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*

In the seminal paper [Metger and Vidick, Quantum '21], they proposed a computational self-testing protocol for Bell states in a single quantum device. Their protocol relies on the fact that the target states are stabilizer states, and hence it is highly non trivial to reveal whether the other class of quantum states, *non-stabilizer states*, can be self-tested within their framework. Among non-stabilizer states, magic states are indispensable resources for universal quantum computation. In this letter, 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 non zero magic.

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 was proposed [14], which replaces the non-communicating multiple provers with a single computationally bounded quantum prover who only performs efficient quantum computation. To remove the non communication assumption, their protocol relies on a standard assumption in post-quantum cryptography where the Learning with Errors (LWE) problem [44] cannot be solved by quantum computers in polynomial time [15]. 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 [45].

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 computationally bounded single-device self-testing (CB-SD-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 the measurements on it with high precision as required by the verifier. So far, the CB-SD-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 [16, 17] 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 non-stabilizer states, constructing CB-SD-ST protocols is non trivial.

Among non-stabilizer states, hypergraph states [18], generated by applying controlled-controlled-Z (CCZ) gates on graph states [19], are useful in various quantum information processing tasks, such as preparing a magic state [20] for quantum computation, decreasing the number of bases for measurement-based quantum computation [21, 22], enhancing the amount of violation of Bell's inequality [23], and demonstrating quantum supremacy [24]. 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 [25–27], where the measurements are assumed to be *trusted*.

In this letter, we construct a CB-SD-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 [22], and for realizing the violation of Bell's inequality [23]. As for magic states, $T|+\rangle$ with $T := |0\rangle\langle 0| + e^{\mathrm{i}\pi/4}|1\rangle\langle 1|$ is a major one, but we show that no CB-SD-ST protocol can be constructed for it within the framework of [14].

We explain an intuitive idea of how to construct the CB-SD-ST protocol for the entangled magic state $CCZ|+\rangle^{\otimes 3}$. 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 i^{th} qubit and the controlled-Z (CZ) gate acting on the j^{th} and k^{th} 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 [26]. 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 [26] so that it works even if the measurements are untrusted.

In constructing CB-SD-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 at the end of this letter.

Recently, by exploiting the ENTCF families, various protocols have been invented for the proof of quantumness [16, 28–31], verification of quantum computations [17, 32–34], remote state preparation [35, 36], and zero-knowledge proofs for quantum computations [37–39]. 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 non zero magic. The magic represents the non-stabilizerness, and it is regarded as quantumness in the sense that implementing non-Clifford gates via the injection of non-stabilizer 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 CB-SD-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 $T^\dagger|+\rangle$ [46]. 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 CB-SD-ST protocol for the entangled magic state. Before we describe it, we briefly introduce the main properties of the ENTCF families [16, 17], where the formal definitions are given in the supplementary material.

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 $\mathcal{Y}$ [47]. 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 CB-SD-ST protocol is the Z-rotated entangled magic state, which is defined for $s_1, s_2, s_3 \in \{0,1\}$ by

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

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 $\boldsymbol{\theta} := \theta_1\theta_2\theta_3$ uniformly at random from set $\mathcal{B} := \{000, 001, 010, 100, 111\}$. 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 the basis choice $\boldsymbol{\theta} = 111$ 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.

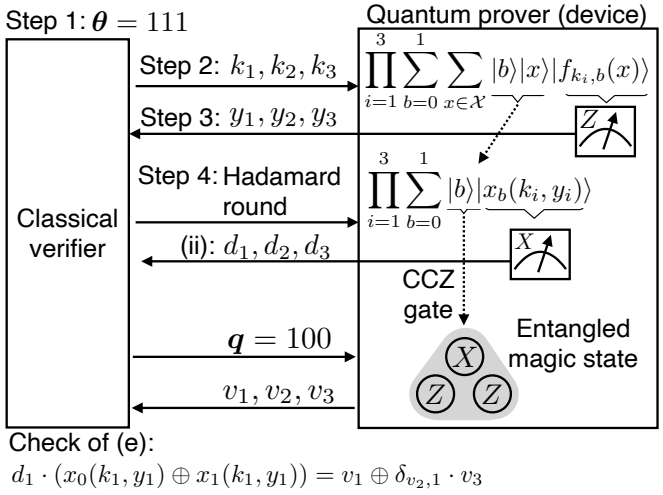

FIG. 1: This figure shows the procedures for the honest device that passes step (e). If the device executes the displayed state preparation, measurements, and CCZ gate operation, where the 3rd register $|f_{k_i,b}(x)\rangle$ [2nd register $|x_b(k_i, y_i)\rangle$] is measured in the computational [Hadamard] basis, the entangled magic state is prepared. The measurement with $\boldsymbol{q} = 100$, which requests Pauli-X (Z) measurement on the 1st qubit (2nd and 3rd 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 passes the check at step (e).

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 $i = 1, 2, 3$).

   (ii) For an 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 $v_1, v_2, v_3 \in \{0, 1\}$ to the verifier. 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 $flag \leftarrow fail_{\mathrm{Test}}$ 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 $flag \leftarrow fail_{\mathrm{Test}}$ 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 $flag \leftarrow fail_{\mathrm{Test}}$ 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 $flag \leftarrow fail_{\mathrm{Test}}$ 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 $flag \leftarrow fail_{\mathrm{Hyper}}$ if one of the following holds:
   $\boldsymbol{q} = 100$ and $u(k_1, y_1, d_1) \neq v_1 \oplus \delta_{v_2,1} \cdot v_3$,
   $\boldsymbol{q} = 010$ and $u(k_2, y_2, d_2) \neq v_2 \oplus \delta_{v_1,1} \cdot v_3$,
   $\boldsymbol{q} = 001$ and $u(k_3, y_3, d_3) \neq v_3 \oplus \delta_{v_1,1} \cdot v_2$,
   with $\boldsymbol{q} := q_1 q_2 q_3$ and $\delta_{x,y}$ being the Kronecker delta.

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* $1 - \mathrm{negl}(\lambda)$. *Here,* $\mathrm{negl}(\lambda)$ *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 the supplementary material. 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 $\boldsymbol{v} := v_1 v_2 v_3 \in \{0, 1\}^3$. 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 $\sigma'^{(s_1,s_2,s_3)} := \sigma^{(s_1,s_2,s_3)} / \mathrm{tr}[\sigma^{(s_1,s_2,s_3)}]$ 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 $fail_{\mathrm{Pre}}$, $fail_{\mathrm{Test}}$ or $fail_{\mathrm{Hyper}}$. We now present the soundness as follows, where $p_{\mathrm{a}} := \Pr\{flag \leftarrow fail_{\mathrm{a}}\}$ with $\mathrm{a} \in \{\mathrm{Pre}, \mathrm{Test}, \mathrm{Hyper}\}$, $||\cdot||_1$ 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),*

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

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

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

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. We give the proof of Theorem 2 in the supplementary material.

Applications to the proof of quantumness.— Recently, various protocols have been invented to enable the classical verifier to certify the quantumness of the device [16, 17, 28, 30, 31, 33]. Here, the meaning of quantumness differs depending on the protocols. For instance, the protocols [16, 30, 31] verify whether the prover has a superposed state or not, the protocols [17, 33] verify whether the prover can efficiently solve BQP problems, and the protocol [28] 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 CB-SD-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 [40]. We adopt this measure for simplicity, but our arguments can be applied to any reasonable measure of the magic. Let $\mathfrak{D}_{\max}(\rho):=\log(1+R_g(\rho))$ be the max-relative entropy of magic of an n-qubit state ρ, where $R_g(\rho)$ is defined by the minimum of $t\ge0$ such that $\rho\in(1+t){\rm STAB}-t\mathcal{S}$, ${\rm STAB}\subset\mathcal{S}$ 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 non-stabilizer state.

Based on above observations, we outline the protocol for the proof of magic as follows [48] (see the supplementary material for the details).

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

2. If the estimated trace norm $T_{\rm est}$ [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 [49], which can be set to any value such as 10^{-10}, the verifier can guarantee that the prover generates a state having non zero magic up to the isometry. If state ρ has no magic, we have $\langle\phi_{\rm H}^{(s_1,s_2,s_3)}|\rho|\phi_{\rm H}^{(s_1,s_2,s_3)}\rangle\le9/16$ because for any stabilizer state $|\psi\rangle$, $F:=|\langle\psi|\phi_{\rm H}^{(s_1,s_2,s_3)}\rangle|^2\le9/16$ [42]. Since $F\le9/16$ results in $||\rho-|\phi_{\rm H}^{(s_1,s_2,s_3)}\rangle\langle\phi_{\rm H}^{(s_1,s_2,s_3)}|||_1\ge1/2$ [43], Hoeffding's inequality with precision $1/6$ implies that $T_{\rm est}<1/3$ 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 $p_{\rm Pre},p_{\rm Test}$ and $p_{\rm Hyper}$ being ${\rm negl}(\lambda)$, and hence from Hoeffding's inequality, $T_{\rm est}\le{\rm negl}(\lambda)+1/6<1/3$ holds except for probability 10^{-10}.

Discussion.— In this letter, we have constructed a CB-SD-ST protocol for the three-qubit entangled magic state. To generalize [14] to n-qubit states, there seems to be two obstacles that must be overcome. (1) The verifier chooses the bases $\theta_1...\theta_n\in_R\{0,1\}^n$, i.e., the Pauli-$Z$ or X basis 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 bases $\boldsymbol{\theta}$ is

sufficient to be $n+2$, which are $\boldsymbol{\theta} = 000$, $\boldsymbol{\theta} = 111$, and $\boldsymbol{\theta}$'s with a single 1. Our construction could be generalized to n-qubit hypergraph states, where the target state can be prepared on average by repeating the protocol $(n+2)$ times. We leave its rigorous analysis and the second problem as future work.

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

[1] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[2] D. Mayers and A. Yao, Proceedings 39th Annual Symposium on Foundations of Computer Science (IEEE, 1998), pp. 503-509 (1998).
[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 **507**, 443 (2014).
[6] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, and T. Vidick, Nature Communications **9**, 459 (2018).
[7] T. Metger, Y. Dulek, A. Coladangelo, and R. Arnon-Friedman, arXiv:2010.04175 (2020).
[8] B. W. Reichardt, F. Unger, and U. Vazirani, Nature **496**,456 (2013).
[9] M. Hajdušek, C. A. Pérez-Delgado, and J. F. Fitzsimons,arXiv:1502.02563 (2015).
[10] D. Mayers and A. Yao, Quantum Info. Comput. **4**, 273 (2004).
[11] M. McKague, T. H. Yang, and V. Scarani, Journal of Physics A: Mathematical and Theoretical **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] O. Regev, J. ACM **56** (2009).
[16] Z. Brakerski, Z. P. Christiano, U. Mahadev, U. Vazirani, and T. Vidick, Proceedings of the 59th Annual Symposium on Foundations of Computer Science (2018) pp.320-331. (2018).
[17] U. Mahadev, Proceedings of the 59th Annual Symposium on Foundations of Computer Science (2018) pp.259-267 (2018).
[18] M. Rossi, M. Huber, D. Bruß, and C. Macchiavello, New Journal of Physics **15**, 113022 (2013).
[19] R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).
[20] S. Bravyi and A. Kitaev, Phys. Rev. A **71**, 022316 (2005).
[21] Y. Takeuchi, T. Morimae, and M. Hayashi, Scientific Reports **9**, 13585 (2019).
[22] J. Miller and A. Miyake, npj Quantum Information **2**, 16036 (2016).
[23] M. Gachechiladze, C. Budroni, and O. Gühne, Phys. Rev. Lett. **116**, 070401 (2016).
[24] M. J. Bremner, A. Montanaro, and D. J. Shepherd, Phys. Rev. Lett. **117**, 080501 (2016).
[25] T. Morimae, Y. Takeuchi, and M. Hayashi, Phys. Rev. A **96**, 062321 (2017).
[26] Y. Takeuchi and T. Morimae, Phys. Rev. X **8**, 021060 (2018).
[27] H. Zhu and M. Hayashi, Phys. Rev. Applied **12**, 054047 (2019).
[28] Z. Brakerski, K. Venkata, U. Vazirani, and T. Vidick, arXiv:2005.04826 (2020).
[29] G. D. Kahanamoku-Meyer, S. Choi, U. Vazirani, and N. Y. Yao, arXiv:2104.00687v1 (2021).
[30] S. Hirahara and F. Le Gall, arXiv:2105.05500v1 (2021).
[31] Z. Liu and A. Gheorghiu, arXiv:2107.02163v1 (2021).
[32] G. Alagic, A. M. Childs, A. B. Grilo, and S.-H. Hung, TCC 2020, Part III, pages 153-180 (2020).
[33] N.-H. Chia, K.-M. Chung, and T. Yamakawa, TCC 2020, Part III, volume 12552 of LNCS, pages 181-206 (2020).
[34] K. Chung, Y. Lee, H. H. Lin, and X. Wu, arXiv preprint arXiv:2012.04848 (2020).
[35] A. Gheorghiu and T. Vidick, Proceedings of the 60th Annual Symposium on Foundations of Computer Science (2019) pp. 1024-1033 (2019) (2019).
[36] A. Cojocaru, L. Colisson, E. Kashefi, and P. Wallden, ASIACRYPT 2019, pp. 615-645. (2019).
[37] T. Morimae and T. Yamakawa, arXiv:2102.09149 (2021).
[38] A. Coladangelo, T. Vidick, and T. Zhang, CRYPTO 2020, Part III, pages 799-828 (2020).
[39] T. Vidick and T. Zhang, Quantum **4**, 266 (2020).
[40] Z.-W. Liu and A. Winter, arXiv:2010.13817 (2020).
[41] D. Gross, S. Nezami, and M. Walter, Communications in Mathematical Physics 385, 1325 (2021).
[42] S. Bravyi, D. Browne, P. Calpin, E. Campbell, D. Gosset, and M. Howard, Quantum **3**, 181 (2019).
[43] M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information 10th Anniversary Edition (Cambridge University Press, 2010), ISBN 521635039.
[44] 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.
[45] 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.
[46] 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 $T^\dagger|+\rangle$.
[47] 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 the supplementary

material.

[48] 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 [41]. Our protocol considers its opposite problem, i.e., asking whether a given state is *not* any stabilizer state, in the *device-independent* scenario.

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

Supplementary material: 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*

I. PRELIMINARIES

A. Notations

Throughout the paper, we use the following notations. We use the bold symbol $\boldsymbol{A}$ meaning $A_1A_2A_3$. For $i \in \{1,2,3\}$, $\boldsymbol{A}_{\bar{i}}$ denotes $\boldsymbol{A}$ except for A_i. Let the Kronecker delta be

$$\delta_{x,y} = \begin{cases} 0 \text{ if } x \neq y \\ 1 \text{ if } x = y. \end{cases}$$

We denote by $|\mathcal{S}|$ the cardinality of set $\mathcal{S}$. For a bit $b \in \{0,1\}$, $\bar{b}$ denotes $b \oplus 1$. We denote $\mathrm{wt}(x)$ by the number of 1's in a bit string x.

We denote $\mathcal{H}$ by an arbitrary finite-dimensional Hilbert space. The set of linear operators on the Hilbert space $\mathcal{H}$ is denoted by $\mathcal{L}(\mathcal{H})$. For $A, B \in \mathcal{L}(\mathcal{H})$, we denote the commutator by $[A,B] = AB - BA$ and the anti-commutator by $\{A,B\} = AB + BA$. $\mathrm{Pos}(\mathcal{H})$ denotes the set of positive semidefinite operators on $\mathcal{H}$, and we denote the set of density matrices on $\mathcal{H}$ by $\mathcal{D}(\mathcal{H}) = \{A \in \mathcal{L}(\mathcal{H}) | A \in \mathrm{Pos}(\mathcal{H}), \mathrm{tr}[A] = 1\}$. A binary observable is defined as an observable (Hermitian operator) that only has eigenvalues $\in \{1, 0, -1\}$. For any binary observable O and $b \in \{0,1\}$, $O^{(b)}$ denotes the projector onto the $(-1)^b$-eigenspace of O. We denote the Pauli-Z and X observables by $\sigma_Z = \sum_{b=0}^{1} (-1)^b |b\rangle\langle b|$ and $\sigma_X = \sum_{b=0}^{1} (-1)^b |(-)^b\rangle\langle(-)^b|$, respectively. Here, $|(-)^b\rangle := (|0\rangle + (-1)^b|1\rangle)/\sqrt{2}$.

Let $\mathrm{negl}(\lambda)$ be a negligible function in the security parameter λ, namely a function that decays faster than any inverse polynomial in λ. For a countable set $\mathcal{X}$, $x \leftarrow \mathcal{X}$ denotes that x is chosen uniformly at random from $\mathcal{X}$.

B. Cryptographic Primitives

Here, we explain the noisy trapdoor claw-free function family, which is the cryptographic primitive underlying our self-testing protocol described in Sec. III.

Definition 1 (Hellinger Distance) *For two probability densities f_1 and f_2 over finite set $\mathcal{X}$, the Hellinger distance between f_1 and f_2 is defined as*

$$H^2(f_1, f_2) := 1 - \sum_{x \in \mathcal{X}} \sqrt{f_1(x) f_2(x)}.$$

Definition 2 (Noisy Trapdoor Claw-free Family [1]) *Let $\lambda \in \mathbb{N}$ be a security parameter. Let $\mathcal{X}$ and $\mathcal{Y}$ be finite sets. Let $\mathcal{K}_{\mathcal{F}}$ be a finite set of keys. A family of functions*

$$\mathcal{F} := \{f_{k,b} : \mathcal{X} \to \mathcal{D}_{\mathcal{Y}}\}_{k \in \mathcal{K}_{\mathcal{F}}, b \in \{0,1\}}$$

is called a noisy trapdoor claw-free (NTCF) family if the following conditions hold:

- *Efficient Function Generation: there exists an efficient probabilistic algorithm $\mathsf{GEN}_{\mathcal{F}}$ that generates a key $k \in \mathcal{K}_{\mathcal{F}}$ together with a trapdoor t_k, $(k, t_k) \leftarrow \mathsf{GEN}_{\mathcal{F}}(1^\lambda)$.*
- *Trapdoor Injective Pair: for all $k \in \mathcal{K}_{\mathcal{F}}$, the following conditions hold.*
  - *Trapdoor: for all $b \in \{0,1\}$ and $x \neq x' \in \mathcal{X}$, $\mathsf{Supp}(f_{k,b}(x)) \cap \mathsf{Supp}(f_{k,b}(x')) = \emptyset$. Moreover, there exists an efficient deterministic algorithm $\mathsf{INV}_{\mathcal{F}}$ such that for all $b \in \{0,1\}$, $x \in \mathcal{X}$ and $y \in \mathsf{Supp}(f_{k,b}(x))$, $\mathsf{INV}_{\mathcal{F}}(t_k, b, y) = x$.*

- *Injective Pair: there exists a perfect matching* $\mathcal{R}_k \subseteq \mathcal{X} \times \mathcal{X}$ *such that* $f_{k,0}(x_0) = f_{k,1}(x_1)$ *if and only if* $(x_0, x_1) \in \mathcal{R}_k$.

- *Efficient Range Superposition: for all* $k \in \mathcal{K}_{\mathcal{F}}$ *and* $b \in \{0,1\}$ *there exists a function* $f'_{k,b} : \mathcal{X} \to \mathcal{D}_{\mathcal{Y}}$ *such that*
  - *For all* $(x_0, x_1) \in \mathcal{R}_k$ *and* $y \in \mathsf{Supp}(f'_{k,b}(x_b))$, $\mathsf{INV}_{\mathcal{F}}(t_k, b, y) = x_b$ *and* $\mathsf{INV}_{\mathcal{F}}(t_k, b \oplus 1, y) = x_{b\oplus 1}$.
  - *There exists an efficient deterministic procedure* $\mathsf{CHK}_{\mathcal{F}}$ *that on input* k, $b \in \{0,1\}$, $x \in \mathcal{X}$, *and* $y \in \mathcal{Y}$, *returns* 1 *if* $y \in \mathsf{Supp}(f'_{k,b}(x))$ *and* 0 *otherwise. Note that* $\mathsf{CHK}_{\mathcal{F}}$ *is not provided the trapdoor* t_k.
  - *For every* $k \in \mathcal{K}_{\mathcal{F}}$ *and* $b \in \{0,1\}$,

    $$\mathrm{E}_{x \leftarrow \mathcal{X}}[H^2(f_{k,b}(x), f'_{k,b}(x))] = \mathrm{negl}(\lambda)$$

    for some negligible function $\mathrm{negl}(\cdot)$, *where the expectation is taken over* $x \leftarrow \mathcal{X}$. *Here* $H^2(\cdot,\cdot)$ *is the Hellinger distance. Moreover, there exists an efficient procedure* $\mathsf{SAMP}_{\mathcal{F}}$ *that on input* k *and* $b \in \{0,1\}$, *prepares the state*

    $$\frac{1}{\sqrt{|\mathcal{X}|}} \sum_{x \in \mathcal{X}, y \in \mathcal{Y}} \sqrt{(f'_{k,b}(x))(y)}|x\rangle|y\rangle.$$

- *Adaptive Hardcore Bit: for all* $k \in \mathcal{K}_{\mathcal{F}}$ *the following conditions hold for some integer* w *that is a polynomially bounded function in* λ.
  - *For all* $b \in \{0,1\}$ *and* $x \in \mathcal{X}$, *there exists a set* $G_{k,b,x} \subseteq \{0,1\}^w$ *such that* $\Pr_{d \leftarrow \{0,1\}^w}\{d \notin G_{k,b,x}\}$ *is negligible in* λ, *and moreover there exists an efficient algorithm that checks for membership in* $G_{k,b,x}$ *given* k, b, x *and the trapdoor* t_k.
  - *There is an efficiently computable injection* $J : \mathcal{X} \to \{0,1\}^w$ *such that* J *can be inverted efficiently on its range, and such that the following holds. Let*

    $$H_k := \{(b, x_b, d, d \cdot (J(x_0) \oplus J(x_1)))\,|b \in \{0,1\}, (x_0, x_1) \in \mathcal{R}_k, d \in G_{k,0,x_0} \cap G_{k,1,x_1}\},$$
    $$\overline{H}_k := \{(b, x_b, d, c \oplus 1) | (b, x_b, d, c) \in H_k\}.$$

    Then for any efficient quantum algorithm $\mathcal{A}$, *there exists a negligible function* $\mathrm{negl}(\cdot)$ *such that*

    $$\left|\Pr_{(k,t_k) \leftarrow \mathsf{GEN}_{\mathcal{F}}(1^\lambda)}\{\mathcal{A}(k) \in H_k\} - \Pr_{(k,t_k) \leftarrow \mathsf{GEN}_{\mathcal{F}}(1^\lambda)}\{\mathcal{A}(k) \in \overline{H}_k\}\right| = \mathrm{negl}(\lambda). \quad (1)$$

Definition 3 (Trapdoor Injective Function Family [1]) *Let* $\lambda \in \mathbb{N}$ *be a security parameter. Let* $\mathcal{X}$ *and* $\mathcal{Y}$ *be finite sets. Let* $\mathcal{K}_{\mathcal{G}}$ *be a finite set of keys. A family of functions*

$$\mathcal{G} := \{f_{k,b} : \mathcal{X} \to \mathcal{D}_{\mathcal{Y}}\}_{k \in \mathcal{K}_{\mathcal{G}}, b \in \{0,1\}}$$

is called a trapdoor injective function family if the following conditions hold:

- *Efficient Function Generation: There exists an efficient probabilistic algorithm* $\mathsf{GEN}_{\mathcal{G}}$ *which generates a key* $k \in \mathcal{K}_{\mathcal{G}}$ *together with a trapdoor* t_k, $(k, t_k) \leftarrow \mathsf{GEN}_{\mathcal{G}}(1^\lambda)$.

- *Disjoint Trapdoor Injective Pair: For all* $k \in \mathcal{K}_{\mathcal{G}}$, *for all* $b, b' \in \{0,1\}$ *and* $x, x' \in \mathcal{X}$, *if* $(b, x) \neq (b', x')$, $\mathsf{Supp}(f_{k,b}(x)) \cap \mathsf{Supp}(f_{k,b'}(x')) = \emptyset$. *Moreover, there exists an efficient deterministic algorithm* $\mathsf{INV}_{\mathcal{G}}$ *such that for all* $b \in \{0,1\}$, $x \in \mathcal{X}$ *and* $y \in \mathsf{Supp}(f_{k,b}(x))$, $\mathsf{INV}_{\mathcal{G}}(t_k, y) = (b, x)$.

- *Efficient Range Superposition: For all* $k \in \mathcal{K}_{\mathcal{G}}$ *and* $b \in \{0,1\}$,
  1. *There exists an efficient deterministic procedure* $\mathsf{CHK}_{\mathcal{G}}$ *that on input* k, $b \in \{0,1\}$, $x \in \mathcal{X}$, *and* $y \in \mathcal{Y}$, *outputs* 1 *if* $y \in \mathsf{Supp}(f_{k,b}(x))$ *and* 0 *otherwise. Note that* $\mathsf{CHK}_{\mathcal{G}}$ *is not provided the trapdoor* t_k.
  2. *There exists an efficient procedure* $\mathsf{SAMP}_{\mathcal{G}}$ *that on input* k *and* $b \in \{0,1\}$ *returns the state*

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

Definition 4 *[Injective Invariance [1]] A NTCF family $\mathcal{F}$ is injective invariant if there exists a trapdoor injective function family $\mathcal{G}$ such that*

- *The algorithm $\mathsf{CHK}_{\mathcal{F}}$ and $\mathsf{SAMP}_{\mathcal{F}}$ are the same as the algorithms $\mathsf{CHK}_{\mathcal{G}}$ and $\mathsf{SAMP}_{\mathcal{G}}$.*
- *For all quantum polynomial-time procedures $\mathcal{A}$, there exists a negligible function $\mathrm{negl}(\cdot)$ such that*

$$\left|\Pr_{(k,t_k)\leftarrow \mathsf{GEN}_{\mathcal{F}}(1^\lambda)}\{\mathcal{A}(k)=0\} - \Pr_{(k,t_k)\leftarrow \mathsf{GEN}_{\mathcal{G}}(1^\lambda)}\{\mathcal{A}(k)=0\}\right| \leq \mathrm{negl}(\lambda).$$

Definition 5 (Extended Trapdoor Claw-free Family [1]) *A NTCF family $\mathcal{F}$ is an extended trapdoor claw-free family if*

- *$\mathcal{F}$ is injective invariant.*
- *For all $k \in \mathcal{K}_{\mathcal{F}}$ and $d \in \{0,1\}^w$, let*

$$H'_{k,d} := \{d \cdot (J(x_0) \oplus J(x_1)) | (x_0, x_1) \in \mathcal{R}_k\}.$$

For all quantum polynomial-time algorithms $\mathcal{A}$, there exists a negligible function $\mathrm{negl}(\cdot)$ such that

$$\left|\Pr_{(k,t_k)\leftarrow \mathsf{GEN}_{\mathcal{F}}(1^\lambda)}\{\mathcal{A}(k) \in H'_{k,d}\} - \frac{1}{2}\right| \leq \mathrm{negl}(\lambda).$$

Definition 6 (Decoding maps for the ENTCF families [2]) *We define the following maps that decode the output of an ENTCF.*

- *For a key $k \in \mathcal{K}_{\mathcal{G}}$ and $y \in \mathcal{Y}$, let $\hat{b}(k,y)$ be the bit such that y is in the union of the supports of the distributions $f_{k,\hat{b}(k,y)}(x)$ over $x \in \mathcal{X}$. This is well-defined because the function pairs in $\mathcal{G}$ have disjoint images.*
- *For a key $k \in \mathcal{K}_{\mathcal{F}}$ or $\mathcal{K}_{\mathcal{G}}$, $y \in \mathcal{Y}$, and $b \in \{0,1\}$, let $\hat{x}_b(k,y)$ be the preimage of the function such that y is in the support of the distribution $f_{k,b}(\hat{x}_b(k,y))$. If y is not in the support, then nothing is defined for $\hat{x}_b(k,y)$ (so instead we define $\hat{x}_b(k,y) := \perp$).*
- *For a key $k \in \mathcal{K}_{\mathcal{F}}$, $y \in \mathcal{Y}$ and $d \in \mathcal{X}$, we define $\hat{u}(k,y,d) := d \cdot (\hat{x}_0(k,y) \oplus \hat{x}_1(k,y))$, where the preimages $\hat{x}_0(k,y)$ and $\hat{x}_1(k,y)$ can be efficiently computed by using the trapdoor information t_k.*

C. Definitions

Throughout the paper, we adopt the following definitions.

Definition 7 *(State-dependent inner product). Let $\mathcal{H}$ be a finite-dimensional Hilbert space, $A, B \in \mathcal{L}(\mathcal{H})$ and $\psi \in \mathrm{Pos}(\mathcal{H})$. We define the state-dependent (semi) inner product of A and B with respect to ψ as*

$$\langle A, B\rangle_\psi := \mathrm{tr}[A^\dagger B \psi].$$

Definition 8 *(Distance measures)*

(i) For $A \in \mathcal{L}(\mathcal{H})$, the schatten-p norm is defined by

$$||A||_p := \mathrm{tr}[|A|^p]^{1/p},$$

where $|A| := \sqrt{A^\dagger A}$. Note that $||A||_1$ is called the trace norm, and $||A||_\infty$ is called the operator norm (largest singular value).

(ii) For $A \in \mathcal{L}(\mathcal{H})$ and $\psi \in \mathrm{Pos}(\mathcal{H})$, we define the state-dependent (semi) norm of A with respect to ψ as

$$||A||_\psi := \sqrt{\mathrm{tr}[A^\dagger A \psi]}.$$

Definition 9 *(Approximate equality) We use the following symbol for describing an approximate equality.*

(i) For $a, b \in \mathbb{C}$, we define

$$a \approx_\epsilon b \Leftrightarrow |a-b| = O(\epsilon) + \mathrm{negl}(\lambda).$$

(ii) For $A, B \in \mathcal{L}(\mathcal{H})$, we define

$$A \approx_\epsilon B \Leftrightarrow ||A-B||_1^2 = O(\epsilon) + \mathrm{negl}(\lambda).$$

(iii) For $A, B \in \mathcal{L}(\mathcal{H})$ and $\psi \in \mathrm{Pos}(\mathcal{H})$, we define

$$A \approx_{\epsilon,\psi} B \Leftrightarrow ||A-B||_\psi^2 = O(\epsilon) + \mathrm{negl}(\lambda).$$

Definition 10 *(Computational indistinguishability) The two states $\psi, \psi' \in \mathcal{D}(\mathcal{H})$ are computationally indistinguishable up to $O(\delta)$ if any efficient distinguisher, which takes as input either ψ or ψ' and outputs the bit b, satisfies*

$$\Pr\{b=0|\psi\} \approx_\delta \Pr\{b=0|\psi'\}.$$

We use the notation

$$\psi \overset{c}{\approx}_\delta \psi'.$$

II. AUXILIARY LEMMAS

In this section, we summarize auxiliary lemmas that will be used in the soundness proof in Sec. V. All the lemmas in this section have been derived in [2]. We state them here just for the self-consistency of this paper.

Lemma 11 *Let A_1 and A_2 be efficient commuting binary observables. Then $A_1 A_2$ is also an efficient binary observable.*

Lemma 12 *Let $\psi, \psi' \in \mathcal{D}(\mathcal{H})$ such that $\psi \overset{c}{\approx}_\delta \psi'$ for some δ. If $\{M^{(a)}\}_{a\in\mathcal{S}}$ is an efficient measurement on $\mathcal{H}$, then*

$$\sum_{a\in\mathcal{S}} M^{(a)} \psi M^{(a)} \overset{c}{\approx}_\delta \sum_{a\in\mathcal{S}} M^{(a)} \psi' M^{(a)}.$$

Lemma 13 *(i) Let $\psi \in \mathrm{Pos}(\mathcal{H})$, and $A, B \in \mathcal{L}(\mathcal{H})$. For $C \in \mathcal{L}(\mathcal{H})$ such that $C^\dagger C \leq I$ we have*

$$A \approx_{\epsilon,\psi} B \Rightarrow CA \approx_{\epsilon,\psi} CB.$$

(ii) Let $\psi_i \in \mathrm{Pos}(\mathcal{H})$ for $i \in \{1, ..., n\}$ with constant n, and $A, B \in \mathcal{L}(\mathcal{H})$. Define $\psi = \sum_i \psi_i$. Then,

$$\forall i \in \{1, ..., n\} : A \approx_{\epsilon,\psi_i} B \Leftrightarrow A \approx_{\epsilon,\psi} B.$$

Lemma 14 *Let $\psi \in \mathrm{Pos}(\mathcal{H})$, $\{M^{(a)}\}_{a\in\mathcal{S}}$ a projective measurement with index set $\mathcal{S}$, and O denotes a binary observable*

$$O = \sum_a (-1)^{s_a} M^{(a)},$$

where $s_a \in \{0, 1\}$. Suppose there exists an $a' \in \mathcal{S}$ such that

$$\mathrm{tr}[M^{(a')}\psi] \approx_\epsilon \mathrm{tr}[\psi].$$

Then,

$$O \approx_{\epsilon,\psi} (-1)^{s_{a'}} I.$$

Lemma 15 *Let $\mathcal{H}_1$, $\mathcal{H}_2$ be Hilbert spaces with $\dim(\mathcal{H}_1) \leq \dim(\mathcal{H}_2)$ and $V : \mathcal{H}_1 \to \mathcal{H}_2$ an isometry. Let A and B be binary observables on $\mathcal{H}_1$ and $\mathcal{H}_2$, respectively, $\psi_1 \in \mathrm{Pos}(\mathcal{H}_1)$, $\psi_2 \in \mathrm{Pos}(\mathcal{H}_2)$, and $\epsilon \geq 0$. Then,*

$$\mathrm{tr}\left[V^\dagger B V A \psi_1\right] \approx_\epsilon \mathrm{tr}[\psi_1] \Rightarrow V^\dagger B V \approx_{\epsilon,\psi_1} A,$$
$$\mathrm{tr}\left[V A V^\dagger B \psi_2\right] \approx_\epsilon \mathrm{tr}[\psi_2] \Rightarrow V A V^\dagger \approx_{\epsilon,\psi_2} B.$$

Lemma 16 *Let O be a binary observable on $\mathcal{H}$ and $\psi \in \mathrm{Pos}(\mathcal{H})$. Then,*

$$O \approx_{\epsilon,\psi} (-1)^b I \Rightarrow O^{(b)} \approx_{\epsilon,\psi} I \text{ and } O^{(\bar{b})} \approx_{\epsilon,\psi} 0.$$

Lemma 17 *(Replacement lemma)*

(i) Let $\psi \in \mathrm{Pos}(\mathcal{H})$, and $A, B, C \in \mathcal{L}(\mathcal{H})$. If $A \approx_{\epsilon,\psi} B$ and $||C||_\infty = O(1)$, then

$$\mathrm{tr}[CA\psi] \approx_{\sqrt{\epsilon}} \mathrm{tr}[CB\psi],$$
$$\mathrm{tr}[AC\psi] \approx_{\sqrt{\epsilon}} \mathrm{tr}[BC\psi].$$

(ii) Let $\psi, \psi' \in \mathrm{Pos}(\mathcal{H})$, and $A \in \mathcal{L}(\mathcal{H})$. If $\psi \approx_\epsilon \psi'$ and $||A||_\infty = O(1)$, then

$$\mathrm{tr}[A\psi] \approx_{\sqrt{\epsilon}} \mathrm{tr}[A\psi'].$$

Lemma 18 *Let $A, B \in \mathcal{L}(\mathcal{H})$ be linear operators, $C \in \mathcal{L}(\mathcal{H})$ a linear operator with constant operator norm, and $\psi \in \mathrm{Pos}(\mathcal{H})$ with $\mathrm{tr}[\psi] \leq 1$. Then,*

$$A \approx_{\epsilon,\psi} B \Rightarrow A\psi C \approx_\epsilon B\psi C \text{ and } C\psi A^\dagger \approx_\epsilon C\psi B^\dagger.$$

Lemma 19 *Let $\mathcal{H}_1$, $\mathcal{H}_2$ be Hilbert spaces with $\dim(\mathcal{H}_1) \leq \dim(\mathcal{H}_2)$, $V : \mathcal{H}_1 \to \mathcal{H}_2$ an isometry, and A and B binary observables on $\mathcal{H}_1$ and $\mathcal{H}_2$, respectively. Then, the following holds for any $\psi \in \mathrm{Pos}(\mathcal{H}_1)$:*

$$VAV^\dagger \approx_{\epsilon, V\psi V^\dagger} B \Rightarrow A \approx_{\epsilon,\psi} V^\dagger BV,$$
$$A \approx_{\epsilon,\psi} V^\dagger BV \Rightarrow VAV^\dagger \approx_{\sqrt{\epsilon}, V\psi V^\dagger} B.$$

Lemma 20 *Let $\mathcal{H}_1$, $\mathcal{H}_2$ be Hilbert spaces with $\dim(\mathcal{H}_1) \leq \dim(\mathcal{H}_2)$ and $V : \mathcal{H}_1 \to \mathcal{H}_2$ an isometry. Let A and B be binary observables on $\mathcal{H}_1$ and $\mathcal{H}_2$, respectively, $\psi \in \mathrm{Pos}(\mathcal{H}_1)$, and $\epsilon \geq 0$. Then, for any $b \in \{0, 1\}$:*

$$V^\dagger BV \approx_{\epsilon,\psi} A \Rightarrow V^\dagger B^{(b)} V \approx_{\epsilon,\psi} A^{(b)},$$
$$B \approx_{\epsilon, V\psi V^\dagger} VAV^\dagger \Rightarrow B^{(b)} \approx_{\epsilon, V\psi V^\dagger} VA^{(b)}V^\dagger.$$

Lemma 21 *(Lifting lemma) Let ψ, $\psi' \in \mathcal{D}(\mathcal{H})$ be computationally indistinguishable: $\psi \overset{c}{\approx}_\delta \psi'$.*

(i) Let A be an efficient binary observable on $\mathcal{H}$. Then,

$$\mathrm{tr}[A\psi] \approx_\delta \mathrm{tr}[A\psi'].$$

(ii) Let A, B be efficient binary observables on $\mathcal{H}$. Then,

$$A \approx_{\epsilon,\psi} B \Rightarrow A \approx_{\delta+\epsilon,\psi'} B.$$

(iii) Let A, B be efficient binary observables on $\mathcal{H}$. Then,

$$[A, B] \approx_{\epsilon,\psi} 0 \Rightarrow [A, B] \approx_{\delta+\epsilon,\psi'} 0.$$

(iv) Let A, B be efficient binary observables on $\mathcal{H}$. Then,

$$\{A, B\} \approx_{\epsilon,\psi} 0 \Rightarrow \{A, B\} \approx_{\delta+\epsilon,\psi'} 0.$$

(v) Let $\mathcal{H}'$ be another Hilbert space with $\dim(\mathcal{H}') \geq \dim(\mathcal{H})$, A an efficient binary observable on $\mathcal{H}$, B an efficient binary observable on $\mathcal{H}'$, and $V : \mathcal{H} \to \mathcal{H}'$ an efficient isometry. Then

$$A \approx_{\epsilon,\psi} V^\dagger BV \Rightarrow A \approx_{\sqrt{\epsilon}+\delta,\psi'} V^\dagger BV.$$

(vi) Let $\mathcal{H}'$ be another Hilbert space with $\dim(\mathcal{H}') \geq \dim(\mathcal{H})$. Also, let $\psi, \psi' \in \mathcal{D}(\mathcal{H}')$ such that $\psi \overset{c}{\approx}_\delta \psi'$, A be an efficient binary observable on $\mathcal{H}$, B an efficient binary observable on $\mathcal{H}'$, and $V : \mathcal{H} \to \mathcal{H}'$ an efficient isometry. Then

$$VAV^\dagger \approx_{\epsilon,\psi} B \Rightarrow VAV^\dagger \approx_{\epsilon^{1/4}+\delta,\psi'} B.$$

III. SELF-TESTING PROTOCOL OF MAGIC STATE FOR CCZ GATE

Here, we formally describe our computationally bounded single-device self-testing protocol for the entangled magic state $CCZ|+\rangle^{\otimes 3}$.

Protocol 1

1. The verifier chooses the bases $\boldsymbol{\theta} = \theta_1\theta_2\theta_3 \in_R \mathcal{B}$ with the set of bases being defined as

$$\mathcal{B} := \{000, 001, 010, 100, 111\}. \tag{2}$$

   The basis choices 0 and 1 correspond to the computational basis and the Hadamard basis, respectively. We call the basis choice $\boldsymbol{\theta} \in \{000, 001, 010, 100\}$ the *test case*, and the basis choice $\boldsymbol{\theta} = 111$ the *hypergraph case*.

2. The verifier samples public keys k_1, k_2, k_3 and trapdoors $t_{k_1}, t_{k_2}, t_{k_3}$ as

$$\begin{cases} (k_i, t_{k_i}) \leftarrow \mathsf{GEN}_{\mathcal{G}}(1^\lambda) \text{ if } \theta_i = 0, \\ (k_i, t_{k_i}) \leftarrow \mathsf{GEN}_{\mathcal{F}}(1^\lambda) \text{ if } \theta_i = 1. \end{cases}$$

   Then, the verifier sends 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 the round type from {preimage round, Hadamard round} uniformly at random and sends the round type to the prover.

   (i) For a preimage round: The verifier receives $(b_1, x_1; b_2, x_2; b_3, x_3)$ from the prover with $b_i \in \{0, 1\}$ and $x_i \in \mathcal{X}$. The verifier sets a flag $flag \leftarrow fail_{\mathrm{Pre}}$ except $\mathsf{CHK}(k_i, y_i, b_i, x_i) = 1$ holds for all $i \in \{1, 2, 3\}$.

   (ii) For an Hadamard round: The verifier receives $d_1, d_2, d_3 \in \{0, 1\}^w$ from the prover. Then, the verifier sends the questions $q_1, q_2, q_3 \in_R \{0, 1\}$ to the prover, and the prover returns the answers $v_1, v_2, v_3 \in \{0, 1\}$ to the verifier. Depending on the basis choice $\boldsymbol{\theta}$, the verifier executes the following checks.

Basis choice	Verifier's check
$\boldsymbol{\theta}$=000	Set $flag \leftarrow fail_{\mathrm{Test}}$ if the following is true for $i \in_R \{1, 2.3\}$: $q_i = 0 \quad \wedge \quad \hat{b}(k_i, y_i) \neq v_i$.
$\boldsymbol{\theta}$=100	Set $flag \leftarrow fail_{\mathrm{Test}}$ if the following is true: $q_1 = 1 \quad \wedge \quad \hat{u}(k_1, y_1, d_1) \oplus \hat{b}(k_2, y_2) \cdot \hat{b}(k_3, y_3) \neq v_1$.
$\boldsymbol{\theta}$=010	Set $flag \leftarrow fail_{\mathrm{Test}}$ if the following is true: $q_2 = 1 \quad \wedge \quad \hat{u}(k_2, y_2, d_2) \oplus \hat{b}(k_1, y_1) \cdot \hat{b}(k_3, y_3) \neq v_2$.
$\boldsymbol{\theta}$=001	Set $flag \leftarrow fail_{\mathrm{Test}}$ if the following is true: $q_3 = 1 \quad \wedge \quad \hat{u}(k_3, y_3, d_3) \oplus \hat{b}(k_1, y_1) \cdot \hat{b}(k_2, y_2) \neq v_3$.
$\boldsymbol{\theta}$=111	Set $flag \leftarrow fail_{\mathrm{Hyper}}$ if one of the following is true: $\boldsymbol{q} = 100 \quad \wedge \quad \hat{u}(k_1, y_1, d_1) \neq v_1 \oplus \delta_{v_2,1} \cdot v_3$, $\boldsymbol{q} = 010 \quad \wedge \quad \hat{u}(k_2, y_2, d_2) \neq v_2 \oplus \delta_{v_1,1} \cdot v_3$, $\boldsymbol{q} = 001 \quad \wedge \quad \hat{u}(k_3, y_3, d_3) \neq v_3 \oplus \delta_{v_1,1} \cdot v_2$.

IV. COMPLETENESS OF THE PROTOCOL

In this section, we prove our Theorem 1 in the main text. Specifically, we show that there exists an honest prover's strategy, which is accepted by the verifier with probability negligibly close to 1.

First, after receiving the keys k_1, k_2, k_3 from the verifier, the prover treats each key separately and prepares the following state for $i \in \{1, 2, 3\}$:

$$\frac{1}{\sqrt{2|\mathcal{X}|}} \sum_{b=0}^{1} \sum_{x \in \mathcal{X}, y \in \mathcal{Y}} \sqrt{(f_{k_i,b}(x))(y)}|b\rangle|x\rangle|y\rangle.$$

The preparation of this state can be efficiently done up to negligible error using the procedures from the definition of ENTCF families (definition 4.2 in [1]). Then, the prover measures the y-register and returns the outcomes $y_1, y_2, y_3 \in \mathcal{Y}$ to the verifier. At this point, the post-measurement state for each $i \in \{1,2,3\}$ is written as

$$\begin{cases} |\hat{b}(k_i,y_i)\rangle|\hat{x}(k_i,y_i)\rangle & \text{if } k_i \in \mathcal{K}_\mathcal{G}, \\ \frac{1}{\sqrt{2}}(|0\rangle|\hat{x}_0(k_i,y_i)\rangle + |1\rangle|\hat{x}_1(k_i,y_i)\rangle) & \text{if } k_i \in \mathcal{K}_\mathcal{F}. \end{cases}$$

Note that bit $\hat{b}(k,y)$ for $k \in \mathcal{K}_\mathcal{G}$ and $y \in \mathcal{Y}$, and preimage $\hat{x}_b(k,y)$ with $b \in \{0,1\}$, $k \in \mathcal{K}_\mathcal{G} \cup \mathcal{K}_\mathcal{F}$ and $y \in \mathcal{Y}$ are defined in Definition 6. For simplicity of notation, we define $\hat{x}(k,y) := \hat{x}_{\hat{b}(k,y)}(k,y)$. If the verifier chooses the preimage round, it is easy to figure out that the prover is accepted by the verifier with probability negligibly close to 1.

If the verifier chooses the Hadamard round, the prover measures the x-register in the Hadamard basis, obtains the outcomes $d_1, d_2, d_3 \in \{0,1\}^w$ and returns these to the verifier. At this point, the prover's state for each $i \in \{1,2,3\}$ is given by

$$\begin{cases} |\hat{b}(k_i,y_i)\rangle & \text{if } k_i \in \mathcal{K}_\mathcal{G}, \\ |(-)^{\hat{u}(k_i,y_i,d_i)}\rangle & \text{if } k_i \in \mathcal{K}_\mathcal{F}. \end{cases}$$

Here, we define

$$\hat{u}(k_i,y_i,d_i) = d_i \cdot (\hat{x}_0(k_i,y_i) \oplus \hat{x}_1(k_i,y_i)).$$

Now, the prover performs the CCZ gate (an entangling three-qubit gate that applies σ_Z to the target qubit if the other qubits are in state $|1\rangle$) among the three qubits and obtains

$$\begin{cases} |\hat{b}(k_1,y_1)\rangle|\hat{b}(k_2,y_2)\rangle|\hat{b}(k_3,y_3)\rangle & \text{if } k_1,k_2,k_3 \in \mathcal{K}_\mathcal{G}, \\ |(-)^{\hat{u}(k_1,y_1,d_1)\oplus\hat{b}(k_2,y_2)\cdot\hat{b}(k_3,y_3)}\rangle|\hat{b}(k_2,y_2)\rangle|\hat{b}(k_3,y_3)\rangle & \text{if } k_1 \in \mathcal{K}_\mathcal{F}, k_2,k_3 \in \mathcal{K}_\mathcal{G}, \\ |\hat{b}(k_1,y_1)\rangle|(-)^{\hat{u}(k_2,y_2,d_2)\oplus\hat{b}(k_1,y_1)\cdot\hat{b}(k_3,y_3)}\rangle|\hat{b}(k_3,y_3)\rangle & \text{if } k_1 \in \mathcal{K}_\mathcal{G}, k_2 \in \mathcal{K}_\mathcal{F}, k_3 \in \mathcal{K}_\mathcal{G}, \\ |\hat{b}(k_1,y_1)\rangle|\hat{b}(k_2,y_2)\rangle|(-)^{\hat{u}(k_3,y_3,d_3)\oplus\hat{b}(k_1,y_1)\cdot\hat{b}(k_2,y_2)}\rangle & \text{if } k_1,k_2 \in \mathcal{K}_\mathcal{G}, k_3 \in \mathcal{K}_\mathcal{F}, \\ |\phi_{\mathrm{H}}^{(\hat{u}(k_1,y_1,d_1),\hat{u}(k_2,y_2,d_2),\hat{u}(k_3,y_3,d_3))}\rangle & \text{if } k_1,k_2,k_3 \in \mathcal{K}_\mathcal{F}, \end{cases} \tag{3}$$

where we define

$$|\phi_{\mathrm{H}}^{(a,b,c)}\rangle := (\sigma_Z^a \otimes \sigma_Z^b \otimes \sigma_Z^c)CCZ|+\rangle^{\otimes 3}.$$

It is easy to find that in the first four cases of Eq. (3), the prover's answer is accepted by the verifier. For the last case of Eq. (3), by rewriting $|\phi_{\mathrm{H}}^{(\hat{u}(k_1,y_1,d_1),\hat{u}(k_2,y_2,d_2),\hat{u}(k_3,y_3,d_3))}\rangle$ depending on $\boldsymbol{q}$ as (we use the simplified notations: $u_1 = \hat{u}(k_1,y_1,d_1), u_2 = \hat{u}(k_2,y_2,d_2), u_3 = \hat{u}(k_3,y_3,d_3)$)

$$\begin{aligned} \boldsymbol{q}=100: &\ \frac{|(-)^{u_1}\rangle|0\rangle\left[|0\rangle + (-1)^{u_3}|1\rangle\right] + (-1)^{u_2}\left[|(-)^{u_1}\rangle|1\rangle|0\rangle + (-1)^{u_3}|(-)^{u_1\oplus 1}\rangle|1\rangle|1\rangle\right]}{2}, \\ \boldsymbol{q}=010: &\ \frac{|0\rangle|(-)^{u_2}\rangle\left[|0\rangle + (-1)^{u_3}|1\rangle\right] + |1\rangle\left[(-1)^{u_1}|(-)^{u_2}\rangle|0\rangle + (-1)^{u_1\oplus u_3}|(-)^{u_2\oplus 1}\rangle|1\rangle\right]}{2}, \\ \boldsymbol{q}=001: &\ \frac{|0\rangle\left[|0\rangle + (-1)^{u_2}|1\rangle\right]|(-)^{u_3}\rangle + |1\rangle\left[(-1)^{u_1}|0\rangle|(-)^{u_3}\rangle + (-1)^{u_1\oplus u_2}|1\rangle|(-)^{u_3\oplus 1}\rangle\right]}{2}, \end{aligned}$$

and if the honest prover measures the qubits in the Pauli-Z or X basis depending on $q_i = 0$ or $q_i = 1$, by returning the measurement outcome as the answer v_i, it is straightforward to figure out that the prover is accepted by the verifier. ■

V. SOUNDNESS OF THE PROTOCOL

In this section, we provide the proof of our Theorem 2 presented in the main text.

