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
minkihhan@kias.re.kr
[2]Yukawa Institute for Theoretical Physics, Kyoto University, Kyoto, Japan
tomoyuki.morimae@yukawa.kyoto-u.ac.jp
[3]NTT Social Informatics Laboratories, Tokyo, Japan
takashi.yamakawa.ga@hco.ntt.co.jp

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.

Contents

1 Introduction

When can we distinguish a superposition of two orthogonal states from their probabilistic mix? A folklore answer to this question was that we can distinguish them whenever we can map one of the states to the other. Recently, Aaronson, Atia and, Susskind [AAS20] 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.[1]

We explain their result in more detail by using the example of Schrödinger's cat following [AAS20]. Let $|\mathrm{Alive}\rangle$ and $|\mathrm{Dead}\rangle$ be orthogonal states, which can be 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 $|\mathrm{Dead}\rangle$.[2] 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 [GL89]. Based on this observation, we tackle the following two problems in quantum cryptography.[3]

Public key encryption from non-abelian group actions. Brassard and Yung [BY91] 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 [BY91] 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. [JQSY19] proposed new instantiations based on general linear group

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

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

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

[3] It may be a priori unclear why these problems are related to [AAS20]. This will become clearer in the technical overview in Section 2.

actions on tensors. Alamati et al. [ADMP20] proposed isogeny-based instantiations based on earlier works [Cou06, RS06, CLM+18]. Both of them are believed to be secure against quantum adversaries.

An important difference between the instantiations in [JQSY19] and [ADMP20] 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 [DH76]. 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.[4] This also naturally gives a public key encryption (PKE) scheme similar to ElGamal encryption [ElG84]. On the other hand, the above construction does not work if G is a non-abelian group. Indeed, cryptographic applications given in [JQSY19] are limited to *Minicrypt* primitives [Imp95], i.e., those that do not imply PKE in a black-box manner. Thus, [JQSY19] raised the following open question:[5]

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[6] 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 [LC97, May97]. 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 other is computationally binding and statistically hiding.[7] 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 [Nao91, HILL99, HR07], 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 [Yan22], based on an earlier work by Crépeau, Légaré, and Salvail [CLS01], 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.

[4] 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.

[5] The statement of the open problem in [JQSY19] 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.

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

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

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 [AAS20].

For **Question 1**, we construct a PKE scheme with quantum ciphertexts based on non-abelian group actions. This resolves the open problem posed by [JQSY19].[8] 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 [BJ15]. 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 [JQSY19]. In addition, we show a "win-win" result similar in spirit to [Zha19]. 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 [AGKZ20].[9] Note that constructing 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 [BDS17], the only known construction in the standard model is based on indistinguishability obfuscation [CLLZ21]. 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 [AAS20] where we consider auxiliary quantum inputs.

We show several applications of our conversion. We remark that our conversion does not give any new feasibility result since similar conversions with worse efficiency were already known [CLS01, Yan22]. However, our conversion gives schemes with better efficiency in terms of the number of calls to the building blocks.

1. In Section 7.1, we apply our conversion to the statistically binding scheme from PRGs by Yan, Weng, Lin, and Quan [YWLQ15]. Then, we obtain the first statistically hiding quantum commitment scheme from PRGs that makes only a single call to the PRGs.

[8] The statement of their open problem (quoted in Footnote 5) 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.

[9] This is a simplified claim and some subtle issues about uniformness of the adversary and "infinitely-often security" are omitted here. See Lemma 4.7 for the formal statement.

2. In Section 7.2, based on a recent work, by Morimae and Yamakawa [MY22], we show that we can use (single-copy-secure) pseudorandom state generators (PRSGs) [JLS18] instead of PRGs in the above construction. As a result, we obtain the the first statistically hiding quantum commitment scheme from PRSGs that makes only a single call to the PRSGs.

3. In Section 7.3, we give a novel simple construction of a perfectly hiding quantum commitment scheme from injective one-way functions that makes a single call to the base function. By applying our conversion to it, we obtain a perfectly binding quantum commitment scheme from injective one-way functions that makes a single call to the base function. Though there is a classical construction of such a scheme based on the Goldreich-Levin theorem [GL89], our construction has a shorter commitment length since a commitment does not need to include a seed for the hardcore predicate.

4. In Section 7.4, we show that replacing injective one-way functions with (sufficiently length-decreasing) collapsing functions [Unr16b] in the above constructions yields commitment schemes with the other flavor. As a result, we obtain the first statistically binding quantum commitment scheme from collapsing hash functions that makes a single call to the collapsing hash function.

We provide more detailed comparisons with existing constructions after the presentation of each construction in Section 7. In addition, we present more applications of our conversion (including applications to the schemes of [HM96, DMS00]) in Appendix B.

1.2 Related Work

Cryptographic group actions. Brassard and Yung [BY91] initiated the study of cryptographic group actions and proposed instantiations based on the hardness of graph isomorphism, discrete logarithm, or factoring. However, they are not suitable for our purpose since it turns out that the graph isomorphism problem can be solved in (classical) quasi polynomial-time [Bab16][10] and discrete logarithm and factoring problems can be solved in quantum polynomial time [Sho99].

Alamati et al. [ADMP20] gave an abstraction of isogeny-based cryptography as group actions. However, the isogeny-based construction only supports limited functionality formalized as *Restricted Effective Group Action* (REGA). Though it might be possible to modify our definition of group actions (Definition 4.13) to capture isogeny-based construction by considering similar restrictions, we do not do so because isogeny-based PKE is already known even without relying on quantum ciphetexts [Cou06, RS06, JD11, CLM+18].

We consider the general linear group action on tensors proposed by [JQSY19] as a main instantiation for our construction of PKE. Though their security is a newly introduced assumption by [JQSY19], they justify it by pointing out reductions to many important problems in different areas including coding theory, computational group theory, and multivariate cryptography [FGS19]. They also discuss potential cryptanalyses and demonstrate that none of them seems to work. See [JQSY19] for the details.

Quantum key distribution. Bennett and Brassard [BB84] constructed an unconditionally secure key exchange protocol with quantum communication, which is known as *quantum key distribution*. We remark that quantum key distribution protocols are inherently interactive unlike our quantum PKE with quantum

[10] Another issue is that the graph isomorphism problem is easy for a uniformly random instance, and thus it cannot satisfy our definition of one-wayness (Definition 4.15) that requires average case hardness. If we modify the definition of the one-wayness to choose the hardest instance, the graph isomorphism-based construction may satisfy it, and such a version suffices for our applications. However, since such a construction can be broken in quasi-polynomial time by Babai's algorithm [Bab16], we do not consider this instantiation and simply consider average case version in the definition of one-wayness. A similar remark can be found in [JQSY19, Remark 1].

ciphertexts. Indeed, it is easy to see that unconditionally secure PKE with classical keys and quantum ciphertexts is impossible since a brute-force search for the correct decryption key would totally break security.

Quantum public key encryption. There are several works that proposed "quantum PKE" schemes. We compare them with our PKE with quantum ciphertexts.

The "quantum PKE" in [OTU00] is entirely classical except that the key generation algorithm can be quantum. The security of their scheme relies on the hardness of the subset-sum problem. Thus, their quantum PKE is incomparable to our PKE with quantum ciphertexts where key generation is classical, and their underlying assumption is also incomparable to ours.

The "quantum PKE" in [KKNY05] is PKE with quantum ciphertexts and *quantum public keys*. On the other hand, our quantum-ciphertext PKE uses quantum ciphertexts and *classical* public keys. Thus, their quantum PKE is a weaker primitive than our PKE with quantum ciphertexts. We remark classical public keys are much more desirable since we can certify classical public keys by using digital signatures while generating signatures on quantum messages is known to be impossible [AGM21]. The technical aspect of our PKE scheme is somewhat similar to [KKNY05] in the sense that both embed messages into phases of quantum states.

Quantum bit commitments. Bennett, Brassard, and Crépeau [BB84, BC91] initiated the study of quantum bit commitments. Unfortunately, it turned out to be impossible to construct an unconditionally secure quantum bit commitments [LC97, May97]. Thus, later works constructed quantum bit commitments relying on complexity assumptions [DMS00, CLS01, KO09, KO11, YWLQ15, MY22, AQY22]. A seminal work by Yan [Yan22] showed that any (possibly interactive) quantum bit commitments can be converted into one in a non-interactive *canonical* form. His definition of quantum bit commitments in the canonical form requires a seemingly weak binding property called *honest-binding*. However, he showed that it is actually equivalent to *sum-binding*, which has been traditionally used as a definition of a binding property of quantum bit commitments [DMS00, CLS01, KO09, KO11, MY22]. In addition, some works [YWLQ15, FUYZ20, Yan21, MY22] showed that quantum bit commitments in the canonical form can be used as a building block of other cryptographic primitives including zero-knowledge proofs or arguments (of knowledge), oblivious transfers, and multi-party computations. Thus, we use quantum bit commitments in the canonical form (with the honest-binding property) as defined in [Yan22] as a default definition of quantum bit commitments in this paper.

Other notions of binding. As explained above, we use honest-binding as a default definition of binding. On the other hand, there are several other definitions of binding for quantum commitments. We review them and give comparisons with honest-binding. (Similar discussions can also be found in [Yan22].)

Bitansky and Brakerski [BB21] introduced the notion of *classical-binding* for quantum commitments. It roughly requires that the committed message is uniquely determined by the commitment. Though this is impossible to achieve for canonical quantum bit commitments, they avoid the impossibility by having the receiver *measure* the commitment in a certain way. The advantage of the classical binding property is that it is conceptually similar to the binding of classical commitments, and thus it is easy to give security proofs when plugging it into some protocol as a substitute for classical commitments. On the other hand, existing works [YWLQ15, FUYZ20, MY22] show that the statistical honest-binding quantum commitments are already useful for many applications. Indeed, there seems no known application for which classical-binding suffices but honest-binding does not.

Ananth, Qian, and Yuen [AQY22] introduced a new definition of a statistical binding property for quantum commitments, which we call AQY-binding. The motivation of this definition is for the application to quantum oblivious transfers and multi-party computation [BCKM21]. However, [MY22, Appendix B] observed that the statistical honest-binding property implies the AQY-binding property based on the technique of [FUYZ20].

A full proof is given in [Yan22, Appendix B].

Yan [Yan21] proved that the *computational* honest-binding property implies what is called the computational *predicate-binding* property, which is sufficient for implementing Blum's Hamiltonicity protocol.

There are several other definitions of *computational* binding for quantum (string) commitments [CDMS04, DFS04] that are shown to be more useful in applications than computational honest binding ones. However, there is no known construction that satisfies the definition of [CDMS04], and the only known construction that satisfies [DFS04] is in the CRS model and based on a special assumption that is tailored to their construction. (See [Unr16b, Yan21] for more details of these definitions.)

1.3 Concurrent Work

A concurrent work by Gunn, Ju, Ma, and Zhandry [GJMZ22] defines commitments to quantum states and shows duality between binding and hiding for them. In particular, as the special case of commitments to classical strings, they give a similar flavor conversion to ours [GJMZ22, Section 4.4.1]. However, we remark that their definitions of binding and hiding are stronger than those in [Yan22], which we use by default. Specifically, they require what they call "Z-binding", which is similar to collapse-binding introduced by Unruh [Unr16b], and "X-hiding", which is a strengthening of the normal hiding that allows the adversary to submit a superposition of classical messages as a challenge message.[11] [12] They show that we can trade statistical (resp. computational) Z-binding and statistical (resp. computational) X-hiding. This is incomparable to our result since they require stronger security for the base scheme and show stronger security for the resulting scheme. Thus, our conversion is applicable to a wider variety of schemes. For example, we have many applications as shown in Section 7 and Appendix B, but it is unclear if their conversion is applicable to those schemes since we do not know if they satisfy Z-binding or X-hiding.

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 [AAS20] at the beginning of Section 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 [BY91] 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 $(h_1^{-1}h_0) \star s_0 = s_1$.

[11] Z and X for Z-binding and X-binding stand for Pauli operators. Do not confuse them with our notation $\mathrm{X}, \mathrm{Y} \in \{\text{computationally,statistically,perfectly}\}$.

[12] It might be possible to show that statistical Z-binding and statistical X-hiding are equivalent to statistical binding and statistical hiding in [Yan22], respectively. On the other hand, it is unlikely that they extend to the computational case.

[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 $h_1 := h_0 g^{-1}$ and vice versa. Though this trapdoor g does not give a 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

$$ct_b := \frac{1}{\sqrt{2}}\left(|0\rangle |f_0^{-1}(y)\rangle + (-1)^b |1\rangle |f_1^{-1}(y)\rangle\right) \tag{1}$$

for a random $y \in S$.[15] Here, $|f_{b'}^{-1}(y)\rangle$ is the uniform superposition over $f_{b'}^{-1}(y) := \{h \in G : f_{b'}(h) = y\}$ for $b' \in \{0,1\}$. The above state can be generated by a standard technique similar to [BCM+18, Mah18]. 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 the 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 [AAS20]. 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 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 [JQSY19] suffices for this purpose. Pseudorandomness requires the following two properties:

[14] The inituition 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 $y \in S$.

[17] See Theorem 3.10 for the precise meaning of the advantage for swapping.

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 [JQSY19] gave justification on 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 [Zha19]. 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. (See Definition A.2 for the formal definition.) 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 completely broken, our idea is to amplify the probability of finding h_1 from $|f_0^{-1}(y)\rangle$ by a parallel repetition. See Appendix A for the full proof. 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 [Yan22]. He (based on earlier works [CKR11, YWLQ15, FUYZ20]) 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 $0 \dots 0$, 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

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

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) 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, [Yan22] proved that it is equivalent to another binding notion called the *sum-binding* [DMS00].[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 [YWLQ15, FUYZ20, Yan21, MY22]. 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 [AAS20]. 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 an ability to swap commitments to 0 and 1 since it may map the commitment to 1 to 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 [AAS20] 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 [AAS20] 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.

[19] A recent work by Bitansky and Brakerski [BB21] 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.

[20] The term "sum-binding" is taken from [Unr16b].

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 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:

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

  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, $Q'_b |0\rangle_{\mathbf{C},\mathbf{R}} |0\rangle_{\mathbf{D}}$ one can first prepare $|0\rangle_{\mathbf{C},\mathbf{R}} (|0\rangle + (-1)^b |1\rangle)_{\mathbf{D}}$ 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 [AAS20] 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 $Q'_b |0\rangle_{\mathbf{C},\mathbf{R}} |0\rangle_{\mathbf{D}}$ without touching $\mathbf{R}' = \mathbf{C}$. Then, their theorem with the above observation gives a swapping algorithm that swaps $(Q_0 |0\rangle_{\mathbf{C},\mathbf{R}}) |0\rangle_{\mathbf{D}}$ and $(Q_1 |0\rangle_{\mathbf{C},\mathbf{R}}) |1\rangle_{\mathbf{D}}$ 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 $Q'_0 |0\rangle_{\mathbf{C}',\mathbf{R}'}$ and $Q'_1 |0\rangle_{\mathbf{C}',\mathbf{R}'}$ needed for [AAS20]. For example, suppose that we have a unitary U such that $UQ'_0 |0\rangle_{\mathbf{C}',\mathbf{R}'} = Q'_1 |0\rangle_{\mathbf{C}',\mathbf{R}'}$ and $UQ'_1 |0\rangle_{\mathbf{C}',\mathbf{R}'} = -Q'_0 |0\rangle_{\mathbf{C}',\mathbf{R}'}$. Clearly, this completely breaks the binding property of $\{Q'_0, Q'_1\}$. However, this is not sufficient for applying [AAS20] since $|\langle 0| {Q'_1}^\dagger U Q'_0 |0\rangle + \langle 0| {Q'_0}^\dagger U Q'_1 |0\rangle| = 0$.
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 [AAS20] does not consider any ancilla qubits.

Both issues are already mentioned in [AAS20]. In particular, Item 1 is an essential issue. They prove the existence of a pair of orthogonal states $|\mathrm{Alive}\rangle$ and $|\mathrm{Dead}\rangle$ such that we can map $|\mathrm{Alive}\rangle$ to $|\mathrm{Dead}\rangle$ by an efficient unitary, but $|\langle \mathrm{Dead}| U |\mathrm{Alive}\rangle + \langle \mathrm{Alive}| U |\mathrm{Dead}\rangle| \approx 0$ for all efficient unitaries U [AAS20, 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 [AAS20, Footnote 2].

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.

[21] We only present how Q'_b works on $|0\rangle_{\mathbf{C},\mathbf{R}} |0\rangle_{\mathbf{D}}$ for simplicity. Its definition on general states can be found in Theorem 6.1.

Solution to Item 1. By the result of [AAS20, 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 [AAS20] without ancilla qubits. Nonetheless, they are not a problem for our purpose.

3 Preliminaries

Basic notations. We use λ to mean the security parameter throughout the paper. The dependence on λ is often implicit. For example, we simply write a function $f : \{0,1\}^n \to \{0,1\}^m$ to mean a collection $\{f_\lambda : \{0,1\}^{n(\lambda)} \to \{0,1\}^{m(\lambda)}\}_{\lambda\in\mathbb{N}}$ for some functions $n(\lambda)$ and $m(\lambda)$ etc. For a finite set X, we write $x \leftarrow X$ to mean that we uniformly take x from X. For a (possibly randomized) classical or quantum algorithm $\mathcal{A}$, we write $y \leftarrow \mathcal{A}(x)$ to mean that $\mathcal{A}$ takes x as input and outputs y. For a function $f : X \to Y$ and $y \in Y$, we write $f^{-1}(y)$ to mean the set of all preimages of y, i.e., $f^{-1}(y) := \{x \in X : f(x) = y\}$. We say that a probability distribution is statistically close to another probability distribution if their statistical distance is negligible.

Notations for quantum computations. For simplicity, $|0...0\rangle$ is sometimes written as $|0\rangle$. Quantum registers are denoted by bold fonts, e.g., $\mathbf{A}, \mathbf{B}$ etc. $\mathrm{Tr}_{\mathbf{A}}(\rho_{\mathbf{A},\mathbf{B}})$ is the partial trace over the register $\mathbf{A}$ of the bipartite state $\rho_{\mathbf{A},\mathbf{B}}$. For simplicity, the tensor product $\otimes$ is sometimes omitted: for example, $|\psi\rangle \otimes |\phi\rangle$ is sometimes written as $|\psi\rangle|\phi\rangle$. I is the identity operator on a single qubit. For simplicity, we often write $I^{\otimes m}$ just as I when the dimension is clear from the context. For any two states ρ_1 and ρ_2, $F(\rho_1, \rho_2)$ is the fidelity between them. For a set S of classical strings, we define $|S\rangle := \frac{1}{\sqrt{|S|}} \sum_{x\in S} |x\rangle$.

Computational models. We say that a classical algorithm is probabilistic polynomial time (PPT) if it can be computed by a polynomial-time (classical) probabilistic Turing machine. We say that a quantum algorithm is quantum polynomial time (QPT) if it can be computed by a polynomial-time quantum Turing machine (or equivalently a quantum circuit generated by a polynomial-time Turing machine). We say that a quantum algorithm is non-uniform QPT if it can be computed by a polynomial-size quantum circuits (or polynomial-time quantum Turing machine) with quantum advice. We use non-uniform QPT algorithms as a default model of adversaries unless otherwise noted.

We say that a sequence $\{U_\lambda\}_{\lambda\in\mathbb{N}}$ of unitary operators is polynomial-time computable if there is a polynomial-time Turing machine that on input 1^λ outputs a description of a quantum circuit that computes U_λ. We often omit the dependence on λ and simply write U is polynomial-time computable to mean the above.

