Quantum Group Actions

Tomoyuki Morimae[1] and Keita Xagawa[2]

[1]Yukawa Institute for Theoretical Physics, Kyoto University, Kyoto, Japan
tomoyuki.morimae@yukawa.kyoto-u.ac.jp
[2]Technology Innovation Institute, Abu Dhabi, UAE
keita.xagawa@tii.ae

Abstract

In quantum cryptography, there could be a new world, Microcrypt, where cryptography is possible but one-way functions (OWFs) do not exist. Although many fundamental primitives and useful applications have been found in Microcrypt, they lack "OWFs-free" concrete hardness assumptions on which they are based. In classical cryptography, many hardness assumptions on concrete mathematical problems have been introduced, such as the discrete logarithm (DL) problems or the decisional Diffie-Hellman (DDH) problems on concrete group structures related to finite fields or elliptic curves. They are then abstracted to generic hardness assumptions such as the DL and DDH assumptions over group actions. Finally, based on these generic assumptions, primitives and applications are constructed. The goal of the present paper is to introduce several abstracted generic hardness assumptions in Microcrypt, which could connect the concrete mathematical hardness assumptions with applications. Our assumptions are based on a quantum analogue of group actions. A group action is a tuple $(G, S, \star)$ of a group G, a set S, and an operation $\star : G \times S \to S$. We introduce a quantum analogue of group actions, which we call quantum group actions (QGAs), where G is a set of unitary operators, S is a set of states, and $\star$ is the application of a unitary on a state. By endowing QGAs with some reasonable hardness assumptions, we introduce a natural quantum analogue of the decisional Diffie-Hellman (DDH) assumption and pseudorandom group actions. Based on these assumptions, we construct classical-query pseudorandom function-like state generators (PRFSGs). PRFSGs are a quantum analogue of pseudorandom functions (PRFs), and have many applications such as IND-CPA SKE, EUF-CMA MAC, and private-key quantum money schemes. Because classical group actions are instantiated with many concrete mathematical hardness assumptions, our QGAs could also have some concrete (even OWFs-free) instantiations.

Contents

1 Introduction

Background. In classical cryptography, the existence of one-way functions (OWFs) is the minimum assumption [IL89], because many primitives (such as pseudorandom generators (PRGs), pseudorandom functions (PRFs), zero-knowledge, commitments, digital signatures, and secret-key encryptions (SKE)) are equivalent to OWFs in terms of existence, and almost all primitives (including public-key encryption (PKE) and multi-party computations) imply OWFs.

On the other hand, recent active studies have demonstrated that in quantum cryptography, OWFs would not necessarily be the minimum assumption. Many fundamental primitives have been introduced, such as pseudorandom unitaries (PRUs) [JLS18], pseudorandom function-like state generators (PRFSGs) [AQY22, AGQY22], unpredictable state generators (UPSGs) [MYY24], pseudorandom state generators (PRSGs) [JLS18], one-way state generators (OWSGs) [MY22], EFI pairs [BCQ23], and one-way puzzles (OWPuzzs) [KT24a]. They seem to be weaker than OWFs [Kre21, KQST23, LMW24], but still imply many useful applications such as commitments [MY22, AQY22, BCQ23, Yan22], multi-party computations [MY22, AQY22], message authentication codes (MAC) [AQY22, MYY24], secret-key encryptions (SKE) [AQY22, MYY24], digital signatures [MY22], private-key quantum money [JLS18], etc.

In classical cryptography, many hardness assumptions on concrete mathematical problems have been introduced, such as the discrete logarithm (DL) problems or the decisional Diffie-Hellman (DDH) problems on concrete group structures related to finite fields or elliptic curves. They are then abstracted to generic hardness assumptions such as the DL and DDH assumptions over group actions. Finally, based on these generic assumptions, primitives and applications are constructed.

On the other hand, in quantum cryptography, the first step has not yet been studied. Because PRUs can be constructed from OWFs [HM24b], and PRUs imply PRFSGs, UPSGs, PRSGs, OWSGs, EFI pairs, and OWPuzzs, all of them can also be constructed from OWFs. (See Figure 2 for the relations.) However, no "OWFs-free" concrete mathematical hardness assumptions on which they are based are known.[1]

1.1 Our Results

The goal of the present paper is to introduce several abstracted generic hardness assumptions, which could connect the concrete mathematical hardness assumptions with applications. As we will explain later, these new assumptions are a quantum analogue of cryptographic group actions [BY91, Cou06, JQSY19, ADMP20]. Because classical group actions have many concrete instantiations [JD11, CLM+18, DD24], our quantum versions of group actions could also have concrete (even OWFs-free) instantiations by considering natural quantum analogue of classical hard problems.

Based on these quantum assumptions, we construct classical-query PRFSGs. PRFSGs are a quantum analogue of PRFs. A PRFSG is a quantum polynomial-time (QPT) algorithm $\mathsf{StateGen}$ that takes a classical key k and a bit string x as input, and outputs a quantum state $|\phi_k(x)\rangle$. The security roughly means that no QPT adversary can distinguish whether it is querying to $\mathsf{StateGen}(k,\cdot)$ with a random k or an oracle that outputs Haar random states, which we call the Haar oracle.[2] PRFSGs imply almost all known primitives such as UPSGs, PRSGs, OWSGs, OWPuzzs, and EFI pairs. PRFSGs also imply useful applications such as IND-CPA SKE, EUF-CMA MAC, private-key quantum money, commitments, multi-party computations, (bounded-poly-time-secure) digital signatures, etc.

[1] See Section 1.2.

[2] More precisely, the oracle works as follows. If it gets x as input and x was not queried before, it samples a Haar random state ψ_x and returns it. If x was queried before, it returns the same state ψ_x that was sampled before when x was queried for the first time.

Unfortunately, PRFSGs that we construct in this paper are secure only against classical queries.[3] It is an open problem whether PRFSGs secure against quantum queries or even PRUs can be constructed from quantum group actions.

Group actions. Our quantum assumptions are based on a "quantization" of group actions. A group action $(\star, G, S)$ is a tuple of a group G, a set S, and an operation $\star : G \times S \to S$ such that $g_1 \star (g_2 \star x) = (g_1 g_2) \star s$ for any $g_1, g_2 \in G$ and $s \in S$. Cryptographic group actions [Cou06, JQSY19, ADMP20, BY91] are group actions endowed with some hardness assumptions. For example, a one-way group action [BY91] is a group action such that given $s \leftarrow S$[4] and $t := g \star s$ with $g \leftarrow G$, it is hard to find a g' such that $g' \star s = t$. One-way group actions are abstractions of several well-studied cryptographic assumptions such as the Discrete-Log assumptions [DH76], isogeny-based assumptions [JD11, CLM+18], and code-based assumptions [DD24]. They have several applications such as identifications, digital signatures, and commitments [BY91].

