



**Classical verification of quantum measurement for the computational basis and the  $XY$ -plane basis**Qingshan Xu <sup>1</sup>, Xiaoqing Tan <sup>1,\*</sup>, Daipengwei Bao,<sup>1</sup> and Rui Huang<sup>2</sup><sup>1</sup>*College of Information Science and Technology, Jinan University, Guangzhou 510632, China*<sup>2</sup>*School of Artificial Intelligence, Shenzhen Polytechnic, Shenzhen 518055, China*

(Received 19 February 2023; accepted 15 May 2023; published 26 May 2023)

Recent advances in quantum technologies raise the urgent need of verifying the correct functionality of a quantum device. Certifying the correctness of a quantum device in a fully classical manner is an important research branch. In this paper, we present a measurement protocol that allows a classical verifier to interact with an efficient quantum prover to verify the computational basis or the  $XY$ -plane basis measurement on a quantum state. With the help of two adaptive hardcore bit properties of a noisy trapdoor claw-free family, the security of measurement protocol is proved, which is under quantum hardness of the learning with error. The security characterizes the distance between the output distribution of measurement protocol and the distribution obtained by measuring certain quantum states in the designated basis, with or without the presence of honest behavior of the prover. Moreover, exploiting the measurement protocol, we present two device-noise-independent verification protocols of graph states and a classical verification protocol of delegated quantum computing whose soundness is 0.5757.

DOI: [10.1103/PhysRevA.107.052616](https://doi.org/10.1103/PhysRevA.107.052616)**I. INTRODUCTION**

Verification of quantum computing, as a type of secure quantum computing, is an interactive protocol that allows a verifier to check the prover's output on quantum computing tasks in a way that preserves some security properties, even in the face of adversarial behavior by the prover. It is related to complexity theory. Depending on the differences of power of verification protocols, there exists many well-known complexity classes [non-deterministic polynomial time (NP), interactive proofs (IP), multiprover interactive proofs (MIP)] and theorems (the PCP theorem and  $IP=PSPACE$ ) [1]. In addition, verification of computing has been widely studied in many cryptographic problems, such as zero knowledge [2]. With the emergence of quantum computers, a new problem of whether one can verify the outcome of quantum computations needs to be answered.

Quantum computers can efficiently solve important problems that are currently out of reach for classical computers, such as boson sampling [3] and integer factorization [4]. Compared with classical algorithms, quantum algorithms can realize dramatic reductions in run time for some problems [5,6]. A rapid development of quantum computing may promise highly useful tools that can be applied to fundamental research and commercial businesses. These prospects come with challenging requirements for certifying the quantum devices correct functioning. The certification can be regarded as a protocol that returns accept if the device is functioning correctly and reject if the device runs wrong.

There are numerous methods [7,8] toward addressing the problem of certification. For example, in order to verify that

a device has produced the correct quantum state, the methods of state tomography [9], direct quantum-state certification [10], direct-fidelity estimation [11], and self-testing [12] have been proposed. As for the verification of quantum processes, i.e., maps on quantum states, the method of direct quantum-process certification [13], randomized benchmarking [14], and cross-entropy benchmarking [15] have been proposed. Here, the verifier is allowed to perform measurements. Another example is verifiable delegated quantum computation [16–22]. In this situation, a client with only the ability to do classical computing and prepare or measure single qubits can delegate computation tasks to a server who has the ability to do universal quantum computation while simultaneously verifying the correctness of the outcome.

In the setting of secure quantum computing, the goal is to allow a client to access remotely quantum computing capabilities of a server in a way that preserves some security properties, even in face of adversarial behavior by the server. The common properties of secure quantum computing contain correctness (the client can obtain correct outcome if the server behaves honestly), blindness (the server learns nothing about the input, algorithm, and output), and verifiability (the client can check the validity of outcome against any malicious server). The verification of quantum computing consists of correctness and verifiability. According to the configuration of the client (verifier) and server (prover), earlier feasible verification protocols can be divided into two types. The first type of methods [16,18] have considered the case where a verifier with limited quantum power interacts with a quantum prover. The second type of methods [19,20] have considered the case where a fully classical verifier interacts with multiple non-communicating provers that share entanglement. However, the case where a classical verifier interacts with a quantum prover to verify quantum computing is not considered.

\*ttanxq@jnu.edu.cn

Recently, a breakthrough result of Mahadev [23] has solved an open problem of verifying quantum computation by a fully classical computer. Specifically, she has constructed a measurement protocol such that a classical verifier can verify that a quantum prover behaves as a trusted Pauli  $X$  or  $Z$  basis measurement device. Applying the measurement protocol to a verification protocol for the class of quantumly tractable problems (BQP), Mahadev has proposed an interactive protocol between an efficient classical (BPP) verifier and an efficient quantum (BQP) prover such that the verifier can verify the result of the BQP computation. Soundness of Mahadev's protocol originates from a widely recognized computational assumption that the learning with errors (LWE) problem is hard for any efficient quantum algorithm. Inspired by Mahadev's protocol, several classical verification of quantum computation (CVQC) protocols with preferable properties and functionality have been proposed. Alagic *et al.* have utilized parallel repetition to construct a CVQC protocol with a negligible soundness [24]. Gheorghiu *et al.* have proposed a blind CVQC protocol [25]. Chung *et al.* have applied Mahadev's protocol to quantum sampling [26]. Zhang has given a CVQC protocol with linear time complexity [27].

Our contributions can be summarized as follows.

(1) We propose a classical verification of multibasis measurement protocol, where a classical verifier interacts with a BQP prover to force the prover to behave as the verifier's trusted Pauli  $Z$  basis or Pauli basis  $X, Y, (X + Y)/\sqrt{2}, (X - Y)/\sqrt{2}$  ( $XY$ -plane basis) measurement device. Without the use of trapdoor injective family, the feasibility of our measurement protocol is based on noisy trapdoor claw-free functions that are existent under LWE assumption.

(2) A comprehensive analysis is presented to prove the completeness and soundness of our measurement protocol. The completeness indicates that, if the prover follows the measurement protocol honestly, the output distribution in measurement round is close to the distribution obtained by measuring the target state in the designated basis. The soundness indicates if a dishonest prover always passes the check of the verifier, then there exists a quantum state  $\rho$ , which is independent of the verifier's measurement basis  $h$ , such that the output distribution of the measurement protocol is computationally indistinguishable from the distribution obtained by measuring  $\rho$  according to  $h$ .

(3) We apply our measurement protocol to the verification of graph states [28] and propose two device-noise-independent verification protocols of graph states. Compared with existing protocols, the newly proposed protocols are robust to the noise of quantum device and have removed the requirement for multiple noncommunicating provers that share entanglement.

(4) We use our measurement protocol to obtain a CVQC protocol with a lower constant soundness. The soundness that indicates the maximum probability of accepting wrong results has been reduced from 0.75 to 0.5757.

The remainder of this paper is organized as follows. In Sec. II, we give some basic notations and definition of noisy trapdoor claw-free functions. In Sec. III, we use the above cryptographic primitive to construct a measurement protocol for verifying the computational basis or the  $XY$ -plane basis measurement. In addition, we prove the completeness and

soundness of our measurement protocol. In Sec. IV, we show how to apply our measure protocol to verification of graph states and verifiable delegated quantum computing. We then conclude, in Sec. V, with some discussions and open problems.

## II. PRELIMINARIES

### A. Notations

For any finite set  $X$ , let  $x \stackrel{U}{\leftarrow} X$  denote a uniformly random element drawn from  $X$ . For any density function  $f$  on domain  $X$ , let  $\text{supp}(f) = \{x \in X | f(x) > 0\}$  denote the support of  $f$  and let  $x \leftarrow f$  denote a sample from the distribution corresponding to density function  $f$ . The total variation distance between density functions  $f_1$  and  $f_2$  is

$$D_{TV}(f_1, f_2) = \frac{1}{2} \sum_{x \in X} |f_1(x) - f_2(x)|. \quad (1)$$

The Minkowski distance between density functions  $f_1$  and  $f_2$  is

$$D_{L_p}(f_1, f_2) = \left( \sum_{x \in X} |f_1(x) - f_2(x)|^p \right)^{1/p}, \quad (2)$$

where  $p$  is a positive integer, and the Minkowski distance becomes the Euclidean distance when  $p = 2$ . The trace distance between quantum states  $\rho_1$  and  $\rho_2$  is defined to be

$$D_{Tr}(\rho_1, \rho_2) = \frac{1}{2} \text{Tr}(\sqrt{(\rho_1 - \rho_2)^2}). \quad (3)$$

The rotation operator  $R_z(\theta)$  is equal to  $\cos \frac{\theta}{2} I - i \sin \frac{\theta}{2} Z$ . A function  $\mu(\lambda) : \mathbb{N} \rightarrow \mathbb{R}_+$  is negligible if, for every polynomial  $p(\lambda)$ ,  $\lim_{\lambda \rightarrow \infty} p(\lambda)\mu(\lambda) = 0$  holds. We say the density function  $f_1$  is computationally indistinguishable from the density function  $f_2$  if for any BQP attackers  $\mathcal{A}$  there exists a negligible function  $\mu$  such that

$$| \Pr_{x \leftarrow f_1} [\mathcal{A}(x) = 0] - \Pr_{x \leftarrow f_2} [\mathcal{A}(x) = 0] | \leq \mu. \quad (4)$$

We say the density matrix  $\rho_1$  is computationally indistinguishable from the distribution  $\rho_2$  if for any efficiently computable CPTP maps  $\mathcal{S}$  there exists a negligible function  $\mu$  such that

$$| \text{Tr}(|0\rangle\langle 0| \otimes I) \mathcal{S}(\rho_1 - \rho_2) | \leq \mu. \quad (5)$$

### B. Noisy trapdoor claw-free functions

Here, we introduce the notion of noisy trapdoor claw-free functions (NTCFs) [23, 25, 29]. We summarize the algorithms used in the NTCF family as follows.

*Definition 1 (Decoding algorithms [30]).* The decoding algorithms of the NTCF family  $\mathcal{F} = \{f_{k,b}\}_{k,b}$  are given by the following.

(1) A function generation algorithm  $\text{GEN}_{\mathcal{F}}$  is used to generate a key  $k \in \mathcal{K}_{\mathcal{F}}$  and a trapdoor  $t_k$ .

(2) For an input consisting of a trapdoor  $t_k$ , a bit  $b \in \{0, 1\}$ , and an image  $y \in \mathcal{Y}$ , if the condition  $y \in \text{supp}[f_{k,b}(x)]$  holds, the output of the algorithm  $\text{INV}_{\mathcal{F}}$  is  $x$ .