Distinguishing advantage. For a quantum algorithm $\mathcal{A}$ and quantum states $|\psi\rangle$ and $|\phi\rangle$, we say that $\mathcal{A}$ distinguishes $|\psi\rangle$ and $|\phi\rangle$ with advantage Δ if

$$|\Pr[\mathcal{A}(|\phi\rangle) = 1] - \Pr[\mathcal{A}(|\psi\rangle) = 1]| = \Delta.$$

3.1 Basic Cryptographic Primitives

Definition 3.1 (One-way functions). *We say that a classical polynomial-time computable function $f : \{0,1\}^n \to \{0,1\}^m$ is a* one-way function (OWF) *if for any non-uniform QPT adversary $\mathcal{A}$, we have*

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

We say that a one-way function f is an injective *one-way function if f is injective, and that a one-way function f is a one-way* permutation *if f is a permutation.*

[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 3.2 (Keyed one-way functions). *We say that a family $\{f_k : \{0,1\}^n \to \{0,1\}^m\}_{k\in\mathcal{K}}$ of classical polynomial-time computable functions is a* keyed *one-way function if for any non-uniform QPT adversary $\mathcal{A}$, we have*

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

We say that a keyed one-way fucntion $\{f_k : \{0,1\}^n \to \{0,1\}^m\}_{k\in\mathcal{K}}$ is a keyed injective *one-way function if f_k is injective for all $k \in \mathcal{K}$.*

Definition 3.3 (Pseudorandom generators). *We say that a classical polynomial-time computable function $G : \{0,1\}^n \to \{0,1\}^m$ is a* pseudorandom generator (PRG) *if $m > n$ and for any non-uniform QPT adversary $\mathcal{A}$, we have*

$$|\Pr[\mathcal{A}(y) = 1 : y \leftarrow \{0,1\}^m] - \Pr[\mathcal{A}(G(x)) = 1 : x \leftarrow \{0,1\}^n]| = \mathsf{negl}(\lambda).$$

It is well-known that PRGs exist if and only if OWFs exist [HILL99].

Definition 3.4 (Collapsing functions [Unr16b]). *For a polynomial-time computable function family $\mathcal{H} = \{H_k : \{0,1\}^L \to \{0,1\}^\ell\}_{k\in\mathcal{K}_\mathcal{H}}$ and an adversary $\mathcal{A}$, we define an experiment $\mathsf{Exp}^{\mathsf{collapse}}_\mathcal{A}(1^\lambda)$ as follows:*

1. *The challenger generates $k \leftarrow \mathcal{K}_\mathcal{H}$.*
2. *$\mathcal{A}$ is given k as input and generates a hash value $y \in \{0,1\}^\ell$ and a quantum state σ over registers $(\mathbf{X}, \mathbf{A})$ where $\mathbf{X}$ stores an element of $\{0,1\}^L$ and $\mathbf{A}$ is $\mathcal{A}$'s internal register. Then it sends y and register $\mathbf{X}$ to the challenger, and keeps $\mathbf{A}$ on its side.*
3. *The challenger picks $b \leftarrow \{0,1\}$. If $b = 0$, the challenger does nothing and if $b = 1$, the challenger measures register $\mathbf{X}$ in the computational basis. The challenger returns register $\mathbf{X}$ to $\mathcal{A}$.*
4. *$\mathcal{A}$ outputs a bit b'. The experiment outputs 1 if $b' = b$ and 0 otherwise.*

We say that $\mathcal{A}$ is a valid adversary if the following is satisfied: if we measure the state in $\mathbf{X}$ right after Step 2, then the outcome x satisfies $H_k(x) = y$ with probability 1.

We say that $\mathcal{H}$ is collapsing *if for any non-uniform QPT valid adversary $\mathcal{A}$, we have*

$$|\Pr[1 \leftarrow \mathsf{Exp}^{\mathsf{collapse}}_\mathcal{A}(1^\lambda)] - 1/2| = \mathsf{negl}(\lambda).$$

As shown in [Unr16b], the collapsing property implies the collision-resistance. That is, if $\mathcal{H} = \{H_k : \{0,1\}^L \to \{0,1\}^\ell\}_{k\in\mathcal{K}_\mathcal{H}}$ is collapsing, then it is also collision-resistant, i.e., no non-uniform QPT adversary can find $x \neq x'$ such that $H_k(x) = H_k(x')$ with non-negligible probability given $k \leftarrow \mathcal{K}_\mathcal{H}$. It is clear that injective functions are collapsing.

Unruh [Unr16a] showed that there is a collapsing function family with arbitrarily long (or even unbounded) input-length under the LWE assumption (or more generally, under the existence of lossy functions in a certain parameter regime).

Definition 3.5 (Single-copy-secure PRSGs [MY22]). *A* single-copy-secure pseudorandom quantum states generator (PRSG) *is a QPT algorithm* $\mathsf{StateGen}$ *that, on input $k \in \{0,1\}^n$, outputs an m-qubit quantum state $|\phi_k\rangle$. As the security, we require the following: for any non-uniform QPT adversary $\mathcal{A}$,*

$$|\Pr_{k\leftarrow\{0,1\}^n}[\mathcal{A}(|\phi_k\rangle) \to 1] - \Pr_{|\psi\rangle\leftarrow\mu_m}[\mathcal{A}(|\psi\rangle) \to 1]| = \mathsf{negl}(\lambda),$$

where μ_m is the Haar measure on m-qubit states.[23]

[23] Intuitively, $|\psi\rangle \leftarrow \mu_m$ means that an m-qubit pure state is sampled uniformly at random from the set of all m-qubit pure states.

Single-copy-secure PRSGs are a restricted version of (poly-copy-secure) PRSGs introduced in [JLS18], where any polynomially many copies of $|\phi_k\rangle$ are computationally indistnguishable from the same number of copies of Haar random states. If one-way functions exist, (poly-copy-secure) PRSGs exist [JLS18]. On the other hand, there is an evidence that (poly-copy-secure) PRSGs do not imply one-way functions [Kre21].

3.2 Canonical Quantum Bit Commitments

We define *canonical* quantum bit commitments as defined in [Yan22].

Definition 3.6 (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 3.7. 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 3.8 (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.*

Definition 3.9 (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 hiding if the LHS is 0 for all unbounded-time unitary U.

3.3 Equivalence between Swapping and Distinguishing

The following theorem was proven in [AAS20].

Theorem 3.10 ([AAS20, 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*

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

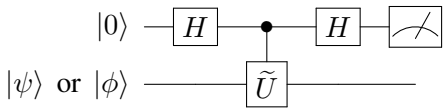

Figure 1: Quantum circuit for $\mathcal{A}$ in Item 1 of Theorem 3.10.

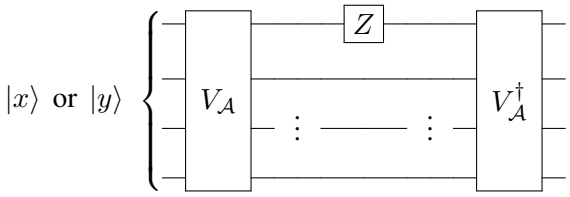

Figure 2: Quantum circuit for U in Item 2 of Theorem 3.10.

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 3.11 (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 [AAS20].

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.

Remark 3.12. Though the final requirement in both items ("Moreover,...") is not explicitly stated in [AAS20, 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 Section 4.1, we introduce a notion of swap-trapdoor function pairs, which can be seen as a variant of trapdoor claw-free function pairs [GMR84]. In Section 4.2, we define quantum-ciphertext PKE and construct it based on STFs. In Section 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 4.1 (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 4.2 (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 Section 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 4.3 (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 4.4 (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 4.5 (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 (Definition 3.4).[24]

Lemma 4.6 (Claw-free and collapsing $\to$ Conversion hard). *If f_0 is collapsing, then claw-freeness implies conversion hardness.*

Proof. Suppose that $(\mathsf{Setup}, \mathsf{Eval}, \mathsf{Swap})$ does not satisfy conversion hardness. Then, there is a non-uniform QPT adversary $\mathcal{A}$ such that

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

is non-negligible. By the assumption that f_0 is collapsing, we can show that

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

Combining the above,

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

is non-negligible.

Then, we use $\mathcal{A}$ to construct a non-uniform QPT adversary $\mathcal{B}$ that breaks claw-freeness as follows.

$\mathcal{B}(\mathsf{pp})$**:** Pick $x_0 \leftarrow \mathcal{X}$, run $x_1 \leftarrow \mathcal{A}(\mathsf{pp}, x_0)$, and output (x_0, x_1).

Then, $\mathcal{B}$ breaks claw-freeness. □

As a special case of Lemma 4.6, 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 [Zha19]. We roughly show that a claw-free but non-conversion-hard STF can be used to construct one-shot signatures [AGKZ20]. 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. (See Definition A.2 for the formal definition.) 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

[24] Collapsingness of f_0 can be naturally defined according to Definition 3.4 where we ignore f_1 and simply consider pp as a function index for f_0.

signatures [BDS17], the only known construction in the standard model is based on indistinguishability obfuscation [CLLZ21]. 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 Section 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 [Zha19, 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 [Zha19].

Then, the lemma is given below.

Lemma 4.7 (Claw-free and non-conversion hard STF $\to$ 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.*

Proof. (sketch.) We give a proof sketch here. The full proof can be found in Appendix A.

For simplicity, suppose that $(\mathsf{Setup}, \mathsf{Eval}, \mathsf{Swap})$ is claw-free but its conversion hardness is totally broken. That is, we assume that we can efficiently find x_1 such that $f_1(x_1) = y$ given $(\mathsf{pp}, |f_0^{-1}(y)\rangle)$. Our idea is to set pp to be the public parameter of one-shot signatures, $|f_0^{-1}(y)\rangle$ 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 $x_0 \in f_0^{-1}(y)$ and set x_0 to be the signature. For signing to 1, the signer runs the adversary against conversion hardness to get x_1 such that $f_1(x_1) = y$. If one can generate signatures to 0 and 1 simultaneously, we can break claw-freeness since $f_0(x_0) = f_1(x_1) = y$. Thus, the above one-shot signature is secure if $(\mathsf{Setup}, \mathsf{Eval}, \mathsf{Swap})$ is claw-free.

In the actual proof, we only assume an adversary that finds x_1 with a non-negligible (or noticeable) probability rather than 1. Then, our idea is to simply repeat the above construction parallelly many times so that at least one of the execution of the adversary succeeds with overwhelming probability.

We need to assume that the adversary is uniform since that is used as part of the signing algorithm. The "infinitely-often" restriction comes from the fact that an inverse of non-negligible function may not be polynomial. □

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

A lattice-based instantiation is also possible if we relax the requirements to allow some "noises" similarly to [BCM+18]. The noisy version is sufficient for our construction of quantum-ciphertext PKE given in Section 4.2. However, since lattice-based (classical) PKE schemes are already known [Reg09, GPV08], 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 [BJ15], 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 4.8 (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.

$\mathsf{Enc}(\mathsf{pk}, b) \to ct$**:** *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.

$\mathsf{Dec}(\mathsf{sk}, ct) \to b'/\bot$**:** *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*

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

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

Definition 4.9 (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*

$$|\Pr[\mathcal{A}(\mathsf{pk}, ct_0) = 1] - \Pr[\mathcal{A}(\mathsf{pk}, ct_1) = 1]| = \mathsf{negl}(\lambda),$$

where $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda)$*,* $ct_0 \leftarrow \mathsf{Enc}(\mathsf{pk}, 0)$*, and* $ct_1 \leftarrow \mathsf{Enc}(\mathsf{pk}, 1)$.

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 $\mathsf{pk} := \mathsf{pp}$ and $\mathsf{sk} := \mathsf{td}$.

$\mathsf{Enc}(\mathsf{pk}, b \in \{0,1\})$**:** 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:[25]

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

The above state is set to be ct.[26]

$\mathsf{Dec}(\mathsf{sk}, ct)$**:** Parse $\mathsf{sk} = \mathsf{td}$. Let U_{td} be a unitary over $\mathbf{D}$ and $\mathbf{X}$ such that[27]

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

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 4.10. $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ *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

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

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

Proof. First, we remark that the IND-CPA security is identical to computational indistinguishability of the following two states $|\psi_0\rangle$ and $|\psi_1\rangle$ against any non-uniform QPT distinguisher $\mathcal{A}$ that does not act on $(\mathbf{Y}, \mathbf{P}')$:

$$|\psi_b\rangle := \sum_{\mathsf{pp}} \sqrt{D(\mathsf{pp})} |\mathsf{pp}\rangle_{\mathbf{P}} |\mathsf{pp}\rangle_{\mathbf{P}'} \sum_{x \in \mathcal{X}} \frac{1}{\sqrt{2|\mathcal{X}|}}(|0\rangle_{\mathbf{D}} |x\rangle_{\mathbf{X}} |f_0(x)\rangle_{\mathbf{Y}} + (-1)^b |1\rangle_{\mathbf{D}} |x\rangle_{\mathbf{X}} |f_1(x)\rangle_{\mathbf{Y}})$$

where $D(\mathsf{pp}) := \Pr[\mathsf{pp}' = \mathsf{pp} : (\mathsf{pp}', \mathsf{td}') \leftarrow \mathsf{Setup}(1^\lambda)]$.

[25] Note that the swapping correctness implies that $|f_0^{-1}(y)| = |f_1^{-1}(y)|$ for any $y \in \mathcal{Y}$.

[26] Remark that one does not need to include y in the ciphertext.

[27] Note that the second operation is possible because $\mathsf{Swap}(\mathsf{td}, 0, \mathsf{Swap}(\mathsf{td}, 1, x)) = x$.

Suppose that there is a non-uniform QPT distinguisher $\mathcal{A}$ with an advice $|\tau\rangle_{\mathbf{Z}}$ that does not act on $(\mathbf{Y}, \mathbf{P}')$ and distinguishes $|\psi_0\rangle$ and $|\psi_1\rangle$ with a non-negligible advantage Δ.

Since $|\psi_0\rangle$ and $|\psi_1\rangle$ are orthogonal, by Item 2 of Theorem 3.10, there exists a polynomial-time computable unitary U over $(\mathbf{P}, \mathbf{D}, \mathbf{X}, \mathbf{Z})$ such that[28]

$$\frac{1}{2}\left|\begin{array}{l}\langle\psi_1'|_{\mathbf{P},\mathbf{P}',\mathbf{D},\mathbf{X},\mathbf{Y}}\langle\tau|_{\mathbf{Z}}(U_{\mathbf{P},\mathbf{D},\mathbf{X},\mathbf{Z}}\otimes I_{\mathbf{P}',\mathbf{Y}})|\psi_0'\rangle_{\mathbf{P},\mathbf{P}',\mathbf{D},\mathbf{X},\mathbf{Y}}|\tau\rangle_{\mathbf{Z}} \\ +\langle\psi_0'|_{\mathbf{P},\mathbf{P}',\mathbf{D},\mathbf{X},\mathbf{Y}}\langle\tau|_{\mathbf{Z}}(U_{\mathbf{P},\mathbf{D},\mathbf{X},\mathbf{Z}}\otimes I_{\mathbf{P}',\mathbf{Y}})|\psi_1'\rangle_{\mathbf{P},\mathbf{P}',\mathbf{D},\mathbf{X},\mathbf{Y}}|\tau\rangle_{\mathbf{Z}}\end{array}\right| = \Delta$$

where

$$|\psi_b'\rangle = \frac{|\psi_0\rangle + (-1)^b|\psi_1\rangle}{\sqrt{2}} = \sum_{\mathsf{pp}}\sqrt{\frac{D(\mathsf{pp})}{|\mathcal{X}|}}|\mathsf{pp}\rangle_{\mathbf{P}}|\mathsf{pp}\rangle_{\mathbf{P}'}\sum_{x\in\mathcal{X}}|b\rangle_{\mathbf{D}}|x\rangle_{\mathbf{X}}|f_b(x)\rangle_{\mathbf{Y}}. \tag{3}$$

In the following, we simply write U to mean $U_{\mathbf{P},\mathbf{D},\mathbf{X},\mathbf{Z}}$ for notational simplicity. Thus, we must have

$$|\langle\psi_1'|_{\mathbf{P},\mathbf{P}',\mathbf{D},\mathbf{X},\mathbf{Y}}\langle\tau|_{\mathbf{Z}}(U\otimes I_{\mathbf{P}',\mathbf{Y}})|\psi_0'\rangle_{\mathbf{P},\mathbf{P}',\mathbf{D},\mathbf{X},\mathbf{Y}}|\tau\rangle_{\mathbf{Z}}| \geq \Delta \tag{4}$$

or

$$|\langle\psi_0'|_{\mathbf{P},\mathbf{P}',\mathbf{D},\mathbf{X},\mathbf{Y}}\langle\tau|_{\mathbf{Z}}(U\otimes I_{\mathbf{P}',\mathbf{Y}})|\psi_1'\rangle_{\mathbf{P},\mathbf{P}',\mathbf{D},\mathbf{X},\mathbf{Y}}|\tau\rangle_{\mathbf{Z}}| \geq \Delta. \tag{5}$$

Without loss of the generality, we assume that the former inequality holds. Then we show that this contradicts conversion hardness of $(\mathsf{Setup}, \mathsf{Eval}, \mathsf{Swap})$. We construct a non-uniform QPT adversary $\mathcal{B}$ that takes $|\tau\rangle$ as an advice and breaks the conversion hardness (Definition 4.4) of $(\mathsf{Setup}, \mathsf{Eval}, \mathsf{Swap})$ as follows.

$\mathcal{B}\left((\mathsf{pp}, |f_0^{-1}(y)\rangle_{\mathbf{X}}); |\tau\rangle_{\mathbf{Z}}\right)$**:** On input $(\mathsf{pp}, |f_0^{-1}(y)\rangle_{\mathbf{X}})$ and a quantum advice $|\tau\rangle_{\mathbf{Z}}$, prepare a single qubit register $\mathbf{D}$ that is initialized to be $|0\rangle_{\mathbf{D}}$, apply U on $|\mathsf{pp}\rangle_{\mathbf{P}}|0\rangle_{\mathbf{D}}|f_0^{-1}(y)\rangle_{\mathbf{X}}|\tau\rangle_{\mathbf{Z}}$, measure $\mathbf{X}$ to obtain an outcome x', and output x'.

[28] For applying Item 2 of Theorem 3.10, we assume that $\mathcal{A}$ does not use an additional ancilla qubits besides $|\tau\rangle_{\mathbf{Z}}$ w.l.o.g. (Sufficiently many qubits that are initialized to be $|0\rangle$ could be included in $|\tau\rangle_{\mathbf{Z}}$.)

