Letter

Computational self-testing for entangled magic states

Akihiro Mizutani,[1] Yuki Takeuchi,[2] Ryo Hiromasa,[1] Yusuke Aikawa,[1] and Seiichiro Tani[2]

[1]*Mitsubishi Electric Corporation, Information Technology R&D Center, 5-1-1 Ofuna, Kamakura-shi, Kanagawa, 247-8501 Japan*
[2]*NTT Communication Science Laboratories, NTT Corporation, 3-1 Morinosato Wakamiya, Atsugi, Kanagawa 243-0198, Japan*

(Received 5 November 2021; revised 6 April 2022; accepted 17 June 2022; published 25 July 2022)

Can classical systems grasp quantum dynamics executed in an untrusted quantum device? Metger and Vidick answered this question affirmatively by proposing a computational self-testing protocol for Bell states that certifies generation of Bell states and measurements on them. Since their protocol relies on the fact that the target states are stabilizer states, it is highly nontrivial to reveal whether the other class of quantum states, *nonstabilizer states*, can be self-tested. Among nonstabilizer states, magic states are indispensable resources for universal quantum computation. Here, we show that a magic state for the *CCZ* gate can be self-tested while that for the T gate cannot. Our result is applicable to a proof of quantumness, where we can classically verify whether a quantum device generates a quantum state having nonzero magic.

DOI: 10.1103/PhysRevA.106.L010601

Introduction. In device-independent quantum information processing, we treat a quantum device as a black box and can only access it classically. By using classical input-output statistics obtained through interacting with the device, our goal is to make statements about the inner workings of the quantum device. A scheme for characterizing a quantum device provides an approach to achieve device-independent quantum key distribution [1–7] and delegated quantum computation [8,9].

A stringent form of device-independent certification for quantum devices is self-testing, which was introduced by Mayers and Yao [10]. In traditional self-testing protocols (see, e.g., [11–13]), a classical verifier certifies that computationally unbounded devices, which are also called provers, have prepared the target state up to some isometry (i.e., a change of basis) and measured qubits with the observable as required by the verifier. Their crucial assumption is that there are multiple provers, and each prover is allowed to be entangled but cannot classically communicate with others. In practice, however, this non-communication assumption is difficult to enforce.

Recently, a different type of self-testing called computational self-testing (C-ST) was proposed [14], which replaces the noncommunicating multiple provers with a single computationally bounded quantum prover who only performs efficient quantum computation. To remove the noncommunication assumption, their protocol relies on a standard assumption in post-quantum cryptography where the learning with errors (LWE) problem [15] cannot be solved by quantum computers in polynomial time [16]. Since the prover is assumed to be computationally bounded, the probability of solving the LWE problem is negligibly small, which we call the *LWE assumption*. Here, it is important to note that unlike in classical public-key cryptography, this LWE assumption must hold *only during* execution of the self-testing protocol [17]. The C-ST [14] has been applied to device-independent quantum key distribution [7] and oblivious transfer [18].

The self-testing protocol [14] consists of interactions between the classical verifier and the prover, and after the interactions the verifier decides to either "accept" or "reject" the prover. In general, a C-ST protocol must satisfy two properties. One is completeness where the honest prover (i.e., the ideal device) is accepted by the verifier with high probability. The other is soundness, where, if the verifier accepts the prover with high probability, the device's functionality is close to the ideal one, i.e., the device generates the target state and executes measurements on it with high precision as required by the verifier. So far, the C-ST protocol has been constructed only for Bell states $(\sigma_X^a \otimes \sigma_X^b)(|0\rangle|+\rangle + |1\rangle|-\rangle)/\sqrt{2}$ with $a, b \in \{0, 1\}$ [14], which are stabilizer states, and their protocol measures the stabilizers $\sigma_Z \otimes \sigma_X$ and $\sigma_X \otimes \sigma_Z$ to self-test them. Here, $|\pm\rangle := (|0\rangle \pm |1\rangle)/\sqrt{2}$ with $\{|0\rangle, |1\rangle\}$ being the computational basis, and σ_Z and σ_X are the Pauli-Z and -X operators, respectively. The underlying primitives of their protocol are the *extended noisy trapdoor claw-free function* (ENTCF) families introduced in [19,20] that are constructed from the LWE problem. The ENTCF families consist of two families of function pairs: one used to check the Pauli-Z operator and the other used for checking the Pauli-X operator. Hence, it should be straightforward to extend the result in [14] to all the stabilizer states whose stabilizers are tensor products of the Pauli-Z and -X operators. However, for other states, such as nonstabilizer states, constructing C-ST protocols is nontrivial.