A. Devices

Definition 22 *An arbitrary prover can be modeled by a device $D := (S, \Pi, M, P)$, which are specified as follows.*

1. *(State just after returning images $\boldsymbol{y}$) We define the set of states $S := \{\psi^{(\boldsymbol{\theta})}\}_{\boldsymbol{\theta}\in\{0,1\}^3}$ as*

$$\psi^{(\boldsymbol{\theta})} = \sum_{\boldsymbol{y}\in\mathcal{Y}^3} \psi_{\boldsymbol{y}}^{(\boldsymbol{\theta})} \otimes |\boldsymbol{y}\rangle\langle\boldsymbol{y}|_Y \in \mathcal{D}(\mathcal{H}_D \otimes \mathcal{H}_Y). \tag{4}$$

Note that $\psi^{(\boldsymbol{\theta})}$ with $\boldsymbol{\theta} \in \mathcal{B}$ represents the state of the prover just after step 3 of Protocol 1, namely the state just after returning images $\boldsymbol{y}$ to the verifier. The state $\psi^{(\boldsymbol{\theta})}$ is implicitly averaged over the keys (k_1, k_2, k_3) chosen by the verifier, and all the statements we make in terms of the device D hold on overage over the keys.

2. *(Measurement in the preimage round) A projective measurement on systems $\mathcal{H}_D \otimes \mathcal{H}_Y$ performed in the preimage round is defined as*

$$\Pi = \left\{ \Pi^{(\boldsymbol{b},\boldsymbol{x})} = \sum_{\boldsymbol{y}\in\mathcal{Y}^3} \Pi_{\boldsymbol{y}}^{(\boldsymbol{b},\boldsymbol{x})} \otimes |\boldsymbol{y}\rangle\langle\boldsymbol{y}|_Y \right\}_{\boldsymbol{b},\boldsymbol{x}}.$$

Here, $\Pi_{\boldsymbol{y}}^{(\boldsymbol{b},\boldsymbol{x})}$ represents the projective measurement to obtain outcomes $\boldsymbol{b} \in \{0,1\}^3$ and $\boldsymbol{x} \in \mathcal{X}^3$ given the images $\boldsymbol{y} \in \mathcal{Y}^3$.

3. *(Measurement and post-measurement states in the Hadamard round) A projective measurement on systems $\mathcal{H}_D \otimes \mathcal{H}_Y$ performed in the Hadamard round to obtain $\boldsymbol{d} \in \{0,1\}^{3w}$ is defined as*

$$M = \left\{ M^{(\boldsymbol{d})} = \sum_{\boldsymbol{y}\in\mathcal{Y}^3} M_{\boldsymbol{y}}^{(\boldsymbol{d})} \otimes |\boldsymbol{y}\rangle\langle\boldsymbol{y}|_Y \right\}_{\boldsymbol{d}}.$$

For any $\boldsymbol{\theta} \in \{0,1\}^3$, the post-measurement normalized state after measurement M is written as

$$\rho^{(\boldsymbol{\theta})} = \sum_{\boldsymbol{y}\in\mathcal{Y}^3, \boldsymbol{d}\in\{0,1\}^{3w}} M_{\boldsymbol{y}}^{(\boldsymbol{d})} \psi_{\boldsymbol{y}}^{(\boldsymbol{\theta})} M_{\boldsymbol{y}}^{(\boldsymbol{d})} \otimes |\boldsymbol{y}, \boldsymbol{d}\rangle\langle\boldsymbol{y}, \boldsymbol{d}|_{YR}. \tag{5}$$

For simplicity, we adopt the following definition

$$\sigma_{\boldsymbol{y},\boldsymbol{d}}^{(\boldsymbol{\theta})} := M_{\boldsymbol{y}}^{(\boldsymbol{d})} \psi_{\boldsymbol{y}}^{(\boldsymbol{\theta})} M_{\boldsymbol{y}}^{(\boldsymbol{d})}.$$

4. *(Measurement after receiving questions $\boldsymbol{q}$ in the Hadamard round) Given the verifier's questions $\boldsymbol{q} \in \{0,1\}^3$, $P_{\boldsymbol{q}}$ denotes the projective measurement on systems $\mathcal{H}_D \otimes \mathcal{H}_Y \otimes \mathcal{H}_R$:*

$$P_{\boldsymbol{q}} = \left\{ P_{\boldsymbol{q}}^{(\boldsymbol{v})} = \sum_{\boldsymbol{y}\in\mathcal{Y}^3, \boldsymbol{d}\in\{0,1\}^{3w}} P_{\boldsymbol{q},\boldsymbol{y},\boldsymbol{d}}^{(\boldsymbol{v})} \otimes |\boldsymbol{y}, \boldsymbol{d}\rangle\langle\boldsymbol{y}, \boldsymbol{d}|_{YR} \right\}_{\boldsymbol{v}\in\{0,1\}^3}.$$

By performing this measurement, the prover obtains the outcomes $\boldsymbol{v} \in \{0,1\}^3$ that are returned to the verifier in the protocol.

B. Marginal observables

Definition 23 *For $D = (S, \Pi, M, P)$, we define the following binary observables using the projective measurement $P_{\boldsymbol{q}}$. A set of binary observables regarding the answer $v_i \in \{0,1\}$ for $i \in \{1,2,3\}$ given questions $\boldsymbol{q} \in \{0,1\}^3$ is defined by*

$$\left\{ A_{i,\boldsymbol{q}} := \sum_{\boldsymbol{v}\in\{0,1\}^3} (-1)^{v_i} P_{\boldsymbol{q}}^{(\boldsymbol{v})} \right\}_{\boldsymbol{q}\in\{0,1\}^3}. \tag{6}$$

We call $\{A_{i,\boldsymbol{q}=000}\}_{i=1}^3$ and $\{A_{i,\boldsymbol{q}=111}\}_{i=1}^3$ the *non-tilde observables*. Any other binary observables $\{A_{i,\boldsymbol{q}}\}_{i,\boldsymbol{q}}$ are called the *tilde observables*. Note that all the $\{A_{i,\boldsymbol{q}}\}_{i,\boldsymbol{q}}$ act on the same Hilbert space regardless of i and $\boldsymbol{q}$. The only difference lies in classical post-processing of the answers $\boldsymbol{v}$, where $\{A_{1,\boldsymbol{q}}\}_{\boldsymbol{q}}$, $\{A_{2,\boldsymbol{q}}\}_{\boldsymbol{q}}$ and $\{A_{3,\boldsymbol{q}}\}_{\boldsymbol{q}}$ respectively focus only on the first outcome v_1 (v_2 and v_3 are marginalized), the second outcome v_2 (v_1 and v_3 are marginalized), and the third outcome v_3 (v_1 and v_2 are marginalized).

C. Success probabilities of a device

In the self-testing protocol described in Sec. III, if the prover's answer is incorrect, the verifier sets a flag. Here, we relate the probabilities that the prover passes these checks to the states and measurements defined in Secs. V A and V B.

Lemma 24 *(Preimage check) Let $D = (S, \Pi, M, P)$ be a device. The probability of passing the i^{th} preimage check (namely $\mathsf{CHK}(k_i, y_i, b_i, x_i) = 1$) conditioned on the basis choice $\boldsymbol{\theta} \in \mathcal{B}$ and the preimage round is written as*

$$\begin{aligned}&\Pr\{\text{Prover passes the } i^{\text{th}} \text{ preimage check}|\boldsymbol{\theta}, \text{preimage round}\}\\ =&\delta_{\theta_i,0} \sum_{\boldsymbol{y},\boldsymbol{x}_{\bar{i}},\boldsymbol{b}_{\bar{i}}} \operatorname{tr}\left[\Pi_{\boldsymbol{y}}^{(\hat{b}(k_i,y_i),\hat{x}(k_i,y_i);\boldsymbol{b}_{\bar{i}},\boldsymbol{x}_{\bar{i}})} \psi_{\boldsymbol{y}}^{(\boldsymbol{\theta})}\right] + \delta_{\theta_i,1} \sum_{\boldsymbol{y},\boldsymbol{x}_{\bar{i}},\boldsymbol{b}_{\bar{i}},b} \operatorname{tr}\left[\Pi_{\boldsymbol{y}}^{(b,\hat{x}_b(k_i,y_i);\boldsymbol{b}_{\bar{i}},\boldsymbol{x}_{\bar{i}})} \psi_{\boldsymbol{y}}^{(\boldsymbol{\theta})}\right]. \end{aligned} \tag{7}$$

Let $p_{\min}$ denote the minimum probability of Eq. (7) over $i \in \{1,2,3\}$ and $\boldsymbol{\theta} \in \mathcal{B}$, and we define

$$\gamma_P(D) := 1 - p_{\min}. \tag{8}$$

Then, the upper bound on $\gamma_P(D)$ is obtained as

$$\gamma_P(D) \leq 15 \cdot \Pr\{flag = fail_{\text{Pre}}|\text{preimage round}\}. \tag{9}$$

Note that $\Pr\{flag = fail_{\text{Pre}}|\text{preimage round}\}$ can be estimated through repeating the self-testing protocol.
(Proof) The probability of obtaining $fail_{\text{Pre}}$ conditioned on choosing the preimage round is written as

$$\begin{aligned}&\Pr\{flag = fail_{\text{Pre}}|\text{preimage round}\}\\ =&1 - \Pr\{\mathsf{CHK}(k_1,y_1,b_1,x_1) = 1 \wedge \mathsf{CHK}(k_2,y_2,b_2,x_2) = 1 \wedge \mathsf{CHK}(k_3,y_3,b_3,x_3) = 1|\text{preimage round}\}. \end{aligned} \tag{10}$$

To upper-bound the second term of Eq. (10), we consider a virtual scenario [1] where the verifier checks only the i^{th} ($i \in \{1,2,3\}$) preimage, whose index i is chosen with probability $\Pr\{i\} = 1/3$. This procedure is virtual in the sense that only the i^{th} preimage check is conducted while all of the i^{th} preimage checks are performed in the actual protocol described in Sec. III. Since the probability of passing only the i^{th} preimage check is larger than that of passing all the preimage checks, we have

$$\begin{aligned}&\Pr\{\mathsf{CHK}(k_1,y_1,b_1,x_1) = 1 \wedge \mathsf{CHK}(k_2,y_2,b_2,x_2) = 1 \wedge \mathsf{CHK}(k_3,y_3,b_3,x_3) = 1|\text{preimage round}\}\\ \leq&\frac{1}{3}\sum_{i=1}^3 \Pr\{\text{Prover passes the } i^{\text{th}} \text{ preimage check}|i, \text{preimage round}\}\\ =&\frac{1}{3}\sum_{i=1}^3 \Pr\{\text{Prover passes the } i^{\text{th}} \text{ preimage check}|\text{preimage round}\}\\ =&\frac{1}{3}\sum_{i=1}^3 \sum_{\boldsymbol{\theta}\in\mathcal{B}} \Pr\{\boldsymbol{\theta}\} \cdot \Pr\{\text{Prover passes the } i^{\text{th}} \text{ preimage check}|\boldsymbol{\theta}, \text{preimage round}\}\\ =&\frac{1}{3|\mathcal{B}|}\sum_{i=1}^3 \sum_{\boldsymbol{\theta}\in\mathcal{B}} \Pr\{\text{Prover passes the } i^{\text{th}} \text{ preimage check}|\boldsymbol{\theta}, \text{preimage round}\}. \end{aligned} \tag{11}$$

---

[1] This virtual procedure appears just for proving this lemma, and we do not employ this procedure in the rest of this paper.

In the second equality, the index i is omitted from the condition. This is guaranteed by the fact that the only difference between the virtual and the actual protocols lies in the probability of choosing i and once conditioned on i, the probability of passing the i^{th} preimage check is obviously equal. By using Eq. (8), Eq. (11) is upper-bounded by

$$\frac{1}{3|\mathcal{B}|}[(3|\mathcal{B}|-1)\times 1+1\times p_{\min}]=1-\frac{\gamma_P(D)}{3|\mathcal{B}|}.$$

Hence, Eq. (10) leads to

$$\Pr\{flag=fail_{\text{Pre}}|\text{preimage round}\}\geq\frac{\gamma_P(D)}{3|\mathcal{B}|}.$$

By noting $|\mathcal{B}|=5$ from Eq. (2), this results in

$$\gamma_P(D)\leq 15\cdot\Pr\{flag=fail_{\text{Pre}}|\text{preimage round}\}.$$

■

Lemma 25 *(Test case) Let $D=(S,\Pi,M,P)$ be a device. We define*

$$\gamma_T(D):=1-\min\mathcal{T} \tag{12}$$

with

$$\mathcal{T}:=\left\{\sum_{\boldsymbol{v}\in\{0,1\}^3}\text{tr}\left[A^{(v_i)}_{i,\boldsymbol{q}|q_i=0}\sigma^{(0,v_1;0,v_2;0,v_3)}\right]\right\}_{i,\boldsymbol{q}_{\bar{i}}}\cup\left\{\sum_{\boldsymbol{v}\in\{0,1\}^3}\text{tr}\left[A^{(v_1)}_{1,\boldsymbol{q}|q_1=1}\sigma^{(1,v_1;0,v_2;0,v_3)}\right]\right\}_{q_2,q_3}$$
$$\cup\left\{\sum_{\boldsymbol{v}\in\{0,1\}^3}\text{tr}\left[A^{(v_2)}_{2,\boldsymbol{q}|q_2=1}\sigma^{(0,v_1;1,v_2;0,v_3)}\right]\right\}_{q_1,q_3}\cup\left\{\sum_{\boldsymbol{v}\in\{0,1\}^3}\text{tr}\left[A^{(v_3)}_{3,\boldsymbol{q}|q_3=1}\sigma^{(0,v_1;0,v_2;1,v_3)}\right]\right\}_{q_1,q_2},$$

where for $v_1,v_2,v_3\in\{0,1\}$

$$\sigma^{(0,v_1;0,v_2;0,v_3)}:=\sum_{\substack{\boldsymbol{y},\boldsymbol{d}:\\ \hat{b}(k_1,y_1)=v_1,\hat{b}(k_2,y_2)=v_2,\hat{b}(k_3,y_3)=v_3}}\sigma^{(000)}_{\boldsymbol{y},\boldsymbol{d}}\otimes|\boldsymbol{y},\boldsymbol{d}\rangle\langle\boldsymbol{y},\boldsymbol{d}|, \tag{13}$$

$$\sigma^{(1,v_1;0,v_2;0,v_3)}:=\sum_{\substack{\boldsymbol{y},\boldsymbol{d}:\\ \hat{u}(k_1,y_1,d_1)\oplus\hat{b}(k_2,y_2)\cdot\hat{b}(k_3,y_3)=v_1,\hat{b}(k_2,y_2)=v_2,\hat{b}(k_3,y_3)=v_3}}\sigma^{(100)}_{\boldsymbol{y},\boldsymbol{d}}\otimes|\boldsymbol{y},\boldsymbol{d}\rangle\langle\boldsymbol{y},\boldsymbol{d}|, \tag{14}$$

$$\sigma^{(0,v_1;1,v_2;0,v_3)}=\sum_{\substack{\boldsymbol{y},\boldsymbol{d}:\\ \hat{u}(k_2,y_2,d_2)\oplus\hat{b}(k_1,y_1)\cdot\hat{b}(k_3,y_3)=v_2,\hat{b}(k_1,y_1)=v_1,\hat{b}(k_3,y_3)=v_3}}\sigma^{(010)}_{\boldsymbol{y},\boldsymbol{d}}\otimes|\boldsymbol{y},\boldsymbol{d}\rangle\langle\boldsymbol{y},\boldsymbol{d}|, \tag{15}$$

$$\sigma^{(0,v_1;0,v_2;1,v_3)}:=\sum_{\substack{\boldsymbol{y},\boldsymbol{d}:\\ \hat{u}(k_3,y_3,d_3)\oplus\hat{b}(k_1,y_1)\cdot\hat{b}(k_2,y_2)=v_3,\hat{b}(k_1,y_1)=v_1,\hat{b}(k_2,y_2)=v_2}}\sigma^{(001)}_{\boldsymbol{y},\boldsymbol{d}}\otimes|\boldsymbol{y},\boldsymbol{d}\rangle\langle\boldsymbol{y},\boldsymbol{d}|. \tag{16}$$

Then, the upper bound on $\gamma_T(D)$ is given by

$$\gamma_T(D)\leq 96\cdot\Pr\{flag=fail_{\text{Test}}|\text{Test},\text{Hadamard round}\}. \tag{17}$$

Note that $\Pr\{flag=fail_{\text{Test}}|\text{Test},\text{Hadamard round}\}$ can be estimated through repeating the self-testing protocol.
(Proof) The probability of obtaining $fail_{\text{Test}}$ conditioned on choosing the test case and the Hadamard round is written as

$$\begin{aligned}\Pr\{flag=fail_{\text{Test}}|\text{Test},\text{Hadamard round}\}=&\Pr\{\boldsymbol{\theta}=000,flag=fail_{\text{Test}}|\text{Test},\text{Hadamard round}\}\\&+\Pr\{\text{wt}(\boldsymbol{\theta})=1,flag=fail_{\text{Test}}|\text{Test},\text{Hadamard round}\}.\end{aligned} \tag{18}$$

We calculate the first and second terms in turn. First, we focus on the first one:

$$\begin{aligned}
&\Pr\{\boldsymbol{\theta}=000, flag=fail_{\rm Test}|\text{Test, Hadamard round}\}\\
=&\Pr\{\boldsymbol{\theta}=000|\text{Test, Hadamard round}\}\cdot\Pr\{flag=fail_{\rm Test}|\boldsymbol{\theta}=000,\text{Hadamard round}\}\\
=&\frac{1}{12}\sum_{i=1}^{3}\sum_{b=0}^{1}\sum_{y_i}\Pr\{q_i=0,\hat{b}(k_i,y_i)=b,v_i=\bar{b}|\boldsymbol{\theta}=000,\text{Hadamard round},i\}\\
=&\frac{1}{12\times 2^3}\sum_{i=1}^{3}\sum_{b=0}^{1}\sum_{y_i}\sum_{\boldsymbol{q}_{\bar{i}}\in\{0,1\}^2}\Pr\{\hat{b}(k_i,y_i)=b,v_i=\bar{b}|\boldsymbol{\theta}=000,\text{Hadamard round},i,q_i=0,\boldsymbol{q}_{\bar{i}}\}\\
=&\frac{1}{8}-\frac{1}{96}\sum_{i=1}^{3}\sum_{b=0}^{1}\sum_{y_i}\sum_{\boldsymbol{q}_{\bar{i}}\in\{0,1\}^2}\Pr\{\hat{b}(k_i,y_i)=v_i=b|\boldsymbol{\theta}=000,\text{Hadamard round},i,q_i=0,\boldsymbol{q}_{\bar{i}}\}.
\end{aligned}\tag{19}$$

Here, $\sum_{b=0}^{1}\sum_{y_i}\Pr\{\hat{b}(k_i,y_i)=v_i=b|\boldsymbol{\theta}=000,\text{Hadamard round},i,q_i=0,\boldsymbol{q}_{\bar{i}}\}$ represents the probability that the prover's answer v_i is accepted by the verifier conditioned on measuring the state $\rho^{(000)}$ when the input to the device is $\boldsymbol{q}$ with $q_i=0$. This probability can be rewritten by using the expressions of the states and measurements as

$$\sum_{b=0}^{1}\mathrm{tr}\left[A^{(v_i=b)}_{i,\boldsymbol{q}|q_i=0}\sum_{y_i:\hat{b}(k_i,y_i)=b}\left(|y_i\rangle\langle y_i|\rho^{(000)}|y_i\rangle\langle y_i|\right)\right]=\sum_{b=0}^{1}\mathrm{tr}\left(A^{(v_i=b)}_{i,\boldsymbol{q}|q_i=0}\sum_{\boldsymbol{y},\boldsymbol{d}:\hat{b}(k_i,y_i)=b}\sigma^{(000)}_{\boldsymbol{y},\boldsymbol{d}}\otimes|\boldsymbol{y},\boldsymbol{d}\rangle\langle\boldsymbol{y},\boldsymbol{d}|\right).\tag{20}$$

By using the definition in Eq. (13), Eq. (20) is rewritten as

$$\sum_{\boldsymbol{v}\in\{0,1\}^3}\mathrm{tr}(A^{(v_i)}_{i,\boldsymbol{q}|q_i=0}\sigma^{(0,v_1;0,v_2;0,v_3)}).$$

Substituting this to Eq. (19) results in

$$\Pr\{\boldsymbol{\theta}=000, flag=fail_{\rm Test}|\text{Test, Hadamard round}\}=\frac{1}{8}-\frac{1}{96}\sum_{i=1}^{3}\sum_{\boldsymbol{q}_{\bar{i}}\in\{0,1\}^2}\sum_{\boldsymbol{v}\in\{0,1\}^3}\mathrm{tr}(A^{(v_i)}_{i,\boldsymbol{q}|q_i=0}\sigma^{(0,v_1;0,v_2;0,v_3)}).\tag{21}$$

Next, we calculate the second term of Eq. (18):

$$\begin{aligned}
&\Pr\{\mathrm{wt}(\boldsymbol{\theta})=1, flag=fail_{\rm Test}|\text{Test, Hadamard round}\}\\
=&\frac{1}{4}\sum_{i=1}^{3}\Pr\{flag=fail_{\rm Test}|\text{Test, Hadamard round},\mathrm{wt}(\boldsymbol{\theta})=1,\theta_i=1\}\\
=&\frac{1}{4}\sum_{i=1}^{3}\Pr\{q_i=1,\hat{u}(k_i,y_i,d_i)\oplus\prod_{j\neq i}\hat{b}(k_j,y_j)\neq v_i|\text{Test, Hadamard round},\mathrm{wt}(\boldsymbol{\theta})=1,\theta_i=1\}\\
=&\frac{1}{32}\sum_{i=1}^{3}\sum_{b=0}^{1}\sum_{\boldsymbol{y},d_i}\sum_{\boldsymbol{q}_{\bar{i}}}\Pr\{\hat{u}(k_i,y_i,d_i)\oplus\prod_{j\neq i}\hat{b}(k_j,y_j)=b,v_i=\bar{b}|\text{Test, Hadamard round},\mathrm{wt}(\boldsymbol{\theta})=1,\theta_i=1,q_i=1,\boldsymbol{q}_{\bar{i}}\}\\
=&\frac{1}{32}\Big[\sum_{i=1}^{3}\sum_{\boldsymbol{q}_{\bar{i}}}1\\
&-\sum_{i=1}^{3}\sum_{b=0}^{1}\sum_{\boldsymbol{y},d_i}\sum_{\boldsymbol{q}_{\bar{i}}}\Pr\{\hat{u}(k_i,y_i,d_i)\oplus\prod_{j\neq i}\hat{b}(k_j,y_j)=v_i=b|\text{Test, Hadamard round},\mathrm{wt}(\boldsymbol{\theta})=1,\theta_i=1,q_i=1,\boldsymbol{q}_{\bar{i}}\}\Big].
\end{aligned}\tag{22}$$

Here, $\sum_{b=0}^{1}\sum_{\boldsymbol{y},d_i}\Pr\{\hat{u}(k_i,y_i,d_i)\oplus\prod_{j\neq i}\hat{b}(k_j,y_j)=v_i=b|\text{Test, Hadamard round},\mathrm{wt}(\boldsymbol{\theta})=1,\theta_i=1,q_i=1,\boldsymbol{q}_{\bar{i}}\}$ expresses the probability that the prover's answer v_i is accepted by the verifier conditioned on measuring the state $\rho^{(\boldsymbol{\theta})}$ with $\mathrm{wt}(\boldsymbol{\theta})=1$ and $\theta_i=1$ when $\boldsymbol{q}$ with $q_i=1$ is input to the device. This probability can be written by using the expressions of the states and measurements as

$$\sum_{b=0}^{1}\mathrm{tr}\left(A^{(v_i=b)}_{i,\boldsymbol{q}|q_i=1}\sum_{\boldsymbol{y},\boldsymbol{d}:\hat{u}(k_i,y_i,d_i)\oplus\prod_{j\neq i}\hat{b}(k_j,y_j)=b}\sigma^{(\boldsymbol{\theta}\text{ s.t. }\mathrm{wt}(\boldsymbol{\theta})=1,\theta_i=1)}_{\boldsymbol{y},\boldsymbol{d}}\otimes|\boldsymbol{y},\boldsymbol{d}\rangle\langle\boldsymbol{y},\boldsymbol{d}|\right).\tag{23}$$

By using the definitions in Eqs. (14)-(16), for $\boldsymbol{\theta}$ such that $\mathrm{wt}(\boldsymbol{\theta})=1$ and $\theta_i=1$, Eq. (23) is rewritten as

$$\sum_{\boldsymbol{v}} \mathrm{tr}\left(A^{(v_i)}_{i,\boldsymbol{q}|q_i=1}\sigma^{(\theta_1,v_1;\theta_2,v_2;\theta_3,v_3)}\right).$$

Substituting this to Eq. (22) results in

$$\Pr\{\mathrm{wt}(\boldsymbol{\theta})=1, flag=fail_{\mathrm{Test}}|\mathrm{Test},\mathrm{Hadamard\ round}\}=\frac{3}{8}-\frac{1}{32}\sum_{i=1}^{3}\sum_{\boldsymbol{q}_{\bar{i}}\in\{0,1\}^2}\sum_{\boldsymbol{v}\in\{0,1\}^3}\mathrm{tr}\left(A^{(v_i)}_{i,\boldsymbol{q}|q_i=1}\sigma^{(\theta_1,v_1;\theta_2,v_2;\theta_3,v_3)}\right). \tag{24}$$

Substituting Eqs. (21) and (24) to Eq. (18), Eq. (18) results in

$$\begin{aligned}&\Pr\{flag=fail_{\mathrm{Test}}|\mathrm{Test},\mathrm{Hadamard\ round}\}\\ =&\frac{1}{2}-\frac{1}{96}\sum_{i=1}^{3}\sum_{\boldsymbol{q}_{\bar{i}}}\left(\mathrm{tr}\left[\sum_{\boldsymbol{v}}A^{(v_i)}_{i,\boldsymbol{q}|q_i=0}\sigma^{(0,v_1;0,v_2;0,v_3)}\right]+3\mathrm{tr}\left[\sum_{\boldsymbol{v}}A^{(v_i)}_{i,\boldsymbol{q}|q_i=1}\sigma^{(\theta_1,v_1;\theta_2,v_2;\theta_3,v_3)}\right]\right).\end{aligned} \tag{25}$$

In Eq. (25), there are 3×2^3 trace terms, and its minimum term is $1-\gamma_T(D)$ as defined in Eq. (12). To take a lower bound on Eq. (25), we replace the $(3\times 2^3-1)$ trace terms by 1 and only one term by $1-\gamma_T(D)$. By doing so, we have

$$\begin{aligned}\Pr\{flag=fail_{\mathrm{Test}}|\mathrm{Test},\mathrm{Hadamard\ round}\}&\geq\frac{1}{2}-\frac{1}{96}\left\{[(3\times 2^2-1)\times 1+1\times(1-\gamma_T(D))]+(3\times 3\times 2^2)\times 1\right\}\\ &=\frac{\gamma_T(D)}{96}.\end{aligned}$$

Therefore, we finally obtain

$$\gamma_T(D)\leq 96\cdot\Pr\{flag=fail_{\mathrm{Test}}|\mathrm{Test},\mathrm{Hadamard\ round}\}.$$

■

Lemma 26 *(Hypergraph case) Let $D=(S,\Pi,M,P)$ be a device. We define*

$$\gamma_H(D):=1-r_{\min} \tag{26}$$

with

$$\begin{aligned}r_{\min}:=\min\Big\{&\sum_{\boldsymbol{s}\in\{0,1\}^3}\mathrm{tr}\left[\left(A_{1,\boldsymbol{q}=100}A^{(0)}_{2,\boldsymbol{q}=100}+A_{1,\boldsymbol{q}=100}A^{(1)}_{2,\boldsymbol{q}=100}A_{3,\boldsymbol{q}=100}\right)^{(s_1)}\sigma^{(1,s_1;1,s_2;1,s_3)}\right],\\ &\sum_{\boldsymbol{s}\in\{0,1\}^3}\mathrm{tr}\left[\left(A^{(0)}_{1,\boldsymbol{q}=010}A_{2,\boldsymbol{q}=010}+A^{(1)}_{1,\boldsymbol{q}=010}A_{2,\boldsymbol{q}=010}A_{3,\boldsymbol{q}=010}\right)^{(s_2)}\sigma^{(1,s_1;1,s_2;1,s_3)}\right],\\ &\sum_{\boldsymbol{s}\in\{0,1\}^3}\mathrm{tr}\left[\left(A^{(0)}_{1,\boldsymbol{q}=001}A_{3,\boldsymbol{q}=001}+A^{(1)}_{1,\boldsymbol{q}=001}A_{2,\boldsymbol{q}=001}A_{3,\boldsymbol{q}=001}\right)^{(s_3)}\sigma^{(1,s_1;1,s_2;1,s_3)}\right]\Big\},\end{aligned}$$

and

$$\sigma^{(1,s_1;1,s_2;1,s_3)}:=\sum_{\substack{\boldsymbol{y},\boldsymbol{d}:\\ \hat{u}(k_1,y_1,d_1)=s_1,\hat{u}(k_2,y_2,d_2)=s_2,\hat{u}(k_3,y_3,d_3)=s_3}}\sigma^{(111)}_{\boldsymbol{y},\boldsymbol{d}}\otimes|\boldsymbol{y},\boldsymbol{d}\rangle\langle\boldsymbol{y},\boldsymbol{d}|. \tag{27}$$

Then, the upper bound on $\gamma_H(D)$ is given by

$$\gamma_H(D)\leq 8\cdot\Pr\{flag=fail_{\mathrm{Hyper}}|\boldsymbol{\theta}=111,\mathrm{Hadamard\ round}\}.$$

Note that $\Pr\{flag = fail_{\rm Hyper}|\boldsymbol{\theta} = 111, \text{Hadamard round}\}$ can be estimated through repeating the self-testing protocol.

(Proof) The probability of obtaining $fail_{\rm Hyper}$ conditioned on choosing the hypergraph case ($\boldsymbol{\theta} = 111$) and the Hadamard round is calculated as

$$\begin{aligned}
&\Pr\{flag = fail_{\rm Hyper}|\boldsymbol{\theta} = 111, \text{Hadamard round}] \\
=&\Pr\{\boldsymbol{q} = 100, \hat{u}(k_1, y_1, d_1) \neq v_1 \oplus \delta_{v_2,1} \cdot v_3|\boldsymbol{\theta} = 111, \text{Hadamard round}\} \\
+&\Pr\{\boldsymbol{q} = 010, \hat{u}(k_2, y_2, d_2) \neq v_2 \oplus \delta_{v_1,1} \cdot v_3|\boldsymbol{\theta} = 111, \text{Hadamard round}\} \\
+&\Pr\{\boldsymbol{q} = 001, \hat{u}(k_3, y_3, d_3) \neq v_3 \oplus \delta_{v_1,1} \cdot v_2|\boldsymbol{\theta} = 111, \text{Hadamard round}\} \\
=&\frac{1}{8}\sum_{b=0}^{1}\sum_{y_1,d_1} \Pr\{\hat{u}(k_1, y_1, d_1) = b, v_1 \oplus \delta_{v_2,1} \cdot v_3 = \bar{b}|\boldsymbol{\theta} = 111, \text{Hadamard round}, \boldsymbol{q} = 100\} \\
+&\frac{1}{8}\sum_{b=0}^{1}\sum_{y_2,d_2} \Pr\{\hat{u}(k_2, y_2, d_2) = b, v_2 \oplus \delta_{v_1,1} \cdot v_3 = \bar{b}|\boldsymbol{\theta} = 111, \text{Hadamard round}, \boldsymbol{q} = 010\} \\
+&\frac{1}{8}\sum_{b=0}^{1}\sum_{y_3,d_3} \Pr\{\hat{u}(k_3, y_3, d_3) = b, v_3 \oplus \delta_{v_1,1} \cdot v_2 = \bar{b}|\boldsymbol{\theta} = 111, \text{Hadamard round}, \boldsymbol{q} = 001\} \\
=&\frac{3}{8} - \frac{1}{8}\sum_{b=0}^{1}\Big(\sum_{y_1,d_1} \Pr\{\hat{u}(k_1, y_1, d_1) = v_1 \oplus \delta_{v_2,1} \cdot v_3 = b|\boldsymbol{\theta} = 111, \text{Hadamard round}, \boldsymbol{q} = 100\} \\
&+ \sum_{y_2,d_2} \Pr\{\hat{u}(k_2, y_2, d_2) = v_2 \oplus \delta_{v_1,1} \cdot v_3 = b|\boldsymbol{\theta} = 111, \text{Hadamard round}, \boldsymbol{q} = 010\} \\
&+ \sum_{y_3,d_3} \Pr\{\hat{u}(k_3, y_3, d_3) = v_3 \oplus \delta_{v_1,1} \cdot v_2 = b|\boldsymbol{\theta} = 111, \text{Hadamard round}, \boldsymbol{q} = 001\}\Big).
\end{aligned} \tag{28}$$

Here, $\sum_{b=0}^{1}\sum_{y_1,d_1} \Pr\{\hat{u}(k_1, y_1, d_1) = v_1 \oplus \delta_{v_2,1} \cdot v_3 = b|\boldsymbol{\theta} = 111, \text{Hadamard round}, \boldsymbol{q} = 100\}$ represents the probability that the prover's answer $v_1 \oplus \delta_{v_2,1} \cdot v_3$ is accepted by the verifier conditioned on measuring the state $\rho^{(111)}$ when $\boldsymbol{q} = 100$ is input to the device. This probability can be rewritten by using the expressions of the states and measurements as

$$\begin{aligned}
&\sum_{b=0}^{1} \mathrm{tr}\left[(A_{1,\boldsymbol{q}=100}A^{(0)}_{2,\boldsymbol{q}=100} + A_{1,\boldsymbol{q}=100}A^{(1)}_{2,\boldsymbol{q}=100}A_{3,\boldsymbol{q}=100})^{(b)} \sum_{\substack{y_1,d_1:\\ \hat{u}(k_1,y_1,d_1)=b}} \Big(|y_1,d_1\rangle\langle y_1,d_1|\rho^{(111)}|y_1,d_1\rangle\langle y_1,d_1|\Big)\right] \\
=&\sum_{\boldsymbol{s}\in\{0,1\}^3} \mathrm{tr}\left[(A_{1,\boldsymbol{q}=100}A^{(0)}_{2,\boldsymbol{q}=100} + A_{1,\boldsymbol{q}=100}A^{(1)}_{2,\boldsymbol{q}=100}A_{3,\boldsymbol{q}=100})^{(s_1)}\sigma^{(1,s_1;1,s_2;1,s_3)}\right],
\end{aligned} \tag{29}$$

where $\sigma^{(1,s_1;1,s_2;1,s_3)}$ is defined in Eq. (27). Analogously, we have

$$\begin{aligned}
&\sum_{b=0}^{1}\sum_{y_2,d_2} \Pr\{\hat{u}(k_2, y_2, d_2) = v_2 \oplus \delta_{v_1,1} \cdot v_3 = b|\boldsymbol{\theta} = 111, \text{Hadamard round}, \boldsymbol{q} = 010\} \\
=&\sum_{\boldsymbol{s}\in\{0,1\}^3} \mathrm{tr}\left[(A^{(0)}_{1,\boldsymbol{q}=010}A_{2,\boldsymbol{q}=010} + A^{(1)}_{1,\boldsymbol{q}=010}A_{2,\boldsymbol{q}=010}A_{3,\boldsymbol{q}=010})^{(s_2)}\sigma^{(1,s_1;1,s_2;1,s_3)}\right],
\end{aligned} \tag{30}$$

and

$$\begin{aligned}
&\sum_{b=0}^{1}\sum_{y_3,d_3} \Pr\{\hat{u}(k_3, y_3, d_3) = v_3 \oplus \delta_{v_1,1} \cdot v_2 = b|\boldsymbol{\theta} = 111, \text{Hadamard round}, \boldsymbol{q} = 001\} \\
=&\sum_{\boldsymbol{s}\in\{0,1\}^3} \mathrm{tr}\left[(A^{(0)}_{1,\boldsymbol{q}=001}A_{3,\boldsymbol{q}=001} + A^{(1)}_{1,\boldsymbol{q}=001}A_{2,\boldsymbol{q}=001}A_{3,\boldsymbol{q}=001})^{(s_3)}\sigma^{(1,s_1;1,s_2;1,s_3)}\right].
\end{aligned} \tag{31}$$

By substituting Eqs. (29)-(31) to Eq. (28), we obtain

$$\begin{aligned}
&\Pr\{flag = fail_{\rm Hyper}|\boldsymbol{\theta} = 111, \text{Hadamard round}\}\\
=&\frac{3}{8} - \frac{1}{8}\Big(\sum_{\boldsymbol{s}} \mathrm{tr}\left[\left(A_{1,\boldsymbol{q}=100}A^{(0)}_{2,\boldsymbol{q}=100} + A_{1,\boldsymbol{q}=100}A^{(1)}_{2,\boldsymbol{q}=100}A_{3,\boldsymbol{q}=100}\right)^{(s_1)}\sigma^{(1,s_1;1,s_2;1,s_3)}\right]\\
&+\sum_{\boldsymbol{s}} \mathrm{tr}\left[\left(A^{(0)}_{1,\boldsymbol{q}=010}A_{2,\boldsymbol{q}=010} + A^{(1)}_{1,\boldsymbol{q}=010}A_{2,\boldsymbol{q}=010}A_{3,\boldsymbol{q}=010}\right)^{(s_2)}\sigma^{(1,s_1;1,s_2;1,s_3)}\right]\\
&+\sum_{\boldsymbol{s}} \mathrm{tr}\left[\left(A^{(0)}_{1,\boldsymbol{q}=001}A_{3,\boldsymbol{q}=001} + A^{(1)}_{1,\boldsymbol{q}=001}A_{2,\boldsymbol{q}=001}A_{3,\boldsymbol{q}=001}\right)^{(s_3)}\sigma^{(1,s_1;1,s_2;1,s_3)}\right]\Big).
\end{aligned}$$

Using the definition in Eq. (26), we obtain its lower bound as

$$\Pr\{flag = fail_{\rm Hyper}|\boldsymbol{\theta} = 111, \text{Hadamard round}\} \geq \frac{3}{8} - \frac{2 + r_{\min}}{8} = \frac{\gamma_H(D)}{8},$$

which results in

$$\gamma_H(D) \leq 8 \cdot \Pr\{flag = fail_{\rm Hyper}|\boldsymbol{\theta} = 111, \text{Hadamard round}\}. \tag{32}$$

■

At the end of this section, we introduce Lemma 27 and Corollary 28 that are frequently used in the rest of the soundness proof. These are respectively introduced in Lemma 4.7 and Corollary 4.8 [2]. For self-consistency of this paper, we describe these statements and proofs.

Lemma 27 *Let $D = (S, \Pi, M, P)$ be a device. For any binary observable O, $\boldsymbol{\theta} \in \mathcal{B}$, $i \in \{1, 2, 3\}$ and $\epsilon \geq 0$,*

$$\sum_{\boldsymbol{v}\in\{0,1\}^3} \mathrm{tr}(O^{(v_i)}\sigma^{(\theta_1,v_1;\theta_2,v_2;\theta_3,v_3)}) \approx_\epsilon 1 \Rightarrow \forall \boldsymbol{v} \in \{0,1\}^3 : \mathrm{tr}(\sigma^{(\theta_1,v_1;\theta_2,v_2;\theta_3,v_3)}) \approx_\epsilon \mathrm{tr}(O^{(v_i)}\sigma^{(\theta_1,v_1;\theta_2,v_2;\theta_3,v_3)}),$$

where the definitions of $\sigma^{(\theta_1,v_1;\theta_2,v_2;\theta_3,v_3)}$ are given in Eqs. (13)-(16) and (27).

(Proof) Since the binary observable satisfies $O^{(v_i)} \leq I$, there exists $\Delta_{\boldsymbol{v}} \geq 0$ such that

$$\mathrm{tr}(O^{(v_i)}\sigma^{(\theta_1,v_1;\theta_2,v_2;\theta_3,v_3)}) = \mathrm{tr}(\sigma^{(\theta_1,v_1;\theta_2,v_2;\theta_3,v_3)}) - \Delta_{\boldsymbol{v}}. \tag{33}$$

From this and the assumption, we have

$$\left|\sum_{\boldsymbol{v}} \mathrm{tr}(O^{(v_i)}\sigma^{(\theta_1,v_1;\theta_2,v_2;\theta_3,v_3)}) - 1\right| = \sum_{\boldsymbol{v}} \Delta_{\boldsymbol{v}} \approx_\epsilon 0.$$

As $\Delta_{\boldsymbol{v}} \geq 0$, $\Delta_{\boldsymbol{v}} \approx_\epsilon 0$ holds for any $\boldsymbol{v}$. Combining $\Delta_{\boldsymbol{v}} \approx_\epsilon 0$ and Eq. (33) results in the desired relation. ■

Corollary 28 *Let $D = (S, \Pi, M, P)$ be a device. For any binary observable O, $\boldsymbol{\theta} \in \mathcal{B}$, $i \in \{1, 2, 3\}$ and $\epsilon \geq 0$,*

$$\sum_{\boldsymbol{v}\in\{0,1\}^3} \mathrm{tr}(O^{(v_i)}\sigma^{(\theta_1,v_1;\theta_2,v_2;\theta_3,v_3)}) \approx_\epsilon 1 \Rightarrow \forall \boldsymbol{v} \in \{0,1\}^3 : O \approx_{\epsilon,\sigma^{(\theta_1,v_1;\theta_2,v_2;\theta_3,v_3)}} (-1)^{v_i} I,$$

where the definitions of states $\sigma^{(\theta_1,v_1;\theta_2,v_2;\theta_3,v_3)}$ are given in Eqs. (13)-(16) and (27).

(Proof) By applying Lemma 27, the assumption leads to

$$\mathrm{tr}(\sigma^{(\theta_1,v_1;\theta_2,v_2;\theta_3,v_3)}) \approx_\epsilon \mathrm{tr}(O^{(v_i)}\sigma^{(\theta_1,v_1;\theta_2,v_2;\theta_3,v_3)}).$$

Then, using Lemma 14 implies the desired relation. ■

D. Reduction to perfect device

In this section, we introduce a *perfect device* that passes the preimage round of our protocol with probability $1-\mathrm{negl}(\lambda)$. This is just for a technical convenience that simplifies the rest of the soundness proof. The arguments in this section are exactly the same as those in Sec 4.2.1 of [2], and here we just summarize their arguments.

Definition 29 *(Perfect device). We call a device $D=(S,\Pi,M,P)$ perfect if*

$$\gamma_P(D)=\mathrm{negl}(\lambda).$$

The following lemma claims that for any efficient device D, we can efficiently construct another efficient perfect device D', which uses the same measurements as D, and whose initial state is close to the one of D. Once the state that is close to the initial state of D in hand, we can replace the actual states $S=\{\psi^{(\boldsymbol{\theta})}\}_{\boldsymbol{\theta}\in\mathcal{B}}$ of D with the virtual ones $S'=\{\psi'^{(\boldsymbol{\theta})}\}_{\boldsymbol{\theta}\in\mathcal{B}}$ of D' [2] .

Lemma 30 *Let $D=(S,\Pi,M,P)$ be an efficient device with $S=\{\psi^{(\boldsymbol{\theta})}\}_{\boldsymbol{\theta}\in\mathcal{B}}$ and $\gamma_P(D)<1-1/\mathrm{poly}(\lambda)$. Then there exists an efficient perfect device $D'=(S',\Pi,M,P)$, which uses the same measurements Π,M,P and whose states $S'=\{\psi'^{(\boldsymbol{\theta})}\}_{\boldsymbol{\theta}\in\mathcal{B}}$ satisfy the following for any $\boldsymbol{\theta}\in\mathcal{B}$:*

$$||\psi^{(\boldsymbol{\theta})}-\psi'^{(\boldsymbol{\theta})}||_1\approx_{\sqrt{\gamma_P(D)}}0. \tag{34}$$

(Proof) In the proof, we explicitly construct the perfect device D' satisfying Eq. (34). In so doing, we first derive the probability of failing the preimage check given the basis choice $\boldsymbol{\theta}\in\mathcal{B}$ in the preimage round:

$$\begin{aligned}
&\Pr\{\text{Prover fails the preimage check}|\boldsymbol{\theta},\text{preimage round}\}\\
=&\Pr\{\text{Prover fails the }1^{\text{st}}\vee 2^{\text{nd}}\vee 3^{\text{rd}}\text{ preimage check}|\boldsymbol{\theta},\text{preimage round}\}\\
\leq&\sum_{i=1}^{3}\Pr\{\text{Prover fails the }i^{\text{th}}\text{ preimage check}|\boldsymbol{\theta},\text{preimage round}\}\\
=&\sum_{i=1}^{3}\left(1-\Pr\{\text{Prover passes the }i^{\text{th}}\text{ preimage check}|\boldsymbol{\theta},\text{preimage round}\}\right).
\end{aligned}$$

The inequality just comes from the union bound. By recalling the definitions in Eqs. (7) and (8), since $\Pr\{\text{Prover passes the }i^{\text{th}}\text{ preimage check}|\boldsymbol{\theta},\text{preimage round}\}\geq 1-\gamma_P(D)$ holds for any $i\in\{1,2,3\}$ and $\boldsymbol{\theta}\in\mathcal{B}$, we obtain

$$\Pr\{\text{Prover fails the preimage check}|\boldsymbol{\theta},\text{preimage round}\}\leq 3\gamma_P(D). \tag{35}$$

Now, we can efficiently construct the states $\psi'^{(\boldsymbol{\theta})}$ as follows. First, the state $\psi^{(\boldsymbol{\theta})}$ is prepared as D does and we perform the measurement to obtain $\boldsymbol{y}$. Second, we execute the preimage check with measurement Π and obtain its result (either a pass or a failure of the preimage check). If the preimage check fails, then we repeat the same procedure. From Eq. (35), since the probability of failing the preimage test is upper-bounded by $3\gamma_P(D)$, if we repeat the same procedure polynomial times to λ, the probability of obtaining failures for all the trials is $\mathrm{negl}(\lambda)$. Hence, if we post-select the state $\psi^{(\boldsymbol{\theta})}$ that passes the preimage check, the device with this state constitutes a perfect device.