For any pp, we have

$$\begin{aligned}
&\Pr\left[f_1(x')=y : x\leftarrow\mathcal{X}, y:=f_0(x), x'\leftarrow\mathcal{B}\left((\mathsf{pp},|f_0^{-1}(y)\rangle_{\mathbf{X}});|\tau\rangle_{\mathbf{Z}}\right)\right]\\
&=\sum_{\substack{y\in\mathcal{Y}\\ x'\in f_1^{-1}(y)}}\frac{|f_0^{-1}(y)|}{|\mathcal{X}|}\left\|\langle x'|_{\mathbf{X}}U|\mathsf{pp}\rangle_{\mathbf{P}}|0\rangle_{\mathbf{D}}|f_0^{-1}(y)\rangle_{\mathbf{X}}|\tau\rangle_{\mathbf{Z}}\right\|^2 &(6)\\
&\geq\frac{1}{|\mathcal{X}|}\left(\sum_{\substack{y\in\mathcal{Y}\\ x'\in f_1^{-1}(y)}}\sqrt{\frac{|f_0^{-1}(y)|}{|\mathcal{X}|}}\left\|\langle x'|_{\mathbf{X}}U|\mathsf{pp}\rangle_{\mathbf{P}}|0\rangle_{\mathbf{D}}|f_0^{-1}(y)\rangle_{\mathbf{X}}|\tau\rangle_{\mathbf{Z}}\right\|\right)^2 &(7)\\
&\geq\frac{1}{|\mathcal{X}|^2}\left\|\sum_{\substack{y\in\mathcal{Y}\\ x'\in f_1^{-1}(y)}}\sqrt{|f_0^{-1}(y)|}\,\langle x'|_{\mathbf{X}}U|\mathsf{pp}\rangle_{\mathbf{P}}|0\rangle_{\mathbf{D}}|f_0^{-1}(y)\rangle_{\mathbf{X}}|\tau\rangle_{\mathbf{Z}}\right\|^2 &(8)\\
&\geq\frac{1}{|\mathcal{X}|^2}\left|\sum_{\substack{y\in\mathcal{Y}\\ x\in f_0^{-1}(y)\\ x'\in f_1^{-1}(y)}}\langle\mathsf{pp}|_{\mathbf{P}}\langle 1|_{\mathbf{D}}\langle x'|_{\mathbf{X}}\langle\tau|_{\mathbf{Z}}U|\mathsf{pp}\rangle_{\mathbf{P}}|0\rangle_{\mathbf{D}}|x\rangle_{\mathbf{X}}|\tau\rangle_{\mathbf{Z}}\right|^2 &(9)\\
&=\frac{1}{|\mathcal{X}|^2}\left|\begin{array}{l}\left(\sum_{x'\in\mathcal{X}}\langle\mathsf{pp}|_{\mathbf{P}}\langle\mathsf{pp}|_{\mathbf{P}'}\langle 1|_{\mathbf{D}}\langle x'|_{\mathbf{X}}\langle f_1(x')|_{\mathbf{Y}}\langle\tau|_{\mathbf{Z}}\right)\\ (U\otimes I_{\mathbf{P}',\mathbf{Y}})\left(\sum_{x\in\mathcal{X}}|\mathsf{pp}\rangle_{\mathbf{P}}|\mathsf{pp}\rangle_{\mathbf{P}'}|0\rangle_{\mathbf{D}}|x\rangle_{\mathbf{X}}|f_0(x)\rangle_{\mathbf{Y}}|\tau\rangle_{\mathbf{Z}}\right)\end{array}\right|^2, &(10)
\end{aligned}$$

where Equation (6) follows from the definition of $\mathcal{B}$, Equation (7) follows from Cauchy–Schwarz inequality and $\sum_{y\in\mathcal{Y}}|f_1^{-1}(y)|=|\mathcal{X}|$, Equation (8) follows from the triangle inequality, and Equation (9) follows from the definition $|f_0^{-1}(y)\rangle=\frac{1}{|f_0^{-1}(y)|^{1/2}}\sum_{x\in f_0^{-1}(y)}|x\rangle$ and the fact that inserting $\langle\mathsf{pp}|_{\mathbf{P}}\langle 1|_{\mathbf{D}}\langle\tau|_{\mathbf{Z}}$ can only decrease the norm.

Therefore, we have

$$\begin{aligned}
&\Pr[f_1(x')=y : (\mathsf{pp},\mathsf{td})\leftarrow\mathsf{Setup}(1^\lambda), x\leftarrow\mathcal{X}, y:=f_0(x), x'\leftarrow\mathcal{B}((\mathsf{pp},|f_0^{-1}(y)\rangle_{\mathbf{X}});|\tau\rangle_{\mathbf{Z}})]\\
&=\sum_{\mathsf{pp}}D(\mathsf{pp})\left[\Pr[f_1(x')=y : x\leftarrow\mathcal{X}, y:=f_0(x), x'\leftarrow\mathcal{B}((\mathsf{pp},|f_0^{-1}(y)\rangle_{\mathbf{X}});|\tau\rangle_{\mathbf{Z}})]\right]\\
&\geq\sum_{\mathsf{pp}}\frac{D(\mathsf{pp})}{|\mathcal{X}|^2}\left|\begin{array}{l}\left(\sum_{x'\in\mathcal{X}}\langle\mathsf{pp}|_{\mathbf{P}}\langle\mathsf{pp}|_{\mathbf{P}'}\langle 1|_{\mathbf{D}}\langle x'|_{\mathbf{X}}\langle f_1(x')|_{\mathbf{Y}}\langle\tau|_{\mathbf{Z}}\right)\\ (U\otimes I_{\mathbf{P}',\mathbf{Y}})\left(\sum_{x\in\mathcal{X}}|\mathsf{pp}\rangle_{\mathbf{P}}|\mathsf{pp}\rangle_{\mathbf{P}'}|0\rangle_{\mathbf{D}}|x\rangle_{\mathbf{X}}|f_0(x)\rangle_{\mathbf{Y}}|\tau\rangle_{\mathbf{Z}}\right)\end{array}\right|^2\\
&\geq\left|\sum_{\mathsf{pp}}\frac{D(\mathsf{pp})}{|\mathcal{X}|}\left(\begin{array}{l}\left(\sum_{x'\in\mathcal{X}}\langle\mathsf{pp}|_{\mathbf{P}}\langle\mathsf{pp}|_{\mathbf{P}'}\langle 1|_{\mathbf{D}}\langle x'|_{\mathbf{X}}\langle f_1(x')|_{\mathbf{Y}}\langle\tau|_{\mathbf{Z}}\right)\\ (U\otimes I_{\mathbf{P}',\mathbf{Y}})\left(\sum_{x\in\mathcal{X}}|\mathsf{pp}\rangle_{\mathbf{P}}|\mathsf{pp}\rangle_{\mathbf{P}'}|0\rangle_{\mathbf{D}}|x\rangle_{\mathbf{X}}|f_0(x)\rangle_{\mathbf{Y}}|\tau\rangle_{\mathbf{Z}}\right)\end{array}\right)\right|^2\\
&=\left|\langle\psi_1'|_{\mathbf{P},\mathbf{P}',\mathbf{D},\mathbf{X},\mathbf{Y}}\langle\tau|_{\mathbf{Z}}(U\otimes I_{\mathbf{P}',\mathbf{Y}})|\psi_0'\rangle_{\mathbf{P},\mathbf{P}',\mathbf{D},\mathbf{X},\mathbf{Y}}|\tau\rangle_{\mathbf{Z}}\right|^2,
\end{aligned}$$

where the first inequality follows from Equation (10), the second inequality follows from Jensen's inequality, and the final equality follows from Equation (3).

This is non-negligible by our assumption. Therefore, $\mathcal{B}$ breaks the conversion hardness of $(\mathsf{Setup},\mathsf{Eval},\mathsf{Swap})$, which is a contradiction. Thus, $(\mathsf{KeyGen},\mathsf{Enc},\mathsf{Dec})$ is IND-CPA secure. □

.

4.3 Instantiation from Group Actions

We review basic definitions about cryptographic group actions and their one-wayness and pseudorandomness following [JQSY19]. Then, we construct a STF based on it.

Basic definitions.

Definition 4.12 (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 [JQSY19].

Definition 4.13 (Group actions with efficient algorithms). *We say that a group action $(G, S, \star)$ has* efficient algorithms *if it satisfies the following:*[29]

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 $s \in S$.*

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 4.14 (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 [JQSY19] except for the "superposition over G" property. We remark that all candidate constructions proposed in [JQSY19] satisfy this property as explained later.

Assumptions. We define one-wayness and pseudorandomness following [JQSY19].

[29] 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.

Definition 4.15 (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 4.16 (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*

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

Remark 4.17 (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 4.18 (Pseudorandom $\rightarrow$ One-way). We remark that the pseudorandomness immediately implies the one-wayness as noted in [JQSY19].

Instantiations. Ji et al. [JQSY19] 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 [JQSY19] 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 4.13, 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 4.13). 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 4.19. *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.*

Proof.

Proof of Item 1. Suppose that $(\mathsf{Setup}, \mathsf{Eval}, \mathsf{Swap})$ is not claw-free. Then there is a non-uniform QPT adversary $\mathcal{A}$ such that

$$\Pr[f_0(h_0) = f_1(h_1) : (\mathsf{pp}, \mathsf{td}) \leftarrow \mathsf{Setup}(1^\lambda), (h_0, h_1) \leftarrow \mathcal{A}(\mathsf{pp})]$$

is non-negligible. We use $\mathcal{A}$ to construct a non-uniform QPT adversary $\mathcal{B}$ that breaks one-wayness of $(G, S, \star)$ as follows:

$\mathcal{B}(s_0, s_1)$**:** Set $\mathsf{pp} := (s_0, s_1)$, run $(h_0, h_1) \leftarrow \mathcal{A}(\mathsf{pp})$, and outputs $h_1^{-1}h_0$.

By the assumption, we have $f_0(h_0) = f_1(h_1)$ with a non-negligible probability. By the definition of f_0 and f_1, $f_0(h_0) = f_1(h_1)$ is equivalent to $h_0 \star s_0 = h_1 \star s_1$, which means $h_1^{-1}h_0 \star s_0 = s_1$. Since this occurs with a non-negligible probability $\mathcal{B}$ breaks one-wayness of $(G, S, \star)$. Thus, $(\mathsf{Setup}, \mathsf{Eval}, \mathsf{Swap})$ is claw-free.

Proof of Item 2. Suppose that $(\mathsf{Setup}, \mathsf{Eval}, \mathsf{Swap})$ is not conversion hard. Then there is a non-uniform QPT algorithm $\mathcal{A}$ such that

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

is non-negligible. This is equivalent to that

$$\Pr\left[h_0 \star s_0 = h_1 \star s_1 : \begin{array}{l} s_0 \leftarrow S, g, h_0 \leftarrow G, \\ s_1 := g \star s_0, y := h_0 \star s_0, \\ h_1 \leftarrow \mathcal{A}(s_0, s_1, |f_0^{-1}(y)\rangle) \end{array}\right]$$

is non-negligible. On the other hand, by Item 1 of Definition 4.16, we have

$$\Pr\left[h_0 \star s_0 = h_1 \star s_1 : \begin{array}{l} s_0, s_1 \leftarrow S, h_0 \leftarrow G, \\ y := h_0 \star s_0, \\ h_1 \leftarrow \mathcal{A}(s_0, s_1, |f_0^{-1}(y)\rangle) \end{array}\right] = \mathsf{negl}(\lambda).$$

Therefore,

$$\left| \Pr\left[h_0 \star s_0 = h_1 \star s_1 : \begin{array}{l} s_0 \leftarrow S, g, h_0 \leftarrow G, \\ s_1 := g \star s_0, y := h_0 \star s_0, \\ h_1 \leftarrow \mathcal{A}(s_0, s_1, |f_0^{-1}(y)\rangle) \end{array}\right] - \Pr\left[h_0 \star s_0 = h_1 \star s_1 : \begin{array}{l} s_0, s_1 \leftarrow S, h_0 \leftarrow G, \\ y := h_0 \star s_0, \\ h_1 \leftarrow \mathcal{A}(s_0, s_1, |f_0^{-1}(y)\rangle) \end{array}\right] \right| \tag{11}$$

is non-negligible.

Then, we construct the following non-uniform QPT adversary $\mathcal{B}$ that breaks pseudorandomness of $(G, S, \star)$:

$\mathcal{B}(s_0, s_1)$**:** Generate a state $\frac{1}{\sqrt{|G|}}\sum_{h_0\in G}|h_0\rangle|h_0 \star s_0\rangle$ and measure the second register to get $y \in S$. Then, the first register collapses to $|f_0^{-1}(y)\rangle$. Run $h_1 \leftarrow \mathcal{A}(s_0, s_1, |f_0^{-1}(y)\rangle)$. Output 1 if $h_1 \star s_1 = y$ and otherwise 0.

We can see that $\mathcal{B}$'s advantage to distinguish the two cases ($s_0 \leftarrow S$, $g \leftarrow G$, $s_1 := g \star s_0$ or $s_0, s_1 \leftarrow S$) is exactly Equation (11), which is non-negligible. This contradicts pseudorandomness of $(G, S, \star)$ (Item 2 of Definition 4.16). Thus, $(\mathsf{Setup}, \mathsf{Eval}, \mathsf{Swap})$ is conversion hard. □

Quantum-ciphertext PKE from group actions. Recall that conversion hard STFs suffice for constructing IND-CPA secure quantum ciphertext PKE (Theorem 4.11). Then, by Lemmata 4.6 and 4.7 and Theorem 4.19, we obtain the following corollaries.

Corollary 4.20. *If there exists a pseudorandom group action with efficient algorithms, there exists an IND-CPA secure quantum-ciphertext PKE.*

Remark 4.21 (Lossy encryption). Actually, we can show that the quantum-ciphertext PKE constructed from a pseudorandom group action is lossy encryption [BHY09], which is stronger than IND-CPA secure one. We omit the detail since our focus is on constructing IND-CPA secure schemes.

Corollary 4.22. *If there exists a one-way group action with efficient algorithms such that f_0 is collapsing,*[30] *there exists a uniform IND-CPA secure quantum-ciphertext PKE scheme.*

Corollary 4.23. *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.*[31]

5 Equivalence between Swapping and Distinguishing with Auxiliary States

For our application to conversion for commitments, we need a generalization of Theorem 3.10 that considers auxiliary quantum states. While it is straightforward to generalize Item 2 to such a setting,[32] 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 $|y\rangle$.[33] Intuitively, we overcome this issue by "uncomputing" the auxiliary state in a certain sense.

Theorem 5.1 (Generalization of Theorem 3.10 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*

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

[30] We currently have no candidate of such a one-way group action.

[31] The uniform IND-CPA security is defined similarly to the IND-CPA security in Definition 4.9 except that the adversary is restricted to be *uniform* QPT.

[32] Indeed, such a generalization of Item 2 is already implicitly used in the proof of Theorem 4.11.

[33] This is also observed in [AAS20, Footnote 2].

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, 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 5.2. 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 3.10 is shown to be tight in [AAS20].

Proof of Theorem 5.1. Item 2 directly follows from Item 2 of Theorem 3.10 by considering $|x\rangle|\tau\rangle$ and $|y\rangle|\tau\rangle$ as $|x\rangle$ and $|y\rangle$ in Theorem 3.10. 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:

$$\widetilde{U} := X_{\mathbf{B}} U^{\dagger}_{\mathbf{A}',\mathbf{Z}} U_{\mathbf{A},\mathbf{Z}} \tag{12}$$

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 5.3. Let $|x\rangle, |y\rangle, |\tau\rangle$, and Γ be as in Item 1 of Theorem 5.1, $\widetilde{U}$ be as defined in Equation (12), and $|\sigma\rangle_{\mathbf{A}',\mathbf{B}}$ be the state over $(\mathbf{A}', \mathbf{B})$ defined as follows:

$$|\sigma\rangle_{\mathbf{A}',\mathbf{B}} := \frac{|x\rangle_{\mathbf{A}'}|0\rangle_{\mathbf{B}} + |y\rangle_{\mathbf{A}'}|1\rangle_{\mathbf{B}}}{\sqrt{2}}. \tag{13}$$

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 5.3 is correct. By Item 1 of Theorem 3.10, Claim 5.3 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 5.3.

Proof of Claim 5.3. 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

$$\Gamma = \left\| |\tau'_{xy}\rangle_{\mathbf{Z}} + |\tau'_{yx}\rangle_{\mathbf{Z}} \right\| \tag{14}$$

and

$$U_{\mathbf{A},\mathbf{Z}} |x\rangle_{\mathbf{A}} |\tau\rangle_{\mathbf{Z}} = |x\rangle_{\mathbf{A}} |\tau'_{xx}\rangle_{\mathbf{Z}} + |y\rangle_{\mathbf{A}} |\tau'_{xy}\rangle_{\mathbf{Z}} + |\mathrm{garbage}_x\rangle_{\mathbf{A},\mathbf{Z}} \tag{15}$$
$$U_{\mathbf{A},\mathbf{Z}} |y\rangle_{\mathbf{A}} |\tau\rangle_{\mathbf{Z}} = |x\rangle_{\mathbf{A}} |\tau'_{yx}\rangle_{\mathbf{Z}} + |y\rangle_{\mathbf{A}} |\tau'_{yy}\rangle_{\mathbf{Z}} + |\mathrm{garbage}_y\rangle_{\mathbf{A},\mathbf{Z}} \tag{16}$$

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

$$(\langle x|_{\mathbf{A}} \otimes I_{\mathbf{Z}}) |\mathrm{garbage}_x\rangle_{\mathbf{A},\mathbf{Z}} = (\langle y|_{\mathbf{A}} \otimes I_{\mathbf{Z}}) |\mathrm{garbage}_x\rangle_{\mathbf{A},\mathbf{Z}} = 0, \tag{17}$$
$$(\langle x|_{\mathbf{A}} \otimes I_{\mathbf{Z}}) |\mathrm{garbage}_y\rangle_{\mathbf{A},\mathbf{Z}} = (\langle y|_{\mathbf{A}} \otimes I_{\mathbf{Z}}) |\mathrm{garbage}_y\rangle_{\mathbf{A},\mathbf{Z}} = 0. \tag{18}$$

Then,

$$\begin{aligned} &\langle y|_{\mathbf{A}} \langle \tau|_{\mathbf{Z}} \langle \sigma|_{\mathbf{A}',\mathbf{B}} \widetilde{U} |x\rangle_{\mathbf{A}} |\tau\rangle_{\mathbf{Z}} |\sigma\rangle_{\mathbf{A}',\mathbf{B}} \\ =& \langle y|_{\mathbf{A}} \langle \tau|_{\mathbf{Z}} \langle \sigma|_{\mathbf{A}',\mathbf{B}} X_{\mathbf{B}} U^\dagger_{\mathbf{A}',\mathbf{Z}} (|x\rangle_{\mathbf{A}} |\tau'_{xx}\rangle_{\mathbf{Z}} + |y\rangle_{\mathbf{A}} |\tau'_{xy}\rangle_{\mathbf{Z}} + |\mathrm{garbage}_x\rangle_{\mathbf{A},\mathbf{Z}}) |\sigma\rangle_{\mathbf{A}',\mathbf{B}} \\ =& \langle \tau|_{\mathbf{Z}} \langle \sigma|_{\mathbf{A}',\mathbf{B}} X_{\mathbf{B}} U^\dagger_{\mathbf{A}',\mathbf{Z}} |\tau'_{xy}\rangle_{\mathbf{Z}} |\sigma\rangle_{\mathbf{A}',\mathbf{B}} \end{aligned} \tag{19}$$

where the first equality follows from Equation (15) and the second equality follows from Equation (17) and the assumption that $|x\rangle$ and $|y\rangle$ are orthogonal. By Equations (13), (15) and (16), it holds that

$$\begin{aligned} &U_{\mathbf{A}',\mathbf{Z}} X_{\mathbf{B}} |\tau\rangle_{\mathbf{Z}} |\sigma\rangle_{\mathbf{A}',\mathbf{B}} \\ =& U_{\mathbf{A}',\mathbf{Z}} \frac{|\tau\rangle_{\mathbf{Z}} (|x\rangle_{\mathbf{A}'} |1\rangle_{\mathbf{B}} + |y\rangle_{\mathbf{A}'} |0\rangle_{\mathbf{B}})}{\sqrt{2}} \\ =& \frac{1}{\sqrt{2}} \left(\begin{array}{l} \left(|x\rangle_{\mathbf{A}'} |\tau'_{xx}\rangle_{\mathbf{Z}} + |y\rangle_{\mathbf{A}'} |\tau'_{xy}\rangle_{\mathbf{Z}} + |\mathrm{garbage}_x\rangle_{\mathbf{A}',\mathbf{Z}}\right) |1\rangle_{\mathbf{B}} \\ + \left(|x\rangle_{\mathbf{A}'} |\tau'_{yx}\rangle_{\mathbf{Z}} + |y\rangle_{\mathbf{A}'} |\tau'_{yy}\rangle_{\mathbf{Z}} + |\mathrm{garbage}_y\rangle_{\mathbf{A}',\mathbf{Z}}\right) |0\rangle_{\mathbf{B}} \end{array} \right) . \end{aligned} \tag{20}$$

Then, it holds that

$$\begin{aligned}
&\langle\tau|_{\mathbf{Z}}\langle\sigma|_{\mathbf{A}',\mathbf{B}} X_{\mathbf{B}} U^{\dagger}_{\mathbf{A}',\mathbf{Z}} |\tau'_{xy}\rangle_{\mathbf{Z}} |\sigma\rangle_{\mathbf{A}',\mathbf{B}} \\
=&\frac{1}{2}\left(\begin{array}{l}\left(\langle x|_{\mathbf{A}'}\langle\tau'_{xx}|_{\mathbf{Z}} + \langle y|_{\mathbf{A}'}\langle\tau'_{xy}|_{\mathbf{Z}} + \langle \mathrm{garbage}_x|_{\mathbf{A}',\mathbf{Z}}\right)\langle 1|_{\mathbf{B}} \\ +\left(\langle x|_{\mathbf{A}'}\langle\tau'_{yx}|_{\mathbf{Z}} + \langle y|_{\mathbf{A}'}\langle\tau'_{yy}|_{\mathbf{Z}} + \langle \mathrm{garbage}_y|_{\mathbf{A}',\mathbf{Z}}\right)\langle 0|_{\mathbf{B}}\end{array}\right)(|x\rangle_{\mathbf{A}'}|0\rangle_{\mathbf{B}} + |y\rangle_{\mathbf{A}'}|1\rangle_{\mathbf{B}})|\tau'_{xy}\rangle_{\mathbf{Z}} \quad (21)\\
=&\frac{1}{2}(\langle\tau'_{xy}| + \langle\tau'_{yx}|)_{\mathbf{Z}}|\tau'_{xy}\rangle_{\mathbf{Z}},
\end{aligned}$$

where the first equality follows from Equations (13) and (20) and the second equality follows from Equations (17) and (18) and the assumption that $|x\rangle$ and $|y\rangle$ are orthogonal.

