Proofs of Quantumness from Trapdoor Permutations

Tomoyuki Morimae[1] and Takashi Yamakawa[1,2]

[1] Yukawa Institute for Theoretical Physics, Kyoto University, Kyoto, Japan
[2] NTT Social Informatics Laboratories, Tokyo, Japan

Abstract. Assume that Alice can do only classical probabilistic polynomial-time computing while Bob can do quantum polynomial-time computing. Alice and Bob communicate over only classical channels, and finally Bob gets a state $|x_0\rangle + |x_1\rangle$ with some bit strings x_0 and x_1. Is it possible that Alice can know $\{x_0, x_1\}$ but Bob cannot? Such a task, called *remote state preparations*, is indeed possible under some complexity assumptions, and is bases of many quantum cryptographic primitives such as proofs of quantumness, (classical-client) blind quantum computing, (classical) verifications of quantum computing, and quantum money. A typical technique to realize remote state preparations is to use 2-to-1 trapdoor collision resistant hash functions: Alice sends a 2-to-1 trapdoor collision resistant hash function f to Bob, and Bob evaluates it coherently, i.e., Bob generates $\sum_x |x\rangle|f(x)\rangle$. Bob measures the second register to get the measurement result y, and sends y to Alice. Bob's post-measurement state is $|x_0\rangle + |x_1\rangle$, where $f(x_0) = f(x_1) = y$. With the trapdoor, Alice can learn $\{x_0, x_1\}$ from y, but due to the collision resistance, Bob cannot. This Alice's advantage can be leveraged to realize the quantum cryptographic primitives listed above. It seems that the collision resistance is essential here. In this paper, surprisingly, we show that the collision resistance is not necessary for a restricted case: we show that (non-verifiable) remote state preparations of $|x_0\rangle + |x_1\rangle$ secure against *classical* probabilistic polynomial-time Bob can be constructed from classically-secure (full-domain) trapdoor permutations. Trapdoor permutations are not likely to imply the collision resistance, because black-box reductions from collision-resistant hash functions to trapdoor permutations are known to be impossible. As an application of our result, we construct proofs of quantumness from classically-secure (full-domain) trapdoor permutations.

1 Introduction

Let us consider a two-party interactive protocol between Alice and Bob. Alice can do only classical probabilistic polynomial-time computing while Bob can do quantum polynomial-time computing. Alice and Bob communicate over only classical channels. After the interaction, Alice finally outputs a pair $\{x_0, x_1\}$ of n-bit strings $x_0, x_1 \in \{0,1\}^n$. If Bob behaves

honestly, he finally outputs the n-qubit state $|x_0\rangle + |x_1\rangle$.[3] On the other hand, no malicious Bob can learn $\{x_0, x_1\}$. Such a task, called *remote state preparations* [DK16,CCKW19,GV19][4], is indeed possible under some complexity assumptions, and is bases of many quantum cryptographic primitives such as proofs of quantumness [BCM+21], (classical-client) blind quantum computing [BFK09,CCKW19,BCC+20], (classical) verifications of quantum computing [Mah18b,GV19], and quantum money [RS19]. In fact, if Alice can generate a quantum state $|x_0\rangle + |x_1\rangle$ and send it to Bob over a quantum channel, Alice can enjoy several advantages over Bob. For example, Bob cannot know the complete classical description of the state, he cannot clone the state, and he has to disturb the state if he measures it, etc. Such an inequivalence between Alice and Bob is clearly useful for quantum cryptography. Remote state preparations somehow "simulate" such situations, and can replace quantum channels with classical channels for some applications.

A typical technique to realize remote state preparations is to use 2-to-1 trapdoor collision resistant hash functions [BCM+21][5]: Alice sends a 2-to-1 trapdoor collision resistant hash function f to Bob, and Bob evaluates it coherently, i.e., Bob generates $\sum_x |x\rangle|f(x)\rangle$. Bob measures the second register to get the measurement result y, and sends y to Alice. Bob's post-measurement state is $|x_0\rangle + |x_1\rangle$, where $f(x_0) = f(x_1) = y$. With the trapdoor, Alice can learn $\{x_0, x_1\}$ from y, but due to the collision resistance, Bob cannot. This Alice's advantage can be leveraged to realize the quantum cryptographic primitives listed above.

---

[3] For simplicity, in this paper, we often omit the normalization factors of quantum states.

[4] Generally speaking, remote state preparations are the task that a classical Alice delegates preparations of quantum states to quantum Bob over a classical channel in such a way that Bob cannot learn which states he is generating. [CCKW19] considered remote state preparations of random single-qubit states for the applications to classical-client blind quantum computing. In this paper, on the other hand, we focus on remote state preparations of an equal-weight superposition $|x_0\rangle + |x_1\rangle$ of two n-qubit computational basis states. Moreover, note that there are also *verifiable* remote state preparations [GV19] where Alice can check whether Bob has generated correct states or not. Verifiability is not necessary for some applications such as classical-client blind quantum computing, but seems to be necessary for some applications such as classical verifications of quantum computing. In this paper, we do not consider the verifiability.

[5] A function $f : \mathcal{X} \to \mathcal{Y}$ is 2-to-1 if $|\{x \in \mathcal{X} \mid f(x) = y\}| = 2$ for all $y \in \mathcal{Y}$. A function f is called a trapdoor collision resistant hash function if given f it is hard to find x and x' such that $f(x) = f(x')$, but it becomes easy if a trapdoor is available.

1.1 Our Results

The collision resistance seems to be essential for remote state preparations (and many other quantum cryptographic primitives over classical channels.) In this paper, surprisingly, we show that the collision resistance is not necessary for a restricted case. We show the following result.

Theorem 1.1. *(Non-verifiable) remote state preparations of $|x_0\rangle + |x_1\rangle$ secure against* **classical** *probabilistic polynomial-time Bob can be constructed from classically-secure (full-domain) trapdoor permutations.*

Here, non-verifiable remote state preparations are remote state preparations that are blind but not verifiable, i.e., no malicious Bob can learn which states he is generating, but Alice cannot verify whether Bob has generated correct states or not. (A formal definition is given in Definition 2.1.) A classically-secure trapdoor permutation is a permutation $f : \mathcal{X} \to \mathcal{X}$ such that inverting it is hard for classical probabilistic polynomial-time adversaries, but it is easy if a trapdoor is available. Full-domain means that $\mathcal{X} = \{0,1\}^n$. (The formal definition is given in Definition 2.3.) A proof of Theorem 1.1 is given in Sec. 3.