(3) For an input consisting of a key  $k \in \mathcal{K}_{\mathcal{F}}$ , a bit  $b \in \{0, 1\}$ , a preimage  $x \in \mathcal{X}$ , and an image  $y \in \mathcal{Y}$ , the output of the algorithm  $\text{CHK}_{\mathcal{F}}$  is 1 if  $y \in \text{supp}[f_{k,b}(x)]$  and 0 otherwise.

(4) For an input consisting of a key  $k \in \mathcal{K}_{\mathcal{F}}$  and a bit  $b \in \{0, 1\}$ , the output of the algorithm  $\text{SAMP}_{\mathcal{F}}$  is a state that is

negligibly close to

$$\frac{1}{\sqrt{|\mathcal{X}|}} \sum_{x \in \mathcal{X}, y \in \mathcal{Y}} \sqrt{[f_{k,b}(x)](y)|x\rangle|y\rangle}. \quad (6)$$

We present two important adaptive hardcore bit properties that will be used to prove the soundness of measurement protocol.

*Definition 2 (Adaptive hardcore bit [30,31]).* For convenience, let  $\mathcal{X} = \{0, 1\}^w$ , where  $w$  is the polynomially bounded function of security parameter  $\lambda$  and a multiple of 3.

(1) There is an efficiently computable injection  $J : \mathcal{X} \rightarrow \mathbb{Z}_8^{w/3}$ , such that  $J$  can be inverted efficiently on its range. For any quantum polynomial-time procedure  $\mathcal{A}$ , there exists a negligible function  $\mu(\cdot)$  such that

$$\left| \Pr_{(k,t_k) \leftarrow \text{GEN}_{\mathcal{F}}(1^\lambda)} [\mathcal{A}(k) \in H_k] - \Pr_{(k,t_k) \leftarrow \text{GEN}_{\mathcal{F}}(1^\lambda)} [\mathcal{A}(k) \in \overline{H}_k] \right| \leq \mu(\lambda), \quad (7)$$

where

$$H_k = \{(b, x_b, d, d[J(x_0) \oplus J(x_1)]) \mid b \in \{0, 1\}, f_{k,0}(x_0) = f_{k,1}(x_1), d \stackrel{U}{\leftarrow} \mathbb{Z}_8^{w/3}\}, \quad (8)$$

$$\overline{H}_k = \{(b, x_b, d, s \oplus 4) \mid (b, x_b, d, s) \in H_k\}. \quad (9)$$

(2) For all  $k \in \mathcal{K}_{\mathcal{F}}$  and  $\hat{d} \in \{0, 1\}^w$ , let

$$H'_{k,\hat{d}} = \{\hat{d}(x_0 \oplus x_1) \mid f_{k,0}(x_0) = f_{k,1}(x_1)\}. \quad (10)$$

For a fixed string  $\hat{d} \in \{0, 1\}^w$  and any quantum polynomial-time procedure  $\mathcal{A}$ , there exists a negligible function  $\mu(\cdot)$  such that

$$\left| \Pr_{(k,t_k) \leftarrow \text{GEN}_{\mathcal{F}}(1^\lambda)} [\mathcal{A}(k) \in H'_{k,\hat{d}}] - \frac{1}{2} \right| \leq \mu(\lambda). \quad (11)$$

Note that the addition and inner product are taken modulo 8 in the first adaptive hardcore bit property and taken modulo 2 in the second adaptive hardcore bit property. Mahadev [23,30] has proved that, under the hardness assumption of solving LWE, there exists a function family  $\mathcal{F}_{\text{LWE}}$  satisfying the second adaptive hardcore bit property, i.e., Eq. (7). Gheorghiu *et al.* [25,31] have proved that  $\mathcal{F}_{\text{LWE}}$  also satisfies the first adaptive hardcore bit property, i.e., Eq. (11).

The learning with errors (LWE) assumption indicates that the distribution  $(A, As + e)$  are computationally indistinguishable from the distribution  $(A, u)$ , where the matrix  $A$  is uniformly random in  $\mathbb{Z}_q^{n \times m}$ , the row vector  $s$  is uniformly random in  $\mathbb{Z}_q^n$ , the noise vector  $e$  is uniformly random in  $\mathbb{Z}_q^m$ , and the vector  $u$  is uniformly random in  $\mathbb{Z}_q^m$ . Here, the noise  $e$  computationally hides  $s$ . With the help of LWE assumption, the noisy trapdoor claw-free function pair can be constructed as follows. According to an LWE sample  $(A, As + e)$ , the NTCF pair is defined by  $f_0(x) = Ax + e_0$  and  $f_1(x) = Ax + e_0 + As + e$ , where  $e_0$  is a random vector. Note that  $f_1(x) = A(x + s) + e_0 + e$ . If we set  $e$  to be 0, then  $f_1(x) = f_0(x + s)$ . Sampling  $e_0$  from a Gaussian much wider than  $e$  can guarantee that the distribution  $f_1(x)$  is statistically close to the distribution  $f_0(x + s)$ . Assume one knows both  $x_0$  and  $x_1$ . Since it holds that  $x_1 = x_0 - s$ , the secret  $s$  is leaked,

a contradiction with the LWE assumption. The adaptive hardcore bit properties of the NTCF family are a stronger form of the claw-free property, which can be guaranteed by the LWE assumption in a similar way.

### III. MEASUREMENT PROTOCOL

In this section, we use the noisy trapdoor claw-free functions  $\mathcal{F}$  in Sec. II to design our measurement protocol. The measurement protocol can realize the verification of the measurement corresponding to a basis choice  $h \in \{0, 1, \dots, 4\}^n$  on an  $n$ -qubit state  $\rho$ . Here,  $h_i = 0$  means that the prover is required to measure the  $i$ th qubit of  $\rho$  in the computational basis and  $h_i = j, j \in \{1, \dots, 4\}$ , means that the prover is required to measure the  $i$ th qubit of  $\rho$  in the rotation basis  $\{|+\phi_j\rangle, |-\phi_j\rangle\}$ , where  $\phi_j = (j - 1)\pi/4$  and  $|\pm\phi_j\rangle = (|0\rangle \pm e^{i\phi_j}|1\rangle)/\sqrt{2}$ . Our measurement protocol is given by Protocol 1. For a state  $|\psi\rangle = \alpha_0|0\rangle|\psi_0\rangle + \alpha_1|1\rangle|\psi_1\rangle$ , the effect of  $\text{SAMP}_{\mathcal{F}}$  on the first qubit of  $|\psi\rangle$  will lead to a state that is negligibly close to

$$\frac{1}{\sqrt{|\mathcal{X}|}} \sum_{\substack{b \in \{0, 1\} \\ x \in \mathcal{X}, y \in \mathcal{Y}}} \alpha_b \sqrt{[f_{k,b}(x)](y)} |b\rangle|x\rangle|\psi_b\rangle|y\rangle. \quad (12)$$

We call the first qubit the committed qubit, the register that contains  $x$  the preimage register, and the string  $y$  the commitment string. The effect of  $\text{SAMP}_{\mathcal{F}}$  on the other qubits of  $|\psi\rangle$  is similar.

*Protocol 1 (Multibasis measurement protocol).*

(1) Verifier  $\rightarrow$  Prover. For  $1 \leq i \leq n$ , the verifier runs algorithm  $\text{GEN}_{\mathcal{F}}$  to produce a pair of a function key  $k_i \in \mathcal{K}_{\mathcal{F}}$  and its trapdoor  $t_{k_i}$ . The verifier sends the function descriptions  $k' = (k_1, \dots, k_n)$  to the prover.

(2) Prover  $\rightarrow$  Verifier. The prover initializes registers and runs algorithm  $\text{SAMP}_{\mathcal{F}}$  to prepare a state in uniform superposition. The prover then measures the registers containing the commitment string and sends the outcome  $y' = (y_1, \dots, y_n)$  to the verifier.

(3) Prover  $\rightarrow$  Verifier. Start a computational basis measurement round. For all  $i$  satisfying  $h_i = 0$ , the prover measures committed qubit  $i$  and preimage register  $i$  in the computational basis, and sends a bit  $b'_i$  and a string  $x'_i$  to the verifier.

(4) Verifier (Output). If  $\text{CHK}_{\mathcal{F}}(k_i, b'_i, x'_i, y_i) = 1$ , the verifier stores  $m_i = b'_i$  as the computational basis measurement result of the  $i$ th qubit. Otherwise, the verifier stores a random bit as the measurement result and rejects.

(5) Verifier  $\rightarrow$  Prover. The verifier chooses to run a test round with probability  $\beta$  and run a rotation basis measurement round with probability  $1 - \beta$ , where  $0 < \beta < 1$ . The verifier then sends the round choice to the prover.

(6) Prover  $\rightarrow$  Verifier. For the test round, for all  $i$  satisfying  $h_i \neq 0$ , the prover measures committed qubit  $i$  and preimage register  $i$  in the computational basis, and sends a bit  $b''_i$  and a string  $x''_i$  to the verifier.

(7) Verifier. If  $\text{CHK}_{\mathcal{F}}(k_i, b''_i, x''_i, y_i) = 0$ , the verifier rejects.

(8) Verifier. For the rotation basis measurement round, for all  $i$  satisfying  $h_i \neq 0$ , the verifier computes the two inverses  $x_{0,y_i}$  and  $x_{1,y_i}$  of  $y_i$  by the algorithm  $\text{INV}_{\mathcal{F}}$ . If either of the

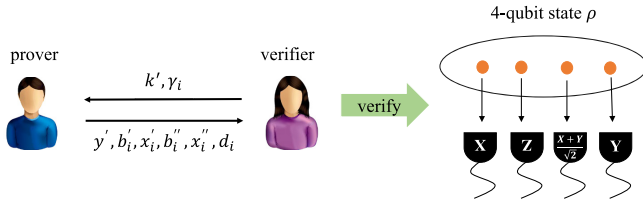


FIG. 1. Example of Protocol 1. The classical verifier interacts with a quantum prover by classical messages to verify a four-qubit state  $\rho$  is measured in the designated basis.

inverses does not exist, the verifier stores a random bit as the measurement result and rejects.

(9) Prover  $\rightarrow$  Verifier. The prover performs the map  $J$  on the preimage register  $i$ , measures it in the Fourier (over  $\mathbb{Z}_8$ ) basis, and then sends a string  $d_i$  to the verifier.

