical verifier who can additionally do the operation E.

There are many examples of such F and $\{\sigma_{h,m}\}_{h,m}$. For example, F is the application of $H^{\otimes N}$, i.e., $F(\rho) = H^{\otimes N} \rho H^{\otimes N}$ for any N-qubit state ρ, and

$$\sigma_{h,m} = \bigotimes_{j=1}^{N} H^{h+1} |m_j\rangle\langle m_j| H^{h+1}.$$

In Theorem 1, we require that F should be independent of (h,m). The reason is that in the definition of quantum randomized encoding the decoder, Dec, and the simulator, Sim, are technically allowed to depend on F. If Sim depends on F, it can depend on (h,m) as well, and in that case, the soundness of our two-round verification protocol no longer holds (see the proof in Sec. 3). A formalism that allows Dec and Sim to depend only partially on F is also introduced in Ref. [3].

An interesting point in the proof of Theorem 1 is that the privacy (of quantum randomized encoding) is transformed to the soundness (of the verification of quantum computing). The privacy of quantum randomized encoding requires that the receiver cannot learn anything except for $F(\sigma_{h,m})$, which means that what the receiver has is

$\mathrm{Sim}(F(\sigma_{h,m}))$, but it also leads to the fact that the server "possessed" $F(\sigma_{h,m})$. The soundness of the verification protocol of Ref. [15] that we use for the proof is kept if it is guaranteed that the prover received $F(\sigma_{h,m})$. This argument can be considered as a quantum version of "from secrecy to soundness" [4]. (For details, see the proof in Sec. 3. In the beginning of Sec. 3, we also provide an explanation of an intuitive idea of the proof.)

The best verification protocol of quantum computing (in terms of the complexity of verifier's quantum operation) is Protocol 3 given in Fig. 3 where the verifier has only to generate a state

$$\bigotimes_{j=1}^{N} H^h |m_j\rangle\langle m_j| H^h \tag{1}$$

with uniformly random (h, m). (Remember that we are interested in the information-theoretical soundness. For the computationally sound case, the classical verifier can verify quantum computing [14].) Theorem 1 suggests that if (restricted) quantum randomized encoding of the generation of Eq. (1) can be constructed with an encoding operation E that is much easier than the generation of Eq. (1), it provides a new two-round verification protocol that updates the best protocol, Protocol 3.

If the operation E that is required to generate $\hat{F}(\sigma_{h,m})$ is a classical operation, i.e., if $\hat{F}(\sigma_{h,m})$ is a mixture of computational-basis states,

$$\hat{F}(\sigma_{h,m}) = \sum_z p_z |z\rangle\langle z|,$$

where $|z\rangle$ is a computational-basis state and $\{p_z\}_z$ is a probability distribution, Theorem 1 means that a two-round verification of quantum computing is possible with a completely classical verifier, which solves the long-standing open problem. However, it means BQP $\subseteq$ IP[2]. We thus obtain the following corollary.

Corollary 1 Let F and $\sigma_{h,m}$ be the quantum operation and quantum state defined in Theorem 1, respectively. Then δ-correct statistical-ϵ-private classical quantum randomized encoding of F for $\{\sigma_{h,m}\}_{h,m}$ with negligible δ and ϵ is impossible unless BQP $\subseteq$ IP[2].

To construct the verification protocol from quantum randomized encoding, we use the verification protocol of Ref. [15]. (See the proof in Sec. 3. The verification protocol of Ref. [15] is also reviewed in Sec. 2.) Another well-studied verification protocol is the Fitzsimons-Kashefi (FK) protocol [7]. It would be possible to use FK protocol instead of the protocol of Ref. [15] to derive a similar result. However, in that case, what we get is a polynomial-round verification protocol, because the FK protocol requires a polynomially many classical communications between the prover and the verifier. Then, its corollary is that if classical quantum randomized encoding is possible then BQP is in IP[*poly*], which is already known to be true (BQP is in PSPACE and PSPACE = IP[*poly*]), and therefore it does not prohibit classical quantum randomized encoding.

In this paper, we consider only the statistical privacy. If we consider the computational one, we would obtain a two-round verification protocol with the computational soundness (i.e., an interactive argument).

1.2 Second result: impossibility of classical quantum randomized encoding

Because BQP $\subseteq$ IP[2] is not believed to happen, Corollary 1 suggests the impossibility of classical quantum randomized encoding. We can actually show a stronger result: if classical quantum randomized encoding is possible, then the no-cloning is violated. It is our second result, and it is stated as the following theorem. (Its proof is given in Sec. 4.)

Theorem 2 Let $\{|\psi_i\rangle\}_{i=1}^r$ be a set of pure states. Let F be a quantum operation and ρ_i be a quantum state such that $F(\rho_i) = |\psi_i\rangle\langle\psi_i|$ for all $i = 1, 2, ..., r$. (F is independent of i.) Assume that δ-correct statistical-ϵ-private (restricted) quantum randomized encoding $\hat{F}$ of F for $\{\rho_i\}_{i=1}^r$ exists with a classical encoding operation. Then, for any integer k and any $a > 0$, the operation $W \equiv \mathrm{Dec}^{\otimes k} \circ V \circ \mathrm{Sim}$ satisfies

$$\frac{1}{2}\left\| W(|\psi_i\rangle\langle\psi_i|) - |\psi_i\rangle\langle\psi_i|^{\otimes k} \right\|_1 < \epsilon + \frac{k\delta}{a} + k\sqrt{a} \tag{2}$$

for all $i = 1, 2, ..., r$, where V is an operation that works as $V(|z\rangle\langle z|) = |z\rangle\langle z|^{\otimes k}$ for all computational basis state $|z\rangle$.

This theorem intuitively means that if classical quantum randomized encoding is possible, then we can construct a cloner W that generates k copies $|\psi_i\rangle^{\otimes k}$ of $|\psi_i\rangle$ from a single $|\psi_i\rangle$. Note that because Dec and Sim are independent of i, W is also independent of i. Furthermore, if Dec and Sim are polynomial-time, then W is also polynomial-time.

For example, if we take $a = \sqrt{\delta}$, and we let $\delta \to 0$ and $\epsilon \to 0$, the right-hand side of Eq. (2) approaches 0.