A pseudorandom group action [ADMP20, JQSY19] is a group action such that $(s, g \star s)$ and (s, u) are computationally indistinguishable, where s is a (fixed) element in S, $u \leftarrow S$, and $g \leftarrow G$. Pseudorandom group actions are abstractions of several well-studied cryptographic assumptions such as the Decisional Diffie-Hellman (DDH) assumptions [DH76] and isogeny-based assumptions [CLM+18].[5] They also have attractive applications such as key exchange, smooth projective hashing, dual-mode PKE, two-message statistically sender-private OT, and PRFs [BY91, ADMP20, JQSY19, Cou06].

Quantum group actions. In this paper, we introduce a quantum analogue of cryptographic group actions, which we call *quantum group actions (QGAs)*. A QGA $(G, S, \star)$ is a tuple of a set G, a set S, and an operation $\star$. G is a set of efficiently-implementable unitary operators[6] and S is a set of efficiently generable states. The action $\star$ is just the application of a unitary in G on a state in S. Then the property $g_1(g_2|s\rangle) = (g_1 g_2)|s\rangle$ is trivially satisfied for any $g_1, g_2 \in G$ and $|s\rangle \in S$.

We endow QGAs with several hardness assumptions. In particular, we construct PRFSGs from these assumptions.

Naor-Reingold PRFs, DDH, and (weak) pseudorandomness. To give an idea, we briefly review the classical construction of the Naor-Reingold (classical) PRFs [NR04] based on some classical assumptions. The Naor-Reingold PRFs can be constructed from a group action as follows [NR04, BKW20, ADMP20, MOT20]. The key k of the PRF f_k is $k := (g_0, g_1, ..., g_\ell)$, where $g_i \leftarrow G$ for $i = 0, 1, ..., \ell$. For an input $x = (x_1, ..., x_\ell) \in \{0,1\}^\ell$, $f_k(x)$ is defined as

$$f_k(x) := (g_\ell^{x_\ell} \cdot \cdots \cdot g_1^{x_1} g_0) \star s_0, \tag{1}$$

where s_0 is a fixed element in S. Roughly speaking, its security is shown by the computational indistinguishability [7]

$$\{(g_i \star s_0, (\tilde{g} g_i) \star s_0) : \tilde{g}, g_i \leftarrow G\}_{i \in [Q]} \approx_c \{(g_i \star s_0, h_i \star s_0) : g_i, h_i \leftarrow G\}_{i \in [Q]}, \tag{2}$$

[3] IND-CPA SKE and EUF-CMA MAC constructed from such PRFSGs are also secure against classical queries.

[4] In this paper, $s \leftarrow S$ means that an element s is sampled uniformly at random from the set S.

[5] While we can treat some code-based assumptions as group actions, they are unlikely to be weakly pseudorandom and weakly unpredictable with large samples [DD24, BCDD+24].

[6] Note that we do not require that G is a group.

[7] Here $\approx_c$ means that the two distributions are computationally indistinguishable.

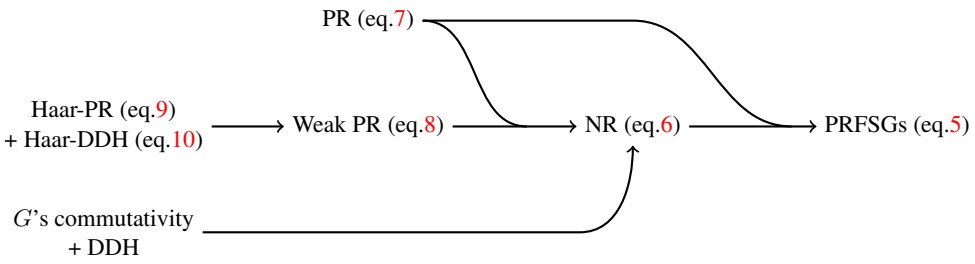

Figure 1: Diagram for our construction.

which, for clearness, we call the Naor-Reingold (NR) assumption. Here, Q is a polynomial of the security parameter. Applying the NR assumption repeatedly, Naor and Reingold showed that $f_k(x)$ is computationally indistinguishable from $f'_k(x) \coloneqq g_x \star s_0$, where $g_x \leftarrow G$ for each x [NR04].

Naor and Reingold [NR04] showed that the NR assumption is derived from the DDH assumption. The DDH assumption says that

$$(s_0, \tilde{g} \star s_0, g \star s_0, (\tilde{g}g) \star s_0) \approx_c (s_0, \tilde{g} \star s_0, g \star s_0, h \star s_0), \tag{3}$$

where s_0 is a fixed element in S and $\tilde{g}, g, h \leftarrow G$. If G is a *commutative ring* with $(\cdot, +)$ and S has a binary operation $\circ$ such that $(g \star s_0) \circ (g' \star s_0) = (g + g') \star s_0$, then the DDH assumption tightly implies the NR assumption, because we can re-randomizing the samples [NR04, BMR10].[8] Boneh, Kogan, and Woo [BKW20] considered the case that G is a *commutative group* and showed that the DDH assumption implies the NR assumption via a hybrid argument. Alamati, De Feo, Montgomery, and Patranabis [ADMP20] took a different approach; they defined weak pseudorandomness,[9] which is the computational indistinguishability

$$\{(s_i, \tilde{g} \star s_i) : \tilde{g} \leftarrow G, s_i \leftarrow S\}_{i \in [Q]} \approx_c \{(s_i, s'_i) : s_i, s'_i \leftarrow S\}_{i \in [Q]}. \tag{4}$$

If the group action is regular,[10] then the distribution $s_i \leftarrow S$ is equivalent to the distribution of $g_i \star s_0$ with $g_i \leftarrow G$. Thus, by replacing s_i and s'_i with $g_i \star s_0$ and $h_i \star s_0$, where $g_i \leftarrow G$ and $h_i \leftarrow G$, respectively, the weak pseudorandomness is tightly equivalent to the NR assumption.

We note that while Alamati et al. focused only on the case that G is commutative, their approach can be extended to non-commutative groups G. We also note that we will not need some properties of G in the proof in Boneh et al. [BKW20] when we employ pseudorandom group actions. For details, see Appendix B.