(10) Verifier  $\rightarrow$  Prover. The verifier then chooses at random a bit  $c_i \in \{0, 1\}$  and keeps it secret to the prover. The verifier sends a bit  $\gamma_i$  to the prover, where

$$\gamma_i = \theta_i + \pi d_i [J(x_{0,y_i}) \oplus J(x_{1,y_i})] / 4 + c_i \pi. \quad (13)$$

(11) Prover  $\rightarrow$  Verifier. The prover measures committed qubit  $i$  and preimage register  $i$  in the basis  $\{|+\gamma_i\rangle, |-\gamma_i\rangle\}$  and sends a bit  $b'_i$  to the verifier.

(12) Verifier (Output). The verifier stores  $m_i = b'_i \oplus c_i$  as the  $\{|+\theta_i\rangle, |-\theta_i\rangle\}$  basis measurement result of the  $i$ th qubit.

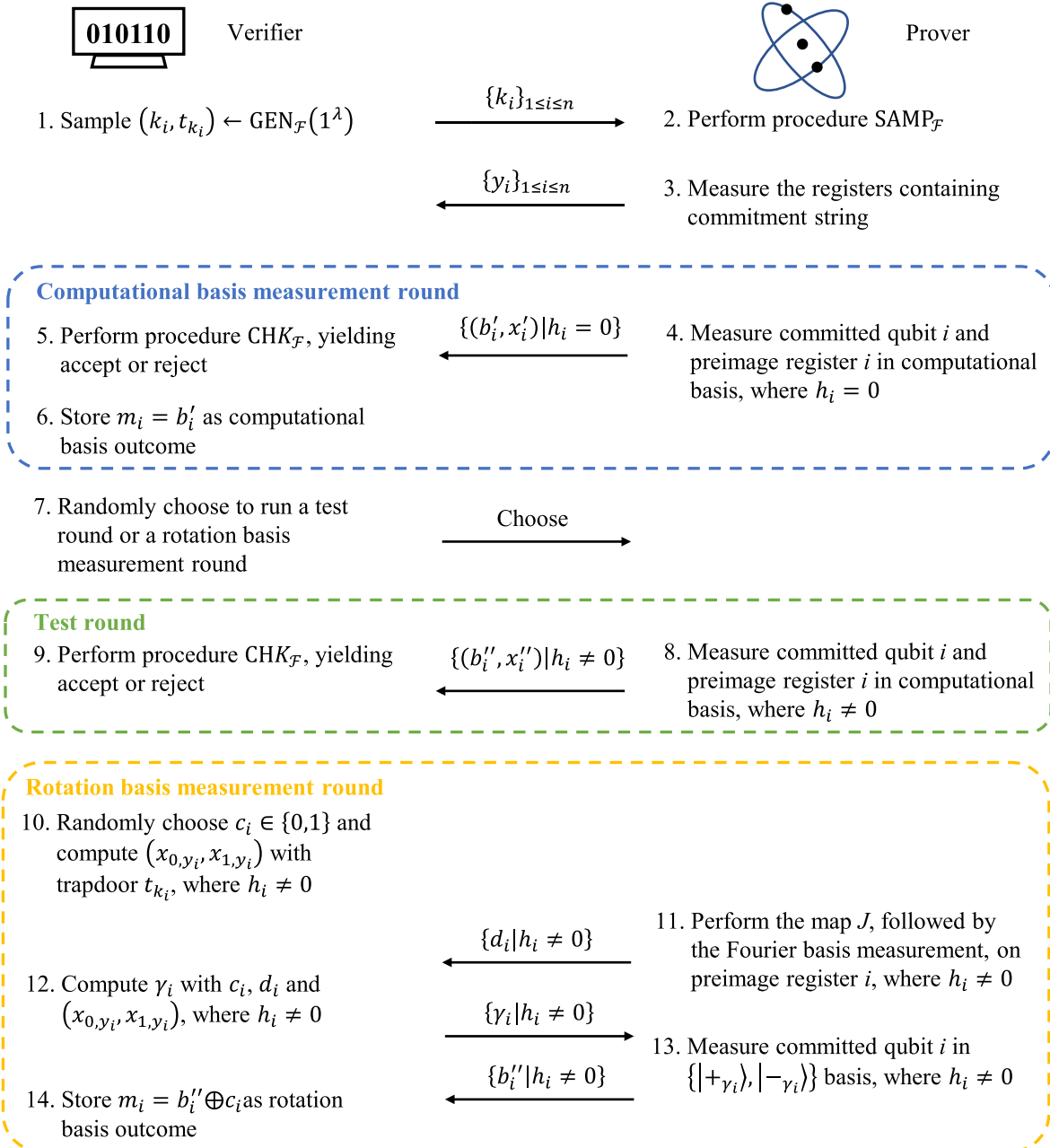


FIG. 2. Schematic representation of our measurement protocol.

Our measurement protocol for a basis choice  $h = (1, 0, 2, 3)$  is shown in Fig. 1, where the verifier sends classical messages  $k', \gamma_i$  to the prover and the prover sends classical messages  $y', b'_i, x'_i, b''_i, x''_i, d_i$  to the verifier. In Fig. 2 we give the formal description of our measurement protocol. We now give some notation for convenience of describing the properties of the measurement protocol. If Protocol 1 has executed the computational basis measurement round and the rotation basis measurement round, then it is called type-I measurement protocol. If Protocol 1 has executed the computational basis measurement round and the test round, then it is called type-II measurement protocol.  $f_{\mathbb{V},h}$  represents the probability density function over keys produced by the algorithm  $\text{GEN}_{\mathcal{F}}$ . A prover is perfect if the prover is always accepted in the type-II measurement protocol.  $f_{\rho,h}$  represents the probability density function over results obtained by measuring the state  $\rho$  in the basis corresponding to  $h$ .  $f_{\mathbb{P},h}$  represents the probability density function over measurement results  $m \in \{0, 1\}^n$  from the type-I measurement protocol with respect to the prover  $\mathbb{P}$ .  $f'_{\mathbb{P},h}$  represents the probability density function over measurement results from the type-I measurement protocol that is accepted by the verifier.  $\sigma_{\mathbb{P},h} = \sum_m f_{\mathbb{P},h}(m)|m\rangle\langle m|$  represents the density matrix with respect to the density function  $f_{\mathbb{P},h}$ .

**A. Completeness of measurement protocol**

The completeness of Protocol 1 is given by Theorem 1.

*Theorem 1.* For all  $n$  qubits states  $\rho$  and for all basis choices  $h \in \{0, 1, 2, 3, 4\}^n$ , an honest prover  $\mathbb{P}$  in Protocol 1 will be accepted by the verifier with probability negligibly close to 1. Moreover, there exists a negligible function  $\mu$  such that

$$D_{TV}(f_{\mathbb{P},h}, f_{\rho,h}) \leq \mu. \tag{14}$$

*Proof.* Consider the case that the prover is honest. The initial state is

$$|\psi\rangle = \sum_{b \in \{0,1\}} \alpha_b |b\rangle |\psi_b\rangle. \tag{15}$$

Take the correctness of the measurement on the first qubit of  $|\psi\rangle$  as an example. Upon receipt of a key  $k$ , the prover performs the  $\text{SAMP}_{\mathcal{F}}$  procedure in superposition and measures the outcome  $y$ . The result state is within negligible trace distance of the state

$$\sum_{b \in \{0,1\}} \alpha_b |b\rangle |x_{b,y}\rangle |\psi_b\rangle, \tag{16}$$

where  $x_{b,y} = \text{INV}_{\mathcal{F}}(t_k, b, y)$ .

If the prover performs the computational basis measurements of committed qubit and preimage register and returns  $(b, x_{b,y})$ , it acts as a standard basis measurement of the first qubit of  $|\psi\rangle$ . This means that the verifier will obtain correct standard basis measurement outcome in step (4) of measurement protocol for  $h_1 = 0$ .

If the prover implements the map  $J$  on the preimage register and then measures it in the Fourier (over  $\mathbb{Z}_8$ ) basis, the postmeasurement state (see Refs. [25,31]) is

$$(R_Z\{\pi d[J(x_{0,y}) \oplus J(x_{1,y})]/4\} \otimes I)|\psi\rangle. \tag{17}$$

This means that the verifier will get the correct  $\{|+\theta\rangle, |-\theta\rangle\}$  basis measurement outcome in step (12) of the measurement protocol for  $h_1 \neq 0$ .

If the negligible deviation caused by the  $\text{SAMP}_{\mathcal{F}}$  procedure is ignored, the verifier will accept the honest prover  $\mathbb{P}$  in all rounds of the measurement protocol. In addition, the density function  $f_{\mathbb{P},h}$  is the same as the density function  $f_{\rho,h}$ . Taking account of the above deviation, which is denoted by a negligible function  $\mu$ , the completeness is derived. ■

**B. Prover’s behavior**

We now model the behavior of an arbitrary prover in Protocol 1, and discuss the relation between the prover’s behavior and an underlying quantum state.

According to the principle [23,30] that a prover  $\mathbb{P}$  in a round that begins with the verifier’s message and ends with the prover’s message behaves exactly the same as a prover that applies one unitary operator and then performs an ideal measurement, the behavior of an arbitrary prover  $\mathbb{P}$  in Protocol 1 can be described as follows.

(1) The prover  $\mathbb{P}$  applies one unitary operator  $U_Z$  to his initial state  $\rho_0$ .  $\mathbb{P}$  then measures the commitment string registers, followed by the measurements of the computational basis measurement round.

(2) For a type-I measurement protocol, (a) the prover  $\mathbb{P}$  successively applies one unitary operator  $U_F$  and the Fourier basis measurements to his entire state and (b) the prover  $\mathbb{P}$  successively applies one unitary operator  $U_R$  and the rotation basis measurements on his entire state.

(3) For a type-II measurement protocol, the prover  $\mathbb{P}$  applies one unitary operator  $U_T$  to his entire state, followed by the measurements of the test round.

Note that the measurements before and after the unitary  $U_T$  are of the same type; this implies that  $U_T$  commutes with the measurements of the computational basis measurement round. In addition, the positions that the Fourier basis measurements act on are separated from the positions that the rotation basis measurements act on. It can be inferred that the unitary  $U_R$  commutes with the Fourier basis measurements. Let  $U_1 = U_T U_Z, U_2 = U_R U_F U_T^\dagger U_J^\dagger$ , where  $U_J$  is one unitary operator corresponding to map  $J$ . The behavior of the prover  $\mathbb{P}$  is equivalent to the following.