By using Eq. (35), we derive the trace distance between $\psi^{(\boldsymbol{\theta})}$ and $\psi'^{(\boldsymbol{\theta})}$ simplify by applying the gentle measurement lemma [4]. Combining this lemma and Eq. (35) results in $||\psi^{(\boldsymbol{\theta})}-\psi'^{(\boldsymbol{\theta})}||_1\approx_{\sqrt{\gamma_P(D)}}0$. ■

---

[2] Note that the replacement of states is also done in the security proof of quantum key distribution (QKD) [3]. In QKD, we can take *any* virtual states for replacement as long as they are the same with the actual states from an eavesdropper's perspective. In this paper, since we discuss the soundness proof in the computational assumptions, we cannot take any virtual states $S'=\{\psi'^{(\boldsymbol{\theta})}\}_{\boldsymbol{\theta}\in\mathcal{B}}$ for replacement but only take those that can be efficiently constructed from the actual states $S=\{\psi^{(\boldsymbol{\theta})}\}_{\boldsymbol{\theta}\in\mathcal{B}}$.

E. Computational indistinguishability of post-measurement states

In this section, we show the computational indistinguishability of the post-measurement states. Specifically, we derive $O(\delta)$ in Definition 10 for the states $\rho^{(\boldsymbol{\theta})}$ that are defined in Eq. (5).

Lemma 31 *Let $\mathcal{F}$ be an extended trapdoor claw-free family. For arbitrary $\boldsymbol{\theta} \in \{0,1\}^3$, let $\rho^{(\boldsymbol{\theta})}$ be a post-measurement normalized state obtained in the protocol execution along with $\mathcal{F}$. Then, for any $\boldsymbol{\theta}, \boldsymbol{\theta}' \in \{0,1\}^3$ and quantum polynomial-time algorithm $\mathcal{D}$, there exists a negligible function* $\mathrm{negl}(\cdot)$ *such that*

$$\left|\Pr\{\mathcal{D}(\rho^{(\boldsymbol{\theta})}) = 0\} - \Pr\{\mathcal{D}(\rho^{(\boldsymbol{\theta}')}) = 0\}\right| \leq \mathrm{negl}(\lambda).$$

The same statement holds for the states $\psi^{(\boldsymbol{\theta})}$, defined in Eq. (4), because the following proof is valid also for $\psi^{(\boldsymbol{\theta})}$.

(Proof) To prove this lemma, we only have to show that for any $\boldsymbol{\theta}, \boldsymbol{\theta}' \in \{0,1\}^3$ such that $\theta_i \neq \theta'_i$ for some $i \in \{1,2,3\}$ and $\theta_j = \theta'_j$ for $j \in \{1,2,3\}\backslash\{i\}$, and for any quantum polynomial-time algorithm $\mathcal{D}$, there exists a negligible function $\mathrm{negl}(\cdot)$ such that

$$\left|\Pr\{\mathcal{D}(\rho^{(\boldsymbol{\theta})}) = 0\} - \Pr\{\mathcal{D}(\rho^{(\boldsymbol{\theta}')}) = 0\}\right| \leq \mathrm{negl}(\lambda). \tag{36}$$

This is because once we obtain Eq. (36), we can lift Eq. (36) to any $\boldsymbol{\theta}, \boldsymbol{\theta}'$. For instance, if $\boldsymbol{\theta} = 000$, $\boldsymbol{\theta}' = 111$, by using the following inequalities from Eq. (36) with negligible functions $\mathrm{negl}_1(\cdot)$, $\mathrm{negl}_2(\cdot)$, and $\mathrm{negl}_3(\cdot)$:

$$\begin{aligned}
&\left|\Pr\{\mathcal{D}(\rho^{(000)}) = 0\} - \Pr\{\mathcal{D}(\rho^{(001)}) = 0\}\right| \leq \mathrm{negl}_1(\lambda),\\
&\left|\Pr\{\mathcal{D}(\rho^{(001)}) = 0] - \Pr\{\mathcal{D}(\rho^{(011)}) = 0\}\right| \leq \mathrm{negl}_2(\lambda),\\
&\left|\Pr\{\mathcal{D}(\rho^{(011)}) = 0\} - \Pr\{\mathcal{D}(\rho^{(111)}) = 0\}\right| \leq \mathrm{negl}_3(\lambda),
\end{aligned}$$

we have

$$\left|\Pr\{\mathcal{D}(\rho^{(000)}) = 0\} - \Pr\{\mathcal{D}(\rho^{(111)}) = 0\}\right| \leq \mathrm{negl}_1(\lambda) + \mathrm{negl}_2(\lambda) + \mathrm{negl}_3(\lambda).$$

Here, the right hand side of this inequality is also a negligible function of λ. Note that our self-testing protocol only runs for $\boldsymbol{\theta} \in \mathcal{B}$, but $\rho^{(\boldsymbol{\theta})}$ is well-defined for any $\boldsymbol{\theta}$. Hence, the above argument can be applied for any $\boldsymbol{\theta}, \boldsymbol{\theta}' \in \{0,1\}^3$.

Therefore, the remaining task is to prove Eq. (36). In so doing, we use the algorithm $\mathcal{D}$ to construct an algorithm $\mathcal{A}$ for the injective invariance of $\mathcal{F}$.

- $b \leftarrow \mathcal{A}(k)$: given a key k of $\mathcal{F}$ or $\mathcal{G}$, $\mathcal{A}$ sets $k_i := k$ and for $j \in \{1,2,3\}\backslash\{i\}$ computes

$$k_j \leftarrow \begin{cases} \mathsf{GEN}_{\mathcal{G}}(1^\lambda) & \text{if } \theta_j = 0,\\ \mathsf{GEN}_{\mathcal{F}}(1^\lambda) & \text{if } \theta_j = 1. \end{cases}$$

  $\mathcal{A}$ prepares a post-measurement normalized state $\rho^{(\boldsymbol{\theta})}$ with k_1, k_2 and k_3, and output $b \leftarrow \mathcal{D}(\rho^{(\boldsymbol{\theta})})$.

Then, we have

$$\begin{aligned}
\Pr\{\mathcal{D}(\rho^{(\boldsymbol{\theta})}) = 0\} &= \Pr_{(k,t_k)\leftarrow\mathsf{GEN}_{\mathcal{G}}(1^\lambda)}\{\mathcal{A}(k) = 0\},\\
\Pr\{\mathcal{D}(\rho^{(\boldsymbol{\theta}')}) = 0\} &= \Pr_{(k,t_k)\leftarrow\mathsf{GEN}_{\mathcal{F}}(1^\lambda)}\{\mathcal{A}(k) = 0\},
\end{aligned}$$

which implies Eq. (36) by the injective invariance of $\mathcal{F}$. ■

In the following Secs. V F, V G and V H, we only discuss the non-tilde observables, namely $\{A_{i,\boldsymbol{q}=000}\}_{i=1}^3$ and $\{A_{i,\boldsymbol{q}=111}\}_{i=1}^3$ that are defined in Definition 23. For simplicity, we use the notations:

$$A_{i,\mathbf{0}} := A_{i,\boldsymbol{q}=000}, \quad A_{i,\mathbf{1}} := A_{i,\boldsymbol{q}=111}.$$

F. Anti-commutation relations of non-tilde observables

The goal of this section is to prove the following Proposition 32, which states the anti-commutation relations of the non-tilde observables.

Proposition 32 *For any efficient perfect device $D = (S, \Pi, M, P)$, we obtain the following approximate anti-commutation relations for non-tilde observables that satisfy for any $i \in \{1,2,3\}$ and $\boldsymbol{\theta} \in \mathcal{B}$:*

$$\{A_{i,\mathbf{0}}, A_{i,\mathbf{1}}\} \approx_{\sqrt{\gamma_T(D)},\rho^{(\boldsymbol{\theta})}} 0.$$

(Proof) We give the proof for $i = 1$, and the other cases can be shown analogously. By the definition of state-dependent norm, the computational indistinguishability of $\rho^{(\boldsymbol{\theta})}$ from Lemma 31 and using Lemma 21 (iv), it suffices to show

$$\mathrm{tr}\left[\{A_{1,\mathbf{0}}, A_{1,\mathbf{1}}\}^2 \rho^{(100)}\right] \approx_{\sqrt{\gamma_T(D)}} 0. \tag{37}$$

Since $A_{1,\mathbf{0}}$ and $A_{1,\mathbf{1}}$ are binary observables, $\{A_{1,\mathbf{0}}, A_{1,\mathbf{1}}\}^2/4$ is calculated as

$$\frac{1}{4}\{A_{1,\mathbf{0}}, A_{1,\mathbf{1}}\}^2 = A_{1,\mathbf{1}} A^{(0)}_{1,\mathbf{0}} A_{1,\mathbf{1}} A^{(0)}_{1,\mathbf{0}} + A^{(1)}_{1,\mathbf{0}} A_{1,\mathbf{1}} A^{(1)}_{1,\mathbf{0}} A_{1,\mathbf{1}}.$$

Using $\rho^{(100)} = \sum_{\boldsymbol{v}} \sigma^{(1,v_1;0,v_2;0,v_3)}$ leads to

$$\frac{1}{4}\mathrm{tr}\left[\{A_{1,\mathbf{0}}, A_{1,\mathbf{1}}\}^2 \rho^{(100)}\right] = \sum_{\boldsymbol{v}} \mathrm{tr}\left[(A_{1,\mathbf{1}} A^{(0)}_{1,\mathbf{0}} A_{1,\mathbf{1}} A^{(0)}_{1,\mathbf{0}} + A^{(1)}_{1,\mathbf{0}} A_{1,\mathbf{1}} A^{(1)}_{1,\mathbf{0}} A_{1,\mathbf{1}}) \sigma^{(1,v_1;0,v_2;0,v_3)}\right].$$

We can replace the leftmost and the rightmost $A_{1,\mathbf{1}}$ with $(-1)^{v_1} I$ by the following arguments. From the definition of $\gamma_T(D)$ and Corollary 28, we have

$$A_{1,\mathbf{1}} \approx_{\gamma_T(D),\sigma^{(1,v_1;0,v_2;0,v_3)}} (-1)^{v_1} I.$$

Then, from Lemma 17 (i), we can replace the two outer $A_{1,\mathbf{1}}$ with $(-1)^{v_1} I$ as

$$\frac{1}{4}\mathrm{tr}\left[\{A_{1,\mathbf{0}}, A_{1,\mathbf{1}}\}^2 \rho^{(100)}\right] \approx_{\sqrt{\gamma_T(D)}} \sum_{\boldsymbol{v},b} (-1)^{v_1} \mathrm{tr}\left(A_{1,\mathbf{1}} A^{(b)}_{1,\mathbf{0}} \sigma^{(1,v_1;0,v_2;0,v_3)} A^{(b)}_{1,\mathbf{0}}\right).$$

From Lemma 38, which will be proven later, we obtain

$$\sum_{\boldsymbol{v},b} (-1)^{v_1} \mathrm{tr}\left(A_{1,\mathbf{1}} A^{(b)}_{1,\mathbf{0}} \sigma^{(1,v_1;0,v_2;0,v_3)} A^{(b)}_{1,\mathbf{0}}\right) \approx_{\sqrt{\gamma_T(D)}} 0.$$

Combining the just above two equations and the triangle inequality results in Eq. (37). ■

The rest of this section is devoted to prove Lemma 38. The following Lemmas 33, 35, 36 and 37, and Corollary 34 are auxiliary statements to prove Lemma 38. First, we prove a similar statement to Lemma 38 in Lemma 33 that holds for any efficient prover.

Lemma 33 *For any efficient device $D = (S, \Pi, M, P)$, the following holds for any $\boldsymbol{\theta} \in \mathcal{B}$ and $i \in \{1,2,3\}$,*

$$\sum_{b=0}^{1} \mathrm{tr}\left(A_{i,\mathbf{1}} A^{(b)}_{i,\mathbf{0}} \rho^{(\boldsymbol{\theta})} A^{(b)}_{i,\mathbf{0}}\right) \approx_{\sqrt{\gamma_T(D)}} 0. \tag{38}$$

(Proof) We show Eq. (38) for $i = 1$, and the others are analogous. As $A_{1,\mathbf{0}}$ is an efficient binary observable, from Lemmas 12 and 31, we have

$$\sum_{b=0}^{1} A^{(b)}_{1,\mathbf{0}} \rho^{(\boldsymbol{\theta})} A^{(b)}_{1,\mathbf{0}} \overset{c}{\approx}_0 \sum_{b=0}^{1} A^{(b)}_{1,\mathbf{0}} \rho^{(\boldsymbol{\theta}')} A^{(b)}_{1,\mathbf{0}}$$

for any different $\boldsymbol{\theta}$ and $\boldsymbol{\theta}'$. From this and by using the fact that $A_{1,\mathbf{1}}$ is an efficient binary observable, Lemma 21 (i) leads to

$$\sum_{b=0}^{1} \mathrm{tr}\left[A_{1,\mathbf{1}} A_{1,\mathbf{0}}^{(b)} \rho^{(\boldsymbol{\theta})} A_{1,\mathbf{0}}^{(b)}\right] \approx_0 \sum_{b=0}^{1} \mathrm{tr}\left[A_{1,\mathbf{1}} A_{1,\mathbf{0}}^{(b)} \rho^{(\boldsymbol{\theta}')} A_{1,\mathbf{0}}^{(b)}\right].$$

Therefore, it suffices to show the lemma for a particular choice of $\boldsymbol{\theta}$, and below we fix $\boldsymbol{\theta} = 000$.

First, from the definition of $\gamma_T(D)$, we obtain

$$\mathrm{tr}\left[\sum_{\boldsymbol{v}} A_{1,\mathbf{0}}^{(v_1)} \sigma^{(0,v_1;0,v_2;0,v_3)}\right] \approx_{\gamma_T(D)} 1,$$

and using Corollary 28 and Lemma 16 leads to

$$A_{1,\mathbf{0}}^{(v_1)} \approx_{\gamma_T(D),\sigma^{(0,v_1;0,v_2;0,v_3)}} I, \tag{39}$$

$$A_{1,\mathbf{0}}^{(\overline{v_1})} \approx_{\gamma_T(D),\sigma^{(0,v_1;0,v_2;0,v_3)}} 0. \tag{40}$$

Since the operator norm of $A_{1,\mathbf{0}}^{(v_1)}$ is constant, Lemma 18 and Eq. (39) lead to

$$A_{1,\mathbf{0}}^{(v_1)} \sigma^{(0,v_1;0,v_2;0,v_3)} A_{1,\mathbf{0}}^{(v_1)} \approx_{\gamma_T(D)} \sigma^{(0,v_1;0,v_2;0,v_3)} A_{1,\mathbf{0}}^{(v_1)}, \tag{41}$$

$$\sigma^{(0,v_1;0,v_2;0,v_3)} A_{1,\mathbf{0}}^{(v_1)} \approx_{\gamma_T(D)} \sigma^{(0,v_1;0,v_2;0,v_3)}. \tag{42}$$

From the triangle inequality of the trace norm, Eqs. (41) and (42) imply

$$A_{1,\mathbf{0}}^{(v_1)} \sigma^{(0,v_1;0,v_2;0,v_3)} A_{1,\mathbf{0}}^{(v_1)} \approx_{\gamma_T(D)} \sigma^{(0,v_1;0,v_2;0,v_3)}. \tag{43}$$

Similarly, using Lemma 18 and Eq. (40) leads to

$$A_{1,\mathbf{0}}^{(\overline{v_1})} \sigma^{(0,v_1;0,v_2;0,v_3)} A_{1,\mathbf{0}}^{(\overline{v_1})} \approx_{\gamma_T(D)} 0. \tag{44}$$

Combining Eqs. (43) and (44) gives

$$\sum_{b=0}^{1} A_{1,\mathbf{0}}^{(b)} \sigma^{(0,v_1;0,v_2;0,v_3)} A_{1,\mathbf{0}}^{(b)} \approx_{\gamma_T(D)} \sigma^{(0,v_1;0,v_2;0,v_3)}.$$

As the operator norm of $A_{1,\mathbf{1}}$ is constant, Lemma 17 (ii) leads to

$$\mathrm{tr}\left[A_{1,\mathbf{1}} \left(\sum_{b=0}^{1} A_{1,\mathbf{0}}^{(b)} \sigma^{(0,v_1;0,v_2;0,v_3)} A_{1,\mathbf{0}}^{(b)}\right)\right] \approx_{\sqrt{\gamma_T(D)}} \mathrm{tr}\left[A_{1,\mathbf{1}} \sigma^{(0,v_1;0,v_2;0,v_3)}\right].$$

By using this and $\rho^{(000)} = \sum_{\boldsymbol{v}} \sigma^{(0,v_1;0,v_2;0,v_3)}$, the LHS of Eq. (38) for $i = 1$ and $\boldsymbol{\theta} = 000$ is calculated as

$$\begin{aligned}\sum_{b=0}^{1} \mathrm{tr}\left[A_{1,\mathbf{1}} A_{1,\mathbf{0}}^{(b)} \sum_{\boldsymbol{v}} \sigma^{(0,v_1;0,v_2;0,v_3)} A_{1,\mathbf{0}}^{(b)}\right] &\approx_{\sqrt{\gamma_T(D)}} \sum_{\boldsymbol{v}} \mathrm{tr}\left[A_{1,\mathbf{1}} \sigma^{(0,v_1;0,v_2;0,v_3)}\right] \\ &= \mathrm{tr}(A_{1,\mathbf{1}} \rho^{(000)}) \\ &\approx_{\gamma_T(D)} 0. \end{aligned} \tag{45}$$

In the last equality, we used Corollary 34, which is proven below. ■

Corollary 34 *Let $D = (S, \Pi, M, P)$ be an efficient perfect device. Then, for any $\boldsymbol{\theta} \in \mathcal{B}$ and $i \in \{1, 2, 3\}$,*

$$\mathrm{tr}(A_{i,\mathbf{1}} \rho^{(\boldsymbol{\theta})}) \approx_{\gamma_T(D)} 0. \tag{46}$$

(Proof) We show Eq. (46) for $i = 1$, and the others are analogous. Using Lemma 21 (i), whose conditions are satisfied due to Lemma 31 and the fact that $A_{1,\mathbf{1}}$ is an efficient binary observable, it suffices to show $\mathrm{tr}(A_{1,\mathbf{1}}\rho^{(100)}) \approx_{\gamma_T(D)} 0$. As $A_{1,\mathbf{1}}$ is a binary observable, $A_{1,\mathbf{1}} = (-1)^{v_1}(2A_{1,\mathbf{1}}^{(v_1)} - I)$ holds for any $v_1 \in \{0,1\}$. Hence,

$$\mathrm{tr}(A_{1,\mathbf{1}}\rho^{(100)}) = \sum_{\boldsymbol{v}} \mathrm{tr}\left[(-1)^{v_1}(2A_{1,\mathbf{1}}^{(v_1)} - I)\sigma^{(1,v_1;0,v_2;0,v_3)}\right].$$

Using this, the definition of $\gamma_T(D)$ in Eq. (12) and Lemma 27 results in

$$\mathrm{tr}(A_{1,\mathbf{1}}\rho^{(100)}) \approx_{\gamma_T(D)} \sum_{\boldsymbol{v}} (-1)^{v_1}\mathrm{tr}\left[\sigma^{(1,v_1;0,v_2;0,v_3)}\right]. \tag{47}$$

Next, in Lemma 35, we will show

$$\sum_{v_2,v_3\in\{0,1\}^2} \mathrm{tr}(\sigma^{(1,0;0,v_2;0,v_3)}) \approx_0 \sum_{v_2,v_3\in\{0,1\}^2} \mathrm{tr}(\sigma^{(1,1;0,v_2;0,v_3)}).$$

By employing this, Eq. (47) leads to

$$\mathrm{tr}(A_{1,\mathbf{1}}\rho^{(100)}) \approx_{\gamma_T(D)} 0.$$

■

Lemma 35 *Let $D = (S, \Pi, M, P)$ be en efficient perfect device. Then*

$$\begin{aligned}
\sum_{v_2,v_3\in\{0,1\}^2} \mathrm{tr}(\sigma^{(1,0;0,v_2;0,v_3)}) &\approx_0 \sum_{v_2,v_3\in\{0,1\}^2} \mathrm{tr}(\sigma^{(1,1;0,v_2;0,v_3)}),\\
\sum_{v_1,v_3\in\{0,1\}^2} \mathrm{tr}(\sigma^{(0,v_1;1,0;0,v_3)}) &\approx_0 \sum_{v_1,v_3\in\{0,1\}^2} \mathrm{tr}(\sigma^{(0,v_1;1,1;0,v_3)}),\\
\sum_{v_1,v_2\in\{0,1\}^2} \mathrm{tr}(\sigma^{(0,v_1;0,v_2;1,0)}) &\approx_0 \sum_{v_1,v_2\in\{0,1\}^2} \mathrm{tr}(\sigma^{(0,v_1;0,v_2;1,1)}).
\end{aligned} \tag{48}$$

(Proof) Here we focus on proving Eq. (48), and the others can be shown analogously. We consider the following efiicient algorithm $\mathcal{A}$ for the adaptive hardcore bit property of $\mathcal{F}$. Given a key $k_1 \in \mathcal{K}_{\mathcal{F}}$, $\mathcal{A}$ samples $(k_2, t_{k_2}) \leftarrow \mathsf{GEN}_{\mathcal{G}}(1^\lambda)$ and $(k_3, t_{k_3}) \leftarrow \mathsf{GEN}_{\mathcal{G}}(1^\lambda)$. $\mathcal{A}$ prepares the state $\psi^{(100)}$ as D does followed by measuring the image registers to obtain $(y_1, y_2, y_3) \in \mathcal{Y}^3$ and then performs the measurement Π to obtain the outcomes $((b_1, b_2, b_3), (x_1, x_2, x_3)) \in \{0,1\}^3 \times \mathcal{X}^3$. $\mathcal{A}$ performs the measurement M to obtain outcomes $(d_1, d_2, d_3) \in \{0,1\}^{3w}$ and outputs the tuple

$$(b_1, x_1, d_1, \hat{b}(k_2, y_2) \cdot \hat{b}(k_3, y_3)),$$

where $b_1 \in \{0,1\}, x_1 \in \mathcal{X}, d_1 \in \{0,1\}^w$ and by the construction of $\mathcal{F}$, there exists $x_1' \in \mathcal{X}$ such that $(x_1, x_1') \in \mathcal{R}_{k_1}$. Note that $\mathcal{A}$ is efficient because D is efficient and $\hat{b}(k_2, y_2)\cdot\hat{b}(k_3, y_3)$ can be efficiently computed by using the trapdoors t_{k_2} and t_{k_3}. As D is a perfect device, $\mathcal{A}$ passes the preimage round with probability $1 - \mathrm{negl}(\lambda)$, and the states before and after the measurement Π are computationally indistinguishable due to the collapsing property of $\mathcal{F}$ (Lemma A.7 in [5]). This implies that $\mathcal{A}$'s distribution over $(y_1, y_2, y_3, d_1, d_2, d_3)$ is computationally indistinguishable from the distribution obtained by D. By the definition of $\sum_{v_2,v_3} \mathrm{tr}(\sigma^{(1,v_1;0,v_2;0,v_3)})$ in Eq. (14), we have the following on average over $k_1 \leftarrow \mathsf{GEN}_{\mathcal{F}}(1^\lambda)$ and $\mathcal{A}$'s distribution over $k_2, k_3, y_1, y_2, y_3, d_1$:

$$\begin{aligned}
\sum_{v_2,v_3} \mathrm{tr}(\sigma^{(1,v_1=0;0,v_2;0,v_3)}) &= \Pr\{\hat{b}(k_2, y_2) \cdot \hat{b}(k_3, y_3) = \hat{u}(k_1, y_1, d_1)\} = \Pr\{\mathcal{A}(k_1) \in H_{k_1}\},\\
\sum_{v_2,v_3} \mathrm{tr}(\sigma^{(1,v_1=1;0,v_2;0,v_3)}) &= \Pr\{\hat{b}(k_2, y_2) \cdot \hat{b}(k_3, y_3) = \hat{u}(k_1, y_1, d_1) \oplus 1\} = \Pr\{\mathcal{A}(k_1) \in \overline{H}_{k_1}\}.
\end{aligned}$$

Hence, we can see that Eq. (48) holds from the above two equations and the adaptive hardcore bit property of $\mathcal{F}$ for identity J. ■

Lemma 36 *Let us define the projectors that project onto the correct preimage answers:*

$$\tilde{\Pi}_{\boldsymbol{y}}^{(\boldsymbol{b})} := \Pi_{\boldsymbol{y}}^{(b_1,\hat{x}_{b_1}(k_1,y_1);b_2,\hat{x}_{b_2}(k_2,y_2);b_3,\hat{x}_{b_3}(k_3,y_3))},$$

where $\tilde{\Pi}_{\boldsymbol{y}}^{(\boldsymbol{b})} := 0$ *if* $\hat{x}_{b_1}(k_1,y_1) = \perp$ *or* $\hat{x}_{b_2}(k_2,y_2) = \perp$ *or* $\hat{x}_{b_3}(k_3,y_3) = \perp$. *We also define the marginals by*

$$\begin{aligned}
\tilde{\Pi}_{1,\boldsymbol{y}}^{(b)} &:= \tilde{\Pi}_{\boldsymbol{y}}^{(b00)} + \tilde{\Pi}_{\boldsymbol{y}}^{(b01)} + \tilde{\Pi}_{\boldsymbol{y}}^{(b10)} + \tilde{\Pi}_{\boldsymbol{y}}^{(b11)},\\
\tilde{\Pi}_{2,\boldsymbol{y}}^{(b)} &:= \tilde{\Pi}_{\boldsymbol{y}}^{(0b0)} + \tilde{\Pi}_{\boldsymbol{y}}^{(0b1)} + \tilde{\Pi}_{\boldsymbol{y}}^{(1b0)} + \tilde{\Pi}_{\boldsymbol{y}}^{(1b1)},\\
\tilde{\Pi}_{3,\boldsymbol{y}}^{(b)} &:= \tilde{\Pi}_{\boldsymbol{y}}^{(00b)} + \tilde{\Pi}_{\boldsymbol{y}}^{(01b)} + \tilde{\Pi}_{\boldsymbol{y}}^{(10b)} + \tilde{\Pi}_{\boldsymbol{y}}^{(11b)}.
\end{aligned}$$

For any efficient perfect device $D = (S, \Pi, M, P)$, *the following holds for any* $\boldsymbol{\theta} \in \mathcal{B}$ *and* $i \in \{1,2,3\}$,

$$\sum_{b=0}^{1}\sum_{\boldsymbol{y},\boldsymbol{d}} \left|\left| M_{\boldsymbol{y}}^{(\boldsymbol{d})}\tilde{\Pi}_{i,\boldsymbol{y}}^{(b)} - A_{i,\mathbf{0},\boldsymbol{y},\boldsymbol{d}}^{(b)} M_{\boldsymbol{y}}^{(\boldsymbol{d})} \right|\right|^2_{\psi_{\boldsymbol{y}}^{(\boldsymbol{\theta})}} \approx_{\gamma_T(D)} 0. \tag{49}$$

Note that since each term in the sum is positive, the statement holds for any sums over any subsets of $b, \boldsymbol{y}, \boldsymbol{d}$.

(Proof) We show the lemma for $i = 1$, and the other cases can be shown analogously. By the definition of state-dependent norm, the LHS of Eq. (49) is equal to

$$\begin{aligned}
&\sum_{b,\boldsymbol{y},\boldsymbol{d}} \mathrm{tr}\left[\left(\tilde{\Pi}_{1,\boldsymbol{y}}^{(b)} M_{\boldsymbol{y}}^{(\boldsymbol{d})} - M_{\boldsymbol{y}}^{(\boldsymbol{d})} A_{1,\mathbf{0},\boldsymbol{y},\boldsymbol{d}}^{(b)}\right)\left(M_{\boldsymbol{y}}^{(\boldsymbol{d})}\tilde{\Pi}_{1,\boldsymbol{y}}^{(b)} - A_{1,\mathbf{0},\boldsymbol{y},\boldsymbol{d}}^{(b)} M_{\boldsymbol{y}}^{(\boldsymbol{d})}\right)\psi_{\boldsymbol{y}}^{(\boldsymbol{\theta})}\right]\\
=&\sum_{b,\boldsymbol{y},\boldsymbol{d}} \mathrm{tr}\left(M_{\boldsymbol{y}}^{(\boldsymbol{d})}\tilde{\Pi}_{1,\boldsymbol{y}}^{(b)}\psi_{\boldsymbol{y}}^{(\boldsymbol{\theta})}\tilde{\Pi}_{1,\boldsymbol{y}}^{(b)} M_{\boldsymbol{y}}^{(\boldsymbol{d})}\right) + \sum_{b,\boldsymbol{y},\boldsymbol{d}} \mathrm{tr}\left(A_{1,\mathbf{0},\boldsymbol{y},\boldsymbol{d}}^{(b)} M_{\boldsymbol{y}}^{(\boldsymbol{d})}\psi_{\boldsymbol{y}}^{(\boldsymbol{\theta})} M_{\boldsymbol{y}}^{(\boldsymbol{d})} A_{1,\mathbf{0},\boldsymbol{y},\boldsymbol{d}}^{(b)}\right)\\
-&\sum_{b,\boldsymbol{y},\boldsymbol{d}} \mathrm{tr}\left[A_{1,\mathbf{0},\boldsymbol{y},\boldsymbol{d}}^{(b)} M_{\boldsymbol{y}}^{(\boldsymbol{d})}(\tilde{\Pi}_{1,\boldsymbol{y}}^{(b)}\psi_{\boldsymbol{y}}^{(\boldsymbol{\theta})} + \psi_{\boldsymbol{y}}^{(\boldsymbol{\theta})}\tilde{\Pi}_{1,\boldsymbol{y}}^{(b)}) M_{\boldsymbol{y}}^{(\boldsymbol{d})}\right].
\end{aligned} \tag{50}$$

By defining

$$\tilde{\Pi}_i^{(b)} := \sum_{\boldsymbol{y}} \tilde{\Pi}_{i,\boldsymbol{y}}^{(b)} \otimes |\boldsymbol{y}\rangle\langle\boldsymbol{y}|,$$

Eq. (50) is equal to

$$\sum_{b,\boldsymbol{d}} \mathrm{tr}\left(M^{(\boldsymbol{d})}\tilde{\Pi}_1^{(b)}\psi^{(\boldsymbol{\theta})}\tilde{\Pi}_1^{(b)} M^{(\boldsymbol{d})}\right) + \sum_{b,\boldsymbol{d}} \mathrm{tr}\left(A_{1,\mathbf{0},\boldsymbol{d}}^{(b)} M^{(\boldsymbol{d})}\psi^{(\boldsymbol{\theta})} M^{(\boldsymbol{d})} A_{1,\mathbf{0},\boldsymbol{d}}^{(b)}\right) - \sum_{b,\boldsymbol{d}} \mathrm{tr}\left[A_{1,\mathbf{0},\boldsymbol{d}}^{(b)} M^{(\boldsymbol{d})}(\tilde{\Pi}_1^{(b)}\psi^{(\boldsymbol{\theta})} + \psi^{(\boldsymbol{\theta})}\tilde{\Pi}_1^{(b)}) M^{(\boldsymbol{d})}\right]. \tag{51}$$

Below, we calculate each term in turn. Regarding the first term, by noting that $\{M^{(\boldsymbol{d})}\}_{\boldsymbol{d}}$ forms a projective measurement and $\tilde{\Pi}_1^{(b)}$ is a projector, the first term equals $\sum_b \mathrm{tr}\left(\tilde{\Pi}_1^{(b)}\psi^{(\boldsymbol{\theta})}\right)$. By the definition of $\tilde{\Pi}_{1,\boldsymbol{y}}^{(b)}$, Eq. (35) and $\gamma_P(D) = \mathrm{negl}(\lambda)$ for a perfect device, we have

$$\sum_b \mathrm{tr}\left(\tilde{\Pi}_1^{(b)}\psi^{(\boldsymbol{\theta})}\right) \approx_0 1. \tag{52}$$

Next, it is easy to find that the second term of Eq. (51) is exactly equal to 1 because $\{M^{(\boldsymbol{d})}\}_{\boldsymbol{d}}$ and $\{A_{1,\mathbf{0},\boldsymbol{d}}^{(b)}\}_{b\in\{0,1\}}$ form projective measurements. Finally, we calculate the third term of Eq. (51):

$$\sum_{b,\boldsymbol{d}} \mathrm{tr}\left[A_{1,\mathbf{0},\boldsymbol{d}}^{(b)} M^{(\boldsymbol{d})}(\tilde{\Pi}_1^{(b)}\psi^{(\boldsymbol{\theta})} + \psi^{(\boldsymbol{\theta})}\tilde{\Pi}_1^{(b)}) M^{(\boldsymbol{d})}\right]. \tag{53}$$

For this, we use the relation

$$\tilde{\Pi}_1^{(0)} + \tilde{\Pi}_1^{(1)} \approx_{0,\psi^{(\boldsymbol{\theta})}} I, \tag{54}$$

which can be proven for a perfect device using Eq. (52) as

$$\mathrm{tr}\left([(\tilde{\Pi}_1^{(0)}+\tilde{\Pi}_1^{(1)})-I]^\dagger[(\tilde{\Pi}_1^{(0)}+\tilde{\Pi}_1^{(1)})-I]\psi^{(\boldsymbol{\theta})}\right)=1-\sum_b \mathrm{tr}\left(\tilde{\Pi}_1^{(b)}\psi^{(\boldsymbol{\theta})}\right)\approx_0 0.$$

By applying Lemma 17 (i) with Eq. (54) and by noting $||\sum_{\boldsymbol{d}} M^{(\boldsymbol{d})}A^{(b)}_{1,\mathbf{0},\boldsymbol{d}}M^{(\boldsymbol{d})}||_\infty \leq 1$, Eq. (53) is calculated as

$$\begin{aligned}
&\sum_{b,\boldsymbol{d}} \mathrm{tr}\left[A^{(b)}_{1,\mathbf{0},\boldsymbol{d}}M^{(\boldsymbol{d})}(\tilde{\Pi}_1^{(b)}\psi^{(\boldsymbol{\theta})}+\psi^{(\boldsymbol{\theta})}\tilde{\Pi}_1^{(b)})M^{(\boldsymbol{d})}\right]\\
\approx_0&\sum_{b,\boldsymbol{d}} \mathrm{tr}\left[A^{(b)}_{1,\mathbf{0},\boldsymbol{d}}M^{(\boldsymbol{d})}\tilde{\Pi}_1^{(b)}\psi^{(\boldsymbol{\theta})}(\tilde{\Pi}_1^{(0)}+\tilde{\Pi}_1^{(1)})M^{(d)}\right]+\sum_{b,\boldsymbol{d}} \mathrm{tr}\left[A^{(b)}_{1,\mathbf{0},\boldsymbol{d}}M^{(\boldsymbol{d})}(\tilde{\Pi}_1^{(0)}+\tilde{\Pi}_1^{(1)})\psi^{(\boldsymbol{\theta})}\tilde{\Pi}_1^{(b)}M^{(d)}\right]\\
=&2\sum_{b,\boldsymbol{d}} \mathrm{tr}\left[A^{(b)}_{1,\mathbf{0},\boldsymbol{d}}M^{(\boldsymbol{d})}\tilde{\Pi}_1^{(b)}\psi^{(\boldsymbol{\theta})}\tilde{\Pi}_1^{(b)}M^{(\boldsymbol{d})}\right]+\sum_{b,\boldsymbol{d}} \mathrm{tr}\left[A^{(b)}_{1,\mathbf{0},\boldsymbol{d}}M^{(\boldsymbol{d})}(\tilde{\Pi}_1^{(0)}\psi^{(\boldsymbol{\theta})}\tilde{\Pi}_1^{(1)}+\tilde{\Pi}_1^{(1)}\psi^{(\boldsymbol{\theta})}\tilde{\Pi}_1^{(0)})M^{(\boldsymbol{d})}\right]\\
=&2\sum_{b,\boldsymbol{d}} \mathrm{tr}\left[A^{(b)}_{1,\mathbf{0},\boldsymbol{d}}M^{(\boldsymbol{d})}(\tilde{\Pi}_1^{(b)}\psi^{(\boldsymbol{\theta})}\tilde{\Pi}_1^{(b)})M^{(\boldsymbol{d})}\right]+\mathrm{tr}\left[\tilde{\Pi}_1^{(1)}\tilde{\Pi}_1^{(0)}\psi^{(\boldsymbol{\theta})}+\tilde{\Pi}_1^{(0)}\tilde{\Pi}_1^{(1)}\psi^{(\boldsymbol{\theta})}\right]\\
=&2\sum_{b,\boldsymbol{d}} \mathrm{tr}\left[A^{(b)}_{1,\mathbf{0},\boldsymbol{d}}M^{(\boldsymbol{d})}(\tilde{\Pi}_1^{(b)}\psi^{(\boldsymbol{\theta})}\tilde{\Pi}_1^{(b)})M^{(\boldsymbol{d})}\right].
\end{aligned}$$

Note that we use $\sum_b A^{(b)}_{1,\mathbf{0},\boldsymbol{d}}=I$ for any $\boldsymbol{d}$ and $\sum_{\boldsymbol{d}} M^{(\boldsymbol{d})}=I$ in the third equality, and $\tilde{\Pi}_1^{(0)}$ and $\tilde{\Pi}_1^{(1)}$ are orthogonal projectors in the final equality. For $\boldsymbol{\theta}=000$, by exploiting Eqs. (13) and (52), we have

$$\sum_{\boldsymbol{d}} M^{(\boldsymbol{d})}\tilde{\Pi}_1^{(b)}\psi^{(000)}\tilde{\Pi}_1^{(b)}M^{(\boldsymbol{d})}\otimes|\boldsymbol{d}\rangle\langle\boldsymbol{d}|\approx_0\sum_{v_2,v_3}\sigma^{(0,b;0,v_2;0,v_3)}.$$

Using Lemma 17 (ii) by noting $||A^{(b)}_{1,\mathbf{0}}||_\infty\leq 1$ and the definition of $\gamma_T(D)$ in Eq. (12), this results in

$$\sum_{b,\boldsymbol{d}} \mathrm{tr}\left[A^{(b)}_{1,\mathbf{0},\boldsymbol{d}}M^{(\boldsymbol{d})}\tilde{\Pi}_1^{(b)}\psi^{(000)}\tilde{\Pi}_1^{(b)}M^{(\boldsymbol{d})}\otimes|\boldsymbol{d}\rangle\langle\boldsymbol{d}|\right]\approx_0\sum_{\boldsymbol{v}}\mathrm{tr}\left[A^{(v_1)}_{1,\mathbf{0}}\sigma^{(0,v_1;0,v_2;0,v_3)}\right]\approx_{\gamma_T(D)}1. \tag{55}$$

To lift up the statement of Eq. (55) to any $\boldsymbol{\theta}\in\mathcal{B}$, we show

$$\sum_{b,\boldsymbol{d}} \mathrm{tr}\left[A^{(b)}_{1,\mathbf{0},\boldsymbol{d}}M^{(\boldsymbol{d})}\tilde{\Pi}_1^{(b)}\psi^{(\boldsymbol{\theta})}\tilde{\Pi}_1^{(b)}M^{(\boldsymbol{d})}\otimes|\boldsymbol{d}\rangle\langle\boldsymbol{d}|\right]\approx_0\sum_{b,\boldsymbol{d}} \mathrm{tr}\left[A^{(b)}_{1,\mathbf{0},\boldsymbol{d}}M^{(\boldsymbol{d})}\Pi_1^{(b)}\psi^{(\boldsymbol{\theta})}\Pi_1^{(b)}M^{(\boldsymbol{d})}\otimes|\boldsymbol{d}\rangle\langle\boldsymbol{d}|\right] \tag{56}$$

with $\Pi_1^{(b)}:=\sum_{x_1,b_2,x_2,b_3,x_3}\Pi^{(b,x_1;b_2,x_2;b_3,x_3)}$ and

$$\sum_{b,\boldsymbol{d}} \mathrm{tr}\left[A^{(b)}_{1,\mathbf{0},\boldsymbol{d}}M^{(\boldsymbol{d})}\Pi_1^{(b)}\psi^{(\boldsymbol{\theta})}\Pi_1^{(b)}M^{(\boldsymbol{d})}\otimes|\boldsymbol{d}\rangle\langle\boldsymbol{d}|\right]\approx_0\sum_{b,\boldsymbol{d}} \mathrm{tr}\left[A^{(b)}_{1,\mathbf{0},\boldsymbol{d}}M^{(\boldsymbol{d})}\Pi_1^{(b)}\psi^{(000)}\Pi_1^{(b)}M^{(\boldsymbol{d})}\otimes|\boldsymbol{d}\rangle\langle\boldsymbol{d}|\right]. \tag{57}$$

Once Eqs. (56) and (57) hold, we obtain for any $\boldsymbol{\theta}\in\mathcal{B}$:

$$\begin{aligned}
\sum_{b,\boldsymbol{d}} \mathrm{tr}\left[A^{(b)}_{1,\mathbf{0},\boldsymbol{d}}M^{(\boldsymbol{d})}\tilde{\Pi}_1^{(b)}\psi^{(\boldsymbol{\theta})}\tilde{\Pi}_1^{(b)}M^{(\boldsymbol{d})}\otimes|\boldsymbol{d}\rangle\langle\boldsymbol{d}|\right]&\approx_0\sum_{b,\boldsymbol{d}} \mathrm{tr}\left[A^{(b)}_{1,\mathbf{0},\boldsymbol{d}}M^{(\boldsymbol{d})}\Pi_1^{(b)}\psi^{(\boldsymbol{\theta})}\Pi_1^{(b)}M^{(\boldsymbol{d})}\otimes|\boldsymbol{d}\rangle\langle\boldsymbol{d}|\right]\quad\text{(from Eq. (56))}\\
&\approx_0\sum_{b,\boldsymbol{d}} \mathrm{tr}\left[A^{(b)}_{1,\mathbf{0},\boldsymbol{d}}M^{(\boldsymbol{d})}\Pi_1^{(b)}\psi^{(000)}\Pi_1^{(b)}M^{(\boldsymbol{d})}\otimes|\boldsymbol{d}\rangle\langle\boldsymbol{d}|\right]\quad\text{(from Eq. (57))}\\
&\approx_0\sum_{b,\boldsymbol{d}} \mathrm{tr}\left[A^{(b)}_{1,\mathbf{0},\boldsymbol{d}}M^{(\boldsymbol{d})}\tilde{\Pi}_1^{(b)}\psi^{(000)}\tilde{\Pi}_1^{(b)}M^{(\boldsymbol{d})}\otimes|\boldsymbol{d}\rangle\langle\boldsymbol{d}|\right]\quad\text{(from Eq. (56))}\\
&\approx_{\gamma_T(D)}1\quad\text{(from Eq. (55)).}
\end{aligned}$$

Eq. (56) follows from applying Lemma 17 (i) by noting $||\sum_{\boldsymbol{d}} M^{(\boldsymbol{d})}A^{(b)}_{1,\mathbf{0},\boldsymbol{d}}M^{(\boldsymbol{d})}||_\infty\leq 1$ and $\tilde{\Pi}_1^{(b)}\approx_{0,\psi^{(\boldsymbol{\theta})}}\Pi_1^{(b)}$ that holds for a perfect prover. Eq. (57) follows from applying Lemma 21 (i) by setting $A:=\sum_{b,\boldsymbol{d}}\Pi_1^{(b)}M^{(\boldsymbol{d})}A^{(b)}_{1,\mathbf{0},\boldsymbol{d}}M^{(\boldsymbol{d})}\Pi_1^{(b)}$ and by noting $\psi^{(\boldsymbol{\theta})}\overset{c}{\approx}_0\psi^{(\boldsymbol{\theta}')}$. Combining the above statements results in Eq. (49). ■

Lemma 37 *For any efficient perfect device $D = (S, \Pi, M, P)$, the following holds for any $b_1 \in \{0,1\}$ and $\boldsymbol{b}_{\bar{1}} := b_2 b_3, \boldsymbol{b}'_{\bar{1}} := b'_2 b'_3$ with $\mathrm{wt}(\boldsymbol{b}_{\bar{1}}, \boldsymbol{b}'_{\bar{1}}) \geq 1$:*

$$\left(\sum_{\boldsymbol{y}} \tilde{\Pi}_{\boldsymbol{y}}^{(b_1 b_2 b_3)} \otimes |\boldsymbol{y}\rangle\langle\boldsymbol{y}|\right) \psi^{(100)} \left(\sum_{\boldsymbol{y}} \tilde{\Pi}_{\boldsymbol{y}}^{(b_1 b'_2 b'_3)} \otimes |\boldsymbol{y}\rangle\langle\boldsymbol{y}|\right) \approx_0 0, \tag{58}$$

for any $b_2 \in \{0,1\}$ and $\boldsymbol{b}_{\bar{2}} := b_1 b_3, \boldsymbol{b}'_{\bar{2}} := b'_1 b'_3$ with $\mathrm{wt}(\boldsymbol{b}_{\bar{2}}, \boldsymbol{b}'_{\bar{2}}) \geq 1$:

$$\left(\sum_{\boldsymbol{y}} \tilde{\Pi}_{\boldsymbol{y}}^{(b_1 b_2 b_3)} \otimes |\boldsymbol{y}\rangle\langle\boldsymbol{y}|\right) \psi^{(010)} \left(\sum_{\boldsymbol{y}} \tilde{\Pi}_{\boldsymbol{y}}^{(b'_1 b_2 b'_3)} \otimes |\boldsymbol{y}\rangle\langle\boldsymbol{y}|\right) \approx_0 0,$$

and for any $b_3 \in \{0,1\}$ and $\boldsymbol{b}_{\bar{3}} := b_1 b_2, \boldsymbol{b}'_{\bar{3}} := b'_1 b'_2$ with $\mathrm{wt}(\boldsymbol{b}_{\bar{3}}, \boldsymbol{b}'_{\bar{3}}) \geq 1$:

$$\left(\sum_{\boldsymbol{y}} \tilde{\Pi}_{\boldsymbol{y}}^{(b_1 b_2 b_3)} \otimes |\boldsymbol{y}\rangle\langle\boldsymbol{y}|\right) \psi^{(001)} \left(\sum_{\boldsymbol{y}} \tilde{\Pi}_{\boldsymbol{y}}^{(b'_1 b'_2 b_3)} \otimes |\boldsymbol{y}\rangle\langle\boldsymbol{y}|\right) \approx_0 0.$$

(Proof) We provide the proof for Eq. (58). The other cases can be shown analogously. We suppose that $\boldsymbol{b}_{\bar{1}}$ and $\boldsymbol{b}'_{\bar{1}}$ differ in bit b_j of $j \in \{2,3\}$. We first prove

$$\sum_{\boldsymbol{y}} \tilde{\Pi}_{\boldsymbol{y}}^{(b_1 b_2 b_3)} \otimes |\boldsymbol{y}\rangle\langle\boldsymbol{y}| \approx_{0,\psi^{(100)}} \sum_{\boldsymbol{y}_{\bar{j}}, y_j \in \mathcal{Y}_{b_j}} \tilde{\Pi}_{\boldsymbol{y}}^{(b_1 b_2 b_3)} \otimes |\boldsymbol{y}\rangle\langle\boldsymbol{y}| \tag{59}$$

with $\mathcal{Y}_{b_j} := \{y_j \in \mathcal{Y} | \hat{b}(k_j, y_j) = b_j\}$. From the definition of the state-dependent norm, we need to show

$$\mathrm{tr}\left[\left(\sum_{\boldsymbol{y}} \tilde{\Pi}_{\boldsymbol{y}}^{(b_1 b_2 b_3)} \otimes |\boldsymbol{y}\rangle\langle\boldsymbol{y}| - \sum_{\boldsymbol{y}_{\bar{j}}, y_j \in \mathcal{Y}_{b_j}} \tilde{\Pi}_{\boldsymbol{y}}^{(b_1 b_2 b_3)} \otimes |\boldsymbol{y}\rangle\langle\boldsymbol{y}|\right)^2 \psi^{(100)}\right] \approx_0 0.$$

This can be proven by calculating the LHS as

$$\mathrm{tr}\left[\sum_{\boldsymbol{y}_{\bar{j}}, y_j \in \mathcal{Y} \setminus \mathcal{Y}_{b_j}} \tilde{\Pi}_{\boldsymbol{y}}^{(b_1 b_2 b_3)} \psi_{\boldsymbol{y}}^{(100)}\right],$$

and from Eq. (8) and the definition of $\mathcal{Y}_{b_j}$, this term is negligibly close to zero for a perfect device.