Among nonstabilizer states, hypergraph states [21], generated by applying controlled-controlled-Z (CCZ) gates on graph states [22], are useful in various quantum information processing tasks, such as preparing a magic state [23] for quantum computation, decreasing the number of bases for measurement-based quantum computation [24,25], enhancing the amount of violation of Bell's inequality [26], and demonstrating quantum supremacy [27]. Experimentally, generating hypergraph states with high fidelity is generally hard since it requires CCZ gates. Hence, it is important to certify whether a generated state is the target hypergraph state. Indeed, several certification methods have been invented [28–30], where the measurements are assumed to be *trusted*.

In this Letter, we construct a C-ST protocol for the entangled magic state $CCZ|+\rangle^{\otimes 3}$. This hypergraph state is useful for use as a magic state or a building block of Union Jack states [25], and for realizing the violation of Bell's inequality [26]. As for magic states, $T|+\rangle$ with $T := |0\rangle\langle 0| + e^{i\pi/4}|1\rangle\langle 1|$ is a major one, but we show that no C-ST protocol can be constructed for it within the framework of [14].

We explain an intuitive idea of how to construct the C-ST protocol for $CCZ|+\rangle^{\otimes 3}$. This state is a simultaneous $+1$ eigenstate of $\sigma_{X,1}CZ_{23}$, $\sigma_{X,2}CZ_{13}$, and $\sigma_{X,3}CZ_{12}$, which we call *generalized stabilizers*. Here, $\sigma_{X,i}$ and CZ_{jk} denote the Pauli-X operator acting on the ith qubit and the controlled-Z (CZ) gate acting on the jth and kth qubits, respectively. Since these three operators are not the tensor products of Pauli Z and X, the arguments in [14] cannot be directly applied. To overcome this problem, we generalize the idea in [29]. This shows that expected values of the generalized stabilizers for a state ρ can be estimated by measuring the individual qubits of ρ with the ideal Pauli-Z and -X measurements followed by classical processing. Since the ideality of the measurements is not assumed in the self-testing scenario, we generalize the result in [29] so that it works even if the measurements are untrusted.

In constructing C-ST protocols for n-qubit states, there are two obstacles that must be overcome. Our construction would overcome one of them, and we will discuss that in Discussion section.

Recently, by exploiting the ENTCF families, various protocols have been invented for the proof of quantumness [19,31–34], verification of quantum computations [20,35–37], remote state preparation [38,39], and zero-knowledge arguments for quantum computations [40–42]. We show that our self-testing protocol for the entangled magic state is applicable to another type of proof of quantumness where the classical verifier can certify whether the device generates a state having nonzero magic. The magic represents the nonstabilizerness, and it is regarded as quantumness in the sense that implementing non-Clifford gates via injection of nonstabilizer states upgrades classically simulatable Clifford circuits to universal quantum circuits.

Computational self-testing of magic states. First, we show that it is impossible to construct a C-ST protocol for the magic state $T|+\rangle$ with the same usage of ENTCF families in [14]. More specifically, with the current usage of these families, the classical verifier can only check Pauli-Z and -X measurements, but the statistics of the outcomes of these two measurements are the same for $T|+\rangle$ and $T^\dagger|+\rangle$ [43]. Therefore, the classical verifier accepts the prover even when the prover generates $T^\dagger|+\rangle$, which violates the aforementioned soundness.

Next, we turn to the C-ST protocol for the entangled magic state. Before we describe it, we briefly introduce the main properties of the ENTCF families [19,20], where the formal definitions are given in Sec. I of the Supplemental Material [44].

Let $\mathcal{X}$ and $\mathcal{Y}$ be finite sets specified by a security parameter (i.e., the value that determines the concrete hardness of solving the underlying LWE problem). ENTCF families consist of two families, $\mathcal{F}$ and $\mathcal{G}$, of function pairs such that each of the functions injectively maps an element of $\mathcal{X}$ to the one of $\mathcal{Y}$ [45]. A function f in these families is injective, namely $f(x) \neq f(x')$ if $x \neq x' \in \mathcal{X}$. A function pair $(f_{k,0}, f_{k,1})$ in $\mathcal{F} = \{(f_{k,0}, f_{k,1})\}_k$ is indexed by a key k, which is public information specifying parameters in the LWE problem, and $f_{k,0}$ and $f_{k,1}$ have the same image over $\mathcal{X}$. Hence, given $y \in \mathcal{Y}$, there exists a claw $(x_0(k,y), x_1(k,y))$ in $\mathcal{X}$ satisfying $y = f_{k,0}(x_0(k,y)) = f_{k,1}(x_1(k,y))$. The function pair is called *claw-free* if it is hard to find a claw in quantum polynomial time. For a claw $(x_0(k,y), x_1(k,y))$ and $d \in \mathcal{X}$, we define bit $u(k,y,d) := d \cdot (x_0(k,y) \oplus x_1(k,y))$. A function pair $(f_{k,0}, f_{k,1})$ in the other family of function pairs $\mathcal{G} = \{(f_{k,0}, f_{k,1})\}_k$ is also indexed by a key k, but $f_{k,0}$ and $f_{k,1}$ have disjoint images over $\mathcal{X}$. Because of its disjointness, bit $b(k,y)$ is uniquely determined such that, given k and y, there exists an element x satisfying $y = f_{k,b(k,y)}(x)$.

