From the Hardness of Detecting Superpositions to Cryptography: Quantum Public Key Encryption and Commitments

Minki Hhan[1], Tomoyuki Morimae[2], and Takashi Yamakawa[2,3]

[1] KIAS, Seoul, Republic of Korea
[2] Yukawa Institute for Theoretical Physics, Kyoto University, Kyoto, Japan
[3] NTT Social Informatics Laboratories, Tokyo, Japan

Abstract. Recently, Aaronson et al. (arXiv:2009.07450) showed that detecting interference between two orthogonal states is as hard as swapping these states. While their original motivation was from quantum gravity, we show its applications in quantum cryptography.

1. We construct the first public key encryption scheme from cryptographic *non-abelian* group actions. Interestingly, the ciphertexts of our scheme are quantum even if messages are classical. This resolves an open question posed by Ji et al. (TCC '19). We construct the scheme through a new abstraction called swap-trapdoor function pairs, which may be of independent interest.
2. We give a simple and efficient compiler that converts the flavor of quantum bit commitments. More precisely, for any prefix $\mathrm{X}, \mathrm{Y} \in$ {computationally,statistically,perfectly}, if the base scheme is X-hiding and Y-binding, then the resulting scheme is Y-hiding and X-binding. Our compiler calls the base scheme only once. Previously, all known compilers call the base schemes polynomially many times (Crépeau et al., Eurocrypt '01 and Yan, Asiacrypt '22). For the security proof of the conversion, we generalize the result of Aaronson et al. by considering quantum auxiliary inputs.

1 Introduction

When can we efficiently distinguish a superposition of two orthogonal states from their probabilistic mix? A folklore answer to this question was that we can efficiently distinguish them whenever we can efficiently map one of the states to the other. Recently, Aaronson, Atia and, Susskind [1] gave a complete answer to the question. They confirmed that the folklore was almost correct but what actually characterizes the distinguishability is the ability to *swap* the two states rather than the ability to map one of the states to the other.[4]

We explain their result in more detail by using the example of Schrödinger's cat following [1]. Let $|\mathrm{Alive}\rangle$ and $|\mathrm{Dead}\rangle$ be orthogonal states, which can be

[4] We remark that the meaning of "swap" here is different from that of the SWAP gate as explained below.

understood as the states of alive and dead cats in Schrödinger's cat experiment. Then, the authors showed that one can efficiently swap $|\mathrm{Alive}\rangle$ and $|\mathrm{Dead}\rangle$ (i.e., there is an efficiently computable unitary U such that $U|\mathrm{Dead}\rangle = |\mathrm{Alive}\rangle$ and $U|\mathrm{Alive}\rangle = |\mathrm{Dead}\rangle$) if and only if there is an efficient distinguisher that distinguishes $\frac{|\mathrm{Alive}\rangle+|\mathrm{Dead}\rangle}{\sqrt{2}}$ and $\frac{|\mathrm{Alive}\rangle-|\mathrm{Dead}\rangle}{\sqrt{2}}$ with certainty. Note that distinguishing $\frac{|\mathrm{Alive}\rangle+|\mathrm{Dead}\rangle}{\sqrt{2}}$ and $\frac{|\mathrm{Alive}\rangle-|\mathrm{Dead}\rangle}{\sqrt{2}}$ is equivalent to distinguishing $\frac{|\mathrm{Alive}\rangle+|\mathrm{Dead}\rangle}{\sqrt{2}}$ and the uniform probabilistic mix of $|\mathrm{Alive}\rangle$ and $|\mathrm{Dead}\rangle$.[5] Moreover, they showed that the equivalence is robust in the sense that a partial ability to swap $|\mathrm{Alive}\rangle$ and $|\mathrm{Dead}\rangle$, i.e., $|\langle\mathrm{Dead}|U|\mathrm{Alive}\rangle + \langle\mathrm{Alive}|U|\mathrm{Dead}\rangle| = \Gamma$ for some $\Gamma > 0$ is equivalent to distinguishability of $\frac{|\mathrm{Alive}\rangle+|\mathrm{Dead}\rangle}{\sqrt{2}}$ and $\frac{|\mathrm{Alive}\rangle-|\mathrm{Dead}\rangle}{\sqrt{2}}$ with advantage $\Delta = \Gamma/2$. They gave an interpretation of their result that observing interference between alive and dead cats is "necromancy-hard", i.e., at least as hard as bringing a dead cat back to life.

While their original motivation was from quantum gravity, we find their result interesting from cryptographic perspective. Roughly speaking, the task of swapping $|\mathrm{Alive}\rangle$ and $|\mathrm{Dead}\rangle$ can be thought of as a kind of search problem where one is given $|\mathrm{Alive}\rangle$ (resp. $|\mathrm{Dead}\rangle$) and asked to "search" for $|\mathrm{Dead}\rangle$ (resp. $|\mathrm{Alive}\rangle$). On the other hand, the task of distinguishing $\frac{|\mathrm{Alive}\rangle+|\mathrm{Dead}\rangle}{\sqrt{2}}$ and $\frac{|\mathrm{Alive}\rangle-|\mathrm{Dead}\rangle}{\sqrt{2}}$ is apparently a decision problem. From this perspective, we can view their result as a "search-to-decision" reduction. Search-to-decision reductions have been playing the central role in cryptography, e.g., the celebrated Goldreich-Levin theorem [20]. Based on this observation, we tackle the following two problems in quantum cryptography.[6]

Public key encryption from non-abelian group actions. Brassard and Yung [8] initiated the study of cryptographic group actions. We say that a group G acts on a set S by an action $\star : G \times S \to S$ if the following are satisfied:

1. For the identity element $e \in G$ and any $s \in S$, we have $e \star s = s$.
2. For any $g, h \in G$ and any $s \in S$, we have $(gh) \star s = g \star (h \star s)$.

For a cryptographic purpose, we assume (at least) that the group action is one-way, i.e., it is hard to find g' such that $g' \star s = g \star s$ given s and $g \star s$. The work of [8] proposed instantiations of such cryptographic group actions based on the hardness of discrete logarithm, factoring, or graph isomorphism problems.

Cryptographic group actions are recently gaining a renewed attention from the perspective of *post-quantum* cryptography. Ji et al. [25] proposed new instantiations based on general linear group actions on tensors. Alamati et al. [2]

[5] The distinguishing advantage is (necessarily) halved. This can be seen by the following equality:

$$\begin{aligned}&\frac{1}{2}\left(|\mathrm{Alive}\rangle\langle\mathrm{Alive}| + |\mathrm{Dead}\rangle\langle\mathrm{Dead}|\right)\\ =&\frac{1}{2}\left(\left(\frac{|\mathrm{Alive}\rangle + |\mathrm{Dead}\rangle}{\sqrt{2}}\right)\left(\frac{\langle\mathrm{Alive}| + \langle\mathrm{Dead}|}{\sqrt{2}}\right) + \left(\frac{|\mathrm{Alive}\rangle - |\mathrm{Dead}\rangle}{\sqrt{2}}\right)\left(\frac{\langle\mathrm{Alive}| - \langle\mathrm{Dead}|}{\sqrt{2}}\right)\right).\end{aligned}$$

[6] It may be a priori unclear why these problems are related to [1]. This will become clearer in the technical overview in Sec. 2.

proposed isogeny-based instantiations based on earlier works [13, 32, 10]. Both of them are believed to be secure against quantum adversaries.

An important difference between the instantiations in [25] and [2] is that the former considers *non-abelian* groups whereas the latter considers *abelian* groups. Abelian group actions are particularly useful because they give rise to a non-interactive key exchange protocol similar to Diffie-Hellman key exchange [15]. Namely, suppose that $s \in S$ is published as a public parameter, Alice publishes $g_A \star s$ as a public key while keeping g_A as her secret key, and Bob publishes $g_B \star s$ as a public key while keeping g_B as his secret key. Then, they can establish a shared key $g_A \star (g_B \star s) = g_B \star (g_A \star s)$. On the other hand, an eavesdropper Eve cannot know the shared key since she cannot know g_A or g_B by the one-wayness of the group action.[7] This also naturally gives a public key encryption (PKE) scheme similar to ElGamal encryption [17]. On the other hand, the above construction does not work if G is a non-abelian group. Indeed, cryptographic applications given in [25] are limited to *Minicrypt* primitives [24], i.e., those that do not imply PKE in a black-box manner. Thus, [25] raised the following open question:[8]

Question 1: *Can we construct PKE from non-abelian group actions?*

Flavor conversion for quantum bit commitments. Commitments are one of the most important primitives in cryptography. It enables one to "commit" to a (classical) bit[9] in such a way that the committed bit is hidden from other parties before the committer reveals it, which is called the *hiding* property, and the committer cannot change the committed bit after sending the commitment, which is called the *binding* property. One can easily see that it is impossible for *classical* commitments to achieve both hiding and binding properties against unbounded-time adversaries. It is known to be impossible even with *quantum* communication [26, 28]. Thus, it is a common practice in cryptography to relax either of them to hold only against computationally bounded adversaries. We say that a commitment scheme is computationally (resp. statistically) binding/hiding, if it holds against (classical or quantum depending on the context) polynomial-time (resp. unbounded-time) adversaries. Then, there are the following two *flavors* of commitments: One is computationally hiding and statistically binding, and the

[7] For the actual security proof, we need a stronger assumption than the one-wayness. This is similar to the necessity of decisional Diffie-Hellman assumption, which is stronger than the mere hardness of the discrete logarithm problem, for proving security of Diffie-Hellman key exchange.

[8] The statement of the open problem in [25] is quoted as follows: "*Finally, it is an important open problem to build quantum-secure public-key encryption schemes based on hard problems about GLAT or its close variations.*" Here, GLAT stands for General Linear Action on Tensors, which is their instantiation of non-abelian group action. Thus, **Question 1** is slightly more general than what they actually ask.

[9] We can also consider commitments for multi-bit strings. But we focus on *bit* commitments in this paper.

other is computationally binding and statistically hiding.[10] In the following, whenever we require statistical hiding or binding, the other one should be understood as computational since it is impossible to statistically achieve both of them as already explained.

In classical cryptography, though commitments of both flavors are known to be equivalent to the existence of one-way functions [30, 23, 22], there is no known direct conversion between them that preserves efficiency or the number of interactions. Thus, their constructions have been studied separately.

Recently, Yan [35], based on an earlier work by Crépeau, Légaré, and Salvail [14], showed that the situation is completely different for quantum bit commitments, which rely on quantum communication between the sender and receiver. First, he showed a round-collapsing theorem, which means that any interactive quantum bit commitments can be converted into non-interactive ones. Then he gave a conversion that converts the flavor of any non-interactive quantum bit commitments using the round-collapsing theorem.

Though Yan's conversion gives a beautiful equivalence theorem, a disadvantage of the conversion is that it does not preserve the efficiency. Specifically, it calls the base scheme polynomially many times (i.e., $\Omega(\lambda^2)$ times for the security parameter λ). Then, it is natural to ask the following question:

> **Question 2:** *Is there an efficiency-preserving flavor conversion for quantum bit commitments?*

1.1 Our Results

We answer both questions affirmatively using (a generalization of) the result of [1].

For **Question 1**, we construct a PKE scheme with quantum ciphertexts based on non-abelian group actions. This resolves the open problem posed by [25].[11] Our main construction only supports classical one-bit messages, but we can convert it into one that supports quantum multi-qubit messages by hybrid encryption with quantum one-time pad as showin in [9]. Interestingly, ciphertexts of our scheme are quantum even if messages are classical. We show that our scheme is IND-CPA secure if the group action satisfies *pseudorandomness*, which is a stronger assumption than the one-wayness introduced in [25]. In addition, we show a "win-win" result similar in spirit to [37]. We show that if the group action is one-way, then our PKE scheme is IND-CPA secure *or* we can use the group action to construct one-shot signatures [3].[12] Note that constructing

[10] Of course, we can also consider computationally hiding and computationally binding one, which is weaker than both flavors.

[11] The statement of their open problem (quoted in Footnote 8) does not specify if we are allowed to use quantum ciphertexts. Thus, we claim to resolve the problem even though we rely on quantum ciphertexts. If they mean *post-quantum* PKE (which has classical ciphertexts), this is still open.

[12] This is a simplified claim and some subtle issues about uniformness of the adversary and "infinitely-often security" are omitted here. See Lemma 2 for the formal statement.

one-shot signatures has been thought to be a very difficult task. The only known construction is relative to a classical oracle and there is no known construction in the standard model. Even for its significantly weaker variant called tokenized signatures [5], the only known construction in the standard model is based on indistinguishability obfuscation [12]. Given the difficulty of constructing tokenized signatures, let alone one-shot signatures, it is reasonable to conjecture that our PKE scheme is IND-CPA secure if we built it on "natural" one-way group actions. Our PKE scheme is constructed through an abstraction called *swap-trapdoor function pairs* (STFs), which may be of independent interest.