For example, let us take $r = 4$,

$$\rho_1 = |00\rangle\langle 00|,$$
$$\rho_2 = |01\rangle\langle 01|,$$
$$\rho_3 = |10\rangle\langle 10|,$$
$$\rho_4 = |11\rangle\langle 11|,$$

and F being the two-qubit quantum circuit such that the controled-Hadamard is applied (the first qubit is the control qubit and the second qubit is the target qubit), and the first qubit is traced out. In other words, F works as follows:

$$F(\rho_1) = F(|00\rangle\langle 00|) = |0\rangle\langle 0| \equiv |\psi_1\rangle\langle\psi_1|,$$
$$F(\rho_2) = F(|01\rangle\langle 01|) = |1\rangle\langle 1| \equiv |\psi_2\rangle\langle\psi_2|,$$
$$F(\rho_3) = F(|10\rangle\langle 10|) = |+\rangle\langle +| \equiv |\psi_3\rangle\langle\psi_3|,$$
$$F(\rho_4) = F(|11\rangle\langle 11|) = |-\rangle\langle -| \equiv |\psi_4\rangle\langle\psi_4|,$$

where $|\pm\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. If classical quantum randomized encoding of F for $\{\rho_i\}_{i=1}^4$ exists, Theorem 2 means

$$\frac{1}{2}\left\| W(|\psi_i\rangle\langle\psi_i|) - |\psi_i\rangle\langle\psi_i|^{\otimes k} \right\|_1 \to 0$$

for all $i = 1, 2, 3, 4$, which violates the no-cloning. (Note that W is independent of i.)

Our first result, Theorem 1, suggests that if we find a good quantum randomized encoding (in terms of the encoding complexity), then we can construct a good verification protocol of quantum computing, but our second result, Theorem 2, shows that too good quantum randomized encoding is impossible (unless the no-cloning is violated). It is an important open problem to find a concrete quantum randomized encoding scheme in the tight trade-off between these two results.

Another no-go result for classical quantum randomized encoding was shown in Ref. [3], but it is different from ours. What they show is that classical quantum randomized encoding for all BQP problems is unlikely. This is because the class, RE, of languages that have statistical-private randomized encoding is in SZK, and therefore BQP $\subseteq$ RE means BQP $\subseteq$ SZK, which is not believed to happen. Our result, Theorem 2, also prohibits classical quantum randomized encoding, but a difference is that what we prohibit is not the entire BQP computing but only generations of unclonable states $|\psi\rangle$ such as a tensor product of $|0\rangle$, $|1\rangle$, $|+\rangle$, and $|-\rangle$, which is much simpler to generate than doing the general BQP computing. Another technical difference is that they consider classical outputs, but our no-go result does not hold for classical outputs (i.e., $\{|\psi_i\rangle\}_{i=1}^r$ are classical states), because classical states can be cloned.

1.3 Third result: blind quantum computing with server-side output

(Classical) randomized encoding can also be used to the secure delegation of computing, i.e., the client delegates the evaluation of $f(x)$ to the server while the input x is kept secret to the server, because the server cannot learn the input x from $\hat{f}(x;r)$. There is a similar task in quantum cryptography, so-called blind quantum computing [16], [17], [18]. The main difference between quantum randomized encoding and blind quantum computing is, however, that in quantum randomized encoding the server gets the output, while in blind quantum computing, the client gets the output and the output is completely hidden to the server. (See the explanation below.) Our third result is to show that a natural modification of blind quantum computing protocols in such a way that the server gets the output is not secure.

Blind quantum computing enables an almost classical client (who can only generate or measure single-qubit states) to delegate her quantum computing to a remote quantum server in such a way that client's input, output, and program are (information-theoretically) hidden to the server. There are mainly two types of protocols. The Broadbent-Fitzsimons-Kashefi (BFK) protocol [17] requires the client to generate randomly-rotated single-qubit states. The Morimae-Fujii (MF) protocol [18], on the other hand, requires the client to measure single-qubit states. (For readers who are not familiar with these protocols, we provide brief reviews of them in Appendix A.1 and Appendix A.2, respectively.)

Assume that the client wants to implement an n-qubit unitary U on the n-qubit initial state $|\psi_{init}\rangle$. In other words, the client wants to generate the state $U|\psi_{init}\rangle$. (The client might have a quantum memory, and receive a state $|\psi_{init}\rangle$ from the third party. Or, if the client is classical, the initial state $|\psi_{init}\rangle$ will be a computational-basis state $|z\rangle$ with a certain n-bit string z or the standard $|0^n\rangle$ state.) Because the client cannot implement U by herself, she delegates the application of U on $|\psi_{init}\rangle$ to the server. The client and the server run a blind quantum computing protocol. At the end of the blind quantum computing protocol, the honest server gets the quantum-one-time-padded version,

$$\left(\bigotimes_{j=1}^{n} X_j^{x_j} Z_j^{z_j}\right) U|\psi_{init}\rangle, \tag{3}$$

of the output state $U|\psi_{init}\rangle$, where $x \equiv (x_1, ..., x_n) \in \{0,1\}^n$ and $z \equiv (z_1, ..., z_n) \in \{0,1\}^n$ are uniformly ran-

dom n-bit strings. The subscript j of X and Z means that they act on the jth qubit. The one-time pad key (x, z) is (information-theoretically) hidden to the server, and therefore what the server has, Eq. (3), is the completely-mixed state $\frac{I^{\otimes n}}{2^n}$ from his view point. In other words, the output state $U|\psi_{init}\rangle$ is information-theoretically hidden to the server. (Note that blind quantum computing protocols information-theoretically hide client's input, output, and program against not only the honest server but also any malicious server's deviation. See Refs. [16], [17], [18].)

If what the client actually wants is the classical output, namely, the computational-basis measurement result on $U|\psi_{init}\rangle$, the server measures his state in the computational basis, and sends the measurement result $m = (m_1, ..., m_n) \in \{0, 1\}^n$ to the client, where m_j is the computational-basis measurement result on the jth qubit of the server's state. The result m is uniformly random due to the quantum one-time pad, but the client can decode it to get the correct output, because the client knows the key (x, z) of the quantum one-time pad. In fact, the client has only to compute $(x_1 \oplus m_1, ..., x_n \oplus m_n)$. If the client wants the quantum output, namely, $U|\psi_{init}\rangle$, the server sends his state to the client. The client applies $\bigotimes_{j=1}^n X_j^{x_j} Z_j^{z_j}$ on it to unlock the quantum one-time pad, and recovers $U|\psi_{init}\rangle$. In either way, the point is that only the client gets the output, and the output is completely hidden to the server.