From Lemma 18 and Eq. (59), we have two approximate relations:

$$\left(\sum_{\boldsymbol{y}} \tilde{\Pi}_{\boldsymbol{y}}^{(b_1 \boldsymbol{b}_{\bar{1}})} \otimes |\boldsymbol{y}\rangle\langle\boldsymbol{y}|\right) \psi^{(100)} \left(\sum_{\boldsymbol{y}} \tilde{\Pi}_{\boldsymbol{y}}^{(b_1 \boldsymbol{b}'_{\bar{1}})} \otimes |\boldsymbol{y}\rangle\langle\boldsymbol{y}|\right) \approx_0 \left(\sum_{\boldsymbol{y}_{\bar{j}}, y_j \in \mathcal{Y}_{b_j}} \tilde{\Pi}_{\boldsymbol{y}}^{(b_1 \boldsymbol{b}_{\bar{1}})} \otimes |\boldsymbol{y}\rangle\langle\boldsymbol{y}|\right) \psi^{(100)} \left(\sum_{\boldsymbol{y}} \tilde{\Pi}_{\boldsymbol{y}}^{(b_1 \boldsymbol{b}'_{\bar{1}})} \otimes |\boldsymbol{y}\rangle\langle\boldsymbol{y}|\right), \tag{60}$$

and

$$\left(\sum_{\boldsymbol{y}_{\bar{j}}, y_j \in \mathcal{Y}_{b_j}} \tilde{\Pi}_{\boldsymbol{y}}^{(b_1 \boldsymbol{b}_{\bar{1}})} \otimes |\boldsymbol{y}\rangle\langle\boldsymbol{y}|\right) \psi^{(100)} \left(\sum_{\boldsymbol{y}} \tilde{\Pi}_{\boldsymbol{y}}^{(b_1 \boldsymbol{b}'_{\bar{1}})} \otimes |\boldsymbol{y}\rangle\langle\boldsymbol{y}|\right) \approx_0 \left(\sum_{\boldsymbol{y}_{\bar{j}}, y_j \in \mathcal{Y}_{b_j}} \tilde{\Pi}_{\boldsymbol{y}}^{(b_1 \boldsymbol{b}_{\bar{1}})} \otimes |\boldsymbol{y}\rangle\langle\boldsymbol{y}|\right) \psi^{(100)} \left(\sum_{\boldsymbol{y}_{\bar{j}}, y_j \in \mathcal{Y}_{\overline{b_j}}} \tilde{\Pi}_{\boldsymbol{y}}^{(b_1 \boldsymbol{b}'_{\bar{1}})} \otimes |\boldsymbol{y}\rangle\langle\boldsymbol{y}|\right). \tag{61}$$

Using the triangle inequality of the trace norm, the LHS of Eq. (60) and the RHS of Eq. (61) are approximately equal, and the RHS of Eq. (61) equals 0 because $\mathcal{Y}_{b_j}$ and $\mathcal{Y}_{\overline{b_j}}$ are disjoint. Therefore, the LHS of Eq. (60) is approximately equal to 0, which ends the proof. ■

Lemma 38 *For any efficient perfect device $D = (S, \Pi, M, P)$, the following holds for any $v_1 \in \{0,1\}$,*

$$\sum_{b=0}^{1} \sum_{v_2,v_3} \mathrm{tr}\left[A_{1,\mathbf{1}} A_{1,\mathbf{0}}^{(b)} \sigma^{(1,v_1;0,v_2;0.v_3)} A_{1,\mathbf{0}}^{(b)}\right] \approx_{\sqrt{\gamma_T(D)}} 0, \tag{62}$$

for any $v_2 \in \{0,1\}$,

$$\sum_{b=0}^{1} \sum_{v_1,v_3} \mathrm{tr}\left[A_{2,\mathbf{1}} A_{2,\mathbf{0}}^{(b)} \sigma^{(0,v_1;1,v_2;0.v_3)} A_{2,\mathbf{0}}^{(b)}\right] \approx_{\sqrt{\gamma_T(D)}} 0,$$

and for any $v_3 \in \{0,1\}$,

$$\sum_{b=0}^{1} \sum_{v_1,v_2} \mathrm{tr}\left[A_{3,\mathbf{1}} A_{3,\mathbf{0}}^{(b)} \sigma^{(0,v_1;0,v_2;1.v_3)} A_{3,\mathbf{0}}^{(b)}\right] \approx_{\sqrt{\gamma_T(D)}} 0.$$

(Proof) We provide the proof of Eq. (62), and the others can be shown analogously. Let the LHS of Eq. (62) be $\chi^{(v_1)} \in \mathbb{C}$. Since Lemma 33 claims

$$\chi^{(0)} + \chi^{(1)} \approx_{\sqrt{\gamma_T(D)}} 0,$$

if we derive

$$\chi^{(0)} \approx_{\sqrt{\gamma_T(D)}} \chi^{(1)}, \tag{63}$$

we obtain the required relation $\chi^{(v_1)} \approx_{\sqrt{\gamma_T(D)}} 0$. Hence, the remaining task is to prove Eq. (63). First, substituting the definition of $\sigma^{(1,v_1;0,v_2;0.v_3)}$ given in Eq. (14), we have

$$\chi^{(v_1)} = \sum_{b=0}^{1} \sum_{\boldsymbol{y},\boldsymbol{d}:\hat{u}(k_1,y_1,d_1)=v_1\oplus\hat{b}(k_2,y_2)\cdot\hat{b}(k_3,y_3)} \mathrm{tr}\left[A_{1,\mathbf{1},\boldsymbol{y},\boldsymbol{d}} A_{1,\mathbf{0},\boldsymbol{y},\boldsymbol{d}}^{(b)} M_{\boldsymbol{y}}^{(\boldsymbol{d})} \psi_{\boldsymbol{y}}^{(100)} M_{\boldsymbol{y}}^{(\boldsymbol{d})} A_{1,\mathbf{0},\boldsymbol{y},\boldsymbol{d}}^{(b)}\right]. \tag{64}$$

One can replace the terms of the form $P := A_{1,\mathbf{0},\boldsymbol{y},\boldsymbol{d}}^{(b)} M_{\boldsymbol{y}}^{(\boldsymbol{d})}$ in $\chi^{(v_1)}$ by terms of the form $R := M_{\boldsymbol{y}}^{(\boldsymbol{d})} \tilde{\Pi}_{1,\boldsymbol{y}}^{(b)}$ as

$$\chi^{(v_1)} \approx_{\sqrt{\gamma_T(D)}} \sum_{b=0}^{1} \sum_{\boldsymbol{y},\boldsymbol{d}:\hat{u}(k_1,y_1,d_1)=v_1\oplus\hat{b}(k_2,y_2)\cdot\hat{b}(k_3,y_3)} \mathrm{tr}\left[A_{1,\mathbf{1},\boldsymbol{y},\boldsymbol{d}} R \psi_{\boldsymbol{y}}^{(100)} R^\dagger\right] =: \xi^{(v_1)}, \tag{65}$$

which is proven as follows.

$$\begin{aligned}
|\chi^{(v_1)} - \xi^{(v_1)}| &\leq \sum_{b=0}^{1} \sum_{\boldsymbol{y},\boldsymbol{d}:\hat{u}(k_1,y_1,d_1)=v_1\oplus\hat{b}(k_2,y_2)\cdot\hat{b}(k_3,y_3)} \left(\left|\mathrm{tr}\left[P^\dagger A_{1,\mathbf{1},\boldsymbol{y},\boldsymbol{d}}(P-R)\psi_{\boldsymbol{y}}^{(100)}\right]\right| + \left|\mathrm{tr}\left[(P^\dagger - R^\dagger) A_{1,\mathbf{1},\boldsymbol{y},\boldsymbol{d}} R \psi_{\boldsymbol{y}}^{(100)}\right]\right|\right) \\
&\leq \sum_{b=0}^{1} \sum_{\boldsymbol{y},\boldsymbol{d}} \left(\left|\langle A_{1,\mathbf{1},\boldsymbol{y},\boldsymbol{d}} P, P-R\rangle_{\psi_{\boldsymbol{y}}^{(100)}}\right| + \left|\langle P-R, A_{1,\mathbf{1},\boldsymbol{y},\boldsymbol{d}} R\rangle_{\psi_{\boldsymbol{y}}^{(100)}}\right|\right) \\
&\leq \sum_{b=0}^{1} \sum_{\boldsymbol{y},\boldsymbol{d}} \left(||A_{1,\mathbf{1},\boldsymbol{y},\boldsymbol{d}} P||_{\psi_{\boldsymbol{y}}^{(100)}} ||P-R||_{\psi_{\boldsymbol{y}}^{(100)}} + ||A_{1,\mathbf{1},\boldsymbol{y},\boldsymbol{d}} R||_{\psi_{\boldsymbol{y}}^{(100)}} ||P-R||_{\psi_{\boldsymbol{y}}^{(100)}}\right) \\
&\leq \sqrt{\sum_{b=0}^{1} \sum_{\boldsymbol{y},\boldsymbol{d}} ||P-R||_{\psi_{\boldsymbol{y}}^{(100)}}^2} \left[\sqrt{\sum_{b=0}^{1} \sum_{\boldsymbol{y},\boldsymbol{d}} ||A_{1,\mathbf{1},\boldsymbol{y},\boldsymbol{d}} P||_{\psi_{\boldsymbol{y}}^{(100)}}^2} + \sqrt{\sum_{b=0}^{1} \sum_{\boldsymbol{y},\boldsymbol{d}} ||A_{1,\mathbf{1},\boldsymbol{y},\boldsymbol{d}} R||_{\psi_{\boldsymbol{y}}^{(100)}}^2}\right].
\end{aligned}$$

The first inequality follows from the triangle inequality, the second one comes from Definition 7 and expanding the range of the sum, and the third and the fourth ones are due to the Cauchy-Schwarz inequality. Finally, by applying Lemma 36, $\sum_{b=0}^{1} \sum_{\boldsymbol{y},\boldsymbol{d}} ||A_{1,\mathbf{1},\boldsymbol{y},\boldsymbol{d}} P||_{\psi_{\boldsymbol{y}}^{(100)}}^2 = 1$ from a direct calculation and $\sum_{b=0}^{1} \sum_{\boldsymbol{y},\boldsymbol{d}} ||A_{1,\mathbf{1},\boldsymbol{y},\boldsymbol{d}} R||_{\psi_{\boldsymbol{y}}^{(100)}}^2 \approx_0 1$ from Eq. (52), we obtain Eq. (65).

By substituting the definition $\tilde{\Pi}^{(b)}_{1,\boldsymbol{y}} = \tilde{\Pi}^{(b00)}_{\boldsymbol{y}} + \tilde{\Pi}^{(b01)}_{\boldsymbol{y}} + \tilde{\Pi}^{(b10)}_{\boldsymbol{y}} + \tilde{\Pi}^{(b11)}_{\boldsymbol{y}}$ to the definition of $\xi^{(v_1)}$ in Eq. (65), we obtain

$$\xi^{(v_1)} = \sum_{\boldsymbol{y},\boldsymbol{d}:\hat{u}(k_1,y_1,d_1)=v_1\oplus\hat{b}(k_2,y_2)\cdot\hat{b}(k_3,y_3)} \mathrm{tr}\Big[\left(M^{(\boldsymbol{d})}_{\boldsymbol{y}} A_{1,\mathbf{1},\boldsymbol{y},\boldsymbol{d}} M^{(\boldsymbol{d})}_{\boldsymbol{y}} \otimes |\boldsymbol{y}\rangle\langle\boldsymbol{y}|\right) \left(\sum_i \left\{ \sum_{j,k}\sum_{\boldsymbol{y}} \tilde{\Pi}^{(ijk)}_{\boldsymbol{y}} \otimes |\boldsymbol{y}\rangle\langle\boldsymbol{y}| \right\} \psi^{(100)} \left\{ \sum_{j,k}\sum_{\boldsymbol{y}} \tilde{\Pi}^{(ijk)}_{\boldsymbol{y}} \otimes |\boldsymbol{y}\rangle\langle\boldsymbol{y}| \right\} \right) \Big]. \tag{66}$$

The off-diagonal terms of $\xi^{(v_1)}$ are written as

$$\sum_{\boldsymbol{y},\boldsymbol{d}:\hat{u}(k_1,y_1,d_1)=v_1\oplus\hat{b}(k_2,y_2)\cdot\hat{b}(k_3,y_3)} \mathrm{tr}\left[\left(M^{(\boldsymbol{d})}_{\boldsymbol{y}} A_{1,\mathbf{1},\boldsymbol{y},\boldsymbol{d}} M^{(\boldsymbol{d})}_{\boldsymbol{y}} \otimes |\boldsymbol{y}\rangle\langle\boldsymbol{y}|\right) L\right], \tag{67}$$

$$L := \sum_{b,\boldsymbol{b}_{\bar{1}},\boldsymbol{b}'_{\bar{1}}:\mathrm{wt}(\boldsymbol{b}_{\bar{1}},\boldsymbol{b}'_{\bar{1}})\geq 1} \left\{ \sum_{\boldsymbol{y}} \tilde{\Pi}^{(b\boldsymbol{b}_{\bar{1}})}_{\boldsymbol{y}} \otimes |\boldsymbol{y}\rangle\langle\boldsymbol{y}| \right\} \psi^{(100)} \left\{ \sum_{\boldsymbol{y}} \tilde{\Pi}^{(b\boldsymbol{b}'_{\bar{1}})}_{\boldsymbol{y}} \otimes |\boldsymbol{y}\rangle\langle\boldsymbol{y}| \right\},$$

where L is an Hermitian and hence it is decomposed with real eigenvalues a_i as $L = \sum_i a_i |i\rangle\langle i|$. By applying Lemma 37 for all b_1, $\boldsymbol{b}_{\bar{1}}$ and $\boldsymbol{b}'_{\bar{1}}$ with $\mathrm{wt}(\boldsymbol{b}_{\bar{1}}, \boldsymbol{b}'_{\bar{1}}) \geq 1$, we have

$$||L||_1 = \mathrm{negl}(\lambda). \tag{68}$$

Substituting the decomposition of L and $A_{1,\mathbf{1},\boldsymbol{y},\boldsymbol{d}} = 2A^{(0)}_{1,\mathbf{1},\boldsymbol{y},\boldsymbol{d}} - I$ to Eq. (67), Eq. (67) is equal to

$$\sum_{\boldsymbol{y},\boldsymbol{d}:\hat{u}(k_1,y_1,d_1)=v_1\oplus\hat{b}(k_2,y_2)\cdot\hat{b}(k_3,y_3),i} a_i \left(2\left\langle i|M^{(\boldsymbol{d})}_{\boldsymbol{y}} A^{(0)}_{1,\mathbf{1},\boldsymbol{y},\boldsymbol{d}} M^{(\boldsymbol{d})}_{\boldsymbol{y}} \otimes |\boldsymbol{y}\rangle\langle\boldsymbol{y}|i\right\rangle - \left\langle i|M^{(\boldsymbol{d})}_{\boldsymbol{y}} \otimes |\boldsymbol{y}\rangle\langle\boldsymbol{y}|i\right\rangle \right). \tag{69}$$

By using $A^{(0)}_{1,\mathbf{1},\boldsymbol{y},\boldsymbol{d}} \leq I$ and $\sum_{\boldsymbol{d}} M^{(\boldsymbol{d})} = I$, it is straightforward to show that the first and the second terms are respectively upper-bounded by $2\sum_i |a_i| = 2||L||_1$ and $\sum_i |a_i| = ||L||_1$, which are both $\mathrm{negl}(\lambda)$ from Eq. (68). Hence, only the diagonal terms of $\xi^{(v_1)}$ remains as non-zero:

$$\xi^{(v_1)} \approx_0 \sum_{\boldsymbol{b},\boldsymbol{y},\boldsymbol{d}:\hat{u}(k_1,y_1,d_1)=v_1\oplus\hat{b}(k_2,y_2)\cdot\hat{b}(k_3,y_3)} \mathrm{tr}\left[A_{1,\mathbf{1},\boldsymbol{y},\boldsymbol{d}} M^{(\boldsymbol{d})}_{\boldsymbol{y}} \tilde{\Pi}^{(\boldsymbol{b})}_{\boldsymbol{y}} \psi^{(100)}_{\boldsymbol{y}} \tilde{\Pi}^{(\boldsymbol{b})}_{\boldsymbol{y}} M^{(\boldsymbol{d})}_{\boldsymbol{y}} \right].$$

It now suffices to show $\xi^{(0)} \approx_0 \xi^{(1)}$, whose proof is similar to the one in Lemma 35. For this, we first prove the relation for the one where $\tilde{\Pi}^{(\boldsymbol{b})}_{\boldsymbol{y}}$ is replaced with $\Pi^{(\boldsymbol{b})}_{\boldsymbol{y}}$, that is

$$\xi'^{(0)} \approx_0 \xi'^{(1)}, \tag{70}$$

$$\xi'^{(v_1)} := \sum_{\boldsymbol{b},\boldsymbol{y},\boldsymbol{d}:\hat{u}(k_1,y_1,d_1)=v_1\oplus\hat{b}(k_2,y_2)\cdot\hat{b}(k_3,y_3)} \mathrm{tr}\left[A_{1,\mathbf{1},\boldsymbol{y},\boldsymbol{d}} M^{(\boldsymbol{d})}_{\boldsymbol{y}} \Pi^{(\boldsymbol{b})}_{\boldsymbol{y}} \psi^{(100)}_{\boldsymbol{y}} \Pi^{(\boldsymbol{b})}_{\boldsymbol{y}} M^{(\boldsymbol{d})}_{\boldsymbol{y}} \right]$$

with

$$\Pi^{(\boldsymbol{b})}_{\boldsymbol{y}} := \sum_{\boldsymbol{x}} \Pi^{(b_1,x_1;b_2;x_2;b_3,x_3)}_{\boldsymbol{y}}.$$

After proving Eq. (70), we show

$$\xi'^{(v_1)} \approx_0 \xi^{(v_1)}, \tag{71}$$

and combining Eqs. (70) and (71) results in $\xi^{(0)} \approx_0 \xi^{(1)}$.

We first prove

$$|\xi'^{(0)} - \xi'^{(1)}| = \mathrm{negl}(\lambda). \tag{72}$$

Its LHS is computed as follows. Using the fact that $A_{1,\mathbf{1},\boldsymbol{y},\boldsymbol{d}}$ is a binary observable leads to

$$A_{1,\mathbf{1},\boldsymbol{y},\boldsymbol{d}} = (-1)^{v_1}(2A^{(v_1)}_{1,\mathbf{1},\boldsymbol{y},\boldsymbol{d}} - I),$$

and substituting this to the LHS gives

$$\begin{aligned}
&|\xi'^{(0)} - \xi'^{(1)}| \\
&= \Bigg| - \sum_{\boldsymbol{b},\boldsymbol{y},\boldsymbol{d}} \mathrm{tr}\left[M_{\boldsymbol{y}}^{(\boldsymbol{d})}\Pi_{\boldsymbol{y}}^{(\boldsymbol{b})}\psi_{\boldsymbol{y}}^{(100)}\Pi_{\boldsymbol{y}}^{(\boldsymbol{b})}M_{\boldsymbol{y}}^{(\boldsymbol{d})}\right] + 2 \sum_{\boldsymbol{b},\boldsymbol{y},\boldsymbol{d}:\hat{u}(k_1,y_1,d_1)=\hat{b}(k_2,y_2)\cdot\hat{b}(k_3,y_3)} \mathrm{tr}\left[A_{1,\mathbf{1},\boldsymbol{y},\boldsymbol{d}}^{(0)}M_{\boldsymbol{y}}^{(\boldsymbol{d})}\Pi_{\boldsymbol{y}}^{(\boldsymbol{b})}\psi_{\boldsymbol{y}}^{(100)}\Pi_{\boldsymbol{y}}^{(\boldsymbol{b})}M_{\boldsymbol{y}}^{(\boldsymbol{d})}\right] \\
&\quad + 2 \sum_{\boldsymbol{b},\boldsymbol{y},\boldsymbol{d}:\hat{u}(k_1,y_1,d_1)=1\oplus\hat{b}(k_2,y_2)\cdot\hat{b}(k_3,y_3)} \mathrm{tr}\left[A_{1,\mathbf{1},\boldsymbol{y},\boldsymbol{d}}^{(1)}M_{\boldsymbol{y}}^{(\boldsymbol{d})}\Pi_{\boldsymbol{y}}^{(\boldsymbol{b})}\psi_{\boldsymbol{y}}^{(100)}\Pi_{\boldsymbol{y}}^{(\boldsymbol{b})}M_{\boldsymbol{y}}^{(\boldsymbol{d})}\right]\Bigg|.
\end{aligned}$$

The first term equals to -1 because $\sum_{\boldsymbol{d}} M_{\boldsymbol{y}}^{(\boldsymbol{d})} = I$ and $\sum_{\boldsymbol{b}} \Pi_{\boldsymbol{y}}^{(\boldsymbol{b})} = I$ hold for any $\boldsymbol{y}$ and $\sum_{\boldsymbol{y}} \mathrm{tr}[\psi_{\boldsymbol{y}}^{(100)}] = 1$. The second and the third terms are twice the probabilities of obtaining $v_1 = u = 0$ and $v_1 = u = 1$, respectively, where u denotes the outcome of the measurement $A_{1,\mathbf{1},\boldsymbol{y},\boldsymbol{d}}$. Combining these, we have $|\xi'^{(0)} - \xi'^{(1)}| = |2\mathrm{Pr}[v_1 = u] - 1|$. For the sake of contradiction, we assume

$$|\xi'^{(0)} - \xi'^{(1)}| = |2\mathrm{Pr}[v_1 = u] - 1| \geq \mu(\lambda) \tag{73}$$

with $\mu(\lambda)$ denoting a non-negligible function, and under this assumption, we can construct an efficient adversary $\mathcal{A}$ that breaks the adaptive hardcore bit property. The construction of $\mathcal{A}$ is as follows. $\mathcal{A}$ takes the first key $k \in \mathcal{K}_{\mathcal{F}}$ and samples the other keys and trapdoors as $(k_2, t_{k_2}) \leftarrow \mathsf{GEN}_{\mathcal{G}}(1^\lambda)$ and $(k_3, t_{k_3}) \leftarrow \mathsf{GEN}_{\mathcal{G}}(1^\lambda)$. Then, $\mathcal{A}$ prepares the state $\psi^{(100)}$ as the device D does, followed by measuring the image registers to obtain $\boldsymbol{y}$. After that $\mathcal{A}$ performs the measurement $\{\Pi^{(b_1,x_1;b_2,x_2;b_3,x_3)}\}_{\boldsymbol{b},\boldsymbol{x}}$, obtaining $(\boldsymbol{b}, \boldsymbol{x})$. Next, $\mathcal{A}$ performs measurement M and obtains the outcomes $\boldsymbol{d}$. Finally, $\mathcal{A}$ performs measurement $A_{1,\mathbf{1}}$ and gets the outcome u. Then, $\mathcal{A}$ outputs the tuple

$$(b_1, x_1, d_1, u \oplus \hat{b}(k_2, y_2) \cdot \hat{b}(k_3, y_3)). \tag{74}$$

Note that since $\mathcal{A}$ knows the trapdoors t_{k_2} and t_{k_3}, $\mathcal{A}$ can efficiently compute $\hat{b}(k_2, y_2) \cdot \hat{b}(k_3, y_3)$. Just after the measurement M, the state of $\mathcal{A}$ is either $\eta^{(0)}$ or $\eta^{(1)}$, where

$$\eta^{(v_1)} := \sum_{\boldsymbol{b},\boldsymbol{y},\boldsymbol{d}:\hat{u}(k_1,y_1,d_1)=v_1\oplus\hat{b}(k_2,y_2)\cdot\hat{b}(k_3,y_3)} M_{\boldsymbol{y}}^{(\boldsymbol{d})}\Pi_{\boldsymbol{y}}^{(\boldsymbol{b})}\psi_{\boldsymbol{y}}^{(100)}\Pi_{\boldsymbol{y}}^{(\boldsymbol{b})}M_{\boldsymbol{y}}^{(\boldsymbol{d})}. \tag{75}$$

In proving that $\mathcal{A}$ breaks the adaptive hardcore bit property, it suffices to show that the deviation of the probabilities where the outcome $u \oplus \hat{b}(k_2, y_2) \cdot \hat{b}(k_3, y_3)$ in Eq. (74) being $\hat{u}(k_1, y_1, d_1)$ and $\hat{u}(k_1, y_1, d_1) \oplus 1$ is non-negligible. Mathematically, we need to show

$$\left|\mathrm{Pr}\left[u \oplus \hat{b}(k_2, y_2) \cdot \hat{b}(k_3, y_3) = \hat{u}(k_1, y_1, d_1)\right] - \mathrm{Pr}\left[u \oplus \hat{b}(k_2, y_2) \cdot \hat{b}(k_3, y_3) = \hat{u}(k_1, y_1, d_1) \oplus 1\right]\right| \geq \mu(\lambda). \tag{76}$$

This is easily obtained as

$$\begin{aligned}
[\text{LHS of Eq. (76)}] = |2\mathrm{Pr}[u \oplus \hat{b}(k_2, y_2) \cdot \hat{b}(k_3, y_3) = \hat{u}(k_1, y_1, d_1)] - 1]| &= |2\mathrm{Pr}[v_1 = u] - 1| \\
&= |\xi'^{(0)} - \xi'^{(1)}| \geq \mu(\lambda),
\end{aligned}$$

where the first line follows from $\hat{u}(k_1, y_1, d_1) = v_1 \oplus \hat{b}(k_2, y_2) \cdot \hat{b}(k_3, y_3)$ by Eq. (75), and the second one comes from Eq. (73). This contradicts the adaptive hardcore bit property, and hence we obtain the negation of Eq. (73), that is,

$$|\xi'^{(0)} - \xi'^{(1)}| = \mathrm{negl}(\lambda). \tag{77}$$

Once we have this equation, the remaining task is to prove Eq. (71), which is proven below.

The proof of Eq. (71) reduces to showing the following for any $a \in \{0, 1\}$ and $\boldsymbol{b} \in \{0, 1\}^3$,

$$\begin{aligned}
&\sum_{\boldsymbol{y},\boldsymbol{d}:\hat{u}(k_1,y_1,d_1)=v_1\oplus\hat{b}(k_2,y_2)\cdot\hat{b}(k_3,y_3)} \mathrm{tr}\left[A_{1,\mathbf{1},\boldsymbol{y},\boldsymbol{d}}^{(a)}M_{\boldsymbol{y}}^{(\boldsymbol{d})}\tilde{\Pi}_{\boldsymbol{y}}^{(\boldsymbol{b})}\psi_{\boldsymbol{y}}^{(100)}\tilde{\Pi}_{\boldsymbol{y}}^{(\boldsymbol{b})}M_{\boldsymbol{y}}^{(\boldsymbol{d})}\right] \\
\approx_0 &\sum_{\boldsymbol{y},\boldsymbol{d}:\hat{u}(k_1,y_1,d_1)=v_1\oplus\hat{b}(k_2,y_2)\cdot\hat{b}(k_3,y_3)} \mathrm{tr}\left[A_{1,\mathbf{1},\boldsymbol{y},\boldsymbol{d}}^{(a)}M_{\boldsymbol{y}}^{(\boldsymbol{d})}\Pi_{\boldsymbol{y}}^{(\boldsymbol{b})}\psi_{\boldsymbol{y}}^{(100)}\Pi_{\boldsymbol{y}}^{(\boldsymbol{b})}M_{\boldsymbol{y}}^{(\boldsymbol{d})}\right].
\end{aligned} \tag{78}$$

By defining an Hermitian operator

$$D := \sum_{\boldsymbol{y},\boldsymbol{d}:\hat{u}(k_1,y_1,d_1)=v_1\oplus\hat{b}(k_2,y_2)\cdot\hat{b}(k_3,y_3)} M^{(\boldsymbol{d})}(I\otimes|\boldsymbol{y}\rangle\langle\boldsymbol{y}|)A^{(a)}_{1,\mathbf{1},\boldsymbol{d}}M^{(\boldsymbol{d})},$$

and

$$\tilde{\Pi}^{(\boldsymbol{b})} := \sum_{\boldsymbol{y}} \Pi_{\boldsymbol{y}}^{(b_1,\hat{x}_{b_1}(k_1,y_1);b_2,\hat{x}_{b_2}(k_2,y_2);b_3,\hat{x}_{b_3}(k_3,y_3))}\otimes|\boldsymbol{y}\rangle\langle\boldsymbol{y}|, \tag{79}$$

$$\Pi^{(\boldsymbol{b})} := \sum_{\boldsymbol{x},\boldsymbol{y}} \Pi_{\boldsymbol{y}}^{(b_1,x_1;b_2;x_2;b_3,x_3)}\otimes|\boldsymbol{y}\rangle\langle\boldsymbol{y}|, \tag{80}$$

the LHS and the RHS of Eq. (78) are respectively equal to

$$\mathrm{tr}[\tilde{\Pi}^{(\boldsymbol{b})}D\tilde{\Pi}^{(\boldsymbol{b})}\psi^{(100)}] \text{ and } \mathrm{tr}[\Pi^{(\boldsymbol{b})}D\Pi^{(\boldsymbol{b})}\psi^{(100)}]. \tag{81}$$

By exploiting Lemma 17 (i), we show that these terms are negligibly close to each other. Concretely, we apply Lemma 17 (i) by setting

$$(C,A,B) := (\tilde{\Pi}^{(\boldsymbol{b})}D,\tilde{\Pi}^{(\boldsymbol{b})},\Pi^{(\boldsymbol{b})}).$$

Since $||C||_\infty \le ||\tilde{\Pi}^{(\boldsymbol{b})}||_\infty||D||_\infty \le 1$, if

$$\tilde{\Pi}^{(\boldsymbol{b})} \approx_{0,\psi^{(\boldsymbol{\theta})}} \Pi^{(\boldsymbol{b})} \tag{82}$$

holds, we obtain

$$\mathrm{tr}[\tilde{\Pi}^{(\boldsymbol{b})}D\tilde{\Pi}^{(\boldsymbol{b})}\psi^{(\boldsymbol{\theta})}] \approx_0 \mathrm{tr}[\tilde{\Pi}^{(\boldsymbol{b})}D\Pi^{(\boldsymbol{b})}\psi^{(\boldsymbol{\theta})}]. \tag{83}$$

Also, we apply Lemma 17 (i) by setting

$$(C',A,B) := (D\Pi^{(\boldsymbol{b})},\tilde{\Pi}^{(\boldsymbol{b})},\Pi^{(\boldsymbol{b})}).$$

Since $||C'||_\infty \le ||D||_\infty||\Pi^{(\boldsymbol{b})}||_\infty \le 1$, if Eq. (82) holds, we also have

$$\mathrm{tr}[\tilde{\Pi}^{(\boldsymbol{b})}D\Pi^{(\boldsymbol{b})}\psi^{(\boldsymbol{\theta})}] \approx_0 \mathrm{tr}[\Pi^{(\boldsymbol{b})}D\Pi^{(\boldsymbol{b})}\psi^{(\boldsymbol{\theta})}]. \tag{84}$$

From Eqs. (83) and (84), we find that the two terms in Eq. (81) are negligibly close:

$$\mathrm{tr}[\tilde{\Pi}^{(\boldsymbol{b})}D\tilde{\Pi}^{(\boldsymbol{b})}\psi^{(100)}] \approx_0 \mathrm{tr}[\Pi^{(\boldsymbol{b})}D\Pi^{(\boldsymbol{b})}\psi^{(100)}].$$

Finally, we prove Eq. (82), namely we show for any perfect prover,

$$\tilde{\Pi}^{(\boldsymbol{b})} \approx_{0,\psi^{(\boldsymbol{\theta})}} \Pi^{(\boldsymbol{b})}.$$

From the definition of the state dependent norm, it suffices to show

$$\mathrm{tr}[(\Pi^{(\boldsymbol{b})}-\tilde{\Pi}^{(\boldsymbol{b})})^2\psi^{(\boldsymbol{\theta})}] = \mathrm{negl}(\lambda).$$

Using Eqs. (79) and (80), we have

$$\begin{aligned}\Pi^{(\boldsymbol{b})}-\tilde{\Pi}^{(\boldsymbol{b})} &= \sum_{\boldsymbol{y}}\left(\sum_{\boldsymbol{x}}\Pi_{\boldsymbol{y}}^{(b_1,x_1;b_2,x_2;b_3,x_3)} - \Pi_{\boldsymbol{y}}^{(b_1,\hat{x}_{b_1}(k_1,y_1);b_2,\hat{x}_{b_2}(k_2,y_2);b_3,\hat{x}_{b_3}(k_3,y_3))}\right)\otimes|\boldsymbol{y}\rangle\langle\boldsymbol{y}| \\ &= \sum_{\boldsymbol{y}}\sum_{x_1\neq\hat{x}_{b_1}(k_1,y_1),x_2\neq\hat{x}_{b_2}(k_2,y_2),x_3\neq\hat{x}_{b_3}(k_3,y_3)}\Pi_{\boldsymbol{y}}^{(b,x_1;b_2,x_2;b_3,x_3)}\otimes|\boldsymbol{y}\rangle\langle\boldsymbol{y}|. \end{aligned}\tag{85}$$

Here, $\Pi_{\boldsymbol{y}}^{(b_1,x_1;b_2,x_2;b_3,x_3)}$ are projectors that are orthogonal if the outcomes are different, and hence squaring Eq. (85) is unchanged. Therefore,

$$\mathrm{tr}[(\Pi^{(\boldsymbol{b})}-\tilde{\Pi}^{(\boldsymbol{b})})^2\psi^{(\boldsymbol{\theta})}] = \mathrm{tr}\left[\sum_{\boldsymbol{y}}\sum_{x_1\neq\hat{x}_{b_1}(k_1,y_1),x_2\neq\hat{x}_{b_2}(k_2,y_2),x_3\neq\hat{x}_{b_3}(k_3,y_3)}\Pi_{\boldsymbol{y}}^{(b_1,x_1;b_2,x_2;b_3,x_3)}\psi_{\boldsymbol{y}}^{(\boldsymbol{\theta})}\otimes|\boldsymbol{y}\rangle\langle\boldsymbol{y}|\right],$$

and this is negligible for a perfect prover.

Combining the arguments so far concludes $|\xi^{(0)}-\xi^{(1)}| = \mathrm{negl}(\lambda)$, which completes the proof. ■

G. Commutation relations of non-tilde observables

The goal of this section is to prove the following Lemma 41, which states the commutation relations of the non-tilde observables. Before we introduce that, we show a trivial commutation relation for the observables with the inputs to the device $\boldsymbol{q}$ being the same.

Lemma 39 *For any device $D = (S, \Pi, M, P)$, we have the commutation relations for any $i, j \in \{1, 2, 3\}$ and $\boldsymbol{q} \in \{0, 1\}^3$,*

$$[A_{i,\boldsymbol{q}}, A_{j,\boldsymbol{q}}] = 0. \tag{86}$$

(Proof) With the definition of $A_{i,\boldsymbol{q}}$ in Eq. (6) and by noting that $\{P_{\boldsymbol{q}}^{(\boldsymbol{v})}\}_{\boldsymbol{v}\in\{0,1\}^3}$ constitutes orthogonal projectors, we obtain Eq. (86). ■

This Lemma 39 can be intuitively derived because the inputs to the devices of the two binary observables $A_{i,\boldsymbol{q}}$ and $A_{j,\boldsymbol{q}}$ are the same as $\boldsymbol{q}$, and the only difference is the classical post-processing of the measurement outcomes. Since classical post-processings obviously commute, Eq. (86) is trivially satisfied. Next, in Lemma 41, we introduce another commutation relation with inputs to the device $\boldsymbol{q}$ being different, which only holds approximately. For this, we prepare Lemma 40 which is the auxiliary lemma to prove Lemma 41.

Lemma 40 *For any efficient device $D = (S, \Pi, M, P)$, we have the following approximate relation that holds for any $\boldsymbol{\theta} \in \mathcal{B}$ with $\theta_j = 1$ and $\theta_i = 0$ for $i \in \{1, 2, 3\} \setminus \{j\}$:*

$$\mathrm{tr}\left[\sum_{\boldsymbol{v}\in\{0,1\}^3} A_{i,\boldsymbol{0}}^{(v_i)} \sigma^{(\theta_1,v_1;\theta_2,v_2;\theta_3,v_3)}\right] \approx_0 \mathrm{tr}\left[\sum_{\boldsymbol{v}\in\{0,1\}^3} A_{i,\boldsymbol{0}}^{(v_i)} \sigma^{(0,v_1;0,v_2;0,v_3)}\right]. \tag{87}$$

(Proof) The RHS [LHS] represents the probability that the prover's answer v_i is accepted by the verifier conditioned on measuring the state $\rho^{(000)}$ [$\rho^{(\boldsymbol{\theta})}$ (with $\theta_j = 1$ and $\theta_i = 0$ for any $i \neq j$)] when the input to the device is $\boldsymbol{q} = 000$. We prove Eq. (87) by contradiction, namely if there exists a non-negligible difference between both sides of Eq. (87), we can construct an adversary $\mathcal{A}$ that distinguishes $\rho^{(000)}$ and $\rho^{(\boldsymbol{\theta})}$ with non-negligible advantage, which contradicts Lemma 31. The construction of $\mathcal{A}$ is as follows.

First, the adversary $\mathcal{A}$ receives the j^{th} key k_j from the verifier and samples the other keys and trapdoors from the distribution $(k_i, t_{k_i}) \leftarrow \mathsf{GEN}_{\mathcal{G}}(1^\lambda)$ for $i \in \{1, 2, 3\} \setminus \{j\}$. Note that $\mathcal{A}$ does not know whether $k_j \in \mathcal{K}_{\mathcal{G}}$ or $k_j \in \mathcal{K}_{\mathcal{F}}$ that indicates $\theta_j = 0$ or $\theta_j = 1$, respectively. Then $\mathcal{A}$ prepares the state $\psi^{(\boldsymbol{\theta})}$ and measures the state to obtain $\boldsymbol{y}$. After that $\mathcal{A}$ performs measurement M and obtains $\boldsymbol{d}$. Next, by using binary observable $\{A_{i,\boldsymbol{0}}^{(v_i)}\}_{v_i}$, $\mathcal{A}$ performs measurement to know whether his outcome v_i is accepted by the verifier, that is $v_i = \hat{b}(k_i, y_i)$ holds, or not. If the outcome v_i is accepted, $\mathcal{A}$ outputs $b = 0$. The reason why $\mathcal{A}$ can judge whether v_i is accepted or not is that $\mathcal{A}$ knows the i^{th} trapdoor. With the negation of Eq. (87), we have

$$|\Pr\{b = 0|\rho^{(\boldsymbol{\theta})}\} - \Pr\{b = 0|\rho^{(000)}\}| \geq \mu(\lambda).$$

This breaks the computational indistinguishability of $\rho^{(\boldsymbol{\theta})}$ stated in Lemma 31. Note that the proof of Lemma 31 reveals that this lemma also holds even when an efficient adversary $\mathcal{A}$ uses the l^{th} trapdoor, where l indicates the common θ in $\boldsymbol{\theta}$ and $\boldsymbol{\theta}'$ with $\mathrm{wt}(\boldsymbol{\theta}, \boldsymbol{\theta}') \in \{1, 2\}$. ■

Lemma 41 *For any efficient device $D = (S, \Pi, M, P)$, we have the approximate commutation relation that holds for any $\boldsymbol{\theta} \in \mathcal{B}$ and any i, j of $i \neq j$:*

$$[A_{i,\boldsymbol{0}}, A_{j,\boldsymbol{1}}] \approx_{\gamma_T(D),\rho^{(\boldsymbol{\theta})}} 0. \tag{88}$$

(Proof) From Lemma 21 (iii) and the indistinguishability of $\rho^{(\boldsymbol{\theta})}$ stated in Lemma 31, it suffices to show Eq. (88) for a specific $\boldsymbol{\theta}$. We here fix $\boldsymbol{\theta}$ to be $\theta_j = 1$ and $\theta_i = 0$ for any $i \neq j$. By the definition of $\gamma_T(D)$, we have

$$\mathrm{tr}\left(\sum_{\boldsymbol{v}} A_{i,\boldsymbol{0}}^{(v_i)} \sigma^{(0,v_1;0,v_2;0,v_3)}\right) \approx_{\gamma_T(D)} 1, \tag{89}$$

$$\mathrm{tr}\left(\sum_{\boldsymbol{v}} A_{j,\boldsymbol{1}}^{(v_j)} \sigma^{(\theta_1,v_1;\theta_2,v_2;\theta_3,v_3)}\right) \approx_{\gamma_T(D)} 1. \tag{90}$$

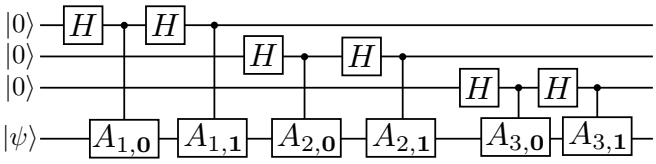

FIG. 1: The quantum circuit implementing the swap isometry V_S. Here, H is the Hadamard operator.

To make σ's in the above two trace terms to be the same, we apply Lemma 40 to Eq. (89), which results in

$$\mathrm{tr}\left(\sum_{\boldsymbol{v}} A_{i,\mathbf{0}}^{(v_i)}\sigma^{(\theta_1,v_1;\theta_2,v_2;\theta_3,v_3)}\right) \approx_{\gamma_T(D)} 1. \tag{91}$$

By using Corollary 28, Eqs. (90) and (91) respectively lead to

$$\begin{aligned} A_{j,\mathbf{1}} &\approx_{\gamma_T(D),\sigma^{(\theta_1,v_1;\theta_2,v_2;\theta_3,v_3)}} (-1)^{v_j} I, \\ A_{i,\mathbf{0}} &\approx_{\gamma_T(D),\sigma^{(\theta_1,v_1;\theta_2,v_2;\theta_3,v_3)}} (-1)^{v_i} I. \end{aligned}$$

Finally, Lemma 13 (i) implies

$$\begin{aligned} A_{i,\mathbf{0}}A_{j,\mathbf{1}} &\approx_{\gamma_T(D),\sigma^{(\theta_1,v_1;\theta_2,v_2;\theta_3,v_3)}} (-1)^{v_j} A_{i,\mathbf{0}} \\ &\approx_{\gamma_T(D),\sigma^{(\theta_1,v_1;\theta_2,v_2;\theta_3,v_3)}} (-1)^{v_i+v_j} I \\ &\approx_{\gamma_T(D),\sigma^{(\theta_1,v_1;\theta_2,v_2;\theta_3,v_3)}} A_{j,\mathbf{1}} \cdot (-1)^{v_i} I \\ &\approx_{\gamma_T(D),\sigma^{(\theta_1,v_1;\theta_2,v_2;\theta_3,v_3)}} A_{j,\mathbf{1}}A_{i,\mathbf{0}}, \end{aligned}$$

which ends the proof. ■

H. Approximate relations of non-tilde observables and Pauli observables

In this section, we first introduce the *swap isometry* V_S. This isometry is a completely positive and trace preserving (CPTP) map that adds a three-qubit Hilbert space $\mathbb{C}^8$ to the prover's Hilbert space $\mathcal{H}$ and swaps the three-qubit space in $\mathcal{H}$ to $\mathbb{C}^8$. The goal of this section is to prove Lemmas 43, 44, 47, and 52, which state that the non-tilde observables $A_{i,\mathbf{0}}$ and $A_{i,\mathbf{1}}$ for $i \in \{1,2,3\}$ are approximately equal to the Pauli observables under this swap isometry.

Definition 42 *Given a device $D = (S, \Pi, M, P)$ with Hilbert space $\mathcal{H}$, we define the swap isometry $V_S : \mathcal{H} \to \mathbb{C}^8 \otimes \mathcal{H}$ using non-tilde observables introduced in Eq. (6) as*

$$V_S = \frac{1}{8}\sum_{a,b,c\in\{0,1\}} |a,b,c\rangle \otimes \left[(A_{3,\mathbf{1}})^c(I+(-1)^c A_{3,\mathbf{0}})(A_{2,\mathbf{1}})^b(I+(-1)^b A_{2,\mathbf{0}})(A_{1,\mathbf{1}})^a(I+(-1)^a A_{1,\mathbf{0}})\right]. \tag{92}$$

Here, the superscripts a, b and c indicate the exponent not the projector.

By noting that non-tilde observables $A_{i,\mathbf{0}}$ and $A_{i,\mathbf{1}}$ are binary ones and $\sum_{a=0}^{1}(I+(-1)^a A_{i,\mathbf{0}})^2 = 4I$, we have

$$V_S^\dagger V_S = I. \tag{93}$$

By a direct calculation, it can be verified that the circuit in Fig. 1 implements the swap isometry V_S. As shown in Lemma 2.4 in [2], if A is an efficient binary observable, then its controlled unitary operation is an efficient unitary operation. Therefore, from the circuit in Fig. 1, V_S is found to be efficient for any efficient device $D = (S, \Pi, M, P)$ because the unitary operator acting on state $|0\rangle^{\otimes 3} \otimes |\psi\rangle$ is efficient.

Lemma 43 *Conjugating Pauli observables by swap isometry V_S gives the following.*

(i) $V_S^\dagger(\sigma_Z \otimes I_2^{\otimes 2} \otimes I)V_S = A_{1,\mathbf{0}}$ (94)

(ii) $V_S^\dagger(I_2 \otimes \sigma_Z \otimes I_2 \otimes I)V_S = \frac{1}{4}\sum_{a=0}^{1}(I+(-1)^a A_{1,\mathbf{0}})A_{1,\mathbf{1}}^a A_{2,\mathbf{0}} A_{1,\mathbf{1}}^a (I+(-1)^a A_{1,\mathbf{0}})$ (95)

(iii) $V_S^\dagger(I_2^{\otimes 2} \otimes \sigma_Z \otimes I)V_S = \frac{1}{16}\sum_{a,b}(I+(-1)^a A_{1,\mathbf{0}})A_{1,\mathbf{1}}^a (I+(-1)^b A_{2,\mathbf{0}})A_{2,\mathbf{1}}^b A_{3,\mathbf{0}} A_{2,\mathbf{1}}^b (I+(-1)^b A_{2,\mathbf{0}})$
$A_{1,\mathbf{1}}^a (I+(-1)^a A_{1,\mathbf{0}})$ (96)

(iv) $V_S^\dagger(\sigma_X \otimes I_2^{\otimes 2} \otimes I)V_S = \frac{1}{4}\sum_{a=0}^{1}(I+(-1)^{\overline{a}} A_{1,\mathbf{0}})A_{1,\mathbf{1}}(I+(-1)^a A_{1,\mathbf{0}})$ (97)

(v) $V_S^\dagger(I_2 \otimes \sigma_X \otimes I_2 \otimes I)V_S = \frac{1}{16}\sum_{a,b}(I+(-1)^a A_{1,\mathbf{0}})A_{1,\mathbf{1}}^a (I+(-1)^b A_{2,\mathbf{0}})A_{2,\mathbf{1}}(I+(-1)^{\overline{b}} A_{2,\mathbf{0}})A_{1,\mathbf{1}}^a (I+(-1)^a A_{1,\mathbf{0}})$ (98)

(vi) $V_S^\dagger(I_2^{\otimes 2} \otimes \sigma_X \otimes I)V_S = \frac{1}{64}\sum_{a,b,c}(I+(-1)^a A_{1,\mathbf{0}})A_{1,\mathbf{1}}^a (I+(-1)^b A_{2,\mathbf{0}})A_{2,\mathbf{1}}^b (I+(-1)^{\overline{c}} A_{3,\mathbf{0}})A_{3,\mathbf{1}}(I+(-1)^c A_{3,\mathbf{0}})$
$A_{2,\mathbf{1}}^b (I+(-1)^b A_{2,\mathbf{0}})A_{1,\mathbf{1}}^a (I+(-1)^a A_{1,\mathbf{0}})$ (99)

Proof of (i)-(iii) A direct calculation by substituting the definition of V_S in Eq. (92) to the LHS of Eqs. (94)-(96) and using the commutation relation $[A_{i,\mathbf{0}}, A_{j,\mathbf{0}}] = 0$ leads to the desired relations.
Proof of (iv) By substituting the definition of V_S, the LHS is equal to

$$\frac{1}{32}\sum_{a,b,c}(I+(-1)^{\overline{a}} A_{1,\mathbf{0}})A_{1,\mathbf{1}}^{\overline{a}}(I+(-1)^b A_{2,\mathbf{0}})A_{2,\mathbf{1}}^b (I+(-1)^c A_{3,\mathbf{0}})A_{2,\mathbf{1}}^b (I+(-1)^b A_{2,\mathbf{0}})A_{1,\mathbf{1}}^a (I+(-1)^a A_{1,\mathbf{0}}),$$

and by using the commutation relation $[A_{i,\mathbf{0}}, A_{j,\mathbf{0}}] = 0$ results in the desired relation.
Proof of (v) Substituting the definition of V_S to the LHS, we obtain

$$\frac{1}{32}\sum_{a,b,c}(I+(-1)^a A_{1,\mathbf{0}})A_{1,\mathbf{1}}^a (I+(-1)^{\overline{b}} A_{2,\mathbf{0}})A_{2,\mathbf{1}}^{\overline{b}}(I+(-1)^c A_{3,\mathbf{0}})A_{2,\mathbf{1}}^b (I+(-1)^b A_{2,\mathbf{0}})A_{1,\mathbf{1}}^a (I+(-1)^a A_{1,\mathbf{0}}),$$

and by using the commutation relation $[A_{i,\mathbf{0}}, A_{j,\mathbf{0}}] = 0$ leads to the desired relation.
Proof of (vi) By substituting the definition of V_S to the LHS and using $A_{3,\mathbf{1}}^c A_{3,\mathbf{1}}^{\overline{c}} = A_{3,\mathbf{1}}$ for any $c \in \{0,1\}$ results in the desired relation. ■

Next, we show that under the swap isometry V_S, the binary observable $A_{1,\mathbf{1}}$ is approximately equal to the Pauli-X observable.