For **Question 2**, We give a new conversion between the two flavors of quantum commitments. That is, for $\mathrm{X}, \mathrm{Y} \in \{\text{computationally,statistically,perfectly}\}$, if the base scheme is X-hiding and Y-binding, then the resulting scheme is Y-hiding and X-binding. Our conversion calls the base scheme only once in superposition. Specifically, if Q_b is the unitary applied by the sender when committing to $b \in \{0,1\}$ in the base scheme, the committing procedure of the resulting scheme consists of a single call to Q_0 or Q_1 controlled by an additional qubit (i.e., application of a unitary such that $|b\rangle|\psi\rangle \mapsto |b\rangle(Q_b|\psi\rangle)$) and additional constant number of gates. For the security proof of our conversion, we develop a generalization of the result of [1] where we consider auxiliary quantum inputs.

We show several applications of our conversion. We remark that our conversion does not give any new feasibility results since similar conversions with worse efficiency were already known [14, 35]. However, our conversion gives schemes with better efficiency in terms of the number of calls to the building blocks.

2 Technical Overview

We give a technical overview of our results. In the overview, we assume that the reader has read the informal explanation of the result of [1] at the beginning of Sec. 1.

2.1 Part I: PKE from Group Actions

Suppose that a (not necessarily abelian) group G acts on a finite set S by a group action $\star : G \times S \to S$. Suppose that it is one-way, i.e., it is hard to find g' such that $g' \star s = g \star s$ given s and $g \star s$.[13]

Our starting point is the observation made in [8] that one-way group actions give claw-free function pairs as follows. Let s_0 and $s_1 := g \star s_0$ be public parameters where $s_0 \in S$ and $g \in G$ are uniformly chosen. Then if we define a function $f_b : G \to S$ by $f_b(h) := h \star s_b$ for $b \in \{0,1\}$, the pair (f_0, f_1) is claw-free, i.e., it is hard to find h_0 and h_1 such that $f_0(h_0) = f_1(h_1)$. This is because if one can find such h_0 and h_1, then one can break the one-wayness of the group action by outputting $h_1^{-1}h_0$, since $f_0(h_0) = f_1(h_1)$ implies $(h_1^{-1}h_0) \star s_0 = s_1$.

[13] We will eventually need pseudorandomness, which is stronger than one-wayness, for the security proof of our PKE scheme. We defer the introduction of pseudorandomness for readability.

Unfortunately, claw-free function pairs are not known to imply PKE. The reason of the difficulty of constructing PKE is that claw-free function pairs do not have trapdoors. Indeed, it is unclear if there is a trapdoor that enables us to invert f_0 and f_1 for the above group-action-based construction. Our first observation is that the above construction actually has a weak form of a trapdoor: If we know g as a trapdoor, then we can find h_1 such that $f_0(h_0) = f_1(h_1)$ from h_0 by simply setting $h_1 \coloneqq h_0 g^{-1}$ and vice versa. Though this trapdoor g does not give the power to invert f_0 or f_1, this enables us to break claw-freeness in a strong sense. We formalize such function pairs as swap-trapdoor function pairs (STFs).[14] For the details of STFs, see Sec. 4.1.

Next, we explain our construction of a PKE scheme with quantum ciphertexts. Though it is a generic construction based on STFs with certain properties, we here focus on the group-action-based instantiation for simplicity. (For the generic construction based on STFs, see Sec. 4.2.) A public key of our PKE scheme consists of s_0 and $s_1 = g \star s_0$ and a secret key is g. For encrypting a bit b, the ciphertext is set to be

$$\mathsf{ct}_b \coloneqq \frac{1}{\sqrt{2}} \left(|0\rangle \, |f_0^{-1}(y)\rangle + (-1)^b \, |1\rangle \, |f_1^{-1}(y)\rangle \right) \tag{1}$$

for a random $y \in S$.[15] Here, $|f_{b'}^{-1}(y)\rangle$ is the uniform superposition over $f_{b'}^{-1}(y) \coloneqq \{h \in G : f_{b'}(h) = y\}$ for $b' \in \{0,1\}$. The above state can be generated by a standard technique similar to [7, 27]. Specifically, we first prepare

$$\frac{1}{\sqrt{2}}(|0\rangle + (-1)^b \, |1\rangle) \otimes \frac{1}{\sqrt{|G|}} \sum_{h \in G} |h\rangle \, ,$$

compute a group action by h in the second register on s_0 or s_1 controlled by the first register to get

$$\frac{1}{\sqrt{2|G|}} \Big(\sum_{h \in G} |0\rangle \, |h\rangle \, |h \star s_0\rangle + (-1)^b \sum_{h \in G} |1\rangle \, |h\rangle \, |h \star s_1\rangle \Big),$$

and measure the third register to get $y \in S$. At this point, the first and second registers collapse to the state in Equation (1).[16] Decryption can be done as follows. Given a ciphertext ct_b, we apply a unitary $|h\rangle \to |hg\rangle$ on the second register controlled on the first register. Observe that the unitary maps $|f_1^{-1}(y)\rangle$ to $|f_0^{-1}(y)\rangle$. Then, the resulting state is $\frac{1}{\sqrt{2}} \left(|0\rangle \, |f_0^{-1}(y)\rangle + (-1)^b \, |1\rangle \, |f_0^{-1}(y)\rangle \right)$. Thus, measuring the first register in the Hadamard basis results in message b.

Next, we discuss how to prove security. Our goal is to prove that the scheme is IND-CPA secure, i.e., ct_0 and ct_1 are computationally indistinguishable. Here, we rely on the result of [1]. According to their result, one can distinguish ct_0 and ct_1 if and only if one can swap $|0\rangle \, |f_0^{-1}(y)\rangle$ and $|1\rangle \, |f_1^{-1}(y)\rangle$. Thus, it suffices

[14] The intuition of the name is that one can "swap" h_0 and h_1 given a trapdoor.
[15] Precisely, y is distributed as $h \star s_0$ for uniformly random $h \in G$.
[16] Note that $|f_0^{-1}(y)| = |f_1^{-1}(y)|$ for all $y \in S$.

to prove the hardness of swapping $|0\rangle|f_0^{-1}(y)\rangle$ and $|1\rangle|f_1^{-1}(y)\rangle$ with a non-negligible advantage.[17] Unfortunately, we do not know how to prove this solely assuming the claw-freeness of (f_0, f_1). Thus, we introduce a new assumption called *conversion hardness*, which requires that one cannot find h_1 such that $f_1(h_1) = y$ given $|f_0^{-1}(y)\rangle$ with a non-negligible probability. Assuming it, the required hardness of swapping follows straightforwardly since if one can swap $|0\rangle|f_0^{-1}(y)\rangle$ and $|1\rangle|f_1^{-1}(y)\rangle$, then one can break the conversion hardness by first mapping $|0\rangle|f_0^{-1}(y)\rangle$ to $|1\rangle|f_1^{-1}(y)\rangle$ and then measuring the second register.

The remaining issue is how to prove conversion hardness based on a reasonable assumption on the group action. We show that pseudorandomness introduced in [25] suffices for this purpose. Pseudorandomness requires the following two properties:

1. The probability that there exists $g \in G$ such that $g \star s_0 = s_1$ is negligible where $s_0, s_1 \in S$ are uniformly random.
2. The distribution of $(s_0, s_1 := g \star s_0)$ where $s_0 \in S$ and $g \in G$ are uniformly random is computationally indistinguishable from the uniform distribution over S^2.

Note that we require Item 1 because otherwise Item 2 may unconditionally hold, in which case there is no useful cryptographic application. We argue that pseudorandomness implies conversion hardness as follows. By Item 2, the attack against the conversion hardness should still succeed with almost the same probability even if we replace s_1 with a uniformly random element of S. However, then there should exist no solution by Item 1. Thus, the original success probability should be negligible.

While [25] gave justification of pseudorandomness of their instantiation of group actions, it is a stronger assumption than one-wayness. Thus, it is more desirable to get PKE scheme solely from one-wayness. Toward this direction, we show the following "win-win" result inspired by [37]. If (f_0, f_1) is claw-free but not conversion hard, then we can construct a one-shot signatures. Roughly one-shot signatures are a quantum primitive which enables us to generate a classical verification key vk along with a quantum signing key sk in such a way that one can use sk to generate a signature for whichever message of one's choice, but cannot generate signatures for different messages simultaneously. For simplicity, suppose that (f_0, f_1) is claw-free but its conversion hardness is totally broken. That is, we assume that we can efficiently find h_1 such that $f_1(h_1) = y$ given $|f_0^{-1}(y)\rangle$. Our idea is to set $|f_0^{-1}(y)\rangle$ to be the secret key and y to be the corresponding verification key. For signing to 0, the signer simply measures $|f_0^{-1}(y)\rangle$ to get $h_0 \in f_0^{-1}(y)$ and set h_0 to be the signature for the message 0. For signing to 1, the signer runs the adversary against conversion hardness to get h_1 such that $f_1(h_1) = y$ and set h_1 to be the signature for the message 1. If one can generate signatures to 0 and 1 simultaneously, we can break claw-freeness since $f_0(h_0) = f_1(h_1) = y$. Thus, the above one-shot signature is secure if (f_0, f_1) is claw-free. In the general case where the conversion hardness is not necessarily

[17] See Theorem 1 for the precise meaning of the advantage for swapping.

completely broken, our idea is to amplify the probability of finding h_1 from $|f_0^{-1}(y)\rangle$ by a parallel repetition. Based on this result, we can see that if the group action is one-way, then our PKE scheme is IND-CPA secure or we can construct one-shot signatures.

2.2 Part II: Flavor Conversion for Commitments

Definition of quantum bit commitments. First, we recall the definition of quantum bit commitments as formalized by Yan [35]. He (based on earlier works [11, 36, 18]) showed that any (possibly interactive) quantum bit commitment scheme can be written in the following (non-interactive) canonical form. A canonical quantum bit commitment scheme is characterized by a pair of unitaries (Q_0, Q_1) over two registers $\mathbf{C}$ (called the commitment register) and $\mathbf{R}$ (called the reveal register) and works as follows.

Commit phase: For committing to a bit $b \in \{0,1\}$, the sender generates the state $Q_b |0\rangle_{\mathbf{C},\mathbf{R}}$ and sends $\mathbf{C}$ to the receiver while keeping $\mathbf{R}$ on its side.[18]

Reveal phase: For revealing the committed bit, the sender sends $\mathbf{R}$ along with the committed bit b to the receiver. Then, the receiver applies $Q_b^\dagger$ to $\mathbf{C}$ and $\mathbf{R}$ and measures both registers. If the measurement outcome is $0\dots0$, the receiver accepts and otherwise rejects.

We require a canonical quantum bit commitment scheme to satisfy the following hiding and binding properties. The hiding property is defined analogously to that of classical commitments. That is, the computational (resp. statistical) hiding property requires that quantum polynomial-time (resp. unbounded-time) receiver (possibly with quantum advice) cannot distinguish commitments to 0 and 1 if only given $\mathbf{C}$.

On the other hand, the binding property is formalized in a somewhat different way from the classical case. The reason is that a canonical quantum commitment scheme cannot satisfy the binding property in the classical sense. The classical binding property roughly requires that a malicious sender can open a commitment to either of 0 or 1 except for a negligible probability. On the other hand, in canonical quantum bit commitment schemes, if the sender generates a uniform superposition of commitments to 0 and 1, it can open the commitment to 0 and 1 with probability 1/2 for each.[19] Thus, we require a weaker binding property called the honest-binding property, which intuitively requires that it is difficult to map an honestly generated commitment of 0 to that of 1 without touching $\mathbf{C}$. More formally, the computational (resp. statistical) honest-binding property requires that for any polynomial-time computable (resp. unbounded-time computable)

[18] We write $|0\rangle$ to mean $|0\dots0\rangle$ for simplicity.

[19] A recent work by Bitansky and Brakerski [6] showed that a quantum commitment scheme may satisfy the classical binding property if the receiver performs a measurement in the commit phase. However, such a measurement is not allowed for canonical quantum bit commitments.

unitary U over $\mathbf{R}$ and an additional register $\mathbf{Z}$ and an auxiliary state $|\tau\rangle_{\mathbf{Z}}$, we have

$$\left\|(Q_1 |0\rangle \langle 0| Q_1^\dagger)_{\mathbf{C},\mathbf{R}}(I_{\mathbf{C}} \otimes U_{\mathbf{R},\mathbf{Z}})((Q_0 |0\rangle)_{\mathbf{C},\mathbf{R}} |\tau\rangle_{\mathbf{Z}})\right\| = \mathsf{negl}(\lambda).$$

One may think that honest-binding is too weak because it only considers honestly generated commitments. However, somewhat surprisingly, [35] proved that it is equivalent to another binding notion called the *sum-binding* [16].[20] The sum-binding property requires that the sum of probabilities that any (quantum polynomial-time, in the case of computational binding) *malicious* sender can open a commitment to 0 and 1 is at most $1 + \mathsf{negl}(\lambda)$. In addition, it has been shown that the honest-binding property is sufficient for cryptographic applications including zero-knowledge proofs/arguments (of knowledge), oblivious transfers, and multi-party computation [36, 18, 34, 29]. In this paper, we refer to honest-binding if we simply write binding.