Trapdoor permutations are not likely to imply the collision resistance, because black-box reductions from collision-resistant hash functions to trapdoor permutations are known to be impossible [HHRS15,HY20]. Classically-secure full-domain trapdoor permutations can be instantiated with the hardness of factoring [BM92,GR13].

We emphasize that our remote state preparations in Theorem 1.1 are proven to be secure against only *classical* Bob, which unfortunately restricts the applications of our result. We do not know how to achieve the quantum security. This is an important open problem. (For more discussion, see Sec. 1.3.)

As an application of Theorem 1.1, we construct proofs of quantumness.

Theorem 1.2. *Proofs of quantumness can be constructed from classically-secure (full-domain) trapdoor permutations.*

Its proof is given in Sec. 4. Proofs of quantumness are two-party protocols between a probabilistic polynomial-time verifier and a prover. A quantum polynomial-time prover can make the verifier accept with high probability, but no probabilistic polynomial-time prover is accepted by the verifier except for a negligible probability. (For a formal definition of proofs of quantumness, see Definition 2.2.) The first construction of proofs of quantumness [BCM+21] is based on trapdoor injective claw-free

functions with the special property called adaptive-hardcore-bit property. Here, an injective claw-free means that given a pair (f_0, f_1) of injective functions, it is hard to find (x_0, x_1) such that $f_0(x_0) = f_1(x_1)$. The adaptive-hardcore-bit property roughly means that given (f_0, f_1), it is hard to find one x_b of a claw (x_0, x_1) and d such that $d \cdot (x_0 \oplus x_1) = 0$ at the same time. It is easy to see that injective claw-free functions imply the collision resistance. [6] A recent paper [KMCVY22] has improved the result of [BCM+21] by removing the necessity of the adaptive-hardcore-bit property. However, it still uses 2-to-1 trapdoor collision resistant hash functions. Our Theorem 1.2 removes the necessity of the collision resistance of [KMCVY22].

1.2 Technical Overview

Our construction of remote state preparations from trapdoor permutations (Theorem 1.1) is based on the statistically-hiding and computationally-binding commitment scheme from one-way permutations [NOVY93], which is explained as follows. Let $f : \{0,1\}^n \to \{0,1\}^n$ be a one-way permutation.

1. The sender of the commitment scheme chooses $x \leftarrow \{0,1\}^n$, and computes $y := f(x)$.
2. The receiver of the commitment scheme chooses $h_j \leftarrow 0^{j-1}1\{0,1\}^{n-j}$ for each $j = 1, 2, ..., n-1$.
3. The receiver and the sender repeat the following procedure for $j = 1, 2, ..., n-1$:
   (a) The receiver sends h_j to the sender.
   (b) The sender returns the value $c_j := h_j \cdot y$ to the receiver.[7]
4. The receiver and the sender finally obtain the system of linear equations $\{h_j \cdot y = c_j\}_{j=1}^{n-1}$ that has two solutions $y_0, y_1 \in \{0,1\}^n$, where y_0 is the lexicographically smaller one. Let $c \in \{0,1\}$ be such that $y_c = y$. The sender sends $b \oplus c$ to the receiver as the commitment of the bit $b \in \{0,1\}$.
5. The opening for the commitment is x and b.

It is shown in [NOVY93] that if a probabilistic polynomial-time sender can find both x_0 and x_1 such that $f(x_0) = y_0$ and $f(x_1) = y_1$ with a

---

[6] Let us define a function g by $g(0x) := f_0(x)$ and $g(1x) := f_1(x)$. Assume that a collision (α, β) of g is easily found, i.e., $g(\alpha) = g(\beta)$. Then, due to the injectivity of f_0 and f_1, the first bit of α and β should be different. Without loss of generality, assume that $\alpha = 0x_0$ and $\beta = 1x_1$. Then, (x_0, x_1) is a claw of (f_0, f_1).

[7] For two bit strings $a, b \in \{0,1\}^n$, $a \cdot b$ is the bitwise inner product, i.e., $a \cdot b := \bigoplus_{j=1}^n a_j b_j$.

non-negligible probability, then a probabilistic polynomial-time adversary that breaks the security of the one-way permutation f can be constructed, which shows the (classical) computational binding of the scheme.

What happens if this NOVY's interactive hashing is run coherently? Namely, let us consider the following "quantum version" of the NOVY's interactive hashing:

1. A quantum polynomial-time Bob prepares $\sum_{x \in \{0,1\}^n} |x\rangle$.
2. A probabilistic polynomial-time Alice chooses $h_j \leftarrow 0^{j-1}1\{0,1\}^{n-j}$ for each $j = 1, 2, ..., n-1$.
3. Alice sends h_1 to Bob.
4. Bob generates

$$\sum_{x \in \{0,1\}^n} |x\rangle |h_1 \cdot f(x)\rangle,$$

   measures the second register to get the measurement result $c_1 \in \{0,1\}$, and sends c_1 to Alice. The post-measurement state is

$$\sum_{x \in \{0,1\}^n : h_1 \cdot f(x) = c_1} |x\rangle.$$

5. Alice sends h_2 to Bob.
6. Bob generates

$$\sum_{x \in \{0,1\}^n : h_1 \cdot f(x) = c_1} |x\rangle |h_2 \cdot f(x)\rangle,$$

   measures the second register to get the measurement result $c_2 \in \{0,1\}$, and sends c_2 to Alice. The post-measurement state is

$$\sum_{x \in \{0,1\}^n : h_1 \cdot f(x) = c_1, h_2 \cdot f(x) = c_2} |x\rangle.$$

7. If they repeat the above procedure for $j = 3, 4, ..., n-1$, Bob finally possesses the state $|x_0\rangle + |x_1\rangle$, where $f(x_0) = y_0$, $f(x_1) = y_1$, and (y_0, y_1) is the two solutions of $\{h_j \cdot y = c_j\}_{j=1}^{n-1}$.

By the (classical) computational-binding of the NOVY's commitment scheme, no probabilistic polynomial-time Bob can learn both x_0 and x_1 at the same time with non-negligible probability. If f is a trapdoor permutation, Alice can compute both x_0 and x_1, and it is clear that the existence of the trapdoor does not degrade the security against Bob.