Depending on the family of function pairs, the verifier generates a key k and trapdoor information t_k. The trapdoor is a piece of secret information that enables the verifier to efficiently compute an element x from $y = f_{k,b}(x)$ for any $b \in \{0,1\}$.

Below, we describe Protocol 1, which consists of a three-round interaction between the classical verifier and the computationally bounded quantum prover (see Fig. 1). The target state of our C-ST protocol is the Z-rotated entangled magic state, which is defined for $s_1, s_2, s_3 \in \{0,1\}$ by

$$\left|\phi_{\mathrm{H}}^{(s_1,s_2,s_3)}\right\rangle := \left(\sigma_Z^{s_1} \otimes \sigma_Z^{s_2} \otimes \sigma_Z^{s_3}\right) CCZ|+\rangle^{\otimes 3}. \tag{1}$$

In the protocol description, $x \in_R \mathcal{T}$ means that the variable x is chosen from set $\mathcal{T}$ uniformly at random.

Protocol 1

(1) The verifier chooses bases $\boldsymbol{\theta} := \theta_1\theta_2\theta_3 \in_R \mathcal{B} := \{000, 001, 010, 100, 111\}$. The basis choices 0 and 1 correspond to the computational and the Hadamard basis, respectively. We call the basis choice $\boldsymbol{\theta} \in \{000, 001, 010, 100\}$ the *test case* and $\boldsymbol{\theta} = 111$ the *hypergraph case*.

(2) For each $i \in \{1,2,3\}$, the verifier chooses the function family $\mathcal{G}$ ($\mathcal{F}$) if $\theta_i = 0$ ($\theta_i = 1$). Depending on the chosen families, the verifier generates keys k_1, k_2, k_3 and trapdoors $t_{k_1}, t_{k_2}, t_{k_3}$. Then, the verifier sends keys k_1, k_2, k_3 to the prover but keeps trapdoors $t_{k_1}, t_{k_2}, t_{k_3}$ secret from the prover.

(3) The verifier receives $y_1, y_2, y_3 \in \mathcal{Y}$ from the prover.

(4) The verifier chooses a round type from {preimage round, Hadamard round} uniformly at random and sends it to the prover.

(i) For a preimage round, the verifier receives preimages $(b_1, x_1; b_2, x_2; b_3, x_3)$ from the prover with $b_i \in \{0,1\}$ and $x_i \in \mathcal{X}$. The verifier rejects the prover and sets a flag $flag \leftarrow fail_{\mathrm{Pre}}$ unless all the preimages are correct [namely, $f_{k_i,b_i}(x_i) = y_i$ holds for $i = 1,2,3$].

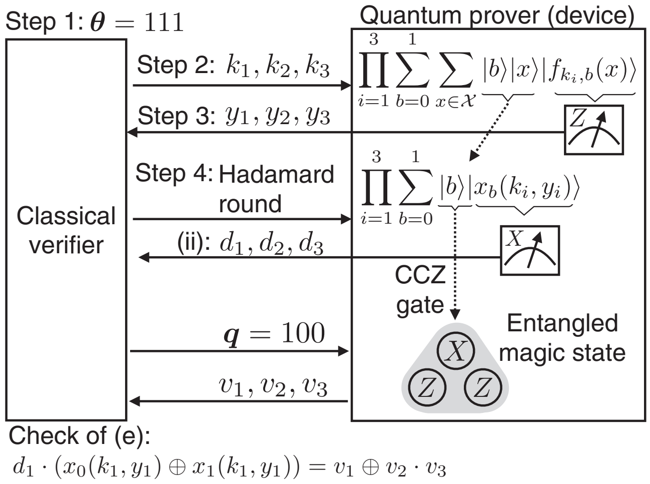
Step 1: $\boldsymbol{\theta} = 111$
Quantum prover (device)
Step 2: k_1, k_2, k_3
$\prod_{i=1}^{3}\sum_{b=0}^{1}\sum_{x\in\mathcal{X}} |b\rangle|x\rangle|f_{k_i,b}(x)\rangle$
Step 3: y_1, y_2, y_3
Z
Step 4: Hadamard round
$\prod_{i=1}^{3}\sum_{b=0}^{1} |b\rangle|x_b(k_i, y_i)\rangle$
Classical verifier
(ii): d_1, d_2, d_3
X
CCZ gate
Entangled magic state
$\boldsymbol{q} = 100$
X
Z
Z
v_1, v_2, v_3
Check of (e):
$d_1 \cdot (x_0(k_1, y_1) \oplus x_1(k_1, y_1)) = v_1 \oplus v_2 \cdot v_3$