(1) The prover  $\mathbb{P}$  applies one unitary operator  $U_1$  to his initial state  $\rho_0$ .  $\mathbb{P}$  then measures the commitment string registers, followed by the measurements of the computational basis measurement round.

(2) For a type-I measurement protocol, the prover  $\mathbb{P}$  successively applies the unitary operator  $U_J$  and one unitary operator  $U_2$  on his entire state.  $\mathbb{P}$  successively performs the Fourier basis measurements and the rotation basis measurements.

(3) For a type-II measurement protocol, the prover  $\mathbb{P}$  performs the measurements of the test round.

Consider a particular prover  $\mathbb{P}$  who applies an additional operator  $U_3$  to  $n$  committed qubits before the measurements of the partial committed qubits in the rotation basis measurement round. Moreover,  $\mathbb{P}$  can pass the computational basis measurement round and the test round perfectly. The attacks  $U_2$  and  $U_3$  commute with the computational basis measurement

on  $n$  committed qubits. We say the above prover  $\mathbb{P}$  is *normal*. The following theorem then holds.

*Theorem 2.* For all normal provers  $\mathbb{P}$  and all  $h \in \{0, 1, 2, 3, 4\}^n$ , there is an  $n$ -qubit state  $\rho$  such that the density function  $f_{\mathbb{P},h}$  is equivalent to the density function  $f_{\rho,h}$ , where the construction of state  $\rho$  is described below.

- (1) Execute step (1) of the behavior of the prover  $\mathbb{P}$ .
- (2) Perform the map  $J$  on  $n$  preimage registers.
- (3) Apply the unitary operators  $U_2$  to the entire state.
- (4) Measure  $n$  preimage registers in the Fourier basis to get outcomes  $d_1, \dots, d_n$ .
- (5) Apply the unitary  $U_3$  to  $n$  committed qubits.
- (6) For  $1 \leq i \leq n$ , apply the unitary  $R_Z\{-\pi d_i[J(x_{0,y_i}) \oplus J(x_{1,y_i})]/4\}$  to the  $i$ th committed qubit.
- (7) Trace out all qubits except  $n$  committed qubits.

*Proof.* As for  $h_i = 0$ , measuring the  $i$ th qubit of  $\rho$  in the computational basis can be transferred to measuring in the computational basis the  $i$ th committed qubit after the step (1) due to the fact that the operations of steps (2)–(7) commute with the computational basis measurement on  $n$  committed qubits. Therefore, the density function of the  $i$ th bit of  $f_{\rho,h}$  is equal to the density function of the  $i$ th bit of  $f_{\mathbb{P},h}$ .

As for  $h_i \neq 0$ , the density function of the  $i$ th bit of  $f_{\mathbb{P},h}$  is obtained from measuring the  $i$ th committed qubit in the  $\{|+\theta'_i\rangle, |-\theta'_i\rangle\}$  basis, where  $\theta'_i = \theta_i + \pi d_i[J(x_{0,y_i}) \oplus J(x_{1,y_i})]/4$ . It is equivalent to applying one unitary operator  $R_Z\{-\pi d_i[J(x_{0,y_i}) \oplus J(x_{1,y_i})]/4\}$ , followed by the  $\{|+\theta_i\rangle, |-\theta_i\rangle\}$  basis measurement. This just reflects the density function of the  $i$ th bit of  $f_{\rho,h}$ . ■

### C. General to $X$ -trivial attack for rotation basis measurement round

In the following we will prove that for an arbitrary perfect prover  $\mathbb{P}$  in Protocol 1, there exists a normal prover  $\mathbb{P}'$  such that  $f_{\mathbb{P},h}$  is computationally indistinguishable from  $f_{\mathbb{P}',h}$ .

We use  $(U_1, U_2, U_3)$  to describe a prover  $\mathbb{P}$ . It means that  $\mathbb{P}$  applies the unitary  $U_1$  before measuring the commitment string registers, the unitary  $U_2$  before the Fourier basis measurements, and the unitary  $U_3$  before the rotation basis measurements. With this at hand, we can state our result that is similar to Refs. [23,30].

*Theorem 3.* For  $1 \leq i \leq n$ , let  $\mathcal{E} = \{E_j\}_j$  and  $\mathcal{E}_i = \{E_{x,j}\}_{x \in \{0,1\}, j}$  be CPTP maps expressed as the Kraus decomposition:

$$E_j = I \otimes E_j^{00} + X \otimes E_j^{10} + Z \otimes E_j^{01} + XZ \otimes E_j^{11}, \quad (18)$$

$$E_{x,j} = I \otimes E_j^{x0} + Z \otimes E_j^{x1}, \quad (19)$$

where the Pauli operators  $I, X, Z, XZ$  are applied on the  $i$ th committed qubit. Let a perfect prover  $\mathbb{P}$  be characterized by  $(U_1, \mathcal{E}, I)$ . There exists a perfect prover  $\mathbb{P}_i$  characterized by  $(U_1, \mathcal{E}_i, U_3)$  such that  $f_{\mathbb{P},h}$  is computationally indistinguishable from  $f_{\mathbb{P}_i,h}$ , where  $U_3$  is one unitary operator that commutes with computational basis measurement on  $n$  committed qubits.

*Proof.* For simplicity, we just prove the case for  $i = 1$ . It is easy to confirm the remaining cases.

We first consider the computational indistinguishability for  $h_1 \neq 0$ . Recall the behavior of the prover  $\mathbb{P}$ . Let state  $|\Phi_y\rangle$  be

written as

$$|0\rangle|J(x_{0,y})\rangle|\psi_{0,y}\rangle|y\rangle + |1\rangle|J(x_{1,y})\rangle|\psi_{1,y}\rangle|y\rangle, \quad (20)$$

where  $y \in \bigcup_{b \in \{0,1\}, x \in \mathcal{X}} \text{supp}[f_{k,b}(x)]$ ,  $x_{b,y} = \text{INV}_{\mathcal{F}}(t_k, b, y)$ , and  $|\psi_{b,y}\rangle$  represents the remaining qubits. Note that the perfect prover  $\mathbb{P}$  can pass the check of the computational basis measurement round and the test round. After the measurements of computational basis measurement round and the application of the map  $J$ , the state shared between the prover and verifier is

$$\sum_y |\Phi_y\rangle\langle\Phi_y|. \quad (21)$$

The CPTP map  $\mathcal{E} = \{E_j\}_j$  followed by the Fourier (over  $\mathbb{Z}_8$ ) basis measurement (the CPTP map written as  $\{|d\rangle\langle d|U_P\}_d$ ) of the first preimage register, the  $\{|+\gamma\rangle, |-\gamma\rangle\}$  basis measurements (the CPTP map written as  $\{|b\rangle\langle b|HR_Z(-\gamma)\}_b$ ) of the first committed qubit, and the verifier's decoding (the Pauli operator  $X^c$  acting on the first committed qubit) will result in the state  $\rho_1$  that can be written as

$$\sum_{\substack{b,c,d,j \\ y \in \Delta_{c,d}}} [|b\rangle\langle b|X^cHR_Z(-\gamma) \otimes |d\rangle\langle d|U_P \otimes I]E_j|\Phi_y\rangle \times \langle\Phi_y|E_j^\dagger[|b\rangle\langle b|X^cHR_Z(-\gamma) \otimes |d\rangle\langle d|U_P \otimes I]^\dagger, \quad (22)$$

where

$$\Delta_{c,d} = \left\{ y \in \bigcup_{b,x} \text{supp}[f_{k,b}(x)] \mid \gamma - \theta - \pi d[J(x_{0,y}) \oplus J(x_{1,y})]/4 / \pi = c \right\}. \quad (23)$$

In other words, the state corresponding to a prover  $\mathbb{P}$  characterized by  $(U_1, \mathcal{E}, I)$  is  $\rho_1$ . Let  $F_{b,c,d,j} = [|b\rangle\langle b|X^cHR_Z(-\gamma) \otimes |d\rangle\langle d|U_P \otimes I]E_j$ . We can rewrite

$$\rho_1 = \sum_{\substack{b,c,d,j \\ y \in \Delta_{c,d}}} F_{b,c,d,j}|\Phi_y\rangle\langle\Phi_y|F_{b,c,d,j}^\dagger. \quad (24)$$

From the  $Z$  Pauli Twirl Lemma [23,30], the following two CPTP maps are equal:

$$\left\{ \frac{1}{\sqrt{2}}(Z^r \otimes I)E_j(Z^r \otimes I) \right\}_{r,j} = \{(X^x \otimes I)E_{x,j}\}_{x,j}. \quad (25)$$

Consider that above CPTP maps are followed by the Fourier basis measurement of the first preimage register and the rotation basis measurement of the first committed qubit. Using the facts that  $R_Z(-\gamma)X = XR_Z(\gamma)$  and the Pauli  $Z$  operator has no effect on the computational basis measurement, we have

$$\begin{aligned} & \left\{ \frac{1}{\sqrt{2}} [|b\rangle\langle b|HR_Z(-\gamma) \otimes |d\rangle\langle d|U_P \otimes I] \right. \\ & \quad \left. \times (Z^r \otimes I)E_j(Z^r \otimes I) \right\}_{b,d,r,j} \\ & = \{ [|b\rangle\langle b|HR_Z(-\gamma)R_Z\{((-1)^{x+1} + 1)\gamma\} \\ & \quad \otimes |d\rangle\langle d|U_P \otimes I]E_{x,j}\}_{b,d,x,j}. \end{aligned} \quad (26)$$

The operator  $R_Z\{[(-1)^{x+1} + 1]\gamma\}$  acting on the first committed qubit has uniquely defined the unitary  $U_3$  that the theorem requires. The state corresponding to a prover  $\mathbb{P}_1$  characterized by  $(U_1, \mathcal{E}_1, U_3)$  is

$$\sum_{\substack{b,c,d,x,j \\ y \in \Delta_{c,d}}} (F'_{b,c,d,x,j})|\Phi_y\rangle\langle\Phi_y|(F'_{b,c,d,x,j})^\dagger, \quad (27)$$

where  $F'_{b,c,d,x,j}$  is defined as

$$(|b\rangle\langle b|X^cHR_Z(-\gamma)R_Z\{[(-1)^{x+1} + 1]\gamma\} \otimes |d\rangle\langle d|U_P \otimes I)E_{x,j}. \quad (28)$$

In order to prove that  $f_{\mathbb{P},h}$  is computationally indistinguishable from  $f_{\mathbb{P}_1,h}$ , it suffices to show that the state  $\rho_1$  is computationally indistinguishable from the state  $\rho_2$ .