In this way, we can construct remote state preparations of $|x_0\rangle +$ $|x_1\rangle$ secure against classical Bob from trapdoor permutations. Proofs of quantumness can be constructed from it based on a similar idea of [KMCVY22], which is a proof of Theorem 1.2: The verifier and the prover first run remote state preparations of $|x_0\rangle + |x_1\rangle$. Then, with probability $1/2$, the verifier asks the prover to measure the state in the computational basis. If the prover returns a correct x_0 or x_1, the verifier accepts. With probability $1/2$, the verifier chooses $r \leftarrow \{0,1\}^n$ and sends it to the prover. The prover generates the state $|r \cdot x_0\rangle|x_0\rangle + |r \cdot x_1\rangle|x_1\rangle$, and measures the second register in the Hadamard basis. If the measurement result is $d \in \{0,1\}^n$, the post-measurement state is $|r \cdot x_0\rangle + (-1)^{d \cdot (x_0 \oplus x_1)}|r \cdot x_1\rangle$, i.e., one of the BB84 states. Then, runing the CHSH game on it leads to proofs of quantumness: the quantum polynomial-time prover can output the correct measurement result with high probability, but no probabilistic polynomial-time prover can output the correct measurement result except for a small probability.

1.3 Open Problems

Our novel idea of running the NOVY's interactive hashing coherently will have many other interesting applications. Let us summarize several open problems.

Weakening assumptions. Our constructions of remote state preparations and proofs of quantumness are based on the full-domain trapdoor permutations. One important open problem is whether the assumption can be weakened or not.

First, can we remove the full-domain property? Though the factoring-based constructions can be made full-domain [BM92, GR13], it is not true in general. For example, the construction of trapdoor permutations based on indistinguishability obfuscation (iO) [BPW16] is not full-domain. In many applications of trapdoor permutations like oblivious transfers [EGL85] and non-interactive zero-knowledge [FLS99], the full-domain property can be weakened to a property called the *doubly enhanced* property [GR13]. Can we replace full-domain trapdoor permutations in our constructions with (non-full-domain) doubly enhanced trapdoor permutations? If this is possible, then we would obtain proofs of quantumness from iO and one-way functions since the iO-based trapdoor permutation [BPW16] satisfies the doubly enhanced property. (Or, it is an interesting open problem whether remote state preparations or proofs of quantumness can be directly constructed from iO (plus one-way functions).)

Second, it is known that the NOVY's commitment scheme with one-way permutations can be improved to that with regular one-way functions [HHK$^+$05] or even any one-way functions [HNO$^+$09].[8] Can we construct remote state preparations or proofs of quantumness from trapdoor functions, not permutations? Known instantiations of trapdoor permutations are only factoring-based ones (for full-domain cases) and iO-based ones (for non-full-domain cases). However, trapdoor functions have many instantiations from Diffie-Hellman assumptions [PW08,GH18], learning with errors [PW08,GPV08], NTRU [HPS98], and coding theory [McE78,Nie86], etc. A potential approach is to coherently run the variant of the NOVY's commitment based on regular one-way functions [HHK$^+$05] since trapdoor functions are automatically regular. However, in such a construction, the state which the honest Bob gets after the interaction is not a superposition of two computational-basis states, $|x_0\rangle + |x_1\rangle$, but that of many computational-basis states, i.e., $\sum_{x \in S} |x\rangle$ with $|S|$ being polynomially or even exponentially large. We do not know how to construct proofs of quantumness from such a superposition of many computational-basis states.

Finally, can we remove even the trapdoor? Is it possible to construct remote state preparations or proofs of quantumness from one-way functions? A recent work [YZ22] constructs proofs of quantumness in the quantum random oracle model. This demonstrates that trapdoors are not inherent for proofs of quantumness. However, a standard-model instantiation of their protocol based on standard assumptions is likely to require a completely new idea.

Other applications. The other important open problem is whether we can construct other quantum cryptographic primitives, such as (classical-client) blind quantum computing and (classical) verifications of quantum computing from trapdoor permutations (or even trapdoor/one-way functions). For that goal, we have to show the *quantum* security of the NOVY's scheme. (Remember that our remote state preparations are known to be secure against only *classical* Bob, because we do not show the security of the NOVY's scheme against quantum adversaries.) The security proof of [NOVY93] makes heavy use of the rewinding technique, and therefore showing the quantum security of NOVY's scheme seems to be a challenging open problem, which is of independent interest.

---

[8] We say that a one-way functions is regular if the preimage sizes are equal for all images.

1.4 Related Works

Remote state preparations. The first construction of (non-verifiable) remote state preparations of single-qubit states so called "QFactory" [CCKW19] used certain 2-to-1 trapdoor collision resistant hash functions with some homomorphic predicates, which can be constructed from the LWE assumption. [GV19,Zha22,GMP22] constructed verifiable remote state preparations of single-qubit states that use the (noisy) trapdoor injective claw-free functions of [BCM+18].

Proofs of quantumness. A simple way of achieving "proofs of quantumness" is to ask the prover to solve (non-interactive) problems in **NP** that can be solved in quantum polynomial-time but are believed to be hard for probabilistic polynomial-time, such as factoring [Sho94], Pell's equation [Hal02], and matrix group membership [BBS09], etc. In this paper, however, we do not consider such approaches.

The original construction [BCM+21] of proofs of quantumness required the adaptive-hardcore-bit property. [BKVV20,KMCVY22] removed the necessity of the adaptive-hardcore-bit property, but [BKVV20] used 2-to-1 trapdoor injective claw-free functions and random oracles that can be queried coherently, and [KMCVY22] used 2-to-1 trapdoor collision resistant hash functions.

Publicly-verifiable proofs of quantumness were also studied. One-shot signatures [AGKZ20] imply proofs of quantumness, but the known construction of one-shot signatures is based on one-shot chameleon hash functions, which satisfy the collision resistance. Moreover, the known construction assumes classical oracles that can be queried coherently. [YZ22] constructed publicly-verifiable non-interactive proofs of quantumness with random oracles. Note that random oracles are collision-resistant.

Recently, [KLVY22] showed a general compiler to transform non-local games to proofs of quantumness via quantum homomorphic encryptions (QHE). Their assumption is only the existence of QHE for certain class of quantum operations (such as controlled-Hadamard gates), which can be instantiated with LWE [Mah18a]. Although homomorphic encryptions generally imply the collision resistance [IKO05], it is not known whether the restricted QHE used in [KLVY22] implies the collision resistance.

The idea of [KLVY22] is that the quantum prover generates a bipartite state, and the classical verifier remotely measures one of the registers via QHE so that the prover gets an unknown state of the other register. It therefore can be also considered as (non-verifiable) remote state preparations via QHE. Remote state preparations via QHE were also introduced in

[Shm21,Shm22] in the contexts of quantum money and quantum tokenized signatures.