Construction of PRFSGs. Based on these classical constructions of the Naor-Reingold PRFs, we try to construct PRFSGs. Jumping ahead, our construction is summarized in Figure 1. Let (G, S) be a QGA.[11] This means that G is a set of efficiently implementable unitary operators and S is a set of efficiently generatable states. We will construct a PRFSG, $\mathsf{StateGen}(k, x) \to |\phi_k(x)\rangle$, as follows: The key k of the PRFSG is $k \coloneqq (g_0, g_1, ..., g_\ell, |s_0\rangle)$, where $g_i \leftarrow G$ for $i = 0, 1, ..., \ell$ and $|s_0\rangle$ is a (fixed) element in S. For an input

[8] [LW09, EHK+13, ABP15] treated some non-commutative cases related to the Matirx DDH assumptions.

[9] Correctly speaking, they defined it as the assumption that $\pi_{\tilde{g}} : s \mapsto \tilde{g} \star s$ is a weak pseudorandom *permutation*.

[10] A group action is *regular* if it is *transitive*, that is, for every $s_1, s_2 \in S$, there exists $g \in G$ satisfying $s_2 = g \star s_1$, and *free*, that is, for each $g \in G$, g is the identity element if and only if there exists $s \in S$ satisfying $s = g \star s$ [ADMP20].

[11] We omit $\star$, because this is trivial.

$x = (x_1, ..., x_\ell) \in \{0,1\}^\ell$, the output of PRFSG $|\phi_k(x)\rangle$ is defined as[12]

$$|\phi_k(x)\rangle := (g_\ell^{x_\ell} \cdot \cdots \cdot g_1^{x_1} g_0)|s_0\rangle. \tag{5}$$

The question is which hardness assumptions should we endow the QGA with so that StateGen satisfies the security of PRFSGs. In quantum group actions, we cannot expect that G has algebraic structures, and the simple analogue of the DDH assumption or/and weak pseudorandomness would not imply the quantum analogue of the NR assumption that roughly states the computational indistinguishability[13]

$$\{(g_i|s_0\rangle, \tilde{g}g_i|s_0\rangle) : \tilde{g}, g_i \leftarrow G\}_{i\in[Q]} \approx_c \{(g_i|s_0\rangle, h_i|s_0\rangle) : g_i, h_i \leftarrow G\}_{i\in[Q]}, \tag{6}$$

where $|s_0\rangle$ is a (fixed) element in S. Thus, we need to put forth simple, plausible assumptions over quantum group actions that imply the quantum analogue of the NR assumption.

In the quantum case, moreover, Equation (6) is not enough to construct PRFSGs unlike the classical case. In the classical construction of NR PRFs, by applying the classical NR assumption repeatedly, we can show that $f_k(x)$ is indistinguishable from $g_x \star s_0$ with $g_x \leftarrow G$ for each x. In the classical case, because of the regularity, $g_x \star s_0$ with $g_x \leftarrow G$ is equivalent to sampling $s \leftarrow S$. However, in the quantum case, we do not have regularity in general, and we cannot expect that $g_x|s_0\rangle$ with $g_x \leftarrow G$ is uniformly at random in some efficiently samplable set S'.[14] Thus, we will require the additional assumption that $g_x|s_0\rangle$ with $g_x \leftarrow G$ is indistinguishable from Haar random states. We call this assumption *pseudorandomness (PR)*, which roughly says the computational indistinguishability

$$(|s_0\rangle, h|s_0\rangle) \approx_c (|s_0\rangle, |s'\rangle), \tag{7}$$

where $|s_0\rangle$ is a (fixed) element in S, $h \leftarrow G$, and $|s'\rangle \leftarrow \mu$. (Here, $|s'\rangle \leftarrow \mu$ means that a state $|s'\rangle$ is sampled uniformly at random with the Haar measure.)[15] By combining the quantum analogue of the NR assumption (Equation (6)) and this PR assumption, we get PRFSGs.

Then, the question is how can we get the quantum analogue of the NR assumption? In the classical case, we get it from the weak pseudorandomness, Equation (4), [ADMP20]. We can introduce a quantum analogue of it, which is the computational indistinguishability

$$\{(|s_i\rangle, \tilde{g}|s_i\rangle) : \tilde{g} \leftarrow G, |s_i\rangle \leftarrow \mu\}_{i\in[Q]} \approx_c \{(|s_i\rangle, |s_i'\rangle) : |s_i\rangle, |s_i'\rangle \leftarrow \mu\}_{i\in[Q]}. \tag{8}$$

In the classical case, the weak pseudorandomness is equivalent to the classical NR assumption, but in the quantum case, again because of the fact that we do not have regularity in general, Equation (8) will not imply the quantum analogue of the NR assumption, Equation (6). However, combining this with the PR assumption (Equation (7)), we will recover Equation (6).

Therefore the goal is to realize the quantum analogue of weak pseudorandomness, Equation (8). To achieve it, we put forth two new assumptions, which we believe plausible and reasonable: The one is *Haar-pseudorandomness (Haar-PR)*, which roughly states the computational indistinguishability

$$(|s\rangle, h|s\rangle) \approx_c (|s\rangle, |s'\rangle), \tag{9}$$

[12] We note that Ananth, Gulati, and Lin [AGL24] gave a similar construction of selectively-secure PRFSGs in the common Haar state model, which is inspired by GGM [GGM86].

[13] Actually, our security game is such that the adversary receives many copies of the state. Hence, the assumption should be read as the computational indistinguishability $\{(g_i|s_0\rangle, \tilde{g}g_i|s_0\rangle)^{\otimes t} : \tilde{g}, g_i \leftarrow G\}_{i\in[Q]} \approx_c \{(g_i|s_0\rangle, h_i|s_0\rangle)^{\otimes t} : g_i, h_i \leftarrow G\}_{i\in[Q]}$ for any polynomial t. However, in this introduction, we ignore the number of copies for ease of notation and use the word "roughly".

[14] S' might differ from S.

[15] Again, here, the computational indistinguishability is that for many copies of states, but for simplicity we omit it.

where $|s\rangle, |s'\rangle \leftarrow \mu$ and $h \leftarrow G$.[16] Interestingly, PR and Haar-PR are not equivalent, because, unlike the classical case with regularity, $h|s_0\rangle$ in the LHS of PR (Equation (7)) may not be distributed according to the Haar measure.