Lemma 44 *For any efficient perfect device $D = (S, \Pi, M, P)$, we have for any $\boldsymbol{\theta} \in \mathcal{B}$,*

$$V_S^\dagger(\sigma_X \otimes I_2 \otimes I_2 \otimes I)V_S \approx_{\sqrt{\gamma_T(D)},\rho^{(\boldsymbol{\theta})}} A_{1,\mathbf{1}}. \tag{100}$$

In this lemma, we consider a perfect device to exploit the anti-commutation relation in Proposition 32 in which a perfect device is assumed.
(Proof) From Lemma 15, it suffices to show

$$\mathrm{tr}\left[V_S^\dagger(\sigma_X \otimes I_2 \otimes I_2 \otimes I)V_S A_{1,\mathbf{1}}\rho^{(\boldsymbol{\theta})}\right] \approx_{\sqrt{\gamma_T(D)}} 1.$$

Subsutituting Eq. (97), the LHS is rewirtten as

$$\frac{1}{4}\mathrm{tr}\left\{\sum_a [I+(-1)^{\bar{a}} A_{1,\mathbf{0}}]A_{1,\mathbf{1}}[I+(-1)^a A_{1,\mathbf{0}}]A_{1,\mathbf{1}}\rho^{(\boldsymbol{\theta})}\right\}. \tag{101}$$

Using Proposition 32: $\{A_{1,\mathbf{0}}, A_{1,\mathbf{1}}\} \approx_{\sqrt{\gamma_T(D)},\rho^{(\boldsymbol{\theta})}} 0$ and Lemma 17 (i), Eq. (101) is calculated as

$$\begin{aligned}
&\approx_{\sqrt{\gamma_T(D)}} \frac{1}{4}\mathrm{tr}\left(\sum_a [I+(-1)^a A_{1,\mathbf{0}}]A_{1,\mathbf{1}}^2[I+(-1)^a A_{1,\mathbf{0}}]\rho^{(\boldsymbol{\theta})}\right)\\
&= \frac{1}{4}\mathrm{tr}\left(\sum_a [I+(-1)^a A_{1,\mathbf{0}}]^2\rho^{(\boldsymbol{\theta})}\right)\\
&= \mathrm{tr}(\rho^{(\boldsymbol{\theta})})\\
&= 1,
\end{aligned}$$

which ends the proof. ■

Combining Eqs. (94) and (100), $A_{1,\boldsymbol{q}=\mathbf{0}}$ and $A_{1,\boldsymbol{q}=\mathbf{1}}$ are shown to be related to the Pauli-Z and X observables, respectively. Using these results, we partially characterize the prover's states. Specifically, we show that the prover's states can be written as product states where the first qubit is the eigenstate of either the Pauli-Z or X observable depending on $\theta_1 \in \{0,1\}$.

Lemma 45 *Let $D = (S, \Pi, M, P)$ be an efficient perfect device. For any $\boldsymbol{v} \in \{0,1\}^3$, there exists positive matrices $\alpha^{(0,v_1;0,v_2;0,v_3)}, \alpha^{(0,v_1;0,v_2;1,v_3)}, \alpha^{(0,v_1;1,v_2;0,v_3)}$ and $\alpha^{(1,v_1;0,v_2;0,v_3)}$ such that the following holds.*

$$\text{(i) } V_S\sigma^{(0,v_1;0,v_2;0,v_3)}V_S^\dagger \approx_{\gamma_T(D)^{1/4}+\gamma_T(D)} |v_1\rangle\langle v_1| \otimes \alpha^{(0,v_1;0,v_2;0,v_3)} \tag{102}$$

$$\text{(ii) } V_S\sigma^{(0,v_1;0,v_2;1,v_3)}V_S^\dagger \approx_{\gamma_T(D)^{1/4}+\gamma_T(D)} |v_1\rangle\langle v_1| \otimes \alpha^{(0,v_1;0,v_2;1,v_3)} \tag{103}$$

$$\text{(iii) } V_S\sigma^{(0,v_1;1,v_2;0,v_3)}V_S^\dagger \approx_{\gamma_T(D)^{1/4}+\gamma_T(D)} |v_1\rangle\langle v_1| \otimes \alpha^{(0,v_1;1,v_2;0,v_3)} \tag{104}$$

$$\text{(iv) } V_S\sigma^{(1,v_1;0,v_2;0,v_3)}V_S^\dagger \approx_{\gamma_T(D)^{1/4}+\gamma_T(D)} |(-)^{v_1}\rangle\langle(-)^{v_1}| \otimes \alpha^{(1,v_1;0,v_2;0,v_3)} \tag{105}$$

There are four approximate relations since there are four states corresponding to $\boldsymbol{\theta} = 000, 001, 010$ and 100 in the test case of the protocol.

(Proof) We first prove (iv). From Lemma 44, we have

$$A_{1,\mathbf{1}} \approx_{\sqrt{\gamma_T(D)},\rho^{(100)}} V_S^\dagger(\sigma_X \otimes I_2^{\otimes 2} \otimes I)V_S, \tag{106}$$

and Lemma 13 (ii) leads to

$$A_{1,\mathbf{1}} \approx_{\sqrt{\gamma_T(D)},\sigma^{(1,v_1;0,v_2;0,v_3)}} V_S^\dagger(\sigma_X \otimes I_2^{\otimes 2} \otimes I)V_S.$$

Then, Lemma 20 implies

$$A_{1,\mathbf{1}}^{(v_1)} \approx_{\sqrt{\gamma_T(D)},\sigma^{(1,v_1;0,v_2;0,v_3)}} V_S^\dagger(|(-)^{v_1}\rangle\langle(-)^{v_1}| \otimes I_2^{\otimes 2} \otimes I)V_S,$$

and using Lemma 17 (i) yields

$$\sum_{\boldsymbol{v}} \mathrm{tr}\left[V_S^\dagger(|(-)^{v_1}\rangle\langle(-)^{v_1}| \otimes I_2^{\otimes 2} \otimes I)V_S\sigma^{(1,v_1;0,v_2;0,v_3)}\right] \approx_{\gamma_T(D)^{1/4}} \sum_{\boldsymbol{v}} \mathrm{tr}[A_{1,\mathbf{1}}^{(v_1)}\sigma^{(1,v_1;0,v_2;0,v_3)}]. \tag{107}$$

From the definition of $\gamma_T(D)$ in Eq. (12), the RHS is approximately equal as $\approx_{\gamma_T(D)} 1$, and hence the LHS results in

$$\sum_{\boldsymbol{v}} \mathrm{tr}\left[V_S^\dagger(|(-)^{v_1}\rangle\langle(-)^{v_1}| \otimes I_2^{\otimes 2} \otimes I)V_S\sigma^{(1,v_1;0,v_2;0,v_3)}\right] \approx_{\gamma_T(D)^{1/4}+\gamma_T(D)} 1.$$

From Lemma 16 and Corollary 28, this leads to

$$|(-)^{v_1}\rangle\langle(-)^{v_1}| \otimes I_2^{\otimes 2} \otimes I \approx_{\gamma_T(D)^{1/4}+\gamma_T(D),V_S\sigma^{(1,v_1;0,v_2;0,v_3)}V_S^\dagger} I.$$

Finally, using Lemma 18 implies

$$V_S\sigma^{(1,v_1;0,v_2;0,v_3)}V_S^\dagger \approx_{\gamma_T(D)^{1/4}+\gamma_T(D)} (|(-)^{v_1}\rangle\langle(-)^{v_1}| \otimes I_2^{\otimes 2} \otimes I)V_S\sigma^{(1,v_1;0,v_2;0,v_3)}V_S^\dagger(|(-)^{v_1}\rangle\langle(-)^{v_1}| \otimes I_2^{\otimes 2} \otimes I).$$

By defining

$$\alpha^{(1,v_1;0,v_2;0,v_3)} := (\langle(-)^{v_1}| \otimes I_2^{\otimes 2} \otimes I)V_S\sigma^{(1,v_1;0,v_2;0,v_3)}V_S^\dagger(|(-)^{v_1}\rangle \otimes I_2^{\otimes 2} \otimes I),$$

we obtain the desired relation of (iv).

The other relations (i)-(iii) can be proven in the same way just by replacing Eq. (106) in the above proof with Eq. (94). ■

In the following discussions, we use the simplified notation

$$A \approx_{R,\psi} B$$

if there exists a constant $c > 0$ such that

$$A \approx_{\gamma_T(D)^c,\psi} B.$$

Lemma 46 *Let $D = (S, \Pi, M, P)$ be an efficient perfect device. There exists a normalized state α such that the following holds for any $v_1 \in \{0, 1\}$:*

$$\sum_{v_2,v_3} V_S\sigma^{(0,v_1;0,v_2;0,v_3)}V_S^\dagger \overset{c}{\approx}_R \frac{|v_1\rangle\langle v_1|}{2} \otimes \alpha, \tag{108}$$

$$\sum_{v_2,v_3} V_S\sigma^{(0,v_1;0,v_2;1,v_3)}V_S^\dagger \overset{c}{\approx}_R \frac{|v_1\rangle\langle v_1|}{2} \otimes \alpha, \tag{109}$$

$$\sum_{v_2,v_3} V_S\sigma^{(0,v_1;1,v_2;0,v_3)}V_S^\dagger \overset{c}{\approx}_R \frac{|v_1\rangle\langle v_1|}{2} \otimes \alpha, \tag{110}$$

$$\sum_{v_2,v_3} V_S\sigma^{(1,v_1;0,v_2;0,v_3)}V_S^\dagger \overset{c}{\approx}_R \frac{|(-)^{v_1}\rangle\langle(-)^{v_1}|}{2} \otimes \alpha. \tag{111}$$

(Proof) We first prove Eq. (111), and by using Eq. (111), we prove the rest of the relations. First, we rewrite Eqs. (102) and (105) respectively as

$$\left|\left|V_S\sigma^{(0,v_1;0,v_2;0,v_3)}V_S^\dagger - |v_1\rangle\langle v_1| \otimes \alpha^{(0,v_1;0,v_2;0,v_3)}\right|\right|_1^2 \leq \epsilon, \tag{112}$$

$$\left|\left|V_S\sigma^{(1,v_1;0,v_2;0,v_3)}V_S^\dagger - |(-)^{v_1}\rangle\langle(-)^{v_1}| \otimes \alpha^{(1,v_1;0,v_2;0,v_3)}\right|\right|_1^2 \leq \epsilon \tag{113}$$

with $\epsilon := O(\gamma_T(D)^{1/4} + \gamma_T(D))$. Then, if $\{\sum_{v_2,v_3} \alpha^{(1,v_1;0,v_2;0,v_3)}\}_{v_1}$ are proven to be computationally indistinguishable up to $O(\gamma_T(D)^c)$ for some constant c, combining Eq. (105) results in Eq. (111). We show this computational indistinguishability by contradiction, namely there exists a POVM $\Lambda := \{\Lambda_0, \Lambda_1\}$ with $\Lambda_0 + \Lambda_1 = I$ such that

$$\left|\mathrm{tr}\left[\Lambda_0 \sum_{v_2,v_3} \alpha^{(1,v_1=0;0,v_2;0,v_3)}\right] - \mathrm{tr}\left[\Lambda_0 \sum_{v_2,v_3} \alpha^{(1,v_1=1;0,v_2;0,v_3)}\right]\right| \geq \mu(\lambda) + 24\sqrt{\epsilon} \tag{114}$$

holds with a non-negligible function $\mu(\lambda)$. Under the existence of this POVM Λ, we can predict the outcome of the following POVM $\{\Gamma, I - \Gamma\}$ with

$$\Gamma := \sum_{u=0}^{1} V_S^\dagger(|(-)^u\rangle\langle(-)^u| \otimes \Lambda_u)V_S. \tag{115}$$

The prediction can be done by performing V_S to the prover's state and measure the first register in the Pauli-X basis and obtain its outcome a, followed by performing POVM Λ to the remaining registers and obtain the outcome u. From the expression of Eq. (115), the outcome corresponding to Γ is obtained when $a = u$. Under the existence of this POVM $\{\Gamma, I-\Gamma\}$, we can construct an adversary $\mathcal{A}$ that distinguishes $\rho^{(000)}$ and $\rho^{(100)}$ with non-negligible advantage.

The adversary $\mathcal{A}$ is randomly given either state $\rho^{(000)}$ or $\rho^{(100)}$, and $\mathcal{A}$ guesses the bit 0 if the outcome corresponding to Γ is obtained by performing measurement $\{\Gamma, I-\Gamma\}$. In this situation, the distinguishing advantage is given by

$$\begin{aligned}
\mathrm{Adv} :=& \left|\Pr\{\text{guess}=0|\rho^{(100)}\} - \Pr\{\text{guess}=0|\rho^{(000)}\}\right| \\
=& |\mathrm{tr}[\Gamma(\rho^{(100)}-\rho^{(000)})]| \\
=& \left|\sum_{u=0}^{1} \mathrm{tr}\left[(|(-)^u\rangle\langle(-)^u|\otimes\Lambda_u)(V_S\rho^{(100)}V_S^\dagger - V_S\rho^{(000)}V_S^\dagger)\right]\right| \\
=& \left|\sum_{u,\boldsymbol{v}\in\{0,1\}^3} \mathrm{tr}\left[(|(-)^u\rangle\langle(-)^u|\otimes\Lambda_u)(V_S\sigma^{(1,v_1;0,v_2;0,v_3)}V_S^\dagger - V_S\sigma^{(0,v_1;0,v_2;0,v_3)}V_S^\dagger)\right]\right|.
\end{aligned}$$

To obtain its lower bound, we exploit the relation [3]

$$|\mathrm{tr}[A(\varphi-\varphi')]| \le \tau \tag{116}$$

for positive operators φ and φ' satisfying $||\varphi-\varphi'||_1 \le \tau$ and a linear operator A satisfying $||A||_\infty \le 1$. From Eqs. (112), (113), (116) and the triangle inequality, we can replace the states inside the trace as

$$\begin{aligned}
\mathrm{Adv} \ge& \left|\sum_{u,\boldsymbol{v}\in\{0,1\}^3} \mathrm{tr}\left[(|(-)^u\rangle\langle(-)^u|\otimes\Lambda_u)\left(|(-)^{v_1}\rangle\langle(-)^{v_1}|\otimes\alpha^{(1,v_1;0,v_2;0,v_3)} - |v_1\rangle\langle v_1|\otimes\alpha^{(0,v_1;0,v_2;0,v_3)}\right)\right]\right| - 16\sqrt{\epsilon} \\
=& \left|\sum_{\boldsymbol{v}\in\{0,1\}^3} \mathrm{tr}\left[\Lambda_{v_1}\alpha^{(1,v_1;0,v_2;0,v_3)}\right] - \frac{1}{2}\sum_{u,\boldsymbol{v}\in\{0,1\}^3} \mathrm{tr}\left[\Lambda_u\alpha^{(0,v_1;0,v_2;0,v_3)}\right]\right| - 16\sqrt{\epsilon}.
\end{aligned} \tag{117}$$

By using $\sum_{v_1}\Lambda_{v_1} = I$, Eq. (117) is equal to

$$\begin{aligned}
&\left|\sum_{v_2,v_3} \mathrm{tr}\left[\Lambda_0(\alpha^{(1,0;0,v_2;0,v_3)} - \alpha^{(1,1;0,v_2;0,v_3)})\right] + \sum_{v_2,v_3}\mathrm{tr}(\alpha^{(1,1;0,v_2;0,v_3)}) - \frac{1}{2}\sum_{\boldsymbol{v}\in\{0,1\}^3}\mathrm{tr}(\alpha^{(0,v_1;0,v_2;0,v_3)})\right| - 16\sqrt{\epsilon} \\
\ge& \mu(\lambda) + 8\sqrt{\epsilon} - \left|\sum_{v_2,v_3}\mathrm{tr}(\alpha^{(1,1;0,v_2;0,v_3)}) - \frac{1}{2}\sum_{\boldsymbol{v}\in\{0,1\}^3}\mathrm{tr}(\alpha^{(0,v_1;0,v_2;0,v_3)})\right|,
\end{aligned} \tag{118}$$

where we use the triangle inequality and Eq. (114) in the inequality. We compute the third and fourth terms in turn.

$$\begin{aligned}
\sum_{v_2,v_3}\mathrm{tr}(\alpha^{(1,1;0,v_2;0,v_3)}) &= \sum_{v_2,v_3}\mathrm{tr}(|-\rangle\langle-|\otimes\alpha^{(1,1;0,v_2;0,v_3)}) \\
&\ge \sum_{v_2,v_3}\mathrm{tr}\left(V_S\sigma^{(1,1;0,v_2;0,v_3)}V_S^\dagger\right) - 4\sqrt{\epsilon} \\
&= \sum_{v_2,v_3}\mathrm{tr}\left(\sigma^{(1,1;0,v_2;0,v_3)}\right) - 4\sqrt{\epsilon} \\
&\approx_0 1/2 - 4\sqrt{\epsilon},
\end{aligned} \tag{119}$$

where in the inequality we use Eqs. (113) and (116), in the second equality we use $V_S^\dagger V_S = I$, and in the last approximate equality we use Lemma 35 and $\sum_{\boldsymbol{v}}\mathrm{tr}(\sigma^{(1,v_1;0,v_2;0,v_3)}) = \mathrm{tr}(\rho^{(100)}) = 1$.

We next compute the fourth term of Eq. (118).

$$\sum_{\boldsymbol{v}}\mathrm{tr}(\alpha^{(0,v_1;0,v_2;0,v_3)}) = \sum_{\boldsymbol{v}}\mathrm{tr}(|v_1\rangle\langle v_1|\otimes\alpha^{(0,v_1;0,v_2;0,v_3)}) \le \sum_{\boldsymbol{v}}\mathrm{tr}\left(V_S\sigma^{(0,v_1;0,v_2;0,v_3)}V_S^\dagger\right) + 8\sqrt{\epsilon} = 1 + 8\sqrt{\epsilon}, \tag{120}$$

---

[3] Note that Eq. (116) can be proven by applying Hölder's inequality as $|\mathrm{tr}[A(\varphi-\varphi')]| \le ||A||_\infty \cdot ||\varphi-\varphi'||_1$.

where in the inequality we use Eqs. (112) and (116). Substituting Eqs. (119) and (120) to Eq. (118) gives

$$|\Pr\{\text{guess} = 0|\rho^{(100)}\} - \Pr\{\text{guess} = 0|\rho^{(000)}\}| \geq \mu(\lambda),$$

which contradicts Lemma 31.

Next, we prove Eqs. (108)-(110) by using Eq. (111). First, from Eq. (111), we have

$$\sum_{\boldsymbol{v}} V_S \sigma^{(1,v_1;0,v_2;0,v_3)} V_S^\dagger \overset{c}{\approx}_R \frac{I_2}{2} \otimes \alpha.$$

Since $\rho^{(\boldsymbol{\theta})}$ are computationally indistinguishable from Lemma 31 and the isometry V_S is efficient, we also obtain

$$\sum_{\boldsymbol{v}} V_S \sigma^{(0,v_1;0,v_2;0,v_3)} V_S^\dagger \overset{c}{\approx}_R \frac{I_2}{2} \otimes \alpha,$$
$$\sum_{\boldsymbol{v}} V_S \sigma^{(0,v_1;0,v_2;1,v_3)} V_S^\dagger \overset{c}{\approx}_R \frac{I_2}{2} \otimes \alpha,$$
$$\sum_{\boldsymbol{v}} V_S \sigma^{(0,v_1;1,v_2;0,v_3)} V_S^\dagger \overset{c}{\approx}_R \frac{I_2}{2} \otimes \alpha.$$

From Eqs. (102), (103) and (104), we respectively obtain

$$\sum_{v_1} |v_1\rangle\langle v_1| \otimes \sum_{v_2,v_3} \alpha^{(0,v_1;0,v_2;0,v_3)} \overset{c}{\approx}_R I_2 \otimes \frac{\alpha}{2},$$
$$\sum_{v_1} |v_1\rangle\langle v_1| \otimes \sum_{v_2,v_3} \alpha^{(0,v_1;0,v_2;1,v_3)} \overset{c}{\approx}_R I_2 \otimes \frac{\alpha}{2},$$
$$\sum_{v_1} |v_1\rangle\langle v_1| \otimes \sum_{v_2,v_3} \alpha^{(0,v_1;1,v_2;0,v_3)} \overset{c}{\approx}_R I_2 \otimes \frac{\alpha}{2}.$$

Since these approximate relations hold for any efficient prover, these relations hold when the first register is measured in the Pauli-Z basis. By considering such a prover, we have

$$\sum_{v_2,v_3} \alpha^{(0,v_1;0,v_2;0,v_3)} \overset{c}{\approx}_R \frac{\alpha}{2},$$
$$\sum_{v_2,v_3} \alpha^{(0,v_1;0,v_2;1,v_3)} \overset{c}{\approx}_R \frac{\alpha}{2},$$
$$\sum_{v_2,v_3} \alpha^{(0,v_1;1,v_2;0,v_3)} \overset{c}{\approx}_R \frac{\alpha}{2}.$$

By taking sums of Eqs. (102)-(104) over v_2 and v_3 and by applying these three approximate relations, we obtain Eqs. (108)-(110), which completes the proof. ■

So far, we have shown that the state of the first register is approximately equal to the eigenstate of the Pauli observable. Next, by using this result of Lemma 46, we prove that the second observables are close to the Pauli observables under the swap isometry V_S.

Lemma 47 *For any efficient perfect device $D = (S, \Pi, M, P)$, we have for any $\boldsymbol{\theta} \in \mathcal{B}$,*

$$V_S^\dagger (I_2 \otimes \sigma_Z \otimes I_2 \otimes I) V_S \approx_{R,\rho^{(\boldsymbol{\theta})}} A_{2,\mathbf{0}}, \tag{121}$$
$$V_S^\dagger (I_2 \otimes \sigma_X \otimes I_2 \otimes I) V_S \approx_{R,\rho^{(\boldsymbol{\theta})}} A_{2,\mathbf{1}}. \tag{122}$$

We prove each relation in turn.

Proof of Eq. (121) From Lemmas 31 and 46, we have

$$V_S \rho^{(\boldsymbol{\theta})} V_S^\dagger \overset{c}{\approx}_R \frac{I_2}{2} \otimes \alpha =: \omega. \tag{123}$$

This implies that

$$\rho^{(\boldsymbol{\theta})} \overset{c}{\approx}_R V_S^\dagger \omega V_S \tag{124}$$

holds. This is because if there exists a distinguisher D that distinguishes $\rho^{(\boldsymbol{\theta})}$ and $V_S^\dagger \omega V_S$, we can construct a distinguisher D' that distinguishes $V_S \rho^{(\boldsymbol{\theta})} V_S^\dagger$ and ω. Given either state $V_S \rho^{(\boldsymbol{\theta})} V_S^\dagger$ or ω to D', D' performs the inverse of the unitary extension of V_S and measures the three qubits in the computational basis to obtain the outcomes $\boldsymbol{z} \in \{0,1\}^3$. Then, if $\boldsymbol{z} = 000$, which corresponds to obtaining the initial state $|0\rangle^{\otimes 3}$ in Fig. 1, D' succeeds in performing $V_S^\dagger$. Hence, if $\boldsymbol{z} = 000$, D' performs $V_S^\dagger$ to the state and call D to distinguish $\rho^{(\boldsymbol{\theta})}$ and $V_S^\dagger \omega V_S$, which results in non-negligible distinguishing advantage. If the input state to Fig. 1 is $\rho^{(\boldsymbol{\theta})}$, $\boldsymbol{z} = 000$ always holds, and hence if $\boldsymbol{z} \neq 000$, D' can correctly guess that the given state is ω.

Since σ_Z and $A_{2,\mathbf{0}}$ are efficient binary observables, using Lemma 21 (v), the proof of Eq. (121) is reduced to proving

$$V_S^\dagger (I_2 \otimes \sigma_Z \otimes I_2 \otimes I) V_S \approx_{R, V_S^\dagger \omega V_S} A_{2,\mathbf{0}}.$$

From Lemma 15, it suffices to show

$$\mathrm{tr}\left[A_{2,\mathbf{0}} V_S^\dagger (I_2 \otimes \sigma_Z \otimes I_2 \otimes I) V_S V_S^\dagger \omega V \right] \approx_R 1.$$

We compute the LHS as follows. By substituting Eq. (95) and inserting $V_S^\dagger V_S = I$ to the LHS, it is equal to

$$\frac{1}{4} \sum_{a=0}^{1} \mathrm{tr}\left[V_S A_{2,\mathbf{0}} (I + (-1)^a A_{1,\mathbf{0}}) A_{1,\mathbf{1}}^a A_{2,\mathbf{0}} A_{1,\mathbf{1}}^a V_S^\dagger V_S (I + (-1)^a A_{1,\mathbf{0}}) V_S^\dagger \omega \right]. \tag{125}$$

As will be proven in Eq. (127) in Lemma 48, using

$$I + (-1)^a \sigma_Z \otimes I_2 \otimes I_2 \otimes I \approx_{R,\omega} V_S (I + (-1)^a A_{1,\mathbf{0}}) V_S^\dagger$$

and Lemma 17 (i) gives an approximate relation of Eq. (125) as

$$\begin{aligned}
&\frac{1}{4} \sum_{a=0}^{1} \mathrm{tr}\left[V_S A_{2,\mathbf{0}} (I + (-1)^a A_{1,\mathbf{0}}) A_{1,\mathbf{1}}^a A_{2,\mathbf{0}} A_{1,\mathbf{1}}^a V_S^\dagger (I + (-1)^a \sigma_Z \otimes I_2 \otimes I_2 \otimes I) \omega \right] \\
=&\frac{1}{4} \sum_{a=0}^{1} \mathrm{tr}\left[(I + (-1)^a \sigma_Z \otimes I_2 \otimes I_2 \otimes I) V_S A_{2,\mathbf{0}} (I + (-1)^a A_{1,\mathbf{0}}) A_{1,\mathbf{1}}^a A_{2,\mathbf{0}} A_{1,\mathbf{1}}^a V_S^\dagger \omega \right].
\end{aligned}$$

Here, in the equation we used the commutation relation $[\sigma_Z \otimes I_2 \otimes I_2 \otimes I, \omega] = 0$. As will be proven in Eq. (128) in Lemma 48, using $V_S [A_{2,\mathbf{0}}, A_{1,\mathbf{1}}] V_S^\dagger \approx_{R,\omega} 0$ leads to

$$\begin{aligned}
\approx_R &\frac{1}{4} \sum_{a=0}^{1} \mathrm{tr}\left[(I + (-1)^a \sigma_Z \otimes I_2 \otimes I_2 \otimes I) V_S A_{2,\mathbf{0}} (I + (-1)^a A_{1,\mathbf{0}}) A_{1,\mathbf{1}}^a V_S^\dagger V_S A_{1,\mathbf{1}}^a A_{2,\mathbf{0}} V_S^\dagger \omega \right] \\
=&\frac{1}{4} \sum_{a=0}^{1} \mathrm{tr}\left[(I + (-1)^a \sigma_Z \otimes I_2 \otimes I_2 \otimes I) V_S A_{2,\mathbf{0}} (I + (-1)^a A_{1,\mathbf{0}}) A_{2,\mathbf{0}} V_S^\dagger \omega \right] \\
=&\frac{1}{4} \sum_{a=0}^{1} \mathrm{tr}\left[(I + (-1)^a \sigma_Z \otimes I_2 \otimes I_2 \otimes I) V_S (I + (-1)^a A_{1,\mathbf{0}}) V_S^\dagger \omega \right] \\
\approx_R &\frac{1}{4} \sum_{a=0}^{1} \mathrm{tr}\left[(I + (-1)^a \sigma_Z \otimes I_2 \otimes I_2 \otimes I)^2 \omega \right] \\
=&\mathrm{tr}(\omega) \\
=&1.
\end{aligned}$$

In the third equation, we used the commutation relation $[A_{1,\mathbf{0}}, A_{2,\mathbf{0}}] = 0$ and $A_{2,\mathbf{0}}^2 = I$. In the second approximate equation, we again used Eq. (127). This ends the proof.

Proof of Eq. (122) From Lemma 15, it suffices to show

$$\mathrm{tr}\left[A_{2,\mathbf{1}}V_S^\dagger(I_2\otimes\sigma_X\otimes I_2\otimes I)V_SV_S^\dagger\omega V_S\right]\approx_R 1.$$

By substituting Eq. (98) and inserting $V_S^\dagger V_S = I$, the LHS is equal to

$$\frac{1}{16}\sum_{a,b=0}^{1}\mathrm{tr}\left[V_SA_{2,\mathbf{1}}(I+(-1)^aA_{1,\mathbf{0}})A_{1,\mathbf{1}}^a(I+(-1)^{\bar{b}}A_{2,\mathbf{0}})A_{2,\mathbf{1}}(I+(-1)^bA_{2,\mathbf{0}})A_{1,\mathbf{1}}^aV_S^\dagger V_S(I+(-1)^aA_{1,\mathbf{0}})V_S^\dagger\omega\right].$$

By using Eq. (127), we have

$$\approx_R\frac{1}{16}\sum_{a,b=0}^{1}\mathrm{tr}\left[(I+(-1)^a\sigma_Z\otimes I_2^{\otimes 2}\otimes I)V_SA_{2,\mathbf{1}}(I+(-1)^aA_{1,\mathbf{0}})A_{1,\mathbf{1}}^a(I+(-1)^{\bar{b}}A_{2,\mathbf{0}})A_{2,\mathbf{1}}(I+(-1)^bA_{2,\mathbf{0}})V_S^\dagger V_SA_{1,\mathbf{1}}^aV_S^\dagger\omega\right].$$

Using Eq. (126) that will be proven in Lemma 48 results in

$$\begin{aligned}\approx_R\frac{1}{16}\sum_{a,b=0}^{1}\mathrm{tr}\Big[&(\sigma_X^a\otimes I_2^{\otimes 2}\otimes I)(I+(-1)^a\sigma_Z\otimes I_2^{\otimes 2}\otimes I)V_SA_{2,\mathbf{1}}(I+(-1)^aA_{1,\mathbf{0}})A_{1,\mathbf{1}}^a(I+(-1)^{\bar{b}}A_{2,\mathbf{0}})\\&A_{2,\mathbf{1}}(I+(-1)^bA_{2,\mathbf{0}})V_S^\dagger\omega\Big].\end{aligned}$$

Applying Eq. (129) that will be proven in Lemma 48 and the commutation relation $[A_{1,\mathbf{1}},A_{2,\mathbf{1}}]=0$ leads to

$$\begin{aligned}\approx_R&\frac{1}{16}\sum_{a,b=0}^{1}\mathrm{tr}\left[(\sigma_X^a\otimes I_2^{\otimes 2}\otimes I)(I+(-1)^a\sigma_Z\otimes I_2^{\otimes 2}\otimes I)V_SA_{2,\mathbf{1}}(I+(-1)^aA_{1,\mathbf{0}})A_{1,\mathbf{1}}^a(I+(-1)^{\bar{b}}A_{2,\mathbf{0}})^2A_{2,\mathbf{1}}V_S^\dagger\omega\right]\\=&\frac{1}{4}\sum_{a=0}^{1}\mathrm{tr}\left[(\sigma_X^a\otimes I_2^{\otimes 2}\otimes I)(I+(-1)^a\sigma_Z\otimes I_2^{\otimes 2}\otimes I)V_SA_{2,\mathbf{1}}(I+(-1)^aA_{1,\mathbf{0}})A_{2,\mathbf{1}}V_S^\dagger V_SA_{1,\mathbf{1}}^aV_S^\dagger\omega\right].\end{aligned}$$

Using Eq. (126) implies

$$\approx_R\frac{1}{4}\sum_{a=0}^{1}\mathrm{tr}\left[(\sigma_X^a\otimes I_2^{\otimes 2}\otimes I)^2(I+(-1)^a\sigma_Z\otimes I_2^{\otimes 2}\otimes I)V_SA_{2,\mathbf{1}}(I+(-1)^aA_{1,\mathbf{0}})A_{2,\mathbf{1}}V_S^\dagger\omega\right].$$

By applying Eq. (130) that will be proven in Lemma 48 and $A_{2,\mathbf{1}}^2=I$, we obtain

$$\approx_R\frac{1}{4}\sum_{a=0}^{1}\mathrm{tr}\left[(I+(-1)^a\sigma_Z\otimes I_2^{\otimes 2}\otimes I)V_S(I+(-1)^aA_{1,\mathbf{0}})V_S^\dagger\omega\right].$$

Again using Eq. (127) gives

$$\approx_R\frac{1}{4}\sum_{a=0}^{1}\mathrm{tr}\left[(I+(-1)^a\sigma_Z\otimes I_2^{\otimes 2}\otimes I)^2\omega\right]=\mathrm{tr}(\omega)=1,$$

which ends the proof. ■

Lemma 48 *(Auxiliary lemma in proving Lemma 47) In this lemma, we define* $\omega := I_2/2\otimes\alpha$.

$$\sigma_X\otimes I_2\otimes I_2\otimes I\approx_{R,\omega}V_SA_{1,\mathbf{1}}V_S^\dagger, \tag{126}$$

$$I+(-1)^a\sigma_Z\otimes I_2\otimes I_2\otimes I\approx_{R,\omega}V_S(I+(-1)^aA_{1,\mathbf{0}})V_S^\dagger, \tag{127}$$

$$V_S[A_{2,\mathbf{0}},A_{1,\mathbf{1}}]V_S^\dagger\approx_{R,\omega}0, \tag{128}$$

$$V_S\{A_{2,\mathbf{1}},A_{2,\mathbf{0}}\}V_S^\dagger\approx_{R,\omega}0, \tag{129}$$

$$V_S[A_{2,\mathbf{1}},A_{1,\mathbf{0}}]V_S^\dagger\approx_{R,\omega}0. \tag{130}$$

Proof of Eq. (126) From $V_S^\dagger(\sigma_X \otimes I_2^{\otimes 2} \otimes I)V_S \approx_{R,\rho^{(\boldsymbol{\theta})}} A_{1,\mathbf{1}}$ given in Lemma 44 and by using Lemma 19, we have

$$\sigma_X \otimes I_2^{\otimes 2} \otimes I \approx_{R,V_S\rho^{(\boldsymbol{\theta})}V_S^\dagger} V_S A_{1,\mathbf{1}} V_S^\dagger.$$

Then, using Eq. (123) and Lemma 21 (vi) enables us to replace $V_S\rho^{(\boldsymbol{\theta})}V_S^\dagger$ with ω.
Proof of Eq. (127) Once we have the following, the triangle inequality of the state dependent norm derives Eq. (127).

$$I \approx_{R,\omega} V_S V_S^\dagger, \tag{131}$$

$$\sigma_Z \otimes I_2 \otimes I_2 \otimes I \approx_{R,\omega} V_S A_{1,\mathbf{0}} V_S^\dagger. \tag{132}$$

Eq. (131) can be proven by combining $I \approx_{0,V_S\rho^{(\boldsymbol{\theta})}V_S^\dagger} V_S V_S^\dagger$ [4], Eq. (123) and Lemma 21 (vi). Eq. (132) can be proven by using Eq. (94) instead of using Lemma 44 in the proof of Eq. (126).
Proof of Eq. (128) From the definition of the state dependent norm, the LHS of Eq. (128) equals

$$\mathrm{tr}\left([A_{2,\mathbf{0}}, A_{1,\mathbf{1}}]^\dagger [A_{2,\mathbf{0}}, A_{1,\mathbf{1}}] V_S^\dagger \omega V_S\right).$$

By using Eq. (124) and Lemmas 21 (iii), this leads to

$$\approx_R \mathrm{tr}\left([A_{2,\mathbf{0}}, A_{1,\mathbf{1}}]^\dagger [A_{2,\mathbf{0}}, A_{1,\mathbf{1}}] \rho^{(\boldsymbol{\theta})}\right).$$

Finally, using Lemma 41 implies that this is approximately equal to zero ($\approx_R 0$), which ends the proof.
Proof of Eq. (129) By using Proposition 32 instead of using Lemma 41 in the proof of Eq. (128), we obtain Eq. (129).
Proof of Eq. (130) This can be proven by following exactly the same arguments done in the proof of Eq. (128).

Now, we have the approximate relations of the non-tilde observables $A_{2,\mathbf{0}}$ and $A_{2,\mathbf{1}}$. Using this result, we will characterize the state of the first and the second registers, which is an extension of Lemma 45. Specifically, we show that the prover's states are approximately equal to the product states where the first and the second qubits are the eigenstates of the Pauli observables depending on θ_1 and θ_2.

Lemma 49 *(Extension of Lemma 45) For any efficient and perfect device $D = (S, \Pi, M, P)$, we have for any $\boldsymbol{v} \in \{0,1\}^3$, there exists positive matrices $\tilde{\alpha}^{(0,v_1;0,v_2;0,v_3)}$, $\tilde{\alpha}^{(0,v_1;0,v_2;1,v_3)}$, $\tilde{\alpha}^{(0,v_1;1,v_2;0,v_3)}$ and $\tilde{\alpha}^{(1,v_1;0,v_2;0,v_3)}$ such that the following holds.*

$$\text{(i) } V_S\sigma^{(0,v_1;0,v_2;0,v_3)}V_S^\dagger \approx_R |v_1\rangle\langle v_1| \otimes |v_2\rangle\langle v_2| \otimes \tilde{\alpha}^{(0,v_1;0,v_2;0,v_3)} \tag{133}$$

$$\text{(ii) } V_S\sigma^{(0,v_1;0,v_2;1,v_3)}V_S^\dagger \approx_R |v_1\rangle\langle v_1| \otimes |v_2\rangle\langle v_2| \otimes \tilde{\alpha}^{(0,v_1;0,v_2;1,v_3)} \tag{134}$$

$$\text{(iii) } V_S\sigma^{(0,v_1;1,v_2;0,v_3)}V_S^\dagger \approx_R |v_1\rangle\langle v_1| \otimes |(-)^{v_2}\rangle\langle(-)^{v_2}| \otimes \tilde{\alpha}^{(0,v_1;1,v_2;0,v_3)} \tag{135}$$

$$\text{(iv) } V_S\sigma^{(1,v_1;0,v_2;0,v_3)}V_S^\dagger \approx_R |(-)^{v_1}\rangle\langle(-)^{v_1}| \otimes |v_2\rangle\langle v_2| \otimes \tilde{\alpha}^{(1,v_1;0,v_2;0,v_3)}$$

(Proof) By following the arguments in the proof of Lemma 45, we prove (iv). The other cases can be proven analogously. First, using Lemmas 47 and 13 (ii), we have

$$A_{2,\mathbf{0}} \approx_{R,\sigma^{(1,v_1;0,v_2;0,v_3)}} V_S^\dagger(I_2 \otimes \sigma_Z \otimes I_2 \otimes I)V_S.$$

Employing Lemma 20 leads to

$$A_{2,\mathbf{0}}^{(v_2)} \approx_{R,\sigma^{(1,v_1;0,v_2;0,v_3)}} V_S^\dagger(I_2 \otimes |v_2\rangle\langle v_2| \otimes I_2 \otimes I)V_S.$$

Using Lemma 17 (i), this results in

$$\sum_{\boldsymbol{v}} \mathrm{tr}\left[A_{2,\mathbf{0}}^{(v_2)}\sigma^{(1,v_1;0,v_2;0,v_3)}\right] \approx_R \sum_{\boldsymbol{v}} \mathrm{tr}\left[V_S^\dagger(I_2 \otimes |v_2\rangle\langle v_2| \otimes I_2 \otimes I)V_S\sigma^{(1,v_1;0,v_2;0,v_3)}\right]. \tag{136}$$

---

[4] Note that this can be proven as $\mathrm{tr}\left[(V_SV_S^\dagger - I)^\dagger(V_SV_S^\dagger - I)V_S\rho^{(\boldsymbol{\theta})}V_S^\dagger\right] = \mathrm{tr}\left[(V_SV_S^\dagger - I)^\dagger(V_S\rho^{(\boldsymbol{\theta})}V_S^\dagger - V_S\rho^{(\boldsymbol{\theta})}V_S^\dagger)\right] = 0$.

From Lemma 40,

$$\sum_{\boldsymbol{v}} \mathrm{tr}[A_{2,\mathbf{0}}^{(v_2)} \sigma^{(1,v_1;0,v_2;0,v_3)}] \approx_0 \sum_{\boldsymbol{v}} \mathrm{tr}[A_{2,\mathbf{0}}^{(v_2)} \sigma^{(0,v_1;0,v_2;0,v_3)}]$$

holds, and by the definition of $\gamma_T(D)$ in Eq. (12), the RHS is approximately equal to 1. This means that the RHS of Eq. (136) is also approximately equal to 1, namely

$$\sum_{\boldsymbol{v}} \mathrm{tr}\left[V_S^\dagger (I_2 \otimes |v_2\rangle\langle v_2| \otimes I_2 \otimes I) V_S \sigma^{(1,v_1;0,v_2;0,v_3)}\right] \approx_R 1.$$

Combining Corollary 28 and Lemma 16 results in

$$I_2 \otimes |v_2\rangle\langle v_2| \otimes I_2 \otimes I \approx_{R, V_S \sigma^{(1,v_1;0,v_2;0,v_3)} V_S^\dagger} I.$$

From Lemma 45, the state in the subscript of $\approx$ is close to $|(-)^{v_1}\rangle\langle(-)^{v_1}| \otimes \alpha^{(1,v_1;0,v_2;0,v_3)}$, and Lemma 17 (ii) enables us to replace the state with $|(-)^{v_1}\rangle\langle(-)^{v_1}| \otimes \alpha^{(1,v_1;0,v_2;0,v_3)}$ as

$$I_2 \otimes |v_2\rangle\langle v_2| \otimes I_2 \otimes I \approx_{R, |(-)^{v_1}\rangle\langle(-)^{v_1}| \otimes \alpha^{(1,v_1;0,v_2;0,v_3)}} I.$$

Finally, from Lemma 45:

$$V_S \sigma^{(1,v_1;0,v_2;0,v_3)} V_S^\dagger \approx_R |(-)^{v_1}\rangle\langle(-)^{v_1}| \otimes \alpha^{(1,v_1;0,v_2;0,v_3)}$$

and Lemma 18, we have

$$\begin{aligned} V_S \sigma^{(1,v_1;0,v_2;0,v_3)} V_S^\dagger &\approx_R I[|(-)^{v_1}\rangle\langle(-)^{v_1}| \otimes \alpha^{(1,v_1;0,v_2;0,v_3)}]I \\ &\approx_R (I_2 \otimes |v_2\rangle\langle v_2| \otimes I_2 \otimes I)[|(-)^{v_1}\rangle\langle(-)^{v_1}| \otimes \alpha^{(1,v_1;0,v_2;0,v_3)}](I_2 \otimes |v_2\rangle\langle v_2| \otimes I_2 \otimes I) \\ &= |(-)^{v_1}\rangle\langle(-)^{v_1}| \otimes |v_2\rangle\langle v_2| \otimes \tilde{\alpha}^{(1,v_1;0,v_2;0,v_3)}. \end{aligned}$$

With $\tilde{\alpha}^{(1,v_1;0,v_2;0,v_3)} := (\langle v_2| \otimes I)\alpha^{(1,v_1;0,v_2;0,v_3)}(|v_2\rangle \otimes I)$, we obtain the desired relation. ■

Using Lemma 49, we next show the lemma that is an extension of Lemma 46.

Lemma 50 *(Extension of Lemma 46) Let $D = (S, \Pi, M, P)$ be an efficient perfect device. There exists a normalized state $\tilde{\alpha}$ such that the following holds for any $v_1, v_2 \in \{0,1\}$.*

$$\text{(i)} \ \sum_{v_3} V_S \sigma^{(0,v_1;0,v_2;0,v_3)} V_S^\dagger \overset{c}{\approx}_R \frac{|v_1\rangle\langle v_1| \otimes |v_2\rangle\langle v_2|}{4} \otimes \tilde{\alpha} \tag{137}$$

$$\text{(ii)} \ \sum_{v_3} V_S \sigma^{(0,v_1;0,v_2;1,v_3)} V_S^\dagger \overset{c}{\approx}_R \frac{|v_1\rangle\langle v_1| \otimes |v_2\rangle\langle v_2|}{4} \otimes \tilde{\alpha} \tag{138}$$

$$\text{(iii)} \ \sum_{v_3} V \sigma^{(0,v_1;1,v_2;0,v_3)} V_S^\dagger \overset{c}{\approx}_R \frac{|v_1\rangle\langle v_1| \otimes |(-)^{v_2}\rangle\langle(-)^{v_2}|}{4} \otimes \tilde{\alpha} \tag{139}$$

$$\text{(iv)} \ \sum_{v_3} V_S \sigma^{(1,v_1;0,v_2;0,v_3)} V_S^\dagger \overset{c}{\approx}_R \frac{|(-)^{v_1}\rangle\langle(-)^{v_1}| \otimes |v_2\rangle\langle v_2|}{4} \otimes \tilde{\alpha} \tag{140}$$

(Proof) The proof is similar to the one of Lemma 46, but we give the full proof for completeness. We first prove (iv), and by using (iv), we prove the rest of the relations. To prove (iv), we need to show that $\{\sum_{v_3} \tilde{\alpha}^{(1,v_1;0,v_2;0,v_3)}\}_{v_1,v_2}$ are computationally indistinguishable. For this, we have shown in Lemma 46 that $\{\sum_{v_2,v_3} \alpha^{(1,v_1;0,v_2;0,v_3)}\}_{v_1}$ are computationally indistinguishable, and by considering Lemmas 45 and 49, this implies that $\{\sum_{v_2,v_3} \tilde{\alpha}^{(1,v_1;0,v_2;0,v_3)}\}_{v_1}$ are also computationally indistinguishable. Therefore, the remaining task is to prove that $\{\sum_{v_3} \tilde{\alpha}^{(1,v_1;0,v_2;0,v_3)}\}_{v_2}$ are computationally indistinguishable for any fixed v_1.