2 Preliminaries

We use the standard notations of quantum computing and cryptography. We use λ as the security parameter. $x \leftarrow A$ means that an element x is sampled uniformly at random from the set A. negl is a negligible function, and poly is a polynomial. For an algorithm A, $y \leftarrow A(x)$ means that the algorithm A outputs y on input x. For two bit strings $a, b \in \{0,1\}^n$, $a \cdot b$ is the bitwise inner product, i.e., $a \cdot b \coloneqq \bigoplus_{j=1}^n a_j b_j$.

Non-verifiable remote state preparations of $|x_0\rangle + |x_1\rangle$ secure against probabilistic polynomial-time Bob are defined as follows.

Definition 2.1 (Remote State Preparations). *Non-verifiable remote state preparations of $|x_0\rangle + |x_1\rangle$ secure against probabilistic polynomial-time Bob are two-party interactive protocols between probabilistic polynomial-time Alice and quantum/probabilistic polynomial-time Bob over a classical channel that satisfy the following two conditions.*

Perfect correctness: *If quantum polynomial-time Bob behaves honestly, Alice outputs a pair $\{x_0, x_1\}$ of two n-bit strings $x_0, x_1 \in \{0,1\}^n$ and Bob outputs the n-qubit state $|x_0\rangle + |x_1\rangle$ with probability 1.*

Classical security (blindness): *For any probabilistic polynomial-time malicious Bob that outputs a pair $\{\alpha, \beta\}$ of two n-bit strings $\alpha, \beta \in \{0,1\}^n$,*

$$\Pr[\{x_0, x_1\} = \{\alpha, \beta\} : \{x_0, x_1\} \leftarrow Alice, \{\alpha, \beta\} \leftarrow Bob] \leq \mathsf{negl}(\lambda).$$

Remark 2.1. Our definition is different from previous ones [CCKW19,GV19] in the following two points. First, they are interested in remotely generating single-qubit states while we consider remote generations of $|x_0\rangle + |x_1\rangle$. Second, [CCKW19,GV19] consider the security against quantum Bob, while we consider the one against only *classical* Bob. It is an important open problem whether we can show the quantum security.

Remark 2.2. Remote state preparations can have the *verifiability* [GV19], which roughly means that Alice can check whether Bob has generated correct states or not. Some applications, such as classical-client blind quantum computing, do not require the verifiability, but it seems that verifiability is necessary for some applications, such as classical verifications of quantum computing. In this paper, we do not consider verifiability.

Remark 2.3. We can consider non-perfect correctness, but in this paper we consider only perfect correctness, because our construction satisfies it. Moreover, it is reasonable to assume in the definition that Alice sometimes outputs $\perp$. However, for simplicity, we assume that Alice never outputs $\perp$. In fact, our construction satisfies it.

Proofs of quantumness are defined as follows.

Definition 2.2 (Proofs of Quantumness). *Proofs of quantumness are two-party protocols between a probabilistic polynomial-time verifier $\mathcal{V}$ and a quantum/probabilistic polynomial-time prover $\mathcal{P}$ over a classical channel such that $\mathcal{V}$ finally outputs $\top$ or $\perp$. We require that the following two conditions, α-correctness and β-soundness, are satisfied for some α and β such that $\alpha - \beta \geq \frac{1}{\mathrm{poly}(\lambda)}$.*

α**-correctness:** *There exists a quantum polynomial-time prover $\mathcal{P}$ such that $\Pr[\mathcal{V} \to \top] \geq \alpha$.*

β**-soundness:** *For any probabilistic polynomial-time prover $\mathcal{P}$, $\Pr[\mathcal{V} \to \top] \leq \beta$.*

Classically-secure full-domain trapdoor permutations are defined as follows.

Definition 2.3 (Trapdoor Permutations). *A family $\{f_k\}_{k \in \mathcal{K}_\lambda}$ of permutations is called a classically-secure full-domain trapdoor permutation family if there is a tuple of algorithms $(\mathsf{Gen}, \mathsf{Eval}, \mathsf{Inv})$ such that*

- $\mathsf{Gen}(1^\lambda) \to (\mathsf{td}, k)$: *It is a probabilistic polynomial-time algorithm that, on input the security parameter λ, outputs a trapdoor td and a key k.*
- $\mathsf{Eval}(x, k) \to x'$: *It is a classical polynomial-time deterministic algorithm that, on input k and a bit string $x \in \{0,1\}^n$, outputs a bit string $x' \in \{0,1\}^n$.*
- $\mathsf{Inv}(\mathsf{td}, x') \to x''$: *It is a classical polynomial-time deterministic algorithm that, on input x' and td, outputs a bit string x''.*

We require the following two types of correctness and the security.

Evaluation correctness: *For any $x \in \{0,1\}^n$,*

$$\Pr[x' = f_k(x) : x' \leftarrow \mathsf{Eval}(x, k), (\mathsf{td}, k) \leftarrow \mathsf{Gen}(1^\lambda)] = 1.$$

Inversion correctness: *For any $x \in \{0,1\}^n$,*

$$\Pr[x'' = x : x'' \leftarrow \mathsf{Inv}(\mathsf{td}, x'), x' \leftarrow \mathsf{Eval}(x, k), (\mathsf{td}, k) \leftarrow \mathsf{Gen}(1^\lambda)] = 1.$$

Classical security: *For any probabilistic polynomial-time adversary $\mathcal{A}$,*

$$\Pr[x'' = x : x'' \leftarrow \mathcal{A}(x', k), x' \leftarrow \mathsf{Eval}(x, k), x \leftarrow \{0, 1\}^n, (\mathsf{td}, k) \leftarrow \mathsf{Gen}(1^\lambda)] \leq \mathsf{negl}(\lambda).$$

We use the following result from [NOVY93]. (They show it for one-way permutations, not trapdoor permutations, but it is clear that the same result holds for the trapdoor permutations.)