The other is a quantum analogue of the DDH assumption with multiple samples and with respect to Haar random states. We call it *Haar-DDH*, which roughly states the computational indistinguishability

$$\{(|s_i\rangle, g|s_i\rangle) : |s_i\rangle \leftarrow \mu, g \leftarrow G\}_{i\in[Q]} \approx_c \{(|s_i\rangle, h_i|s_i\rangle) : |s_i\rangle \leftarrow \mu, h_i \leftarrow G\}_{i\in[Q]}. \tag{10}$$

The combination of Haar-PR and Haar-DDH assumptions implies the quantum analogue of weak pseudorandomness, Equation (8). Combining it with the PR assumption, we can show a quantum analogue of the NR assumption (Equation (6)). We can show the security of our NR-style PRFSGs from the quantum analogue of the NR assumption and the PR assumption.

In general, PRFSGs are defined against quantum-query adversaries [AQY22, AGQY22]. This means that the security holds against any QPT adversary that can query x in superposition. Unfortunately, our proof only works for *classical-query* cases, and there are several barriers to the construction of PRFSGs secure against quantum queries. For details, see Section 4.2. It is an open problem to construct PRFSGs secure against quantum queries or even PRUs from QGAs (or other OWFs-free assumptions).

In the classical case, PRFs can be constructed from pseudorandom group actions [JQSY19]. On the other hand, we do not know how to construct PRFSGs from PR or Haar-PR QGAs. One reason is that the construction of PRFs in [JQSY19] is the GGM one [GGM84], and we do not know how to use the GGM technique in the quantum setting. For example, we do not know how to hash quantum states. Moreover, in the classical case, we can construct PRFs from PRGs [GGM84], but it is an open problem whether we can construct PRFSGs from PRSGs.[17]

PRSGs from PR QGAs. As we have explained, PR QGAs is the computational indistinguishability $(|s_0\rangle, h|s_0\rangle)^{\otimes t} \approx_c (|s_0\rangle, |s'\rangle)^{\otimes t}$ for any polynomial t, where $|s_0\rangle$ is a (fixed) element in S, $h \leftarrow G$, and $|s'\rangle \leftarrow \mu$. As an additional result, we observe that PRSGs can be constructed from PR QGAs.

Lemma 1.1. *PR QGAs imply PRSGs.*

OWSGs from one-way QGAs. It is also natural to define a quantum analogue of one-way group actions. In the security game of classical one-way group actions, the adversary receives classical bit strings s and $g \star s$. In our one-way QGAs, the adversary receives $|s\rangle^{\otimes t}$ and $(g|s\rangle)^{\otimes t}$ for any polynomial t. We show the following.

Lemma 1.2. *One-way QGAs imply pure one-way state generators (OWSGs).*

Candidates of QGAs. Finally, we briefly argue about some candidates for QGAs. We expect that QGAs based on random quantum circuits and random IQP circuits are PR, Haar-PR, and DDH QGAs.

Open Problems. Figure 2 is a summary of the new and known relations between cryptographic primitives and QGAs, in which we separate primitives with classical-query and quantum-query securities. As is shown in the figure, our results could open a new avenue to connect quantum cryptographic applications with concrete OWFs-free hardness assumptions.

We leave some interesting open problems:

[16] Note that we give unbounded-polynomial copies of the sample to the adversary. If the number of copies is constant, then there exists a statistical construction [AGL24, Section 4].

[17] PRFSGs with $O(\log)$ input length can be constructed from PRSGs [AQY22], but it is open for PRFSGs with poly input length.