This is opposite to quantum randomized encoding where the server gets the output. Can we modify blind quantum computing protocols in such a way that the server gets the output like quantum randomized encoding? A trivial modification is that the server sends the state of Eq. (3) to the client, the client unlocks the quantum one-time pad, and returns the state to the server. This modification has two problems. First, it needs the extra two rounds of quantum communication. Second, it requires the client to have a quantum memory. If the client is completely classical, this idea is impossible. Another way is that the client sends the key of the quantum one-time pad to the server, which is given in Fig. 1 as Protocol 1. In that case, only a single extra communication is required, and it is classical. Furthermore, the client does not need any quantum memory, and therefore it is possible for the completely classical client.

Does this modified protocol, Protocol 1, still satisfy the security? Here, the security means that the server cannot learn anything except for the output state $U|\psi_{init}\rangle$. More formally, we define the security as follows.

1. Run a blind quantum computing protocol such as the BFK or the MF protocol.
2. At the end of the protocol, the honest server possesses the state of Eq. (3).
3. The client sends the key (x, z) of the quantum one-time pad to the server.
4. The server applies $\bigotimes_{j=1}^n X_j^{x_j} Z_j^{z_j}$ on his state to recover $U|\psi_{init}\rangle$.

図 1 The modified blind quantum computing protocol.

Definition 5 Let ρ be the state that any (even computationally-unbounded) malicious server possesses after the modified protocol, Protocol 1. We say that the protocol is ϵ-blind if there exists a (not necessarily polynomial-time) quantum operation, Sim, which we call a simulator, such that

$$\frac{1}{2}\left\|\rho - \mathrm{Sim}(U|\psi_{init}\rangle\langle\psi_{init}|U^\dagger)\right\|_1 \leq \epsilon \tag{4}$$

for any U. Importantly, Sim should be independent of U.

Note that the term "ϵ-blindness" was first defined in Ref. [20], and the above definition is not equivalent to their definition, because now we consider the modification of blind quantum computing in such a way that the server gets the output. (Our definition is, however, inspired by their definition: The above definition intuitively means that anything that the malicious server can get can be generated from the ideal output. The definition of the (local) ϵ-blindness in Ref. [20] intuitively means that anything that the malicious server can get can be generated from his initial information.)

As our third result, we show that Protocol 1 does not satisfy the blindness. (Its proof is given in Sec. 5.)

Theorem 3 Protocol 1 is not ϵ-blind for any $\epsilon < \frac{1}{2}$.

The reason why the ϵ-blindness is not satisfied again comes from the "from secrecy to soundness" [4]. The requirement Eq. (4) is that for the security, but at the same time, it requires that the server "possessed" the correct output state $U|\psi_{init}\rangle$. In other words, the security also means the soundness. Blind quantum computing protocols (such as the BFK and the MF protocols) are not verifiable: whatever the malicious server does, the server cannot learn the secret, but the server can modify the computation without being detected by the client. In fact, we show Theorem 3 by constructing a counter example, and the construction uses the fact that the server can modify the computation.

1.4 Organization

The remaining parts of this paper are organized as follows. The proof of Theorem 1 uses the verification protocol of Ref. [15]. For readers who are not familiar with the protocol, we first explain it in Sec. 2. We then show Theorem 1 in Sec. 3. We next show Theorem 2 in Sec. 4. We finally show Theorem 3 in Sec. 5. Short reviews of the BFK and MF protocols are also provided in Appendix A.1 and Appendix A.2, respectively.

2. Verification protocol of Ref. [15]

In this section, we review the verification protocol of Ref. [15]. Readers who know the protocol can skip this section. The protocol is given in Fig. 2. It was shown in Ref. [15] that the protocol is a verification of quantum computing:

Theorem 4 (Ref. [15]) For any promise problem $A = (A_{yes}, A_{no})$ in BQP, Protocol 2 satisfies both of the following with some c and s such that $c - s \geq \frac{1}{poly(|x|)}$:

- If $x \in A_{yes}$, the honest quantum polynomial-time prover's behavior makes the verifier accept with probability at least c.
- If $x \in A_{no}$, the verifier's acceptance probability is at most s for any (even computationally-unbounded) prover's deviation.

In Ref. [15], the completeness and the soundness are shown by introducing virtual protocols where the prover teleports quantum states to the verifier. In Appendix of Ref. [19], a direct proof of the completeness and the soundness is also given.

If the role of the trusted center is played by the verifier, i.e., the verifier generates $\bigotimes_{j=1}^{N} H^h|m_j\rangle\langle m_j|H^h$ with uniform random (h, m) and sends it to the prover, we have a two-round verification protocol with the first quantum and second classical communication. (See Fig. 3.)

3. Proof of Theorem 1

In this section, we give a proof of Theorem 1. Let us first explain an intuitive idea of the proof. We construct the two-round verification protocol, Protocol 4 (Fig. 4), by modifying Protocol 2 in such a way that the verifier uniformly randomly chooses (h, m) and sends $\hat{F}(\sigma_{h,m})$ to the prover. If the prover is honest, he decodes $\hat{F}(\sigma_{h,m})$ to get $\bigotimes_{j=1}^{N} H^h|m_j\rangle\langle m_j|H^h$, on which the honest prover can simulate the remaining steps of Protocol 2, and therefore the completeness of Protocol 4 is satisfied due to the completeness of Protocol 2. If the prover is malicious, on the other hand, he can do any measurement on the received state $\hat{F}(\sigma_{h,m})$, but because $\hat{F}(\sigma_{h,m})$ is ϵ-close to

$$\mathrm{Sim}(F(\sigma_{h,m})) = \mathrm{Sim}\Big[\Big(\bigotimes_{j=1}^{N} H^h|m_j\rangle\langle m_j|H^h\Big) \otimes \eta_{junk}\Big],$$

any malicious prover's attack on $\hat{F}(\sigma_{h,m})$ is simulated by another attack on $\bigotimes_{j=1}^{N} H^h|m_j\rangle\langle m_j|H^h$, which is sound due to the soundness of Protocol 2.

Now let us give the proof. By assumption, there exist quantum operations, Dec and Sim, such that

$$\frac{1}{2}\Big\|\mathrm{Dec}(\hat{F}(\sigma_{h,m})) - F(\sigma_{h,m})\Big\|_1 \leq \delta \tag{5}$$

and

$$\frac{1}{2}\Big\|\hat{F}(\sigma_{h,m}) - \mathrm{Sim}(F(\sigma_{h,m}))\Big\|_1 \leq \epsilon \tag{6}$$

with negligible δ and ϵ for any $(h, m) \in \{0,1\} \times \{0,1\}^N$.