Theorem 2.1 ([NOVY93]). *Let $\{f_k\}_{k \in \mathcal{K}_\lambda}$ be a classically-secure full-domain trapdoor permutation family. Let $(\mathsf{Gen}, \mathsf{Eval}, \mathsf{Inv})$ be the associated tuple of algorithms. Let us consider the following security game between a probabilistic polynomial-time challenger $\mathcal{C}$ and a probabilistic polynomial-time adversary $\mathcal{A}$.*

1. *$\mathcal{C}$ runs $(\mathsf{td}, k) \leftarrow \mathsf{Gen}(1^\lambda)$. $\mathcal{C}$ sends k to $\mathcal{A}$.*
2. *$\mathcal{C}$ chooses $h_j \leftarrow 0^{j-1}1\{0, 1\}^{n-j}$ for each $j \in \{1, 2, ..., n-1\}$.*
3. *$\mathcal{C}$ and $\mathcal{A}$ repeat the following for $j = 1, 2, ..., n-1$:*
    (a) *$\mathcal{C}$ sends h_j to $\mathcal{A}$.*
    (b) *$\mathcal{A}$ sends $c_j \in \{0, 1\}$ to $\mathcal{C}$.*
4. *$\mathcal{A}$ sends $\alpha, \beta \in \{0, 1\}^n$ to $\mathcal{C}$.*
5. *There exist exactly two $y_0, y_1 \in \{0, 1\}^n$ such that $h_j \cdot y_b = c_j$ for all $b \in \{0, 1\}$ and all $j \in \{1, 2, ..., n-1\}$. $\mathcal{C}$ outputs $\top$ if $f_k(\alpha) = y_0$ and $f_k(\beta) = y_1$, or $f_k(\alpha) = y_1$ and $f_k(\beta) = y_0$. Otherwise, $\mathcal{C}$ outputs $\bot$.*

Then, for any probabilistic polynomial-time adversary $\mathcal{A}$, $\Pr[\mathcal{C} \to \top] \leq \mathsf{negl}(\lambda).$

3 Proof of Theorem 1.1

In this section, we provide a proof of Theorem 1.1.

Proof of Theorem 1.1. Let $\{f_k\}_{k \in \mathcal{K}_\lambda}$ be a classically-secure full-domain trapdoor permutation family. Let $(\mathsf{Gen}, \mathsf{Eval}, \mathsf{Inv})$ be the associated tuple of algorithms. From them, we construct non-verifiable remote state preparations of $|x_0\rangle + |x_1\rangle$ secure against probabilistic polynomial-time Bob as follows.

1. Alice runs $(\mathsf{td}, k) \leftarrow \mathsf{Gen}(1^\lambda)$. Alice sends k to Bob.
2. Alice chooses $h_j \leftarrow 0^{j-1}1\{0, 1\}^{n-j}$ for each $j \in \{1, 2, ..., n-1\}$.
3. Alice and Bob repeat the following for $j = 1, 2, ..., n-1$:
    (a) Alice sends h_j to Bob.

(b) Bob possesses the state $\sum_{x \in X_{j-1}} |x\rangle$, where

$$X_j := \left\{ x \in \{0,1\}^n \ \middle| \ \bigwedge_{i=1}^{j} (h_i \cdot f_k(x) = c_i) \right\}.$$

Bob generates

$$\sum_{x \in X_{j-1}} |x\rangle |h_j \cdot f_k(x)\rangle,$$

measures the second register to get the measurement result $c_j \in \{0,1\}$, and sends c_j to Alice. The post-measurement state of the first register is

$$\sum_{x \in X_j} |x\rangle.$$

4. Bob finally gets the state $|x_0\rangle + |x_1\rangle$, where there are exactly two bit strings $y_0, y_1 \in \{0,1\}^n$ such that $h_j \cdot y_b = c_j$ for all $b \in \{0,1\}$ and all $j \in \{1, 2, ..., n-1\}$, and $f_k(x_0) = y_0$ and $f_k(x_1) = y_1$. Bob outputs the state.

5. From td, $\{h_j\}_{j=1}^{n-1}$ and $\{c_j\}_{j=1}^{n-1}$, Alice computes $\{x_0, x_1\}$ and outputs it.

The perfect correctness is clear. The classical security is obtained from Theorem 2.1. $\qquad\square$

4 Proof of Theorem 1.2

In this section, we show Theorem 1.2.

Proof of Theorem 1.2. Let us consider the following construction of proofs of quantumness, which is similar to that of [KMCVY22].

1. The verifier $\mathcal{V}$ and the prover $\mathcal{P}$ run non-verifiable remote state preparations of $|x_0\rangle + |x_1\rangle$ secure against probabilistic polynomial-time Bob whose existence is guaranteed from the existence of classically-secure full-domain trapdoor permutations due to Theorem 1.1. $\mathcal{V}$ gets a pair $\{x_0, x_1\}$ of n-bit strings $x_0, x_1 \in \{0,1\}^n$. Honest $\mathcal{P}$ gets the state $|x_0\rangle + |x_1\rangle$.

2. $\mathcal{V}$ chooses $v_1 \leftarrow \{0,1\}$. $\mathcal{V}$ chooses $r \leftarrow \{0,1\}^n$. $\mathcal{V}$ sends v_1 and r to $\mathcal{P}$.

3.   − If $v_1 = 0$: $\mathcal{P}$ measures $|x_0\rangle + |x_1\rangle$ in the computational basis to get the measurement result $x \in \{0,1\}^n$. $\mathcal{P}$ sends x to $\mathcal{V}$. If $x \in \{x_0, x_1\}$, $\mathcal{V}$ outputs $\top$ and terminates the protocol. Otherwise, $\mathcal{V}$ outputs $\bot$ and aborts.

     − If $v_1 = 1$: $\mathcal{P}$ changes $|x_0\rangle + |x_1\rangle$ into

$$|r \cdot x_0\rangle|x_0\rangle + |r \cdot x_1\rangle|x_1\rangle,$$

measures its second register in the Hadamard basis to get the measurement result $d \in \{0,1\}^n$, and sends d to $\mathcal{V}$. The post-measurement state of the first register is

$$|r \cdot x_0\rangle + (-1)^{d \cdot (x_0 \oplus x_1)}|r \cdot x_1\rangle.$$

4. $\mathcal{V}$ chooses $v_2 \leftarrow \{0,1\}$. $\mathcal{V}$ sends v_2 to $\mathcal{P}$.
5. $\mathcal{P}$ measures the state in the basis

$$\left\{ \cos\frac{\pi}{8}|0\rangle + \sin\frac{\pi}{8}|1\rangle, \sin\frac{\pi}{8}|0\rangle - \cos\frac{\pi}{8}|1\rangle \right\}$$

if $v_2 = 0$, and in the basis

$$\left\{ \cos\frac{\pi}{8}|0\rangle - \sin\frac{\pi}{8}|1\rangle, \sin\frac{\pi}{8}|0\rangle + \cos\frac{\pi}{8}|1\rangle \right\}$$

if $v_2 = 1$. Let $\eta \in \{0,1\}$ be the measurement result. (For the measurement in the basis $\{|\phi\rangle, |\phi^\perp\rangle\}$, the result 0 corresponds to $|\phi\rangle$ and the result 1 corresponds to $|\phi^\perp\rangle$.) $\mathcal{P}$ sends η to $\mathcal{V}$.
6. $\mathcal{V}$ outputs $\top$ if

$$(r \cdot x_0 = r \cdot x_1) \wedge (\eta = r \cdot x_0),$$

or

$$(r \cdot x_0 \neq r \cdot x_1) \wedge (\eta = v_2 \oplus d \cdot (x_0 \oplus x_1)).$$

Otherwise, it outputs $\bot$.