By Equations (19) and (21), we have

$$\langle y|_{\mathbf{A}}\langle\tau|_{\mathbf{Z}}\langle\sigma|_{\mathbf{A}',\mathbf{B}}\widetilde{U}|x\rangle_{\mathbf{A}}|\tau\rangle_{\mathbf{Z}}|\sigma\rangle_{\mathbf{A}',\mathbf{B}} = \frac{1}{2}(\langle\tau'_{xy}| + \langle\tau'_{yx}|)_{\mathbf{Z}}|\tau'_{xy}\rangle_{\mathbf{Z}}. \quad (22)$$

By a similar calculation, we have

$$\langle x|_{\mathbf{A}}\langle\tau|_{\mathbf{Z}}\langle\sigma|_{\mathbf{A}',\mathbf{B}}\widetilde{U}|y\rangle_{\mathbf{A}}|\tau\rangle_{\mathbf{Z}}|\sigma\rangle_{\mathbf{A}',\mathbf{B}} = \frac{1}{2}(\langle\tau'_{xy}| + \langle\tau'_{yx}|)_{\mathbf{Z}}|\tau'_{yx}\rangle_{\mathbf{Z}}. \quad (23)$$

By Equations (22) and (23), 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 (14), we complete the proof of Claim 5.3. □

This completes the proof of Theorem 5.1. □

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 5.1.

Theorem 6.1 (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:*

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

  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 $(\mathbf{C}, \mathbf{R}, \mathbf{D})$.

Proof of Theorem 6.1. Since the proofs are almost identical for all the three cases of $\mathtt{X}, \mathtt{Y} \in \{$computationally,statistically, perfectly$\}$, we focus on the case of $\mathtt{X} = \mathtt{Y} =$ "computationally".

Proof of Item 1. Suppose that $\{Q'_0, Q'_1\}$ is not computationally binding. Then, there exists a polynomial-time computable unitary U over $\mathbf{R}' = \mathbf{C}$ and an ancillary register $\mathbf{Z}$ and a state $|\tau\rangle_{\mathbf{Z}}$ such that

$$\left\| ((\langle 0| {Q'_1}^\dagger)_{\mathbf{C}',\mathbf{R}'} \otimes I_{\mathbf{Z}})(I_{\mathbf{C}'} \otimes U_{\mathbf{R}',\mathbf{Z}})((Q'_0 |0\rangle)_{\mathbf{C}',\mathbf{R}'} |\tau\rangle_{\mathbf{Z}}) \right\|$$

is non-negligible. We observe that U does not act on $\mathbf{D}$ (since that is not part of the reveal register $\mathbf{R}'$ of $\{Q'_0, Q'_1\}$), and thus it cannot cause any interference between states that take 0 and 1 in $\mathbf{D}$. Based on this observation and the denifition of $\{Q'_0, Q'_1\}$, we have

$$\begin{aligned}
&((\langle 0| {Q'_1}^\dagger)_{\mathbf{C}',\mathbf{R}'} \otimes I_{\mathbf{Z}})(I_{\mathbf{C}'} \otimes U_{\mathbf{R}',\mathbf{Z}})((Q'_0 |0\rangle)_{\mathbf{C}',\mathbf{R}'} |\tau\rangle_{\mathbf{Z}}) \\
=&\frac{1}{2} \begin{pmatrix} ((\langle 0| Q_0^\dagger)_{\mathbf{C},\mathbf{R}} \langle 0|_{\mathbf{D}} \otimes I_{\mathbf{Z}})(I_{\mathbf{R},\mathbf{D}} \otimes U_{\mathbf{C},\mathbf{Z}})((Q_0 |0\rangle)_{\mathbf{C},\mathbf{R}} |0\rangle_{\mathbf{D}} |\tau\rangle_{\mathbf{Z}}) \\ -((\langle 0| Q_1^\dagger)_{\mathbf{C},\mathbf{R}} \langle 1|_{\mathbf{D}} \otimes I_{\mathbf{Z}})(I_{\mathbf{R},\mathbf{D}} \otimes U_{\mathbf{C},\mathbf{Z}})((Q_1 |0\rangle)_{\mathbf{C},\mathbf{R}} |1\rangle_{\mathbf{D}} |\tau\rangle_{\mathbf{Z}}) \end{pmatrix}.
\end{aligned}$$

Similarly, we have

$$\begin{aligned}
&((\langle 0| {Q'_0}^\dagger)_{\mathbf{C}',\mathbf{R}'} \otimes I_{\mathbf{Z}})(I_{\mathbf{C}'} \otimes U_{\mathbf{R}',\mathbf{Z}})((Q'_1 |0\rangle)_{\mathbf{C}',\mathbf{R}'} |\tau\rangle_{\mathbf{Z}}) \\
=&\frac{1}{2} \begin{pmatrix} ((\langle 0| Q_0^\dagger)_{\mathbf{C},\mathbf{R}} \langle 0|_{\mathbf{D}} \otimes I_{\mathbf{Z}})(I_{\mathbf{R},\mathbf{D}} \otimes U_{\mathbf{C},\mathbf{Z}})((Q_0 |0\rangle)_{\mathbf{C},\mathbf{R}} |0\rangle_{\mathbf{D}} |\tau\rangle_{\mathbf{Z}}) \\ -((\langle 0| Q_1^\dagger)_{\mathbf{C},\mathbf{R}} \langle 1|_{\mathbf{D}} \otimes I_{\mathbf{Z}})(I_{\mathbf{R},\mathbf{D}} \otimes U_{\mathbf{C},\mathbf{Z}})((Q_1 |0\rangle)_{\mathbf{C},\mathbf{R}} |1\rangle_{\mathbf{D}} |\tau\rangle_{\mathbf{Z}}) \end{pmatrix}.
\end{aligned}$$

In particular,

$$\begin{aligned}
&((\langle 0| {Q'_1}^\dagger)_{\mathbf{C}',\mathbf{R}'} \otimes I_{\mathbf{Z}})(I_{\mathbf{C}'} \otimes U_{\mathbf{R}',\mathbf{Z}})((Q'_0 |0\rangle)_{\mathbf{C}',\mathbf{R}'} |\tau\rangle_{\mathbf{Z}}) \\
=&((\langle 0| {Q'_0}^\dagger)_{\mathbf{C}',\mathbf{R}'} \otimes I_{\mathbf{Z}})(I_{\mathbf{C}'} \otimes U_{\mathbf{R}',\mathbf{Z}})((Q'_1 |0\rangle)_{\mathbf{C}',\mathbf{R}'} |\tau\rangle_{\mathbf{Z}}).
\end{aligned}$$

Therefore,

$$\left\| \begin{aligned} &((\langle 0| {Q'_1}^\dagger)_{\mathbf{C}',\mathbf{R}'} \otimes I_{\mathbf{Z}})(I_{\mathbf{C}'} \otimes U_{\mathbf{R}',\mathbf{Z}})((Q'_0 |0\rangle)_{\mathbf{C}',\mathbf{R}'} |\tau\rangle_{\mathbf{Z}}) \\ &+((\langle 0| {Q'_0}^\dagger)_{\mathbf{C}',\mathbf{R}'} \otimes I_{\mathbf{Z}})(I_{\mathbf{C}'} \otimes U_{\mathbf{R}',\mathbf{Z}})((Q'_1 |0\rangle)_{\mathbf{C}',\mathbf{R}'} |\tau\rangle_{\mathbf{Z}}) \end{aligned} \right\|$$

is non-negligible. If we set $|x\rangle = Q'_0 |0\rangle_{\mathbf{C}',\mathbf{R}'}$ and $|y\rangle = Q'_1 |0\rangle_{\mathbf{C}',\mathbf{R}'}$, then $|x\rangle$ and $|y\rangle$ are orthogonal. Then, by Item 1 of Theorem 5.1, there exists a non-uniform QPT distinguisher $\mathcal{A}$ with a polynomial-size advice $|\tau'\rangle$ that does not act on $\mathbf{C}' = (\mathbf{R}, \mathbf{D})$ and distinguishes

$$|\psi\rangle = \frac{|x\rangle + |y\rangle}{\sqrt{2}} = (Q_0 |0\rangle)_{\mathbf{C},\mathbf{R}} |0\rangle_{\mathbf{D}}$$

and

$$|\phi\rangle = \frac{|x\rangle - |y\rangle}{\sqrt{2}} = (Q_1 |0\rangle)_{\mathbf{C},\mathbf{R}} |1\rangle_{\mathbf{D}}$$

with a non-negligible advantage. This means that the computational hiding property of $\{Q_0, Q_1\}$ is broken, which contradicts the assumption. Thus, $\{Q'_0, Q'_1\}$ is computationally binding. This completes the proof of Item 1.

Proof of Item 2. Suppose that $\{Q'_0, Q'_1\}$ is not computationally hiding. Then, there exists a non-uniform QPT distinguisher $\mathcal{A}$ with advice $|\tau\rangle_{\mathbf{Z}}$ that does not act on $\mathbf{R}' = \mathbf{C}$ and distinguishes

$$|\psi\rangle := \frac{1}{\sqrt{2}} ((Q_0 |0\rangle)_{\mathbf{C},\mathbf{R}} |0\rangle_{\mathbf{D}} + (Q_1 |0\rangle)_{\mathbf{C},\mathbf{R}} |1\rangle_{\mathbf{D}})$$

and

$$|\phi\rangle := \frac{1}{\sqrt{2}} ((Q_0 |0\rangle)_{\mathbf{C},\mathbf{R}} |0\rangle_{\mathbf{D}} - (Q_1 |0\rangle)_{\mathbf{C},\mathbf{R}} |1\rangle_{\mathbf{D}})$$

with a non-negligible advantage Δ.

Since $|\psi\rangle$ and $|\phi\rangle$ are orthogonal, by Item 2 of Theorem 5.1, there exists a polynomial-time computable unitary U over $(\mathbf{R}, \mathbf{D}, \mathbf{Z})$ such that

$$\frac{|\langle y|_{\mathbf{C},\mathbf{R},\mathbf{D}} \langle\tau|_{\mathbf{Z}} (U_{\mathbf{R},\mathbf{D},\mathbf{Z}} \otimes I_{\mathbf{C}}) |x\rangle_{\mathbf{C},\mathbf{R},\mathbf{D}} |\tau\rangle_{\mathbf{Z}} + \langle x|_{\mathbf{C},\mathbf{R},\mathbf{D}} \langle\tau|_{\mathbf{Z}} (U_{\mathbf{R},\mathbf{D},\mathbf{Z}} \otimes I_{\mathbf{C}}) |y\rangle_{\mathbf{C},\mathbf{R},\mathbf{D}} |\tau\rangle_{\mathbf{Z}}|}{2} = \Delta$$

where

$$|x\rangle = \frac{|\psi\rangle + |\phi\rangle}{\sqrt{2}} = (Q_0 |0\rangle)_{\mathbf{C},\mathbf{R}} |0\rangle_{\mathbf{D}}$$

and

$$|y\rangle = \frac{|\psi\rangle - |\phi\rangle}{\sqrt{2}} = (Q_1 |0\rangle)_{\mathbf{C},\mathbf{R}} |1\rangle_{\mathbf{D}}.$$

Thus, we must have $|\langle y|_{\mathbf{C},\mathbf{R},\mathbf{D}} \langle\tau|_{\mathbf{Z}} (U_{\mathbf{R},\mathbf{D},\mathbf{Z}} \otimes I_{\mathbf{C}}) |x\rangle_{\mathbf{C},\mathbf{R},\mathbf{D}} |\tau\rangle_{\mathbf{Z}}| \geq \Delta$ or $|\langle x|_{\mathbf{C},\mathbf{R},\mathbf{D}} \langle\tau|_{\mathbf{Z}} (U_{\mathbf{R},\mathbf{D},\mathbf{Z}} \otimes I_{\mathbf{C}}) |y\rangle_{\mathbf{C},\mathbf{R},\mathbf{D}} |\tau\rangle_{\mathbf{Z}}| \geq \Delta$. We assume the former w.l.o.g., i.e., we have

$$\left| \left((\langle 0| Q_1^\dagger)_{\mathbf{C},\mathbf{R}} \langle 1|_{\mathbf{D}} \langle\tau|_{\mathbf{Z}} \right) (U_{\mathbf{R},\mathbf{D},\mathbf{Z}} \otimes I_{\mathbf{C}}) ((Q_0 |0\rangle)_{\mathbf{C},\mathbf{R}} |0\rangle_{\mathbf{D}} |\tau\rangle_{\mathbf{Z}}) \right| \geq \Delta.$$

In particular, we have

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

This means that U with the auxiliary state $|0\rangle_{\mathbf{D}} |\tau\rangle_{\mathbf{Z}}$ breaks the computational binding property of $\{Q_0, Q_1\}$, which contradicts the assumption. Thus, $\{Q'_0, Q'_1\}$ is computationally hiding. This completes the proof of Item 2.

□

7 Applications of Our Conversion

In this section, we show applications of our conversion (Theorem 6.1). More applications can be found in Appendix B.

When we describe a canonical quantum bit commitment scheme $\{Q_0, Q_1\}$, we only describe how Q_0 and Q_1 act on $|0\rangle$ for simplicity. Quantum circuits that implement Q_0 and Q_1 can be defined in a natural way.

7.1 Construction from PRG

Naor [Nao91] constructed a two-message *classical* commitment scheme that is computationally hiding and statistically binding based on PRGs. Yan et al. [YWLQ15] constructed a quantum *non-interactive* version of Naor's commitment.[34] Let $G : \{0,1\}^n \to \{0,1\}^{3n}$ be a PRG. Then Yan et al.'s commitment scheme $\{Q_{\mathsf{YWLQ},0}, Q_{\mathsf{YWLQ},1}\}$ is described as follows:

$$Q_{\mathsf{YWLQ},0}\,|0\rangle_{\mathbf{C},\mathbf{R}} := \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |G(x)\rangle_{\mathbf{C}}\,|x, 0^{2n}\rangle_{\mathbf{R}}$$
$$Q_{\mathsf{YWLQ},1}\,|0\rangle_{\mathbf{C},\mathbf{R}} := \frac{1}{\sqrt{2^{3n}}} \sum_{y\in\{0,1\}^{3n}} |y\rangle_{\mathbf{C}}\,|y\rangle_{\mathbf{R}}\,.$$

Yan et al. [YWLQ15] proved the following theorem.

Theorem 7.1 ([YWLQ15]). *If G is a PRG, $\{Q_{\mathsf{YWLQ},0}, Q_{\mathsf{YWLQ},1}\}$ is computationally hiding and statistically binding.*

By applying our conversion to $\{Q_{\mathsf{YWLQ},0}, Q_{\mathsf{YWLQ},1}\}$, we obtain the following scheme $\{Q'_{\mathsf{YWLQ},0}, Q'_{\mathsf{YWLQ},1}\}$.

$$Q'_{\mathsf{YWLQ},b}\,|0\rangle_{\mathbf{C}',\mathbf{R}'} := \frac{1}{\sqrt{2^{n+1}}} \sum_{x\in\{0,1\}^n} |0, x, 0^{2n}\rangle_{\mathbf{C}'}\,|G(x)\rangle_{\mathbf{R}'} + (-1)^b \frac{1}{\sqrt{2^{3n+1}}} \sum_{y\in\{0,1\}^{3n}} |1, y\rangle_{\mathbf{C}'}\,|y\rangle_{\mathbf{R}'}\,.$$

By Theorems 6.1 and 7.1, we obtain the following theorem.

Theorem 7.2. *If G is a PRG, $\{Q'_{\mathsf{YWLQ},0}, Q'_{\mathsf{YWLQ},1}\}$ is statistically hiding and computationally binding.*

This is the first statistically hiding and computationally binding quantum bit commitment scheme from PRG that makes only a single call to the PRG. If we apply existing conversions [CLS01, Yan22] to $\{Q_{\mathsf{YWLQ},0}, Q_{\mathsf{YWLQ},1}\}$ (or other PRG-based schemes), they result in schemes that make $\Omega(\lambda^2)$ calls to the PRG.

Note that it is known that PRG exists assuming the existence of one-way functions [HILL99].[35] In the current state of the art, a construction of PRG makes at least $\Omega(\lambda^3)$ calls to the base one-way function [HRV10, VZ12]. Thus, if we construct a PRG from a one-way function and count the number of calls to the one-way function, $\{Q'_{\mathsf{YWLQ},0}, Q'_{\mathsf{YWLQ},1}\}$ makes $\Omega(\lambda^3)$ calls to the one-way function. We observe that this is asymptotically the same number as that of Koshiba and Odaira [KO11]. However, it does not seem possible to instantiate the scheme of [KO11] with a single call to a PRG instead of $\Omega(\lambda^3)$ calls to a one-way function. Also, our security analysis is much simpler than theirs once we establish Theorem 6.1.

[34] Yan [Yan22, Appendix C] shows an alternative more direct translation of Naor's commitment to the quantum setting. We could also apply our conversion to that scheme, but we focus on the scheme of [YWLQ15] since that is simpler.

[35] Though the original security proof in [HILL99] only considers classical adversaries, it also works against quantum adversaries as well assuming quantum-secure one-way functions.

7.2 Construction from Pseudorandom State Generators

Ananth, Qian, Yuen [AQY22], and Morimae and Yamakawa [MY22] concurrently showed that a primitive called pseudorandom state generators (PRSGs) [JLS18] can be used to construct computationally hiding and statistically binding quantum bit commitments. Especially, Morimae and Yamakawa [MY22, footnote 12] mentioned that simply replacing PRGs with single-copy secure PRSGs in $\{Q_{\mathsf{YWLQ},0}, Q_{\mathsf{YWLQ},1}\}$ yields a computationally hiding and statistically binding scheme.