FIG. 1. This figure shows the procedures for the honest device that passes step (e). If the device executes the displayed state preparation, measurements, and CCZ gate operation, where the register $|f_{k_i,b}(x)\rangle$ [second register $|x_b(k_i, y_i)\rangle$] is measured in the computational (Hadamard) basis, the entangled magic state is prepared. The measurement with $\boldsymbol{q} = 100$, which requests Pauli-X (-Z) measurement on the first qubit (second and third qubits), corresponds to measuring the generalized stabilizer of the entangled magic state. Therefore, the outcomes v_1, v_2, v_3 of this honest device pass the check at step (e).

(ii) For a Hadamard round, the verifier receives $d_1, d_2, d_3 \in \mathcal{X}$ from the prover. Then, the verifier sends measurement bases $q_1, q_2, q_3 \in_R \{0, 1\}$ to the prover, and the prover returns measurement outcomes $v_1, v_2, v_3 \in \{0, 1\}$. Depending on the bases $\boldsymbol{\theta}$, the verifier executes the following checks. If the flag is set, the verifier rejects the prover.

(a) $\boldsymbol{\theta} = 000$: set $flag \leftarrow fail_{\rm Test}$ if, for $i \in_R \{1, 2, 3\}$, $q_i = 0$ and $b(k_i, y_i) \neq v_i$ hold.

(b) $\boldsymbol{\theta} = 100$: set $flag \leftarrow fail_{\rm Test}$ if $q_1 = 1$ and $u(k_1, y_1, d_1) \oplus b(k_2, y_2) \cdot b(k_3, y_3) \neq v_1$ hold.

(c) $\boldsymbol{\theta} = 010$: set $flag \leftarrow fail_{\rm Test}$ if $q_2 = 1$ and $u(k_2, y_2, d_2) \oplus b(k_1, y_1) \cdot b(k_3, y_3) \neq v_2$ hold.

(d) $\boldsymbol{\theta} = 001$: set $flag \leftarrow fail_{\rm Test}$ if $q_3 = 1$ and $u(k_3, y_3, d_3) \oplus b(k_1, y_1) \cdot b(k_2, y_2) \neq v_3$ hold.

(e) $\boldsymbol{\theta} = 111$: set $flag \leftarrow fail_{\rm Hyper}$ if one of the following holds:
$\boldsymbol{q} = 100$ and $u(k_1, y_1, d_1) \neq v_1 \oplus v_2 \cdot v_3$,
$\boldsymbol{q} = 010$ and $u(k_2, y_2, d_2) \neq v_2 \oplus v_1 \cdot v_3$,
$\boldsymbol{q} = 001$ and $u(k_3, y_3, d_3) \neq v_3 \oplus v_1 \cdot v_2$,
with $\boldsymbol{q} := q_1q_2q_3$.

Completeness. We show in Theorem 1 that Protocol 1 satisfies the aforementioned completeness.

Theorem 1. There exists a computationally bounded quantum prover that is accepted in Protocol 1 with probability $1 - {\rm negl}(\lambda)$. Here, ${\rm negl}(\lambda)$ is a negligible function in the security parameter λ, namely a function that decays faster than any inverse polynomial in λ.

The device is accepted in Protocol 1 if all the checks in the preimage and Hadamard rounds are passed, whose details are given in Sec. III of the Supplemental Material [44]. Here, we particularly explain the procedures for the honest device that can pass step (e). Since step (e) corresponds to the check of the generalized stabilizers, the honest device passes this check if it generates the entangled magic state. Figure 1 shows how to generate this state. After returning d_1, d_2, d_3, the state of the honest device is close to a tensor product of three Pauli-X basis eigenstates due to the claw-free property of function family $\mathcal{F}$, and hence applying the CCZ gate to this state results in the entangled magic state up to Pauli-Z operators.