For the correctness, a straightforward calculation similarly to [KMCVY22] shows that

$$\Pr[\mathcal{V} \to \top] = \frac{1}{2} + \frac{1}{2}\cos^2\frac{\pi}{8} \simeq 0.925.$$

For the soundness, by almost the same argument as that in [KMCVY22], we can show that for any probabilistic polynomial-time cheating prover, we have

$$\Pr[\mathcal{V} \to \top] \leq \frac{7}{8} + \mathsf{negl}(\lambda).$$

Note that $\frac{7}{8} = 0.875 < 0.925$. We include the full proof in Appendix A for completeness.

$\square$

References

AGKZ20.   Ryan Amos, Marios Georgiou, Aggelos Kiayias, and Mark Zhandry. One-shot signatures and applications to hybrid quantum/classical authentication. In *52nd ACM STOC*, pages 255–268. ACM Press, 2020.

BBS09.   László Babai, Robert Beals, and Ákos Seress. Polynomial-time theory of matrix groups. In Michael Mitzenmacher, editor, *41st ACM STOC*, pages 55–64. ACM Press, May / June 2009.

BCC$^+$20.   Christian Badertscher, Alexandru Cojocaru, Léo Colisson, Elham Kashefi, Dominik Leichtle, Atul Mantri, and Petros Wallden. Security limitations of classical-client delegated quantum computing. In *ASIACRYPT 2020, Part II*, LNCS, pages 667–696. Springer, Heidelberg, December 2020.

BCM$^+$18.   Zvika Brakerski, Paul Christiano, Urmila Mahadev, Umesh V. Vazirani, and Thomas Vidick. A cryptographic test of quantumness and certifiable randomness from a single quantum device. In Mikkel Thorup, editor, *59th FOCS*, pages 320–331. IEEE Computer Society Press, October 2018.

BCM$^+$21.   Zvika Brakerski, Paul Christiano, Urmila Mahadev, Umesh Vazirani, and Thomas Vidick. A cryptographic test of quantumness and certifiable randomness from a single quantum device. *Journal of the ACM*, 68(5):31:1–31:47, 2021.

BFK09.   Anne Broadbent, Joseph Fitzsimons, and Elham Kashefi. Universal blind quantum computation. In *50th FOCS*, pages 517–526. IEEE Computer Society Press, October 2009.

BKVV20.   Zvika Brakerski, Venkata Koppula, Umesh Vazirani, and Thomas Vidick. Simpler proofs of quantumness. In Steven T. Flammia, editor, *15th Conference on the Theory of Quantum Computation, Communication and Cryptography, TQC 2020, June 9-12, 2020, Riga, Latvia*, volume 158 of *LIPIcs*, pages 8:1–8:14. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020.

BM92.   Mihir Bellare and Silvio Micali. How to sign given any trapdoor permutation. *J. ACM*, 39(1):214–233, 1992.

BPW16.   Nir Bitansky, Omer Paneth, and Daniel Wichs. Perfect structure on the edge of chaos - trapdoor permutations from indistinguishability obfuscation. In Eyal Kushilevitz and Tal Malkin, editors, *TCC 2016-A, Part I*, volume 9562 of *LNCS*, pages 474–502. Springer, Heidelberg, January 2016.

CCKW19.   Alexandru Cojocaru, Léo Colisson, Elham Kashefi, and Petros Wallden. QFactory: Classically-instructed remote secret qubits preparation. In

Steven D. Galbraith and Shiho Moriai, editors, *ASIACRYPT 2019, Part I*, volume 11921 of *LNCS*, pages 615–645. Springer, Heidelberg, December 2019.

DK16.   Vedran Dunjko and Elham Kashefi. Blind quantum computing with two almost identical states. *arXiv:1604.01586*, 2016.

EGL85.   Shimon Even, Oded Goldreich, and Abraham Lempel. A randomized protocol for signing contracts. *Communications of the ACM*, 28(6):637–647, 1985.

FLS99.   Uriel Feige, Dror Lapidot, and Adi Shamir. Multiple noninteractive zero knowledge proofs under general assumptions. *SIAM J. Comput.*, 29(1):1–28, 1999.

GH18.   Sanjam Garg and Mohammad Hajiabadi. Trapdoor functions from the computational Diffie-Hellman assumption. In Hovav Shacham and Alexandra Boldyreva, editors, *CRYPTO 2018, Part II*, volume 10992 of *LNCS*, pages 362–391. Springer, Heidelberg, August 2018.

GL89.   Oded Goldreich and Leonid A Levin. A hard-core predicate for all one-way functions. In *STOC*, pages 25–32. ACM, 1989.

GMP22.   Alexandru Gheorghiu, Tony Metger, and Alexander Poremba. Quantum cryptography with classical communication: parallel remote state preparation for copy-protection, verification, and more. *arXiv:2201.13445*, 2022.

GPV08.   Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In Richard E. Ladner and Cynthia Dwork, editors, *40th ACM STOC*, pages 197–206. ACM Press, May 2008.

GR13.   Oded Goldreich and Ron D. Rothblum. Enhancements of trapdoor permutations. *Journal of Cryptology*, 26(3):484–512, July 2013.

GV19.   Alexandru Gheorghiu and Thomas Vidick. Computationally-secure and composable remote state preparation. In David Zuckerman, editor, *60th FOCS*, pages 1024–1033. IEEE Computer Society Press, November 2019.

Hal02.   Sean Hallgren. Polynomial-time quantum algorithms for Pell's equation and the principal ideal problem. In *34th ACM STOC*, pages 653–658. ACM Press, May 2002.

HHK+05.   Iftach Haitner, Omer Horvitz, Jonathan Katz, Chiu-Yuen Koo, Ruggero Morselli, and Ronen Shaltiel. Reducing complexity assumptions for statistically-hiding commitment. In Ronald Cramer, editor, *EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 58–77. Springer, Heidelberg, May 2005.

HHRS15.   Iftach Haitner, Jonathan J. Hoch, Omer Reingold, and Gil Segev. Finding collisions in interactive protocols - tight lower bounds on the round and communication complexities of statistically hiding commitments. *SIAM J. Comput.*, 44(1):193–242, 2015.

HNO+09.   Iftach Haitner, Minh-Huyen Nguyen, Shien Jin Ong, Omer Reingold, and Salil P. Vadhan. Statistically hiding commitments and statistical zero-knowledge arguments from any one-way function. *SIAM J. Comput.*, 39(3):1153–1218, 2009.