Our conversion. We propose an efficiency-preserving flavor conversion for quantum bit commitments inspired by the result of [1]. Our key observation is that the swapping ability and distinguishability look somewhat similar to breaking binding and hiding of quantum commitments, respectively. The correspondence between distinguishability and breaking hiding is easier to see: The hiding property directly requires that distinguishing commitments to 0 and 1 is hard. The correspondence between the swapping ability and breaking binding is less clear, but one can find similarities by recalling the definition of (honest-)binding for quantum commitments: Roughly, the binding property requires that it is difficult to map the commitment to 0 to that to 1. Technically, a binding adversary does not necessarily give the ability to swap commitments to 0 and 1 since it may map the commitment to 1 to an arbitrary state instead of to the commitment to 0. But ignoring this issue (which we revisit later), breaking binding property somewhat corresponds to swapping.

However, an important difference between security notions of quantum commitments and the setting of the theorem of [1] is that the former put some restrictions on registers the adversary can touch: For hiding, the adversary cannot touch the reveal register $\mathbf{R}$, and for binding, the adversary cannot touch the commitment register $\mathbf{C}$. To deal with this issue, we make another key observation that the equivalence between swapping and distinguishing shown in [1] preserves *locality*. That is, if the swapping unitary does not touch some qubits of $|\mathrm{Alive}\rangle$ or $|\mathrm{Dead}\rangle$, then the corresponding distinguisher does not touch those qubits either, and vice versa.

The above observations suggest the following conversion. Let $\{Q_0, Q_1\}$ be a canonical quantum bit commitment scheme. Then, we construct another scheme $\{Q'_0, Q'_1\}$ as follows:

- The roles of commitment and reveal registers are swapped from $\{Q_0, Q_1\}$ and the commitment register is augmented by an additional one-qubit register. That is, if $\mathbf{C}$ and $\mathbf{R}$ are the commitment and reveal registers of $\{Q_0, Q_1\}$, then

[20] The term "sum-binding" is taken from [33].

the commitment and reveal registers of $\{Q'_0, Q'_1\}$ are defined as $\mathbf{C}' := (\mathbf{R}, \mathbf{D})$ and $\mathbf{R}' := \mathbf{C}$ where $\mathbf{D}$ is a one-qubit register.
- For $b \in \{0,1\}$, the unitary Q'_b is defined as follows:

$$Q'_b \left|0\right\rangle_{\mathbf{C},\mathbf{R}} \left|0\right\rangle_{\mathbf{D}} := \frac{1}{\sqrt{2}} \left((Q_0 \left|0\right\rangle)_{\mathbf{C},\mathbf{R}} \left|0\right\rangle_{\mathbf{D}} + (-1)^b (Q_1 \left|0\right\rangle)_{\mathbf{C},\mathbf{R}} \left|1\right\rangle_{\mathbf{D}} \right), \quad (2)$$

where $(\mathbf{C}', \mathbf{R}')$ is rearranged as $(\mathbf{C}, \mathbf{R}, \mathbf{D})$.[21]

One can see that $\{Q'_0, Q'_1\}$ is almost as efficient as $\{Q_0, Q_1\}$: For generating, $Q'_b \left|0\right\rangle_{\mathbf{C},\mathbf{R}} \left|0\right\rangle_{\mathbf{D}}$ one can first prepare $\left|0\right\rangle_{\mathbf{C},\mathbf{R}} (\left|0\right\rangle + (-1)^b \left|1\right\rangle)_{\mathbf{D}}$ and then apply Q_0 or Q_1 to $(\mathbf{C}, \mathbf{R})$ controlled by $\mathbf{D}$. We prove that the hiding and binding properties of $\{Q_0, Q_1\}$ imply binding and hiding properties of $\{Q'_0, Q'_1\}$, respectively. Moreover, the reduction preserves all three types of computational/statistical/perfect security. Thus, this gives a conversion between different flavors of quantum bit commitments.

Security proof. At an intuitive level, the theorem of [1] with the above "locality-preserving" observation seems to easily give a reduction from security of $\{Q'_0, Q'_1\}$ to that of $\{Q_0, Q_1\}$: If we can break the hiding property of $\{Q'_0, Q'_1\}$, then we can distinguish $Q'_b \left|0\right\rangle_{\mathbf{C},\mathbf{R}} \left|0\right\rangle_{\mathbf{D}}$ without touching $\mathbf{R}' = \mathbf{C}$. Then, their theorem with the above observation gives a swapping algorithm that swaps $(Q_0 \left|0\right\rangle_{\mathbf{C},\mathbf{R}}) \left|0\right\rangle_{\mathbf{D}}$ and $(Q_1 \left|0\right\rangle_{\mathbf{C},\mathbf{R}}) \left|1\right\rangle_{\mathbf{D}}$ without touching $\mathbf{R}' = \mathbf{C}$, which clearly breaks the binding property of $\{Q_0, Q_1\}$. One may expect that the reduction from binding to hiding works analogously. However, it is not as easy as one would expect due to the following reasons.

1. An adversary that breaks the binding property is weaker than a "partial" swapping unitary that swaps $Q'_0 \left|0\right\rangle_{\mathbf{C}',\mathbf{R}'}$ and $Q'_1 \left|0\right\rangle_{\mathbf{C}',\mathbf{R}'}$ needed for [1]. For example, suppose that we have a unitary U such that $UQ'_0 \left|0\right\rangle_{\mathbf{C}',\mathbf{R}'} = Q'_1 \left|0\right\rangle_{\mathbf{C}',\mathbf{R}'}$ and $UQ'_1 \left|0\right\rangle_{\mathbf{C}',\mathbf{R}'} = -Q'_0 \left|0\right\rangle_{\mathbf{C}',\mathbf{R}'}$. Clearly, this completely breaks the binding property of $\{Q'_0, Q'_1\}$. However, this is not sufficient for applying [1] since $|\left\langle 0\right| {Q'_1}^\dagger U Q'_0 \left|0\right\rangle + \left\langle 0\right| {Q'_0}^\dagger U Q'_1 \left|0\right\rangle| = 0$.
2. For security of quantum bit commitments, we have to consider adversaries with quantum advice, or at least those with ancilla qubits even for security against uniform adversaries. However, the theorem of [1] does not consider any ancilla qubits.

Both issues are already mentioned in [1]. In particular, Item 1 is an essential issue. They prove the existence of a pair of orthogonal states $\left|\mathrm{Alive}\right\rangle$ and $\left|\mathrm{Dead}\right\rangle$ such that we can map $\left|\mathrm{Alive}\right\rangle$ to $\left|\mathrm{Dead}\right\rangle$ by an efficient unitary, but $|\left\langle \mathrm{Dead}\right| U \left|\mathrm{Alive}\right\rangle + \left\langle \mathrm{Alive}\right| U \left|\mathrm{Dead}\right\rangle| \approx 0$ for all efficient unitaries U [1, Theorem 3]. For Item 2, they (with acknowledgment to Daniel Gottesman) observe that the conversion from a distinguisher to a swapping unitary works even with any quantum advice, but the other direction does not work if there are ancilla qubits [1, Footnote 2].

[21] We only present how Q'_b works on $\left|0\right\rangle_{\mathbf{C},\mathbf{R}} \left|0\right\rangle_{\mathbf{D}}$ for simplicity. Its definition on general states can be found in Theorem 7.

One can see that the above issues are actually not relevant to the reduction from the hiding of $\{Q'_0, Q'_1\}$ to the binding of $\{Q_0, Q_1\}$. However, for the reduction from the binding of $\{Q'_0, Q'_1\}$ to the hiding of $\{Q_0, Q_1\}$, both issues are non-trivial. Below, we show how to resolve those issues.

Solution to Item 1. By the result of [1, Theorem 3] as already explained, this issue cannot be resolved if we think of $Q'_0 |0\rangle_{\mathbf{C}',\mathbf{R}'}$ and $Q'_1 |0\rangle_{\mathbf{C}',\mathbf{R}'}$ as general orthogonal states. Thus, we look into the actual form of them presented in Equation (2). Then, we observe that an adversary against the binding property does not touch $\mathbf{D}$ since that is part of the commitment register $\mathbf{C}'$ of $\{Q'_0, Q'_1\}$. Therefore, he cannot cause any interference between $(Q_0 |0\rangle)_{\mathbf{C},\mathbf{R}} |0\rangle_{\mathbf{D}}$ and $(Q_1 |0\rangle)_{\mathbf{C},\mathbf{R}} |1\rangle_{\mathbf{D}}$. Therefore, if it maps

$$\frac{1}{\sqrt{2}} \left((Q_0 |0\rangle)_{\mathbf{C},\mathbf{R}} |0\rangle_{\mathbf{D}} + (Q_1 |0\rangle)_{\mathbf{C},\mathbf{R}} |1\rangle_{\mathbf{D}} \right) \mapsto \frac{1}{\sqrt{2}} \left((Q_0 |0\rangle)_{\mathbf{C},\mathbf{R}} |0\rangle_{\mathbf{D}} - (Q_1 |0\rangle)_{\mathbf{C},\mathbf{R}} |1\rangle_{\mathbf{D}} \right),$$

then it should also map

$$\frac{1}{\sqrt{2}} \left((Q_0 |0\rangle)_{\mathbf{C},\mathbf{R}} |0\rangle_{\mathbf{D}} - (Q_1 |0\rangle)_{\mathbf{C},\mathbf{R}} |1\rangle_{\mathbf{D}} \right) \mapsto \frac{1}{\sqrt{2}} \left((Q_0 |0\rangle)_{\mathbf{C},\mathbf{R}} |0\rangle_{\mathbf{D}} + (Q_1 |0\rangle)_{\mathbf{C},\mathbf{R}} |1\rangle_{\mathbf{D}} \right).$$

Thus, the ability to map $Q'_0 |0\rangle_{\mathbf{C}',\mathbf{R}'}$ to $Q'_1 |0\rangle_{\mathbf{C}',\mathbf{R}'}$ is equivalent to swapping them for this particular construction when one is not allowed to touch $\mathbf{D}$. A similar observation extends to the imperfect case as well. Therefore, Item 1 is not an issue for the security proof of this construction.

Solution to Item 2. To better understand the issue, we review how the conversion from a swapping unitary to a distinguisher works. For simplicity, we focus on the perfect case here, i.e., we assume that there is a unitary U such that $U |\mathrm{Dead}\rangle = |\mathrm{Alive}\rangle$ and $U |\mathrm{Alive}\rangle = |\mathrm{Dead}\rangle$ for orthogonal states $|\mathrm{Alive}\rangle$ and $|\mathrm{Dead}\rangle$. Then, we can construct a distinguisher $\mathcal{A}$ that distinguishes $\frac{|\mathrm{Alive}\rangle+|\mathrm{Dead}\rangle}{\sqrt{2}}$ and $\frac{|\mathrm{Alive}\rangle-|\mathrm{Dead}\rangle}{\sqrt{2}}$ as follows: Given a state $|\eta\rangle$, which is either of the above two states $\frac{|\mathrm{Alive}\rangle+|\mathrm{Dead}\rangle}{\sqrt{2}}$ or $\frac{|\mathrm{Alive}\rangle-|\mathrm{Dead}\rangle}{\sqrt{2}}$, it prepares $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ in an ancilla qubit, applies U controlled by the ancilla, and measures the ancilla in Hadamard basis. An easy calculation shows that the measurement outcome is 1 with probability 1 if $|\eta\rangle = \frac{|\mathrm{Alive}\rangle+|\mathrm{Dead}\rangle}{\sqrt{2}}$ and 0 with probability 1 if $|\eta\rangle = \frac{|\mathrm{Alive}\rangle-|\mathrm{Dead}\rangle}{\sqrt{2}}$.

Then, let us consider what happens if the swapping unitary uses ancilla qubits. That is, suppose that we have $U |\mathrm{Dead}\rangle |\tau\rangle = |\mathrm{Alive}\rangle |\tau'\rangle$ and $U |\mathrm{Alive}\rangle |\tau\rangle = |\mathrm{Dead}\rangle |\tau'\rangle$ for some ancilla states $|\tau\rangle$ and $|\tau'\rangle$. When $|\tau\rangle$ and $|\tau'\rangle$ are orthogonal, the above distinguisher does not work because there does not occur interference between states with 0 and 1 in the control qubit. To resolve this issue, our idea is to "uncompute" the ancilla state. A naive idea to do so is to apply $U^\dagger$, but then this is meaningless since it just goes back to the original state. Instead, we prepare a "dummy" register that is initialized to be $\frac{|\mathrm{Alive}\rangle+|\mathrm{Dead}\rangle}{\sqrt{2}}$. Then, we add an application of $U^\dagger$ to the ancilla qubits and the dummy register controlled by the control qubit. Then, the ancilla qubit goes back to $|\tau\rangle$ while the state in the dummy register does not change because it is invariant under the swapping of

$|\mathrm{Alive}\rangle$ and $|\mathrm{Dead}\rangle$. Then, we can see that this modified distinguisher distinguishes $\frac{|\mathrm{Alive}\rangle+|\mathrm{Dead}\rangle}{\sqrt{2}}$ and $\frac{|\mathrm{Alive}\rangle-|\mathrm{Dead}\rangle}{\sqrt{2}}$ with advantage 1.