Soundness. We next show in Theorem 2 that Protocol 1 satisfies the aforementioned soundness. For the purpose of self-testing, we are interested in the last round of the interaction [step 4(ii)] when $\boldsymbol{\theta} = 111$. Here, the verifier sends the measurement bases $\boldsymbol{q} \in \{0, 1\}^3$ to the device and receives the outcomes $\boldsymbol{v} := v_1v_2v_3 \in \{0, 1\}^3$. We can model the behavior of the device in step 4(ii) when $\boldsymbol{\theta} = 111$ by the unnormalized state $\sigma^{(s_1,s_2,s_3)}$ on the device's Hilbert space $\mathcal{H}$ with $s_1, s_2, s_3 \in \{0, 1\}$ and projective measurements $\{P_{\boldsymbol{q}}^{(\boldsymbol{v})}\}_{\boldsymbol{v}}$ on this state that output $\boldsymbol{v}$ given inputs $\boldsymbol{q}$ to the device. Here, s_i is determined by bit $u(k_i, y_i, d_i)$ for $i \in \{1, 2, 3\}$.

The goal of Protocol 1 is to ensure that the state $\sigma'^{(s_1,s_2,s_3)} := \sigma^{(s_1,s_2,s_3)}/{\rm tr}[\sigma^{(s_1,s_2,s_3)}]$ is close to the entangled magic state defined in Eq. (1), which is the target state to certify, and measurements $P_{\boldsymbol{q}}^{(\boldsymbol{v})}$ are specific tensor products of Pauli measurements, up to an isometry and a small error. This error is quantified by the probabilities that the verifier rejects the prover, namely the verifier sets a $flag$ to $fail_{\rm Pre}$, $fail_{\rm Test}$, or $fail_{\rm Hyper}$. We now present the soundness as follows, where $p_{\rm a} := \Pr\{flag \leftarrow fail_{\rm a}\}$ with ${\rm a} \in \{{\rm Pre}, {\rm Test}, {\rm Hyper}\}$, $||\cdot||_1$ being the trace norm, and $P[|\cdot\rangle] := |\cdot\rangle\langle\cdot|$.

Theorem 2. Consider a device that is rejected by the verifier with probabilities $p_{\rm Pre}$, $p_{\rm Test}$, and $p_{\rm Hyper}$, and make the LWE assumption. Let $|\phi_{\rm H}^{(s_1,s_2,s_3)}\rangle$ be the target entangled magic state to certify with $s_1, s_2, s_3 \in \{0, 1\}$, state $\sigma'^{(s_1,s_2,s_3)}$ defined above, λ the security parameter, $\mathcal{H}$ the device's Hilbert space, and $\mathcal{H}'$ some Hilbert space. Then, there exists an isometry $V : \mathcal{H} \to \mathbb{C}^8 \otimes \mathcal{H}'$, states $\zeta_{\mathcal{H}'}^{(s_1,s_2,s_3)}$ on $\mathcal{H}'$, and a constant $r > 0$ such that, in the case of $\boldsymbol{\theta} = 111$ (hypergraph case),

$$\left|\left|V\sigma'^{(s_1,s_2,s_3)}V^\dagger - |\phi_{\rm H}^{(s_1,s_2,s_3)}\rangle\langle\phi_{\rm H}^{(s_1,s_2,s_3)}| \otimes \zeta_{\mathcal{H}'}^{(s_1,s_2,s_3)}\right|\right|_1^2 \leqslant O(p_{\rm Pre}^r + p_{\rm Test}^r + p_{\rm Hyper}^r) + {\rm negl}(\lambda), \qquad (2)$$

and, for any $a, b, c \in \{0, 1\}$ and $q_1, q_2, q_3 \in \{0, 1\}$,

$$\Big|\Big|VP_{q_1q_2q_3}^{(abc)}\sigma'^{(s_1,s_2,s_3)}P_{q_1q_2q_3}^{(abc)}V^\dagger - P[|a_{q_1}, b_{q_2}, c_{q_3}\rangle] |\phi_{\rm H}^{(s_1,s_2,s_3)}\rangle\langle\phi_{\rm H}^{(s_1,s_2,s_3)}|P[|a_{q_1}, b_{q_2}, c_{q_3}\rangle] \otimes \zeta_{\mathcal{H}'}^{(s_1,s_2,s_3)}\Big|\Big|_1^2 \leqslant O(p_{\rm Pre}^r + p_{\rm Test}^r + p_{\rm Hyper}^r) + {\rm negl}(\lambda). \qquad (3)$$

Here, $|a_{q_1}\rangle$ with $a, q_1 \in \{0, 1\}$ is $|a_{q_1}\rangle := |a\rangle$ if $q_1 = 0$ and $|a_{q_1}\rangle := (|0\rangle + (-1)^a|1\rangle)/\sqrt{2}$ if $q_1 = 1$. $|b_{q_2}\rangle$ and $|c_{q_3}\rangle$ are defined analogously.