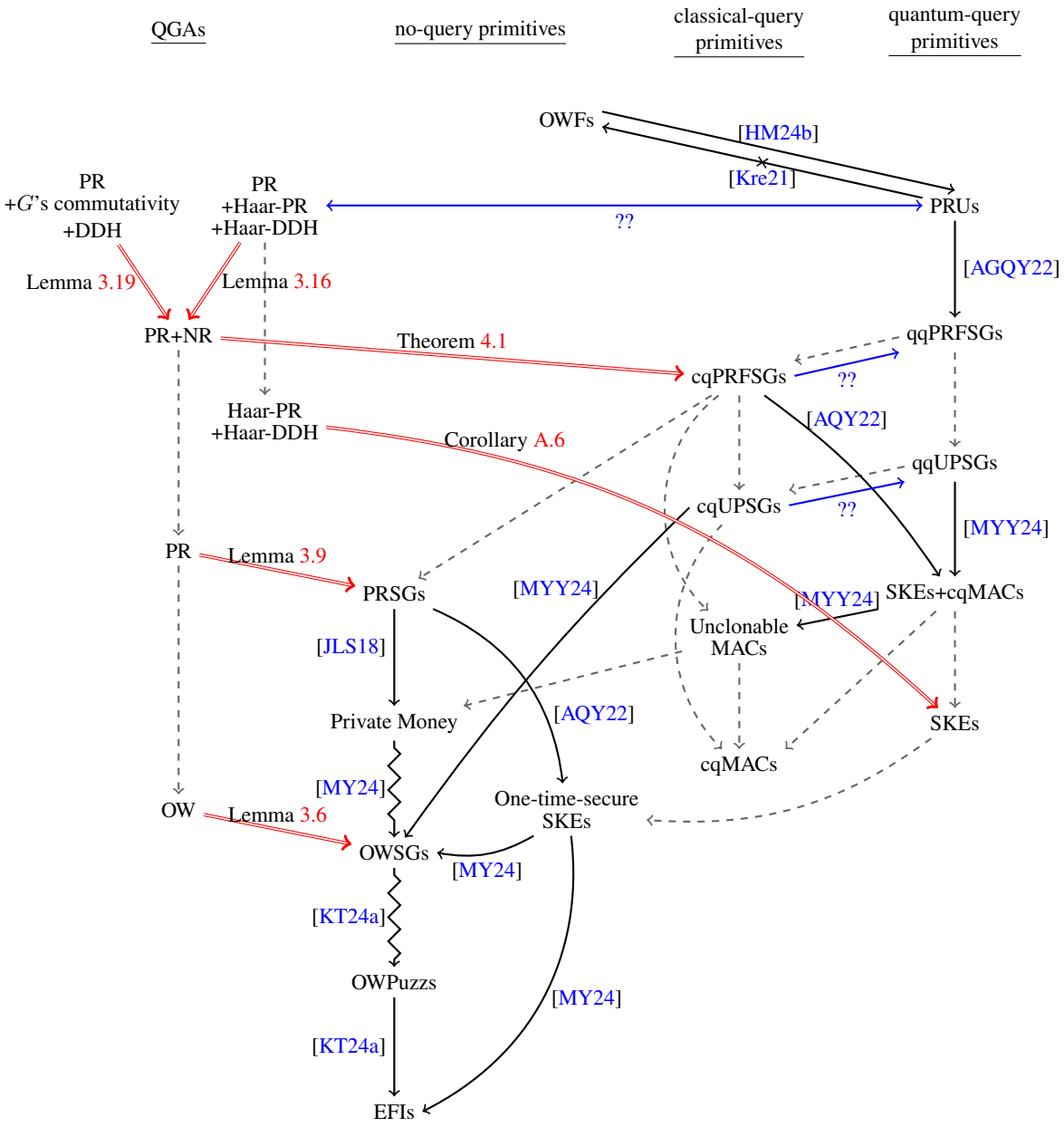

Figure 2: Relations among primitives and QGAs. "cq" and "qq" denote classical-query and quantum-query, respectively. An arrow from primitive A to primitive B (except for those with crosses) represents that A implies B. An arrow with a cross represents that there exists a black-box separation between A and B. A gray dashed arrow represents that A trivially implies B. A zigzag arrow represents that A with pure outputs implies B. A red double arrow represents that the relation is shown in this paper. A blue arrow from primitive A to primitive B represents that we do not know the implication from A to B. cqPRFSGs with the input space $\{0,1\}^\ell$ for $\ell = O(\log(\lambda))$ can be constructed from PRSGs [AQY22].

1. Do PR, Haar-PR, and Haar-DDH assumptions over QGAs imply *quantum-query* PRFSGs? Or, can we show the separation between quantum-query/classical-query PRFSGs?

2. Can we construct PR, Haar-PR, and Haar-DDH QGAs from PRUs?

3. Can we construct PRUs from PR, Haar-PR, and Haar-DDH QGAs, or from other "genuinely quantum" assumptions?

1.2 Related Works

As we have explained in Introduction, the important open problem is to base "Microcrypt" primitives on "OWFs-free" concrete mathematical hardness assumptions. Recently, the following three papers that tackle the problem have been uploaded on arXiv during the preparation of this manuscript.

Khurana and Tomer [KT24b] constructed OWPuzzs from some hardness assumptions that imply sampling-based quantum advantage [BFNV19, AA11, TD04, BJS11, BMS16, FKM+18] (plus a mild complexity assumption, $\mathbf{P}^{\#\mathbf{P}} \not\subseteq (io)\mathbf{BQP}/\mathbf{qpoly}$).

Hiroka and Morimae [HM24a] and Cavalar, Goldin, Gray, and Hall [private communication] constructed OWPuzzs from quantum-average-hardness of GapK problem. GapK problem is a promise problem to decide whether a given bit string x has a small Kolmogorov complexity or not. Its quantum-average-hardness means that the instance x is sampled from a quantum-polynomial-time samplable distribution, and no quantum-polynomial-time algorithm can solve the problem.

Their assumptions are more concrete and already studied in other contexts than cryptography, namely, quantum advantage and (classical) meta-complexity. On the other hand, the present paper construct PRFSGs (and therefore UPSGs, PRSGs, OWSGs, private-key quantum money schemes, IND-CPA SKE, EUF-CMA MAC, OWPuzzs, and EFI pairs). It is an interesting open problem whether our QGAs assumptions can be instantiated with some concrete assumptions related to quantum advantage or meta-complexity.

2 Preliminaries

2.1 Basic Notations

We use the standard notations of quantum information and cryptography. For a finite set X, $x \leftarrow X$ means that an element x is sampled from X uniformly at random. We write μ_m to denote the Haar measure over m-qubits space. We often drop the subscription m. For an algorithm $\mathcal{A}$, $y \leftarrow \mathcal{A}(x)$ means that $\mathcal{A}$ is run on input x and output y is obtained. For a non-negative integer Q, $[Q]$ is the set $\{1, 2, ..., Q\}$. QPT stands for quantum polynomial time. λ is the security parameter. negl is a negligible function. For two distributions D and D', we sometimes use $D \approx_c D'$ to denote D and D' are computationally indistinguishable with respect to a quantum adversary.

2.2 Quantum Cryptographic Primitives

We review quantum cryptographic primitives in the literature.

Definition 2.1 (Pseudorandom State Generators (PRSGs) [JLS18]). *A pseudorandom state generator (PRSG) is a tuple* $(\mathsf{KeyGen}, \mathsf{StateGen})$ *of algorithms such that*

- $\mathsf{KeyGen}(1^\lambda) \to k$: *It is a QPT algorithm that, on input* 1^λ*, outputs a key* k*.*

- $\mathsf{StateGen}(k) \to |\phi_k\rangle$: *It is a QPT algorithm that, on input k, outputs a quantum state $|\phi_k\rangle$.*

We require that for any QPT adversary $\mathcal{A}$ and any polynomial t,

$$\left|\Pr_{k\leftarrow\mathsf{KeyGen}(1^\lambda)}[1\leftarrow\mathcal{A}(1^\lambda,|\phi_k\rangle^{\otimes t})]-\Pr_{|\psi\rangle\leftarrow\mu}[1\leftarrow\mathcal{A}(1^\lambda,|\psi\rangle^{\otimes t})]\right|\leq \mathsf{negl}(\lambda), \tag{11}$$

where μ is a Haar measure.

Definition 2.2 (One-Way State Generators (OWSGs) [MY22, MY24]). *A one-way state generator (OWSG) is a tuple $(\mathsf{KeyGen},\mathsf{StateGen},\mathsf{Ver})$ of algorithms such that*

- $\mathsf{KeyGen}(1^\lambda)\to k$: *It is a QPT algorithm that, on input 1^λ, outputs a classical bit string $k\in\{0,1\}^{\kappa(\lambda)}$, where κ is a polynomial.*
- $\mathsf{StateGen}(k)\to|\phi_k\rangle$: *It is a QPT algorithm that, on input k, outputs a quantum state $|\phi_k\rangle$.*
- $\mathsf{Ver}(k',|\phi_k\rangle)\to\top/\bot$: *It is a QPT algorithm that, on input k' and $|\phi_k\rangle$, outputs $\top/\bot$.*

We require the following correctness and one-wayness.