HPS98.   Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. NTRU: A ring-based public key cryptosystem. In Joe Buhler, editor, *Algorithmic Number Theory, Third International Symposium, ANTS-III, Portland, Oregon, USA, June 21-25, 1998, Proceedings*, volume 1423 of *Lecture Notes in Computer Science*, pages 267–288. Springer, 1998.

HY20.   Akinori Hosoyamada and Takashi Yamakawa. Finding collisions in a quantum world: Quantum black-box separation of collision-resistance and one-wayness. In *ASIACRYPT 2020, Part I*, LNCS, pages 3–32. Springer, Heidelberg, December 2020.

IKO05.   Yuval Ishai, Eyal Kushilevitz, and Rafail Ostrovsky. Sufficient conditions for collision-resistant hashing. In Joe Kilian, editor, *TCC 2005*, volume 3378 of *LNCS*, pages 445–456. Springer, Heidelberg, February 2005.

KLVY22.   Yael Tauman Kalai, Alex Lombardi, Vinod Vaikuntanathan, and Lisa Yang. Quantum advantage from any non-local game. Cryptology ePrint Archive, Paper 2022/400, 2022. https://eprint.iacr.org/2022/400.

KMCVY22.   Gregory D. Kahanamoku-Meyer, Soonwon Choi, Umesh V. Vazirani, and Norman Y. Yao. Classically verifiable quantum advantage from a computational bell test. *Nature Physics*, 2022.

Mah18a.   Urmila Mahadev. Classical homomorphic encryption for quantum circuits. In Mikkel Thorup, editor, *59th FOCS*, pages 332–338. IEEE Computer Society Press, October 2018.

Mah18b.   Urmila Mahadev. Classical verification of quantum computations. In Mikkel Thorup, editor, *59th FOCS*, pages 259–267. IEEE Computer Society Press, October 2018.

McE78.   Robert J. McEliece. . a public key cryptosystem based on algebraic coding theory. *DSN progress report*, 1978.

Nie86.   Harald Niederreiter. Knapsack-type cryptosystems and algebraic coding theory. *Prob. Contr. Inform. Theory*, 15(2):157–166, 1986.

NOVY93.   Moni Naor, Rafail Ostrovsky, Ramarathnam Venkatesan, and Moti Yung. Perfect zero-knowledge arguments for NP can be based on general complexity assumptions (extended abstract). In Ernest F. Brickell, editor, *CRYPTO'92*, volume 740 of *LNCS*, pages 196–214. Springer, Heidelberg, August 1993.

PW08.   Chris Peikert and Brent Waters. Lossy trapdoor functions and their applications. In Richard E. Ladner and Cynthia Dwork, editors, *40th ACM STOC*, pages 187–196. ACM Press, May 2008.

RS19.   Roy Radian and Or Sattath. Semi-quantum money. *arXiv*, abs/1908.08889, 2019.

Shm21.   Omri Shmueli. Public-key quantum money with a classical bank. Cryptology ePrint Archive, Paper 2021/1427, 2021. https://eprint.iacr.org/2021/1427.

Shm22.   Omri Shmueli. Semi-quantum tokenized signatures. Cryptology ePrint Archive, Paper 2022/228, 2022. https://eprint.iacr.org/2022/228.

Sho94.   Peter W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *35th FOCS*, pages 124–134. IEEE Computer Society Press, November 1994.

YZ22.   Takashi Yamakawa and Mark Zhandry. Verifiable quantum advantage without structure. Cryptology ePrint Archive, Paper 2022/434, 2022. https://eprint.iacr.org/2022/434.

Zha22.   Jiayu Zhang. Classical verification of quantum computations in linear time. Cryptology ePrint Archive, Paper 2022/432, 2022. https://eprint.iacr.org/2022/432.

A   Proof of Soundness

We give the omitted proof of the soundness of the proof of quantumness protocol given in Section 4. Note that this is almost identical to that in [KMCVY22].

Our goal is to prove that for any probabilistic polynomial-time cheating prover,

$$\Pr[\mathcal{V} \to \top] \leq \frac{7}{8} + \mathsf{negl}(\lambda). \tag{1}$$

Toward contradiction, suppose that there is a probabilistic polynomial-time cheating prover $\mathcal{A}$ and a polynomial poly such that

$$\Pr[\mathcal{V} \to \top] \geq \frac{7}{8} + \frac{1}{\mathrm{poly}(\lambda)}$$

for infinitely many λ. In the following, we focus on such λ. Let $\mathsf{ST}_{\mathcal{A}}$ be $\mathcal{A}$'s state (including the transcript and its own randomness) right after finishing the remote state preparation protocol run in Step 1 and $\{x_0, x_1\}$ be $\mathcal{V}$'s output for the remote state preparation protocol. Then, by a standard averaging argument, for $\frac{1}{2\mathrm{poly}(\lambda)}$-fraction of $(\mathsf{ST}_{\mathcal{A}}, \{x_0, x_1\})$, we have

$$\Pr[\mathcal{V} \to \top \mid (\mathsf{ST}_{\mathcal{A}}, \{x_0, x_1\})] \geq \frac{7}{8} + \frac{1}{2\mathrm{poly}(\lambda)}, \tag{2}$$

where $\Pr[\mathcal{V} \to \top \mid (\mathsf{ST}_{\mathcal{A}}, \{x_0, x_1\})]$ denotes $\mathcal{V}$'s acceptance probability conditioned on a fixed $(\mathsf{ST}_{\mathcal{A}}, \{x_0, x_1\})$. We fix such $(\mathsf{ST}_{\mathcal{A}}, \{x_0, x_1\})$ until Equation 7.

We define the following probabilities all of which are conditioned on the fixed value of $(\mathsf{ST}_{\mathcal{A}}, \{x_0, x_1\})$:

p_0: The probability that $\mathcal{V}$ returns $\top$ conditioned on $v_1 = 0$.
p_1: The probability that $\mathcal{V}$ returns $\top$ conditioned on $v_1 = 1$.
$p_{1,0}$: The probability that $\mathcal{V}$ returns $\top$ conditioned on $v_1 = 1$ and $v_2 = 0$.
$p_{1,1}$: The probability that $\mathcal{V}$ returns $\top$ conditioned on $v_1 = 1$ and $v_2 = 1$.