Unfortunately, when the swapping ability is imperfect, the above distinguisher does not work. However, we show that the following slight variant of the above works: Instead of preparing $\frac{|\mathrm{Alive}\rangle+|\mathrm{Dead}\rangle}{\sqrt{2}}$, it prepares $\frac{|\mathrm{Alive}\rangle|0\rangle+|\mathrm{Dead}\rangle|1\rangle}{\sqrt{2}}$. After the controlled application of $U^\dagger$, it flips the rightmost register (i.e., apply Pauli X to it). In the perfect case, this variant also works with advantage 1 since the state in the dummy register becomes $\frac{|\mathrm{Dead}\rangle|0\rangle+|\mathrm{Alive}\rangle|1\rangle}{\sqrt{2}}$ after the application of the controlled $U^\dagger$, which goes back to the original state $\frac{|\mathrm{Alive}\rangle|0\rangle+|\mathrm{Dead}\rangle|1\rangle}{\sqrt{2}}$ by the flip. Our calculation shows that this version is robust, i.e., it works even for the imperfect case.

There are several caveats for the above. First, it requires the distinguisher to take an additional quantum advice $\frac{|\mathrm{Alive}\rangle|0\rangle+|\mathrm{Dead}\rangle|1\rangle}{\sqrt{2}}$, which is not necessarily efficiently generatable in general.[22] Second, there occurs a quadratic reduction loss unlike the original theorem in [1] without ancilla qubits. Nonetheless, they are not a problem for our purpose.

3 Preliminaries

Notations used throughout the paper and definitions of basic cryptographic primitives are given in the full version.

3.1 Canonical Quantum Bit Commitments

We define *canonical* quantum bit commitments as defined in [35].

Definition 1 (Canonical quantum bit commitments). *A canonical quantum bit commitment scheme is represented by a family $\{Q_0(\lambda), Q_1(\lambda)\}_{\lambda\in\mathbb{N}}$ of polynomial-time computable unitaries over two registers $\mathbf{C}$ (called the* commitment *register) and $\mathbf{R}$ (called the* reveal *register). In the rest of the paper, we often omit λ and simply write Q_0 and Q_1 to mean $Q_0(\lambda)$ and $Q_1(\lambda)$.*

Remark 1. Canonical quantum bit commitments are supposed to be used as follows. In the commit phase, to commit to a bit $b \in \{0,1\}$, the sender generates a state $Q_b|0\rangle_{\mathbf{C},\mathbf{R}}$ and sends $\mathbf{C}$ to the receiver while keeping $\mathbf{R}$. In the reveal phase, the sender sends b and $\mathbf{R}$ to the receiver. The receiver projects the state on $(\mathbf{C},\mathbf{R})$ onto $Q_b|0\rangle_{\mathbf{C},\mathbf{R}}$, and accepts if it succeeds and otherwise rejects.

Definition 2 (Hiding). *We say that a canonical quantum bit commitment scheme $\{Q_0, Q_1\}$ is computationally (rep. statistically)* hiding *if $\mathrm{Tr}_{\mathbf{R}}(Q_0(|0\rangle\langle 0|)_{\mathbf{C},\mathbf{R}}Q_0^\dagger)$ is computationally (resp. statistically) indistinguishable from $\mathrm{Tr}_{\mathbf{R}}(Q_1(|0\rangle\langle 0|)_{\mathbf{C},\mathbf{R}}Q_1^\dagger)$. We say that it is perfectly hiding if they are identical states.*

[22] We remark that they are efficiently generatable in our application where $|\mathrm{Alive}\rangle$ and $|\mathrm{Dead}\rangle$ correspond to commitments to 0 and 1.

Definition 3 (Binding). *We say that a canonical quantum bit commitment scheme $\{Q_0, Q_1\}$ is computationally (rep. statistically)* binding *if for any polynomial-time computable (resp. unbounded-time) unitary U over $\mathbf{R}$ and an additional register $\mathbf{Z}$ and any polynomial-size state $|\tau\rangle_{\mathbf{Z}}$, it holds that*

$$\left\| (Q_1 |0\rangle \langle 0| Q_1^\dagger)_{\mathbf{C},\mathbf{R}} (I_{\mathbf{C}} \otimes U_{\mathbf{R},\mathbf{Z}})((Q_0 |0\rangle)_{\mathbf{C},\mathbf{R}} |\tau\rangle_{\mathbf{Z}}) \right\| = \mathsf{negl}(\lambda).$$

We say that it is perfectly binding if the LHS is 0 for all unbounded-time unitary U.

3.2 Equivalence between Swapping and Distinguishing

The following theorem was proven in [1].

Theorem 1 ([1, Theorem 2]).

1. *Let $|x\rangle, |y\rangle$ be orthogonal n-qubit states. Let U be a polynomial-time computable unitary over n-qubit states and define Γ as*

$$\Gamma := |\langle y| U |x\rangle + \langle x| U |y\rangle|.$$

   Then, there exists a QPT distinguisher $\mathcal{A}$ that makes a single black-box access to controlled-U and distinguishes $|\psi\rangle := \frac{|x\rangle+|y\rangle}{\sqrt{2}}$ and $|\phi\rangle := \frac{|x\rangle-|y\rangle}{\sqrt{2}}$ with advantage $\frac{\Gamma}{2}$. Moreover, if U does not act on some qubits, then $\mathcal{A}$ also does not act on those qubits.
2. *Let $|\psi\rangle, |\phi\rangle$ be orthogonal n-qubit states, and suppose that a QPT distinguisher $\mathcal{A}$ distinguishes $|\psi\rangle$ and $|\phi\rangle$ with advantage Δ without using any ancilla qubits. Then, there exists a polynomial-time computable unitary U over n-qubit states such that*

$$\frac{|\langle y| U |x\rangle + \langle x| U |y\rangle|}{2} = \Delta$$

   where $|x\rangle := \frac{|\psi\rangle+|\phi\rangle}{\sqrt{2}}$ and $|y\rangle := \frac{|\psi\rangle-|\phi\rangle}{\sqrt{2}}$. Moreover, if $\mathcal{A}$ does not act on some qubits, then U also does not act on those qubits.

Remark 2 (Descriptions of quantum circuits.). For the reader's convenience, we give the concrete descriptions of quantum circuits for the above theorem, which are presented in [1].

For Item 1, let $\widetilde{U} := e^{i\theta} U$ for θ such that

$$\mathrm{Re}(\langle y| \widetilde{U} |x\rangle + \langle x| \widetilde{U} |y\rangle) = |\langle y| U |x\rangle + \langle x| U |y\rangle|.$$

Then, $\mathcal{A}$ is described in Figure 1.

For Item 2, let $V_{\mathcal{A}}$ be a unitary such that

$$V_{\mathcal{A}} |\psi\rangle = \sqrt{p} |1\rangle |\psi_1\rangle + \sqrt{1-p} |0\rangle |\psi_0\rangle$$
$$V_{\mathcal{A}} |\phi\rangle = \sqrt{1-p+\Delta} |0\rangle |\phi_0\rangle + \sqrt{p-\Delta} |1\rangle |\phi_1\rangle$$

for some $|\psi_0\rangle$, $|\psi_1\rangle$, $|\phi_0\rangle$, and $|\phi_1\rangle$. That is, $V_{\mathcal{A}}$ is the unitary part of $\mathcal{A}$. Then, U is described in Figure 2.

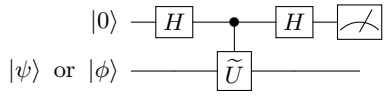

Fig. 1. Quantum circuit for $\mathcal{A}$ in Item 1 of Theorem 1.

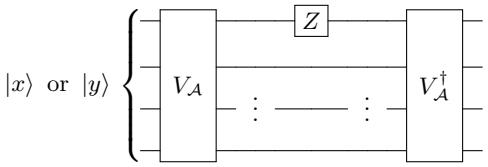

Fig. 2. Quantum circuit for U in Item 2 of Theorem 1.

Remark 3. Though the final requirement in both items ("Moreover,...") is not explicitly stated in [1, Theorem 2], it is easy to see from Figures 1 and 2. This observation is important for our application to commitments and PKE.

4 Quantum-Ciphertext Public Key Encryption

In Sec. 4.1, we introduce a notion of swap-trapdoor function pairs, which can be seen as a variant of trapdoor claw-free function pairs [21]. In Sec. 4.2, we define quantum-ciphertext PKE and construct it based on STFs. In Sec. 4.3, we construct STFs based on group actions.

4.1 Swap-Trapdoor Function Pairs

We introduce a notion of swap-trapdoor function pairs (STFs). Similarly to trapdoor claw-free function pairs, a STF consists of two functions $f_0, f_1 : \mathcal{X} \to \mathcal{Y}$. We require that there is a trapdoor which enables us to "swap" preimages under f_0 and f_1, i.e., given x_b, we can find $x_{b\oplus 1}$ such that $f_{b\oplus 1}(x_{b\oplus 1}) = f_b(x_b)$. The formal definition of STFs is given below.

Definition 4 (Swap-trapdoor function pair). *A* swap-trapdoor function pair (STF) *consists of algorithms* $(\mathsf{Setup}, \mathsf{Eval}, \mathsf{Swap})$.

$\mathsf{Setup}(1^\lambda) \to (\mathsf{pp}, \mathsf{td})$**:** *This is a PPT algorithm that takes the security parameter* 1^λ *as input, and outputs a public parameter* pp *and a trapdoor* td*. The public parameter* pp *specifies functions* $f_b^{(\mathsf{pp})} : \mathcal{X} \to \mathcal{Y}$ *for each* $b \in \{0,1\}$*. We often omit the dependence on* pp *and simply write* f_b *when it is clear from the context.*

$\mathsf{Eval}(\mathsf{pp}, b, x) \to y$**:** *This is a deterministic classical polynomial-time algorithm that takes a public parameter* pp*, a bit* $b \in \{0,1\}$*, and an element* $x \in \mathcal{X}$ *as input, and outputs* $y \in \mathcal{Y}$*.*

$\mathsf{Swap}(\mathsf{td}, b, x) \to x'$**:** *This is a deterministic classical polynomial-time algorithm that takes a trapdoor* td*, a bit* $b \in \{0,1\}$*, and an element* $x \in \mathcal{X}$ *as input, and outputs* $x' \in \mathcal{X}$*.*

We require a STF to satisfy the following:

Evaluation correctness. *For any* $(\mathsf{pp}, \mathsf{td}) \leftarrow \mathsf{Setup}(1^\lambda)$ *,* $b \in \{0,1\}$*, and* $x \in \mathcal{X}$*, we have* $\mathsf{Eval}(\mathsf{pp}, b, x) = f_b(x)$*.*

Swapping correctness. *For any* $(\mathsf{pp}, \mathsf{td}) \leftarrow \mathsf{Setup}(1^\lambda)$*,* $b \in \{0,1\}$*, and* $x \in \mathcal{X}$*, if we let* $x' \leftarrow \mathsf{Swap}(\mathsf{td}, b, x)$*, then we have* $f_{b\oplus 1}(x') = f_b(x)$ *and* $\mathsf{Swap}(\mathsf{td}, b\oplus 1, x') = x$*. In particular,* $\mathsf{Swap}(\mathsf{td}, b, \cdot)$ *induces an efficiently computable and invertible one-to-one mapping between* $f_0^{-1}(y)$ *and* $f_1^{-1}(y)$ *for any* $y \in \mathcal{Y}$*.*

Efficient random sampling over $\mathcal{X}$***.*** *There is a PPT algorithm that samples an almost uniform element of* $\mathcal{X}$ *(i.e., the distribution of the sample is statistically close to the uniform distribution).*

Efficient superposition over $\mathcal{X}$***.*** *There is a QPT algorithm that generates a state whose trace distance from* $|\mathcal{X}\rangle = \frac{1}{\sqrt{|\mathcal{X}|}}\sum_{x\in\mathcal{X}}|x\rangle$ *is* $\mathsf{negl}(\lambda)$*.*

Remark 4 (A convention on "Efficient random sampling over $\mathcal{X}$*" and "Efficient superposition over* $\mathcal{X}$*" properties).* In the rest of this paper, we assume that we can sample elements from *exactly* the uniform distribution of $\mathcal{X}$. Similarly, we assume that we can *exactly* generate $|\mathcal{X}\rangle$ in QPT. They are just for simplifying the presentations of our results, and all the results hold with the above imperfect version with additive negligible loss for security or correctness.

We define two security notions for STFs which we call *claw-freeness* and *conversion hardness*. Looking ahead, what we need in our construction of quantum-ciphertext PKE in Sec. 4.2 is only conversion hardness. However, since there are interesting relations between them as we show later, we define both of them here.