Let $\mathsf{StateGen}$ be a single-copy-secure PRSG that, on input $k \in \{0,1\}^n$, outputs an m-qubit state $|\phi_k\rangle$ where $m = 3n$. Then, Morimae and Yamakawa's commitment scheme $\{Q_{\mathsf{MY},0}, Q_{\mathsf{MY},1}\}$ is described as follows:

$$Q_{\mathsf{MY},0}\,|0\rangle_{\mathbf{C},\mathbf{R}} := \frac{1}{\sqrt{2^n}} \sum_{k\in\{0,1\}^n} |\phi_k\rangle_{\mathbf{C}}\,|k, 0^{2n}\rangle_{\mathbf{R}}$$
$$Q_{\mathsf{MY},1}\,|0\rangle_{\mathbf{C},\mathbf{R}} := \frac{1}{\sqrt{2^{3n}}} \sum_{r\in\{0,1\}^{3n}} |r\rangle_{\mathbf{C}}\,|r\rangle_{\mathbf{R}}\,.$$

Theorem 7.3. *If* $\mathsf{StateGen}$ *is single-copy-secure, then* $\{Q_{\mathsf{MY},0}, Q_{\mathsf{MY},1}\}$ *is computationally hiding and statistically binding.*

Since the above is not the main construction of [MY22], they did not give a security proof. Thus, we give a security proof for completeness.

Proof of Theorem 7.3. We let $|\psi_b\rangle_{\mathbf{C},\mathbf{R}} := Q_{\mathsf{MY},b}\,|0\rangle_{\mathbf{C},\mathbf{R}}$.

Computational hiding. Note that $\mathrm{Tr}_{\mathbf{R}}\left(|\psi_1\rangle\langle\psi_1|_{\mathbf{C},\mathbf{R}}\right)$ is a maximally mixed state, which is a Haar random state when given a single copy. On the other hand, we have $\mathrm{Tr}_{\mathbf{R}}\left(|\psi_0\rangle\langle\psi_0|_{\mathbf{C},\mathbf{R}}\right) = \frac{1}{2^n}\sum_{k\in\{0,1\}^n} |\phi_k\rangle\langle\phi_k|$. Thus, the computational hiding property immediately follows from the single-copy security of $\mathsf{StateGen}$.

Statistical binding. The proof is similar to the proof of binding in [MY22]. Let $F(\rho,\sigma)$ be the fidelity between ρ and σ. Then, we have

$$\begin{aligned}
&F\Big(\mathrm{Tr}_{\mathbf{R}}(|\psi_0\rangle\langle\psi_0|_{\mathbf{C},\mathbf{R}}), \mathrm{Tr}_{\mathbf{R}}(|\psi_1\rangle\langle\psi_1|_{\mathbf{C},\mathbf{R}})\Big)\\
&= F\Big(\frac{1}{2^n}\sum_k |\phi_k\rangle\langle\phi_k|, \frac{I^{\otimes m}}{2^m}\Big)\\
&= \Big\|\sum_{i=1}^{\xi} \sqrt{\lambda_i}\frac{1}{\sqrt{2^m}}|\lambda_i\rangle\langle\lambda_i|\Big\|_1^2\\
&= \left(\sum_{i=1}^{\xi} \sqrt{\lambda_i}\frac{1}{\sqrt{2^m}}\right)^2\\
&\le \left(\sum_{i=1}^{\xi} \lambda_i\right)\left(\sum_{i=1}^{\xi} \frac{1}{2^m}\right)\\
&\le 2^{-2n},
\end{aligned}$$

where in the second equality, $\sum_{i=1}^{\xi}\lambda_i|\lambda_i\rangle\langle\lambda_i|$ is the diagonalization of $\frac{1}{2^n}\sum_k|\phi_k\rangle\langle\phi_k|$, in the first inequality, we have used Cauchy–Schwarz inequality, and in the final inequality, we have used $\xi\le 2^n$ and $m=3n$. This means that $\{Q_{\mathsf{MY},0},Q_{\mathsf{MY},1}\}$ is statistically binding [Yan22]. □

By applying our conversion to $\{Q_{\mathsf{MY},0},Q_{\mathsf{MY},1}\}$, we obtain the following scheme $\{Q'_{\mathsf{MY},0},Q'_{\mathsf{MY},1}\}$.[36]

$$Q'_{\mathsf{MY},b}|0\rangle_{\mathbf{C}',\mathbf{R}'}:=\frac{1}{\sqrt{2^{n+1}}}\sum_{k\in\{0,1\}^n}|0,k,0^{2n}\rangle_{\mathbf{C}'}|\phi_k\rangle_{\mathbf{R}'}+(-1)^b\frac{1}{\sqrt{2^{3n+1}}}\sum_{r\in\{0,1\}^{3n}}|1,r\rangle_{\mathbf{C}'}|r\rangle_{\mathbf{R}'}.$$

By Theorems 6.1 and 7.3, we obtain the following theorem.

Theorem 7.4. *If* StateGen *is single-copy-secure, then* $\{Q'_{\mathsf{MY},0},Q'_{\mathsf{MY},1}\}$ *is statistically hiding and computationally binding.*

This is the first statistically hiding and computationally binding quantum bit commitment scheme from PRSGs that makes only a single call to the PRSG. If we apply existing conversions [CLS01, Yan22] to $\{Q_{\mathsf{MY},0},Q_{\mathsf{MY},1}\}$ (or other PRSG-based schemes [AQY22]), they result in a schemes that make $\Omega(\lambda^2)$ calls to the PRSG.

7.3 Construction from Injective One-Way Functions

In this section, we show simple constructions of commitments based on any injective one-way functions.

Perfectly hiding and computationally binding commitment. We first construct a perfectly hiding and computationally binding quantum bit commitment scheme from injective one-way function. We note that such a commitment is already known from any one-way *permutations* in [DMS00]. (See Appendix B.1 for details.) Our construction is more general since every permutation is also injective but the converse is not true.

Let $f:\{0,1\}^n\to\{0,1\}^m$ be an injective one-way function. Then, we define a canonical quantum bit commitment scheme $\{Q_{\mathsf{inj},0},Q_{\mathsf{inj},1}\}$ as follows:

$$Q_{\mathsf{inj},0}|0\rangle_{\mathbf{C},\mathbf{R}}:=\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle_{\mathbf{C}}|f(x)\rangle_{\mathbf{R}}$$
$$Q_{\mathsf{inj},1}|0\rangle_{\mathbf{C},\mathbf{R}}:=\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle_{\mathbf{C}}|x,0^{m-n}\rangle_{\mathbf{R}}.$$

Theorem 7.5. *If f is an injective one-way function, $\{Q_{\mathsf{inj},0},Q_{\mathsf{inj},1}\}$ is perfectly hiding and computationally binding.*

Proof.

Perfect hiding. By the injectivity of f, if we trace out $\mathbf{R}$, then the reduced state in $\mathbf{C}$ is $\sum_{x\in\{0,1\}^n}|x\rangle\langle x|$ for both $b=0,1$. This implies perfect hiding.

Computational binding. Suppose that the $\{Q_{\mathsf{inj},0},Q_{\mathsf{inj},1}\}$ is not computationally binding. Then there exists a polynomial-time computable unitary U over $(\mathbf{R},\mathbf{Z})$ and an auxiliary state $|\tau\rangle_{\mathbf{Z}}$ such that

$$\left\|(Q_{\mathsf{inj},1}|0\rangle\langle 0|Q_{\mathsf{inj},1}^\dagger)_{\mathbf{C},\mathbf{R}}(I_{\mathbf{C}}\otimes U_{\mathbf{R},\mathbf{Z}})((Q_{\mathsf{inj},0}|0\rangle)_{\mathbf{C},\mathbf{R}}|\tau\rangle_{\mathbf{Z}})\right\|$$

[36] We could also apply our conversion to the main construction of [MY22] to obtain a similar scheme.

is non-negligible. In particular, its square is also non-negligible. It holds that

$$\begin{aligned}
&\left\|(Q_{\mathsf{inj},1}\left|0\right\rangle\left\langle 0\right|Q_{\mathsf{inj},1}^{\dagger})_{\mathbf{C},\mathbf{R}}(I_{\mathbf{C}}\otimes U_{\mathbf{R},\mathbf{Z}})((Q_{\mathsf{inj},0}\left|0\right\rangle)_{\mathbf{C},\mathbf{R}}\left|\tau\right\rangle_{\mathbf{Z}})\right\|^2\\
=&\frac{1}{2^{2n}}\left\|\sum_{x\in\{0,1\}^n}\langle x,0^{m-n}|_{\mathbf{R}}\,U_{\mathbf{R},\mathbf{Z}}\left|f(x)\right\rangle_{\mathbf{R}}\left|\tau\right\rangle_{\mathbf{Z}}\right\|^2\\
\leq&\frac{1}{2^{2n}}\left(\sum_{x\in\{0,1\}^n}\left\|\langle x,0^{m-n}|_{\mathbf{R}}\,U_{\mathbf{R},\mathbf{Z}}\left|f(x)\right\rangle_{\mathbf{R}}\left|\tau\right\rangle_{\mathbf{Z}}\right\|\right)^2\\
\leq&\frac{1}{2^{n}}\sum_{x\in\{0,1\}^n}\left\|\langle x,0^{m-n}|_{\mathbf{R}}\,U_{\mathbf{R},\mathbf{Z}}\left|f(x)\right\rangle_{\mathbf{R}}\left|\tau\right\rangle_{\mathbf{Z}}\right\|^2,
\end{aligned}\tag{24}$$

where the first equality follows from the definition of $\{Q_{\mathsf{inj},0},Q_{\mathsf{inj},1}\}$, the first inequality follows from the triangle inequality, and the second inequality follows from the Cauchy–Schwarz inequality. Thus, the value of Equation (24) is non-negligible.

Then, we can construct an adversary $\mathcal{A}$ that breaks the one-wayness of f with advice $\left|\tau\right\rangle$ as follows:

$\mathcal{A}(y;\left|\tau\right\rangle)$**:** Given an instance y and advice $\left|\tau\right\rangle$, it generates a state $U\left|y\right\rangle_{\mathbf{R}}\left|\tau\right\rangle_{\mathbf{Z}}$ and measures $\mathbf{R}$. If the measurement outcome is $(x,0^{m-n})$ such that $f(x)=y$, it outputs x and otherwise $\perp$.

We can see that the probability that $\mathcal{A}$ outputs the correct preimage x is the value of Equation (24), which is non-negligible. This contradicts the one-wayness of f. Thus, $\{Q_{\mathsf{inj},0},Q_{\mathsf{inj},1}\}$ is computationally binding. □

This is the first *perfectly* hiding quantum bit commitment scheme from injective one-way functions that makes only a single quantum call to the base function. Before our work, such a commitment scheme was only known to exist from one-way *permutations* [DMS00] (which is described in Appendix B.1). We remark that Koshiba and Odaira [KO09, KO11] generalized [DMS00] to make the assumption weaker than the existence of injective one-way functions, but those constructions only achieve *statistical* hiding.

Alternatively, we can also construct such a commitment scheme by applying our conversion to the (purified version of) construction of computationally hiding and perfectly binding commitment scheme based on Goldreich-Levin theorem [GL89]. See Appendix B.2 for details.

Computationally hiding and perfectly binding commitment. Next, we apply our conversion to $\{Q_{\mathsf{inj},0},Q_{\mathsf{inj},1}\}$ to obtain the following scheme $\{Q'_{\mathsf{inj},0},Q'_{\mathsf{inj},1}\}$:

$$Q'_{\mathsf{inj},b}\left|0\right\rangle_{\mathbf{C}',\mathbf{R}'}:=\frac{1}{\sqrt{2^{n+1}}}\sum_{x\in\{0,1\}^n}\left(\left|0\right\rangle\left|f(x)\right\rangle+(-1)^b\left|1\right\rangle\left|x,0^{m-n}\right\rangle\right)_{\mathbf{C}'}\otimes\left|x\right\rangle_{\mathbf{R}'}.$$

By Theorems 6.1 and 7.5, we obtain the following theorem.

Theorem 7.6. *If f is an injective one-way function, $\{Q'_{\mathsf{inj},0},Q'_{\mathsf{inj},1}\}$ is computationally hiding and perfectly binding.*

Comparison with classical construction. It is well-known that we can *classically* construct a computationally hiding and perfectly binding non-interactive commitment scheme from injective one-way functions by using Goldreich-Levin theorem [GL89]. (See Appendix B.2 for more details.) The construction also only makes a

single call to the base function. Then, one may wonder if it is meaningful to give a *quantum* construction for that. We argue this by remarking the following two points.

The first is a minor parameter improvement. Our construction has a shorter commitment size than the classical construction (albeit with the apparent disadvantage of the usage of quantum communication). Specifically, commitment length of our construction is $m+1$ whereas it is $n+m+1$ in the classical construction. The additional n-bit is needed to send the seed for the hardcore bit function in the classical construction. We remark that the decommitment length is the same, n for both constructions. Though the improvement is somewhat minor, we believe that it is still worthwhile to show that the quantum communication can reduce the communication complexity of such an important construction of commitments from injective one-way functions.

The second is rather conceptual. We remark that our construction does not make use of any sort of classical hardcore predicates. On the other hand, to our knowledge, the only known way to classically construct a commitment scheme from injective one-way functions (or even one-way permutations) is to rely on some hardcore predicates [GL89, GRS00, HMS04]. Thus, the source of the pseudorandomness of our construction seems conceptually very different from that for classical constructions. In a nutshell, we interpret the theorem shown by [AAS20] in a completely irrelevant context as a kind of search-to-decision reduction. We believe that this new search-to-decision reduction technique is interesting and will be useful in the future work.

Construction from keyed injective one-way functions. Unfortunately, there is no known candidate of post-quantum injective one-way functions based on standard assumptions.[37] On the other hand, there are many candidates of *keyed* injective one-way functions. We remark that our construction can be easily extended to one based on keyed injective one-way functions. Let $\{f_k : \{0,1\}^n \to \{0,1\}^m\}_{k\in\mathcal{K}}$ be a keyed injective one-way function. Then, we construct a modified scheme $\{Q_{\mathsf{keyed\text{-}inj},0}, Q_{\mathsf{keyed\text{-}inj},1}\}$ as follows:

$$Q_{\mathsf{keyed\text{-}inj},0}\left|0\right\rangle_{\mathbf{C},\mathbf{R}} := \frac{1}{\sqrt{2^n|\mathcal{K}|}}\sum_{x\in\{0,1\}^n,k\in\mathcal{K}}\left|x,k\right\rangle_{\mathbf{C}}\left|f_k(x),k\right\rangle_{\mathbf{R}}$$
$$Q_{\mathsf{keyed\text{-}inj},1}\left|0\right\rangle_{\mathbf{C},\mathbf{R}} := \frac{1}{\sqrt{2^n|\mathcal{K}|}}\sum_{x\in\{0,1\}^n}\left|x,k\right\rangle_{\mathbf{C}}\left|x,0^{m-n},k\right\rangle_{\mathbf{R}}$$

Then, we can show that $\{Q_{\mathsf{keyed\text{-}inj},0}, Q_{\mathsf{keyed\text{-}inj},1}\}$ is perfectly hiding and computationally binding similarly to the proof of Theorem 7.5.

By applying our conversion, we obtain the following scheme $\{Q'_{\mathsf{keyed\text{-}inj},0}, Q'_{\mathsf{keyed\text{-}inj},1}\}$.

$$Q'_{\mathsf{keyed\text{-}inj},b}\left|0\right\rangle_{\mathbf{C}',\mathbf{R}'} := \frac{1}{\sqrt{2^{n+1}|\mathcal{K}|}}\sum_{x\in\{0,1\}^n,k\in\mathcal{K}}\left(\left|0\right\rangle\left|f_k(x),k\right\rangle + (-1)^b\left|1\right\rangle\left|x,0^{m-n},k\right\rangle\right)_{\mathbf{C}'}\otimes\left|x,k\right\rangle_{\mathbf{R}'}.$$

By Theorem 6.1, $\{Q'_{\mathsf{keyed\text{-}inj},0}, Q'_{\mathsf{keyed\text{-}inj},1}\}$ is computationally binding and statistically hiding.

We remark that we can also view it as a quantum-ciphertext PKE (Definition 4.8) if we assume that f_k is a trapdoor function. That is, we can use $\mathrm{Tr}_{\mathbf{R}'}\left(Q'_{\mathsf{keyed\text{-}inj},b}\left|0\right\rangle_{\mathbf{C}',\mathbf{R}'}\left\langle 0\right|_{\mathbf{C}',\mathbf{R}'}Q'^{\dagger}_{\mathsf{keyed\text{-}inj},b}\right)$ as an encryption of b. We can decrypt it with a trapdoor for f_k by applying a unitary $\left|x,0^{m-n},k\right\rangle \mapsto \left|f_k(x),k\right\rangle$ on the second register of $\mathbf{C}'$ controlled on the first register of $\mathbf{C}'$ (which is efficiently computable with the trapdoor) and

[37] Candidate constructions of post-quantum injective one-way functions based on hash functions or block ciphers can be found in [Unr12, Section 5].

then measuring the first register of $\mathbf{C}'$ in the Hamadard basis. The IND-CPA security directly follows from the computational hiding property of $\{Q'_{\mathsf{keyed\text{-}inj},0}, Q'_{\mathsf{keyed\text{-}inj},1}\}$. This gives a conceptually different way to construct (quantum-ciphertext) PKE from trapdoor functions than that based on hardcore predicates.

7.4 Construction from Collapsing Functions

In this section, we show simple constructions of commitments based on collapsing functions. Interestingly, the constructions are almost identical to those based on injective one-way functions given in Section 7.3, but they achieve the other flavors of security than those based on injective one-way functions.

Computationally hiding and statistically binding commitment. We first construct a computationally hiding and statistically binding quantum bit commitment scheme from collapsing functions (Definition 3.4).

Let $\{H_k : \{0,1\}^n \to \{0,1\}^m\}_{k\in\mathcal{K}}$ be a family of collapsing functions such that $n \geq m + \lambda$. Then, we define a canonical quantum bit commitment scheme $\{Q_{\mathsf{col},0}, Q_{\mathsf{col},1}\}$ as follows:

$$Q_{\mathsf{col},0}\left|0\right\rangle_{\mathbf{C},\mathbf{R}} := \frac{1}{\sqrt{2^n|\mathcal{K}|}}\sum_{x\in\{0,1\}^n,k\in\mathcal{K}}\left|x,k\right\rangle_{\mathbf{C}}\left|H_k(x),0^{n-m},k\right\rangle_{\mathbf{R}}$$
$$Q_{\mathsf{col},1}\left|0\right\rangle_{\mathbf{C},\mathbf{R}} := \frac{1}{\sqrt{2^n|\mathcal{K}|}}\sum_{x\in\{0,1\}^n,k\in\mathcal{K}}\left|x,k\right\rangle_{\mathbf{C}}\left|x,k\right\rangle_{\mathbf{R}}.$$

Theorem 7.7. *If $\{H_k : \{0,1\}^n \to \{0,1\}^m\}_{k\in\mathcal{K}}$ is a family of collapsing functions such that $n \geq m + \lambda$, $\{Q_{\mathsf{inj},0}, Q_{\mathsf{inj},1}\}$ is computationally hiding and statistically binding.*

Proof.