0. The input is an instance $x \in A$ of a promise problem $A = (A_{yes}, A_{no})$ in BQP, and a corresponding N-qubit local Hamiltonian
$$\mathcal{H} \equiv \sum_{i<j} \frac{p_{i,j}}{2}\Big(\frac{I^{\otimes N} + s_{i,j}X_i \otimes X_j}{2} + \frac{I^{\otimes N} + s_{i,j}Z_i \otimes Z_j}{2}\Big)$$
with $N = poly(|x|)$ such that if $x \in A_{yes}$ then the ground energy is less than α, and if $x \in A_{no}$ then the ground energy is larger than β with $\beta - \alpha \geq \frac{1}{poly(|x|)}$. Here, $I \equiv |0\rangle\langle 0| + |1\rangle\langle 1|$ is the two-dimensional identity operator, X_i is the Pauli X operator acting on the ith qubit, Z_i is the Pauli Z operator acting on the ith qubit, $p_{i,j} > 0$, $\sum_{i<j} p_{i,j} = 1$, and $s_{i,j} \in \{+1, -1\}$.
1. The trusted center uniformly randomly chooses $(h, m_1, ..., m_N) \in \{0,1\}^{N+1}$. The trusted center sends $\bigotimes_{j=1}^{N}(H^h|m_j\rangle)$ to the prover. The trusted center sends (h, m) to the verifier, where $m \equiv (m_1, ..., m_N) \in \{0,1\}^N$.
2. Let $x \equiv (x_1, ..., x_N) \in \{0,1\}^N$ and $z \equiv (z_1, ..., z_N) \in \{0,1\}^N$. The prover does a POVM measurement $\{\Pi_{x,z}\}_{x,z}$ on the received state. When the prover is honest, the POVM corresponds to the teleportation of a low-energy state $|E_0\rangle$ of the local Hamiltonian $\mathcal{H}$ as if the states sent from the trusted center are halves of Bell pairs. The prover sends the measurement result, (x, z), to the verifier.
3. The verifier samples (i, j) with probability $p_{i,j}$, and accepts if and only if $(-1)^{m'_i}(-1)^{m'_j} = -s_{i,j}$, where $m'_i \equiv m_i \oplus (hz_i + (1-h)x_i)$.

図 2 The verification protocol of Ref. [15].

0. The same as Protocol 2.
1. The verifier uniformly randomly chooses $(h, m_1, ..., m_N) \in \{0,1\}^{N+1}$, and sends $\bigotimes_{j=1}^{N}(H^h|m_j\rangle)$ to the prover.
2. The same as Protocol 2.
3. The same as Protocol 2.

図 3 The two-round verification protocol with the verifier who generates random BB84 states.

0. The same as Protocol 2.
1. The verifier uniformly randomly chooses $(h,m) \in \{0,1\} \times \{0,1\}^N$ and sends $\hat{F}(\sigma_{h,m})$ to the prover. The verifier requires the operation E to generate $\hat{F}(\sigma_{h,m})$. If the prover is honest, it applies the decoding operation Dec on $\hat{F}(\sigma_{h,m})$ to get $\mathrm{Dec}(\hat{F}(\sigma_{h,m}))$.
2. The same as Protocol 2 except that the honest prover applies the POVM on $\mathrm{Tr}_{junk}[\mathrm{Dec}(\hat{F}(\sigma_{h,m}))]$, where Tr_{junk} is the partial trace of the subsystem $junk$. (Remember that $\mathrm{Dec}(\hat{F}(\sigma_{h,m}))$ is δ-close to
$$F(\sigma_{h,m}) = \Big(\bigotimes_{j=1}^{N} H^h|m_j\rangle\langle m_j|H^h\Big) \otimes \eta_{junk}.$$
We define the subsystem $junk$ as the one for η_{junk}.)
3. The same as Protocol 2.

図 4 The two-round verification protocol with quantum randomized encoding.

By assumption, Dec can be implemented in quantum polynomial-time in terms of the number of qubits of $\hat{F}(\sigma_{h,m})$.

Consider the two-round protocol, Protocol 4, shown in Fig. 4. We show that Protocol 4 is a verification of quantum computing.

First, let us consider the case when $x \in A_{yes}$. Let p^1_{acc} and p^3_{acc} be verifier's acceptance probabilities with the honest provers in Protocol 2 and Protocol 4, respectively. Let $\{\Pi_{x,z}\}_{x,z}$ be the POVM measurement that the honest prover applies. (Remember that both of the honest provers in Protocol 2 and Protocol 4 apply the same POVM measurement.) Let us define

$$P^1_P(x,z|h,m) \equiv \mathrm{Tr}\Big[\Pi_{x,z}\bigotimes_{j=1}^{N} H^h|m_j\rangle\langle m_j|H^h\Big],$$
$$P^3_P(x,z|h,m) \equiv \mathrm{Tr}\Big[\Pi_{x,z}\mathrm{Tr}_{junk}(\mathrm{Dec}(\hat{F}(\sigma_{h,m})))\Big].$$

Note that

$$\begin{aligned}
&\sum_{x,z}\Big|P^3_P(x,z|h,m) - P^1_P(x,z|h,m)\Big| \qquad (7)\\
&\le \Big\|\mathrm{Tr}_{junk}(\mathrm{Dec}(\hat{F}(\sigma_{h,m}))) - \bigotimes_{j=1}^{N} H^h|m_j\rangle\langle m_j|H^h\Big\|_1\\
&\le \Big\|\mathrm{Dec}(\hat{F}(\sigma_{h,m})) - \Big(\bigotimes_{j=1}^{N} H^h|m_j\rangle\langle m_j|H^h\Big)\otimes\eta_{junk}\Big\|_1\\
&= \Big\|\mathrm{Dec}(\hat{F}(\sigma_{h,m})) - F(\sigma_{h,m})\Big\|_1\\
&\le 2\delta, \qquad (8)
\end{aligned}$$

where in the second inequality we have used the monotonicity of the trace distance with respect to the partial trace Tr_{junk}, and in the last inequality we have used Eq. (5).