Let

$$\mathcal{E}_r = \sum_{\substack{b,c,d,j \\ y \in \Delta_{c,d}}} F_{b,c \oplus r,d,j} \tilde{\rho}_y F_{b,c \oplus r,d,j}^\dagger, \quad (29)$$

$$\mathcal{E}'_r = \sum_y (Z^r \otimes I)|\Phi_y\rangle\langle\Phi_y|(Z^r \otimes I), \quad (30)$$

where  $\tilde{\rho}_y$  is the diagonal term of  $|\Phi_y\rangle\langle\Phi_y|$ , i.e.,

$$\tilde{\rho}_y = \sum_b [ |b\rangle\langle b|J(x_{b,y})|\psi_{b,y}\rangle\langle\psi_{b,y}|y\rangle][ |b\rangle\langle b|J(x_{b,y})|\psi_{b,y}\rangle\langle\psi_{b,y}|y\rangle]^\dagger. \quad (31)$$

Similar to Refs. [23,30], the problem can be reduced to proving that  $\mathcal{E}_0$  is computationally indistinguishable from  $\mathcal{E}_1$  and that  $\mathcal{E}'_0$  is computationally indistinguishable from  $\mathcal{E}'_1$ .

Assume  $\mathcal{E}_0$  is computationally distinguishable from  $\mathcal{E}_1$ . There exists efficiently computable CPTP maps  $\mathcal{S}$  such that for all negligible function  $\mu$ ,

$$|\text{Tr}(|0\rangle\langle 0| \otimes I)\mathcal{S}(\mathcal{E}_0 - \mathcal{E}_1)| > \mu. \quad (32)$$

We now construct a quantum attacker  $\mathcal{A}$  that breaks the hardcore bit property of  $\mathcal{F}$ .

- (1)  $\mathcal{A}$  follows step (1) of the behavior of the prover  $\mathbb{P}$ .
- (2)  $\mathcal{A}$  measures the first committed qubit and first preimage register in the computational basis, storing the measurement outcomes  $(b, x_{b,y})$ .
- (3)  $\mathcal{A}$  follows step (2) of the behavior of the prover  $\mathbb{P}$ , storing the Fourier basis measurement outcome  $d$ .
- (4)  $\mathcal{A}$  chooses a bit  $c' \in \{0, 1\}$  uniformly at random and performs the Pauli operator  $X^{c'}$  to the first committed qubit.
- (5)  $\mathcal{A}$  applies the CPTP map  $\mathcal{S}$ , followed by the computational basis measurement of the first committed qubit.  $\mathcal{A}$  stores the measurement outcome  $s$ .

(6)  $\mathcal{A}$  outputs  $\{b, x_{b,y}, d, 4[\gamma - \theta - (c' \oplus s)\pi]/\pi\}$ .

Similar to Refs. [23,30], it is easy to check that  $\mathcal{A}$  breaks the first hardcore bit property of  $\mathcal{F}$ , i.e., Eq. (7).

Assume  $\mathcal{E}'_0$  is computationally distinguishable from  $\mathcal{E}'_1$ . It means that there exists an attacker  $\mathcal{A}'$  who can distinguish whether or not a Pauli Z operator acts on the first committed qubit of  $|\Phi_y\rangle\langle\Phi_y|$ . We now construct the behavior of the quantum attacker  $\mathcal{A}'$  as follows.

- (1)  $\mathcal{A}'$  follows step (1) of the behavior of the prover  $\mathbb{P}$ .
- (2)  $\mathcal{A}'$  applies the operator  $Z^{\hat{d}}$  acting on the first preimage register, where  $\hat{d}$  is an arbitrary selected bit string.

(3)  $\mathcal{A}'$  applies  $U_J$  to the first preimage register.

The final state of the attacker  $\mathcal{A}'$  is

$$\sum_y (Z^{\hat{d}(x_{0,y} \oplus x_{1,y})} \otimes I)|\Phi_y\rangle\langle\Phi_y|(Z^{\hat{d}(x_{0,y} \oplus x_{1,y})} \otimes I). \quad (33)$$

According to Refs. [23,30], it shows that  $\mathcal{A}'$  can determine the bit  $\hat{d}(x_{0,y} \oplus x_{1,y})$ . It is a contradiction with the second hardcore bit property of  $\mathcal{F}$ , i.e., Eq. (11).

Consider the computational indistinguishability for  $h_1 = 0$ . Since the density function of the first bit of  $f_{\mathbb{P},h}$  depends on the computational basis measurement of the first committed qubit before the application of the CPTP map  $\mathcal{E}$ , the attacks applied in the rotation basis measurement round have no effect on the density function. ■

Theorem 3 shows that replacing the attacks of the rotation basis measurement round with the attacks acting  $X$  trivially on the  $i$ th committed qubit will not change the density function over measurement outcomes. Generalizing it to the case of all  $n$  committed qubits leads to the following result.

*Corollary 1.* For  $1 \leq i \leq n$ , let  $\mathcal{E} = \{E_j\}_j$  and  $\mathcal{E}' = \{E_{\vec{x},j}\}_{\vec{x} \in \{0,1\}^n, j}$  be CPTP maps expressed as the Kraus decomposition:

$$E_j = \sum_{\vec{x}, \vec{z} \in \{0,1\}^n} \left( \bigotimes_{i=1}^n X^{\vec{x}(i)} Z^{\vec{z}(i)} \right) \otimes E_j^{\vec{x}\vec{z}}, \quad (34)$$

$$E_{\vec{x},j} = \sum_{\vec{z} \in \{0,1\}^n} \left( \bigotimes_{i=1}^n Z^{\vec{z}(i)} \right) \otimes E_j^{\vec{x}\vec{z}}, \quad (35)$$

where  $\vec{x}(i)$  (or  $\vec{z}(i)$ ) is the  $i$ th value of the vector  $\vec{x}$  (or  $\vec{z}$ ), respectively, and the  $n$ -qubit Pauli operators are applied on  $n$  committed qubits. Let a perfect prover  $\mathbb{P}$  be characterized by  $(U_1, \mathcal{E}, I)$ . There exists a perfect prover  $\mathbb{P}'$  characterized by  $(U_1, \mathcal{E}', U_3)$  such that  $f_{\mathbb{P},h}$  is computationally indistinguishable from  $f_{\mathbb{P}',h}$ , where  $U_3$  is one unitary operator that commutes with a computational basis measurement on  $n$  committed qubits.

#### D. Soundness of measurement protocol

The soundness of Protocol 1 is given by Theorem 4.

*Theorem 4.* For an arbitrary prover  $\mathbb{P}$  and any basis choice  $h = \{0, 1, 2, 3, 4\}^n$  in Protocol 1, let  $\Lambda_1^h$  be the probability that the verifier rejects  $\mathbb{P}$  in the type-I measurement protocol and let  $\Lambda_2^h$  be the probability that the verifier rejects  $\mathbb{P}$  in the type-II measurement protocol. There exists a perfect prover  $\tilde{\mathbb{P}}$  such that  $D_{TV}(f'_{\tilde{\mathbb{P}},h}, f_{\tilde{\mathbb{P}},h})$  belongs to the interval

$$[|\Lambda_1^h + \sqrt{1 - \Lambda_2^h} - 1|, \Lambda_1^h + \sqrt{\Lambda_2^h}] \quad (36)$$

and  $D_{L_2}(f'_{\tilde{\mathbb{P}},h}, f_{\tilde{\mathbb{P}},h})$  belongs to the interval

$$\left[ \frac{1}{\sqrt{2^{n-2}}} |\Lambda_1^h + \sqrt{1 - \Lambda_2^h} - 1|, 2(\Lambda_1^h + \sqrt{\Lambda_2^h}) \right]. \quad (37)$$

In addition, there exists a state  $\rho$  such that  $f_{\tilde{\mathbb{P}},h}$  is computationally indistinguishable from  $f_{\rho,h}$ .

*Proof.* Without loss of generality, assume the prover  $\mathbb{P}$  is characterized by  $(U_1, U_2, I)$ . We will prove that the prover  $\tilde{\mathbb{P}}$  characterized by  $(I, U_2, I)$  satisfies the requirement of the theorem.

Let  $\rho'$  ( $\rho''$ ) be the state of the system corresponding to  $\mathbb{P}$  ( $\tilde{\mathbb{P}}$ ) at the beginning of measurements of the computational basis measurement round. Let  $|\varphi_{0,k'}\rangle$  be the state that can pass the check of the computational basis measurement round and the test round for function key  $k'$  and let  $|\varphi_{1,k'}\rangle$  be the orthogonal state of  $|\varphi_{0,k'}\rangle$ . Then  $\rho'$  can be written as

$$\sum_{k'} f_{\mathbb{V},h}(k') (\sqrt{1 - \Lambda_2^h} |\varphi_{0,k'}\rangle + \sqrt{\Lambda_2^h} |\varphi_{1,k'}\rangle) \times (\sqrt{1 - \Lambda_2^h} \langle\varphi_{0,k'}| + \sqrt{\Lambda_2^h} \langle\varphi_{1,k'}|). \quad (38)$$

Note that  $\tilde{\mathbb{P}}$  behaves honestly before the rotation basis measurement round. It implies that  $\tilde{\mathbb{P}}$  can pass the computational basis measurement round and the test round with probability negligibly close to 1, i.e.,  $\tilde{\mathbb{P}}$  is perfect. So, it follows that  $\rho''$  is negligibly close to

$$\sum_{k'} f_{\mathbb{V},h}(k') |\varphi_{0,k'}\rangle \langle\varphi_{0,k'}|. \quad (39)$$

Thus we have

$$D_{\text{tr}}(\rho', \rho'') \leq \sqrt{1 - F(\rho', \rho'')} = \sqrt{\Lambda_2^h}, \quad (40)$$

$$D_{\text{tr}}(\rho', \rho'') \geq 1 - \sqrt{F(\rho', \rho'')} = 1 - \sqrt{1 - \Lambda_2^h}, \quad (41)$$

where  $F(\rho', \rho'')$  is the fidelity between  $\rho'$  and  $\rho''$ . Refer to Refs. [23,30]; Eq. (40) implies

$$D_{\text{TV}}(f'_{\mathbb{P},h}, f_{\tilde{\mathbb{P}},h}) \leq \Lambda_1^h + \sqrt{\Lambda_2^h}. \quad (42)$$