Correctness.

$$\Pr[\top\leftarrow\mathsf{Ver}(k,|\phi_k\rangle):k\leftarrow\mathsf{KeyGen}(1^\lambda),|\phi_k\rangle\leftarrow\mathsf{StateGen}(k)]\geq 1-\mathsf{negl}(\lambda). \tag{12}$$

One-wayness. *For any QPT adversary $\mathcal{A}$ and any polynomial t,*

$$\Pr[\top\leftarrow\mathsf{Ver}(k',|\phi_k\rangle):k\leftarrow\mathsf{KeyGen}(1^\lambda),|\phi_k\rangle\leftarrow\mathsf{StateGen}(k),k'\leftarrow\mathcal{A}(1^\lambda,|\phi_k\rangle^{\otimes t})]\leq\mathsf{negl}(\lambda). \tag{13}$$

Remark 2.3. If all $|\phi_k\rangle$ are pure and $\Pr[\top\leftarrow\mathsf{Ver}(k,|\phi_k\rangle)]\geq 1-\mathsf{negl}(\lambda)$ is satisfied for all k, we can replace Ver with the following canonical verification algorithm: Project $|\phi_k\rangle$ onto $|\phi_{k'}\rangle$. If the projection is successful, output $\top$. Otherwise, output $\bot$.

Definition 2.4 (Weak OWSGs [MY24]). *The definition of weak OWSGs is the same as that of OWSGs except that the one-wayness is replaced with the following weak one-wayness: there exists a polynomial p such that for any QPT $\mathcal{A}$ and polynomial t*

$$\Pr[\top\leftarrow\mathsf{Ver}(k',|\phi_k\rangle):k\leftarrow\mathsf{KeyGen}(1^\lambda),|\phi_k\rangle\leftarrow\mathsf{StateGen}(k),k'\leftarrow\mathcal{A}(1^\lambda,|\phi_k\rangle^{\otimes t})]\leq 1-\frac{1}{p(\lambda)}. \tag{14}$$

Remark 2.5. It is shown in Theorem 3.7 of [MY24] that OWSGs exist if and only if weak OWSGs exist.

Definition 2.6 (Pseudorandom Function-Like State Generators (PRFSGs) [AQY22]). *A pseudorandom function-like state generator (PRFSG) is a tuple $(\mathsf{KeyGen},\mathsf{StateGen})$ of algorithms such that*

- $\mathsf{KeyGen}(1^\lambda)\to k$: *It is a QPT algorithm that, on input 1^λ, outputs $k\in\{0,1\}^{\kappa(\lambda)}$, where κ is a polynomial.*
- $\mathsf{StateGen}(k,x)\to|\phi_k(x)\rangle$: *It is a QPT algorithm that, on input k and $x\in\{0,1\}^\ell$, outputs a quantum state $|\phi_k(x)\rangle$, where ℓ is a polynomial.*

We require the following security: For any QPT adversary $\mathcal{A}$,

$$\left|\Pr_{k\leftarrow\mathsf{KeyGen}(1^\lambda)}[1\leftarrow\mathcal{A}^{\mathsf{StateGen}(k,\cdot)}(1^\lambda)]-\Pr[1\leftarrow\mathcal{A}^{\mathcal{O}_{\mathrm{Haar}}}(1^\lambda)]\right|\leq\mathsf{negl}(\lambda). \tag{15}$$

The oracle $\mathcal{O}_{\mathrm{Haar}}$ is the following oracle:

1. *When x is queried and it is not queried before, sample $|\psi_x\rangle\leftarrow\mu$ and return $|\psi_x\rangle$.*
2. *When x is queried and it was queried before, return $|\psi_x\rangle$.*

Definition 2.7 (Classical-Query PRFSGs). *A PRFSG is called a classical-query PRFSG if it is secure against only adversaries that query the oracle classically.*

Remark 2.8. In [AQY22, AGQY22], general PRFSGs where adversaries can quantumly query the oracle are defined and constructed from PRUs or OWFs. In this paper, however, we mainly focus on classical-query ones.

2.3 Design and Haar Measure

We will use the following lemmas to show our results.

Lemma 2.9 (Lemma 20 and Lemma 21 of [Kre21]). *For each $n,t\in\mathbb{N}$ and $\epsilon>0$, there exists a $\mathrm{poly}(n,t,\log\frac{1}{\epsilon})$-time quantum algorithm $\mathcal{S}$ that outputs an n-qubit state such that for any quantum algorithm $\mathcal{A}$*

$$(1-\epsilon)\Pr_{|\psi\rangle\leftarrow\mu}[1\leftarrow\mathcal{A}(|\psi\rangle^{\otimes t})]\leq\Pr_{|\psi\rangle\leftarrow\mathcal{S}}[1\leftarrow\mathcal{A}(|\psi\rangle^{\otimes t})]\leq(1+\epsilon)\Pr_{|\psi\rangle\leftarrow\mu}[1\leftarrow\mathcal{A}(|\psi\rangle^{\otimes t})]. \tag{16}$$

Lemma 2.10.

$$\mathbb{E}_{|\psi\rangle,|\phi\rangle\leftarrow\mu_n}|\langle\psi|\phi\rangle|^2\leq\frac{1}{2^n}. \tag{17}$$

Proof. It is known that $\mathbb{E}_{|\psi\rangle\leftarrow\mu_n}|\psi\rangle\langle\psi|=\frac{I^{\otimes n}}{2^n}$, where $I:=|0\rangle\langle0|+|1\rangle\langle1|$ is the two-dimentional identity operator. Therefore,

$$\mathbb{E}_{|\psi\rangle,|\phi\rangle\leftarrow\mu_n}|\langle\psi|\phi\rangle|^2=\mathbb{E}_{|\phi\rangle\leftarrow\mu_n}\langle\phi|[\mathbb{E}_{|\psi\rangle\leftarrow\mu_n}|\psi\rangle\langle\psi|]|\phi\rangle=\frac{1}{2^n}. \tag{18}$$

□

3 Quantum Group Actions and Hardness Assumptions

In this section, we define quantum group actions (QGAs) and endow them with several hardness assumptions including one-wayness and variants of pseudorandomness.

3.1 Quantum Group Actions

We first define quantum group actions (QGAs).

Definition 3.1 (Quantum Group Actions (QGAs)). *A quantum group action (QGA) is a pair (G, S) of algorithms such that*

- $G(1^\lambda) \to [g]$: *It is a QPT algorithm that takes 1^λ as input, and outputs an efficient classical description $[g]$ of a unitary operator g.*
- $S(1^\lambda) \to [|s\rangle]$: *It is a QPT algorithm that takes 1^λ as input, and outputs an efficient classical description $[|s\rangle]$ of a quantum state $|s\rangle$.*

Remark 3.2. Note that we do not require that the set $\{g : [g] \leftarrow G(1^\lambda)\}$ is a group of unitary operators. However, we call (G, S) a quantum group action, because it is a quantum analogue of a group action.