Definition 5 (Claw-freeness). *We say that a STF* $(\mathsf{Setup}, \mathsf{Eval}, \mathsf{Swap})$ *satisfies* claw-freeness *if for any non-uniform QPT algorithm* $\mathcal{A}$*, we have*

$$\Pr[f_0(x_0) = f_1(x_1) : (\mathsf{pp}, \mathsf{td}) \leftarrow \mathsf{Setup}(1^\lambda), (x_0, x_1) \leftarrow \mathcal{A}(\mathsf{pp})] = \mathsf{negl}(\lambda).$$

Definition 6 (Conversion hardness). *We say that a STF* $(\mathsf{Setup}, \mathsf{Eval}, \mathsf{Swap})$ *satisfies* conversion hardness *if for any non-uniform QPT algorithm* $\mathcal{A}$*, we have*

$$\Pr[f_1(x_1) = y : (\mathsf{pp}, \mathsf{td}) \leftarrow \mathsf{Setup}(1^\lambda), x_0 \leftarrow \mathcal{X}, y := f_0(x_0), x_1 \leftarrow \mathcal{A}(\mathsf{pp}, |f_0^{-1}(y)\rangle)] = \mathsf{negl}(\lambda)$$

where we remind that $|f_0^{-1}(y)\rangle := \frac{1}{\sqrt{|f_0^{-1}(y)|}}\sum_{x\in f_0^{-1}(y)}|x\rangle$*.*

Remark 5 (On asymmetry of f_0 *and* f_1*.).* Conversion hardness requires that it is hard to find x_1 such that $f_1(x_1) = y$ given $|f_0^{-1}(y)\rangle$. We could define it in the other way, i.e., it is hard to find x_0 such that $f_0(x_0) = y$ given $|f_1^{-1}(y)\rangle$. These two definitions do not seem to be equivalent. However, it is easy to see that if there is a STF that satisfies one of them, then it can be modified to satisfy the other one by just swapping the roles of f_0 and f_1. In this sense, the choice of the definition from these two versions is arbitrary.

We show several lemmas on the relationship between claw-freeness and conversion hardness.

First, we show that claw-freeness implies conversion hardness if f_0 is collapsing.

Lemma 1 (Claw-free and collapsing → Conversion hard). *If f_0 is collapsing, then claw-freeness implies conversion hardness.*

We defer the proof to the full version.

As a special case of Lemma 1, claw-freeness implies conversion hardness when f_0 is *injective* (in which case f_1 is also injective). This is because any injective function is trivially collapsing.

We remark that a conversion hard STF is not necessarily claw-free, because a claw can be augmented in STF without hurting the conversion hardness.

Next, we show a "win-win" result inspired from [37]. We roughly show that a claw-free but non-conversion-hard STF can be used to construct one-shot signatures [3]. Roughly one-shot signatures are a genuinely quantum primitive which enables us to generate a classical verification key vk along with a quantum signing key sk in such a way that one can use sk to generate a signature for whichever message of one's choice, but cannot generate signatures for different messages simultaneously. The only known construction of one-shot signatures is relative to a classical oracle and there is no known construction in the standard model. Even for its weaker variant called tokenized signatures [5], the only known construction in the standard model is based on indistinguishability obfuscation [12]. Given the difficulty of constructing tokenized signatures, let alone one-shot signatures, it is reasonable to conjecture that natural candidate constructions of STFs satisfy conversion hardness if it satisfies claw-freeness. This is useful because claw-freeness often follows from weaker assumptions than conversion hardness, which is indeed the case for the group action-based construction in Sec. 4.3.

Before stating the lemma, we remark some subtlety about the lemma. Actually, we need to assume a STF that is claw-free but not *infinitely-often uniform* conversion hard. Here, "infinitely-often" means that it only requires the security to hold for infinitely many security parameters rather than all security parameters. (See [37, Sec. 4.1] for more explanations about infinitely-often security.) The "uniform" means that security is required to hold only against uniform adversaries as opposed to non-uniform ones. Alternatively, we can weaken the assumption to a STF that is claw-free but not uniform conversion hard if we weaken the goal to be *infinitely-often* one-shot signatures. We remark that similar limitations also exist for the "win-win" result in [37].

Then, the lemma is given below.

Lemma 2 (Claw-free and non-conversion hard STF → One-shot signatures). *Let $(\mathsf{Setup}, \mathsf{Eval}, \mathsf{Swap})$ be a STF that satisfies claw-freeness. Then, the following statements hold:*

1. *If $(\mathsf{Setup}, \mathsf{Eval}, \mathsf{Swap})$ is not infinitely-often uniform conversion hard, then we can use it to construct one-shot signatures.*
2. *If $(\mathsf{Setup}, \mathsf{Eval}, \mathsf{Swap})$ is not uniform conversion hard, then we can use it to construct infinitely-often one-shot signatures.*

We defer the proof to the full version since the idea is already explained in Sec. 2.1.

Instantiations. Our main instantiation of STFs is based on group actions, which is given in Sec. 4.3.

A lattice-based instantiation is also possible if we relax the requirements to allow some "noises" similarly to [7]. The noisy version is sufficient for our construction of quantum-ciphertext PKE given in Sec. 4.2. However, since lattice-based (classical) PKE schemes are already known [31, 19], we do not try to capture lattice-based instantiations in the definition of STFs.

4.2 Quantum-Ciphertext Public Key Encryption

In this section, we define quantum-ciphertext PKE and construct it based on STFs.

Definition. We define quantum-ciphertext PKE for one-bit messages for simplicity. The multi-bit message version can be defined analogously, and a simple parallel repetition works to expand the message length. Moreover, we can further extend the message space to quantum states by a hybrid encryption with quantum one-time pad as in [9], i.e., we encrypt a quantum message by a quantum one-time pad, and then encrypt the key of the quantum one-time pad by quantum PKE for classical messages.

Definition 7 (Quantum-ciphertext public key encryption). *A* quantum-ciphertext public key encryption (quantum-ciphertext PKE) *scheme (with single-bit messages) consists of algorithms* $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$.

$\mathsf{KeyGen}(1^\lambda) \to (\mathsf{pk}, \mathsf{sk})$**:** *This is a PPT algorithm that takes the security parameter* 1^λ *as input, and outputs a classical public key* pk *and a classical secret key* sk.

$\mathsf{Enc}(\mathsf{pk}, b) \to \mathit{ct}$**:** *This is a QPT algorithm that takes a public key* pk *and a message* $b \in \{0,1\}$ *as input, and outputs a quantum ciphertext* ct.

$\mathsf{Dec}(\mathsf{sk}, \mathit{ct}) \to b'/\bot$**:** *This is a QPT algorithm that takes a secret key* sk *and a ciphertext* ct *as input, and outputs a message* $b' \in \{0,1\}$ *or* $\bot$.

It must satisfy correctness as defined below:

Correctness. *For any* $m \in \{0,1\}$*, we have*

$$\Pr[m' = m : (\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda), \mathit{ct} \leftarrow \mathsf{Enc}(\mathsf{pk}, m), m' \leftarrow \mathsf{Dec}(\mathsf{sk}, \mathit{ct})] = 1 - \mathsf{negl}(\lambda).$$

We define IND-CPA security for quantum-ciphertext PKE similarly to that for classical PKE as follows.

Definition 8 (IND-CPA security). *We say that a quantum-ciphertext PKE scheme* $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ *is* IND-CPA secure *if for any non-uniform QPT adversary* $\mathcal{A}$*, we have*

$$|\Pr[\mathcal{A}(\mathsf{pk}, \mathit{ct}_0) = 1] - \Pr[\mathcal{A}(\mathsf{pk}, \mathit{ct}_1) = 1]| = \mathsf{negl}(\lambda),$$

where $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda)$*,* $\mathit{ct}_0 \leftarrow \mathsf{Enc}(\mathsf{pk}, 0)$*, and* $\mathit{ct}_1 \leftarrow \mathsf{Enc}(\mathsf{pk}, 1)$.

Construction. Let $(\mathsf{Setup}, \mathsf{Eval}, \mathsf{Swap})$ be a STF. We construct a quantum-ciphertext PKE scheme $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ as follows.

$\mathsf{KeyGen}(1^\lambda)$**:** Generate $(\mathsf{pp}, \mathsf{td}) \leftarrow \mathsf{Setup}(1^\lambda)$ and output $\mathsf{pk} \coloneqq \mathsf{pp}$ and $\mathsf{sk} \coloneqq \mathsf{td}$.

$\mathsf{Enc}(\mathsf{pk}, b \in \{0,1\})$**:** Parse $\mathsf{pk} = \mathsf{pp}$. Prepare two registers $\mathbf{D}$ and $\mathbf{X}$. Generate the state

$$\frac{1}{\sqrt{2}}(|0\rangle + (-1)^b |1\rangle)_{\mathbf{D}} |\mathcal{X}\rangle_{\mathbf{X}} = \frac{1}{\sqrt{2|\mathcal{X}|}}(|0\rangle + (-1)^b |1\rangle)_{\mathbf{D}} \sum_{x\in\mathcal{X}} |x\rangle_{\mathbf{X}}.$$

Prepare another register $\mathbf{Y}$, coherently compute f_0 or f_1 into $\mathbf{Y}$ controlled by $\mathbf{D}$ to get

$$\sum_{x\in\mathcal{X}} \frac{1}{\sqrt{2|\mathcal{X}|}}(|0\rangle_{\mathbf{D}} |x\rangle_{\mathbf{X}} |f_0(x)\rangle_{\mathbf{Y}} + (-1)^b |1\rangle_{\mathbf{D}} |x\rangle_{\mathbf{X}} |f_1(x)\rangle_{\mathbf{Y}}),$$

and measure $\mathbf{Y}$ to get $y \in \mathcal{Y}$. At this point, $\mathbf{D}$ and $\mathbf{X}$ collapse to the following state:[23]

$$\frac{1}{\sqrt{2}}(|0\rangle_{\mathbf{D}} |f_0^{-1}(y)\rangle_{\mathbf{X}} + (-1)^b |1\rangle_{\mathbf{D}} |f_1^{-1}(y)\rangle_{\mathbf{X}}).$$

The above state is set to be ct.[24]

$\mathsf{Dec}(\mathsf{sk}, \mathit{ct})$**:** Parse $\mathsf{sk} = \mathsf{td}$. Let U_{td} be a unitary over $\mathbf{D}$ and $\mathbf{X}$ such that[25]

$$U_{\mathsf{td}} |0\rangle_{\mathbf{D}} |x\rangle_{\mathbf{X}} = |0\rangle_{\mathbf{D}} |x\rangle_{\mathbf{X}},$$
$$U_{\mathsf{td}} |1\rangle_{\mathbf{D}} |x\rangle_{\mathbf{X}} = |1\rangle_{\mathbf{D}} |\mathsf{Swap}(\mathsf{td}, 1, x)\rangle_{\mathbf{X}}.$$

Apply U_{td} on the register $(\mathbf{D}, \mathbf{X})$ and measure $\mathbf{D}$ in the Hadamard basis and output the measurement outcome $b' \in \{0,1\}$.

Correctness.

Theorem 2. $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ *satisfies correctness.*

Proof. An honestly generated ciphertext ct is of the form

$$\frac{1}{\sqrt{2}}(|0\rangle_{\mathbf{D}} |f_0^{-1}(y)\rangle_{\mathbf{X}} + (-1)^b |1\rangle_{\mathbf{D}} |f_1^{-1}(y)\rangle_{\mathbf{X}}).$$

By the definition of U_{td} and the swapping correctness, it is easy to see that we have

$$U_{\mathsf{td}} |0\rangle_{\mathbf{D}} |f_0^{-1}(y)\rangle_{\mathbf{X}} = |0\rangle_{\mathbf{D}} |f_0^{-1}(y)\rangle_{\mathbf{X}},$$
$$U_{\mathsf{td}} |1\rangle_{\mathbf{D}} |f_1^{-1}(y)\rangle_{\mathbf{X}} = |1\rangle_{\mathbf{D}} |f_0^{-1}(y)\rangle_{\mathbf{X}}.$$

[23] Note that the swapping correctness implies that $|f_0^{-1}(y)| = |f_1^{-1}(y)|$ for any $y \in \mathcal{Y}$.
[24] Remark that one does not need to include y in the ciphertext.
[25] Note that the second operation is possible because $\mathsf{Swap}(\mathsf{td}, 0, \mathsf{Swap}(\mathsf{td}, 1, x)) = x$.

Thus, applying U_{td} on ct results in the following state:

$$\frac{1}{\sqrt{2}}(|0\rangle_{\mathbf{D}}|f_0^{-1}(y)\rangle_{\mathbf{X}}+(-1)^b|1\rangle_{\mathbf{D}}|f_0^{-1}(y)\rangle_{\mathbf{X}})=\frac{1}{\sqrt{2}}(|0\rangle_{\mathbf{D}}+(-1)^b|1\rangle_{\mathbf{D}})\otimes|f_0^{-1}(y)\rangle_{\mathbf{X}}.$$

The measurement of $\mathbf{D}$ in the Hadamard basis therefore results in b. □

Security.

Theorem 3. *If* $(\mathsf{Setup},\mathsf{Eval},\mathsf{Swap})$ *satisfies conversion hardness,* $(\mathsf{KeyGen},\mathsf{Enc},\mathsf{Dec})$ *is IND-CPA secure.*

We can prove Theorem 3 by using Item 2 of Theorem 1. We defer the proof to the full version since the idea is already explained in Sec. 2.1.

4.3 Instantiation from Group Actions

We review basic definitions about cryptographic group actions and their one-wayness and pseudorandomness following [25]. Then, we construct a STF based on it.

Basic definitions.

Definition 9 (Group actions). *Let G be a (not necessarily abelian) group, S be a set, and $\star : G\times S\to S$ be a function where we write $g\star s$ to mean $\star(g,s)$. We say that $(G,S,\star)$ is a* group action *if it satisfies the following:*

1. *For the identity element $e\in G$ and any $s\in S$, we have $e\star s=s$.*
2. *For any $g,h\in G$ and any $s\in S$, we have $(gh)\star s=g\star(h\star s)$.*

To be useful for cryptography, we have to at least assume that basic operations about $(G,S,\star)$ have efficient algorithms. We require the following efficient algorithms similarly to [25].