In the following discussions, we fix v_1. From Lemma 49, there exists a $d > 0$ such that for any v_2, v_3,

$$\left|\left| V_S \sigma^{(0,v_1;1,v_2;0,v_3)} V_S^\dagger - |v_1\rangle\langle v_1| \otimes |(-)^{v_2}\rangle\langle(-)^{v_2}| \otimes \tilde{\alpha}^{(0,v_1;1,v_2;0,v_3)} \right|\right|_1^2 \leq \epsilon, \tag{141}$$

$$\left|\left| V_S \sigma^{(1,v_1;0,v_2;0,v_3)} V_S^\dagger - |(-)^{v_1}\rangle\langle(-)^{v_1}| \otimes |v_2\rangle\langle v_2| \otimes \tilde{\alpha}^{(1,v_1;0,v_2;0,v_3)} \right|\right|_1^2 \leq \epsilon \tag{142}$$

hold with $\epsilon := O(\gamma_T(D)^d)$. From Lemmas 45 and 49, we have that for any efficient measurement $M := \{M_0, M_1\}$,

$$\left|\mathrm{tr}\left[M_0 \sum_{v_2',v_3'} \tilde{\alpha}^{(1,v_1=0;0,v_2';0,v_3')}\right] - \mathrm{tr}\left[M_0 \sum_{v_2',v_3'} \tilde{\alpha}^{(1,v_1=1;0,v_2';0,v_3')}\right]\right| \leq 2\sqrt{\epsilon}. \tag{143}$$

For the sake of contradiction, we assume that there exists a POVM $\Lambda := \{\Lambda_0, \Lambda_1\}$ with $\Lambda_0 + \Lambda_1 = I$ such that

$$\left|\mathrm{tr}\left[\Lambda_0 \sum_{v_3} \tilde{\alpha}^{(1,v_1;0,v_2=0;0,v_3)}\right] - \mathrm{tr}\left[\Lambda_0 \sum_{v_3} \tilde{\alpha}^{(1,v_1;0,v_2=1;0,v_3)}\right]\right| \geq 2\mu(\lambda) + 42\sqrt{\epsilon} \tag{144}$$

holds with a non-negligible function $\mu(\lambda)$. Under the existence of this POVM, we can construct an adversary $\mathcal{A}$ that distinguishes states $\rho^{(100)}$ and $\rho^{(010)}$ with non-negligible advantage using an efficient measurement $\{\Gamma, I-\Gamma\}$ with

$$\Gamma := V_S^\dagger(|(-)^{v_1}\rangle\langle(-)^{v_1}| \otimes |0\rangle\langle 0| \otimes \Lambda_0)V_S.$$

The distinguishing advantage is calculated as follows:

$$\begin{aligned}
\mathrm{Adv} :=& \left|\Pr\{\mathrm{guess} = 0|\rho^{(100)}\} - \Pr\{\mathrm{guess} = 0|\rho^{(010)}\}\right| \\
=& |\mathrm{tr}[\Gamma(\rho^{(100)} - \rho^{(010)})]| \\
=& \left|\mathrm{tr}\left[(|(-)^{v_1}\rangle\langle(-)^{v_1}| \otimes |0\rangle\langle 0| \otimes \Lambda_0)(V_S\rho^{(100)}V_S^\dagger - V_S\rho^{(010)}V_S^\dagger)\right]\right| \\
=& \left|\sum_{\boldsymbol{v}'\in\{0,1\}^3} \mathrm{tr}\left[(|(-)^{v_1}\rangle\langle(-)^{v_1}| \otimes |0\rangle\langle 0| \otimes \Lambda_0)(V_S\sigma^{(1,v_1';0,v_2';0,v_3')}V_S^\dagger - V_S\sigma^{(0,v_1';1,v_2';0,v_3')}V_S^\dagger)\right]\right|.
\end{aligned}$$

By applying Eq. (116) with Eqs. (141) and (142), we have

$$\begin{aligned}
\mathrm{Adv} \geq& \Big|\sum_{\boldsymbol{v}'\in\{0,1\}^3} \mathrm{tr}\Big[(|(-)^{v_1}\rangle\langle(-)^{v_1}| \otimes |0\rangle\langle 0| \otimes \Lambda_0) \\
&\left(|(-)^{v_1'}\rangle\langle(-)^{v_1'}| \otimes |v_2'\rangle\langle v_2'| \otimes \tilde{\alpha}^{(1,v_1';0,v_2';0,v_3')} - |v_1'\rangle\langle v_1'| \otimes |(-)^{v_2'}\rangle\langle(-)^{v_2'}| \otimes \tilde{\alpha}^{(0,v_1';1,v_2';0,v_3')}\right)\Big]\Big| - 16\sqrt{\epsilon} \\
=& \left|\sum_{v_3'} \mathrm{tr}\left[\Lambda_0\tilde{\alpha}^{(1,v_1;0,0;0,v_3')}\right] - \frac{1}{4}\sum_{\boldsymbol{v}'} \mathrm{tr}\left[\Lambda_0\tilde{\alpha}^{(0,v_1';1,v_2';0,v_3')}\right]\right| - 16\sqrt{\epsilon} \\
=& \left|\frac{1}{2}\sum_{v_3'} \mathrm{tr}\left[\Lambda_0(\tilde{\alpha}^{(1,v_1;0,0;0,v_3')} - \tilde{\alpha}^{(1,v_1;0,1;0,v_3')})\right] + \frac{1}{2}\sum_{v_2',v_3'} \mathrm{tr}[\Lambda_0\tilde{\alpha}^{(1,v_1;0,v_2';0,v_3')}] - \frac{1}{4}\sum_{\boldsymbol{v}'} \mathrm{tr}\left[\Lambda_0\tilde{\alpha}^{(0,v_1';1,v_2';0,v_3')}\right]\right| - 16\sqrt{\epsilon} \\
\geq& \mu(\lambda) + 5\sqrt{\epsilon} - \frac{1}{2}\left|\sum_{v_2',v_3'} \mathrm{tr}[\Lambda_0\tilde{\alpha}^{(1,v_1;0,v_2';0,v_3')}] - \frac{1}{2}\sum_{\boldsymbol{v}'} \mathrm{tr}\left[\Lambda_0\tilde{\alpha}^{(0,v_1';1,v_2';0,v_3')}\right]\right| \\
\geq& \mu(\lambda) + 5\sqrt{\epsilon} - \frac{1}{2}\left[\left|\sum_{v_2',v_3'} \mathrm{tr}[\Lambda_0\tilde{\alpha}^{(1,v_1;0,v_2';0,v_3')}] - \frac{1}{2}\sum_{\boldsymbol{v}'} \mathrm{tr}\left[\Lambda_0\tilde{\alpha}^{(1,v_1';0,v_2';0,v_3')}\right]\right|\right. \\
&\left. + \frac{1}{2}\left|\sum_{\boldsymbol{v}'} \mathrm{tr}\left[\Lambda_0\tilde{\alpha}^{(0,v_1';1,v_2';0,v_3')}\right] - \sum_{\boldsymbol{v}'} \mathrm{tr}\left[\Lambda_0\tilde{\alpha}^{(1,v_1';0,v_2';0,v_3')}\right]\right|\right] \\
\geq& \mu(\lambda) + 4\sqrt{\epsilon} - \frac{1}{4}\left|\sum_{\boldsymbol{v}'} \mathrm{tr}\left[\Lambda_0\left(\tilde{\alpha}^{(0,v_1';1,v_2';0,v_3')} - \tilde{\alpha}^{(1,v_1';0,v_2';0,v_3')}\right)\right]\right| \\
=& \mu(\lambda) + 4\sqrt{\epsilon} \\
&- \frac{1}{4}\left|\sum_{\boldsymbol{v}'} \mathrm{tr}\left[\Lambda_0\left(|v_1'\rangle\langle v_1'| \otimes |(-)^{v_2'}\rangle\langle(-)^{v_2'}| \otimes \tilde{\alpha}^{(0,v_1';1,v_2';0,v_3')} - |(-)^{v_1'}\rangle\langle(-)^{v_1'}| \otimes |v_2'\rangle\langle v_2'| \otimes \tilde{\alpha}^{(1,v_1';0,v_2';0,v_3')}\right)\right]\right|,
\end{aligned}$$

where we use the triangle inequality and Eq. (144) in the second inequality, the third one follows from the triangle inequality, and the fourth one comes from Eq. (143). Again, by applying Eq. (116) with Eqs. (141) and (142), we obtain

$$\begin{aligned}\mathrm{Adv} \geq& \mu(\lambda) - \frac{1}{4}\left|\mathrm{tr}\left[\Lambda_0\left(\sum_{\boldsymbol{v}'} V_S\sigma^{(0,v_1';1,v_2';0,v_3')}V_S^\dagger - \sum_{\boldsymbol{v}'} V_S\sigma^{(1,v_1';0,v_2';0,v_3')}V_S^\dagger\right)\right]\right| \\ =& \mu(\lambda) - \frac{1}{4}\left|\mathrm{tr}\left[(V_S^\dagger\Lambda_0 V_S)\left(\rho^{(010)} - \rho^{(100)}\right)\right]\right|.\end{aligned}$$

Since $\{V_S^\dagger\Lambda_0 V_S, I - V_S^\dagger\Lambda_0 V_S\}$ is an efficient measurement, the computational indistinguishability in Lemma 31 states that the second term is $\mathrm{negl}(\lambda)$. Therefore, the distinguishing advantage is non-negligible that contradicts Lemma 31, which completes the proof of Eq. (140).

Next, we prove Eqs. (137)-(139) using Eq. (140). First, from Eq. (140), we have

$$\sum_{\boldsymbol{v}} V_S\sigma^{(1,v_1;0,v_2;0,v_3)}V_S^\dagger \overset{c}{\approx}_R \frac{I_2^{\otimes 2}}{4}\otimes\tilde{\alpha}.$$

Since $\rho^{(\boldsymbol{\theta})}$ are computationally indistinguishable from Lemma 31 and the isometry V_S is efficient, we also obtain

$$\begin{aligned}\sum_{\boldsymbol{v}} V_S\sigma^{(0,v_1;0,v_2;0,v_3)}V_S^\dagger &\overset{c}{\approx}_R \frac{I_2^{\otimes 2}}{4}\otimes\tilde{\alpha}, \\ \sum_{\boldsymbol{v}} V_S\sigma^{(0,v_1;0,v_2;1,v_3)}V_S^\dagger &\overset{c}{\approx}_R \frac{I_2^{\otimes 2}}{4}\otimes\tilde{\alpha}, \\ \sum_{\boldsymbol{v}} V_S\sigma^{(0,v_1;1,v_2;0,v_3)}V_S^\dagger &\overset{c}{\approx}_R \frac{I_2^{\otimes 2}}{4}\otimes\tilde{\alpha}.\end{aligned}$$

From Eqs. (133)-(135), we respectively obtain

$$\begin{aligned}\sum_{v_1}|v_1\rangle\langle v_1|\otimes\sum_{v_2}|v_2\rangle\langle v_2|\otimes\sum_{v_3}\tilde{\alpha}^{(0,v_1;0,v_2;0,v_3)} &\overset{c}{\approx}_R I_2^{\otimes 2}\otimes\frac{\tilde{\alpha}}{4}, \\ \sum_{v_1}|v_1\rangle\langle v_1|\otimes\sum_{v_2}|v_2\rangle\langle v_2|\otimes\sum_{v_3}\tilde{\alpha}^{(0,v_1;0,v_2;1,v_3)} &\overset{c}{\approx}_R I_2^{\otimes 2}\otimes\frac{\tilde{\alpha}}{4}, \\ \sum_{v_1}|v_1\rangle\langle v_1|\otimes\sum_{v_2}|(-)^{v_2}\rangle\langle(-)^{v_2}|\otimes\sum_{v_3}\tilde{\alpha}^{(0,v_1;1,v_2;0,v_3)} &\overset{c}{\approx}_R I_2^{\otimes 2}\otimes\frac{\tilde{\alpha}}{4}.\end{aligned}$$

Since these approximate relations hold for any efficient prover, these relations hold when the first and the second registers are measured in the Pauli bases. By considering such a prover, we have

$$\begin{aligned}\sum_{v_3}\tilde{\alpha}^{(0,v_1;0,v_2;0,v_3)} &\overset{c}{\approx}_R \frac{\tilde{\alpha}}{4}, \\ \sum_{v_3}\tilde{\alpha}^{(0,v_1;0,v_2;1,v_3)} &\overset{c}{\approx}_R \frac{\tilde{\alpha}}{4}, \\ \sum_{v_3}\tilde{\alpha}^{(0,v_1;1,v_2;0,v_3)} &\overset{c}{\approx}_R \frac{\tilde{\alpha}}{4}.\end{aligned}$$

By taking sums of Eqs. (133)-(135) over v_3 and by applying these three approximate relations, we obtain Eqs. (137)-(139), which completes the proof. ■

With Lemma 50 in hand, we obtain a simple corollary describing an approximate relation of state $\rho^{(\boldsymbol{\theta})}$.

Corollary 51 *Let $D = (S, \Pi, M, P)$ be an efficient perfect device. There exists a normalized state $\tilde{\alpha}$ such that $\forall\boldsymbol{\theta}\in\mathcal{B}$,*

$$V_S\rho^{(\boldsymbol{\theta})}V_S^\dagger \overset{c}{\approx}_R \frac{I_2\otimes I_2}{4}\otimes\tilde{\alpha}. \tag{145}$$

(Proof) Taking the sum of the equations in Lemma 50 over v_1 and v_2 yields the the statement for $\boldsymbol{\theta}$ of the test case. We can lift up the statement for any $\boldsymbol{\theta} \in \mathcal{B}$ thanks to Lemma 31. ■

So far, we have shown that the prover's states are approximately equal to the product states where the first and the second registers are in the qubit states. Using this result of Corollary 51, we prove that the non-tilde observables $A_{3,\mathbf{0}}$ and $A_{3,\mathbf{1}}$ are approximately equal to the Pauli observables under the swap isometry V_S.

Lemma 52 *For any efficient perfect device $D = (S, \Pi, M, P)$, we have for any $\boldsymbol{\theta} \in \mathcal{B}$,*

$$V_S^\dagger (I_2 \otimes I_2 \otimes \sigma_Z \otimes I) V_S \approx_{R,\rho^{(\boldsymbol{\theta})}} A_{3,\mathbf{0}}, \tag{146}$$

$$V_S^\dagger (I_2 \otimes I_2 \otimes \sigma_X \otimes I) V_S \approx_{R,\rho^{(\boldsymbol{\theta})}} A_{3,\mathbf{1}}. \tag{147}$$

We prove each relation in turn.
Proof of Eq. (146) First, from Corollary 51,

$$V_S \rho^{(\boldsymbol{\theta})} V_S^\dagger \overset{c}{\approx}_R \frac{I_2 \otimes I_2}{4} \otimes \tilde{\alpha} =: \kappa. \tag{148}$$

By doing the same arguments to obtain Eq. (124), we have

$$\rho^{(\boldsymbol{\theta})} \overset{c}{\approx}_R V_S^\dagger \kappa V_S. \tag{149}$$

Since σ_Z and $A_{3,\mathbf{0}}$ are efficient binary observables, by using Lemma 21 (v), the proof of Eq. (146) is reduced to proving

$$V_S^\dagger (I_2 \otimes I_2 \otimes \sigma_Z \otimes I) V_S \approx_{R,V_S^\dagger \kappa V_S} A_{3,\mathbf{0}}.$$

From Lemma 15, it suffices to show

$$\mathrm{tr}\left[A_{3,\mathbf{0}} V_S^\dagger (I_2 \otimes I_2 \otimes \sigma_Z \otimes I) V_S (V_S^\dagger \kappa V_S) \right] \approx_R 1.$$

By substituting Eq. (96) to the LHS, the LHS is equal to

$$\frac{1}{16} \sum_{a,b} \mathrm{tr}\left[A_{3,\mathbf{0}} (I + (-1)^a A_{1,\mathbf{0}}) A^a_{1,\mathbf{1}} (I + (-1)^b A_{2,\mathbf{0}}) A^b_{2,\mathbf{1}} A_{3,\mathbf{0}} A^b_{2,\mathbf{1}} (I + (-1)^b A_{2,\mathbf{0}}) A^a_{1,\mathbf{1}} (I + (-1)^a A_{1,\mathbf{0}}) (V_S^\dagger \kappa V_S) \right].$$

Inserting $V_S^\dagger V_S = I$ leads to

$$= \frac{1}{16} \sum_{a,b} \mathrm{tr}\left[V_S A_{3,\mathbf{0}} (I + (-1)^a A_{1,\mathbf{0}}) A^a_{1,\mathbf{1}} (I + (-1)^b A_{2,\mathbf{0}}) A^b_{2,\mathbf{1}} A_{3,\mathbf{0}} A^b_{2,\mathbf{1}} (I + (-1)^b A_{2,\mathbf{0}}) A^a_{1,\mathbf{1}} V_S^\dagger V_S (I + (-1)^a A_{1,\mathbf{0}}) V_S^\dagger \kappa \right]. \tag{150}$$

Using Eq. (127) by replacing the state $I_2/2 \otimes \alpha$ with $I_2^{\otimes 2}/4 \otimes \tilde{\alpha}$ gives that Eq. (150) is approximately equal to

$$\frac{1}{16} \sum_{a,b} \mathrm{tr}\Big[V_S (I + (-1)^a \sigma_Z \otimes I_2^{\otimes 2} \otimes I) V_S A_{3,\mathbf{0}} (I + (-1)^a A_{1,\mathbf{0}}) A^a_{1,\mathbf{1}} (I + (-1)^b A_{2,\mathbf{0}})$$
$$A^b_{2,\mathbf{1}} A_{3,\mathbf{0}} A^b_{2,\mathbf{1}} (I + (-1)^b A_{2,\mathbf{0}}) V_S^\dagger (V_S A^a_{1,\mathbf{1}} V_S^\dagger) \kappa \Big].$$

Using Eq. (126) by replacing the state $I_2/2 \otimes \alpha$ with $I_2^{\otimes 2}/4 \otimes \tilde{\alpha}$ leads to

$$\approx_R \frac{1}{16} \sum_{a,b} \mathrm{tr}\Big[(\sigma^a_X \otimes I_2^{\otimes 2} \otimes I)(I + (-1)^a \sigma_Z \otimes I_2^{\otimes 2} \otimes I) V_S A_{3,\mathbf{0}} (I + (-1)^a A_{1,\mathbf{0}}) A^a_{1,\mathbf{1}} (I + (-1)^b A_{2,\mathbf{0}}) A^b_{2,\mathbf{1}} A_{3,\mathbf{0}} A^b_{2,\mathbf{1}} V_S^\dagger$$
$$V_S (I + (-1)^b A_{2,\mathbf{0}}) V_S^\dagger \kappa \Big]. \tag{151}$$

Next, since

$$V_S [I + (-1)^b A_{2,\mathbf{0}}] V_S^\dagger \approx_{R,\kappa} I + (-1)^b I_2 \otimes \sigma_Z \otimes I_2 \otimes I, \tag{152}$$

which will be proven in Lemma 53 (i) below, Eq. (151) is approximately equal to

$$\frac{1}{16}\sum_{a,b}\mathrm{tr}\Big[(I+(-1)^b I_2\otimes\sigma_Z\otimes I_2\otimes I)(\sigma_X^a\otimes I_2^{\otimes 2}\otimes I)(I+(-1)^a\sigma_Z\otimes I_2^{\otimes 2}\otimes I)V_S A_{3,\mathbf{0}}(I+(-1)^a A_{1,\mathbf{0}})A_{1,\mathbf{1}}^a$$
$$(I+(-1)^b A_{2,\mathbf{0}})A_{2,\mathbf{1}}^b V_S^\dagger V_S A_{3,\mathbf{0}} A_{2,\mathbf{1}}^b V_S^\dagger\kappa\Big]. \tag{153}$$

Also, since we have

$$V_S[A_{3,\mathbf{0}},A_{2,\mathbf{1}}]V_S^\dagger\approx_{R,\kappa}0,$$

which will be proven in Lemma 53 (ii) below, Eq. (153) is approximately equal to

$$\frac{1}{16}\sum_{a,b}\mathrm{tr}\Big[(I+(-1)^b I_2\otimes\sigma_Z\otimes I_2\otimes I)(\sigma_X^a\otimes I_2^{\otimes 2}\otimes I)(I+(-1)^a\sigma_Z\otimes I_2^{\otimes 2}\otimes I)$$
$$V_S A_{3,\mathbf{0}}(I+(-1)^a A_{1,\mathbf{0}})A_{1,\mathbf{1}}^a(I+(-1)^b A_{2,\mathbf{0}})A_{2,\mathbf{1}}^b V_S^\dagger V_S A_{2,\mathbf{1}}^b A_{3,\mathbf{0}}V_S^\dagger\kappa\Big].$$

Using $V_S^\dagger V_S=I$, $A_{2,\mathbf{1}}^2=I$ and $[A_{2,\mathbf{0}},A_{3,\mathbf{0}}]=0$ leads to

$$=\frac{1}{16}\sum_{a,b}\mathrm{tr}\Big[(I+(-1)^b I_2\otimes\sigma_Z\otimes I_2\otimes I)(\sigma_X^a\otimes I_2^{\otimes 2}\otimes I)(I+(-1)^a\sigma_Z\otimes I_2^{\otimes 2}\otimes I)$$
$$V_S A_{3,\mathbf{0}}(I+(-1)^a A_{1,\mathbf{0}})A_{1,\mathbf{1}}^a A_{3,\mathbf{0}}V_S^\dagger[V_S(I+(-1)^b A_{2,\mathbf{0}})V_S^\dagger]\kappa\Big].$$

We again use Eq. (152) and obtain

$$\approx_R\frac{1}{16}\sum_{a,b}\mathrm{tr}\Big[(I+(-1)^b I_2\otimes\sigma_Z\otimes I_2\otimes I)^2(\sigma_X^a\otimes I_2^{\otimes 2}\otimes I)(I+(-1)^a\sigma_Z\otimes I_2^{\otimes 2}\otimes I)$$
$$V_S A_{3,\mathbf{0}}(I+(-1)^a A_{1,\mathbf{0}})V_S^\dagger[V_S A_{1,\mathbf{1}}^a A_{3,\mathbf{0}}V_S^\dagger]\kappa\Big]$$
$$=\frac{1}{4}\sum_a\mathrm{tr}\Big[(\sigma_X^a\otimes I_2^{\otimes 2}\otimes I)(I+(-1)^a\sigma_Z\otimes I_2^{\otimes 2}\otimes I)V_S A_{3,\mathbf{0}}(I+(-1)^a A_{1,\mathbf{0}})V_S^\dagger[V_S A_{1,\mathbf{1}}^a A_{3,\mathbf{0}}V_S^\dagger]\kappa\Big]. \tag{154}$$

Also, as

$$V_S[A_{3,\mathbf{0}},A_{1,\mathbf{1}}]V_S^\dagger\approx_{R,\kappa}0,$$

which will be proven in Lemma 53 (ii) below, we have that Eq. (154) is approximately equal to

$$\frac{1}{4}\sum_a\mathrm{tr}\left[(\sigma_X^a\otimes I_2^{\otimes 2}\otimes I)(I+(-1)^a\sigma_Z\otimes I_2^{\otimes 2}\otimes I)V_S A_{3,\mathbf{0}}(I+(-1)^a A_{1,\mathbf{0}})V_S^\dagger V_S A_{3,\mathbf{0}}A_{1,\mathbf{1}}^a V_S^\dagger\kappa\right].$$

Using $V_S^\dagger V_S=I$, $[A_{1,\mathbf{0}},A_{3,\mathbf{0}}]=0$ and $A_{3,\mathbf{0}}^2=I$ leads to

$$=\frac{1}{4}\sum_a\mathrm{tr}\left[(\sigma_X^a\otimes I_2^{\otimes 2}\otimes I)(I+(-1)^a\sigma_Z\otimes I_2^{\otimes 2}\otimes I)V_S(I+(-1)^a A_{1,\mathbf{0}})V_S^\dagger[V_S A_{1,\mathbf{1}}^a V_S^\dagger]\kappa\right].$$

Again, by using Eq. (126) by replacing the state $I_2/2\otimes\alpha$ with $I_2^{\otimes 2}/4\otimes\tilde{\alpha}$, we have

$$\approx_R\frac{1}{4}\sum_a\mathrm{tr}\left[(\sigma_X^a\otimes I_2^{\otimes 2}\otimes I)^2(I+(-1)^a\sigma_Z\otimes I_2^{\otimes 2}\otimes I)V_S(I+(-1)^a A_{1,\mathbf{0}})V_S^\dagger\kappa\right]$$
$$=\frac{1}{4}\sum_a\mathrm{tr}\left[(I+(-1)^a\sigma_Z\otimes I_2^{\otimes 2}\otimes I)V_S(I+(-1)^a A_{1,\mathbf{0}})V_S^\dagger\kappa\right].$$

Finally, using Eq. (127) by replacing the state $I_2/2\otimes\alpha$ with $I_2^{\otimes 2}/4\otimes\tilde{\alpha}$ gives

$$\approx_R\frac{1}{4}\sum_a\mathrm{tr}\left[(I+(-1)^a\sigma_Z\otimes I_2^{\otimes 2}\otimes I)^2\kappa\right]=\mathrm{tr}(\kappa)=1,$$

which ends the proof. ■

Proof of Eq. (147) From Eq. (149), the proof of Eq. (147) is reduced to showing

$$V_S^\dagger(I_2^{\otimes 2}\otimes\sigma_X\otimes I)V_S \approx_{R,V_S^\dagger\kappa V_S} A_{3,\mathbf{1}}.$$

From Lemma 15, it suffices to prove

$$\mathrm{tr}\left[A_{3,\mathbf{1}}V_S^\dagger(I_2^{\otimes 2}\otimes\sigma_X\otimes I)V_S(V_S^\dagger\kappa V_S)\right]\approx_R 1.$$

Substituting Eq. (99) to the LHS, the LHS leads to

$$\begin{aligned}=\frac{1}{64}\sum_{a,b,c}\mathrm{tr}\Big[&A_{3,\mathbf{1}}[I+(-1)^aA_{1,\mathbf{0}}]A_{1,\mathbf{1}}^a[I+(-1)^bA_{2,\mathbf{0}}]A_{2,\mathbf{1}}^b[I+(-1)^{\bar c}A_{3,\mathbf{0}}]A_{3,\mathbf{1}}\\&[I+(-1)^cA_{3,\mathbf{0}}]A_{2,\mathbf{1}}^b[I+(-1)^bA_{2,\mathbf{0}}]A_{1,\mathbf{1}}^a[I+(-1)^aA_{1,\mathbf{0}}]V_S^\dagger\kappa V_S\Big].\end{aligned}$$

Inserting $V_S^\dagger V_S=I$ results in

$$\begin{aligned}=\frac{1}{64}\sum_{a,b,c}\mathrm{tr}\Big[&V_SA_{3,\mathbf{1}}[I+(-1)^aA_{1,\mathbf{0}}]A_{1,\mathbf{1}}^a[I+(-1)^bA_{2,\mathbf{0}}]A_{2,\mathbf{1}}^b[I+(-1)^{\bar c}A_{3,\mathbf{0}}]A_{3,\mathbf{1}}[I+(-1)^cA_{3,\mathbf{0}}]A_{2,\mathbf{1}}^b\\&[I+(-1)^bA_{2,\mathbf{0}}]A_{1,\mathbf{1}}^aV_S^\dagger[V_S(I+(-1)^aA_{1,\mathbf{0}})V_S^\dagger]\kappa\Big].\end{aligned}\tag{155}$$

Using Eq. (127) by replacing the state $I_2/2\otimes\alpha$ with $I_2^{\otimes 2}/4\otimes\tilde\alpha$ gives that Eq. (155) is approximately equal to

$$\begin{aligned}\frac{1}{64}\sum_{a,b,c}\mathrm{tr}\Big[&(I+(-1)^a\sigma_Z\otimes I_2^{\otimes 2}\otimes I)V_SA_{3,\mathbf{1}}[I+(-1)^aA_{1,\mathbf{0}}]A_{1,\mathbf{1}}^a[I+(-1)^bA_{2,\mathbf{0}}]A_{2,\mathbf{1}}^b[I+(-1)^{\bar c}A_{3,\mathbf{0}}]A_{3,\mathbf{1}}[I+(-1)^cA_{3,\mathbf{0}}]\\&A_{2,\mathbf{1}}^b[I+(-1)^bA_{2,\mathbf{0}}]V_S^\dagger[V_SA_{1,\mathbf{1}}^aV_S^\dagger]\kappa\Big].\end{aligned}\tag{156}$$

Also, using Eq. (126) by replacing the state $I_2/2\otimes\alpha$ with $I_2^{\otimes 2}/4\otimes\tilde\alpha$ derives the approximate relation of Eq. (156) as

$$\begin{aligned}\frac{1}{64}\sum_{a,b,c}\mathrm{tr}\Big[&(\sigma_X^a\otimes I_2^{\otimes 2}\otimes I)(I+(-1)^a\sigma_Z\otimes I_2^{\otimes 2}\otimes I)V_SA_{3,\mathbf{1}}[I+(-1)^aA_{1,\mathbf{0}}]A_{1,\mathbf{1}}^a[I+(-1)^bA_{2,\mathbf{0}}]A_{2,\mathbf{1}}^b[I+(-1)^{\bar c}A_{3,\mathbf{0}}]A_{3,\mathbf{1}}\\&[I+(-1)^cA_{3,\mathbf{0}}]A_{2,\mathbf{1}}^bV_S^\dagger V_S[I+(-1)^bA_{2,\mathbf{0}}]V_S^\dagger\kappa\Big].\end{aligned}$$

Next, from Eq. (152), we have

$$\begin{aligned}\approx_R\frac{1}{64}\sum_{a,b,c}\mathrm{tr}\Big[&(I+(-1)^bI_2\otimes\sigma_Z\otimes I_2\otimes I)(\sigma_X^a\otimes I_2^{\otimes 2}\otimes I)(I+(-1)^a\sigma_Z\otimes I_2^{\otimes 2}\otimes I)V_SA_{3,\mathbf{1}}[I+(-1)^aA_{1,\mathbf{0}}]A_{1,\mathbf{1}}^a\\&[I+(-1)^bA_{2,\mathbf{0}}]A_{2,\mathbf{1}}^b[I+(-1)^{\bar c}A_{3,\mathbf{0}}]A_{3,\mathbf{1}}[I+(-1)^cA_{3,\mathbf{0}}]V_S^\dagger[V_SA_{2,\mathbf{1}}^bV_S^\dagger]\kappa\Big].\end{aligned}\tag{157}$$

Since

$$I_2\otimes\sigma_X\otimes I_2\otimes I\approx_{R,\kappa}V_SA_{2,\mathbf{1}}V_S^\dagger,\tag{158}$$

which will be proven in Lemma 53 (iii) below, Eq. (157) is approximately equal to

$$\begin{aligned}\frac{1}{64}\sum_{a,b,c}\mathrm{tr}\Big[&(I_2\otimes\sigma_X^b\otimes I_2\otimes I)(I+(-1)^bI_2\otimes\sigma_Z\otimes I_2\otimes I)(\sigma_X^a\otimes I_2^{\otimes 2}\otimes I)(I+(-1)^a\sigma_Z\otimes I_2^{\otimes 2}\otimes I)\\&V_SA_{3,\mathbf{1}}[I+(-1)^aA_{1,\mathbf{0}}]A_{1,\mathbf{1}}^a[I+(-1)^bA_{2,\mathbf{0}}]A_{2,\mathbf{1}}^b[I+(-1)^{\bar c}A_{3,\mathbf{0}}]V_S^\dagger\left[V_SA_{3,\mathbf{1}}(I+(-1)^cA_{3,\mathbf{0}})V_S^\dagger\right]\kappa\Big].\end{aligned}$$

Using

$$V_S\{A_{3,\mathbf{1}},A_{3,\mathbf{0}}\}V_S^\dagger\approx_{R,\kappa}0,$$

which will be proven in Lemma 53 (iv) below, we have

$$\approx_R \frac{1}{64}\sum_{a,b,c}\mathrm{tr}\Big[(I_2\otimes\sigma_X^b\otimes I_2\otimes I)(I+(-1)^b I_2\otimes\sigma_Z\otimes I_2\otimes I)(\sigma_X^a\otimes I_2^{\otimes 2}\otimes I)(I+(-1)^a\sigma_Z\otimes I_2^{\otimes 2}\otimes I)$$
$$V_S A_{3,\mathbf{1}}[I+(-1)^a A_{1,\mathbf{0}}]A_{1,\mathbf{1}}^a[I+(-1)^b A_{2,\mathbf{0}}]A_{2,\mathbf{1}}^b[I+(-1)^{\bar{c}}A_{3,\mathbf{0}}]V_S^\dagger V_S[I+(-1)^{\bar{c}}A_{3,\mathbf{0}}]A_{3,\mathbf{1}}V_S^\dagger\kappa\Big].$$

Substituting $V_S^\dagger V_S = I$ and $\sum_c[I+(-1)^{\bar{c}}A_{3,\mathbf{0}}]^2 = 4I$ results in

$$=\frac{1}{16}\sum_{a,b}\mathrm{tr}\Big[(I_2\otimes\sigma_X^b\otimes I_2\otimes I)(I+(-1)^b I_2\otimes\sigma_Z\otimes I_2\otimes I)(\sigma_X^a\otimes I_2^{\otimes 2}\otimes I)(I+(-1)^a\sigma_Z\otimes I_2^{\otimes 2}\otimes I)$$
$$V_S A_{3,\mathbf{1}}[I+(-1)^a A_{1,\mathbf{0}}]A_{1,\mathbf{1}}^a[I+(-1)^b A_{2,\mathbf{0}}][A_{2,\mathbf{1}}^b A_{3,\mathbf{1}}]V_S^\dagger\kappa\Big].$$

The commutation relation $[A_{2,\mathbf{1}}, A_{3,\mathbf{1}}] = 0$ leads to

$$=\frac{1}{16}\sum_{a,b}\mathrm{tr}\Big[(I_2\otimes\sigma_X^b\otimes I_2\otimes I)(I+(-1)^b I_2\otimes\sigma_Z\otimes I_2\otimes I)(\sigma_X^a\otimes I_2^{\otimes 2}\otimes I)(I+(-1)^a\sigma_Z\otimes I_2^{\otimes 2}\otimes I)$$
$$V_S A_{3,\mathbf{1}}[I+(-1)^a A_{1,\mathbf{0}}]A_{1,\mathbf{1}}^a[I+(-1)^b A_{2,\mathbf{0}}]A_{3,\mathbf{1}}V_S^\dagger[V_S A_{2,\mathbf{1}}^b V_S^\dagger]\kappa\Big].$$

Using Eq. (158), this is approximately equal to

$$\frac{1}{16}\sum_{a,b}\mathrm{tr}\Big[(I_2\otimes\sigma_X^b\otimes I_2\otimes I)^2(I+(-1)^b I_2\otimes\sigma_Z\otimes I_2\otimes I)(\sigma_X^a\otimes I_2^{\otimes 2}\otimes I)(I+(-1)^a\sigma_Z\otimes I_2^{\otimes 2}\otimes I)$$
$$V_S A_{3,\mathbf{1}}[I+(-1)^a A_{1,\mathbf{0}}]A_{1,\mathbf{1}}^a V_S^\dagger[V_S(I+(-1)^b A_{2,\mathbf{0}})A_{3,\mathbf{1}}V_S^\dagger]\kappa\Big]$$
$$=\frac{1}{16}\sum_{a,b}\mathrm{tr}\Big[(I+(-1)^b I_2\otimes\sigma_Z\otimes I_2\otimes I)(\sigma_X^a\otimes I_2^{\otimes 2}\otimes I)(I+(-1)^a\sigma_Z\otimes I_2^{\otimes 2}\otimes I)$$
$$V_S A_{3,\mathbf{1}}[I+(-1)^a A_{1,\mathbf{0}}]A_{1,\mathbf{1}}^a V_S^\dagger[V_S(I+(-1)^b A_{2,\mathbf{0}})A_{3,\mathbf{1}}V_S^\dagger]\kappa\Big]. \tag{159}$$

Using

$$V_S[A_{3,\mathbf{1}}, A_{2,\mathbf{0}}]V_S^\dagger \approx_{R,\kappa} 0,$$

which will be proven in Lemma 53 (v) below, we have that Eq. (159) is approximately equal to

$$\frac{1}{16}\sum_{a,b}\mathrm{tr}\Big[(I+(-1)^b I_2\otimes\sigma_Z\otimes I_2\otimes I)(\sigma_X^a\otimes I_2^{\otimes 2}\otimes I)(I+(-1)^a\sigma_Z\otimes I_2^{\otimes 2}\otimes I)$$
$$V_S A_{3,\mathbf{1}}[I+(-1)^a A_{1,\mathbf{0}}]A_{1,\mathbf{1}}^a A_{3,\mathbf{1}}V_S^\dagger[V_S(I+(-1)^b A_{2,\mathbf{0}})V_S^\dagger]\kappa\Big].$$

Eq. (152) gives its approximate relation as

$$\frac{1}{16}\sum_{a,b}\mathrm{tr}\Big[(I+(-1)^b I_2\otimes\sigma_Z\otimes I_2\otimes I)^2(\sigma_X^a\otimes I_2^{\otimes 2}\otimes I)(I+(-1)^a\sigma_Z\otimes I_2^{\otimes 2}\otimes I)V_S A_{3,\mathbf{1}}[I+(-1)^a A_{1,\mathbf{0}}]A_{1,\mathbf{1}}^a A_{3,\mathbf{1}}V_S^\dagger\kappa\Big]$$
$$=\frac{1}{4}\sum_a\mathrm{tr}\left[(\sigma_X^a\otimes I_2^{\otimes 2}\otimes I)(I+(-1)^a\sigma_Z\otimes I_2^{\otimes 2}\otimes I)V_S A_{3,\mathbf{1}}[I+(-1)^a A_{1,\mathbf{0}}]A_{1,\mathbf{1}}^a A_{3,\mathbf{1}}V_S^\dagger\kappa\right].$$

The commutation relation $[A_{1,\mathbf{1}}, A_{3,\mathbf{1}}] = 0$ implies

$$=\frac{1}{4}\sum_a\mathrm{tr}\left[(\sigma_X^a\otimes I_2^{\otimes 2}\otimes I)(I+(-1)^a\sigma_Z\otimes I_2^{\otimes 2}\otimes I)V_S A_{3,\mathbf{1}}[I+(-1)^a A_{1,\mathbf{0}}]A_{3,\mathbf{1}}V_S^\dagger[V_S A_{1,\mathbf{1}}^a V_S^\dagger]\kappa\right].$$

Using Eq. (126) by replacing state $I_2/2\otimes\alpha$ with $I_2^{\otimes 2}/4\otimes\tilde{\alpha}$ leads to

$$\approx_R\frac{1}{4}\sum_a\mathrm{tr}\left[(\sigma_X^a\otimes I_2^{\otimes 2}\otimes I)^2(I+(-1)^a\sigma_Z\otimes I_2^{\otimes 2}\otimes I)V_S A_{3,\mathbf{1}}[I+(-1)^a A_{1,\mathbf{0}}]A_{3,\mathbf{1}}V_S^\dagger\kappa\right]$$
$$=\frac{1}{4}\sum_a\mathrm{tr}\left[(I+(-1)^a\sigma_Z\otimes I_2^{\otimes 2}\otimes I)V_S A_{3,\mathbf{1}}V_S^\dagger[V_S(I+(-1)^a A_{1,\mathbf{0}})A_{3,\mathbf{1}}V_S^\dagger]\kappa\right]. \tag{160}$$

Next, we have

$$V_S[A_{3,\mathbf{1}}, A_{1,\mathbf{0}}]V_S^\dagger \approx_{R,\kappa} 0,$$

which will be proven in Lemma 53 (v) below, Eq. (160) is approximately equal to

$$\begin{aligned}&\frac{1}{4}\sum_a \mathrm{tr}\left[(I+(-1)^a\sigma_Z\otimes I_2^{\otimes 2}\otimes I)V_S A_{3,\mathbf{1}}^2[I+(-1)^a A_{1,\mathbf{0}}]V_S^\dagger\kappa\right]\\ =&\frac{1}{4}\sum_a \mathrm{tr}\left[(I+(-1)^a\sigma_Z\otimes I_2^{\otimes 2}\otimes I)[V_S(I+(-1)^a A_{1,\mathbf{0}})V_S^\dagger]\kappa\right]. \end{aligned} \tag{161}$$

Finally, using Eq. (127) by replacing the state $I_2/2\otimes\alpha$ with $I_2^{\otimes 2}/4\otimes\tilde{\alpha}$ gives the approximate relation of Eq. (161) as

$$\frac{1}{4}\sum_a \mathrm{tr}\left[(I+(-1)^a\sigma_Z\otimes I_2^{\otimes 2}\otimes I)^2\kappa\right] = \mathrm{tr}(\kappa) = 1,$$

which ends the proof. ■

Lemma 53 *(Auxiliary lemma in proving Lemma 52) In this lemma, we define* $\kappa := I_2^{\otimes 2}/4\otimes\tilde{\alpha}$.
(i)

$$V_S[I+(-1)^b A_{2,\mathbf{0}}]V_S^\dagger \approx_{R,\kappa} I+(-1)^b I_2\otimes\sigma_Z\otimes I_2\otimes I$$

(ii) For $i\in\{1,2\}$,

$$V_S[A_{3,\mathbf{0}}, A_{i,\mathbf{1}}]V_S^\dagger \approx_{R,\kappa} 0.$$

(iii)

$$I_2\otimes\sigma_X\otimes I_2\otimes I \approx_{R,\kappa} V_S A_{2,\mathbf{1}}V_S^\dagger$$

(iv)

$$V_S\{A_{3,\mathbf{1}}, A_{3,\mathbf{0}}\}V_S^\dagger \approx_{R,\kappa} 0$$

(v) For $i\in\{1,2\}$,

$$V_S[A_{3,\mathbf{1}}, A_{i,\mathbf{0}}]V_S^\dagger \approx_{R,\kappa} 0.$$

(vi) Trivial extension of Eq. (127):

$$I+(-1)^a\sigma_Z\otimes I_2\otimes I_2\otimes I \approx_{R,\kappa} V_S(I+(-1)^a A_{1,\mathbf{0}})V_S^\dagger.$$

(vii) Trivial extension of Eq. (126):

$$\sigma_X\otimes I_2\otimes I_2\otimes I \approx_{R,\kappa} V_S A_{1,\mathbf{1}}V_S^\dagger.$$

Note that (i) and (ii) are used to prove Eq. (146), while (iii)-(vii) are used to prove Eq. (147).
Proof of (i) From the triangle inequality of the state dependent norm, it suffices to prove the following.

$$V_S V_S^\dagger \approx_{R,\kappa} I, \tag{162}$$

$$V_S A_{2,\mathbf{0}}V_S^\dagger \approx_{R,\kappa} I_2\otimes\sigma_Z\otimes I_2\otimes I. \tag{163}$$

Eq. (162) can be proven by $V_S V_S^\dagger \approx_{0,V_S\rho^{(\boldsymbol{\theta})}V_S^\dagger} I$ and by replacing $V_S\rho^{(\boldsymbol{\theta})}V_S^\dagger$ with κ, which is guaranteed by Corollary 51 and Lemma 21 (vi). Regarding the proof of Eq. (163), by combining Lemmas 47 and 19, we obtain

$$V_S A_{2,\mathbf{0}}V_S^\dagger \approx_{R,V_S\rho^{(\boldsymbol{\theta})}V_S^\dagger} I_2\otimes\sigma_Z\otimes I_2\otimes I.$$

By replacing $V_S\rho^{(\boldsymbol{\theta})}V_S^\dagger$ with κ using Corollary 51 and Lemma 21 (vi) gives the desired relation.
Proof of (ii) From the definition of the state dependent norm, we have

$$\mathrm{tr}\left[(V_S[A_{3,\mathbf{0}},A_{i,\mathbf{1}}]V_S^\dagger)^\dagger(V_S[A_{3,\mathbf{0}},A_{i,\mathbf{1}}]V_S^\dagger)\kappa\right]=\mathrm{tr}\left([A_{3,\mathbf{0}},A_{i,\mathbf{1}}]^\dagger[A_{3,\mathbf{0}},A_{i,\mathbf{1}}]V_S^\dagger\kappa V_S\right).$$

Using Eq. (149) and Lemma 21 (iii), the state in the trace can be replaced with $\rho^{(\boldsymbol{\theta})}$ as

$$\begin{aligned}&\approx_R \mathrm{tr}([A_{3,\mathbf{0}},A_{i,\mathbf{1}}]^\dagger[A_{3,\mathbf{0}},A_{i,\mathbf{1}}]\rho^{(\boldsymbol{\theta})})\\&\approx_R 0,\end{aligned}$$

where the second approximate equality comes from the approximate commutation relation in Lemma 41.
Proof of (iii) We start from using Lemmas 47 and 19:

$$I_2\otimes\sigma_X\otimes I_2\otimes I\approx_{R,V_S\rho^{(\boldsymbol{\theta})}V_S^\dagger}V_SA_{2,\mathbf{1}}V_S^\dagger. \tag{164}$$

Thanks to Corollary 51 and Lemma 21 (ii), the state $V_S\rho^{(\boldsymbol{\theta})}V_S^\dagger$ in Eq. (164) can be replaced with κ.
Proof of (iv) From the definition of the state dependent norm, we have

$$\mathrm{tr}\left[(V_S\{A_{3,\mathbf{1}},A_{3,\mathbf{0}}\}V_S^\dagger)^\dagger(V_S\{A_{3,\mathbf{1}},A_{3,\mathbf{0}}\}V_S^\dagger)\kappa\right]=\mathrm{tr}\left[\{A_{3,\mathbf{1}},A_{3,\mathbf{0}}\}^\dagger\{A_{3,\mathbf{1}},A_{3,\mathbf{0}}\}V_S^\dagger\kappa V_S\right].$$

By using Eq. (149) and Lemma 21(iv), we can replace $V_S^\dagger\kappa V_S$ in the trace with $\rho^{(\boldsymbol{\theta})}$ as

$$\begin{aligned}&\approx_R \mathrm{tr}\left[\{A_{3,\mathbf{1}},A_{3,\mathbf{0}}\}^\dagger\{A_{3,\mathbf{1}},A_{3,\mathbf{0}}\}\rho^{(\boldsymbol{\theta})}\right]\\&\approx_R 0,\end{aligned}$$

where the second approximate equation is from Proposition 32.
Proof of (v) The proof can be done by following the same arguments in proving Lemma 53 (ii).
Proof of (vi) Following the same arguments done in the proof of Eq. (127) by replacing $I_2/2\otimes\alpha$ with κ gives (vi).
Proof of (vii) Following the same arguments done in the proof of Eq. (126) by replacing $I_2/2\otimes\alpha$ with κ gives (vii).

I. Approximate relations of tilde observables and Pauli observables

In Sec. V H, we have proven that the non-tilde observables $A_{i,\mathbf{0}}$ and $A_{i,\mathbf{1}}$ for $i\in\{1,2,3\}$ are approximately equal to the Pauli observables under the swap isometry V_S. In this section, we prove that the tilde observables, introduced in Eq. (6), are also approximately equal to the Pauli observables. For this, we first prove that the tilde observables are approximately equal to the non-tilde ones.

Lemma 54 *For any efficient perfect device $D=(S,\Pi,M,P)$, we have for any $\boldsymbol{\theta}\in\mathcal{B}$,*

$$\begin{aligned}&\forall q_2q_3\in\{01,10,11\},\quad A_{1,0q_2q_3}\approx_{\gamma_T(D),\rho^{(\boldsymbol{\theta})}}A_{1,\mathbf{0}},\\&\forall q_2q_3\in\{00,01,10\},\quad A_{1,1q_2q_3}\approx_{\gamma_T(D),\rho^{(\boldsymbol{\theta})}}A_{1,\mathbf{1}},\\&\forall q_1q_3\in\{01,10,11\},\quad A_{2,q_10q_3}\approx_{\gamma_T(D),\rho^{(\boldsymbol{\theta})}}A_{2,\mathbf{0}},\\&\forall q_1q_3\in\{00,01,10\},\quad A_{2,q_11q_3}\approx_{\gamma_T(D),\rho^{(\boldsymbol{\theta})}}A_{2,\mathbf{1}},\\&\forall q_1q_2\in\{01,10,11\},\quad A_{3,q_1q_20}\approx_{\gamma_T(D),\rho^{(\boldsymbol{\theta})}}A_{3,\mathbf{0}},\\&\forall q_1q_2\in\{00,01,10\},\quad A_{3,q_1q_21}\approx_{\gamma_T(D),\rho^{(\boldsymbol{\theta})}}A_{3,\mathbf{1}}.\end{aligned}$$

(Proof) We prove $A_{1,001}\approx_{\gamma_T(D),\rho^{(\boldsymbol{\theta})}}A_{1,\mathbf{0}}$. The others can be proven analogously. Once we prove

$$A_{1,001}\approx_{\gamma_T(D),\rho^{(000)}}A_{1,\mathbf{0}}, \tag{165}$$

Lemma 21 (ii) implies $A_{1,001}\approx_{\gamma_T(D),\rho^{(\boldsymbol{\theta})}}A_{1,\mathbf{0}}$ for any $\boldsymbol{\theta}\in\mathcal{B}$. The conditions of Lemma 21 (ii) are guaranteed by the computational indistinguishability of $\rho^{(\boldsymbol{\theta})}$ in Lemma 31 and by the fact that $A_{1,001}$ and $A_{1,\mathbf{0}}$ are efficient binary

observables. Therefore, it suffices to show Eq. (165). Moreover, thanks to Lemma 13 (ii), the proof is reduced to showing

$$A_{1,001} \approx_{\gamma_T(D),\sigma^{(0,v_1;0,v_2;0,v_3)}} A_{1,\mathbf{0}}.$$

From the definition of $\gamma_T(D)$ in Eq. (12) and Corollary 28, we have

$$A_{1,001} \approx_{\gamma_T(D),\sigma^{(0,v_1;0,v_2;0,v_3)}} (-1)^{v_1} I, \quad A_{1,\mathbf{0}} \approx_{\gamma_T(D),\sigma^{(0,v_1;0,v_2;0,v_3)}} (-1)^{v_1} I$$

for any $\boldsymbol{v} \in \{0,1\}^3$. Hence, the triangle inequality of the state dependent norm results in

$$A_{1,001} \approx_{\gamma_T(D),\sigma^{(0,v_1;0,v_2;0,v_3)}} A_{1,\mathbf{0}},$$

which ends the proof. ■

By using this lemma, the tilde observables are shown to be approximately equal to the Pauli observables.