Let $P_V(acc|x,z,h,m)$ be the probability that the verifier accepts given (x,z,h,m). (Remember that both of the verifiers in Protocol 2 and Protocol 4 do the same classical computing to make the decision.) Then, we obtain

$$\begin{aligned}
|p^3_{acc} - p^1_{acc}| &= \Big|\frac{1}{2^{N+1}}\sum_{h,m}\sum_{x,z} P^3_P(x,z|h,m)P_V(acc|x,z,h,m)\\
&\quad - \frac{1}{2^{N+1}}\sum_{h,m}\sum_{x,z} P^1_P(x,z|h,m)P_V(acc|x,z,h,m)\Big|\\
&\le \frac{1}{2^{N+1}}\sum_{h,m}\sum_{x,z}\Big|P^3_P(x,z|h,m)P_V(acc|x,z,h,m)\\
&\quad - P^1_P(x,z|h,m)P_V(acc|x,z,h,m)\Big|\\
&= \frac{1}{2^{N+1}}\sum_{h,m}\sum_{x,z}\Big|P^3_P(x,z|h,m)\\
&\quad - P^1_P(x,z|h,m)\Big|P_V(acc|x,z,h,m)\\
&\le \frac{1}{2^{N+1}}\sum_{h,m}\sum_{x,z}\Big|P^3_P(x,z|h,m)\\
&\quad - P^1_P(x,z|h,m)\Big|\\
&\le \frac{1}{2^{N+1}}\sum_{h,m} 2\delta\\
&= 2\delta,
\end{aligned}$$

where in the fifth inequality, we have used Eq. (8).

Due to the completeness of Protocol 2, $p^1_{acc} \ge c$ with a certain c. (It is actually $1-\alpha$ [15], [19].) We therefore obtain

$$p^3_{acc} \ge p^1_{acc} - 2\delta \ge c - 2\delta \equiv c'. \qquad (9)$$

Next, let us consider the case when $x \in A_{no}$. For any POVM measurement $\{\Lambda_{x,z}\}_{x,z}$, define

$$P^1_P(x,z|h,m) \equiv \mathrm{Tr}\Big[\Lambda_{x,z}\mathrm{Sim}\Big(\Big(\bigotimes_{j=1}^{N} H^h|m_j\rangle\langle m_j|H^h\Big)\otimes\eta_{junk}\Big)\Big],$$
$$P^3_P(x,z|h,m) \equiv \mathrm{Tr}\Big[\Lambda_{x,z}\hat{F}(\sigma_{h,m})\Big].$$

Note that

$$\begin{aligned}
&\sum_{x,z}\Big|P^3_P(x,z|h,m) - P^1_P(x,z|h,m)\Big| \qquad (10)\\
&\le \Big\|\hat{F}(\sigma_{h,m}) - \mathrm{Sim}\Big(\Big(\bigotimes_{j=1}^{N} H^h|m_j\rangle\langle m_j|H^h\Big)\otimes\eta_{junk}\Big)\Big\|_1\\
&= \Big\|\hat{F}(\sigma_{h,m}) - \mathrm{Sim}(F(\sigma_{h,m}))\Big\|_1\\
&\le 2\epsilon, \qquad (11)
\end{aligned}$$

where the last inequality is from Eq. (6).

Let $P_V(acc|x,z,h,m)$ be the probability that the verifier accepts given (x,z,h,m). Let p^3_{acc} be the verifier's acceptance probability in Protocol 4 when the malicious prover applies the POVM measurement $\{\Lambda_{x,z}\}_{x,z}$ on the

received state $\hat{F}(\sigma_{h,m})$. Let p^1_{acc} be the verifier's acceptance probability in Protocol 2 with the following malicious prover:

1. The prover first adds η_{junk} to the received state $\bigotimes_{j=1}^N H^h|m_j\rangle\langle m_j|H^h$ to generate $\left(\bigotimes_{j=1}^N H^h|m_j\rangle\langle m_j|H^h\right)\otimes\eta_{junk}$.
2. The prover next applies Sim on it to generate $\mathrm{Sim}\left[\left(\bigotimes_{j=1}^N H^h|m_j\rangle\langle m_j|H^h\right)\otimes\eta_{junk}\right]$.
3. The prover finally does the POVM measurement $\{\Lambda_{x,z}\}_{x,z}$ on it.

Then, we obtain

$$\begin{aligned}
|p^3_{acc}-p^1_{acc}| &= \Big|\frac{1}{2^{N+1}}\sum_{h,m}\sum_{x,z}P^3_P(x,z|h,m)P_V(acc|x,z,h,m)\\
&\quad -\frac{1}{2^{N+1}}\sum_{h,m}\sum_{x,z}P^1_P(x,z|h,m)P_V(acc|x,z,h,m)\Big|\\
&\le \frac{1}{2^{N+1}}\sum_{h,m}\sum_{x,z}\Big|P^3_P(x,z|h,m)P_V(acc|x,z,h,m)\\
&\quad -P^1_P(x,z|h,m)P_V(acc|x,z,h,m)\Big|\\
&= \frac{1}{2^{N+1}}\sum_{h,m}\sum_{x,z}\Big|P^3_P(x,z|h,m)\\
&\quad -P^1_P(x,z|h,m)\Big|P_V(acc|x,z,h,m)\\
&\le \frac{1}{2^{N+1}}\sum_{h,m}\sum_{x,z}\Big|P^3_P(x,z|h,m)\\
&\quad -P^1_P(x,z|h,m)\Big|\\
&\le \frac{1}{2^{N+1}}\sum_{h,m}2\epsilon\\
&= 2\epsilon,
\end{aligned}$$

where the fifth inequality comes from Eq. (11).

Due to the soundness of Protocol 2, $p^1_{acc}\le s$ with a certain s. (It is actually $1-\beta$ [15], [19].) We therefore obtain

$$p^3_{acc}\le p^1_{acc}+2\epsilon\le s+2\epsilon\equiv s' \tag{12}$$

for any POVM measurement $\{\Lambda_{x,z}\}_{x,z}$. From Eqs. (9) and (12),

$$c'-s'=c-2\delta-(s+2\epsilon)=c-s-2\delta-2\epsilon\ge\frac{1}{poly(|x|)},$$

the inverse-polynomial completeness-soundness gap is satisfied for Protocol 4.

4. Proof of Theorem 2

In this section, we show Theorem 2. Let us first explain an intuitive idea of the proof. Assume that we want to clone $F(\rho_i)$. We first apply Sim on $F(\rho_i)$ to get $\mathrm{Sim}(F(\rho_i))$, which is ϵ-close to $\hat{F}(\rho_i)$. By assumption, $\hat{F}(\rho_i)$ is a classical state and therefore we can clone it to get $[\hat{F}(\rho_i)]^{\otimes k}$. (In fact, we cannot clone mixed states in general, and therefore some twists are necessary, but an intuitive idea is to "clone" the classical state $\hat{F}(\rho_i)$. For more precise calculations, see the proof below.) If we decode each $\hat{F}(\rho_i)$ by applying Dec, we obtain $[\mathrm{Dec}(\hat{F}(\rho_i))]^{\otimes k}\approx[F(\rho_i)]^{\otimes k}$, and thus our goal is achieved.