Definition 10 (Group actions with efficient algorithms). *We say that a group action $(G,S,\star)$ has* efficient algorithms *if it satisfies the following:*[26]

Unique representations: *Each element of G and S can be represented as a bit string of length* $\mathrm{poly}(\lambda)$ *in a unique manner. Thus, we identify these elements and their representations.*

Group operations: *There are classical deterministic polynomial-time algorithms that compute gh from $g\in G$ and $h\in G$ and g^{-1} from $g\in G$.*

Group action: *There is a classical deterministic polynomial-time algorithm that computes $g\star s$ from $g\in G$ and $s\in S$.*

[26] Strictly speaking, we have to consider a family $\{(G_\lambda,S_\lambda,\star_\lambda)\}_{\lambda\in\mathbb{N}}$ of group actions parameterized by the security parameter to meaningfully define the efficiency requirements. We omit the dependence on λ for notational simplicity throughout the paper.

Efficient recognizability: *There are classical deterministic polynomial-time algorithms that decide if a given bit string represents an element of G or S, respectively.*

Random sampling: *There are PPT algorithms that sample almost uniform elements of G or S (i.e., the distribution of the sample is statistically close to the uniform distribution), respectively.*

Superposition over G: *There is a QPT algorithm that generates a state whose trace distance from $|G\rangle$ is* $\mathsf{negl}(\lambda)$.

Remark 6 (A convention on "Random sampling" and "Superposition over G" properties). In the rest of this paper, we assume that we can sample elements from *exactly* uniform distributions of G and S. Similarly, we assume that we can *exactly* generate $|G\rangle$ in QPT. They are just for simplifying the presentations of our results, and all the results hold with the above imperfect version with additive negligible loss for security or correctness.

The above requirements are identical to those in [25] except for the "superposition over G" property. We remark that all candidate constructions proposed in [25] satisfy this property as explained later.

Assumptions. We define one-wayness and pseudorandomness following [25].

Definition 11 (One-wayness). *We say that a group action $(G, S, \star)$ with efficient algorithms is* one-way *if for any non-uniform QPT adversary $\mathcal{A}$, we have*

$$\Pr\left[g' \star s = g \star s : s \leftarrow S, g \leftarrow G, g' \leftarrow \mathcal{A}(s, g \star s)\right] = \mathsf{negl}(\lambda).$$

Definition 12 (Pseudorandomness). *We say that a group action $(G, S, \star)$ with efficient algorithms is* pseudorandom *if it satisfies the following:*

1. *We have*

$$\Pr[\exists g \in G \text{ s.t. } g \star s = t : s, t \leftarrow S] = \mathsf{negl}(\lambda).$$

2. *For any non-uniform QPT adversary $\mathcal{A}$, we have*

$$|\Pr\left[1 \leftarrow \mathcal{A}(s, t) : s \leftarrow S, g \leftarrow G, t \coloneqq g \star s\right] - \Pr\left[1 \leftarrow \mathcal{A}(s, t) : s, t \leftarrow S\right]| = \mathsf{negl}(\lambda).$$

Remark 7 (On Item 1). We require Item 1 to make Item 2 non-trivial. For example, if $(G, S, \star)$ is transitive, i.e., for any $s, t \in S$, there is $g \in G$ such that $g \star s = t$, Item 2 trivially holds because the distributions of $t = g \star s$ is uniformly distributed over S for any fixed s and random $g \leftarrow G$.

Remark 8 (Pseudorandom $\rightarrow$ One-way). We remark that the pseudorandomness immediately implies the one-wayness as noted in [25].

Instantiations. Ji et al. [25] gave several candidate constructions of one-way and pseudorandom group actions with efficient algorithms based on general linear group actions on tensors. We briefly describe one of their candidates below. Let

$\mathbb{F}$ be a finite field, and k, $d_1, d_2 ..., d_k$ be positive integers (which are typically set as $k = 3$ and $d_1 = d_2 = d_3$). We set $G := \prod_{j=1}^{k} GL_{d_j}(\mathbb{F})$, $S := \bigotimes_{j=1}^{k} \mathbb{F}^{d_j}$, and define the group action by the matrix-vector multiplication as

$$(M_j)_{j\in[k]} \star T := \left(\bigotimes_{j=1}^{k} M_j\right) T$$

for $(M_j)_{j\in[k]} \in \prod_{j=1}^{k} GL_{d_j}(\mathbb{F})$ and $T \in \bigotimes_{j=1}^{k} \mathbb{F}^{d_j}$. See [25] for attempts of cryptanalysis and justification of the one-wayness and pseudorandomness. We remark that we introduced an additional requirement of the "superposition over G" property in Definition 10, but their candidates satisfy this property. In their candidates, the group G is a direct product of general linear groups over finite fields (or symmetric groups for one of the candidates), and a uniformly random matrix over finite fields is invertible with overwhelming probability for appropriate parameters.

Construction of STF. We construct a STF based on group actions. Let $(G, S, \star)$ be a group action with efficient algorithms (as defined in Definition 10). Then, we construct a STF as follows.

$\mathsf{Setup}(1^\lambda)$**:** Generate $s_0 \leftarrow S$ and $g \leftarrow G$, set $s_1 := g \star s_0$, and output $\mathsf{pp} := (s_0, s_1)$ and $\mathsf{td} := g$. For $b \in \{0, 1\}$, we define $f_b : G \to S$ by $f_b(h) := h \star s_b$.
$\mathsf{Eval}(\mathsf{pp} = (s_0, s_1), b, h)$**:** Output $f_b(h) = h \star s_b$.
$\mathsf{Swap}(\mathsf{td} = g, b, h)$**:** If $b = 0$, output hg^{-1}. If $b = 1$, output hg.

The evaluation correctness is trivial. The swapping correctness can be seen as follows: For any $h \in G$, $f_1(\mathsf{Swap}(\mathsf{td}, 0, h)) = f_1(hg^{-1}) = (hg^{-1}) \star s_1 = h \star s_0 = f_0(h)$. Similarly, for any $h \in G$, $f_0(\mathsf{Swap}(\mathsf{td}, 1, h)) = f_0(hg) = (hg) \star s_0 = h \star s_1 = f_1(h)$. For any $h \in G$, $\mathsf{Swap}(\mathsf{td}, 1, \mathsf{Swap}(\mathsf{td}, 0, h)) = \mathsf{Swap}(\mathsf{td}, 1, hg^{-1}) = (hg^{-1})g = h$.

The efficient sampling and efficient superposition properties directly follow from the corresponding properties of the group action.

We prove the following theorem.

Theorem 4. *The following hold:*

1. *If $(G, S, \star)$ is one-way, then $(\mathsf{Setup}, \mathsf{Eval}, \mathsf{Swap})$ is claw-free.*
2. *If $(G, S, \star)$ is pseudorandom, then $(\mathsf{Setup}, \mathsf{Eval}, \mathsf{Swap})$ is conversion hard.*

We defer the proof to the full version because it is easy.

Quantum-ciphertext PKE from group actions. Recall that conversion hard STFs suffice for constructing IND-CPA secure quantum ciphertext PKE (Theorem 3). Then, by Lemmata 1 and 2 and Theorem 4, we obtain the following corollaries.

Corollary 1. *If there exists a pseudorandom group action with efficient algorithms, there exists an IND-CPA secure quantum-ciphertext PKE.*

Remark 9 (Lossy encryption). Actually, we can show that the quantum-ciphertext PKE constructed from a pseudorandom group action is lossy encryption [4], which is stronger than IND-CPA secure one. We omit the detail since our focus is on constructing IND-CPA secure schemes.

Corollary 2. *If there exists a one-way group action with efficient algorithms such that f_0 is collapsing,*[27] *there exists a uniform IND-CPA secure quantum-ciphertext PKE scheme.*

Corollary 3. *If there exists a one-way group action with efficient algorithms, there exists a uniform IND-CPA secure quantum-ciphertext PKE scheme or infinitely-often one-shot signatures.*[28]

5 Equivalence between Swapping and Distinguishing with Auxiliary States

For our application to conversion for commitments, we need a generalization of Theorem 1 that considers auxiliary quantum states. While it is straightforward to generalize Item 2 to such a setting,[29] a generalization of Item 1 is non-trivial. The problems is that the unitary U may not preserve the auxiliary state when it "swaps" $|x\rangle$ and $|y\rangle$.[30] Intuitively, we overcome this issue by "uncomputing" the auxiliary state in a certain sense.

Theorem 5 (Generalization of Theorem 1 with auxiliary states).

1. *Let $|x\rangle, |y\rangle$ be orthogonal n-qubit states and $|\tau\rangle$ be an m-qubit state. Let U be a polynomial-time computable unitary over $(n+m)$-qubit states and define Γ as*

$$\Gamma := \left\| (\langle y| \otimes I^{\otimes m}) U |x\rangle |\tau\rangle + (\langle x| \otimes I^{\otimes m}) U |y\rangle |\tau\rangle \right\|.$$

   Then, there exists a non-uniform QPT distinguisher $\mathcal{A}$ with advice $|\tau'\rangle = |\tau\rangle \otimes \frac{|x\rangle|0\rangle+|y\rangle|1\rangle}{\sqrt{2}}$ that distinguishes $|\psi\rangle = \frac{|x\rangle+|y\rangle}{\sqrt{2}}$ and $|\phi\rangle = \frac{|x\rangle-|y\rangle}{\sqrt{2}}$ with advantage $\frac{\Gamma^2}{4}$. Moreover, if U does not act on some qubits, then $\mathcal{A}$ also does not act on those qubits.
2. *Let $|\psi\rangle, |\phi\rangle$ be orthogonal n-qubit states, and suppose that a non-uniform QPT distinguisher A with an m-qubit advice $|\tau\rangle$ distinguishes $|\psi\rangle$ and $|\phi\rangle$ with advantage Δ without using additional ancilla qubits besides $|\tau\rangle$. Then,*

[27] We currently have no candidate of such a one-way group action.
[28] The uniform IND-CPA security is defined similarly to the IND-CPA security in Definition 8 except that the adversary is restricted to be *uniform* QPT.
[29] Indeed, such a generalization of Item 2 is already implicitly used in the proof of Theorem 3.
[30] This is also observed in [1, Footnote 2].

there exists a polynomial-time computable unitary U over $(n+m)$-qubit states such that

$$\frac{|\langle y|\langle\tau|U|x\rangle|\tau\rangle + \langle x|\langle\tau|U|y\rangle|\tau\rangle|}{2} = \Delta$$

where $|x\rangle := \frac{|\psi\rangle+|\phi\rangle}{\sqrt{2}}$ and $|y\rangle := \frac{|\psi\rangle-|\phi\rangle}{\sqrt{2}}$. Moreover, if $\mathcal{A}$ does not act on some qubits, then U also does not act on those qubits.

Remark 10. We remark that Item 1 does *not* preserve the auxiliary state unlike Item 2. Though this does not capture the intuition that "one can distinguish $|\psi\rangle$ and $|\phi\rangle$ whenever he can swap $|x\rangle$ and $|y\rangle$", this is good enough for our purpose. We also remark that there is a quadratic reduction loss in Item 1. We do not know if it is tight while both items of Theorem 1 is shown to be tight in [1].

Proof of Theorem 5. Item 2 directly follows from Item 2 of Theorem 1 by considering $|x\rangle|\tau\rangle$ and $|y\rangle|\tau\rangle$ as $|x\rangle$ and $|y\rangle$ in Theorem 1. We prove Item 1 below.

Proof of Item 1. Let $\mathbf{A}$ and $\mathbf{A}'$ be n-qubit registers, $\mathbf{Z}$ be an m-qubit register, and $\mathbf{B}$ be a 1-qubit register. We define a unitary $\widetilde{U}$ over $(\mathbf{A},\mathbf{Z},\mathbf{A}',\mathbf{B})$ as follows:

$$\widetilde{U} := X_{\mathbf{B}} U^{\dagger}_{\mathbf{A}',\mathbf{Z}} U_{\mathbf{A},\mathbf{Z}} \tag{3}$$

where $X_{\mathbf{B}}$ is the Pauli X operator on $\mathbf{B}$ and $U^{\dagger}_{\mathbf{A}',\mathbf{Z}}$ means the inverse of $U_{\mathbf{A}',\mathbf{Z}}$, which works similarly to $U_{\mathbf{A},\mathbf{Z}}$ except that it acts on $\mathbf{A}'$ instead of on $\mathbf{A}$.

Then, we prove the following claim.