Remark 3.3. Note that G and S are not deterministic. This means that each execution of G or (S) can output different $[g]$ (or $[|s\rangle]$).

Remark 3.4. An efficient classical description $[g]$ of g means, for example, a classical description of a $\mathrm{poly}(\lambda)$-size quantum circuit that implements g. An efficient classical description $[|s\rangle]$ of $|s\rangle$ means, for example, a classical description of a $\mathrm{poly}(\lambda)$-size quantum circuit that generates $|s\rangle$. For simplicity, we often write $[g]$ and $[|s\rangle]$ just as g and $|s\rangle$, respectively, if there is no confusion.

3.2 One-Way QGAs

We next define a quantum analogue of one-way group actions.

Definition 3.5 (One-Way QGAs (OW QGAs)). *A QGA (G, S) is called a one-way QGA (OW QGA) if for any QPT adversary $\mathcal{A}$ and any polynomial t, $\Pr[\top \leftarrow \mathcal{C}] \leq \mathsf{negl}(\lambda)$ is satisfied in the following security game.*

1. *The challenger $\mathcal{C}$ runs $[|s\rangle] \leftarrow S(1^\lambda)$ and $[g] \leftarrow G(1^\lambda)$.*
2. *$\mathcal{C}$ sends $|s\rangle^{\otimes t}$ and $(g|s\rangle)^{\otimes t}$ to $\mathcal{A}$.*
3. *$\mathcal{A}$ returns an efficient classical description $[g']$ of a unitary g'.*[18]
4. *$\mathcal{C}$ projects $g|s\rangle$ onto $g'|s\rangle$. If the projection is successful, $\mathcal{C}$ outputs $\top$. Otherwise, it outputs $\bot$.*

Lemma 3.6. *If OW QGAs exist then OWSGs exist.*

Proof. Let (G, S) be a OW QGA. From it, we construct a weak OWSG $(\mathsf{KeyGen}, \mathsf{StateGen}, \mathsf{Ver})$ as follows.

- $\mathsf{KeyGen}(1^\lambda) \to k$: Run $[|s\rangle] \leftarrow S(1^\lambda)$ and $[g] \leftarrow G(1^\lambda)$. Output $k := ([|s\rangle], [g])$.
- $\mathsf{StateGen}(k) \to |\phi_k\rangle$: Parse $k = ([|s\rangle], [g])$. Output $|\phi_k\rangle := |s\rangle \otimes g|s\rangle$.
- $\mathsf{Ver}(k', |\phi_k\rangle) \to \top/\bot$: Parse $k' = ([|s'\rangle], [g'])$. Apply $g' \otimes I$ on $|\phi_k\rangle$ and do the SWAP test between the two registers.

[18] $[g']$ could be outside of the support of G.

Assume that this is not weak one-way. Then, for any polynomial p, there exists a QPT $\mathcal{A}$ and a polynomial t such that

$$\sum_{[|s\rangle],[g]} \Pr[[|s\rangle] \leftarrow S(1^\lambda)] \Pr[[g] \leftarrow G(1^\lambda)] \sum_{[|s'\rangle],[g']} \Pr[([|s'\rangle],[g']) \leftarrow \mathcal{A}(1^\lambda, (|s\rangle \otimes g|s\rangle)^{\otimes t})] \cdot \frac{1+|\langle s|(g')^\dagger g|s\rangle|^2}{2} \tag{19}$$

$$\geq 1 - \frac{1}{p(\lambda)}, \tag{20}$$

which means that

$$\sum_{[|s\rangle],[g]} \Pr[[|s\rangle] \leftarrow S(1^\lambda)] \Pr[[g] \leftarrow G(1^\lambda)] \sum_{[|s'\rangle],[g']} \Pr[([|s'\rangle],[g']) \leftarrow \mathcal{A}(1^\lambda, (|s\rangle \otimes g|s\rangle)^{\otimes t})] \cdot |\langle s|(g')^\dagger g|s\rangle|^2 \tag{21}$$

$$\geq 1 - \frac{2}{p(\lambda)}. \tag{22}$$

It is clear that we can construct a QPT adversary that breaks the OW QGA from this $\mathcal{A}$.

From Theorem 3.7 of [MY24], we obtain a pure OWSG $(\mathsf{KeyGen}', \mathsf{StateGen}', \mathsf{Ver}')$ from this weak OWSG. Moreover, we can check that $\Pr[\top \leftarrow \mathsf{Ver}'(k, |\phi_k\rangle)] \geq 1 - \mathsf{negl}(\lambda)$ is satisfied for all k. Then, as is shown in Appendix B of [MY24], we can construct another OWSG with the canonical verification. □

3.3 Pseudorandom QGAs

We also introduce quantum analogue of pseudorandom group actions. We define three types of pseudorandomness of QGAs, which we call pseudorandom (PR), Haar-pseudorandom (Haar-PR), and DDH.

Definition 3.7 (PR QGAs). *We say that a QGA (G, S) is* pseudorandom (PR) *if the following two distributions are computationally indistinguishable for any polynomial t:*

$$D_{\mathrm{pr},0} : |s_0\rangle \leftarrow S, h \leftarrow G;\ \textit{return}\ (|s_0\rangle, h\,|s_0\rangle)^{\otimes t}$$
$$D_{\mathrm{pr},1} : |s_0\rangle \leftarrow S, |s\rangle \leftarrow \mu;\ \textit{return}\ (|s_0\rangle, |s\rangle)^{\otimes t}.$$

We can show that the multiple samples are also pseudorandom.

Lemma 3.8. *Let (G, S) be a PR QGA. Then the following two distributions are computationally indistinguishable for any polynomials Q and t:*

$$D'_{\mathrm{pr},0} : |s_0\rangle \leftarrow S,\ \textit{for}\ q \in [Q]\ h_q \leftarrow G;\ \textit{return}\ \{(h_q\,|s_0\rangle)^{\otimes t}\}_{q\in[Q]}$$
$$D'_{\mathrm{pr},1} : \textit{for}\ q \in [Q]\ \ |s_q\rangle \leftarrow \mu;\ \textit{return}\ \{|s_q\rangle^{\otimes t}\}_{q\in[Q]}.$$

Proof. Let (G, S) be a PR QGA. Define the distributions $H_j^{t,Q}$ for $j = 0, \ldots, Q$ as follows.

- $|s_0\rangle \leftarrow S$
- For $q \in \{1, 2, ..., j\}$, $|s_q\rangle \leftarrow \mu$.
- For $q \in \{j+1, ..., Q\}$, $h_q \leftarrow G$.