Let the CPTP map  $\mathcal{O}$  be composed of the measurement of the computational basis measurement round and the implementation of the rotation basis measurement round; we then get

$$\begin{aligned} D_{\text{tr}}(\sigma_{\mathbb{P},h}, \sigma_{\tilde{\mathbb{P}},h}) &= D_{\text{tr}}(\mathcal{O}\rho', \mathcal{O}\rho'') \\ &\geq 1 - \sqrt{F(\mathcal{O}\rho', \mathcal{O}\rho'')} \\ &\geq 1 - \sqrt{F(\rho', \rho'')} = 1 - \sqrt{1 - \Lambda_2^h}. \end{aligned} \quad (43)$$

Using a triangle inequality, we obtain

$$\begin{aligned} D_{\text{TV}}(f'_{\mathbb{P},h}, f_{\tilde{\mathbb{P}},h}) &\geq |D_{\text{TV}}(f'_{\mathbb{P},h}, f_{\mathbb{P},h}) - D_{\text{TV}}(f_{\mathbb{P},h}, f_{\tilde{\mathbb{P}},h})| \\ &= |\Lambda_1^h - D_{\text{tr}}(\sigma_{\mathbb{P},h}, \sigma_{\tilde{\mathbb{P}},h})| \\ &\geq |\Lambda_1^h + \sqrt{1 - \Lambda_2^h} - 1|. \end{aligned} \quad (44)$$

The Euclidean distance between density functions  $f_{\mathbb{P},h}$  and  $f_{\tilde{\mathbb{P}},h}$  satisfies

$$\begin{aligned} D_{L_2}(f'_{\mathbb{P},h}, f_{\tilde{\mathbb{P}},h}) &\leq D_{L_1}(f'_{\mathbb{P},h}, f_{\tilde{\mathbb{P}},h}) \\ &= 2 D_{\text{TV}}(f'_{\mathbb{P},h}, f_{\tilde{\mathbb{P}},h}) = 2(\Lambda_1^h + \sqrt{\Lambda_2^h}), \end{aligned} \quad (45)$$

$$\begin{aligned} D_{L_2}(f'_{\mathbb{P},h}, f_{\tilde{\mathbb{P}},h}) &\geq \frac{1}{\sqrt{2^n}} D_{L_1}(f'_{\mathbb{P},h}, f_{\tilde{\mathbb{P}},h}) \\ &\geq \frac{1}{\sqrt{2^{n-2}}} |\Lambda_1^h + \sqrt{1 - \Lambda_2^h} - 1|, \end{aligned} \quad (46)$$

where the first inequality of Eq. (46) is based on the fact that the mean square root mean is greater than or equal to

the arithmetic mean and the fact that the domain of density functions scales as  $2^n$ .

By Corollary 1, there exists a normal prover  $\mathbb{P}'$  such that  $f_{\tilde{\mathbb{P}},h}$  is computationally indistinguishable from  $f_{\mathbb{P}',h}$ . Utilizing Theorem 2, there exists a state  $\rho$  such that  $f_{\mathbb{P}',h}$  is equivalent to  $f_{\rho,h}$ . We therefore conclude that  $f_{\tilde{\mathbb{P}},h}$  is computationally indistinguishable from  $f_{\rho,h}$ . ■

#### IV. APPLICATIONS OF MEASUREMENT PROTOCOL

This section presents the applications of measurement protocol to verification of graph states and verifiable delegated quantum computing.

##### A. Verification of graph states on honest-but-noisy devices

In this subsection, we will propose two protocols that aim at verifying a graph state with a device-noise-independent method. Graph states are widely used as resource states for measurement-based quantum computation (MBQC) [32,33]. The verification of graph states is important for verifying quantum computation. The available techniques [18,34] to certify the correctness of a graph state generated by an untrusted device usually rely on performing sequential single-qubit measurements of Pauli operators on the prepared states. However, it requires that the measurement device is ideal. The imperfections of a nonmalicious device could make the protocol invalid. Here, using our measurement protocol to substitute for the Pauli basis measurements, we can remove this unpractical requirement. The imperfect universal quantum device owned by an individual is called prover and this individual is called verifier. Our first noise-robustness verification protocol consists of the verification protocol of the graph states from Ref. [18] and our measurement protocol, which runs as follows.

*Protocol 2 (Device-noise-independent verification of graph state  $|G\rangle$  with Pauli  $X$  and  $Z$  basis measurements)*

(1) The verifier asks the prover to prepare  $2k + 1$  copies of an  $n$ -qubit graph state  $|G\rangle$ . Honest prover will prepare  $|G\rangle^{2k+1}$ . However, an honest-but-noisy prover will generate an arbitrary state.

(2) The verifier uniformly and randomly chooses  $2k$  copies for the stabilizer tests. The remaining copy is the target state  $\rho_{\text{tgt}}$ . The Pauli  $X$  basis measurements and Pauli  $Z$  basis measurements required for the stabilizer tests partially defines a basis choice  $h$ . All undefined  $h_i$  are set to be 0.

(3) The verifier and the prover participate in the measurement protocol.

(4) Repeat steps (1)–(3)  $N$  times. The number of type-I (type-II) measurement protocols is denoted by  $N_1$  ( $N_2$ ). The number of type-I (type-II) measurement protocols rejected by the verifier is denoted by  $N'_1$  ( $N'_2$ ).

(5) The verifier chooses one of the type-I measurement protocols that is accepted. The verifier then assesses each stabilizer test according to the measurement results of this type-I measurement protocol. If all stabilizer tests are passed, the verifier accepts the prover.

The soundness and completeness of Protocol 2 are shown in Theorem 5. The soundness means that when the verifier accepts the prover, there is a high probability for the state



prepared by the prover to be close to graph state  $|G\rangle$ . The completeness means that when the prover is honest, there is a high probability that the verifier accepts a correct result.

*Theorem 5.* If the verifier accepts the honest-but-noisy prover in Protocol 2, the target state  $\rho_{\text{tgt}}$  satisfies, with probability at least  $1 - N'_1/N_1 - \sqrt{N'_2/N_2} - \alpha$ ,

$$\langle G | \rho_{\text{tgt}} | G \rangle \geq 1 - \frac{1}{\alpha(2k + 1)}, \quad (47)$$

where  $\alpha$  is any constant satisfying  $\alpha > [1/(2k + 1)]$ . If the prover is ideal, the verifier accepts the prover with probability negligibly close to 1.

*Proof.* Let  $p(f)$  be the probability that the  $n$  bit string sampled from the probability density function  $f$  passes all stabilizer tests in step (5) of Protocol 2. Then the probability that the verifier accepts the prover in step (5) is  $p(f'_{\mathbb{P},h})$ . From Theorem 4, we can guarantee that

$$\begin{aligned} p(f'_{\mathbb{P},h}) &\leq \Lambda_1^h + \sqrt{\Lambda_2^h} + p(f_{\mathbb{P},h}) \\ &\leq \Lambda_1^h + \sqrt{\Lambda_2^h} + \mu_h + p(f_{\rho,h}), \end{aligned} \quad (48)$$

where  $\mu_h$  is a negligible function. By Theorem 1 of Ref. [18], if  $\text{Tr}(\Pi^\perp \rho_{\text{tgt}}) > 1/[\alpha(2k + 1)]$ , then  $p(f_{\rho,h}) < \alpha$ , i.e.,

$$p(f'_{\mathbb{P},h}) \leq \Lambda_1^h + \sqrt{\Lambda_2^h} + \mu_h + \alpha. \quad (49)$$

Here,  $\Pi^\perp$  is the  $n$ -qubit projector  $I^{\otimes n} - |G\rangle\langle G|$ . This implies that if the verifier accepts the prover in step (5), we have

$$\begin{aligned} \Pr\left(\langle G | \rho_{\text{tgt}} | G \rangle \geq 1 - \frac{1}{\alpha(2k + 1)}\right) \\ \geq 1 - \Lambda_1^h - \sqrt{\Lambda_2^h} - \mu_h - \alpha. \end{aligned} \quad (50)$$

To recall Protocol 2, when the number  $N$  of repetitions is large enough, it follows that  $\Lambda_1^h = N'_1/N_1$  and  $\Lambda_2^h = N'_2/N_2$ . Bringing this into Eq. (50) obtains the soundness of Protocol 2.

Now we consider the case that the prover is ideal. By Theorem 1, we can guarantee that

$$p(f'_{\mathbb{P},h}) \geq -\mu'_h + p(f_{|G\rangle\langle G|,h}), \quad (51)$$

where  $\mu'_h$  is a negligible function. The completeness of the verification protocol of Ref. [18] shows that  $p(f_{|G\rangle\langle G|,h}) = 1$ . Taking this into Eq. (51) gets the completeness of Protocol 2. ■

Here, we give another device-noise-independent verification protocol for graph states to show the advantages of our measurement protocol, which can be used to verify the Pauli  $X$ ,  $Y$ , and  $Z$  basis measurements. Protocol 3 consists of the verification protocol of the graph states from Ref. [10] and our measurement protocol.

*Protocol 3 (Device-noise-independent verification of graph state  $|G\rangle$  with Pauli  $X$ ,  $Y$ , and  $Z$  basis measurements)*

(1) The verifier asks the prover to prepare  $\tilde{N} = (2^n - 1)k + 1$  copies of an  $n$ -qubit graph state  $|G\rangle$ .

(2) The verifier uniformly and randomly chooses one copy for the target state  $\rho_{\text{tgt}}$ . The remaining  $(2^n - 1)k$  copies are divided into  $2^n - 1$  groups such that which copy is assigned to the  $i$ th group is uniformly random. Let  $\{g_i\}_{i=1}^n$  be  $n$  stabilizers

of the  $n$ -qubit graph state  $|G\rangle$ . Let the set  $\{\tau_1, \tau_2, \dots, \tau_{2^n-1}\}$  of nontrivial stabilizer operators of  $|G\rangle$  be written by the set  $\{\prod_{i=1}^n g_i^{w_i}\}_{\vec{w}=w_1 w_2 \dots w_n}$ , where  $\vec{w} \in \{0, 1\}^n$ ,  $\vec{w} \neq 0$ . The verifier asks the prover to perform the measurement for  $\tau_i$  on every copy in the  $i$ th group, which defines a basis choice  $h$ .

(3) The verifier and the prover participate in the measurement protocol.

(4) Repeat steps (1)–(3)  $N$  times. Similar to Protocol 2, the numbers  $N_1$ ,  $N_2$ ,  $N'_1$ , and  $N'_2$  are counted.