Corollary 55 *(Approximate relation of tilde-observables and Pauli observables) For any efficient perfect device $D = (S, \Pi, M, P)$, we have the following for any $\boldsymbol{\theta} \in \mathcal{B}$,*

$$\forall q_2 q_3 \in \{01, 10, 11\}, \quad A_{1,0q_2q_3} \approx_{R,\rho^{(\boldsymbol{\theta})}} V_S^\dagger(\sigma_Z \otimes I_2 \otimes I_2 \otimes I) V_S, \tag{166}$$

$$\forall q_2 q_3 \in \{00, 01, 10\}, \quad A_{1,1q_2q_3} \approx_{R,\rho^{(\boldsymbol{\theta})}} V_S^\dagger(\sigma_X \otimes I_2 \otimes I_2 \otimes I) V_S, \tag{167}$$

$$\forall q_1 q_3 \in \{01, 10, 11\}, \quad A_{2,q_1 0q_3} \approx_{R,\rho^{(\boldsymbol{\theta})}} V_S^\dagger(I_2 \otimes \sigma_Z \otimes I_2 \otimes I) V_S, \tag{168}$$

$$\forall q_1 q_3 \in \{00, 01, 10\}, \quad A_{2,q_1 1q_3} \approx_{R,\rho^{(\boldsymbol{\theta})}} V_S^\dagger(I_2 \otimes \sigma_X \otimes I_2 \otimes I) V_S, \tag{169}$$

$$\forall q_1 q_2 \in \{01, 10, 11\}, \quad A_{3,q_1q_20} \approx_{R,\rho^{(\boldsymbol{\theta})}} V_S^\dagger(I_2 \otimes I_2 \otimes \sigma_Z \otimes I) V_S, \tag{170}$$

$$\forall q_1 q_2 \in \{00, 01, 10\}, \quad A_{3,q_1q_21} \approx_{R,\rho^{(\boldsymbol{\theta})}} V_S^\dagger(I_2 \otimes I_2 \otimes \sigma_X \otimes I) V_S. \tag{171}$$

(Proof) Eqs. (166)-(171) can be proven by combining Lemma 54, the triangle inequality of the state dependent norm, and respectively with Eqs. (94), (100), (121), (122), (146) and (147). ■

J. Approximate relations of joint observables and products of Pauli observables

We have shown so far that any single non-tilde observable and any single tilde one are approximately equal to the Pauli observable in Secs. V H and V I, respectively. Our next goal is to prove that the joint observables such as $A_{1,\mathbf{0}} A_{2,\mathbf{0}} A_{3,\mathbf{0}}$ are approximately equal to the products of Pauli observables under the swap isometry V_S. These relations will be shown in Lemmas 59, 60 and 61, which are the crux of proving our main result, Theorem 62. To derive these relations, we first prepare the extended statements of Lemmas 49 and 50 and Corollary 51 in Lemmas 56 and 57 and Corollary 58, respectively.

Lemma 56 *(Extension of Lemma 49) For any efficient and perfect device $D = (S, \Pi, M, P)$, we have for any $\boldsymbol{v} \in \{0,1\}^3$, there exists positive matrices $\tilde{\tilde{\alpha}}^{(0,v_1;0,v_2;0,v_3)}$, $\tilde{\tilde{\alpha}}^{(0,v_1;0,v_2;1,v_3)}$, $\tilde{\tilde{\alpha}}^{(0,v_1;1,v_2;0,v_3)}$ and $\tilde{\tilde{\alpha}}^{(1,v_1;0,v_2;0,v_3)}$ such that the following holds.*

$$\text{(i) } V_S \sigma^{(0,v_1;0,v_2;0,v_3)} V_S^\dagger \approx_R |v_1\rangle\langle v_1| \otimes |v_2\rangle\langle v_2| \otimes |v_3\rangle\langle v_3| \otimes \tilde{\tilde{\alpha}}^{(0,v_1;0,v_2;0,v_3)} \tag{172}$$

$$\text{(ii) } V_S \sigma^{(0,v_1;0,v_2;1,v_3)} V_S^\dagger \approx_R |v_1\rangle\langle v_1| \otimes |v_2\rangle\langle v_2| \otimes |(-)^{v_3}\rangle\langle(-)^{v_3}| \otimes \tilde{\tilde{\alpha}}^{(0,v_1;0,v_2;1,v_3)} \tag{173}$$

$$\text{(iii) } V_S \sigma^{(0,v_1;1,v_2;0,v_3)} V_S^\dagger \approx_R |v_1\rangle\langle v_1| \otimes |(-)^{v_2}\rangle\langle(-)^{v_2}| \otimes |v_3\rangle\langle v_3| \otimes \tilde{\tilde{\alpha}}^{(0,v_1;1,v_2;0,v_3)}$$

$$\text{(iv) } V_S \sigma^{(1,v_1;0,v_2;0,v_3)} V_S^\dagger \approx_R |(-)^{v_1}\rangle\langle(-)^{v_1}| \otimes |v_2\rangle\langle v_2| \otimes |v_3\rangle\langle v_3| \otimes \tilde{\tilde{\alpha}}^{(1,v_1;0,v_2;0,v_3)} \tag{174}$$

(Proof) By following the same arguments done in the proof of Lemma 49, we prove (iv). The others can be shown analogously. First, from Lemma 52 we have

$$A_{3,\mathbf{0}} \approx_{R,\rho^{(100)}} V_S^\dagger(I_2^{\otimes 2} \otimes \sigma_Z \otimes I) V_S,$$

and from Lemma 13 (ii), this implies

$$A_{3,\mathbf{0}} \approx_{R,\sigma^{(1,v_1;0,v_2;0,v_3)}} V_S^\dagger(I_2^{\otimes 2} \otimes \sigma_Z \otimes I) V_S.$$

Using Lemma 20 leads to

$$A_{3,\mathbf{0}}^{(v_3)} \approx_{R,\sigma^{(1,v_1;0,v_2;0,v_3)}} V_S^\dagger (I_2^{\otimes 2} \otimes |v_3\rangle\langle v_3| \otimes I) V_S.$$

From Lemma 17 (i), we have

$$\sum_{\boldsymbol{v}} \mathrm{tr}\left[A_{3,\mathbf{0}}^{(v_3)} \sigma^{(1,v_1;0,v_2;0,v_3)}\right] \approx_R \sum_{\boldsymbol{v}} \mathrm{tr}\left[V_S^\dagger (I_2^{\otimes 2} \otimes |v_3\rangle\langle v_3| \otimes I) V_S \sigma^{(1,v_1;0,v_2;0,v_3)}\right]. \tag{175}$$

We find that the LHS is approximately equal to 1 from Lemma 40 and the definition of $\gamma_T(D)$ in Eq. (12), namely

$$\sum_{\boldsymbol{v}} \mathrm{tr}\left[A_{3,\mathbf{0}}^{(v_3)} \sigma^{(1,v_1;0,v_2;0,v_3)}\right] \approx_0 \sum_{\boldsymbol{v}} \mathrm{tr}\left[A_{3,\mathbf{0}}^{(v_3)} \sigma^{(0,v_1;0,v_2;0,v_3)}\right] \approx_R 1.$$

Hence, the RHS of Eq. (175) is also approximately equal to 1:

$$\sum_{\boldsymbol{v}} \mathrm{tr}\left[V_S^\dagger (I_2^{\otimes 2} \otimes |v_3\rangle\langle v_3| \otimes I) V_S \sigma^{(1,v_1;0,v_2;0,v_3)}\right] \approx_R 1.$$

By applying Corollary 28 and Lemma 16, this implies

$$I_2^{\otimes 2} \otimes |v_3\rangle\langle v_3| \otimes I \approx_{R, V_S \sigma^{(1,v_1;0,v_2;0,v_3)} V_S^\dagger} I.$$

From Lemma 49, $V_S\sigma^{(1,v_1;0,v_2;0,v_3)}V_S^\dagger$ is close to $|(-)^{v_1}\rangle\langle(-)^{v_1}| \otimes |v_2\rangle\langle v_2| \otimes \tilde{\alpha}^{(1,v_1;0,v_2;0,v_3)}$, and Lemma 17 (ii) enables us to replace these states. In doing so, we obtain

$$I_2^{\otimes 2} \otimes |v_3\rangle\langle v_3| \otimes I \approx_{R, |(-)^{v_1}\rangle\langle(-)^{v_1}| \otimes |v_2\rangle\langle v_2| \otimes \tilde{\alpha}^{(1,v_1;0,v_2;0,v_3)}} I.$$

By combining this with

$$\text{Lemma 49}: \quad V_S\sigma^{(1,v_1;0,v_2;0,v_3)}V_S^\dagger \approx_R |(-)^{v_1}\rangle\langle(-)^{v_1}| \otimes |v_2\rangle\langle v_2| \otimes \tilde{\alpha}^{(1,v_1;0,v_2;0,v_3)}$$

and Lemma 18, we finally obtain

$$\begin{aligned} V_S\sigma^{(1,v_1;0,v_2;0,v_3)}V_S^\dagger &\approx_R I[|(-)^{v_1}\rangle\langle(-)^{v_1}| \otimes |v_2\rangle\langle v_2| \otimes \tilde{\alpha}^{(1,v_1;0,v_2;0,v_3)}]I \\ &\approx_R (I_2^{\otimes 2} \otimes |v_3\rangle\langle v_3| \otimes I)[|(-)^{v_1}\rangle\langle(-)^{v_1}| \otimes |v_2\rangle\langle v_2| \otimes \tilde{\alpha}^{(1,v_1;0,v_2;0,v_3)}](I_2^{\otimes 2} \otimes |v_3\rangle\langle v_3| \otimes I) \\ &= |(-)^{v_1}\rangle\langle(-)^{v_1}| \otimes |v_2\rangle\langle v_2| \otimes |v_3\rangle\langle v_3| \otimes \tilde{\tilde{\alpha}}^{(1,v_1;0,v_2;0,v_3)}, \end{aligned}$$

where we define $\tilde{\tilde{\alpha}}^{(1,v_1;0,v_2;0,v_3)} := (\langle v_3| \otimes I)\tilde{\alpha}^{(1,v_1;0,v_2;0,v_3)}(|v_3\rangle \otimes I)$. ■

Using Lemma 56, we next show the lemma that is an extension of Lemma 50.

Lemma 57 *(Extension of Lemma 50) Let $D = (S, \Pi, M, P)$ be an efficient perfect device. There exists a normalized state $\tilde{\tilde{\alpha}}$ such that the following holds for any $\boldsymbol{v} \in \{0,1\}^3$.*

$$\text{(i)}\ V_S\sigma^{(0,v_1;0,v_2;0,v_3)}V_S^\dagger \overset{c}{\approx}_R \frac{|v_1\rangle\langle v_1| \otimes |v_2\rangle\langle v_2| \otimes |v_3\rangle\langle v_3|}{8} \otimes \tilde{\tilde{\alpha}} \tag{176}$$

$$\text{(ii)}\ V_S\sigma^{(0,v_1;0,v_2;1,v_3)}V_S^\dagger \overset{c}{\approx}_R \frac{|v_1\rangle\langle v_1| \otimes |v_2\rangle\langle v_2| \otimes |(-)^{v_3}\rangle\langle(-)^{v_3}|}{8} \otimes \tilde{\tilde{\alpha}} \tag{177}$$

$$\text{(iii)}\ V_S\sigma^{(0,v_1;1,v_2;0,v_3)}V_S^\dagger \overset{c}{\approx}_R \frac{|v_1\rangle\langle v_1| \otimes |(-)^{v_2}\rangle\langle(-)^{v_2}| \otimes |v_3\rangle\langle v_3|}{8} \otimes \tilde{\tilde{\alpha}} \tag{178}$$

$$\text{(iv)}\ V_S\sigma^{(1,v_1;0,v_2;0,v_3)}V_S^\dagger \overset{c}{\approx}_R \frac{|(-)^{v_1}\rangle\langle(-)^{v_1}| \otimes |v_2\rangle\langle v_2| \otimes |v_3\rangle\langle v_3|}{8} \otimes \tilde{\tilde{\alpha}} \tag{179}$$

(Proof) The proof is similar to the one of Lemma 50, but we give the full proof for completeness. We first prove (iii), and by using (iii), we prove the rest of the relations. To prove (iii), we need to show that $\{\tilde{\tilde{\alpha}}^{(0,v_1;1,v_2;0,v_3)}\}_{v_1,v_2,v_3}$ are computationally indistinguishable. For this, we already have shown in Lemma 50 that $\{\sum_{v_3} \tilde{\alpha}^{(0,v_1;1,v_2;0,v_3)}\}_{v_2}$ are computationally indistinguishable for any v_1, and by considering Lemmas 49 and 56, this implies that $\{\sum_{v_3} \tilde{\tilde{\alpha}}^{(0,v_1;1,v_2;0,v_3)}\}_{v_2}$

are also computationally indistinguishable for any v_1. Therefore, the remaining task is to prove that $\{\tilde{\tilde{\alpha}}^{(0,v_1;1,v_2;0,v_3)}\}_{v_3}$ are computationally indistinguishable for any fixed v_1 and v_2.

In the following discussions, we fix v_1 and v_2. From Lemma 56, there exists a $d>0$ such that for any v_1,v_2,v_3,

$$\left|\left|V_S\sigma^{(0,v_1;1,v_2;0,v_3)}V_S^\dagger-|v_1\rangle\langle v_1|\otimes|(-)^{v_2}\rangle\langle(-)^{v_2}|\otimes|v_3\rangle\langle v_3|\otimes\tilde{\tilde{\alpha}}^{(0,v_1;1,v_2;0,v_3)}\right|\right|_1^2\leq\epsilon, \tag{180}$$

$$\left|\left|V_S\sigma^{(0,v_1;0,v_2;1,v_3)}V_S^\dagger-|v_1\rangle\langle v_1|\otimes|v_2\rangle\langle v_2|\otimes|(-)^{v_3}\rangle\langle(-)^{v_3}|\otimes\tilde{\tilde{\alpha}}^{(0,v_1;0,v_2;1,v_3)}\right|\right|_1^2\leq\epsilon \tag{181}$$

hold with $\epsilon:=O(\gamma_T(D)^d)$. From Lemmas 49 and 56, we have that

$$\left|\mathrm{tr}\left[M_0\sum_{v_3'}\tilde{\tilde{\alpha}}^{(0,v_1;1,v_2=0;0,v_3')}\right]-\mathrm{tr}\left[M_0\sum_{v_3'}\tilde{\tilde{\alpha}}^{(0,v_1;1,v_2=1;0,v_3')}\right]\right|\leq 2\sqrt{\epsilon} \tag{182}$$

holds for any v_1 and any efficient measurement $M:=\{M_0,M_1\}$.

For the sake of contradiction, we assume that there exists a POVM $\Lambda:=\{\Lambda_0,\Lambda_1\}$ with $\Lambda_0+\Lambda_1=I$ such that

$$\left|\mathrm{tr}\left[\Lambda_0\tilde{\tilde{\alpha}}^{(0,v_1;1,v_2;0,v_3=0)}\right]-\mathrm{tr}\left[\Lambda_0\tilde{\tilde{\alpha}}^{(0,v_1;1,v_2;0,v_3=1)}\right]\right|\geq 2\mu(\lambda)+42\sqrt{\epsilon} \tag{183}$$

holds with a non-negligible function $\mu(\lambda)$. Under the existence of this POVM, we can construct an adversary $\mathcal{A}$ that breaks the injective invariance property in Definition 4 using an efficient measurement $\{\Gamma,I-\Gamma\}$ with

$$\Gamma:=V_S^\dagger(|v_1\rangle\langle v_1|\otimes|(-)^{v_2}\rangle\langle(-)^{v_2}|\otimes|0\rangle\langle 0|\otimes\Lambda_0)V_S.$$

Below, we describe the procedure of $\mathcal{A}$ that breaks the injective invariance property.

$\mathcal{A}$ is given keys (k_2,k_3), and the task is to distinguish whether the input is $(\theta_2,\theta_3)=(0,1)$ or $(\theta_2,\theta_3)=(1,0)$. For this, $\mathcal{A}$ samples the other key and a trapdoor $(k_1,t_{k_1})\leftarrow\mathsf{GEN}_{\mathcal{G}}(1^\lambda)$, prepares the state $\psi^{(\boldsymbol{\theta})}$ by performing the same operations as the device D, measures the Y-register to obtain $\boldsymbol{y}$, followed by measuring the R-register to obtain $\boldsymbol{d}$. At this moment, $\mathcal{A}$ prepares the state $\rho^{(\boldsymbol{\theta})}$. Finally, $\mathcal{A}$ performs the measurement $\{\Gamma,I-\Gamma\}$. This procedure is efficient because the device D and the POVM $\{\Gamma,I-\Gamma\}$ are efficient. In this procedure, we calculate the distinguishing advantage Adv in obtaining the outcome corresponding to Γ for the states $\rho^{(010)}$ and $\rho^{(001)}$. Once we show that this advantage is non-negligible under Eq. (183), this contradicts the injective invariance property. Hence, by taking a contraposition, we obtain the negation of Eq. (183), which is the required statement in the proof. By this discussion, we only need to prove that the advantage Adv is non-negligible from Eq. (183), which is shown below.

First, by the definitions of Γ and $\rho^{(\boldsymbol{\theta})}$, we have

$$\begin{aligned}\mathrm{Adv}:=&|\mathrm{tr}[\Gamma(\rho^{(010)}-\rho^{(001)})]|\\ =&\left|\mathrm{tr}\left[(|v_1\rangle\langle v_1|\otimes|(-)^{v_2}\rangle\langle(-)^{v_2}|\otimes|0\rangle\langle 0|\otimes\Lambda_0)\left(\sum_{\boldsymbol{v}'}V_S\sigma^{(0,v_1';1,v_2';0,v_3')}V_S^\dagger-\sum_{\boldsymbol{v}'}V_S\sigma^{(0,v_1';0,v_2';1,v_3')}V_S^\dagger\right)\right]\right|.\end{aligned} \tag{184}$$

By applying Eq. (116) with Eqs. (180) and (181), we have

$$\begin{aligned}
\mathrm{Adv} \geq & \Big| \sum_{\boldsymbol{v}' \in \{0,1\}^3} \mathrm{tr}\Big[(|v_1\rangle\langle v_1| \otimes |(-)^{v_2}\rangle\langle(-)^{v_2}| \otimes |0\rangle\langle 0| \otimes \Lambda_0)\Big(|v_1'\rangle\langle v_1'| \otimes |(-)^{v_2'}\rangle\langle(-)^{v_2'}| \otimes |v_3'\rangle\langle v_3'| \otimes \tilde{\tilde{\alpha}}^{(0,v_1';1,v_2';0,v_3')} \\
& - |v_1'\rangle\langle v_1'| \otimes |v_2'\rangle\langle v_2'| \otimes |(-)^{v_3'}\rangle\langle(-)^{v_3'}| \otimes \tilde{\tilde{\alpha}}^{(0,v_1';0,v_2';1,v_3')} \Big) \Big] \Big| - 16\sqrt{\epsilon} \\
= & \left| \mathrm{tr}\left[\Lambda_0 \tilde{\tilde{\alpha}}^{(0,v_1;1,v_2;0,0)} \right] - \frac{1}{4} \sum_{v_2',v_3'} \mathrm{tr}\left[\Lambda_0 \tilde{\tilde{\alpha}}^{(0,v_1;0,v_2';1,v_3')} \right] \right| - 16\sqrt{\epsilon} \\
= & \left| \frac{1}{2} \mathrm{tr}\left[\Lambda_0 (\tilde{\tilde{\alpha}}^{(0,v_1;1,v_2;0,0)} - \tilde{\tilde{\alpha}}^{(0,v_1;1,v_2;0,1)}) \right] + \frac{1}{2} \sum_{v_3'} \mathrm{tr}[\Lambda_0 \tilde{\tilde{\alpha}}^{(0,v_1;1,v_2;0,v_3')}] - \frac{1}{4} \sum_{v_2',v_3'} \mathrm{tr}\left[\Lambda_0 \tilde{\tilde{\alpha}}^{(0,v_1;0,v_2';1,v_3')} \right] \right| - 16\sqrt{\epsilon} \\
\geq & \mu(\lambda) + 5\sqrt{\epsilon} - \frac{1}{2} \left| \sum_{v_3'} \mathrm{tr}[\Lambda_0 \tilde{\tilde{\alpha}}^{(0,v_1;1,v_2;0,v_3')}] - \frac{1}{2} \sum_{v_2',v_3'} \mathrm{tr}\left[\Lambda_0 \tilde{\tilde{\alpha}}^{(0,v_1;0,v_2';1,v_3')} \right] \right| \\
\geq & \mu(\lambda) + 5\sqrt{\epsilon} - \frac{1}{2} \Bigg[\left| \sum_{v_3'} \mathrm{tr}[\Lambda_0 \tilde{\tilde{\alpha}}^{(0,v_1;1,v_2;0,v_3')}] - \frac{1}{2} \sum_{v_2',v_3'} \mathrm{tr}\left[\Lambda_0 \tilde{\tilde{\alpha}}^{(0,v_1;1,v_2';0,v_3')} \right] \right| \\
& + \left| \frac{1}{2} \sum_{v_2',v_3'} \mathrm{tr}\left[\Lambda_0 \tilde{\tilde{\alpha}}^{(0,v_1;1,v_2';0,v_3')} \right] - \frac{1}{2} \sum_{v_2',v_3'} \mathrm{tr}\left[\Lambda_0 \tilde{\tilde{\alpha}}^{(0,v_1;0,v_2';1,v_3')} \right] \right| \Bigg] \\
\geq & \mu(\lambda) + 4\sqrt{\epsilon} - \frac{1}{4} \left| \sum_{v_2',v_3'} \mathrm{tr}\left[\Lambda_0 \left(\tilde{\tilde{\alpha}}^{(0,v_1;1,v_2';0,v_3')} - \tilde{\tilde{\alpha}}^{(0,v_1;0,v_2';1,v_3')} \right) \right] \right| \\
= & \mu(\lambda) + 4\sqrt{\epsilon} \\
& - \frac{1}{4} \left| \sum_{v_2',v_3'} \mathrm{tr}\left[\Lambda_0 \left\{ |v_1\rangle\langle v_1| \otimes \left(|(-)^{v_2'}\rangle\langle(-)^{v_2'}| \otimes |v_3'\rangle\langle v_3'| \otimes \tilde{\tilde{\alpha}}^{(0,v_1;1,v_2';0,v_3')} - |v_2\rangle\langle v_2| \otimes |(-)^{v_3'}\rangle\langle(-)^{v_3'}| \otimes \tilde{\alpha}^{(0,v_1;0,v_2';1,v_3')} \right\} \right) \right] \right|,
\end{aligned}$$

where we use the triangle inequality and Eq. (183) in the second inequality, the third one follows from the triangle inequality, and the fourth one comes from Eq. (182). Again, by applying Eq. (116) with Eqs. (180) and (181), we obtain

$$\mathrm{Adv} \geq \mu(\lambda) - \frac{1}{4} \left| \mathrm{tr}\left[\Lambda_0 \left(\sum_{v_2',v_3'} V_S \sigma^{(0,v_1;1,v_2';0,v_3')} V_S^\dagger - \sum_{v_2',v_3'} V_S \sigma^{(0,v_1;0,v_2';1,v_3')} V_S^\dagger \right) \right] \right|.$$

Finally, by Eqs. (15), (16) and $\rho^{(\boldsymbol{\theta})} := \sum_{\boldsymbol{v}} \sigma^{(\theta_1,v_1;\theta_2,v_2;\theta_3,v_3)}$, this is equal to

$$\mu(\lambda) - \frac{1}{4} \left| \mathrm{tr}\left[W \left(\rho^{(010)} - \rho^{(001)} \right) \right] \right|$$

with

$$W := \sum_{y_1 : \hat{b}(k_1,y_1) = v_1} |y_1\rangle\langle y_1| V_S^\dagger \Lambda_0 V_S \sum_{y_1 : \hat{b}(k_1,y_1) = v_1} |y_1\rangle\langle y_1|.$$

The measurement $\{W, I - W\}$ is efficient since $\mathcal{A}$ has the information of the trapdoor t_{k_1} and computing $\hat{b}(k_1, y_1)$ is efficient. Hence, the computational indistinguishability in Lemma 31 reveals that the second term is $\mathrm{negl}(\lambda)$. Therefore, we conclude

$$\mathrm{Adv} \geq \mu(\lambda) - \mathrm{negl}(\lambda),$$

which contradicts Lemma 31 and completes the proof of Eq. (178).

Next, we prove Eqs. (176), (177) and (179) using Eq. (178). First, from Eq. (178), we have

$$\sum_{\boldsymbol{v}} V_S \sigma^{(0,v_1;1,v_2;0,v_3)} V_S^\dagger \overset{c}{\approx}_R \frac{I_2^{\otimes 3}}{8} \otimes \tilde{\tilde{\alpha}}.$$

Since $\rho^{(\boldsymbol{\theta})}$ are computationally indistinguishable from Lemma 31 and the isometry V_S is efficient, we also obtain

$$\sum_{\boldsymbol{v}} V_S \sigma^{(0,v_1;0,v_2;0,v_3)} V_S^\dagger \stackrel{c}{\approx}_R \frac{I_2^{\otimes 3}}{8} \otimes \tilde{\tilde{\alpha}},$$
$$\sum_{\boldsymbol{v}} V_S \sigma^{(0,v_1;0,v_2;1,v_3)} V_S^\dagger \stackrel{c}{\approx}_R \frac{I_2^{\otimes 3}}{8} \otimes \tilde{\tilde{\alpha}},$$
$$\sum_{\boldsymbol{v}} V_S \sigma^{(1,v_1;0,v_2;0,v_3)} V_S^\dagger \stackrel{c}{\approx}_R \frac{I_2^{\otimes 3}}{8} \otimes \tilde{\tilde{\alpha}}.$$

From Eqs. (172), (173) and (174), we respectively obtain

$$\sum_{v_1} |v_1\rangle\langle v_1| \otimes \sum_{v_2} |v_2\rangle\langle v_2| \otimes \sum_{v_3} |v_3\rangle\langle v_3| \otimes \tilde{\tilde{\alpha}}^{(0,v_1;0,v_2;0,v_3)} \stackrel{c}{\approx}_R I_2^{\otimes 3} \otimes \frac{\tilde{\tilde{\alpha}}}{8},$$
$$\sum_{v_1} |v_1\rangle\langle v_1| \otimes \sum_{v_2} |v_2\rangle\langle v_2| \otimes \sum_{v_3} |(-)^{v_3}\rangle\langle (-)^{v_3}| \otimes \tilde{\tilde{\alpha}}^{(0,v_1;0,v_2;1,v_3)} \stackrel{c}{\approx}_R I_2^{\otimes 3} \otimes \frac{\tilde{\tilde{\alpha}}}{8},$$
$$\sum_{v_1} |(-)^{v_1}\rangle\langle (-)^{v_1}| \otimes \sum_{v_2} |v_2\rangle\langle v_2| \otimes \sum_{v_3} |v_3\rangle\langle v_3| \otimes \tilde{\tilde{\alpha}}^{(1,v_1;0,v_2;0,v_3)} \stackrel{c}{\approx}_R I_2^{\otimes 3} \otimes \frac{\tilde{\tilde{\alpha}}}{8}.$$

Since these approximate relations hold for any efficient prover, these relations hold when the first, the second and the third registers are measured in the Pauli bases. By considering such a prover, we have

$$\tilde{\tilde{\alpha}}^{(0,v_1;0,v_2;0,v_3)} \stackrel{c}{\approx}_R \frac{\tilde{\tilde{\alpha}}}{8},$$
$$\tilde{\tilde{\alpha}}^{(0,v_1;0,v_2;1,v_3)} \stackrel{c}{\approx}_R \frac{\tilde{\tilde{\alpha}}}{8},$$
$$\tilde{\tilde{\alpha}}^{(1,v_1;0,v_2;0,v_3)} \stackrel{c}{\approx}_R \frac{\tilde{\tilde{\alpha}}}{8}.$$

By applying these three approximate relations to Eqs. (172), (173) and (174), we respectively obtain Eqs. (176), (177) and (179), which completes the proof. ■

With Lemma 57 in hand, we obtain a simple corollary describing an approximate relation of state $\rho^{(\boldsymbol{\theta})}$.

Corollary 58 *(Extension of Corollary 51) Let $D = (S, \Pi, M, P)$ be an efficient perfect device. There exists a normalized state $\tilde{\tilde{\alpha}}$ such that for any $\boldsymbol{\theta} \in \mathcal{B}$,*

$$V_S \rho^{(\boldsymbol{\theta})} V_S^\dagger \stackrel{c}{\approx}_R \frac{I_2^{\otimes 3}}{8} \otimes \tilde{\tilde{\alpha}}. \tag{185}$$

(Proof) Taking the sum of the equations in Lemma 57 over $\boldsymbol{v}$ yields the statement for $\boldsymbol{\theta}$ of the test case. We can lift up the statement for any $\boldsymbol{\theta} \in \mathcal{B}$ thanks to Lemma 31. ■

Below, we present three crucial Lemmas 59, 60 and 61 for proving our main results, Theorem 62. The following Lemma 59 shows that any two joint observables are approximately equal to the products of the Pauli observables.

Lemma 59 *(Characterization of the first and second observables) For any efficient perfect device $D = (S, \Pi, M, P)$,*

we have the following for any $\boldsymbol{\theta} \in \mathcal{B}$.

$$V_S(A_{1,\mathbf{0}}A_{2,\mathbf{0}})V_S^\dagger \approx_{R,V_S\rho(\boldsymbol{\theta})V_S^\dagger} (\sigma_Z \otimes \sigma_Z \otimes I_2 \otimes I), \tag{186}$$

$$V_S(A_{1,\mathbf{0}}A_{3,\mathbf{0}})V_S^\dagger \approx_{R,V_S\rho(\boldsymbol{\theta})V_S^\dagger} (\sigma_Z \otimes I_2 \otimes \sigma_Z \otimes I), \tag{187}$$

$$V_S(A_{2,\mathbf{0}}A_{3,\mathbf{0}})V_S^\dagger \approx_{R,V_S\rho(\boldsymbol{\theta})V_S^\dagger} (I_2 \otimes \sigma_Z \otimes \sigma_Z \otimes I), \tag{188}$$

$$V_S(A_{1,\mathbf{1}}A_{2,\mathbf{1}})V_S^\dagger \approx_{R,V_S\rho(\boldsymbol{\theta})V_S^\dagger} (\sigma_X \otimes \sigma_X \otimes I_2 \otimes I),$$

$$V_S(A_{1,\mathbf{1}}A_{3,\mathbf{1}})V_S^\dagger \approx_{R,V_S\rho(\boldsymbol{\theta})V_S^\dagger} (\sigma_X \otimes I_2 \otimes \sigma_X \otimes I),$$

$$V_S(A_{2,\mathbf{1}}A_{3,\mathbf{1}})V_S^\dagger \approx_{R,V_S\rho(\boldsymbol{\theta})V_S^\dagger} (I_2 \otimes \sigma_X \otimes \sigma_X \otimes I),$$

$$V_S(A_{1,001}A_{2,001})V_S^\dagger \approx_{R,V_S\rho(\boldsymbol{\theta})V_S^\dagger} (\sigma_Z \otimes \sigma_Z \otimes I_2 \otimes I),$$

$$V_S(A_{1,001}A_{3,001})V_S^\dagger \approx_{R,V_S\rho(\boldsymbol{\theta})V_S^\dagger} (\sigma_Z \otimes I_2 \otimes \sigma_X \otimes I),$$

$$V_S(A_{2,001}A_{3,001})V_S^\dagger \approx_{R,V_S\rho(\boldsymbol{\theta})V_S^\dagger} (I_2 \otimes \sigma_Z \otimes \sigma_X \otimes I),$$

$$V_S(A_{1,010}A_{2,010})V_S^\dagger \approx_{R,V_S\rho(\boldsymbol{\theta})V_S^\dagger} (\sigma_Z \otimes \sigma_X \otimes I_2 \otimes I),$$

$$V_S(A_{1,010}A_{3,010})V_S^\dagger \approx_{R,V_S\rho(\boldsymbol{\theta})V_S^\dagger} (\sigma_Z \otimes I_2 \otimes \sigma_Z \otimes I),$$

$$V_S(A_{2,010}A_{3,010})V_S^\dagger \approx_{R,V_S\rho(\boldsymbol{\theta})V_S^\dagger} (I_2 \otimes \sigma_X \otimes \sigma_Z \otimes I),$$

$$V_S(A_{1,100}A_{2,100})V_S^\dagger \approx_{R,V_S\rho(\boldsymbol{\theta})V_S^\dagger} (\sigma_X \otimes \sigma_Z \otimes I_2 \otimes I),$$

$$V_S(A_{1,100}A_{3,100})V_S^\dagger \approx_{R,V_S\rho(\boldsymbol{\theta})V_S^\dagger} (\sigma_X \otimes I_2 \otimes \sigma_Z \otimes I),$$

$$V_S(A_{2,100}A_{3,100})V_S^\dagger \approx_{R,V_S\rho(\boldsymbol{\theta})V_S^\dagger} (I_2 \otimes \sigma_Z \otimes \sigma_Z \otimes I),$$

$$V_S(A_{1,011}A_{2,011})V_S^\dagger \approx_{R,V_S\rho(\boldsymbol{\theta})V_S^\dagger} (\sigma_Z \otimes \sigma_X \otimes I_2 \otimes I),$$

$$V_S(A_{1,011}A_{3,011})V_S^\dagger \approx_{R,V_S\rho(\boldsymbol{\theta})V_S^\dagger} (\sigma_Z \otimes I_2 \otimes \sigma_X \otimes I),$$

$$V_S(A_{2,011}A_{3,011})V_S^\dagger \approx_{R,V_S\rho(\boldsymbol{\theta})V_S^\dagger} (I_2 \otimes \sigma_X \otimes \sigma_X \otimes I),$$

$$V_S(A_{1,101}A_{2,101})V_S^\dagger \approx_{R,V_S\rho(\boldsymbol{\theta})V_S^\dagger} (\sigma_X \otimes \sigma_Z \otimes I_2 \otimes I),$$

$$V_S(A_{1,101}A_{3,101})V_S^\dagger \approx_{R,V_S\rho(\boldsymbol{\theta})V_S^\dagger} (\sigma_X \otimes I_2 \otimes \sigma_X \otimes I),$$

$$V_S(A_{2,101}A_{3,101})V_S^\dagger \approx_{R,V_S\rho(\boldsymbol{\theta})V_S^\dagger} (I_2 \otimes \sigma_Z \otimes \sigma_X \otimes I),$$

$$V_S(A_{1,110}A_{2,110})V_S^\dagger \approx_{R,V_S\rho(\boldsymbol{\theta})V_S^\dagger} (\sigma_X \otimes \sigma_X \otimes I_2 \otimes I),$$

$$V_S(A_{1,110}A_{3,110})V_S^\dagger \approx_{R,V_S\rho(\boldsymbol{\theta})V_S^\dagger} (\sigma_X \otimes I_2 \otimes \sigma_Z \otimes I),$$

$$V_S(A_{2,110}A_{3,110})V_S^\dagger \approx_{R,V_S\rho(\boldsymbol{\theta})V_S^\dagger} (I_2 \otimes \sigma_X \otimes \sigma_Z \otimes I).$$

Note that Lemma 59 will be used to prove Theorem 62 (ii).
(Proof) We prove Eq. (186), and the others can be shown analogously. As $[A_{1,\mathbf{0}}, A_{2,\mathbf{0}}] = 0$ from Lemma 39, and $A_{1,\mathbf{0}}$ and $A_{2,\mathbf{0}}$ are efficient binary observables, Lemma 11 implies that $A_{1,\mathbf{0}}A_{2,\mathbf{0}}$ is an efficient binary observable. Since V_S, $A_{1,\mathbf{0}}A_{2,\mathbf{0}}$ and σ_Z are all efficient, Corollary 51 and Lemma 21 (vi) reduced the proof of Eq. (186) to showing

$$V_S(A_{1,\mathbf{0}}A_{2,\mathbf{0}})V_S^\dagger \approx_{R,\kappa} \sigma_Z \otimes \sigma_Z \otimes I_2 \otimes I.$$

Recall that $\kappa := I_2 \otimes I_2/4 \otimes \tilde{\alpha}$. From Lemma 15, it suffices to show

$$\mathrm{tr}\left[(\sigma_Z \otimes \sigma_Z \otimes I_2 \otimes I)(V_S A_{1,\mathbf{0}}A_{2,\mathbf{0}}V_S^\dagger)\kappa\right] \approx_R 1. \tag{189}$$

Here, we recall that

$$\text{Eq. (94) and Lemma 19} \Rightarrow V_S A_{1,\mathbf{0}} V_S^\dagger \approx_{R,V_S\rho(\boldsymbol{\theta})V_S^\dagger} \sigma_Z \otimes I_2^{\otimes 2} \otimes I, \tag{190}$$

$$\text{Lemmas 19 and 47} \Rightarrow V_S A_{2,\mathbf{0}} V_S^\dagger \approx_{R,V_S\rho(\boldsymbol{\theta})V_S^\dagger} I_2 \otimes \sigma_Z \otimes I_2 \otimes I, \tag{191}$$

and using Eq. (148) and Lemma 21 (vi), Eqs. (190) and (191) imply

$$V_S A_{1,\mathbf{0}} V_S^\dagger \approx_{R,\kappa} \sigma_Z \otimes I_2^{\otimes 2} \otimes I, \tag{192}$$
$$V_S A_{2,\mathbf{0}} V_S^\dagger \approx_{R,\kappa} I_2 \otimes \sigma_Z \otimes I_2 \otimes I. \tag{193}$$

Hence, using Eqs. (192) and (193), the LHS of Eq. (189) is computed as

$$\begin{aligned}
&=\mathrm{tr}\left[(\sigma_Z \otimes \sigma_Z \otimes I_2 \otimes I)(V_S A_{1,\mathbf{0}} V_S^\dagger)(V_S A_{2,\mathbf{0}} V_S^\dagger)\kappa\right] \\
&\approx_R \mathrm{tr}\left[(\sigma_Z \otimes \sigma_Z \otimes I_2 \otimes I)(V_S A_{1,\mathbf{0}} V_S^\dagger)(I_2 \otimes \sigma_Z \otimes I_2 \otimes I)\kappa\right] \\
&=\mathrm{tr}\left[(\sigma_Z \otimes I_2 \otimes I_2 \otimes I)(V_S A_{1,\mathbf{0}} V_S^\dagger)\kappa\right] \\
&\approx_R \mathrm{tr}\left[(\sigma_Z \otimes I_2 \otimes I_2 \otimes I)(\sigma_Z \otimes I_2 \otimes I_2 \otimes I)\kappa\right] \\
&=\mathrm{tr}(\kappa) \\
&=1,
\end{aligned}$$

where Eq. (193) is used in the first approximate equation, the commutation relation $[I_2 \otimes \sigma_Z \otimes I_2 \otimes I, \kappa] = 0$ is used in the third line, and Eq. (192) is used in the second approximate equation. ■

We next prove that any three joint observables are approximately equal to the products of the Pauli observables.

Lemma 60 *For any efficient perfect device $D = (S, \Pi, M, P)$, we have the following for any $\boldsymbol{\theta} \in \mathcal{B}$.*

$$\begin{aligned}
&V_S(A_{1,\mathbf{0}}A_{2,\mathbf{0}}A_{3,\mathbf{0}})V_S^\dagger \approx_{R,V_S\rho^{(\boldsymbol{\theta})}V_S^\dagger} (\sigma_Z \otimes \sigma_Z \otimes \sigma_Z \otimes I), \\
&V_S(A_{1,\mathbf{1}}A_{2,\mathbf{1}}A_{3,\mathbf{1}})V_S^\dagger \approx_{R,V_S\rho^{(\boldsymbol{\theta})}V_S^\dagger} (\sigma_X \otimes \sigma_X \otimes \sigma_X \otimes I), \\
&V_S(A_{1,001}A_{2,001}A_{3,001})V_S^\dagger \approx_{R,V_S\rho^{(\boldsymbol{\theta})}V_S^\dagger} (\sigma_Z \otimes \sigma_Z \otimes \sigma_X \otimes I), \\
&V_S(A_{1,010}A_{2,010}A_{3,010})V_S^\dagger \approx_{R,V_S\rho^{(\boldsymbol{\theta})}V_S^\dagger} (\sigma_Z \otimes \sigma_X \otimes \sigma_Z \otimes I), \\
&V_S(A_{1,100}A_{2,100}A_{3,100})V_S^\dagger \approx_{R,V_S\rho^{(\boldsymbol{\theta})}V_S^\dagger} (\sigma_X \otimes \sigma_Z \otimes \sigma_Z \otimes I), \\
&V_S(A_{1,011}A_{2,011}A_{3,011})V_S^\dagger \approx_{R,V_S\rho^{(\boldsymbol{\theta})}V_S^\dagger} (\sigma_Z \otimes \sigma_X \otimes \sigma_X \otimes I), \\
&V_S(A_{1,101}A_{2,101}A_{3,101})V_S^\dagger \approx_{R,V_S\rho^{(\boldsymbol{\theta})}V_S^\dagger} (\sigma_X \otimes \sigma_Z \otimes \sigma_X \otimes I), \\
&V_S(A_{1,110}A_{2,110}A_{3,110})V_S^\dagger \approx_{R,V_S\rho^{(\boldsymbol{\theta})}V_S^\dagger} (\sigma_X \otimes \sigma_X \otimes \sigma_Z \otimes I).
\end{aligned} \tag{194}$$

Note that Lemma 60 will be used to prove Theorem 62 (ii).
(Proof) We prove Eq. (194), and the others can be shown analogously. Since $[A_{3,\mathbf{0}}, A_{1,\mathbf{0}}A_{2,\mathbf{0}}] = 0$ from Lemma 39, and $A_{3,\mathbf{0}}$ and $A_{1,\mathbf{0}}A_{2,\mathbf{0}}$ are efficient binary observables as explained in the proof of Lemma 59, Lemma 11 implies that $A_{1,\mathbf{0}}A_{2,\mathbf{0}}A_{3,\mathbf{0}}$ is also an efficient binary observable. As V_S, $A_{1,\mathbf{0}}A_{2,\mathbf{0}}A_{3,\mathbf{0}}$ and σ_Z are all efficient, from Lemma 21 (vi) and Corollary 58, the proof of Eq. (194) is reduced to showing

$$V_S(A_{1,\mathbf{0}}A_{2,\mathbf{0}}A_{3,\mathbf{0}})V_S^\dagger \approx_{R,\underbrace{\frac{1}{8}I_2^{\otimes 3} \otimes \tilde{\tilde{\alpha}}}_{=:\phi}} \sigma_Z \otimes \sigma_Z \otimes \sigma_Z \otimes I.$$

From Lemma 15 and $V_S^\dagger V_S = I$, it suffices to show

$$\mathrm{tr}\left[(\sigma_Z^{\otimes 3} \otimes I)(V_S A_{1,\mathbf{0}} V_S^\dagger)(V_S A_{2,\mathbf{0}} V_S^\dagger)(V_S A_{3,\mathbf{0}} V_S^\dagger)\phi\right] \approx_R 1. \tag{195}$$

Here, we recall that

$$\begin{aligned}
\text{Eq. (94) and Lemma 19} &\Rightarrow V_S A_{1,\mathbf{0}} V_S^\dagger \approx_{R,V_S\rho^{(\boldsymbol{\theta})}V_S^\dagger} \sigma_Z \otimes I_2^{\otimes 2} \otimes I, \\
\text{Lemmas 19 and 47} &\Rightarrow V_S A_{2,\mathbf{0}} V_S^\dagger \approx_{R,V_S\rho^{(\boldsymbol{\theta})}V_S^\dagger} I_2 \otimes \sigma_Z \otimes I_2 \otimes I, \\
\text{Lemmas 19 and 52} &\Rightarrow V_S A_{3,\mathbf{0}} V_S^\dagger \approx_{R,V_S\rho^{(\boldsymbol{\theta})}V_S^\dagger} I_2^{\otimes 2} \otimes \sigma_Z \otimes I,
\end{aligned} \tag{196}$$

and Corollary 58 and Lemma 21 (vi) lead to

$$V_S A_{1,\mathbf{0}} V_S^\dagger \approx_{R,\phi} \sigma_Z \otimes I_2^{\otimes 2} \otimes I, \tag{197}$$

$$V_S A_{2,\mathbf{0}} V_S^\dagger \approx_{R,\phi} I_2 \otimes \sigma_Z \otimes I_2 \otimes I, \tag{198}$$

$$V_S A_{3,\mathbf{0}} V_S^\dagger \approx_{R,\phi} I_2^{\otimes 2} \otimes \sigma_Z \otimes I. \tag{199}$$

By using Eqs. (197)-(199) and Lemma 17 (i), we show that the LHS of Eq. (195) is approximately equal to 1.

$$\begin{aligned}
&\mathrm{tr}\left[(\sigma_Z^{\otimes 3}\otimes I)(V_S A_{1,\mathbf{0}} V_S^\dagger)(V_S A_{2,\mathbf{0}} V_S^\dagger)(V_S A_{3,\mathbf{0}} V_S^\dagger)\phi\right]\\
\approx_R &\mathrm{tr}\left[(\sigma_Z^{\otimes 3}\otimes I)(V_S A_{1,\mathbf{0}} V_S^\dagger)(V_S A_{2,\mathbf{0}} V_S^\dagger)(I_2^{\otimes 2}\otimes\sigma_Z\otimes I)\phi\right]\\
= &\mathrm{tr}\left[(I_2^{\otimes 2}\otimes\sigma_Z\otimes I)(\sigma_Z^{\otimes 3}\otimes I)(V_S A_{1,\mathbf{0}} V_S^\dagger)(V_S A_{2,\mathbf{0}} V_S^\dagger)\phi\right]\\
\approx_R &\mathrm{tr}\left[(I_2^{\otimes 2}\otimes\sigma_Z\otimes I)(\sigma_Z^{\otimes 3}\otimes I)(V_S A_{1,\mathbf{0}} V_S^\dagger)(I_2^{\otimes 2}\otimes\sigma_Z\otimes I_2\otimes I)\phi\right]\\
= &\mathrm{tr}\left[(I_2^{\otimes 2}\otimes\sigma_Z\otimes I_2\otimes I)(I_2^{\otimes 2}\otimes\sigma_Z\otimes I)(\sigma_Z^{\otimes 3}\otimes I)(V_S A_{1,\mathbf{0}} V_S^\dagger)\phi\right]\\
\approx_R &\mathrm{tr}\left[(I_2\otimes\sigma_Z\otimes I_2\otimes I)(I_2^{\otimes 2}\otimes\sigma_Z\otimes I)(\sigma_Z^{\otimes 3}\otimes I)(\sigma_Z\otimes I_2^{\otimes 2}\otimes I)\phi\right]\\
= &\mathrm{tr}(\phi)\\
= &1,
\end{aligned}$$

which ends the proof. ■

By exploiting the result of Corollary 58, we show that the prover's measurements corresponding to obtaining the outcomes $v_3 \oplus \delta_{v_1,1}\cdot v_2$, $v_2 \oplus \delta_{v_1,1}\cdot v_3$ and $v_1 \oplus \delta_{v_2,1}\cdot v_3$ at step (e) of the protocol in Sec. III are approximately equal to the generalized stabilizer measurements of the entangled magic state $CCZ|+\rangle^{\otimes 3}$.

Lemma 61 *For any efficient perfect device $D = (S, \Pi, M, P)$, the following holds for any $\boldsymbol{\theta} \in \mathcal{B}$.*

$$V_S(A^{(0)}_{1,001}A_{3,001} + A^{(1)}_{1,001}A_{2,001}A_{3,001})V_S^\dagger \approx_{R,V_S\rho^{(\boldsymbol{\theta})}V_S^\dagger} (\sigma_Z^{(0)}\otimes I_2\otimes\sigma_X + \sigma_Z^{(1)}\otimes\sigma_Z\otimes\sigma_X)\otimes I_{\mathcal{H}}, \tag{200}$$

$$V_S(A^{(0)}_{1,010}A_{2,010} + A^{(1)}_{1,010}A_{2,010}A_{3,010})V_S^\dagger \approx_{R,V_S\rho^{(\boldsymbol{\theta})}V_S^\dagger} (\sigma_Z^{(0)}\otimes\sigma_X\otimes I_2 + \sigma_Z^{(1)}\otimes\sigma_X\otimes\sigma_Z)\otimes I_{\mathcal{H}}, \tag{201}$$

$$V_S(A_{1,100}A^{(0)}_{2,100} + A_{1,100}A^{(1)}_{2,100}A_{3,100})V_S^\dagger \approx_{R,V_S\rho^{(\boldsymbol{\theta})}V_S^\dagger} (\sigma_X\otimes\sigma_Z^{(0)}\otimes I_2 + \sigma_X\otimes\sigma_Z^{(1)}\otimes\sigma_Z)\otimes I_{\mathcal{H}}. \tag{202}$$

Note that Lemma 61 will be used to prove Theorem 62 (i).