Computational hiding. We have

$$\mathrm{Tr}_{\mathbf{R}}(Q_{\mathsf{col},0}\left|0\right\rangle_{\mathbf{C},\mathbf{R}}) = \frac{1}{|\mathcal{K}|}\sum_{y\in\{0,1\}^m,k\in\mathcal{K}}\frac{|S_{k,y}|}{2^n}\left(\frac{1}{\sqrt{|S_{k,y}|}}\sum_{x\in S_{k,y}}\left|x,k\right\rangle\right)\left(\frac{1}{\sqrt{|S_{k,y}|}}\sum_{x'\in S_{k,y}}\left\langle x',k\right|\right)$$

where

$$S_{k,y} := \{x \in \{0,1\}^n : H_k(x) = y\}.$$

Then, by the collapsing property of $\{H_k\}_{k\in\mathcal{K}}$, we can show that $\mathrm{Tr}_{\mathbf{R}}(Q_{\mathsf{col},0}\left|0\right\rangle_{\mathbf{C},\mathbf{R}})$ is computationally indistinguishable from

$$\frac{1}{2^n|\mathcal{K}|}\sum_{x\in\{0,1\}^n,k\in\mathcal{K}}\left|x,k\right\rangle\left\langle x,k\right|.$$

The above state is exactly the same as $\mathrm{Tr}_{\mathbf{R}}(Q_{\mathsf{col},1}\left|0\right\rangle_{\mathbf{C},\mathbf{R}})$. Thus, the computational hiding property is proven.

Statistical binding. Suppose that the $\{Q_{\mathsf{col},0}, Q_{\mathsf{col},1}\}$ is not statistically binding. Then by a similar argument to that for the proof of computational binding of $\{Q_{\mathsf{inj},0}, Q_{\mathsf{inj},1}\}$ in Section 7.3, we can construct an unbounded-time adversary $\mathcal{A}$ such that

$$\Pr[\mathcal{A}(k, H_k(x)) = x : k \leftarrow \mathcal{K}, x \leftarrow \{0,1\}^n]$$

is non-negligible. However, this is information-theoretically impossible since $n \geq m + \lambda$. Thus, $\{Q_{\mathsf{col},0}, Q_{\mathsf{col},1}\}$ is statistically binding. □

This is the first *statistically* binding quantum bit commitment scheme from collapsing functions that makes only a single quantum call to the base function. To our knowledge, the only known way to construct statistically binding (classical or quantum) commitments from collapsing functions (or collision-resistant functions in the classical case) is to first construct PRGs regarding collapsing (or collision-resistant) functions as one-way functions and then convert it to commitments by [Nao91]. This requires super-constant number of calls to the base function since known constructions of PRGs from one-way functions require super-constant number of calls [HILL99, HRV10, VZ12].

Note that post-quantum statistically *hiding* commitments from collapsing functions are known [HM96, Unr16b]. Thus, by applying our conversion to the purified version of the scheme, we can obtain an alternative construction of statistically binding commitments from collapsing functions. See Appendix B.3 for details.

Statistically hiding and computationally binding commitment. Next, we apply our conversion to $\{Q_{\mathsf{col},0}, Q_{\mathsf{col},1}\}$ to obtain the following scheme $\{Q'_{\mathsf{col},0}, Q'_{\mathsf{col},1}\}$:

$$Q'_{\mathsf{col},b}\left|0\right\rangle_{\mathbf{C}',\mathbf{R}'} := \frac{1}{\sqrt{2^{n+1}|\mathcal{K}|}} \sum_{x\in\{0,1\}^n, k\in\mathcal{K}} \Big(\left|0\right\rangle\left|H_k(x), 0^{n-m}, k\right\rangle + (-1)^b\left|1\right\rangle\left|x,k\right\rangle\Big)_{\mathbf{C}'} \otimes \left|x,k\right\rangle_{\mathbf{R}'}.$$

By Theorems 6.1 and 7.7, we obtain the following theorem.

Theorem 7.8. *If $\{H_k\}_{k\in\mathcal{K}}$ is a family of collapsing functions, $\{Q'_{\mathsf{col},0}, Q'_{\mathsf{col},1}\}$ is statistically hiding and computationally binding.*

As already mentioned, statistically hiding and computationally binding commitments from collapsing functions are known even without using quantum communications [HM96, Unr16b]. The above theorem gives an alternative construction for such commitments albeit with quantum communications.

References

[AAS20] Scott Aaronson, Yosi Atia, and Leonard Susskind. On the hardness of detecting macroscopic superpositions. *Electron. Colloquium Comput. Complex.*, page 146, 2020. (Cited on page 1, 3, 6, 7, 9, 10, 11, 12, 14, 15, 26, 27, 36.)

[AC02] Mark Adcock and Richard Cleve. A quantum goldreich-levin theorem with cryptographic applications. In Helmut Alt and Afonso Ferreira, editors, *STACS 2002, 19th Annual Symposium on Theoretical Aspects of Computer Science, Antibes - Juan les Pins, France, March 14-16, 2002, Proceedings*, volume 2285 of *Lecture Notes in Computer Science*, pages 323–334. Springer, 2002. (Cited on page 46.)

[ADMP20] Navid Alamati, Luca De Feo, Hart Montgomery, and Sikhar Patranabis. Cryptographic group actions and applications. In Shiho Moriai and Huaxiong Wang, editors, *ASIACRYPT 2020, Part II*, volume 12492 of *LNCS*, pages 411–439. Springer, Heidelberg, December 2020. (Cited on page 2, 4.)

[AGKZ20] Ryan Amos, Marios Georgiou, Aggelos Kiayias, and Mark Zhandry. One-shot signatures and applications to hybrid quantum/classical authentication. In Konstantin Makarychev, Yury Makarychev, Madhur Tulsiani, Gautam Kamath, and Julia Chuzhoy, editors, *52nd ACM STOC*, pages 255–268. ACM Press, June 2020. (Cited on page 3, 17, 44.)

[AGM21] Gorjan Alagic, Tommaso Gagliardoni, and Christian Majenz. Can you sign a quantum state? *Quantum*, 5:603, dec 2021. (Cited on page 5.)

[AQY22] Prabhanjan Ananth, Luowen Qian, and Henry Yuen. Cryptography from pseudorandom quantum states. In *CRYPTO 2022*, 2022. (Cited on page 5, 33, 34.)

[Bab16] László Babai. Graph isomorphism in quasipolynomial time [extended abstract]. In Daniel Wichs and Yishay Mansour, editors, *48th ACM STOC*, pages 684–697. ACM Press, June 2016. (Cited on page 4.)

[BB84] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, pages 175–179, 1984. (Cited on page 4, 5.)

[BB21] Nir Bitansky and Zvika Brakerski. Classical binding for quantum commitments. In Kobbi Nissim and Brent Waters, editors, *TCC 2021, Part I*, volume 13042 of *LNCS*, pages 273–298. Springer, Heidelberg, November 2021. (Cited on page 5, 9.)

[BC91] Gilles Brassard and Claude Crépeau. Quantum bit commitment and coin tossing protocols. In Alfred J. Menezes and Scott A. Vanstone, editors, *CRYPTO'90*, volume 537 of *LNCS*, pages 49–61. Springer, Heidelberg, August 1991. (Cited on page 5.)

[BCKM21] James Bartusek, Andrea Coladangelo, Dakshita Khurana, and Fermi Ma. One-way functions imply secure computation in a quantum world. In Tal Malkin and Chris Peikert, editors, *CRYPTO 2021, Part I*, volume 12825 of *LNCS*, pages 467–496, Virtual Event, August 2021. Springer, Heidelberg. (Cited on page 5.)

[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. (Cited on page 7, 18.)

[BDS17] Shalev Ben-David and Or Sattath. Quantum tokens for digital signatures. Cryptology ePrint Archive, Paper 2017/094, 2017. https://eprint.iacr.org/2017/094. (Cited on page 3, 18.)

[BHY09] Mihir Bellare, Dennis Hofheinz, and Scott Yilek. Possibility and impossibility results for encryption and commitment secure under selective opening. In Antoine Joux, editor, *EUROCRYPT 2009*, volume 5479 of *LNCS*, pages 1–35. Springer, Heidelberg, April 2009. (Cited on page 26.)

[BJ15] Anne Broadbent and Stacey Jeffery. Quantum homomorphic encryption for circuits of low T-gate complexity. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *CRYPTO 2015, Part II*, volume 9216 of *LNCS*, pages 609–629. Springer, Heidelberg, August 2015. (Cited on page 3, 19.)

[BY91] Gilles Brassard and Moti Yung. One-way group actions. In Alfred J. Menezes and Scott A. Vanstone, editors, *CRYPTO'90*, volume 537 of *LNCS*, pages 94–107. Springer, Heidelberg, August 1991. (Cited on page 1, 4, 6.)

[CDMS04] Claude Crépeau, Paul Dumais, Dominic Mayers, and Louis Salvail. Computational collapse of quantum state with application to oblivious transfer. In Moni Naor, editor, *TCC 2004*, volume 2951 of *LNCS*, pages 374–393. Springer, Heidelberg, February 2004. (Cited on page 6.)

[CKR11] André Chailloux, Iordanis Kerenidis, and Bill Rosgen. Quantum commitments from complexity assumptions. In Luca Aceto, Monika Henzinger, and Jiri Sgall, editors, *ICALP 2011, Part I*, volume 6755 of *LNCS*, pages 73–85. Springer, Heidelberg, July 2011. (Cited on page 8.)

[CLLZ21] Andrea Coladangelo, Jiahui Liu, Qipeng Liu, and Mark Zhandry. Hidden cosets and applications to unclonable cryptography. In Tal Malkin and Chris Peikert, editors, *CRYPTO 2021, Part I*, volume 12825 of *LNCS*, pages 556–584, Virtual Event, August 2021. Springer, Heidelberg. (Cited on page 3, 18.)

[CLM+18] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. CSIDH: An efficient post-quantum commutative group action. In Thomas Peyrin and Steven Galbraith, editors, *ASIACRYPT 2018, Part III*, volume 11274 of *LNCS*, pages 395–427. Springer, Heidelberg, December 2018. (Cited on page 2, 4.)

[CLS01] Claude Crépeau, Frédéric Légaré, and Louis Salvail. How to convert the flavor of a quantum bit commitment. In Birgit Pfitzmann, editor, *EUROCRYPT 2001*, volume 2045 of *LNCS*, pages 60–77. Springer, Heidelberg, May 2001. (Cited on page 2, 3, 5, 32, 34.)

[Cou06] Jean-Marc Couveignes. Hard homogeneous spaces. Cryptology ePrint Archive, Paper 2006/291, 2006. https://eprint.iacr.org/2006/291. (Cited on page 2, 4.)

[CW79] Larry Carter and Mark N. Wegman. Universal classes of hash functions. *J. Comput. Syst. Sci.*, 18(2):143–154, 1979. (Cited on page 48.)

[DFS04] Ivan Damgård, Serge Fehr, and Louis Salvail. Zero-knowledge proofs and string commitments withstanding quantum attacks. In Matthew Franklin, editor, *CRYPTO 2004*, volume 3152 of *LNCS*, pages 254–272. Springer, Heidelberg, August 2004. (Cited on page 6.)

[DH76] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Trans. Inf. Theory*, 22(6):644–654, 1976. (Cited on page 2.)

[DMS00] Paul Dumais, Dominic Mayers, and Louis Salvail. Perfectly concealing quantum bit commitment from any quantum one-way permutation. In Bart Preneel, editor, *EUROCRYPT 2000*, volume 1807 of *LNCS*, pages 300–315. Springer, Heidelberg, May 2000. (Cited on page 4, 5, 9, 34, 35, 46.)

[ElG84] Taher ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In G. R. Blakley and David Chaum, editors, *CRYPTO'84*, volume 196 of *LNCS*, pages 10–18. Springer, Heidelberg, August 1984. (Cited on page 2.)

[FGS19] Vyacheslav Futorny, Joshua A. Grochow, and Vladimir V. Sergeichuk. Wildness for tensors. *Linear Algebra and its Applications*, 566:212–244, apr 2019. (Cited on page 4.)

[FUYZ20] Junbin Fang, Dominique Unruh, Jun Yan, and Dehua Zhou. How to base security on the perfect/statistical binding property of quantum bit commitment? Cryptology ePrint Archive, Report 2020/621, 2020. https://ia.cr/2020/621. (Cited on page 5, 8, 9.)

[GJMZ22] Sam Gunn, Nathan Ju, Fermi Ma, and Mark Zhandry. Commitments to quantum states. arXiv:2210.05138, 2022. (Cited on page 6.)

[GL89] Oded Goldreich and Leonid A. Levin. A hard-core predicate for all one-way functions. In *21st ACM STOC*, pages 25–32. ACM Press, May 1989. (Cited on page 1, 4, 35, 36, 46.)

[GMR84] Shafi Goldwasser, Silvio Micali, and Ronald L. Rivest. A "paradoxical" solution to the signature problem (extended abstract). In *25th FOCS*, pages 441–448. IEEE Computer Society Press, October 1984. (Cited on page 15.)

[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. (Cited on page 18.)

[GRS00] Oded Goldreich, Ronitt Rubinfeld, and Madhu Sudan. Learning polynomials with queries: The highly noisy case. *SIAM J. Discret. Math.*, 13(4):535–570, 2000. (Cited on page 36.)

[HILL99] Johan Håstad, Russell Impagliazzo, Leonid A. Levin, and Michael Luby. A pseudorandom generator from any one-way function. *SIAM J. Comput.*, 28(4):1364–1396, 1999. (Cited on page 2, 13, 32, 38, 48.)

[HM96] Shai Halevi and Silvio Micali. Practical and provably-secure commitment schemes from collision-free hashing. In Neal Koblitz, editor, *CRYPTO'96*, volume 1109 of *LNCS*, pages 201–215. Springer, Heidelberg, August 1996. (Cited on page 4, 38, 47, 48.)

[HMS04] Thomas Holenstein, Ueli M. Maurer, and Johan Sjödin. Complete classification of bilinear hard-core functions. In Matthew Franklin, editor, *CRYPTO 2004*, volume 3152 of *LNCS*, pages 73–91. Springer, Heidelberg, August 2004. (Cited on page 36.)

[HR07] Iftach Haitner and Omer Reingold. Statistically-hiding commitment from any one-way function. In David S. Johnson and Uriel Feige, editors, *39th ACM STOC*, pages 1–10. ACM Press, June 2007. (Cited on page 2.)

[HRV10] Iftach Haitner, Omer Reingold, and Salil P. Vadhan. Efficiency improvements in constructing pseudorandom generators from one-way functions. In Leonard J. Schulman, editor, *42nd ACM STOC*, pages 437–446. ACM Press, June 2010. (Cited on page 32, 38.)

[Imp95] Russell Impagliazzo. 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*, pages 134–147. IEEE Computer Society, 1995. (Cited on page 2.)

[JD11] David Jao and Luca De Feo. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In Bo-Yin Yang, editor, *Post-Quantum Cryptography - 4th International Workshop, PQCrypto 2011*, pages 19–34. Springer, Heidelberg, November / December 2011. (Cited on page 4.)

[JLS18] Zhengfeng Ji, Yi-Kai Liu, and Fang Song. Pseudorandom quantum states. In Hovav Shacham and Alexandra Boldyreva, editors, *CRYPTO 2018, Part III*, volume 10993 of *LNCS*, pages 126–152. Springer, Heidelberg, August 2018. (Cited on page 4, 14, 33.)

[JQSY19] Zhengfeng Ji, Youming Qiao, Fang Song, and Aaram Yun. General linear group action on tensors: A candidate for post-quantum cryptography. In Dennis Hofheinz and Alon Rosen, editors, *TCC 2019, Part I*, volume 11891 of *LNCS*, pages 251–281. Springer, Heidelberg, December 2019. (Cited on page 1, 2, 3, 4, 7, 8, 23, 24.)

[KKNY05] Akinori Kawachi, Takeshi Koshiba, Harumichi Nishimura, and Tomoyuki Yamakami. Computational indistinguishability between quantum states and its cryptographic application. In Ronald Cramer, editor, *EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 268–284. Springer, Heidelberg, May 2005. (Cited on page 5.)

[KO09] Takeshi Koshiba and Takanori Odaira. Statistically-hiding quantum bit commitment from approximable-preimage-size quantum one-way function. In Andrew M. Childs and Michele Mosca, editors, *Theory of Quantum Computation, Communication, and Cryptography, 4th Workshop, TQC 2009, Waterloo, Canada, May 11-13, 2009, Revised Selected Papers*, volume 5906 of *Lecture Notes in Computer Science*, pages 33–46. Springer, 2009. (Cited on page 5, 35.)

[KO11] Takeshi Koshiba and Takanori Odaira. Non-interactive statistically-hiding quantum bit commitment from any quantum one-way function. arXiv:1102.3441, 2011. (Cited on page 5, 32, 35.)

[Kre21] William Kretschmer. Quantum pseudorandomness and classical complexity. In Min-Hsiu Hsieh, editor, *16th Conference on the Theory of Quantum Computation, Communication and Cryptography, TQC 2021, July 5-8, 2021, Virtual Conference*, volume 197 of *LIPIcs*, pages 2:1–2:20. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021. (Cited on page 14.)

[LC97] Hoi-Kwong Lo and Hoi Fung Chau. Is quantum bit commitment really possible? *Physical Review Letters*, 78(17):3410, 1997. (Cited on page 2, 5.)

[Mah18] Urmila Mahadev. Classical homomorphic encryption for quantum circuits. In Mikkel Thorup, editor, *59th FOCS*, pages 332–338. IEEE Computer Society Press, October 2018. (Cited on page 7.)

[May97] Dominic Mayers. Unconditionally secure quantum bit commitment is impossible. *Physical review letters*, 78(17):3414, 1997. (Cited on page 2, 5.)

[MY22] Tomoyuki Morimae and Takashi Yamakawa. Quantum commitments and signatures without one-way functions. In *CRYPTO 2022*, 2022. (Cited on page 4, 5, 9, 13, 33, 34.)

[Nao91] Moni Naor. Bit commitment using pseudorandomness. *Journal of Cryptology*, 4(2):151–158, January 1991. (Cited on page 2, 32, 38.)

[OTU00] Tatsuaki Okamoto, Keisuke Tanaka, and Shigenori Uchiyama. Quantum public-key cryptosystems. In Mihir Bellare, editor, *CRYPTO 2000*, volume 1880 of *LNCS*, pages 147–165. Springer, Heidelberg, August 2000. (Cited on page 5.)

[Reg09] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *J. ACM*, 56(6):34:1–34:40, 2009. (Cited on page 18.)

[RS06] Alexander Rostovtsev and Anton Stolbunov. Public-key cryptosystem based on isogenies. Cryptology ePrint Archive, Paper 2006/145, 2006. https://eprint.iacr.org/2006/145. (Cited on page 2, 4.)

[Sho99] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Rev.*, 41(2):303–332, 1999. (Cited on page 4.)

[Unr12] Dominique Unruh. Quantum proofs of knowledge. In David Pointcheval and Thomas Johansson, editors, *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 135–152. Springer, Heidelberg, April 2012. (Cited on page 36.)

[Unr16a] Dominique Unruh. Collapse-binding quantum commitments without random oracles. In Jung Hee Cheon and Tsuyoshi Takagi, editors, *ASIACRYPT 2016, Part II*, volume 10032 of *LNCS*, pages 166–195. Springer, Heidelberg, December 2016. (Cited on page 13.)

[Unr16b] Dominique Unruh. Computationally binding quantum commitments. In Marc Fischlin and Jean-Sébastien Coron, editors, *EUROCRYPT 2016, Part II*, volume 9666 of *LNCS*, pages 497–527. Springer, Heidelberg, May 2016. (Cited on page 4, 6, 9, 13, 38, 47.)

[VZ12] Salil P. Vadhan and Colin Jia Zheng. Characterizing pseudoentropy and simplifying pseudorandom generator constructions. In Howard J. Karloff and Toniann Pitassi, editors, *44th ACM STOC*, pages 817–836. ACM Press, May 2012. (Cited on page 32, 38.)