(5) The verifier chooses one of the type-I measurement protocols that is accepted. Let  $o_{ij} \in \{+1, -1\}$  be the measurement outcome corresponding to the  $j$ th copy in the  $i$ th group for  $1 \leq i \leq 2^n - 1$ ,  $1 \leq j \leq k$ . If all  $o_{ij}$  are equal to 1, the verifier accepts the prover.

The soundness and completeness of Protocol 3 are shown in Theorem 6.

*Theorem 6.* Let  $\tilde{N} = \lceil 2\epsilon^{-1} \ln \delta^{-1} \rceil$ , where  $\epsilon$  is a parameter related to the infidelity and  $\delta$  is a parameter related to the significance level. If the verifier accepts the honest-but-noisy prover in Protocol 3, the target state  $\rho_{\text{tgt}}$  satisfies, with probability at least  $1 - N'_1/N_1 - \sqrt{N'_2/N_2} - \delta$ ,

$$\langle G | \rho_{\text{tgt}} | G \rangle \geq 1 - \epsilon. \quad (52)$$

If the prover is ideal, the verifier accepts the prover with probability negligibly close to 1.

*Proof.* According to Ref. [10], in step (1) of Protocol 3 the requirement of  $\tilde{N} = \lceil 2\epsilon^{-1} \ln \delta^{-1} \rceil$  copies can lead to the target state  $\rho_{\text{tgt}}$  satisfying  $\langle G | \rho_{\text{tgt}} | G \rangle \geq 1 - \epsilon$  with probability at least  $1 - \delta$ . It means that if  $\text{Tr}(\Pi^\perp \rho_{\text{tgt}}) > \epsilon$ , then  $p(f_{\rho,h}) < \delta$ . Similar to the proof of Theorem 5, the soundness and completeness can be obtained. ■

We now compare the resource overhead of our verification protocols for graph states with the existing protocols. To verify the graph state  $|G\rangle$  within infidelity  $\epsilon$  and significance level  $\delta$ , the number of required copies of  $|G\rangle$  in Ref. [18] is at least  $\lceil \epsilon^{-1} \delta^{-1} \rceil$ . Our method needs at least  $N \lceil \epsilon^{-1} (\delta - N'_1/N_1 - \sqrt{N'_2/N_2})^{-1} \rceil$  copies of  $|G\rangle$ , where  $N, N_1/N'_1, N_2/N'_2$  are constant. The additional overhead originates from the facts that our Protocol 2 needs the higher significance level to achieve the same fidelity and the measurement protocol is performed  $N$  times. However, the extra overhead results in a desirable property, i.e., the robustness for device noise. Similarly, the protocol of Ref. [10] can achieve infidelity  $\epsilon$  and significance level  $\delta$  with at least  $\lceil 2\epsilon^{-1} \ln \delta^{-1} \rceil$  copies of  $|G\rangle$ . Our Protocol 3 takes at least  $N \lceil 2\epsilon^{-1} \ln (\delta - N'_1/N_1 - \sqrt{N'_2/N_2})^{-1} \rceil$  copies of  $|G\rangle$ .

### B. Verifiable delegated quantum computing

Verifiable delegated quantum computing [19] is a kind of cloud quantum computing, where the client can ensure the integrity of the computations. Applying a Pauli  $X/Z$  basis measurement protocol to a *post hoc* verification protocol [35], Mahadev proposed the first verification protocol [23,30] that allows a classical verifier to delegate computations to a single prover. The soundness of Mahadev's protocol is 0.75. We will show that replacing the Pauli  $X/Z$  basis measurement protocol with our Protocol 1 results in a CVQC protocol with soundness of 0.5757. Our protocol works as follows.

*Protocol 4 (Improved classical verification of quantum computation).*

(1) The verifier and the prover receive an instance of  $x$ . The aim of the protocol is to verify that  $x \in L$  for a language  $L \in \text{BQP}$ . The Hamiltonian corresponding to  $x$  can be written as  $H = \sum_i a_i S_i$ , where  $a_i$  is a real number and  $S_i$  is a tensor product consisting of Pauli  $X$  and  $Z$  operators and the identity  $I$ .

(2) The verifier asks the prover to prepare  $r$  copies of the ground state of Hamiltonian  $H' = \sum_i p_i \frac{I + \text{sgn}(a_i) S_i}{2}$ , where  $p_i = \frac{|a_i|}{\sum_i |a_i|}$ .

(3) The verifier samples  $r$  terms  $(S'_1, \dots, S'_r)$  of the set  $\{S_i\}_i$  according to probability distribution  $\{p_i\}_i$ .

(4) In order to measure the  $r$  selected  $XZ$  terms on the  $r$  copies prepared by the prover, the verifier and the prover participate in the measurement protocol, where the parameter  $\beta$  is set to be 0.28. The verifier accepts or rejects according to the measurement protocol. If the executive measurement protocol belongs to type I, the verifier proceeds to the next step. Otherwise, the whole protocol is aborted.

(5) The verifier initializes one counter  $\hat{C} = 0$ . For each  $XZ$ -term  $S'_i$ , which represents  $S_j$ , if the verifier obtains the outcome  $-\text{sgn}(a_j)$  of the measurement, the verifier sets  $\hat{C} = \hat{C} + 1$ . The verifier accepts if  $\hat{C} \geq r/2$ .

The soundness and completeness of Protocol 4 are shown in Theorem 7. The completeness means the lower bound of the probability that the verifier accepts the honest prover for the case of  $x \in L$ . The soundness means the upper bound of the probability that the verifier accepts the prover, who may be malicious, for the case of  $x \notin L$ .

*Theorem 7.* Protocol 4 is a quantum-prover interactive argument for the class BQP with completeness negligibly close to 1 and soundness negligibly close to 0.5757.

*Proof.* Let  $p(f)$  be the probability that  $n$  bit string sampled from the probability density function  $f$  passes the check in step (5) of Protocol 4 and let  $v_h$  be the probability that the basis  $h$  is chosen. Similar to Eq. (180) of Ref. [30], the probability that the verifier accepts the prover in Protocol 4 is

$$\sum_h v_h [\beta(1 - \Lambda_2^h) + (1 - \beta)(1 - \Lambda_1^h) p(f'_{\mathbb{P},h})], \quad (53)$$

where the first item is the probability that the verifier runs a type-II measurement protocol and accepts the prover in step (4) of Protocol 4 and the second item is the probability that the verifier runs a type-I measurement protocol and accepts the prover in step (4) and step (5) of Protocol 4.

In order to obtain the soundness, we need to get the upper bound of  $p(f'_{\mathbb{P},h})$ . By the property of the total variation distance and Theorem 4, we have

$$p(f'_{\mathbb{P},h}) - p(f_{\mathbb{P},h}) \leq D_{TV}(f'_{\mathbb{P},h}, f_{\mathbb{P},h}) \leq \Lambda_1^h + \sqrt{\Lambda_2^h}. \quad (54)$$

Thus we have to get the upper bound  $p(f_{\mathbb{P},h})$ . Similarly, we have

$$p(f_{\mathbb{P},h}) - p(f_{\rho,h}) \leq D_{TV}(f'_{\mathbb{P},h}, f_{\rho,h}) \leq \mu_1, \quad (55)$$

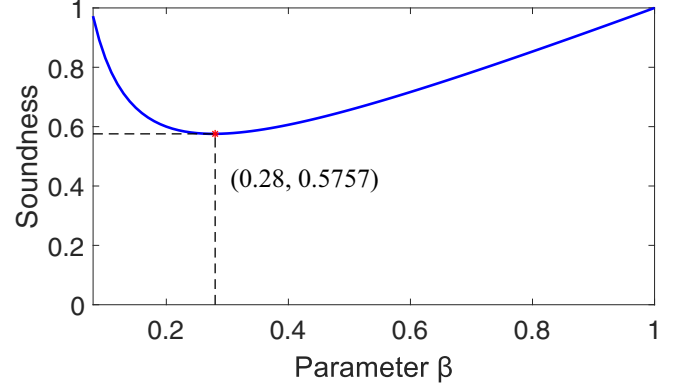


FIG. 3. Soundness as a function of the parameter  $\beta$ .

where  $\mu_1$  is a negligible function. According to the soundness of *post hoc* verification protocol [35], it holds that

$$\sum_h v_h p(f_{\rho,h}) \leq \mu_2, \quad (56)$$

where  $\mu_2$  is a negligible function. By the above analysis, the soundness is

$$\mu' + \sum_h v_h \left[ \beta(1 - \Lambda_2^h) + (1 - \beta)(1 - \Lambda_1^h) \left( \Lambda_1^h + \sqrt{\Lambda_2^h} \right) \right], \quad (57)$$

where  $\mu'$  is a negligible function. Calculating the optimal soundness can be converted to solving the following optimization problem, i.e.,

$$\min_{\beta \in (0,1)} \max_{\Lambda_1^h \in [0,1], \Lambda_2^h \in [0,1]} f_{\text{opt}}(\beta, \Lambda_1^h, \Lambda_2^h), \quad (58)$$

where

$$f_{\text{opt}} = \beta(1 - \Lambda_2^h) + (1 - \beta)(1 - \Lambda_1^h) \left( \Lambda_1^h + \sqrt{\Lambda_2^h} \right). \quad (59)$$

From the extreme value theory of quadratic function, the maximum value is obtained when  $\Lambda_1^h = 1/2$ ,  $\Lambda_2^h = (1 - \beta)/(4\beta)$ . The soundness corresponding to the parameter  $\beta$  is shown in Fig. 3. According to the numerical result, the minimum value 0.5757 is derived when  $\beta = 0.28$ .

In order to obtain the completeness, we need to get the minimal probability that the verifier accepts the honest prover in Protocol 4. This means that we need to calculate the upper bound of  $\Lambda_1^h$  and  $\Lambda_2^h$  as well as the lower bound of  $p(f'_{\mathbb{P},h})$ . From Theorem 1, it follows that

$$\Lambda_1^h \leq \mu_3, \quad \Lambda_2^h \leq \mu_4, \quad (60)$$

where  $\mu_3$  and  $\mu_4$  are negligible functions. By the property of the total variation distance and Theorem 1, we have

$$p(f_{\rho,h}) - p(f'_{\mathbb{P},h}) \leq D_{TV}(f_{\rho,h}, f'_{\mathbb{P},h}) \leq \mu_5, \quad (61)$$

where  $\mu_5$  is a negligible function. Thus we have to get the lower bound  $p(f_{\rho,h})$ . According to the completeness of *post hoc* verification protocol [35], it holds that

$$\sum_h v_h p(f_{\rho,h}) \geq 1 - \mu_6, \quad (62)$$

TABLE I. Performance of our measurement protocol compared with Mahadev’s protocol.