Here, Eq. (2) guarantees how precisely the prover generates the entangled magic state under the isometry V, and Eq. (3) how precisely it implements the specific single-qubit measurements on it according to the measurement bases $\boldsymbol{q}$. Using $V^\dagger V = I$, Eq. (3) also reveals that the actual probability distribution of the device $\{{\rm tr}[P_{q_1q_2q_3}^{(abc)}\sigma'^{(s_1,s_2,s_3)}]\}_{a,b,c}$ is close to the ideal one obtained by measuring $|\phi_{\rm H}^{(s_1,s_2,s_3)}\rangle$ in the Pauli-Z and -X bases. Note that Eqs. (2) and (3) are analogous to the statements in the traditional self-testing (see, e.g., [11–13]). One notable difference from the traditional self-testing is that our isometry V is allowed to be a global operation acting on the whole device's Hilbert space $\mathcal{H}$ because we do consider the single quantum device. The proof of Theorem 2 is given in Sec. IV of the Supplemental Material [44].

Applications to the proof of quantumness. Recently, various protocols have been invented to enable the classical verifier to certify the quantumness of the device [19,20,31,33,34,36]. Here, the meaning of quantumness differs depending on the protocols. For instance, the protocols [19,33,34] verify whether the prover has a superposed state or not, the protocols [20,36] verify whether the prover can efficiently solve BQP problems, and the protocol [31] verifies that the prover can query to an oracle in superposition. Importantly, if the prover is accepted by the verifier, then the prover has quantum capability.

Our C-ST protocol given as Protocol 1 can be used for the proof of magic under the IID scenario where the device's functionality is the same for each repetition of the protocol. To measure the magic, we focus on the max-relative entropy of magic [46]. We adopt this measure for simplicity, but our arguments can be applied to any reasonable measure of the magic. Let $\mathfrak{D}_{\max}(\rho) := \log_2 [1 + R_g(\rho)]$ be the max-relative entropy of magic of an n-qubit state ρ, where $R_g(\rho)$ is defined by the minimum of $t \geqslant 0$ such that $\rho \in (1+t)\mathrm{STAB} - t\mathcal{S}$, $\mathrm{STAB} \subset \mathcal{S}$ is the convex hull of all n-qubit stabilizer states, and $\mathcal{S}$ is the set of n-qubit states. If ρ is a stabilizer state, $R_g(\rho) = 0$, and hence $\mathfrak{D}_{\max}(\rho) = 0$. By contraposition, if $\mathfrak{D}_{\max}(\rho) > 0$, state ρ is a nonstabilizer state. Based on above observations, we outline the protocol for the proof of magic as follows [47] (see Sec. V of the Supplemental Material [44]).

Protocol 2

(1) The verifier and prover repeat Protocol 1 a constant number of times, and the verifier estimates the error probabilities p_{Pre}, p_{Test}, and p_{Hyper} using Hoeffding's inequality from the numbers of set flags.

(2) If the estimated trace norm T_{est} [the square root of the right-hand side of Eq. (2)] is strictly less than $1/3$, then the verifier accepts the prover. Otherwise, the verifier rejects the prover.

We first show that if our protocol is passed, with a small significance level [48], which can be set to any value such as 10^{-10}, the verifier can guarantee that the prover generates a state having nonzero magic up to the isometry. If state ρ has no magic, we have $\langle\phi_{\mathrm{H}}^{(s_1,s_2,s_3)}|\rho|\phi_{\mathrm{H}}^{(s_1,s_2,s_3)}\rangle \leqslant 9/16$ because for any stabilizer state $|\psi\rangle$, $F := |\langle\psi|\phi_{\mathrm{H}}^{(s_1,s_2,s_3)}\rangle|^2 \leqslant 9/16$ [49]. Since $F \leqslant 9/16$ results in $||\rho - |\phi_{\mathrm{H}}^{(s_1,s_2,s_3)}\rangle\langle\phi_{\mathrm{H}}^{(s_1,s_2,s_3)}|||_1 \geqslant 1/2$ [50], Hoeffding's inequality with precision $1/6$ implies that $T_{\mathrm{est}} < 1/3$ holds with probability 10^{-10}. Therefore, such a state ρ is accepted with probability of at most 10^{-10}.

On the other hand, there is a strategy that passes this protocol with probability $1 - 10^{-10}$. This is because Theorem 1 states that there exists a prover's strategy that achieves all of the error probabilities p_{Pre}, p_{Test}, and p_{Hyper} being $\mathrm{negl}(\lambda)$, and hence, from Hoeffding's inequality, $T_{\mathrm{est}} \leqslant \mathrm{negl}(\lambda) + 1/6 < 1/3$ holds except for probability 10^{-10}.