[Yan21] Jun Yan. Quantum computationally predicate-binding commitments with application in quantum zero-knowledge arguments for NP. In Mehdi Tibouchi and Huaxiong Wang, editors, *ASIACRYPT 2021, Part I*, volume 13090 of *LNCS*, pages 575–605. Springer, Heidelberg, December 2021. (Cited on page 5, 6, 9.)

[Yan22] Jun Yan. General properties of quantum bit commitments. In *ASIACRYPT 2022*, 2022. (Cited on page 2, 3, 5, 6, 8, 9, 14, 32, 34, 46.)

[YWLQ15] Jun Yan, Jian Weng, Dongdai Lin, and Yujuan Quan. Quantum bit commitment with application in quantum zero-knowledge proof (extended abstract). In Khaled M. Elbassioni and Kazuhisa Makino, editors, *Algorithms and Computation - 26th International Symposium, ISAAC 2015, Nagoya, Japan, December 9-11, 2015, Proceedings*, volume 9472 of *Lecture Notes in Computer Science*, pages 555–565. Springer, 2015. (Cited on page 3, 5, 8, 9, 32.)

[Zha19] Mark Zhandry. Quantum lightning never strikes the same state twice. In Yuval Ishai and Vincent Rijmen, editors, *EUROCRYPT 2019, Part III*, volume 11478 of *LNCS*, pages 408–438. Springer, Heidelberg, May 2019. (Cited on page 3, 8, 17, 18.)

A Proof of Lemma 4.7

We give a proof of Lemma 4.7. Before giving the proof, we clarify definitions of terms that appear in the statement of the lemma. First, we define (infinitely-often) uniform conversion hardness for group actions.

Definition A.1 ((Infinitely-often) uniform conversion hardness). *We say that an STF* $(\mathsf{Setup}, \mathsf{Eval}, \mathsf{Swap})$ *is uniform conversion hard if for any uniform QPT adversary* $\mathcal{A}$*, we have*

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

We say that it is infinitely-often uniform conversion hard if the above holds for infinitely many security parameters $\lambda \in \mathbb{N}$.

Next, we define (infinitely-often) one-shot signatures. We focus on the case of single-bit messages for simplicity. The message space can be extended to multiple bits by a simple parallel repetition as shown in [AGKZ20].

Definition A.2 (One-shot signatures). *A one-shot signature scheme consists of algorithms* $(\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Vrfy})$.

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

$\mathsf{KeyGen}(\mathsf{pp}) \to (\mathsf{vk}, \mathit{sk})$**:** *This is a QPT algorithm that takes a public parameter* pp *as input, and outputs a classical verification key* vk *and a quantum signing key* sk.

$\mathsf{Sign}(\mathsf{pp}, \mathit{sk}, b) \to \sigma$**:** *This is a QPT algorithm that takes a public parameter* pp*, a signing key* sk *and a message* $b \in \{0,1\}$ *as input, and outputs a classical signature* σ.

$\mathsf{Vrfy}(\mathsf{pp}, \mathsf{vk}, b, \sigma) \to \top/\bot$**:** *This is a PPT algorithm that takes a public parameter* pp*, a verification key* vk*, a message* b*, and a signature* σ *as input, and outputs the decision* $\top$ *or* $\bot$.

We require a one-shot signature scheme to satisfy the following properties.

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

$$\Pr\left[\mathsf{Vrfy}(\mathsf{pp}, \mathsf{vk}, b, \sigma) \to \top : \mathsf{pp} \leftarrow \mathsf{Setup}(1^\lambda), (\mathsf{pk}, \mathit{sk}) \leftarrow \mathsf{KeyGen}(\mathsf{pp}), \sigma \leftarrow \mathsf{Sign}(\mathsf{pp}, \mathit{sk}, b)\right] = 1 - \mathsf{negl}(\lambda).$$

(Infinitely-often) Security. *We say that a one-shot signature scheme is secure if for any non-uniform QPT adversary* $\mathcal{A}$*, we have*

$$\Pr\left[\forall b \in \{0,1\}\ \mathsf{Vrfy}(\mathsf{pp}, \mathsf{vk}, b, \sigma_b) = \top : \mathsf{pp} \leftarrow \mathsf{Setup}(1^\lambda), (\mathsf{vk}, \sigma_0, \sigma_1) \leftarrow \mathcal{A}(\mathsf{pp})\right] = \mathsf{negl}(\lambda).$$

We say that it is infinitely-often secure if the above holds for infinitely many security parameters $\lambda \in \mathbb{N}$.

Then, we give a proof of Lemma 4.7.

Proof of Lemma 4.7. Since the proof is almost identical for both Items 1 and 2, we first prove Item 1 and then explain how to modify it to prove Item 2.

Proof of Item 1. Let $(\mathsf{Setup}, \mathsf{Eval}, \mathsf{Swap})$ be an STF that is claw-free but not infinitely-often uniform conversion hard. Then, there is a uniform QPT algorithm $\mathcal{A}$ and a polynomial poly such that

$$\Pr[f_1(x_1) = y : (\mathsf{pp}, \mathsf{td}) \leftarrow \mathsf{Setup}(1^\lambda), x_0 \leftarrow \mathcal{X}, y := f_0(x_0), x_1 \leftarrow \mathcal{A}(\mathsf{pp}, |f_0^{-1}(y)\rangle)] > 1/\mathrm{poly}(\lambda) \tag{25}$$

for all λ. Then, we construct a one-shot signature scheme as follows. Let $N := \mathrm{poly}(\lambda) \cdot \lambda$.

$\mathsf{Setup}(1^\lambda)$**:** For $i \in [N]$, generate $(\mathsf{pp}_i, \mathsf{td}_i) \leftarrow \mathsf{Setup}(1^\lambda)$, and output $\mathsf{pp} := \{\mathsf{pp}_i\}_{i\in[N]}$. We write $f_{i,0}$ and $f_{i,1}$ to mean $f_0^{(\mathsf{pp}_i)}$ and $f_1^{(\mathsf{pp}_i)}$, respectively.

$\mathsf{KeyGen}(\mathsf{pp})$**:** Given $\mathsf{pp} = \{\mathsf{pp}_i\}_{i\in[N]}$, for $i \in [N]$, generate

$$|\mathcal{X}\rangle = \frac{1}{|\mathcal{X}|^{1/2}} \sum_{x\in\mathcal{X}} |x\rangle\,,$$

coherently compute $f_{i,0}$ in another register to get

$$|\mathcal{X}\rangle = \frac{1}{|\mathcal{X}|^{1/2}} \sum_{x\in\mathcal{X}} |x\rangle\,|f_{i,0}(x)\rangle\,,$$

measure the second register to get y_i. At this point, the first register collapses to $|f_{i,0}^{-1}(y_i)\rangle$. Output $\mathsf{vk} := \{y_i\}_{i\in[N]}$ and $\mathsf{sk} := \{y_i, |f_{i,0}^{-1}(y_i)\rangle\}_{i\in[N]}$.

$\mathsf{Sign}(\mathsf{pp}, \mathsf{sk}, b) \to \sigma$**:** Given $\mathsf{pp} = \{\mathsf{pp}_i\}_{i\in[N]}$, $\mathsf{sk} = \{y_i, |f_{i,0}^{-1}(y_i)\rangle\}_{i\in[N]}$, and $b \in \{0,1\}$, do the following.

- If $b = 0$, for $i \in [N]$, measure $|f_{i,0}^{-1}(y_i)\rangle$ to get $x_i \in f_{i,0}^{-1}(y_i)$ and output $\sigma := \{x_i\}_{i\in[N]}$.
- If $b = 1$, for $i \in [N]$, run $\mathcal{A}(\mathsf{pp}_i, |f_{i,0}^{-1}(y_i)\rangle)$ to get x'_i. If $f_{i,1}(x'_i) \neq y_i$ for all $i \in [N]$, it aborts. Otherwise, it outputs $\sigma := (i^*, x'_{i^*})$ where i^* is the smallest index such that $f_{i^*,1}(x'_{i^*}) = y_{i^*}$.

$\mathsf{Vrfy}(\mathsf{pp}, \mathsf{vk}, b, \sigma) \to \top/\bot$**:** Given $\mathsf{pp} = \{\mathsf{pp}_i\}_{i\in[N]}$, $\mathsf{vk} = \{y_i\}_{i\in[N]}$, $b \in \{0,1\}$, and a signature σ, do the following.

- If $b = 0$, parse $\sigma = \{x_i\}_{i\in[N]}$, and output $\top$ if $f_{i,0}(x_i) = y_i$ for all $i \in [N]$ and $\bot$ otherwise.
- If $b = 1$, parse $\sigma = (i, x'_i)$, and output $\top$ if $f_{i,1}(x'_i) = y_i$ and $\bot$ otherwise.

Correctness. It is easy to see that the signing algorithm outputs a valid signature whenever it does not abort. By Equation (25), the probability that the signing algorithm abort (when $b = 1$) is

$$(1 - 1/\mathrm{poly})^N = \mathsf{negl}(\lambda)$$

by $N = \mathrm{poly}(\lambda) \cdot \lambda$.

Security. Suppose that there is a non-uniform QPT adversary that breaks the above one-shot signature scheme. The adversary is given $\mathsf{pp} = \{\mathsf{pp}_i\}_{i\in[N]}$ and finds $\mathsf{vk} = \{y_i\}_{i\in[N]}$, $\sigma_0 = \{x_i\}_{i\in[N]}$, and $\sigma_1 = (i^*, x'_{i^*})$ such that $f_{i,0}(x_i) = y_i$ for all $i \in [N]$ and $f_{i^*,1}(x'_{i^*}) = y_{i^*}$ with a non-negligible probability. In particular, when the above happens, (x_{i^*}, x'_{i^*}) forms a claw, i.e., we have $f_{i^*,0}(x_{i^*}) = f_{i^*,1}(x'_{i^*})$. Thus, by randomly guessing i^* and embedding a problem instance of the claw-freeness into the i^*-th coordinate, we can break the claw-freeness of the STF $(\mathsf{Setup}, \mathsf{Eval}, \mathsf{Swap})$, which is a contradiction. Thus, the above one-shot signature scheme is secure.

This completes the proof of Item 1.

Proof of Item 2. The proof is similar to that of Item 1. The difference is that since we only assume the STF is not uniform conversion hard, we can only assume that Equation (25) holds for infinitely many λ rather than all λ. In this case, the correctness of the above one-shot signature scheme only holds for infinitely many λ. To deal with this, we modify the verification algorithm so that it approximates $\mathcal{A}$'s success probability up to additive error $1/(4\mathrm{poly}(\lambda))$ (except for a negligible probability) and simply accepts if the approximated success probability is smaller than $1/(2\mathrm{poly}(\lambda))$. Then, the correctness holds on all $\lambda \in \mathbb{N}$ because

- if the real success probability is smaller than $1/(4\mathrm{poly}(\lambda))$, the estimated success probability is smaller than $1/(2\mathrm{poly}(\lambda))$ with overwhelming probability, and thus the verification algorithm accepts with overwhelming probability on these security parameters, and
- if the real success probability is larger than $1/(4\mathrm{poly}(\lambda))$, the signing algorithm should succeed in generating a valid proof with overwhelming probability and thus the verification algorithm accepts with overwhelming probability on these security parameters.

For the security, we observe that the estimated success probability is smaller than $1/(2\mathrm{poly}(\lambda))$ with a negligible probability when the real success probability is larger than $1/\mathrm{poly}(\lambda)$. Thus, for those security parameters, the adversary should find valid signatures in the original scheme. Since there are infinitely many such λ, this is not possible by the claw-freeness of the STF. □

B More Applications of Our Conversion

B.1 Construction from One-Way Permutations via Dumais-Mayers-Salvail Commitment

Dumais, Mayers and Salvail [DMS00] constructed a perfectly hiding and computationally binding commitment from one-way permutations as follows.[38] Let $f : \{0,1\}^n \to \{0,1\}^n$ be a one-way permutation. Then, we define a canonical quantum bit commitment scheme $\{Q_{\mathsf{DMS},0}, Q_{\mathsf{DMS},1}\}$ as follows:

$$Q_{\mathsf{DMS},b} |0\rangle_{\mathbf{C},\mathbf{R}} := \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} ((H^b)^{\otimes n} |f(x)\rangle)_{\mathbf{C}} |x\rangle_{\mathbf{R}} .$$

Theorem B.1 ([DMS00]). *If f is a one-way permutation, $\{Q_{\mathsf{DMS},0}, Q_{\mathsf{DMS},1}\}$ is perfectly hiding and computationally binding.*

By applying our conversion to $\{Q_{\mathsf{DMS},0}, Q_{\mathsf{DMS},1}\}$, we obtain the following scheme $\{Q'_{\mathsf{DMS},0}, Q'_{\mathsf{DMS},1}\}$:

$$Q'_{\mathsf{DMS},b} |0\rangle_{\mathbf{C}',\mathbf{R}'} := \frac{1}{\sqrt{2^{n+1}}} \left(\sum_{x\in\{0,1\}^n} \left(|0,x\rangle_{\mathbf{C}'} |f(x)\rangle_{\mathbf{R}'} + (-1)^b |1,x\rangle_{\mathbf{C}'} (H^{\otimes n} |f(x)\rangle)_{\mathbf{R}'} \right) \right) .$$

By Theorem B.1 and Theorem 6.1, we obtain the following theorem.

Theorem B.2. *If f is a one-way permutation, $\{Q'_{\mathsf{DMS},0}, Q'_{\mathsf{DMS},1}\}$ is computationally hiding and perfectly binding.*

B.2 Constructions from Injective One-Way Functions via Goldreich-Levin Theorem

Goldreich and Levin [GL89] showed that for any one-way function $f : \{0,1\}^n \to \{0,1\}^m$, $r \cdot x$ is computationally indistinguishable from a uniform bit given $(f(x), r)$ for $x, r \xleftarrow{\$} \{0,1\}^n$. Here, $r \cdot x := \sum_{i\in\{0,1\}^n} r_i x_i \mod 2$ where r_i and x_i are the i-th bits of r and x, respectively. It is well-known that the above theorem gives us a simple *classical* non-interactive commitment scheme that is computationally hiding and perfectly binding from any injective one-way function: Let $f : \{0,1\}^n \to \{0,1\}^m$ be an injective one-way function. Then, a commitment to bit $b \in \{0,1\}$ is set to be $(f(x), r, r \cdot x \oplus b)$. By purifying this construction, we obtain the following canonical quantum bit commitment scheme $\{Q_{\mathsf{GL},0}, Q_{\mathsf{GL},1}\}$:

$$Q_{\mathsf{GL},b} |0\rangle_{\mathbf{C},\mathbf{R}} := \frac{1}{2^n} \sum_{x\in\{0,1\}^n, r\in\{0,1\}^n} |f(x), r, r \cdot x \oplus b\rangle_{\mathbf{C}} |x, r\rangle_{\mathbf{R}} .$$

By Goldreich-Levin theorem (or its quantum version with a better reduction loss shown by Adcock and Cleve [AC02]), it is straightforward to prove the following theorem.

[38] We describe it in the canonical form as in [Yan22, Section 5].

Theorem B.3. *If f is an injective one-way function, $\{Q_{\mathsf{GL},0}, Q_{\mathsf{GL},1}\}$ is computationally hiding and perfectly binding.*

By applying our conversion to $\{Q_{\mathsf{GL},0}, Q_{\mathsf{GL},1}\}$, we obtain the following scheme $\{Q'_{\mathsf{GL},0}, Q'_{\mathsf{GL},1}\}$.

$$Q'_{\mathsf{GL},b}\left|0\right\rangle_{\mathbf{C}',\mathbf{R}'} := \frac{1}{2^n}\sum_{x\in\{0,1\}^n, r\in\{0,1\}^n}\left(\left|0,x,r\right\rangle_{\mathbf{C}'}\left|f(x),r,r\cdot x\right\rangle_{\mathbf{R}'} + (-1)^b\left|1,x,r\right\rangle_{\mathbf{C}'}\left|f(x),r,r\cdot x\oplus 1\right\rangle_{\mathbf{R}'}\right).$$

By Theorems 6.1 and B.3, we obtain the following theorem.

Theorem B.4. *If f is an injective one-way function, $\{Q'_{\mathsf{GL},0}, Q'_{\mathsf{GL},1}\}$ is perfectly hiding and computationally binding.*

Construction from injective one-way functions with trusted setup.

Similarly to the schemes in Section 7.3, the above schemes work based on injective one-way functions with trusted setup. Let $\mathcal{R}$ be the randomness space for the setup and f_R be the (description of) injective one-way function generated from the randomness $R\in\mathcal{R}$. Then, we construct a modified scheme $\{Q_{\mathsf{GL\text{-}setup},0}, Q_{\mathsf{GL\text{-}setup},1}\}$:

$$Q_{\mathsf{GL\text{-}setup},b}\left|0\right\rangle_{\mathbf{C},\mathbf{R}} := \frac{1}{2^n\sqrt{|\mathcal{R}|}}\sum_{x\in\{0,1\}^n, r\in\{0,1\}^n, R\in\mathcal{R}}\left|f_R(x),r,r\cdot x\oplus b,R\right\rangle_{\mathbf{C}}\left|x,r,R\right\rangle_{\mathbf{R}}.$$

It is easy to show that $\{Q_{\mathsf{GL\text{-}setup},0}, Q_{\mathsf{GL\text{-}setup},1}\}$ is computationally hiding and perfectly binding. By applying our conversion to $\{Q_{\mathsf{GL\text{-}setup},0}, Q_{\mathsf{GL\text{-}setup},1}\}$, we obtain the following scheme $\{Q'_{\mathsf{GL\text{-}setup},0}, Q'_{\mathsf{GL\text{-}setup},1}\}$:

$$\begin{aligned}Q'_{\mathsf{GL\text{-}setup},b}\left|0\right\rangle_{\mathbf{C}',\mathbf{R}'} := \frac{1}{2^n\sqrt{|\mathcal{R}|}}\sum_{x\in\{0,1\}^n, r\in\{0,1\}^n, R\in\mathcal{R}}\Big(&\left|0,x,r,R\right\rangle_{\mathbf{C}'}\left|f_R(x),r,r\cdot x,R\right\rangle_{\mathbf{R}'}\\ &+(-1)^b\left|1,x,r,R\right\rangle_{\mathbf{C}'}\left|f_R(x),r,r\cdot x\oplus 1,R\right\rangle_{\mathbf{R}'}\Big).\end{aligned}$$

By Theorem 6.1, $\{Q'_{\mathsf{GL\text{-}setup},0}, Q'_{\mathsf{GL\text{-}setup},1}\}$ is perfectly hiding and computationally binding.

B.3 Construction from Collapsing Hash Functions via Halevi-Micali Commitments

Halevi and Micali [HM96] constructed a two-message statistically hiding and computationally binding commitment scheme from any collision-resistant hash functions in the classical setting. Unruh [Unr16b] pointed out that the scheme may not be secure against quantum adversaries, and showed that it is secure if we assume a stronger security than the collision-resistance called *collapsing* property Definition 3.4.

In this section, we consider the canonical form of the scheme of [HM96] and show that it is statistically hiding and computationally binding assuming the collapsing hash functions. Then, we convert it into computationally hiding and statistically binding one by our conversion.

Preparation. Before describing the canonical form of the scheme of [HM96], we define universal functions and the leftover hash lemma.

Definition B.5 (Universal functions.). *A polynomial-time computable function family $\mathcal{F} = \{f_k : \{0,1\}^L \to \{0,1\}^\ell\}_{k\in\mathcal{K}_\mathcal{F}}$ is universal if for any $x, x' \in \{0,1\}^L$ such that $x\neq x'$, we have*

$$\Pr_{k\leftarrow\mathcal{K}_\mathcal{F}}[f_k(x) = f_k(x')] = 2^{-\ell}.$$

For any polynomials L, ℓ in the security parameter, there unconditionally exists a universal function family from $\{0,1\}^L$ to $\{0,1\}^\ell$ [CW79, HILL99].