Measurement protocol	Functions	Measurement basis
Our protocol	NTCFs	$X, Y, \frac{X+Y}{\sqrt{2}}, \frac{X-Y}{\sqrt{2}}, Z$
Mahadev’s protocol	NTCFs + Trapdoor injective family	$X, Z$

where  $\mu_6$  is a negligible function. By the above analysis, the completeness is  $1 - \mu''$ , where  $\mu''$  is a negligible function. ■

V. CONCLUSION

In this paper, our main result is a classical verification protocol of multibasis measurement. Existing protocol [23] has realized the goal that a classical verifier can interact with a quantum prover to verify the result of computational basis or Pauli  $X$  basis measurement. Our measurement protocol has extended to the classical verification of computational basis or  $XY$ -plane rotation basis measurement. We have analyzed the completeness and soundness of our measurement protocol. The soundness of our method is guaranteed by a slightly stronger variant [31] of the adaptive hardcore bit property of the noisy trapdoor claw-free family in Ref. [30]. Our scheme is conditioned on the hardness of the LWE problem for quantum computers, which is inherited from the use of NTCFs. Compared with Ref. [30], our measurement protocol have removed the requirement for the trapdoor injective family. The differences between our measurement protocol and Mahadev’s protocol have been summarized in Table I, including constructed functions and realized measurement basis.

The local operations and classical communication (LOCC) [36] is a certain type of transformation of states in quantum information theory. LOCC protocols are usually used to obtain a maximally entangled state with respect to some entanglement measure. The similarity between our measurement protocol and LOCC protocols is that the communication between Alice (verifier) and Bob (prover) is two-way classical. One of the differences is that our protocol has considered the adversarial scenario, i.e., the prover can be malicious and send wrong classical messages to the verifier. As for LOCC protocols, the scenario is nonadversarial, i.e., Bob is required to cooperate with Alice. The other one is that the observers in LOCC protocols require local operations, such as measurements and unitary operations. It implies that both Alice and Bob need quantum abilities. As for our measurement protocol, only the prover needs universal quantum abilities.

Based on our measurement protocol, we have constructed two device-noise-independent verification protocols for the certification of graph states. Different from the traditional methods [18,37], our schemes are independent of the assumption that the device is ideal and there is no need for multiple noncommunicating provers that share entanglement.

Another application of our measurement protocol is verifiable delegated quantum computing. We have constructed a CVQC protocol, where a better soundness is obtained by optimizing the probability of choosing to run a test round or a rotation basis measurement round.

Many efficient verification protocols for quantum states, such as the verification of ground states of Hamiltonians [38], must require Pauli  $X, Y$ , and  $Z$  basis measurements. If we apply our measurement protocol to the verification of these states, the classical verification of  $XY$ -plane rotation basis measurement will yield considerable advantages. In order to explore the classical verification of  $XZ$ -plane basis or  $YZ$ -plane basis measurement, let us recall that, in our protocol 1, after the Fourier basis (over  $\mathbb{Z}_8$ ) measurement on the preimage register  $i$ , the state of  $i$ th committed qubit is  $(R_Z\{\pi d_i[J(x_{0,y_i}) \oplus J(x_{1,y_i})]/4\} \otimes I)|\psi\rangle$ . Since the first adaptive hardcore bit property of the NTCF family ensures that  $d_i[J(x_{0,y_i}) \oplus J(x_{1,y_i})]$  is computationally indistinguishable from  $\{d_i[J(x_{0,y_i}) \oplus J(x_{1,y_i})]\} \oplus 4$ , the prover cannot derive the information of bit  $c_i$  from the bit  $\gamma_i = \theta_i + \pi d_i[J(x_{0,y_i}) \oplus J(x_{1,y_i})]/4 + c_i\pi$  sent by the verifier. The security of our measurement protocol is exactly based on the design of  $\gamma_i$ . If one can find one transform followed by the computational basis measurement such that the post-measurement state is  $(R_Y\{\pi d_i[J(x_{0,y_i}) \oplus J(x_{1,y_i})]/4\} \otimes I)|\psi\rangle$  or  $(R_X\{\pi d_i[J(x_{0,y_i}) \oplus J(x_{1,y_i})]/4\} \otimes I)|\psi\rangle$ , where  $R_Y(\theta) = \cos \frac{\theta}{2}I - i \sin \frac{\theta}{2}Y$  and  $R_X(\theta) = \cos \frac{\theta}{2}I - i \sin \frac{\theta}{2}X$ , then our measurement protocol can adjust to verifying the  $XZ$ -plane basis or  $YZ$ -plane basis measurement. In addition, it is necessary to prove the computational indistinguishability of distributions when the attacks of the  $YZ$ -plane ( $XZ$ -plane) rotation basis measurement round become  $Z$  trivial ( $X$  trivial).

ACKNOWLEDGMENTS

The research was partly funded by the Natural Science Foundation of Guangdong Province of China under Grant No. 2021A1515011440, the Major Program of Guangdong Basic and Applied Research under Grant No. 2019B030302008, the National Natural Science Foundation of China under Grant No. 62032009, and the Outstanding Innovative Talents Cultivation Funded Programs for Doctoral Students of Jinan University under Grant No. 2021CXB007.

[1] S. Arora and B. Barak, *Computational Complexity: A Modern Approach* (Cambridge University Press, Cambridge, UK, 2009).  
 [2] U. Feige and A. Shamir, *Zero Knowledge Proofs of Knowledge in Two Rounds* (Springer, New York, 1990).

[3] S. Aaronson and A. Arkhipov, *43th Annual ACM Symposium on Theory of Computing* (ACM, New York, 2011), p. 333.  
 [4] P. W. Shor, *Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science* (IEEE, New York, 1994), p. 124.

- [5] J. Biamonte, P. Wittek, N. Pancotti, P. Rebentrost, N. Wiebe, and S. Lloyd, *Nature (London)* **549**, 195 (2017).
- [6] N. R. Zhou, T. F. Zhang, X. W. Xie, and J. Y. Wu, *Signal Process. Image Commun.* **110**, 116891 (2023).
- [7] J. Eisert, D. Hangleiter, N. Walk, I. Roth, D. Markham, R. Parekh, U. Chabaud, and E. Kashefi, *Nat. Rev. Phys.* **2**, 382 (2020).
- [8] M. Kliesch and I. Roth, *PRX Quantum* **2**, 010201 (2021).
- [9] Z. Hradil, *Phys. Rev. A* **55**, R1561 (1997).
- [10] S. Pallister, N. Linden, and A. Montanaro, *Phys. Rev. Lett.* **120**, 170502 (2018).
- [11] S. T. Flammia and Y.-K. Liu, *Phys. Rev. Lett.* **106**, 230501 (2011).
- [12] I. Šupić and J. Bowles, *Quantum* **4**, 337 (2020).
- [13] Y.-C. Liu, J. Shang, X.-D. Yu, and X. Zhang, *Phys. Rev. A* **101**, 042315 (2020).
- [14] E. Magesan, J. M. Gambetta, and J. Emerson, *Phys. Rev. Lett.* **106**, 180504 (2011).
- [15] S. Boixo, S. V. Isakov, V. N. Smelyanskiy, R. Babbush, N. Ding, Z. Jiang, M. J. Bremner, J. M. Martinis, and H. Neven, *Nat. Phys.* **14**, 595 (2018).
- [16] J. F. Fitzsimons and E. Kashefi, *Phys. Rev. A* **96**, 012303 (2017).
- [17] A. Broadbent, *Theor. Comput.* **14**, 1 (2008).
- [18] M. Hayashi and T. Morimae, *Phys. Rev. Lett.* **115**, 220502 (2015).
- [19] A. Gheorghiu, T. Kapourniotis, and E. Kashefi, *Theory Comput. Syst.* **63**, 715 (2019).
- [20] A. Coladangelo, A. B. Grilo, S. Jeffery, and T. Vidick, *Annual International Conference on the Theory and Applications of Cryptographic Techniques* (Springer, New York, 2019), p. 247.
- [21] Q. Xu, X. Tan, R. Huang, and M. Li, *Phys. Rev. A* **104**, 042412 (2021).
- [22] D. Leichtle, L. Music, E. Kashefi, and H. Ollivier, *PRX Quantum* **2**, 040302 (2021).
- [23] U. Mahadev, *IEEE 59th Annual Symposium on Foundations of Computer Science* (IEEE, New York, 2018), p. 259.
- [24] G. Alagic, A. M. Childs, A. B. Grilo, and S.-H. Hung, *Theory of Cryptography Conference* (Springer, New York, 2020), p. 153.
- [25] A. Gheorghiu and T. Vidick, *IEEE 60th Annual Symposium on Foundations of Computer Science* (IEEE, New York, 2019), p. 1024.
- [26] K. M. Chung, Y. Lee, H.-H. Lin, and X. Wu, *Annual International Conference on the Theory and Applications of Cryptographic Techniques* (Springer, New York, 2022), p. 707.
- [27] J. Zhang, *IEEE 63rd Annual Symposium on Foundations of Computer Science* (IEEE, New York, 2022), p. 46.
- [28] M. Hein, J. Eisert, and H. J. Briegel, *Phys. Rev. A* **69**, 062311 (2004).
- [29] Z. Brakerski, P. Christiano, U. Mahadev, U. Vazirani, and T. Vidick, *J. ACM* **68**, 1 (2021).
- [30] U. Mahadev, [arXiv:1804.01082](https://arxiv.org/abs/1804.01082).
- [31] A. Gheorghiu and T. Vidick, [arXiv:1904.06320](https://arxiv.org/abs/1904.06320).
- [32] H. J. Briegel, D. E. Browne, W. Dur, R. Raussendorf, and M. Van den Nest, *Nat. Phys.* **5**, 19 (2009).
- [33] R. Raussendorf, D. E. Browne, and H. J. Briegel, *Phys. Rev. A* **68**, 022312 (2003).
- [34] Y. Takeuchi, A. Mantri, T. Morimae, A. Mizutani, and J. F. Fitzsimons, *npj Quantum Inf.* **5**, 27 (2019).
- [35] J. F. Fitzsimons, M. Hajdušek, and T. Morimae, *Phys. Rev. Lett.* **120**, 040501 (2018).
- [36] H. Fan, *Phys. Rev. Lett.* **92**, 177905 (2004).
- [37] M. McKague, *Theory Comput.* **12**, 1 (2016).
- [38] Y. Takeuchi and T. Morimae, *Phys. Rev. X* **8**, 021060 (2018).