Claim 6. *Let $|x\rangle, |y\rangle, |\tau\rangle$, and Γ be as in Item 1 of Theorem 5, $\widetilde{U}$ be as defined in Equation (3), and $|\sigma\rangle_{\mathbf{A}',\mathbf{B}}$ be the state over $(\mathbf{A}',\mathbf{B})$ defined as follows:*

$$|\sigma\rangle_{\mathbf{A}',\mathbf{B}} := \frac{|x\rangle_{\mathbf{A}'}|0\rangle_{\mathbf{B}} + |y\rangle_{\mathbf{A}'}|1\rangle_{\mathbf{B}}}{\sqrt{2}}. \tag{4}$$

Then, it holds that

$$\left|\langle y|_{\mathbf{A}}\langle\tau|_{\mathbf{Z}}\langle\sigma|_{\mathbf{A}',\mathbf{B}}\widetilde{U}|x\rangle_{\mathbf{A}}|\tau\rangle_{\mathbf{Z}}|\sigma\rangle_{\mathbf{A}',\mathbf{B}} + \langle x|_{\mathbf{A}}\langle\tau|_{\mathbf{Z}}\langle\sigma|_{\mathbf{A}',\mathbf{B}}\widetilde{U}|y\rangle_{\mathbf{A}}|\tau\rangle_{\mathbf{Z}}|\sigma\rangle_{\mathbf{A}',\mathbf{B}}\right| = \frac{\Gamma^2}{2}.$$

We first finish the proof of Item 1 assuming that Claim 6 is correct. By Item 1 of Theorem 1, Claim 6 implies that there is a QPT distinguisher $\widetilde{\mathcal{A}}$ that distinguishes

$$|\widetilde{\psi}\rangle = \frac{(|x\rangle+|y\rangle)_{\mathbf{A}}|\tau\rangle_{\mathbf{Z}}|\sigma\rangle_{\mathbf{A}',\mathbf{B}}}{\sqrt{2}}$$

and

$$|\widetilde{\phi}\rangle = \frac{(|x\rangle-|y\rangle)_{\mathbf{A}}|\tau\rangle_{\mathbf{Z}}|\sigma\rangle_{\mathbf{A}',\mathbf{B}}}{\sqrt{2}}$$

with advantage $\frac{\Gamma^2}{4}$. Moreover, $\widetilde{\mathcal{A}}$ does not act on qubits on which $\widetilde{U}$ does not act. In particular, $\widetilde{\mathcal{A}}$ does not act on qubits of $\mathbf{A}$ and $\mathbf{Z}$ on which $U_{\mathbf{A},\mathbf{Z}}$ does not act since $\widetilde{U}$ acts on $\mathbf{A}$ and $\mathbf{Z}$ only through $U_{\mathbf{A},\mathbf{Z}}$ and $U^\dagger_{\mathbf{A}',\mathbf{Z}}$. Thus, by considering $\widetilde{\mathcal{A}}$ as a distinguisher $\mathcal{A}$ with advice $|\tau'\rangle = |\tau\rangle_{\mathbf{Z}} |\sigma\rangle_{\mathbf{A}',\mathbf{B}}$ that distinguishes $|\psi\rangle = \frac{|x\rangle+|y\rangle}{\sqrt{2}}$ and $|\phi\rangle = \frac{|x\rangle-|y\rangle}{\sqrt{2}}$, Item 1 is proven. Below, we prove Claim 6.

Proof of Claim 6. For $(a,b) \in \{(x,x),(x,y),(y,x),(y,y)\}$, we define

$$|\tau'_{ab}\rangle_{\mathbf{Z}} := (\langle b|_{\mathbf{A}} \otimes I_{\mathbf{Z}}) U_{\mathbf{A},\mathbf{Z}} |a\rangle_{\mathbf{A}} |\tau\rangle_{\mathbf{Z}} .$$

Then, we have

$$\Gamma = \left\| |\tau'_{xy}\rangle_{\mathbf{Z}} + |\tau'_{yx}\rangle_{\mathbf{Z}} \right\| \tag{5}$$

and

$$U_{\mathbf{A},\mathbf{Z}} |x\rangle_{\mathbf{A}} |\tau\rangle_{\mathbf{Z}} = |x\rangle_{\mathbf{A}} |\tau'_{xx}\rangle_{\mathbf{Z}} + |y\rangle_{\mathbf{A}} |\tau'_{xy}\rangle_{\mathbf{Z}} + |\mathrm{garbage}_x\rangle_{\mathbf{A},\mathbf{Z}} \tag{6}$$
$$U_{\mathbf{A},\mathbf{Z}} |y\rangle_{\mathbf{A}} |\tau\rangle_{\mathbf{Z}} = |x\rangle_{\mathbf{A}} |\tau'_{yx}\rangle_{\mathbf{Z}} + |y\rangle_{\mathbf{A}} |\tau'_{yy}\rangle_{\mathbf{Z}} + |\mathrm{garbage}_y\rangle_{\mathbf{A},\mathbf{Z}} \tag{7}$$

where $|\mathrm{garbage}_x\rangle_{\mathbf{A},\mathbf{Z}}$ and $|\mathrm{garbage}_y\rangle_{\mathbf{A},\mathbf{Z}}$ are (not necessarily normalized) states such that

$$(\langle x|_{\mathbf{A}} \otimes I_{\mathbf{Z}}) |\mathrm{garbage}_x\rangle_{\mathbf{A},\mathbf{Z}} = (\langle y|_{\mathbf{A}} \otimes I_{\mathbf{Z}}) |\mathrm{garbage}_x\rangle_{\mathbf{A},\mathbf{Z}} = 0, \tag{8}$$
$$(\langle x|_{\mathbf{A}} \otimes I_{\mathbf{Z}}) |\mathrm{garbage}_y\rangle_{\mathbf{A},\mathbf{Z}} = (\langle y|_{\mathbf{A}} \otimes I_{\mathbf{Z}}) |\mathrm{garbage}_y\rangle_{\mathbf{A},\mathbf{Z}} = 0. \tag{9}$$

Then,

$$\begin{aligned}
&\langle y|_{\mathbf{A}} \langle \tau|_{\mathbf{Z}} \langle \sigma|_{\mathbf{A}',\mathbf{B}} \widetilde{U} |x\rangle_{\mathbf{A}} |\tau\rangle_{\mathbf{Z}} |\sigma\rangle_{\mathbf{A}',\mathbf{B}} \\
=& \langle y|_{\mathbf{A}} \langle \tau|_{\mathbf{Z}} \langle \sigma|_{\mathbf{A}',\mathbf{B}} X_{\mathbf{B}} U^\dagger_{\mathbf{A}',\mathbf{Z}} (|x\rangle_{\mathbf{A}} |\tau'_{xx}\rangle_{\mathbf{Z}} + |y\rangle_{\mathbf{A}} |\tau'_{xy}\rangle_{\mathbf{Z}} + |\mathrm{garbage}_x\rangle_{\mathbf{A},\mathbf{Z}}) |\sigma\rangle_{\mathbf{A}',\mathbf{B}} \\
=& \langle \tau|_{\mathbf{Z}} \langle \sigma|_{\mathbf{A}',\mathbf{B}} X_{\mathbf{B}} U^\dagger_{\mathbf{A}',\mathbf{Z}} |\tau'_{xy}\rangle_{\mathbf{Z}} |\sigma\rangle_{\mathbf{A}',\mathbf{B}}
\end{aligned} \tag{10}$$

where the first equality follows from Equation (6) and the second equality follows from Equation (8) and the assumption that $|x\rangle$ and $|y\rangle$ are orthogonal. By Equations (4), (6) and (7), it holds that

$$\begin{aligned}
&U_{\mathbf{A}',\mathbf{Z}} X_{\mathbf{B}} |\tau\rangle_{\mathbf{Z}} |\sigma\rangle_{\mathbf{A}',\mathbf{B}} \\
=& U_{\mathbf{A}',\mathbf{Z}} \frac{|\tau\rangle_{\mathbf{Z}} (|x\rangle_{\mathbf{A}'} |1\rangle_{\mathbf{B}} + |y\rangle_{\mathbf{A}'} |0\rangle_{\mathbf{B}})}{\sqrt{2}} \\
=& \frac{1}{\sqrt{2}} \begin{pmatrix} \left(|x\rangle_{\mathbf{A}'} |\tau'_{xx}\rangle_{\mathbf{Z}} + |y\rangle_{\mathbf{A}'} |\tau'_{xy}\rangle_{\mathbf{Z}} + |\mathrm{garbage}_x\rangle_{\mathbf{A}',\mathbf{Z}}\right) |1\rangle_{\mathbf{B}} \\ + \left(|x\rangle_{\mathbf{A}'} |\tau'_{yx}\rangle_{\mathbf{Z}} + |y\rangle_{\mathbf{A}'} |\tau'_{yy}\rangle_{\mathbf{Z}} + |\mathrm{garbage}_y\rangle_{\mathbf{A}',\mathbf{Z}}\right) |0\rangle_{\mathbf{B}} \end{pmatrix} .
\end{aligned} \tag{11}$$

Then, it holds that

$$\begin{aligned}
&\langle\tau|_{\mathbf{Z}}\langle\sigma|_{\mathbf{A}',\mathbf{B}} X_{\mathbf{B}} U^{\dagger}_{\mathbf{A}',\mathbf{Z}} |\tau'_{xy}\rangle_{\mathbf{Z}} |\sigma\rangle_{\mathbf{A}',\mathbf{B}} \\
=&\frac{1}{2}\left(\begin{array}{l}\left(\langle x|_{\mathbf{A}'}\langle\tau'_{xx}|_{\mathbf{Z}} + \langle y|_{\mathbf{A}'}\langle\tau'_{xy}|_{\mathbf{Z}} + \langle \mathrm{garbage}_x|_{\mathbf{A}',\mathbf{Z}}\right)\langle 1|_{\mathbf{B}} \\ +\left(\langle x|_{\mathbf{A}'}\langle\tau'_{yx}|_{\mathbf{Z}} + \langle y|_{\mathbf{A}'}\langle\tau'_{yy}|_{\mathbf{Z}} + \langle \mathrm{garbage}_y|_{\mathbf{A}',\mathbf{Z}}\right)\langle 0|_{\mathbf{B}}\end{array}\right)(|x\rangle_{\mathbf{A}'}|0\rangle_{\mathbf{B}} + |y\rangle_{\mathbf{A}'}|1\rangle_{\mathbf{B}})|\tau'_{xy}\rangle_{\mathbf{Z}} \\
=&\frac{1}{2}(\langle\tau'_{xy}| + \langle\tau'_{yx}|)_{\mathbf{Z}}|\tau'_{xy}\rangle_{\mathbf{Z}},
\end{aligned} \tag{12}$$

where the first equality follows from Equations (4) and (11) and the second equality follows from Equations (8) and (9) and the assumption that $|x\rangle$ and $|y\rangle$ are orthogonal.

By Equations (10) and (12), we have

$$\langle y|_{\mathbf{A}}\langle\tau|_{\mathbf{Z}}\langle\sigma|_{\mathbf{A}',\mathbf{B}}\widetilde{U}|x\rangle_{\mathbf{A}}|\tau\rangle_{\mathbf{Z}}|\sigma\rangle_{\mathbf{A}',\mathbf{B}} = \frac{1}{2}(\langle\tau'_{xy}| + \langle\tau'_{yx}|)_{\mathbf{Z}}|\tau'_{xy}\rangle_{\mathbf{Z}}. \tag{13}$$

By a similar calculation, we have

$$\langle x|_{\mathbf{A}}\langle\tau|_{\mathbf{Z}}\langle\sigma|_{\mathbf{A}',\mathbf{B}}\widetilde{U}|y\rangle_{\mathbf{A}}|\tau\rangle_{\mathbf{Z}}|\sigma\rangle_{\mathbf{A}',\mathbf{B}} = \frac{1}{2}(\langle\tau'_{xy}| + \langle\tau'_{yx}|)_{\mathbf{Z}}|\tau'_{yx}\rangle_{\mathbf{Z}}. \tag{14}$$

By Equations (13) and (14), we have

$$\begin{aligned}
&\langle y|_{\mathbf{A}}\langle\tau|_{\mathbf{Z}}\langle\sigma|_{\mathbf{A}',\mathbf{B}}\widetilde{U}|x\rangle_{\mathbf{A}}|\tau\rangle_{\mathbf{Z}}|\sigma\rangle_{\mathbf{A}',\mathbf{B}} + \langle x|_{\mathbf{A}}\langle\tau|_{\mathbf{Z}}\langle\sigma|_{\mathbf{A}',\mathbf{B}}\widetilde{U}|y\rangle_{\mathbf{A}}|\tau\rangle_{\mathbf{Z}}|\sigma\rangle_{\mathbf{A}',\mathbf{B}} \\
=&\frac{1}{2}\left\||\tau'_{xy}\rangle_{\mathbf{Z}} + |\tau'_{yx}\rangle_{\mathbf{Z}}\right\|^2.
\end{aligned}$$

By combining the above with Equation (5), we complete the proof of Claim 6. □

This completes the proof of Theorem 5. □

6 Our Conversion for Commitments

In this section, we give a conversion for canonical quantum bit commitments that converts the flavors of security using Theorem 5.