Lemma B.6 (Leftover hash lemma [HILL99]). *Let $\mathcal{F} = \{f_k : \{0,1\}^L \to \{0,1\}^\ell\}_{k\in\mathcal{K}_\mathcal{F}}$ be a universal function family. Let X be a random variable over $\{0,1\}^L$ such that $H_\infty(X) \geq \ell + 2\log\epsilon^{-1}$ where $H_\infty(X) := -\log\max_{x\in\{0,1\}^L}\Pr[X=x]$. Then, we have*

$$\Delta((k, f_k(X)), (k, U_\ell)) \leq \epsilon$$

where Δ denotes the statistical distance, $k \leftarrow \mathcal{K}$, and $U_\ell \leftarrow \{0,1\}^\ell$.

Construction. Let $\mathcal{H} = \{H_k : \{0,1\}^L \to \{0,1\}^\ell\}_{k\in\mathcal{K}_\mathcal{H}}$ be a collapsing function family and $\mathcal{F} = \{f_{k'} : \{0,1\}^L \to \{0,1\}\}_{k'\in\mathcal{K}_\mathcal{F}}$ be a universal function family where $L = \ell + 2\lambda + 1$. The canonical form of the scheme of [HM96] $\{Q_{\mathsf{HM},0}, Q_{\mathsf{HM},1}\}$ is described as follows:

$$Q_{\mathsf{HM},b}\left|0\right\rangle_{\mathbf{C},\mathbf{R}} := \frac{1}{\sqrt{2^L|\mathcal{K}_\mathcal{H}||\mathcal{K}_\mathcal{F}|}}\sum_{k\in\mathcal{K}_\mathcal{H},k'\in\mathcal{K}_\mathcal{F},x\in\{0,1\}^L}\left|k,k',H_k(x),f_{k'}(x)\oplus b\right\rangle_\mathbf{C}\left|k,k',x\right\rangle_\mathbf{R}$$

Theorem B.7. *$\{Q_{\mathsf{HM},0}, Q_{\mathsf{HM},1}\}$ is statistically hiding and computationally binding.*

Proof.

Hiding. For $b \in \{0,1\}$, we have

$$\begin{aligned}&\mathrm{Tr}_\mathbf{R}(Q_{\mathsf{HM},b}\left|0\right\rangle_{\mathbf{C},\mathbf{R}})\\ &= \frac{1}{2^L|\mathcal{K}_\mathcal{H}||\mathcal{K}_\mathcal{F}|}\sum_{k\in\mathcal{K}_\mathcal{H},k'\in\mathcal{K}_\mathcal{F},x\in\{0,1\}^L}\left|k,k',H_k(x),f_{k'}(x)\oplus b\right\rangle_\mathbf{C}\left\langle k,k',H_k(x),f_{k'}(x)\oplus b\right|_\mathbf{C}\end{aligned}$$

Thus, breaking the hiding property is equivalent to distinguishing the classical distributions $\{(k,k',H_k(x),f_{k'}(x)\oplus b) : k\leftarrow\mathcal{K}_\mathcal{H}, k'\leftarrow\mathcal{K}_\mathcal{F}, x\leftarrow\{0,1\}^L\}$ for $b=0,1$. For any fixed $k\in\mathcal{K}_\mathcal{H}$ and $y\in\{0,1\}^\ell$, let $X_{k,y}$ be the conditional distribution of $x\leftarrow\{0,1\}^L$ conditioned on $H_k(x)=y$. Since ℓ-bit side information can decrease the min-entropy by at most ℓ, we have $H_\infty(X_{k,y}) \geq L-\ell = 2\lambda+1$. Thus, by the leftover hash lemma (Lemma B.6), for any fixed k, we have

$$\Delta((k,k',H_k(x),f_{k'}(x)),(k,k',H_k(x),U_1)) \leq 2^{-\lambda}$$

where $k'\leftarrow\mathcal{K}_\mathcal{F}$, $x\leftarrow\{0,1\}^L$, and $U_1\leftarrow\{0,1\}$. Combined with the above observation, this implies that $\{Q_{\mathsf{HM},0}, Q_{\mathsf{HM},1}\}$ is statistically hiding.

Binding. Suppose that the $\{Q_{\mathsf{HM},0}, Q_{\mathsf{HM},1}\}$ is not computationally binding. Then there exists a polynomial-time computable unitary U over $(\mathbf{R},\mathbf{Z})$ and a auxiliary state $\left|\tau\right\rangle_\mathbf{Z}$ such that

$$\left\|(Q_{\mathsf{HM},1}\left|0\right\rangle\left\langle 0\right|Q_{\mathsf{HM},1}^\dagger)_{\mathbf{C},\mathbf{R}}(I_\mathbf{C}\otimes U_{\mathbf{R},\mathbf{Z}})((Q_{\mathsf{HM},0}\left|0\right\rangle)_{\mathbf{C},\mathbf{R}}\left|\tau\right\rangle_\mathbf{Z})\right\|$$

is non-negligible. In particular, its square is also non-negligible.

Let $\mathbf{R}_\mathsf{K}$ and $\mathbf{R}_\mathsf{X}$ be sub-registers of $\mathbf{R}$ that store (k,k') and x, respectively. For $k\in\mathcal{K}_\mathcal{H}$, $k'\in\mathcal{K}_\mathcal{F}$, $y\in\{0,1\}^\ell$, and $z\in\{0,1\}$, we define a subset $S_{k,k',y,z}\subseteq\{0,1\}^L$ as

$$S_{k,k',y,z} := \{x\in\{0,1\}^L : H_k(x)=y \ \wedge\ f_{k'}(x)=z\}$$

and define the state $|S_{k,k',y,z}\rangle_{\mathbf{R}_\mathsf{X}}$ as

$$|S_{k,k',y,z}\rangle_{\mathbf{R}_\mathsf{X}} := \frac{1}{\sqrt{|S_{k,k',y,z}|}} \sum_{x \in S_{k,k',y,z}} |x\rangle_{\mathbf{R}_\mathsf{X}}.$$

For notational convenience, we also define a (non-normalized) state $|\widetilde{S}_{k,k',y,z}\rangle_{\mathbf{R}_\mathsf{X}}$ as

$$|\widetilde{S}_{k,k',y,z}\rangle_{\mathbf{R}_\mathsf{X}} := \sqrt{|S_{k,k',y,z}|}\,|S_{k,k',y,z}\rangle_{\mathbf{R}_\mathsf{X}} = \sum_{x \in S_{k,k',y,z}} |x\rangle_{\mathbf{R}_\mathsf{X}}.$$

Clearly, for any $k \in \mathcal{K}_\mathcal{H}$ and $k' \in \mathcal{K}_\mathcal{F}$, we have

$$\sum_{y \in \{0,1\}^\ell, z \in \{0,1\}} |S_{k,k',y,z}| = 2^L. \tag{26}$$

Then, it holds that

$$\begin{aligned}
&\left\|(Q_{\mathsf{HM},1}|0\rangle\langle 0|Q_{\mathsf{HM},1}^\dagger)_{\mathbf{C},\mathbf{R}}(I_\mathbf{C}\otimes U_{\mathbf{R},\mathbf{Z}})((Q_{\mathsf{HM},0}|0\rangle)_{\mathbf{C},\mathbf{R}}|\tau\rangle_\mathbf{Z})\right\|^2 \\
=&\frac{1}{(2^L|\mathcal{K}_\mathcal{H}||\mathcal{K}_\mathcal{F}|)^2}\left\|\sum_{\substack{k\in\mathcal{K}_\mathcal{H},k'\in\mathcal{K}_\mathcal{F},\\ y\in\{0,1\}^\ell,z\in\{0,1\}}} \langle k,k'|_{\mathbf{R}_\mathsf{K}}\langle\widetilde{S}_{k,k',y,z\oplus 1}|_{\mathbf{R}_\mathsf{X}} U_{\mathbf{R},\mathbf{Z}}|k,k'\rangle_{\mathbf{R}_\mathsf{K}}|\widetilde{S}_{k,k',y,z}\rangle_{\mathbf{R}_\mathsf{X}}|\tau\rangle_\mathbf{Z}\right\|^2 \\
\le&\frac{1}{(2^L|\mathcal{K}_\mathcal{H}||\mathcal{K}_\mathcal{F}|)^2}\left\|\sum_{\substack{k\in\mathcal{K}_\mathcal{H},k'\in\mathcal{K}_\mathcal{F},\\ y\in\{0,1\}^\ell,z\in\{0,1\}}} \langle\widetilde{S}_{k,k',y,z\oplus 1}|_{\mathbf{R}_\mathsf{X}} U_{\mathbf{R},\mathbf{Z}}|k,k'\rangle_{\mathbf{R}_\mathsf{K}}|\widetilde{S}_{k,k',y,z}\rangle_{\mathbf{R}_\mathsf{X}}|\tau\rangle_\mathbf{Z}\right\|^2 \\
=&\frac{1}{(2^L|\mathcal{K}_\mathcal{H}||\mathcal{K}_\mathcal{F}|)^2}\left\|\sum_{\substack{k\in\mathcal{K}_\mathcal{H},k'\in\mathcal{K}_\mathcal{F},\\ y\in\{0,1\}^\ell,z\in\{0,1\}}}\sum_{x\in S_{k,k',y,z\oplus 1}} \langle x|_{\mathbf{R}_\mathsf{X}} U_{\mathbf{R},\mathbf{Z}}|k,k'\rangle_{\mathbf{R}_\mathsf{K}}|\widetilde{S}_{k,k',y,z}\rangle_{\mathbf{R}_\mathsf{X}}|\tau\rangle_\mathbf{Z}\right\|^2 \\
\le&\frac{1}{(2^L|\mathcal{K}_\mathcal{H}||\mathcal{K}_\mathcal{F}|)^2}\left(\sum_{\substack{k\in\mathcal{K}_\mathcal{H},k'\in\mathcal{K}_\mathcal{F},\\ y\in\{0,1\}^\ell,z\in\{0,1\}}}\sum_{x\in S_{k,k',y,z\oplus 1}} \left\|\langle x|_{\mathbf{R}_\mathsf{X}} U_{\mathbf{R},\mathbf{Z}}|k,k'\rangle_{\mathbf{R}_\mathsf{K}}|\widetilde{S}_{k,k',y,z}\rangle_{\mathbf{R}_\mathsf{X}}|\tau\rangle_\mathbf{Z}\right\|\right)^2 \\
\le&\frac{1}{2^L|\mathcal{K}_\mathcal{H}||\mathcal{K}_\mathcal{F}|}\sum_{\substack{k\in\mathcal{K}_\mathcal{H},k'\in\mathcal{K}_\mathcal{F},\\ y\in\{0,1\}^\ell,z\in\{0,1\}}}\sum_{x\in S_{k,k',y,z\oplus 1}} \left\|\langle x|_{\mathbf{R}_\mathsf{X}} U_{\mathbf{R},\mathbf{Z}}|k,k'\rangle_{\mathbf{R}_\mathsf{K}}|\widetilde{S}_{k,k',y,z}\rangle_{\mathbf{R}_\mathsf{X}}|\tau\rangle_\mathbf{Z}\right\|^2 \\
\le&\frac{1}{|\mathcal{K}_\mathcal{H}||\mathcal{K}_\mathcal{F}|}\sum_{\substack{k\in\mathcal{K}_\mathcal{H},k'\in\mathcal{K}_\mathcal{F},\\ y\in\{0,1\}^\ell,z\in\{0,1\}}}\frac{|S_{k,k',y,z}|}{2^L}\sum_{x\in S_{k,k',y,z\oplus 1}} \left\|\langle x|_{\mathbf{R}_\mathsf{X}} U_{\mathbf{R},\mathbf{Z}}|k,k'\rangle_{\mathbf{R}_\mathsf{K}}|S_{k,k',y,z}\rangle_{\mathbf{R}_\mathsf{X}}|\tau\rangle_\mathbf{Z}\right\|^2
\end{aligned} \tag{27}$$

where the first equality follows from the definition of $\{Q_{\mathsf{HM},0}, Q_{\mathsf{HM},1}\}$, the second equality follows from the definition of $|\widetilde{S}_{k,k',y,z\oplus 1}\rangle_{\mathbf{R}_\mathsf{X}}$, the second inequality follows from the triangle inequality, the third inequality

follows from the Cauchy–Schwarz inequality and Equation (26), and the fourth inequality follows from $L \geq \ell + 1$. Therefore, the value of Equation (27) is non-negligible.

Below, we give an algorithmic interpretation for the value of Equation (27). Let $\mathcal{A}$ be an algorithm that works as follows with advice $|\tau\rangle$.

$\mathcal{A}(k, k'; |\tau\rangle)$**:** Given $k \in \mathcal{K}_{\mathcal{H}}$ and $k' \in \mathcal{K}_{\mathcal{F}}$ as input and advice $|\tau\rangle$, it generates a state

$$\sum_{x \in \{0,1\}^L} |x\rangle_{\mathbf{R}_{\mathsf{X}}} |H_k(x), f_{k'}(x)\rangle_{\mathbf{A}}$$

where $\mathbf{A}$ is an additional register and measures $\mathbf{A}$. Let (y, z) be the outcome. At this point, the state in $\mathbf{R}_{\mathsf{X}}$ collapses to $|S_{k,k',y,z}\rangle_{\mathbf{R}_{\mathsf{X}}}$. Then, it computes $U_{\mathbf{R},\mathbf{Z}} |k, k'\rangle_{\mathbf{R}_{\mathsf{K}}} |S_{k,k',y,z}\rangle_{\mathbf{R}_{\mathsf{X}}} |\tau\rangle_{\mathbf{Z}}$ and measures $\mathbf{R}_{\mathsf{X}}$. Let x be the outcome. If $x \in S_{k,k',y,z\oplus 1}$, then it outputs 1. Otherwise, it outputs 0.

The probability that the measurement outcome of $\mathbf{A}$ by $\mathcal{A}$ is (y, z) is $\frac{|S_{k,k',y,z}|}{2^L}$. Therefore, $\Pr_{k \xleftarrow{\$} \mathcal{K}_{\mathcal{H}}, k' \xleftarrow{\$} \mathcal{K}_{\mathcal{F}}}[\mathcal{A}(k, k'; |\tau\rangle) = 1]$ is exactly the value of Equation (27), which is non-negligible.

Next, we consider a modified algorithm $\mathcal{A}'$ that works similarly to $\mathcal{A}$ except that it measures $\mathbf{R}_{\mathsf{X}}$ before applying $U_{\mathbf{R},\mathbf{Z}}$. Equivalently, instead of generating the state $\sum_{x \in \{0,1\}^L} |x\rangle_{\mathbf{R}_{\mathsf{X}}} |H_k(x), f_{k'}(x)\rangle_{\mathbf{A}}$, $\mathcal{A}'$ classically samples $x \xleftarrow{\$} \{0,1\}^L$, computes $y := H_k(x)$ and $z := f_{k'}(y)$ and uses $|x\rangle_{\mathbf{R}_{\mathsf{X}}}$ instead of $|S_{k,k',y,z}\rangle_{\mathbf{R}_{\mathsf{X}}}$. By a straightforward reduction to the collapsing property of $\mathcal{H}$,

$$\left| \Pr_{k \xleftarrow{\$} \mathcal{K}_{\mathcal{H}}, k' \xleftarrow{\$} \mathcal{K}_{\mathcal{F}}}[\mathcal{A}'(k, k'; |\tau\rangle) = 1] - \Pr_{k \xleftarrow{\$} \mathcal{K}_{\mathcal{H}}, k' \xleftarrow{\$} \mathcal{K}_{\mathcal{F}}}[\mathcal{A}(k, k'; |\tau\rangle) = 1] \right| = \mathsf{negl}(\lambda).$$

Therefore, $\Pr_{k \xleftarrow{\$} \mathcal{K}_{\mathcal{H}}, k' \xleftarrow{\$} \mathcal{K}_{\mathcal{F}}}[\mathcal{A}'(k, k'; |\tau\rangle) = 1]$ is non-negligible.

By using the above, we construct a non-uniform QPT algorithm $\mathcal{B}$ that breaks the collision-resistance of $\mathcal{H}$ as follows.

$\mathcal{B}(k; |\tau\rangle)$**:** Given an input $k \in \mathcal{K}_{\mathcal{H}}$ and advice $|\tau\rangle$, it picks $k' \xleftarrow{\$} \mathcal{K}_{\mathcal{F}}$ and $x \xleftarrow{\$} \{0,1\}^N$. It computes $U_{\mathbf{R},\mathbf{Z}} |k, k'\rangle_{\mathbf{R}_{\mathsf{K}}} |x\rangle_{\mathbf{R}_{\mathsf{X}}} |\tau\rangle_{\mathbf{Z}}$ and measures $\mathbf{R}_{\mathsf{X}}$. Let x' be the outcome. It outputs (x, x').

It is easy to see that

$$\Pr_{k \xleftarrow{\$} \mathcal{K}_{\mathcal{H}}}[x' \in S_{k,k',H_k(x),f_{k'}(x)\oplus 1} : (x, x') \xleftarrow{\$} \mathcal{B}(k; |\tau\rangle)] = \Pr_{k \xleftarrow{\$} \mathcal{K}_{\mathcal{H}}, k' \xleftarrow{\$} \mathcal{K}_{\mathcal{F}}}[\mathcal{A}'(k, k'; |\tau\rangle) = 1]$$

where k' in the LHS is the one picked by $\mathcal{B}$. Since the RHS is non-negligible, the LHS is non-negligible. Moreover, when $x' \in S_{k,k',H_k(x),f_{k'}(x)\oplus 1}$, we have $H_k(x) = H_k(x')$ and $x \neq x'$ by the definition of $S_{k,k',H_k(x),f_{k'}(x)\oplus 1}$. Therefore,

$$\Pr_{k \xleftarrow{\$} \mathcal{K}_{\mathcal{H}}}[H_k(x) = H_k(x') \ \wedge \ x \neq x' : (x, x') \xleftarrow{\$} \mathcal{B}(k; |\tau\rangle)]$$

is non-negligible. This means that $\mathcal{B}$ with advice $|\tau\rangle$ breaks the collision-resistance of $\mathcal{H}$. This contradicts the assumption that $\mathcal{H}$ is collapsing since the collapsing property implies the collision-resistance. Thus, $\{Q_{\mathsf{HM},0}, Q_{\mathsf{HM},1}\}$ is computationally binding. This completes the proof of Theorem B.7. □

By applying our conversion, we obtain the following scheme $\{Q'_{\mathsf{HM},0}, Q'_{\mathsf{HM},1}\}$

$$Q'_{\mathsf{HM},b}\left|0\right\rangle_{\mathbf{C}',\mathbf{R}'} := \frac{1}{\sqrt{2^{L+1}|\mathcal{K}_{\mathcal{H}}||\mathcal{K}_{\mathcal{F}}|}} \sum_{k\in\mathcal{K}_{\mathcal{H}},k'\in\mathcal{K}_{\mathcal{F}},x\in\{0,1\}^L} \Big(\left|0,k,k',x\right\rangle_{\mathbf{C}'} \left|k,k',H_k(x),f_{k'}(x)\right\rangle_{\mathbf{R}'} + (-1)^b \left|1,k,k',x\right\rangle_{\mathbf{C}'} \left|k,k',H_k(x),f_{k'}(x)\oplus 1\right\rangle_{\mathbf{R}'} \Big)$$

By Theorems 6.1 and B.7, we obtain the following theorem.

Theorem B.8. *$\{Q'_{\mathsf{HM},0}, Q'_{\mathsf{HM},1}\}$ is computationally hiding and statistically binding.*