Now we give the proof. Because the following argument holds for every i $(i=1,2,...,r)$, we fix i. For simplicity, we remove the subscript i of $|\psi_i\rangle$ and ρ_i, and just write them as $|\psi\rangle$ and ρ, respectively. Let us denote $\hat{\psi}\equiv\hat{F}(\rho)$. By assumption, the statistical-ϵ-privacy,

$$\frac{1}{2}\left\|\mathrm{Sim}(|\psi\rangle\langle\psi|)-\hat{\psi}\right\|_1\le\epsilon, \tag{13}$$

and the δ-correctness,

$$\frac{1}{2}\left\|\mathrm{Dec}(\hat{\psi})-|\psi\rangle\langle\psi|\right\|_1\le\delta, \tag{14}$$

are satisfied. Furthermore, by assumption, $\hat{\psi}$ can be generated with a classical operation. In other words,

$$\hat{\psi}=\sum_z p_z|z\rangle\langle z|, \tag{15}$$

where $|z\rangle$ is a computational basis state and $\{p_z\}_z$ is a probability distribution. We define the operation W by

$$W\equiv\mathrm{Dec}^{\otimes k}\circ V\circ\mathrm{Sim},$$

where V is an operation that works as $V(|z\rangle\langle z|)=|z\rangle\langle z|^{\otimes k}$ for any computational basis state $|z\rangle$.

First, we obtain

$$\begin{aligned}
&\frac{1}{2}\left\|W(|\psi\rangle\langle\psi|)-\mathrm{Dec}^{\otimes k}\circ V(\hat{\psi})\right\|_1 &(16)\\
&=\frac{1}{2}\left\|\mathrm{Dec}^{\otimes k}\circ V\circ\mathrm{Sim}(|\psi\rangle\langle\psi|)-\mathrm{Dec}^{\otimes k}\circ V(\hat{\psi})\right\|_1\\
&\le\frac{1}{2}\left\|\mathrm{Sim}(|\psi\rangle\langle\psi|)-\hat{\psi}\right\|_1\\
&\le\epsilon, &(17)
\end{aligned}$$

where in the second inequality, we have used the monotonicity of the trace distance with respect to the operation $\mathrm{Dec}^{\otimes k}\circ V$, and the third inequality comes from Eq. (13).

Second, we obtain

$$\begin{aligned}
\sum_z p_z\Big[1-\langle\psi|\mathrm{Dec}(|z\rangle\langle z|)|\psi\rangle\Big] &\le \frac{1}{2}\Big\|\sum_z p_z\mathrm{Dec}(|z\rangle\langle z|)-|\psi\rangle\langle\psi|\Big\|_1\\
&= \frac{1}{2}\left\|\mathrm{Dec}(\hat{\psi})-|\psi\rangle\langle\psi|\right\|_1\\
&\le \delta, &(18)
\end{aligned}$$

where the first inequality is from the property of the trace distance, and the second equality is from Eq. (15). The last inequality is from Eq. (14).

For any $a>0$, let us define

$$G\equiv\Big\{z\ \Big|\ 1-\langle\psi|\mathrm{Dec}(|z\rangle\langle z|)|\psi\rangle\ge a\Big\}.$$

Then, from Eq. (18),

$$\begin{aligned}\delta &\geq \sum_z p_z \Big[1 - \langle\psi|\mathrm{Dec}(|z\rangle\langle z|)|\psi\rangle\Big] \\ &= \sum_{z\in G} p_z \Big[1 - \langle\psi|\mathrm{Dec}(|z\rangle\langle z|)|\psi\rangle\Big] \\ &\quad + \sum_{z\notin G} p_z \Big[1 - \langle\psi|\mathrm{Dec}(|z\rangle\langle z|)|\psi\rangle\Big] \\ &\geq a\sum_{z\in G} p_z + 0\times\sum_{z\notin G} p_z \\ &= a\sum_{z\in G} p_z,\end{aligned}$$

which means

$$\sum_{z\in G} p_z \leq \frac{\delta}{a}. \tag{19}$$

Hence

$$\begin{aligned}&\frac{1}{2}\Big\|W(|\psi\rangle\langle\psi|) - |\psi\rangle\langle\psi|^{\otimes k}\Big\|_1 \\ &\leq \frac{1}{2}\Big\|W(|\psi\rangle\langle\psi|) - \mathrm{Dec}^{\otimes k}\circ V(\hat{\psi})\Big\|_1 \\ &\quad + \frac{1}{2}\Big\|\mathrm{Dec}^{\otimes k}\circ V(\hat{\psi}) - |\psi\rangle\langle\psi|^{\otimes k}\Big\|_1 \\ &\leq \epsilon + \frac{1}{2}\Big\|\sum_z p_z \mathrm{Dec}(|z\rangle\langle z|)^{\otimes k} - |\psi\rangle\langle\psi|^{\otimes k}\Big\|_1 \\ &\leq \epsilon + \frac{1}{2}\sum_z p_z \Big\|\mathrm{Dec}(|z\rangle\langle z|)^{\otimes k} - |\psi\rangle\langle\psi|^{\otimes k}\Big\|_1 \\ &\leq \epsilon + \frac{k}{2}\sum_z p_z \Big\|\mathrm{Dec}(|z\rangle\langle z|) - |\psi\rangle\langle\psi|\Big\|_1 \\ &\leq \epsilon + k\sum_z p_z \sqrt{1 - \langle\psi|\mathrm{Dec}(|z\rangle\langle z|)|\psi\rangle} \\ &= \epsilon + k\sum_{z\in G} p_z \sqrt{1 - \langle\psi|\mathrm{Dec}(|z\rangle\langle z|)|\psi\rangle} \\ &\quad + k\sum_{z\notin G} p_z \sqrt{1 - \langle\psi|\mathrm{Dec}(|z\rangle\langle z|)|\psi\rangle} \\ &< \epsilon + k\sum_{z\in G} p_z + k\sqrt{a}\sum_{z\notin G} p_z \\ &\leq \epsilon + \frac{k\delta}{a} + k\sqrt{a}.\end{aligned}$$

In the second inequality, we have used Eq. (17). In the last inequality, we have used Eq. (19).

5. Proof of Theorem 3

In this section, we show that the modified blind quantum computing protocol, Protocol 1, of Fig 1 is not ϵ-blind for any $\epsilon < \frac{1}{2}$. To show it, we construct a simple counter example.