Discussions. In this Letter, we have constructed a computational self-testing protocol for the three-qubit entangled magic state. To generalize [14] to n-qubit states, there are two obstacles: (1) The verifier chooses the state bases $\theta_1 \ldots \theta_n \in_R \{0, 1\}^n$ with which the prover is requested to generate the state for n times. Since the target state is prepared only when all the θ's are 1, it takes exponential time on average to generate the target state. (2) The verifier checks all the patterns of measurements, namely it checks the correctness of Pauli-Z and -X measurements for each qubit, which takes 2^n times.

Our construction would solve the first problem. We have shown for $n = 3$ that the number of state bases is sufficient to be $n + 2$, which means the target state is prepared on average by repeating the protocol $(n + 2)$ times. We leave its rigorous analysis and the second problem as future work.

Note added. Recently, we became aware of independent related works [52] and [53] that extend the result [14] to self-test n Bell states and n BB84 states, respectively. By exploiting these results, it could be possible to extend our result to self-test n tensor products of CCZ magic states $CCZ|+\rangle^{\otimes 3}$.

Acknowledgments. The authors thank Tony Metger for valuable discussions on [14], and Go Kato, Yasuhiro Takahashi, and Tomoyuki Morimae for helpful comments. A.M. is supported by JST, ACT-X Grant No. JPMJAX210O, Japan. Y.T. is supported by MEXT Quantum Leap Flagship Program (MEXT Q-LEAP) Grants No. JPMXS0118067394 and No. JPMXS0120319794, the Grant-in-Aid for Scientific Research (A) No. JP22H00522 of JSPS, and JST (Moonshot R&D – MILLENNIA Program) Grant No. JPMJMS2061. S.T. is partially supported by the Grant-in-Aid for Transformative Research Areas No. JP20H05966 of JSPS, and the Grant-in-Aid for Scientific Research (A) No. JP22H00522 of JSPS.

[1] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[2] D. Mayers and A. Yao, in *Proceedings of the 39th Annual Symposium on Foundations of Computer Science* (IEEE, Piscataway, NJ, 1998), pp. 503–509.

[3] C. C. W. Lim, C. Portmann, M. Tomamichel, R. Renner, and N. Gisin, Phys. Rev. X **3**, 031006 (2013).

[4] U. Vazirani and T. Vidick, Phys. Rev. Lett. **113**, 140501 (2014).

[5] A. Ekert and R. Renner, Nature (London) **507**, 443 (2014).

[6] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, and T. Vidick, Nat. Commun. **9**, 459 (2018).

[7] T. Metger, Y. Dulek, A. Coladangelo, and R. Arnon-Friedman, New J. Phys. **23**, 123021 (2021).

[8] B. W. Reichardt, F. Unger, and U. Vazirani, Nature (London) **496**, 456 (2013).

[9] M. Hajdušek, C. A. Pérez-Delgado, and J. F. Fitzsimons, arXiv:1502.02563.

[10] D. Mayers and A. Yao, Quantum Inf. Comput. **4**, 273 (2004).

[11] M. McKague, T. H. Yang, and V. Scarani, J. Phys. A: Math. Theor. **45**, 455304 (2012).

[12] A. Coladangelo, K. Goh, and V. Scarani, Nat. Commun. **8**, 15485 (2017).

[13] I. Šupić and J. Bowles, Quantum **4**, 337 (2020).

[14] T. Metger and T. Vidick, Quantum **5**, 544 (2021).

[15] The LWE problem is to solve a noisy system of linear equations, and so far there exists no efficient quantum algorithm to solve this problem.

[16] O. Regev, J. ACM **56**, 1(2009).

[17] Note that encrypted messages using classical public-key cryptography are decrypted once it becomes technologically feasible to break the underlying computational assumption. On the other hand, the LWE assumption supposed in [14] is only exploited to prevent the malicious prover from tricking the verifier into accepting the prover as honest. Hence, as long as the LWE assumption holds during the self-testing protocol, if this assumption is broken after the protocol, the results already obtained never be compromised.

[18] A. Broadbent and P. Yuen, arXiv:2111.08595.

[19] Z. Brakerski, Z. P. Christiano, U. Mahadev, U. Vazirani, and T. Vidick, *in Proceedings of the 59th Annual Symposium on Foundations of Computer Science* (IEEE, Piscataway, NJ, 2018), pp. 320–331.

[20] U. Mahadev, *in Proceedings of the 59th Annual Symposium on Foundations of Computer Science* (IEEE, Piscataway, NJ, 2018), pp. 259–267.

[21] M. Rossi, M. Huber, D. Bruß, and C. Macchiavello, New J. Phys. **15**, 113022 (2013).

[22] R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).