(Proof) We prove Eq. (200), and the others can be proven in the same way. Note that $(A^{(0)}_{1,001}A_{3,001} + A^{(1)}_{1,001}A_{2,001}A_{3,001})$ is an efficient binary observable [5] acting on the Hilbert space $\mathcal{H}$ that determines the bit $\delta_{v_1,1}\cdot v_2 \oplus v_3$. Using Corollary 58:

$$V_S\rho^{(\boldsymbol{\theta})}V_S^\dagger \overset{c}{\approx}_R \frac{I_2^{\otimes 3}}{8}\otimes\tilde{\tilde{\alpha}} =: \phi,$$

and Lemma 21 (vi), whose conditions are satisfied because $(A^{(0)}_{1,001}A_{3,001} + A^{(1)}_{1,001}A_{2,001}A_{3,001})$ and $(\sigma_Z^{(0)}\otimes I\otimes\sigma_X + \sigma_Z^{(1)}\otimes\sigma_Z\otimes\sigma_X)$ are efficient binary observables, reduces the proof of Eq. (200) to showing

$$V_S(A^{(0)}_{1,001}A_{3,001} + A^{(1)}_{1,001}A_{2,001}A_{3,001})V_S^\dagger \approx_{R,\phi} (\sigma_Z^{(0)}\otimes I\otimes\sigma_X + \sigma_Z^{(1)}\otimes\sigma_Z\otimes\sigma_X).$$

By using Lemma 15, it suffices to prove

$$\mathrm{tr}\left[(\sigma_Z^{(0)}\otimes I_2\otimes\sigma_X + \sigma_Z^{(1)}\otimes\sigma_Z\otimes\sigma_X)V_S(A^{(0)}_{1,001}A_{3,001} + A^{(1)}_{1,001}A_{2,001}A_{3,001})V_S^\dagger\phi\right] \approx_R \mathrm{tr}(\phi) = 1. \tag{203}$$

---

[5] Since $(A^{(0)}_{1,001}A_{3,001} + A^{(1)}_{1,001}A_{2,001}A_{3,001}) = [P^{(000)}_{001} + P^{(100)}_{001} + P^{(111)}_{001} + P^{(010)}_{001}] - [P^{(101)}_{001} + P^{(110)}_{001} + P^{(001)}_{001} + P^{(011)}_{001}]$ from a direct calculation using Eq. (6), we find that this operator is an Hermitian linear operator and has eigenvalues ± 1.

The LHS is equal to

$$\mathrm{tr}\left[\underbrace{(\sigma_Z^{(0)}\otimes I_2\otimes\sigma_X+\sigma_Z^{(1)}\otimes\sigma_Z\otimes\sigma_X)[(V_SA_{1,001}^{(0)}V_S^\dagger)+(V_SA_{1,001}^{(1)}V_S^\dagger)(V_SA_{2,001}V_S^\dagger)]}_{=:C}(V_SA_{3,001}V_S^\dagger)\phi\right]. \tag{204}$$

From Eq. (171) and Lemma 19, we have

$$V_SA_{3,001}V_S^\dagger\approx_{R,V_S\rho^{(\boldsymbol{\theta})}V_S^\dagger} I_2\otimes I_2\otimes\sigma_X\otimes I,$$

and the state $V_S\rho^{(\boldsymbol{\theta})}V_S^\dagger$ can be replaced with ϕ thanks to Lemmas 21 (vi) and Corollary 58 as

$$V_SA_{3,001}V_S^\dagger\approx_{R,\phi} I_2\otimes I_2\otimes\sigma_X\otimes I.$$

Since the operator norm of C defined in Eq. (204) is constant, from Lemma 17 (i) we have the approximate equation of Eq. (204) as

$$\begin{aligned}&\mathrm{tr}\left[(\sigma_Z^{(0)}\otimes I_2\otimes\sigma_X+\sigma_Z^{(1)}\otimes\sigma_Z\otimes\sigma_X)[(V_SA_{1,001}^{(0)}V_S^\dagger)+(V_SA_{1,001}^{(1)}V_S^\dagger)(V_SA_{2,001}V_S^\dagger)](I_2\otimes I_2\otimes\sigma_X)\phi\right]\\ =&\mathrm{tr}\left[(\sigma_Z^{(0)}\otimes I_2^{\otimes2}+\sigma_Z^{(1)}\otimes\sigma_Z\otimes I_2)(V_SA_{1,001}^{(0)}V_S^\dagger)\phi\right]\\ +&\mathrm{tr}\left[(\sigma_Z^{(0)}\otimes I_2^{\otimes2}+\sigma_Z^{(1)}\otimes\sigma_Z\otimes I_2)(V_SA_{1,001}^{(1)}V_S^\dagger)(V_SA_{2,001}V_S^\dagger)\phi\right],\end{aligned} \tag{205}$$

where we used the commutation relation $[I_2\otimes I_2\otimes\sigma_X,\phi]=0$ in the equation. In the following, we compute the first and the second terms of Eqs. (205) separately.

First, we calculate the second term of Eq. (205). From Eq. (168) and Lemma 19, we have

$$V_SA_{2,001}V_S^\dagger\approx_{R,V_S\rho^{(\boldsymbol{\theta})}V_S^\dagger} I_2\otimes\sigma_Z\otimes I_2\otimes I.$$

Using Lemma 21(vi) and Corollary 58 enables us to replace $V_S\rho^{(\boldsymbol{\theta})}V_S^\dagger$ with ϕ as

$$V_SA_{2,001}V_S^\dagger\approx_{R,\phi} I_2\otimes\sigma_Z\otimes I_2\otimes I.$$

From this and Lemma 17 (i), the second term of Eq. (205) is approximately equal to

$$\begin{aligned}&\mathrm{tr}\left[(\sigma_Z^{(0)}\otimes I_2^{\otimes2}+\sigma_Z^{(1)}\otimes\sigma_Z\otimes I_2)(V_SA_{1,001}^{(1)}V_S^\dagger)(I_2\otimes\sigma_Z\otimes I_2\otimes I)\phi\right]\\ =&\mathrm{tr}\left[(\sigma_Z^{(0)}\otimes\sigma_Z\otimes I_2+\sigma_Z^{(1)}\otimes I_2^{\otimes2})(V_SA_{1,001}^{(1)}V_S^\dagger)\phi\right],\end{aligned} \tag{206}$$

where we used the commutation relation $[I_2\otimes\sigma_Z\otimes I_2\otimes I,\phi]=0$. Using $A_{1,001}=\sum_{v_2,v_3}\left(P_{001}^{(0v_2v_3)}-P_{001}^{(1v_2v_3)}\right)$ from Eq. (6) and $I=\sum_{v_2,v_3}\left(P_{001}^{(0v_2v_3)}+P_{001}^{(1v_2v_3)}\right)$ leads to

$$A_{1,001}^{(b)}=\frac{I+(-1)^bA_{1,001}}{2}. \tag{207}$$

Substituting this to Eq. (206), Eq. (206) equals

$$\frac{1}{2}\mathrm{tr}\left[(\sigma_Z^{(0)}\otimes\sigma_Z\otimes I_2+\sigma_Z^{(1)}\otimes I_2^{\otimes2})V_SV_S^\dagger\phi\right]-\frac{1}{2}\mathrm{tr}\left[(\sigma_Z^{(0)}\otimes\sigma_Z\otimes I_2+\sigma_Z^{(1)}\otimes I_2^{\otimes2})(V_SA_{1,001}V_S^\dagger)\phi\right]. \tag{208}$$

Its first term can be computed by using

$$V_SV_S^\dagger\approx_{0,V_S\rho^{(\boldsymbol{\theta})}V_S^\dagger} I\Rightarrow V_SV_S^\dagger\approx_{R,\phi} I, \tag{209}$$

which is guaranteed by Lemma 21 (vi) and Corollary 58, and Lemma 17 (i) as

$$\mathrm{tr}\left[(\sigma_Z^{(0)}\otimes\sigma_Z\otimes I_2+\sigma_Z^{(1)}\otimes I_2^{\otimes2})V_SV_S^\dagger\phi\right]\approx_R\mathrm{tr}\left[(|0\rangle\langle0|\otimes\sigma_Z\otimes I_2+|1\rangle\langle1|\otimes I_2^{\otimes2})\phi\right]. \tag{210}$$

Next, we compute the second term of Eq. (208). From Eq. (166) and Lemma 19, we have

$$V_S A_{1,001} V_S^\dagger \approx_{R, V_S \rho^{(\boldsymbol{\theta})} V_S^\dagger} \sigma_Z \otimes I_2^{\otimes 2} \otimes I.$$

By employing Lemma 21 (vi) and Corollary 58, this leads to

$$V_S A_{1,001} V_S^\dagger \approx_{R,\phi} \sigma_Z \otimes I_2^{\otimes 2} \otimes I. \tag{211}$$

From Lemma 17 (i), the second term of Eq. (208) is approximately equal to

$$\mathrm{tr}\left[(\sigma_Z^{(0)} \otimes \sigma_Z \otimes I_2 + \sigma_Z^{(1)} \otimes I_2^{\otimes 2})(\sigma_Z \otimes I_2^{\otimes 2})\phi\right] = \mathrm{tr}\left[(|0\rangle\langle 0| \otimes \sigma_Z \otimes I_2 - |1\rangle\langle 1| \otimes I_2^{\otimes 2})\phi\right]. \tag{212}$$

Combining Eqs. (210) and (212), we find that Eq. (208) is approximately equal to $\mathrm{tr}[(|1\rangle\langle 1| \otimes I_2^{\otimes 2})\phi]$. Hence, the LHS of Eq. (203), which is the main target of computation in the proof, is approximately equal to as

$$\text{LHS of Eq. (203)} \approx_R (\text{first term of Eq.(205)}) + \mathrm{tr}[(|1\rangle\langle 1| \otimes I_2 \otimes I_2 \otimes I_{\mathcal{H}})\phi]. \tag{213}$$

Hence, the remaining task is to compute the first term of Eq. (205).

Using Eq. (207), we have that the first term of Eq. (205) is equal to

$$\frac{1}{2}\mathrm{tr}\left[(\sigma_Z^{(0)} \otimes I_2^{\otimes 2} + \sigma_Z^{(1)} \otimes \sigma_Z \otimes I_2)(V_S V_S^\dagger)\phi\right] + \frac{1}{2}\mathrm{tr}\left[(\sigma_Z^{(0)} \otimes I_2^{\otimes 2} + \sigma_Z^{(1)} \otimes \sigma_Z \otimes I_2)(V_S A_{1,001} V_S^\dagger)\phi\right].$$

From the right part of Eq. (209) and Lemma 17 (i), we obtain

$$\frac{1}{2}\mathrm{tr}\left[(\sigma_Z^{(0)} \otimes I_2^{\otimes 2} + \sigma_Z^{(1)} \otimes \sigma_Z \otimes I_2)(V_S V_S^\dagger)\phi\right] \approx_R \frac{1}{2}\mathrm{tr}\left[(\sigma_Z^{(0)} \otimes I_2^{\otimes 2} + \sigma_Z^{(1)} \otimes \sigma_Z \otimes I_2)\phi\right].$$

Also, from Eq. (211) and Lemma 17 (i), we have

$$\frac{1}{2}\mathrm{tr}\left[(\sigma_Z^{(0)} \otimes I_2^{\otimes 2} + \sigma_Z^{(1)} \otimes \sigma_Z \otimes I_2)(V_S A_{1,001} V_S^\dagger)\phi\right] \approx_R \frac{1}{2}\mathrm{tr}\left[(\sigma_Z^{(0)} \otimes I_2^{\otimes 2} + \sigma_Z^{(1)} \otimes \sigma_Z \otimes I_2)(\sigma_Z \otimes I_2^{\otimes 2})\phi\right].$$

Hence, the first term of Eq.(205) is approximately equal to

$$\begin{aligned}&\frac{1}{2}\mathrm{tr}\left[(\sigma_Z^{(0)} \otimes I_2^{\otimes 2} + \sigma_Z^{(1)} \otimes \sigma_Z \otimes I_2)\phi\right] + \frac{1}{2}\mathrm{tr}\left[(\sigma_Z^{(0)} \otimes I_2^{\otimes 2} + \sigma_Z^{(1)} \otimes \sigma_Z \otimes I_2)(\sigma_Z \otimes I_2^{\otimes 2})\phi\right] \\ =&\mathrm{tr}\left[(|0\rangle\langle 0| \otimes I_2^{\otimes 2} \otimes I_{\mathcal{H}})\phi\right].\end{aligned}$$

Finally, substituting this into Eq. (213) results in

$$\text{LHS of Eq. (203)} \approx_R \mathrm{tr}(\phi) = 1,$$

which ends the proof. ■

K. Certifying entangled magic states

Theorem 62 *We define the Z-rotated entangled magic states as*

$$|\phi_{\mathrm{H}}^{(a,b,c)}\rangle := (\sigma_Z^a \otimes \sigma_Z^b \otimes \sigma_Z^c) CCZ |+\rangle^{\otimes 3}$$

with CCZ representing the controlled-controlled-Z gate. For $b \in \{0,1\}$, we use the notation

$$|b_0\rangle := |b\rangle, \quad |b_1\rangle := |(-)^b\rangle.$$

Let $D = (S, \Pi, M, P)$ be an efficient device, the device's Hilbert space be $\mathcal{H}$, $\sigma^{(1,s_1;1,s_2;1,s_3)}$ be defined in Eq. (27), and $\mathcal{H}'$ be some Hilbert space. Then, there exists an isometry $V : \mathcal{H} \to \mathbb{C}^8 \otimes \mathcal{H}'$, and a constant $d > 0$ such that there are normalized states $\zeta^{(s_1,s_2,s_3)} \in \mathcal{D}(\mathcal{H}')$ for $s_1, s_2, s_3 \in \{0,1\}$ satisfying the following. In the description, $\gamma_P(D), \gamma_T(D)$ and $\gamma_H(D)$ are defined in Lemmas 24, 25, and 26, respectively, which are the device's probabilities of failing the verifier's checks in the preimage round, the Hadamard round with the test case, and the Hadamard round with the

hyperpgrah one, respectively [6].
(i) The unnormalized state of the prover in an Hadamard round is close to the entangled magic state up to the isometry V:

$$V\sigma^{(1,s_1;1,s_2;1,s_3)}V^\dagger \approx_{\gamma_P(D)^d+\gamma_T(D)^d+\gamma_H(D)^d} \frac{1}{8}|\phi_{\rm H}^{(s_1,s_2,s_3)}\rangle\langle\phi_{\rm H}^{(s_1,s_2,s_3)}| \otimes \zeta^{(s_1,s_2,s_3)},$$

where the different $\zeta^{(s_1,s_2,s_3)}$ are computationally indistinguishable.
(ii) Under the isometry V, the measurements $\{P^{(abc)}_{q_1q_2q_3}\}_{a,b,c}$ acting on the prover's state $\sigma^{(1,s_1;1,s_2;1,s_3)}$ is close to the Pauli-Z and X measurements acting on the entangled magic state $|\phi_{\rm H}^{(s_1,s_2,s_3)}\rangle$:

$$\begin{aligned}V P^{(abc)}_{q_1q_2q_3}\sigma^{(1,s_1;1,s_2;1,s_3)}P^{(abc)}_{q_1q_2q_3}V^\dagger \approx_{\gamma_P(D)^d+\gamma_T(D)^d+\gamma_H(D)^d} &\frac{1}{8}(|a_{q_1},b_{q_2},c_{q_3}\rangle\langle a_{q_1},b_{q_2},c_{q_3}|)|\phi_{\rm H}^{(s_1,s_2,s_3)}\rangle\langle\phi_{\rm H}^{(s_1,s_2,s_3)}|\\ &(|a_{q_1},b_{q_2},c_{q_3}\rangle\langle a_{q_1},b_{q_2},c_{q_3}|)\otimes\zeta^{(s_1,s_2,s_3)}.\end{aligned}$$

In the both proofs of (i) and (ii), by Lemma 30, up to an additional error $O(\sqrt{\gamma_P(D)})$, we can assume that the device D is perfect [7]. In these proofs, we take the isometry V as the swap isometry V_S defined in Eq. (92).

1. *Proof of (i)*

First, using Eq. (200) and Lemma 19 leads to

$$A^{(0)}_{1,001}A_{3,001}+A^{(1)}_{1,001}A_{2,001}A_{3,001} \approx_{R,\rho^{(\boldsymbol{\theta})}} V_S^\dagger\left(\sum_{i=0}^{1}|i\rangle\langle i|\otimes\sigma_Z^i\otimes\sigma_X\right)V_S. \tag{214}$$

By applying Lemma 13 (ii) to this, we have

$$A^{(0)}_{1,001}A_{3,001}+A^{(1)}_{1,001}A_{2,001}A_{3,001} \approx_{R,\sigma^{(1,s_1;1,s_2;1,s_3)}} V_S^\dagger\left(\sum_{i=0}^{1}|i\rangle\langle i|\otimes\sigma_Z^i\otimes\sigma_X\right)V_S.$$

By noting that the LHS and $(\sum_{i=0}^{1}|i\rangle\langle i|\otimes\sigma_Z^i\otimes\sigma_X)$ are both binary observables, Lemma 20 implies

$$(A^{(0)}_{1,001}A_{3,001}+A^{(1)}_{1,001}A_{2,001}A_{3,001})^{(a)} \approx_{R,\sigma^{(1,s_1;1,s_2;1,s_3)}} V_S^\dagger\left(\sum_{i=0}^{1}|i\rangle\langle i|\otimes\sigma_Z^i\otimes\sigma_X\right)^{(a)}V_S.$$

Using this and Lemma 17 (i) leads to

$$\mathrm{tr}\left[\left(\sum_{i=0}^{1}|i\rangle\langle i|\otimes\sigma_Z^i\otimes\sigma_X\right)^{(a)}\varphi^{(s_1,s_2,s_3)}\right] \approx_R \mathrm{tr}\left[(A^{(0)}_{1,001}A_{3,001}+A^{(1)}_{1,001}A_{2,001}A_{3,001})^{(a)}\sigma^{(1,s_1;1,s_2;1,s_3)}\right], \tag{215}$$

where

$$\varphi^{(s_1,s_2,s_3)} := V_S\sigma^{(1,s_1;1,s_2;1,s_3)}V_S^\dagger.$$

By the definition of $\gamma_H(D)$ given in Eq. (26), we have

$$\sum_{\boldsymbol{s}}\mathrm{tr}\left[(A^{(0)}_{1,001}A_{3,001}+A^{(1)}_{1,001}A_{2,001}A_{3,001})^{(s_3)}\sigma^{(1,s_1;1,s_2;1,s_3)}\right] \approx_{\gamma_H(D)} 1,$$

---

[6] Note that $\gamma_P(D),\gamma_T(D)$ and $\gamma_H(D)$ are upper-bounded by the probabilities of obtaining the flag in the preimage round, the Hadamard round with the test case and the Hadamard round with the hypergraph one, which are shown in Eqs. (9), (17) and (32), respectively.
[7] Note that Lemma 30 implies the statement for $\sigma^{(1,s_1;1,s_2;1,s_3)}$ since application of a CPTP map cannot increase the trace distance.

and by using Lemma 27 and $V_S^\dagger V_S = I$, this leads to

$$\mathrm{tr}[(A_{1,001}^{(0)}A_{3,001} + A_{1,001}^{(1)}A_{2,001}A_{3,001})^{(s_3)}\sigma^{(1,s_1;1,s_2;1,s_3)}] \approx_{\gamma_H(D)} \mathrm{tr}(\varphi^{(s_1,s_2,s_3)}). \tag{216}$$

Combining Eqs. (215), (216) and the triangle inequality results in

$$\mathrm{tr}\left[\left(\sum_{i=0}^{1}|i\rangle\langle i|\otimes\sigma_Z^i\otimes\sigma_X\right)^{(s_3)}\varphi^{(s_1,s_2,s_3)}\right] \approx_R \mathrm{tr}(\varphi^{(s_1,s_2,s_3)}). \tag{217}$$

Using Lemma 14 (by noting that $V_S\sigma^{(1,s_1;1,s_2;1,s_3)}V_S^\dagger \geq 0$ and $\sum_{i=0}^{1}|i\rangle\langle i|\otimes\sigma_Z^i\otimes\sigma_X$ is a binary observable), Eq. (217) and Lemma 16 lead to

$$O_1^{(a)} := \left(\sum_{i=0}^{1}|i\rangle\langle i|\otimes\sigma_Z^i\otimes\sigma_X\right)^{(a)} \approx_{R,\varphi^{(s_1,s_2,s_3)}} \delta_{a,s_3}I.$$

By replacing Eq. (214) with Eqs. (201) and (202), and by following the same arguments done so far, we respectively obtain

$$O_2^{(b)} := \left(\sum_{i=0}^{1}|i\rangle\langle i|\otimes\sigma_X\otimes\sigma_Z^i\right)^{(b)} \approx_{R,\varphi^{(s_1,s_2,s_3)}} \delta_{b,s_2}I$$

and

$$O_3^{(c)} := \left(\sigma_X\otimes\sum_{i=0}^{1}|i\rangle\langle i|\otimes\sigma_Z^i\right)^{(c)} \approx_{R,\varphi^{(s_1,s_2,s_3)}} \delta_{c,s_1}I.$$

Once we have

$$O_1^{(a)} \approx_{R,\varphi^{(s_1,s_2,s_3)}} \delta_{a,s_3}I, \tag{218}$$
$$O_2^{(b)} \approx_{R,\varphi^{(s_1,s_2,s_3)}} \delta_{b,s_2}I, \tag{219}$$
$$O_3^{(c)} \approx_{R,\varphi^{(s_1,s_2,s_3)}} \delta_{c,s_1}I, \tag{220}$$

we can prove

$$\begin{aligned}&\varphi^{(s_1,s_2,s_3)} \approx_R O_3^{(s_1)}O_2^{(s_2)}O_1^{(s_3)}\left(\sum_{\boldsymbol{s}}\varphi^{(s_1,s_2,s_3)}\right)O_1^{(s_3)}O_2^{(s_2)}O_3^{(s_1)}\\ \Leftrightarrow &V_S\sigma^{(1,s_1;1,s_2;1,s_3)}V_S^\dagger \approx_R O_3^{(s_1)}O_2^{(s_2)}O_1^{(s_3)}(V_S\rho^{(111)}V_S^\dagger)O_1^{(s_3)}O_2^{(s_2)}O_3^{(s_1)}.\end{aligned} \tag{221}$$

The proof of Eq. (221) can be done by showing the following eight approximate relations and using the triangle inequality of the trace distance.

$$\varphi^{(s_1,s_2,s_3)} \approx_R O_3^{(s_1)}O_2^{(s_2)}O_1^{(s_3)}\varphi^{(s_1,s_2,s_3)}O_1^{(s_3)}O_2^{(s_2)}O_3^{(s_1)}, \tag{222}$$
$$0 \approx_R O_3^{(\overline{s_1})}O_2^{(s_2)}O_1^{(s_3)}\varphi^{(s_1,s_2,s_3)}O_1^{(s_3)}O_2^{(s_2)}O_3^{(s_1)}, \tag{223}$$
$$0 \approx_R O_3^{(s_1)}O_2^{(\overline{s_2})}O_1^{(s_3)}\varphi^{(s_1,s_2,s_3)}O_1^{(s_3)}O_2^{(s_2)}O_3^{(s_1)}, \tag{224}$$
$$0 \approx_R O_3^{(s_1)}O_2^{(s_2)}O_1^{(\overline{s_3})}\varphi^{(s_1,s_2,s_3)}O_1^{(s_3)}O_2^{(s_2)}O_3^{(s_1)}, \tag{225}$$
$$0 \approx_R O_3^{(\overline{s_1})}O_2^{(\overline{s_2})}O_1^{(s_3)}\varphi^{(s_1,s_2,s_3)}O_1^{(s_3)}O_2^{(s_2)}O_3^{(s_1)}, \tag{226}$$
$$0 \approx_R O_3^{(\overline{s_1})}O_2^{(s_2)}O_1^{(\overline{s_3})}\varphi^{(s_1,s_2,s_3)}O_1^{(s_3)}O_2^{(s_2)}O_3^{(s_1)}, \tag{227}$$
$$0 \approx_R O_3^{(s_1)}O_2^{(\overline{s_2})}O_1^{(\overline{s_3})}\varphi^{(s_1,s_2,s_3)}O_1^{(s_3)}O_2^{(s_2)}O_3^{(s_1)}, \tag{228}$$
$$0 \approx_R O_3^{(\overline{s_1})}O_2^{(\overline{s_2})}O_1^{(\overline{s_3})}\varphi^{(s_1,s_2,s_3)}O_1^{(s_3)}O_2^{(s_2)}O_3^{(s_1)}. \tag{229}$$

The proofs of Eqs. (222)-(229) are as follows. Using Lemma 13 (i) (by noting $(O_2^{(b)})^\dagger O_2^{(b)} = O_2^{(b)} \leq I$), Eqs. (218) and (219) give

$$O_1^{(a)} \approx_{R,\varphi^{(s_1,s_2,s_3)}} \delta_{a,s_3} I \Rightarrow O_2^{(b)} O_1^{(a)} \approx_{R,\varphi^{(s_1,s_2,s_3)}} \delta_{a,s_3} O_2^{(b)}.$$

According to the value of s_3, this yields the following two approximate relations:

$$O_2^{(b)} O_1^{(s_3)} \approx_{R,\varphi^{(s_1,s_2,s_3)}} O_2^{(b)} \approx_{R,\varphi^{(s_1,s_2,s_3)}} \delta_{b,s_2} I, \tag{230}$$

$$O_2^{(b)} O_1^{(\overline{s_3})} \approx_{R,\varphi^{(s_1,s_2,s_3)}} 0. \tag{231}$$

By employing Eq. (220), Eqs. (230) and (231) respectively lead to

$$O_2^{(s_2)} O_1^{(s_3)} \approx_{R,\varphi^{(s_1,s_2,s_3)}} I \Rightarrow \begin{cases} O_3^{(s_1)} O_2^{(s_2)} O_1^{(s_3)} \approx_{R,\varphi^{(s_1,s_2,s_3)}} I \\ O_3^{(\overline{s_1})} O_2^{(s_2)} O_1^{(s_3)} \approx_{R,\varphi^{(s_1,s_2,s_3)}} 0 \end{cases} \tag{232}$$

$$O_2^{(\overline{s_2})} O_1^{(s_3)} \approx_{R,\varphi^{(s_1,s_2,s_3)}} 0 \Rightarrow O_3^{(c)} O_2^{(\overline{s_2})} O_1^{(s_3)} \approx_{R,\varphi^{(s_1,s_2,s_3)}} 0 \tag{233}$$

and

$$O_3^{(c)} O_2^{(b)} O_1^{(\overline{s_3})} \approx_{R,\varphi^{(s_1,s_2,s_3)}} 0. \tag{234}$$

There are eight approximate relations in Eqs. (232), (233) and (234), and combining each approximate relation with Lemma 18 derives Eqs. (222)-(229).

Now, we have Eq. (221), and $O_3^{(s_1)} O_2^{(s_2)} O_1^{(s_3)}$ in Eq. (221) is equal to as

$$|\phi_{\rm H}^{(s_1,s_2,s_3)}\rangle\langle\phi_{\rm H}^{(s_1,s_2,s_3)}| = O_3^{(s_1)} O_2^{(s_2)} O_1^{(s_3)}, \tag{235}$$

whose proof is as follows. We define $U := CCZ(H \otimes H \otimes H)$ with H denoting the Hadamard operator, and $|\phi_{\rm H}^{(0,0,0)}\rangle\langle\phi_{\rm H}^{(0,0,0)}|$ is rewritten as

$$\begin{aligned} |\phi_{\rm H}^{(0,0,0)}\rangle\langle\phi_{\rm H}^{(0,0,0)}| &= U|0,0,0\rangle\langle 0,0,0|U^\dagger \\ &= U \left(\frac{I_2^{\otimes 3} + \sigma_Z \otimes I_2^{\otimes 2}}{2} \frac{I_2^{\otimes 3} + I_2 \otimes \sigma_Z \otimes I_2}{2} \frac{I_2^{\otimes 3} + I_2^{\otimes 2} \otimes \sigma_Z}{2} \right) U^\dagger \\ &= \frac{I_2^{\otimes 3} + U(\sigma_Z \otimes I_2^{\otimes 2})U^\dagger}{2} \frac{I_2^{\otimes 3} + U(I_2 \otimes \sigma_Z \otimes I_2)U^\dagger}{2} \frac{I_2^{\otimes 3} + U(I_2^{\otimes 2} \otimes \sigma_Z)U^\dagger}{2}. \end{aligned}$$

Since a direct calculation leads to

$$U(\sigma_Z \otimes I_2 \otimes I_2)U^\dagger = O_3,\ U(I_2 \otimes \sigma_Z \otimes I_2)U^\dagger = O_2,\ U(I_2 \otimes I_2 \otimes \sigma_Z)U^\dagger = O_1,$$

we have

$$|\phi_{\rm H}^{(0,0,0)}\rangle\langle\phi_{\rm H}^{(0,0,0)}| = O_3^{(0)} O_2^{(0)} O_1^{(0)}.$$

Next, we define unitary operator $W := (\sigma_Z^{s_1} \otimes \sigma_Z^{s_2} \otimes \sigma_Z^{s_3})$, and a direct calculation leads to

$$\begin{aligned} |\phi_{\rm H}^{(s_1,s_2,s_3)}\rangle\langle\phi_{\rm H}^{(s_1,s_2,s_3)}| &= W|\phi_H^{(0,0,0)}\rangle\langle\phi_H^{(0,0,0)}|W^\dagger \\ &= W(O_3^{(0)} O_2^{(0)} O_1^{(0)})W^\dagger \\ &= (WO_3^{(0)}W^\dagger)(WO_2^{(0)}W^\dagger)(WO_1^{(0)}W^\dagger) \\ &= O_3^{(s_1)} O_2^{(s_2)} O_1^{(s_3)}. \end{aligned}$$

Hence, we obtain Eq. (235). Finally, substituting Eq. (235) into Eq. (221) and using Corollary 58 results in

$$V_S \sigma^{(1,s_1;1,s_2;1,s_3)} V_S^\dagger \approx_R |\phi_{\rm H}^{(s_1,s_2,s_3)}\rangle\langle\phi_{\rm H}^{(s_1,s_2,s_3)}| V_S \rho^{(111)} V_S^\dagger |\phi_{\rm H}^{(s_1,s_2,s_3)}\rangle\langle\phi_{\rm H}^{(s_1,s_2,s_3)}| \tag{236}$$

$$\overset{c}{\approx}_R \frac{1}{8} |\phi_{\rm H}^{(s_1,s_2,s_3)}\rangle\langle\phi_{\rm H}^{(s_1,s_2,s_3)}| \otimes \tilde{\tilde{\alpha}}_H. \tag{237}$$

By defining $\zeta^{(s_1,s_2,s_3)}$ to be the renormalized state of $\xi^{(s_1,s_2,s_3)} := \langle\phi_H^{(s_1,s_2,s_3)}|V_S\rho^{(111)}V_S^\dagger|\phi_{\rm H}^{(s_1,s_2,s_3)}\rangle$, the RHS of Eq. (236) equals to $|\phi_{\rm H}^{(s_1,s_2,s_3)}\rangle\langle\phi_{\rm H}^{(s_1,s_2,s_3)}|\otimes{\rm tr}[\xi^{(s_1,s_2,s_3)}]\zeta^{(s_1,s_2,s_3)}$. Then, using Eq. (237) results in

$$V_S\sigma^{(1,s_1;1,s_2;1,s_3)}V_S^\dagger\approx_R\frac{1}{8}|\phi_{\rm H}^{(s_1,s_2,s_3)}\rangle\langle\phi_{\rm H}^{(s_1,s_2,s_3)}|\otimes\zeta^{(s_1,s_2,s_3)}, \tag{238}$$

which shows the desired relation. Also, Eqs. (237) and (238) express the computationally indistinguishability of different $\zeta^{(s_1,s_2,s_3)}$. As a consequence of Eq. (238), we obtain the normalized version:

$$V_S\sigma'^{(1,s_1;1,s_2;1,s_3)}V^\dagger := \frac{V_S\sigma^{(1,s_1;1,s_2;1,s_3)}V_S^\dagger}{{\rm tr}[\sigma^{(1,s_1;1,s_2;1,s_3)}]}\approx_R|\phi_{\rm H}^{(s_1,s_2,s_3)}\rangle\langle\phi_{\rm H}^{(s_1,s_2,s_3)}|\otimes\zeta^{(s_1,s_2,s_3)}. \tag{239}$$

This is obtained by calculating as

$$\begin{aligned}
&\left|\left|V_S\sigma'^{(1,s_1;1,s_2;1,s_3)}V_S^\dagger-|\phi_{\rm H}^{(s_1,s_2,s_3)}\rangle\langle\phi_{\rm H}^{(s_1,s_2,s_3)}|\otimes\zeta^{(s_1,s_2,s_3)}\right|\right|_1\\
\le&\left|\left|8V_S\sigma^{(1,s_1;1,s_2;1,s_3)}V_S^\dagger-|\phi_{\rm H}^{(s_1,s_2,s_3)}\rangle\langle\phi_{\rm H}^{(s_1,s_2,s_3)}|\otimes\zeta^{(s_1,s_2,s_3)}\right|\right|+\left|\left|\left(1-8{\rm tr}[\sigma^{(1,s_1;1,s_2;1,s_3)}]\right)V_S\sigma'^{(1,s_1;1,s_2;1,s_3)}V_S^\dagger\right|\right|_1\\
\le&O(R)+\left|1-8{\rm tr}[\sigma^{(1,s_1;1,s_2;1,s_3)}]\right|\\
\le&O(R),
\end{aligned}$$

where the first inequality comes from the triangle inequality, the second one follows by Eq. (238) and the homogeneity of the trace norm, and the third one is from Eq. (238).

2. *Proof of (ii)*

We show (ii) for the case of $\boldsymbol{q}=000$. The other cases can be shown analogously. First, we have

$$\begin{aligned}
V_SP_{000}^{(abc)}V_S^\dagger&=V_SA_{1,\mathbf{0}}^{(a)}A_{2,\mathbf{0}}^{(b)}A_{3,\mathbf{0}}^{(c)}V_S^\dagger\\
&=V_S\left[\frac{I_{\mathcal H}+(-1)^aA_{1,\mathbf{0}}}{2}\frac{I_{\mathcal H}+(-1)^bA_{2,\mathbf{0}}}{2}\frac{I_{\mathcal H}+(-1)^cA_{3,\mathbf{0}}}{2}\right]V_S^\dagger,
\end{aligned}$$

where the first equation comes from using Eq. (6). Below, we prove

$$\begin{aligned}
V_SP_{000}^{(abc)}V_S^\dagger&\approx_{R,V_S\rho^{(\boldsymbol{\theta})}V_S^\dagger}\frac{I_2+(-1)^a\sigma_Z}{2}\otimes\frac{I_2+(-1)^b\sigma_Z}{2}\otimes\frac{I_2+(-1)^c\sigma_Z}{2}\otimes I_{\mathcal H}\\
&=|a\rangle\langle a|\otimes|b\rangle\langle b|\otimes|c\rangle\langle c|\otimes I_{\mathcal H}.
\end{aligned} \tag{240}$$

Once we have the following eight approximate relations, the triangle inequality of the state dependent norm implies Eq. (240).

(I) $V_SV_S^\dagger\approx_{R,V_S\rho^{(\boldsymbol{\theta})}V_S^\dagger}I_2^{\otimes3}\otimes I_{\mathcal H}$

(II) $V_SA_{1,\mathbf{0}}V_S^\dagger\approx_{R,V_S\rho^{(\boldsymbol{\theta})}V_S^\dagger}\sigma_Z\otimes I_2^{\otimes2}\otimes I_{\mathcal H}$

(III) $V_SA_{2,\mathbf{0}}V_S^\dagger\approx_{R,V_S\rho^{(\boldsymbol{\theta})}V_S^\dagger}I_2\otimes\sigma_Z\otimes I_2\otimes I_{\mathcal H}$

(IV) $V_SA_{3,\mathbf{0}}V_S^\dagger\approx_{R,V_S\rho^{(\boldsymbol{\theta})}V_S^\dagger}I_2^{\otimes2}\otimes\sigma_Z\otimes I_{\mathcal H}$

(V) $V_SA_{1,\mathbf{0}}A_{2,\mathbf{0}}V_S^\dagger\approx_{R,V_S\rho^{(\boldsymbol{\theta})}V_S^\dagger}\sigma_Z\otimes\sigma_Z\otimes I_2\otimes I_{\mathcal H}$

(VI) $V_SA_{1,\mathbf{0}}A_{3,\mathbf{0}}V_S^\dagger\approx_{R,V_S\rho^{(\boldsymbol{\theta})}V_S^\dagger}\sigma_Z\otimes I_2\otimes\sigma_Z\otimes I_{\mathcal H}$

(VII) $V_SA_{2,\mathbf{0}}A_{3,\mathbf{0}}V_S^\dagger\approx_{R,V_S\rho^{(\boldsymbol{\theta})}V_S^\dagger}I_2\otimes\sigma_Z\otimes\sigma_Z\otimes I_{\mathcal H}$

(VIII) $V_SA_{1,\mathbf{0}}A_{2,\mathbf{0}}A_{3,\mathbf{0}}V_S^\dagger\approx_{R,V_S\rho^{(\boldsymbol{\theta})}V_S^\dagger}\sigma_Z\otimes\sigma_Z\otimes\sigma_Z\otimes I_{\mathcal H}$

We can prove (I) from a direct calculation using the definition of the state dependent norm. As for (II)-(VIII), these have already been proven in Eq. (94), Lemma 47, Lemma 52, Eq. (186) in Lemma 59, Eq. (187) in Lemma 59, Eq. (188) in Lemma 59 and Eq. (194) in Lemma 60, respectively.

Now we have Eq. (240), and Eq. (240) and Lemma 13 (ii) imply

$$V_S P_{000}^{(abc)} V_S^\dagger \approx_{R, V_S\sigma^{(1,s_1;1s_2;1,s_3)}V_S^\dagger} |a\rangle\langle a| \otimes |b\rangle\langle b| \otimes |c\rangle\langle c| \otimes I_{\mathcal{H}}.$$

Hence, Lemma 18 leads to

$$\begin{aligned} V_S P_{000}^{(abc)} \sigma^{(1,s_1;1s_2;1,s_3)} P_{000}^{(abc)} V_S^\dagger &= (V_S P_{000}^{(abc)} V_S^\dagger)(V_S \sigma^{(1,s_1;1s_2;1,s_3)} V_S^\dagger)(V_S P_{000}^{(abc)} V_S^\dagger) \\ &\approx_R (|a\rangle\langle a| \otimes |b\rangle\langle b| \otimes |c\rangle\langle c| \otimes I_{\mathcal{H}})(V_S \sigma^{(1,s_1;1s_2;1,s_3)} V_S^\dagger)(|a\rangle\langle a| \otimes |b\rangle\langle b| \otimes |c\rangle\langle c| \otimes I_{\mathcal{H}}). \end{aligned} \tag{241}$$

Since acting projector does not increase trace distance [8], using Theorem 62 (i) enables us to replace $V_S\sigma^{(1,s_1;1s_2;1,s_3)}V_S^\dagger$ with

$$\frac{1}{8}|\phi_{\mathrm{H}}^{(a,b,c)}\rangle\langle\phi_{\mathrm{H}}^{(a,b,c)}| \otimes \zeta^{(s_1,s_2,s_3)},$$

which is the desired relation. Note that by following the same discussions done to obtain Eq. (239), we have the normalized version of Eq. (241) with the normalized state $\sigma'^{(1,s_1;1s_2;1,s_3)}$:

$$V_S P_{000}^{(abc)} \sigma'^{(1,s_1;1s_2;1,s_3)} P_{000}^{(abc)} V_S^\dagger \approx_R (|a\rangle\langle a| \otimes |b\rangle\langle b| \otimes |c\rangle\langle c|)|\phi_{\mathrm{H}}^{(a,b,c)}\rangle\langle\phi_{\mathrm{H}}^{(a,b,c)}|(|a\rangle\langle a| \otimes |b\rangle\langle b| \otimes |c\rangle\langle c|) \otimes \zeta^{(s_1,s_2,s_3)}.$$

■

VI. PROTOCOL FOR PROOF OF MAGIC

In this section, we show the details of our protocol for the proof of magic presented in the main text. Our protocol for the proof of magic exploits Eq. (239), which states that there exists a positive constant c' and a negligible function $\mathrm{negl}_1(\lambda)$ satisfying

$$\begin{aligned} &\left|\left|V_S\sigma'^{(1,s_1;1,s_2;1,s_3)}V_S^\dagger - |\phi_{\mathrm{H}}^{(s_1,s_2,s_3)}\rangle\langle\phi_{\mathrm{H}}^{(s_1,s_2,s_3)}| \otimes \zeta^{(s_1,s_2,s_3)}\right|\right|_1^2 \\ \le& c'\left(p_{\mathrm{Pre}}^r + p_{\mathrm{Test}}^r + p_{\mathrm{Hyper}}^r\right) + \mathrm{negl}_1(\lambda) \\ \le& \left[\sqrt{c'}\left(\sqrt{p_{\mathrm{Pre}}^r} + \sqrt{p_{\mathrm{Test}}^r} + \sqrt{p_{\mathrm{Hyper}}^r}\right) + \sqrt{\mathrm{negl}_1(\lambda)}\right]^2 =: T^2. \end{aligned} \tag{242}$$

For simplicity of notations, we define $c := \sqrt{c'}$ and $\mathrm{negl}_2(\lambda) := \sqrt{\mathrm{negl}_1(\lambda)}$ (note that the square root of a negligible function is also a negligible one). Since the exact value of T cannot be obtained by repeating the protocols in a finite number of times, we need to estimate it from the number of set flags. Specifically, our goal is to derive the estimated value T_{est} of T satisfying

$$\Pr\left[|T - T_{\mathrm{est}}| \le \epsilon\right] \ge 1 - \delta$$

for an $\epsilon > 0$ and $\delta > 0$. Below, we show that when these ϵ and δ are constant, the number of repeating our protocol for the proof of magic is also constant.

---

[8] Specifically, for any linear operators $A, B \in \mathcal{L}(\mathcal{H})$ and any projector $P \in \mathcal{L}(\mathcal{H})$,

$$||PAP - PBP||_1 \le ||A - B||_1$$

is satisfied. This can be proven by writing the trace norm as $||A||_1 = \max_{X\in\mathcal{L}(\mathcal{H}):||X||_\infty\le 1} |\mathrm{tr}[XA]|$ and calculating as

$$\begin{aligned} ||PAP - PBP||_1 =& \max_{X\in\mathcal{L}(\mathcal{H}):||X||_\infty\le 1} |\mathrm{tr}[PXP(A-B)]| \\ \le& \max_{Y\in\mathcal{L}(\mathcal{H}):||Y||_\infty\le 1} |\mathrm{tr}[Y(A-B)]| \\ =& ||A - B||_1. \end{aligned}$$

From the numbers of set flags obtained at step 1 of our protocol, we have the estimated value p'_a of p_a for each $\mathrm{a} \in \{\mathrm{Pre}, \mathrm{Test}, \mathrm{Hyper}\}$ by employing Hoeffding's inequality as

$$\Pr\left[|p_a - p'_a| \leq \epsilon'\right] \geq 1 - \delta' \tag{243}$$

for an $\epsilon' > 0$ and $\delta' > 0$. This relation can be obtained by repeating

$$N_{\epsilon',\delta'} := O\left(\frac{1}{\epsilon'^2} \ln \frac{1}{\delta'}\right)$$

times of the protocol on average. Using these estimated probabilities $p'_{\mathrm{Pre}}, p'_{\mathrm{Test}}$ and p'_{Hyper}, we define the estimated value of the trace norm T_{est} as

$$T_{\mathrm{est}} := c\left(\sqrt{p'^r_{\mathrm{Pre}}} + \sqrt{p'^r_{\mathrm{Test}}} + \sqrt{p'^r_{\mathrm{Hyper}}}\right) + \mathrm{negl}_2(\lambda). \tag{244}$$

Then, by substituting the definitions in Eqs. (242) and (244) to $|T - T_{\mathrm{est}}|$, we have

$$|T - T_{\mathrm{est}}| = c\left|\sum_{\mathrm{a}\in\{\mathrm{Pre,Test,Hyper}\}} (\sqrt{p^r_{\mathrm{a}}} - \sqrt{p'^r_{\mathrm{a}}})\right| \leq c \sum_{\mathrm{a}\in\{\mathrm{Pre,Test,Hyper}\}} \left|\sqrt{p^r_{\mathrm{a}}} - \sqrt{p'^r_{\mathrm{a}}}\right|.$$

Using the result in Eq. (243), with probability at least $(1-\delta')^3 \geq 1 - 3\delta'$, we obtain

$$|T - T_{\mathrm{est}}| \leq \begin{cases} c\sum_{\mathrm{a}\in\{\mathrm{Pre,Test,Hyper}\}} \left(\sqrt{(p_{\mathrm{a}} + \epsilon')^r} - \sqrt{p^r_{\mathrm{a}}}\right) & (\text{if } p'_a \geq p_a) \\ c\sum_{\mathrm{a}\in\{\mathrm{Pre,Test,Hyper}\}} \left(\sqrt{p^r_{\mathrm{a}}} - \sqrt{(p_{\mathrm{a}} - \epsilon')^r}\right) & (\text{if } p'_a < p_a). \end{cases}$$

In the case of $p'_a \geq p_a$, by a simple calculation, it is easy to find that $\sqrt{(p_{\mathrm{a}} + \epsilon')^r}$ is upper-bounded by

$$\sqrt{(p_{\mathrm{a}} + \epsilon')^r} \leq \begin{cases} \sqrt{p^r_{\mathrm{a}}} + \sqrt{\epsilon'^r} & (0 < \frac{r}{2} < 1) \\ \sqrt{p^r_{\mathrm{a}}} + (\sqrt{2^r} - 1)\epsilon' & (\frac{r}{2} \in \mathbb{N}) \\ \sqrt{p^r_{\mathrm{a}}} + (2\sqrt{2^r} - 1)\epsilon'^x & (1 \leq \frac{r}{2}, \frac{r}{2} \notin \mathbb{N}), \end{cases}$$

where in the third case, we express $r/2$ as $x+n$ with x $(0 < x < 1)$ being the decimal number and n being the integer. Hence, $\sqrt{(p_{\mathrm{a}} + \epsilon')^r} \leq \sqrt{p^r_{\mathrm{a}}} + O(\epsilon'^t)$ holds with t being a non-zero constant value.

In the other case of $p'_a < p_a$, when $p_a < \epsilon'$, $\sqrt{p^r_a} - \sqrt{p'^r_a} \leq \sqrt{p^r_a} < \sqrt{\epsilon'^r}$. When $p_a \geq \epsilon'$, by a simple calculation, it is easy to find that $\sqrt{(p_{\mathrm{a}} - \epsilon')^r}$ is lower-bounded by

$$\sqrt{(p_{\mathrm{a}} - \epsilon')^r} \geq \begin{cases} \sqrt{p^r_{\mathrm{a}}} - \sqrt{\epsilon'^r} & (0 < \frac{r}{2} < 1) \\ \sqrt{p^r_{\mathrm{a}}} - (\sqrt{2^r} - 1)\epsilon' & (\frac{r}{2} \in \mathbb{N}) \\ \sqrt{p^r_{\mathrm{a}}} - \sqrt{2^r}\epsilon'^x & (1 \leq \frac{r}{2}, \frac{r}{2} \notin \mathbb{N}), \end{cases}$$

where in the third case, we express $r/2$ as $x+n$ with x $(0 < x < 1)$ being the decimal number and n being the integer. Hence, $\sqrt{(p_{\mathrm{a}} + \epsilon')^r} \leq \sqrt{p^r_{\mathrm{a}}} + O(\epsilon'^t)$ holds with t being a non-zero constant value.

By combining the arguments so far, as c is a constant value, we finally obtain

$$\Pr\left[|T - T_{\mathrm{est}}| \leq O(\epsilon'^t)\right] \geq 1 - 3\delta'.$$

By setting $\delta = 3\delta'$ and $\epsilon = O(\epsilon'^t)$, if δ and ϵ are constant, then the number of times $N_{\epsilon',\delta'}$ repeating the Protocol 1 at step 1 results in the constant number.

In the main text, we have set $\epsilon = 1/6$ and $\delta = 10^{-10}$ for simplicity of the arguments, but for any $\epsilon > 0$ and $\delta > 0$, the number of times repeating the Protocol 1 at step 1 of our protocol for the proof of magic becomes constant.

[1] U. Mahadev, Proceedings of the 59th Annual Symposium on Foundations of Computer Science (2018) pp.259-267 (2018).
[2] T. Metger and T. Vidick, Quantum **5**, 544 (2021).
[3] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[4] M. Wilde, arXiv:1106.1445 (2011).
[5] A. Gheorghiu and T. Vidick, arXiv:1904.06320 (2019).