Theorem 7 (Converting Flavors). *Let $\{Q_0, Q_1\}$ be a canonical quantum bit commitment scheme. Let $\{Q'_0, Q'_1\}$ be a canonical quantum bit commitment scheme described as follows:*

- *The roles of commitment and reveal registers are swapped from $\{Q_0, Q_1\}$ and the commitment register is augmented by an additional one-qubit register. That is, if $\mathbf{C}$ and $\mathbf{R}$ are the commitment and reveal registers of $\{Q_0, Q_1\}$, then the commitment and reveal registers of $\{Q'_0, Q'_1\}$ are defined as $\mathbf{C}' := (\mathbf{R}, \mathbf{D})$ and $\mathbf{R}' := \mathbf{C}$ where $\mathbf{D}$ is a one-qubit register.*

– *For $b \in \{0,1\}$, the unitary Q'_b is defined as follows:*

$$Q'_b := (Q_0 \otimes |0\rangle\langle 0|_{\mathbf{D}} + Q_1 \otimes |1\rangle\langle 1|_{\mathbf{D}}) \left(I_{\mathbf{R},\mathbf{C}} \otimes Z_{\mathbf{D}}^b H_{\mathbf{D}}\right)$$

where $Z_{\mathbf{D}}$ and $H_{\mathbf{D}}$ denote the Pauli Z and the Hadamard operators on $\mathbf{D}$.

Then, the following hold for $\mathtt{X}, \mathtt{Y} \in \{$computationally,statistically,perfectly$\}$:

1. *If $\{Q_0, Q_1\}$ is $\mathtt{X}$ hiding, then $\{Q'_0, Q'_1\}$ is $\mathtt{X}$ binding.*
2. *If $\{Q_0, Q_1\}$ is $\mathtt{Y}$ binding, then $\{Q'_0, Q'_1\}$ is $\mathtt{Y}$ hiding.*

Note that we have

$$Q'_b |0\rangle_{\mathbf{C}',\mathbf{R}'} = \frac{1}{\sqrt{2}} \left((Q_0 |0\rangle)_{\mathbf{C},\mathbf{R}} |0\rangle_{\mathbf{D}} + (-1)^b (Q_1 |0\rangle)_{\mathbf{C},\mathbf{R}} |1\rangle_{\mathbf{D}}\right)$$

for $b \in \{0,1\}$ where $(\mathbf{C}', \mathbf{R}')$ is rearranged as $(\mathbf{C}, \mathbf{R}, \mathbf{D})$.

We defer the proof of Theorem 7 to the full version since it easily follows from Theorem 5 as explained in Sec. 2.2.

Applications. We give applications of Theorem 7 in the full version.

Acknowledgements. MH is supported by a KIAS Individual Grant QP089801. TM is supported by JST Moonshot R&D JPMJMS2061-5-1-1, JST FOREST, MEXT QLEAP, the Grant-in-Aid for Scientific Research (B) No.JP19H04066, the Grant-in Aid for Transformative Research Areas (A) 21H05183, and the Grant-in-Aid for Scientific Research (A) No.22H00522.

References

1. Aaronson, S., Atia, Y., Susskind, L.: On the hardness of detecting macroscopic superpositions. Electron. Colloquium Comput. Complex. p. 146 (2020)
2. Alamati, N., De Feo, L., Montgomery, H., Patranabis, S.: Cryptographic group actions and applications. In: Moriai, S., Wang, H. (eds.) ASIACRYPT 2020, Part II. LNCS, vol. 12492, pp. 411–439. Springer, Heidelberg (Dec 2020). https://doi.org/10.1007/978-3-030-64834-3_14
3. Amos, R., Georgiou, M., Kiayias, A., Zhandry, M.: One-shot signatures and applications to hybrid quantum/classical authentication. In: Makarychev, K., Makarychev, Y., Tulsiani, M., Kamath, G., Chuzhoy, J. (eds.) 52nd ACM STOC. pp. 255–268. ACM Press (Jun 2020). https://doi.org/10.1145/3357713.3384304
4. Bellare, M., Hofheinz, D., Yilek, S.: Possibility and impossibility results for encryption and commitment secure under selective opening. In: Joux, A. (ed.) EUROCRYPT 2009. LNCS, vol. 5479, pp. 1–35. Springer, Heidelberg (Apr 2009). https://doi.org/10.1007/978-3-642-01001-9_1
5. Ben-David, S., Sattath, O.: Quantum tokens for digital signatures. Cryptology ePrint Archive, Paper 2017/094 (2017), https://eprint.iacr.org/2017/094, https://eprint.iacr.org/2017/094
6. Bitansky, N., Brakerski, Z.: Classical binding for quantum commitments. In: Nissim, K., Waters, B. (eds.) TCC 2021, Part I. LNCS, vol. 13042, pp. 273–298. Springer, Heidelberg (Nov 2021). https://doi.org/10.1007/978-3-030-90459-3_10

7. Brakerski, Z., Christiano, P., Mahadev, U., Vazirani, U.V., Vidick, T.: A cryptographic test of quantumness and certifiable randomness from a single quantum device. In: Thorup, M. (ed.) 59th FOCS. pp. 320–331. IEEE Computer Society Press (Oct 2018). https://doi.org/10.1109/FOCS.2018.00038
8. Brassard, G., Yung, M.: One-way group actions. In: Menezes, A.J., Vanstone, S.A. (eds.) CRYPTO'90. LNCS, vol. 537, pp. 94–107. Springer, Heidelberg (Aug 1991). https://doi.org/10.1007/3-540-38424-3_7
9. Broadbent, A., Jeffery, S.: Quantum homomorphic encryption for circuits of low T-gate complexity. In: Gennaro, R., Robshaw, M.J.B. (eds.) CRYPTO 2015, Part II. LNCS, vol. 9216, pp. 609–629. Springer, Heidelberg (Aug 2015). https://doi.org/10.1007/978-3-662-48000-7_30
10. Castryck, W., Lange, T., Martindale, C., Panny, L., Renes, J.: CSIDH: An efficient post-quantum commutative group action. In: Peyrin, T., Galbraith, S. (eds.) ASIACRYPT 2018, Part III. LNCS, vol. 11274, pp. 395–427. Springer, Heidelberg (Dec 2018). https://doi.org/10.1007/978-3-030-03332-3_15
11. Chailloux, A., Kerenidis, I., Rosgen, B.: Quantum commitments from complexity assumptions. In: Aceto, L., Henzinger, M., Sgall, J. (eds.) ICALP 2011, Part I. LNCS, vol. 6755, pp. 73–85. Springer, Heidelberg (Jul 2011). https://doi.org/10.1007/978-3-642-22006-7_7
12. Coladangelo, A., Liu, J., Liu, Q., Zhandry, M.: Hidden cosets and applications to unclonable cryptography. In: Malkin, T., Peikert, C. (eds.) CRYPTO 2021, Part I. LNCS, vol. 12825, pp. 556–584. Springer, Heidelberg, Virtual Event (Aug 2021). https://doi.org/10.1007/978-3-030-84242-0_20
13. Couveignes, J.M.: Hard homogeneous spaces. Cryptology ePrint Archive, Paper 2006/291 (2006), https://eprint.iacr.org/2006/291
14. Crépeau, C., Légaré, F., Salvail, L.: How to convert the flavor of a quantum bit commitment. In: Pfitzmann, B. (ed.) EUROCRYPT 2001. LNCS, vol. 2045, pp. 60–77. Springer, Heidelberg (May 2001). https://doi.org/10.1007/3-540-44987-6_5
15. Diffie, W., Hellman, M.E.: New directions in cryptography. IEEE Trans. Inf. Theory **22**(6), 644–654 (1976). https://doi.org/10.1109/TIT.1976.1055638
16. Dumais, P., Mayers, D., Salvail, L.: Perfectly concealing quantum bit commitment from any quantum one-way permutation. In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, pp. 300–315. Springer, Heidelberg (May 2000). https://doi.org/10.1007/3-540-45539-6_21
17. ElGamal, T.: A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory **31**, 469–472 (1985)
18. Fang, J., Unruh, D., Yan, J., Zhou, D.: How to base security on the perfect/statistical binding property of quantum bit commitment? In: Bae, S.W., Park, H. (eds.) 33rd International Symposium on Algorithms and Computation, ISAAC 2022, December 19-21, 2022, Seoul, Korea. LIPIcs, vol. 248, pp. 26:1–26:12. Schloss Dagstuhl - Leibniz-Zentrum für Informatik (2022). https://doi.org/10.4230/LIPIcs.ISAAC.2022.26
19. Gentry, C., Peikert, C., Vaikuntanathan, V.: Trapdoors for hard lattices and new cryptographic constructions. In: Ladner, R.E., Dwork, C. (eds.) 40th ACM STOC. pp. 197–206. ACM Press (May 2008). https://doi.org/10.1145/1374376.1374407
20. Goldreich, O., Levin, L.A.: A hard-core predicate for all one-way functions. In: 21st ACM STOC. pp. 25–32. ACM Press (May 1989). https://doi.org/10.1145/73007.73010

21. Goldwasser, S., Micali, S., Rivest, R.L.: A "paradoxical" solution to the signature problem (extended abstract). In: 25th FOCS. pp. 441–448. IEEE Computer Society Press (Oct 1984). https://doi.org/10.1109/SFCS.1984.715946
22. Haitner, I., Reingold, O.: Statistically-hiding commitment from any one-way function. In: Johnson, D.S., Feige, U. (eds.) 39th ACM STOC. pp. 1–10. ACM Press (Jun 2007). https://doi.org/10.1145/1250790.1250792
23. Håstad, J., Impagliazzo, R., Levin, L.A., Luby, M.: A pseudorandom generator from any one-way function. SIAM J. Comput. **28**(4), 1364–1396 (1999). https://doi.org/10.1137/S0097539793244708
24. Impagliazzo, R.: A personal view of average-case complexity. In: Proceedings of the Tenth Annual Structure in Complexity Theory Conference, Minneapolis, Minnesota, USA, June 19-22, 1995. pp. 134–147. IEEE Computer Society (1995). https://doi.org/10.1109/SCT.1995.514853
25. Ji, Z., Qiao, Y., Song, F., Yun, A.: General linear group action on tensors: A candidate for post-quantum cryptography. In: Hofheinz, D., Rosen, A. (eds.) TCC 2019, Part I. LNCS, vol. 11891, pp. 251–281. Springer, Heidelberg (Dec 2019). https://doi.org/10.1007/978-3-030-36030-6_11
26. Lo, H.K., Chau, H.F.: Is quantum bit commitment really possible? Physical Review Letters **78**(17), 3410 (1997). https://doi.org/10.1103/physrevlett.78.3410
27. Mahadev, U.: Classical homomorphic encryption for quantum circuits. In: Thorup, M. (ed.) 59th FOCS. pp. 332–338. IEEE Computer Society Press (Oct 2018). https://doi.org/10.1109/FOCS.2018.00039
28. Mayers, D.: Unconditionally secure quantum bit commitment is impossible. Physical review letters **78**(17), 3414 (1997). https://doi.org/10.1103/physrevlett.78.3414
29. Morimae, T., Yamakawa, T.: Quantum commitments and signatures without one-way functions. In: Dodis, Y., Shrimpton, T. (eds.) CRYPTO 2022, Part I. LNCS, vol. 13507, pp. 269–295. Springer, Heidelberg (Aug 2022). https://doi.org/10.1007/978-3-031-15802-5_10
30. Naor, M.: Bit commitment using pseudorandomness. Journal of Cryptology **4**(2), 151–158 (Jan 1991). https://doi.org/10.1007/BF00196774
31. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. J. ACM **56**(6), 34:1–34:40 (2009). https://doi.org/10.1145/1568318.1568324
32. Rostovtsev, A., Stolbunov, A.: Public-key cryptosystem based on isogenies. Cryptology ePrint Archive, Paper 2006/145 (2006), https://eprint.iacr.org/2006/145
33. Unruh, D.: Computationally binding quantum commitments. In: Fischlin, M., Coron, J.S. (eds.) EUROCRYPT 2016, Part II. LNCS, vol. 9666, pp. 497–527. Springer, Heidelberg (May 2016). https://doi.org/10.1007/978-3-662-49896-5_18
34. Yan, J.: Quantum computationally predicate-binding commitments with application in quantum zero-knowledge arguments for NP. In: Tibouchi, M., Wang, H. (eds.) ASIACRYPT 2021, Part I. LNCS, vol. 13090, pp. 575–605. Springer, Heidelberg (Dec 2021). https://doi.org/10.1007/978-3-030-92062-3_20
35. Yan, J.: General properties of quantum bit commitments (extended abstract). In: Agrawal, S., Lin, D. (eds.) Advances in Cryptology - ASIACRYPT 2022 - 28th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, December 5-9, 2022, Proceedings, Part IV. Lecture Notes in Computer Science, vol. 13794, pp. 628–657. Springer (2022). https://doi.org/10.1007/978-3-031-22972-5_22
36. Yan, J., Weng, J., Lin, D., Quan, Y.: Quantum bit commitment with application in quantum zero-knowledge proof (extended abstract). In: Elbassioni,

K.M., Makino, K. (eds.) Algorithms and Computation - 26th International Symposium, ISAAC 2015, Nagoya, Japan, December 9-11, 2015, Proceedings. Lecture Notes in Computer Science, vol. 9472, pp. 555–565. Springer (2015). https://doi.org/10.1007/978-3-662-48971-0_47

37. Zhandry, M.: Quantum lightning never strikes the same state twice. In: Ishai, Y., Rijmen, V. (eds.) EUROCRYPT 2019, Part III. LNCS, vol. 11478, pp. 408–438. Springer, Heidelberg (May 2019). https://doi.org/10.1007/978-3-030-17659-4_14