[23] S. Bravyi and A. Kitaev, Phys. Rev. A **71**, 022316 (2005).

[24] Y. Takeuchi, T. Morimae, and M. Hayashi, Sci. Rep. **9**, 13585 (2019).

[25] J. Miller and A. Miyake, npj Quantum Inf. **2**, 16036 (2016).

[26] M. Gachechiladze, C. Budroni, and O. Gühne, Phys. Rev. Lett. **116**, 070401 (2016).

[27] M. J. Bremner, A. Montanaro, and D. J. Shepherd, Phys. Rev. Lett. **117**, 080501 (2016).

[28] T. Morimae, Y. Takeuchi, and M. Hayashi, Phys. Rev. A **96**, 062321 (2017).

[29] Y. Takeuchi and T. Morimae, Phys. Rev. X **8**, 021060 (2018).

[30] H. Zhu and M. Hayashi, Phys. Rev. Applied **12**, 054047 (2019).

[31] Z. Brakerski, K. Venkata, U. Vazirani, and T. Vidick, arXiv:2005.04826.

[32] G. D. Kahanamoku-Meyer, S. Choi, U. Vazirani, and N. Y. Yao, arXiv:2104.00687.

[33] S. Hirahara and F. Le Gall, in *Proceedings of the 46th International Symposium on Mathematical Foundations of Computer Science (MFCS 2021)* (2021), pp. 59:1–59:15.

[34] Z. Liu and A. Gheorghiu, arXiv:2107.02163.

[35] G. Alagic, A. M. Childs, A. B. Grilo, and S.-H. Hung, in *Theory of Cryptography: 18th International Conference, TCC 2020*, Lecture Notes in Computer Science, Vol. 12552 (Springer, Cham, 2020), Part III, pp. 153–180.

[36] N.-H. Chia, K.-M. Chung, and T. Yamakawa, in *Theory of Cryptography: 18th International Conference, TCC 2020*, Lecture Notes in Computer Science, Vol. 12552 (Springer, Cham, 2020), Part III, pp. 181–206.

[37] K. Chung, Y. Lee, H. H. Lin, and X. Wu, arXiv:2012.04848.

[38] A. Gheorghiu and T. Vidick, in *Proceedings of the 60th Annual Symposium on Foundations of Computer Science* (IEEE, Piscataway, NJ, 2019), pp. 1024–1033.

[39] A. Cojocaru, L. Colisson, E. Kashefi, and P. Wallden, in *ASIACRYPT 2019: International Conference on The Theory and Application of Cryptology and Information Security* (IACR, Carson City, NV, 2019), pp. 615–645.

[40] T. Morimae and T. Yamakawa, arXiv:2102.09149.

[41] A. Coladangelo, T. Vidick, and T. Zhang, in *CRYPTO 2020: International Cryptology Conference* (IACR, Carson City, NV, 2020), Part III, pp. 799–828.

[42] T. Vidick and T. Zhang, Quantum **4**, 266 (2020).

[43] When $T|+\rangle$ is measured in the Pauli-Z basis, the outcomes 0 and 1 are obtained with equal probability. On the other hand, if it is measured in the Pauli-X basis, they are obtained with probabilities $(2+\sqrt{2})/4$ and $(2-\sqrt{2})/4$, respectively. These statistics are the same for $T^\dagger|+\rangle$.

[44] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevA.106.L010601 for detailed information of the proofs of our theorems and Protocol 2.

[45] Note that we assume for simplicity that the outputs of the functions are elements of set $\mathcal{Y}$, but, precisely, the outputs are probability distributions over $\mathcal{Y}$. The rigorous definitions of ENTCF families are given in Sec. I of the Supplemental Material [44].

[46] Z.-W. Liu and A. Winter, PRX Quantum **3**, 020333 (2022).

[47] Note that as a related work to our proof of magic, the problem of asking whether a given state is any stabilizer state was studied in the *device-dependent* scenario [51]. Our protocol considers its opposite problem, i.e., asking whether a given state is *not* any stabilizer state, in the *device-independent* scenario.

[48] Note that the significant level is defined by the maximum probability of passing our protocol with a state having no magic.

[49] S. Bravyi, D. Browne, P. Calpin, E. Campbell, D. Gosset, and M. Howard, Quantum **3**, 181 (2019).

[50] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition* (Cambridge University Press, Cambridge, 2010).

[51] D. Gross, S. Nezami, and M. Walter, Commun. Math. Phys. **385**, 1325 (2021).

[52] H. Fu, D. Wang, and Q. Zhao, arXiv:2201.13430 (2022).

[53] A. Gheorghiu, T. Metger, and A. Poremba, arXiv:2201.13445.