Clearly, we have

$$\Pr[\mathcal{V} \to \top | (\mathsf{ST}_{\mathcal{A}}, \{x_0, x_1\})] = \frac{p_0 + p_1}{2} \tag{3}$$

and

$$p_1 = \frac{p_{1,0} + p_{1,1}}{2}. \tag{4}$$

By Inequality 2, Equation 3, and a trivial inequality $p_0, p_1 \leq 1$, we have

$$p_0 \geq \frac{3}{4} + \frac{1}{\text{poly}(\lambda)} \tag{5}$$

and

$$p_1 \geq \frac{3}{4} + \frac{1}{\text{poly}(\lambda)}. \tag{6}$$

Let $\mathcal{B}$ be a classical deterministic polynomial-time algorithm that works as follows:

1. $\mathcal{B}$ takes $\mathsf{ST}_{\mathcal{A}}$ and $r \in \{0,1\}^n$ as input.
2. $\mathcal{B}$ runs Step 3 of $\mathcal{A}$ whose state is initialized to $\mathsf{ST}_{\mathcal{A}}$ where $\mathcal{B}$ plays the role of $\mathcal{V}$ with $v_1 = 1$ and the given r. Let $d \in \{0,1\}^n$ be the message sent from $\mathcal{A}$ to $\mathcal{V}$ and $\mathsf{ST}'_{\mathcal{A}}$ be $\mathcal{A}$'s state at this point.
3. $\mathcal{B}$ runs Step 5 of $\mathcal{A}$ whose state is initialized to $\mathsf{ST}'_{\mathcal{A}}$ where $\mathcal{B}$ plays the role of $\mathcal{V}$ with $v_2 = 0$. Let $\eta_{1,0}$ be the message sent from $\mathcal{A}$ to $\mathcal{V}$.
4. $\mathcal{B}$ runs Step 5 of $\mathcal{A}$ whose state is initialized to $\mathsf{ST}'_{\mathcal{A}}$ where $\mathcal{B}$ plays the role of $\mathcal{V}$ withs $v_2 = 1$. Let $\eta_{1,1}$ be the message sent from $\mathcal{A}$ to $\mathcal{V}$. We note that this step is possible because $\mathcal{A}$ is classical and in particular $\mathsf{ST}'_{\mathcal{A}}$ is classical and thus can be copied.
5. Output $\eta_{1,0} \oplus \eta_{1,1}$.

By the union bound, the probability that both $(d, \eta_{1,0})$ and $(d, \eta_{1,1})$ pass the verification is at least

$$1 - (1 - p_{1,0}) - (1 - p_{1,1}) = -1 + 2p_1 \geq \frac{1}{2} + \frac{1}{\text{poly}(\lambda)},$$

where the equation follows from Equation 4 and the inequality follows from Inequality 6. When this occurs, for each $v_2 \in \{0,1\}$, we have

$$(r \cdot x_0 = r \cdot x_1) \wedge (\eta_{1,v_2} = r \cdot x_0),$$

or

$$(r \cdot x_0 \neq r \cdot x_1) \wedge (\eta_{1,v_2} = v_2 \oplus d \cdot (x_0 \oplus x_1)).$$

(Remark that the same d is used for both cases of $v_2 = 0$ and $v_2 = 1$.) This implies that

$$\eta_{1,0} \oplus \eta_{1,1} = r \cdot (x_0 \oplus x_1).$$

Therefore, we have

$$\Pr_{r \leftarrow \{0,1\}^n}[\mathcal{B}(\mathsf{ST}_{\mathcal{A}}, r) = r \cdot (x_0 \oplus x_1)] \geq \frac{1}{2} + \frac{1}{\mathrm{poly}(\lambda)}.$$

Thus, by the Goldreich-Levin theorem [GL89], there is a probabilistic polynomial-time algorithm $\mathcal{E}$ such that

$$\Pr[\mathcal{E}(\mathsf{ST}_{\mathcal{A}}) = x_0 \oplus x_1] \geq \frac{1}{\mathrm{poly}'(\lambda)} \tag{7}$$

for some polynomial poly'. (Remark that what we showed so far is that the above hold for $\frac{1}{2\mathrm{poly}(\lambda)}$-fraction of $(\mathsf{ST}_{\mathcal{A}}, \{x_0, x_1\})$.)

Then, we construct a probabilistic polynomial-time algorithm $\mathcal{C}$ that breaks the security of the remote state preparation protocol as follows:

1. $\mathcal{C}$ interacts with $\mathcal{V}$ in the same way as $\mathcal{A}$ does in Step 1 of the proof of quantumness protocol. Let $\mathsf{ST}_{\mathcal{A}}$ be $\mathcal{A}$'s state after completing this stage. Note that $\{x_0, x_1\}$ is implicitly defined as an outcome of $\mathcal{V}$ for the remote state preparation protocol.
2. $\mathcal{C}$ runs $\mathcal{A}$ for $v_1 = 0$ and $r \leftarrow \{0,1\}^n$ to get the response x'.
3. $\mathcal{C}$ runs $\mathcal{E}(\mathsf{ST}_{\mathcal{A}})$ to get the output z.
4. $\mathcal{C}$ outputs $\{x', x' \oplus z\}$.

For $\frac{1}{2\mathrm{poly}(\lambda)}$-fraction of $(\mathsf{ST}_{\mathcal{A}}, \{x_0, x_1\})$, by Inequalities 5 and 7, we have

$$\Pr[x' \in \{x_0, x_1\} | (\mathsf{ST}_{\mathcal{A}}, \{x_0, x_1\})] \geq \frac{3}{4} + \frac{1}{\mathrm{poly}(\lambda)}$$

and

$$\Pr[z = x_0 \oplus x_1 | (\mathsf{ST}_{\mathcal{A}}, \{x_0, x_1\})] \geq \frac{1}{\mathrm{poly}'(\lambda)}.$$

Moreover, the two events $x' \in \{x_0, x_1\}$ and $z = x_0 \oplus x_1$ are independent once we fix $(\mathsf{ST}_{\mathcal{A}}, \{x_0, x_1\})$. Therefore, for $\frac{1}{2\mathrm{poly}(\lambda)}$-fraction of $(\mathsf{ST}_{\mathcal{A}}, \{x_0, x_1\})$, we have

$$\Pr[x' \in \{x_0, x_1\} \wedge z = x_0 \oplus x_1 | (\mathsf{ST}_{\mathcal{A}}, \{x_0, x_1\})] \geq \frac{3}{4\mathrm{poly}'(\lambda)}.$$

Therefore, we have

$$\Pr[\mathcal{C} \rightarrow \{x_0, x_1\}] \geq \frac{3}{8\mathrm{poly}(\lambda)\mathrm{poly}'(\lambda)}.$$

This contradicts the security of the remote state preparation protocol (Definition 2.1). Therefore, Equation 1 holds and the proof of soundness is completed.

Table of Contents