We first explain an intuitive idea of the proof. We show that for some unitary V a deviated server can generate the state $UV|\psi_{init}\rangle$ instead of the correct output state $U|\psi_{init}\rangle$. If we require the ϵ-blindness, $UV|\psi_{init}\rangle$ should be generated (ϵ-approximately) from $U|\psi_{init}\rangle$ with a simulator Sim that is independent of U. However, generating $UV|\psi_{init}\rangle$ from a given single copy of $U|\psi_{init}\rangle$ is impossible when the information about U is not available. (If you have already applied U on $|\psi_{init}\rangle$, you can no longer "squeeze" V between U and $|\psi_{init}\rangle$ if you do not know U.)

Next, let us give a more precise proof. Because our goal is to construct a simple counter example, let us consider a single-qubit quantum computing implemented on the one-dimensional linear graph state. Assume that the client wants to implement a single-qubit unitary U on the initial state $|+\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. We can construct a specific deviation of the malicious server in such a way that the server gets the state

$$\Big(\bigotimes_{j=1}^{n} X_j^{x_j} Z_j^{z_j}\Big) U e^{i\frac{\xi}{2}Z}|+\rangle, \tag{20}$$

instead of

$$\Big(\bigotimes_{j=1}^{n} X_j^{x_j} Z_j^{z_j}\Big) U|+\rangle,$$

in the step 2 of Protocol 1, where ξ is arbitrarily chosen by the server. In fact, if the BFK protocol is used in the step 1 of Protocol 1, the server has only to measure the first qubit with angle $\delta_1 + \xi$ (instead of δ_1) when the server receives δ_1 from the client. If the MF protocol is used in the step 1 of Protocol 1, on the other hand, the server has only to apply $e^{i\frac{\xi}{2}Z}$ on the first qubit of the one-dimensional graph state before sending it to the client. (For more details of the BFK and MF protocols, see Appendix A.1 and Appendix A.2, respectively.) In the step 3 of Protocol 1, the client sends the quantum one-time pad key (x, z) to the server. In the step 4 of Protocol 1, the server unlocks the quantum one-time pad to obtain $Ue^{i\frac{\xi}{2}Z}|+\rangle$.

Assume that Protocol 1 is ϵ-blind with $\epsilon < \frac{1}{2}$ against this specific attack by the malicious server. It means that there exists a quantum operation Sim, which is independent of U, such that

$$\frac{1}{2}\Big\|\mathrm{Sim}(U|+\rangle\langle+|U^\dagger) - Ue^{i\frac{\xi}{2}Z}|+\rangle\langle+|e^{-i\frac{\xi}{2}Z}U^\dagger\Big\|_1 \leq \epsilon \tag{21}$$

for all U. Let us take $\xi = \frac{\pi}{2}$. If $U = I$, Eq. (21) becomes

$$\frac{1}{2}\Big\|\mathrm{Sim}(|+\rangle\langle+|) - e^{i\frac{\pi}{4}Z}|+\rangle\langle+|e^{-i\frac{\pi}{4}Z}\Big\|_1 \leq \epsilon, \tag{22}$$

but if $U = X$, Eq. (21) becomes

$$\frac{1}{2}\Big\|\mathrm{Sim}(|+\rangle\langle+|) - e^{-i\frac{\pi}{4}Z}|+\rangle\langle+|e^{i\frac{\pi}{4}Z}\Big\|_1 \leq \epsilon. \tag{23}$$

From Eqs. (22) and (23),

$$
\begin{aligned}
1 &= \frac{1}{2}\left\| e^{i\frac{\pi}{4}Z}|+\rangle\langle+|e^{-i\frac{\pi}{4}Z} - e^{-i\frac{\pi}{4}Z}|+\rangle\langle+|e^{i\frac{\pi}{4}Z}\right\|_1 \\
&\leq \frac{1}{2}\left\| \mathrm{Sim}(|+\rangle\langle+|) - e^{i\frac{\pi}{4}Z}|+\rangle\langle+|e^{-i\frac{\pi}{4}Z}\right\|_1 \\
&\quad + \frac{1}{2}\left\| \mathrm{Sim}(|+\rangle\langle+|) - e^{-i\frac{\pi}{4}Z}|+\rangle\langle+|e^{i\frac{\pi}{4}Z}\right\|_1 \\
&\leq 2\epsilon,
\end{aligned}
$$

and therefore $\epsilon \geq \frac{1}{2}$, but it contradicts the assumption that $\epsilon < \frac{1}{2}$.

付　　録

A.1 BFK protocol

In this appendix, we review the BFK protocol [17]. For simplicity, let us consider the measurement-based quantum computation on a linear graph state. The client first sends n qubits, $\{|+_{\theta_j}\rangle\}_{j=1}^n$, to the server, where $|\pm_\theta\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle \pm e^{i\theta}|1\rangle)$, and each θ_j is chosen uniformly at random from $\{\frac{k\pi}{8} \mid k = 0, 1, ..., 7\}$. The server applies CZ gates to generate the state

$$
|\Psi_{Bob}\rangle \equiv \Big(\prod_{i=1}^{n-1} CZ_{i,i+1}\Big)\Big[\bigotimes_{j=1}^{n} |+_{\theta_j}\rangle\Big].
$$

Because Z-rotations and CZ commute with each other,

$$
\begin{aligned}
|\Psi_{Bob}\rangle &= \Big(\prod_{i=1}^{n-1} CZ_{i,i+1}\Big)\Big[\bigotimes_{j=1}^{n} e^{-i\frac{\theta_j}{2}Z}|+\rangle\Big] \\
&= \Big(\bigotimes_{j=1}^{n} e^{-i\frac{\theta_j}{2}Z}\Big)\Big(\prod_{i=1}^{n-1} CZ_{i,i+1}\Big)|+\rangle^{\otimes n} \\
&= \Big(\bigotimes_{j=1}^{n} e^{-i\frac{\theta_j}{2}Z}\Big)|G\rangle,
\end{aligned}
$$

where $|G\rangle$ is the n-qubit linear graph state.

Assume that the client wants to measure the first qubit of $|G\rangle$ in the basis $|\pm_{\phi_1}\rangle$ for a certain $\phi_1 \in \{\frac{k\pi}{8} \mid k = 0, 1, 2, ..., 7\}$. The client sends $\delta_1 \equiv \phi_1 + \theta_1 + r_1\pi$ to the server, where $r_1 \in \{0, 1\}$ is a uniform random bit. The server measures the first qubit of $|\Psi_{Bob}\rangle$ in the basis $|\pm_{\delta_1}\rangle$. The post-measurement state is

$$
\begin{aligned}
&\Big(\langle\pm_{\delta_1}| \otimes I^{\otimes n-1}\Big)\Big(\bigotimes_{j=1}^{n} e^{-i\frac{\theta_j}{2}Z}\Big)|G\rangle \\
&= \Big(I \otimes \bigotimes_{j=2}^{n} e^{-i\frac{\theta_j}{2}Z}\Big)\Big(\langle\pm|e^{i\frac{\delta_1}{2}Z}e^{-i\frac{\theta_1}{2}Z} \otimes I^{\otimes n-1}\Big)|G\rangle \\
&= \Big(I \otimes \bigotimes_{j=2}^{n} e^{-i\frac{\theta_j}{2}Z}\Big)\Big(\langle\pm|e^{i\frac{\phi_1+r_1\pi}{2}Z} \otimes I^{\otimes n-1}\Big)|G\rangle \\
&= \Big(I \otimes \bigotimes_{j=2}^{n} e^{-i\frac{\theta_j}{2}Z}\Big)\Big(\langle\pm_{\phi_1+r_1\pi}| \otimes I^{\otimes n-1}\Big)|G\rangle,
\end{aligned}
$$

but this is equal to the post-measurement state when the first qubit of $|G\rangle$ is measured in the basis $|\pm_{\phi_1+r_1\pi}\rangle$. (The effect of r_1 is only the flip of the measurement result.) In this way, if the server is honest, the client can let the server do the correct measurement-based quantum computation. Multi-qubit universal quantum computing is also possible on appropriate universal resource states such the brickwork state [17]. (For details, see Ref. [17].)

An intuitive idea of the blindness of the BFK protocol is that the client's true measurement angle ϕ_j is "one-time padded" by "the key" θ_j, and therefore the server cannot learn ϕ_j from δ_j. If the server measures $|\theta_j\rangle$, he can learn a single bit of information about θ_j, but this information is "scrambled" by the randomly chosen r_j. For more precise proofs of the blindness of the BFK protocol, see Refs. [17], [20].

A.2 MF protocol

In this appendix, we review the MF protocol [18]. In the MF protocol, the server first prepares a graph state, and sends each qubit of the graph state (except for the qubits in the last layer) to the client. (If the server sends each qubit one-by-one sequentially, the client does not need any quantum memory.) The client measures each qubit according to the measurement pattern of her measurement-based quantum computing.

It is clear that if the server is honest, i.e., if the server prepares the correct graph state, the last layer of the graph state that the server possesses becomes Eq. (3) after the client measures all qubits sent to her. It is also obvious that whatever the malicious server does, client's measurement angles are hidden to the server due to the no-signaling.

参考文献

[1] B. Applebaum, Garbled Circuits as Randomized Encodings of Functions: a Primer. In: Lindell Y. (eds) Tutorials on the Foundations of Cryptography. Information Security and Cryptography. Springer, Cham.
[2] A. C.-C. Yao, How to generate and exchange secrets (extended abstract). In 27th FOCS, pages 162-167. IEEE Computer Society Press, Oct. 1986.
[3] Z. Brakerski and H. Yuen, Quantum garbled circuits. arXiv:2006.01085
[4] B. Applebaum, Y. Ishai, and E. Kushilevitz, From secrecy to soundness: efficient verification via secure computation. In: Abramsky S., Gavoille C., Kirchner C., Meyer auf der Heide F., Spirakis P.G. (eds) Automata, Languages and Programming. ICALP 2010. Lecture Notes in Computer Science, vol 6198. Springer, Berlin, Heidelberg.
[5] D. Aharonov and U. Vazirani, Is quantum mechanics falsifiable? A computational perspective on the foundations

of quantum mechanics. arXiv:1206.3686
[6] A. Gheorghiu, T. Kapourniotis, and E. Kashefi, Verification of quantum computation: an overview of existing approaches. Theory of Computing Systems **63**, 715-808 (2019); arXiv:1709.06984
[7] J. F. Fitzsimons and E. Kashefi, Unconditionally verifiable blind computation. Phys. Rev. A **96**, 012303 (2017).
[8] J. F. Fitzsimons, M. Hajdušek, and T. Morimae, Post hoc verification of quantum computation. Phys. Rev. Lett. **120**, 040501 (2018).
[9] M. McKague, Interactive proofs for BQP via self-tested graph states. Theory of Computing **12**, 1 (2016).
[10] Z. Ji, Classical verification of quantum proofs. Proceedings of the 48th annual ACM symposium on Theory of Computing (STOC 2016) p.885 (2016).
[11] B. W. Reichardt, F. Unger, and U. Vazirani, Classical command of quantum systems. Nature **496**, 456 (2013).
[12] A. B. Grilo, A simple protocol for verifiable delegation of quantum computation in one round. 46th International Colloquium on Automata, Languages, and Programming (ICALP 2019).
[13] A. Coladangelo, A. B. Grilo, S. Jeffery, and T. Vidick, Verifier-on-a-Leash: new schemes for verifiable delegated quantum computation, with quasilinear resources. arXiv:1708.07359; EUROCRYPT 2019.
[14] U. Mahadev, Classical verification of quantum computations. IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS), Paris, 2018, pp.259-267; arXiv:1804.01082
[15] T. Morimae, Information-theoretically-sound non-interactive classical verification of quantum computing with trusted center, arXiv:2003.10712
[16] J. F. Fitzsimons, Private quantum computation: an introduction to blind quantum computing and related protocols. npj Quantum Information **3**, 23 (2017).
[17] A. Broadbent, J. F. Fitzsimons, and E. Kashefi, in Proceedings of the 50th Annual IEEE Symposiumon Foundations of Computer Science (IEEE Computer Society, Los Alamitos, CA, USA, 2009), pp. 517-526.
[18] T. Morimae and K. Fujii, Blind quantum computation protocol in which Alice only makes measurements, Phys. Rev. A **87**, 050301(R) (2013).
[19] T. Morimae and Y. Takeuchi, Trusted center verification model and classical channel remote state preparation, arXiv:2008.05033
[20] V. Dunjko, J. F. Fitzsimons, C. Portmann, and R. Renner Composable Security of Delegated Quantum Computation. In: Sarkar P., Iwata T. (eds) Advances in Cryptology-ASIACRYPT 2014. Lecture Notes in Computer Science, vol 8874. Springer, Berlin, Heidelberg.
[21] After uploading this paper on arXiv, Ref. [3] was revised and in the revised version, a zero-knowledge protocol for QMA is constructed by using quantum randomized encoding.