- Output $\{|s_q\rangle^{\otimes t}\}_{q\in\{1,\dots,j\}}$ and $\{(h_q\,|s_0\rangle)^{\otimes t}\}_{q\in\{j+1,\dots,Q\}}$.

It is clear that $D'_{\mathrm{pr},0} = H_0^{t,Q}$ and $D'_{\mathrm{pr},1} = H_Q^{t,Q}$. We claim that for any QPT adversary $\mathcal{A}$, any polynomials Q, t, and any $j \in [Q]$

$$\left|\Pr[1 \leftarrow \mathcal{A}(H_{j-1}^{t,Q})] - \Pr[1 \leftarrow \mathcal{A}(H_j^{t,Q})]\right| \leq \mathsf{negl}(\lambda).$$

To show this claim, assume that there exist a QPT $\mathcal{A}$, polynomials Q, t, p, and $j \in [Q]$ such that

$$\left|\Pr[1 \leftarrow \mathcal{A}(H_{j-1}^{t,Q})] - \Pr[1 \leftarrow \mathcal{A}(H_j^{t,Q})]\right| \geq \frac{1}{p(\lambda)}$$

for infinitely many λ. Then we can construct a QPT adversary $\mathcal{B}$ that breaks the security of the PR QGA as follows:

1. The challenger $\mathcal{C}$ chooses $|s_0\rangle \leftarrow S$ and $b \leftarrow \{0,1\}$.
2. If $b = 0$, $\mathcal{C}$ chooses $h \leftarrow G$ and sends $(|s_0\rangle, h|s_0\rangle)^{\otimes Qt}$ to $\mathcal{B}$. If $b = 1$, $\mathcal{C}$ chooses $|s\rangle \leftarrow \mu$ and sends $(|s_0\rangle, |s\rangle)^{\otimes Qt}$ to $\mathcal{B}$.
3. $\mathcal{B}$ runs $\mathcal{A}$ on input $\{|s_q\rangle^{\otimes t}\}_{q\in\{1,\dots,j-1\}}$, the received state (i.e., $(h|s_0\rangle)^{\otimes t}$ or $|s\rangle^{\otimes t}$), and $\{(h_q|s_0\rangle)^{\otimes t}\}_{q\in\{j+1,\dots,Q\}}$, and outputs $\mathcal{A}$'s output. Here, all $|s_q\rangle$ are t-designs and each $h_q \leftarrow G$. (From Lemma 2.9, we can replace Haar random states with t-design states.) Note that $\mathcal{B}$ can efficiently generate the $\{(h_q|s_0\rangle)^{\otimes t}\}_{q\in\{j+1,\dots,Q\}}$ because $\mathcal{B}$ receives $|s_0\rangle^{\otimes Qt}$ from $\mathcal{C}$.

We have

$$\left|\Pr[1 \leftarrow \mathcal{B} \mid b = 0] - \Pr[1 \leftarrow \mathcal{A}(H_{j-1}^{t,Q})]\right| \leq \mathsf{negl}(\lambda),$$
$$\left|\Pr[1 \leftarrow \mathcal{B} \mid b = 1] - \Pr[1 \leftarrow \mathcal{A}(H_j^{t,Q})]\right| \leq \mathsf{negl}(\lambda).$$

Therefore, we have

$$\begin{aligned}
&|\Pr[1 \leftarrow \mathcal{B} \mid b = 0] - \Pr[1 \leftarrow \mathcal{B} \mid b = 1]| \\
&\geq \left|\Pr[1 \leftarrow \mathcal{A}(H_{j-1}^{t,Q})] - \Pr[1 \leftarrow \mathcal{A}(H_j^{t,Q})]\right| - \mathsf{negl}(\lambda) \\
&\geq \frac{1}{p(\lambda)} - \mathsf{negl}(\lambda)
\end{aligned}$$

for infinitely many λ, which means that the PR QGA is broken. □

It is obvious that PR QGAs directly imply PRSGs.

Lemma 3.9. *If PR QGAs exist, then PRSGs exist.*

Proof. Let (G, S) be a PR QGA. From it, we construct a PRSG, $(\mathsf{KeyGen}, \mathsf{StateGen})$, as follows.

- $\mathsf{KeyGen}(1^\lambda) \to k$: Run $|s\rangle \leftarrow S(1^\lambda)$ and $g \leftarrow G(1^\lambda)$. Output $k := (|s\rangle, g)$.
- $\mathsf{StateGen}(1^\lambda, k) \to |\phi_k\rangle$: Parse $k = (|s\rangle, g)$. Output $|\phi_k\rangle := g|s\rangle$.

It is clear that this satisfies the security of PRSGs. □

Next, we give a variant of pseudorandomness, which we call *Haar-pseudorandom (Haar-PR)* because underlying states are generated according to the Haar measure.

Definition 3.10 (Haar-PR QGAs). *A QGA (G, S) is called* Haar-pseudorandom (Haar-PR) *if the following two distributions are computationally indistinguishable for any polynomial t:*

$$D_{\mathrm{HaarPR},0} : |s\rangle \leftarrow \mu, h \leftarrow G;\ \textit{return}\ (|s\rangle, h|s\rangle)^{\otimes t}$$
$$D_{\mathrm{HaarPR},1} : |s\rangle \leftarrow \mu, |s'\rangle \leftarrow \mu;\ \textit{return}\ (|s\rangle, |s'\rangle)^{\otimes t}$$

Remark 3.11. Haar-PR QGAs can be considered as a computational version of the statistical construction of PRSGs in the common Haar state model [AGL24, CCS24].

We can show that the multiple samples are also pseudorandom as in the case of PR QGAs Lemma 3.8.

Lemma 3.12. *Let (G, S) be a Haar-PR QGA. Then the following two distributions are computationally indistinguishable for any polynomials Q and t:*

$$D'_{\mathrm{HaarPR},0} : \textit{for}\ q \in [Q]\ |s_q\rangle \leftarrow \mu, h_q \leftarrow G;\ \textit{return}\ \{(|s_q\rangle, h_q|s_q\rangle)^{\otimes t}\}_{q\in[Q]}$$
$$D'_{\mathrm{HaarPR},1} : \textit{for}\ q \in [Q]\ |s_q\rangle \leftarrow \mu, |s'_q\rangle \leftarrow \mu;\ \textit{return}\ \{(|s_q\rangle, |s'_q\rangle)^{\otimes t}\}_{q\in[Q]}.$$

Proof. Let (G, S) be a Haar-PR QGA. For each $j \in \{0, 1, ..., Q\}$, define the following distribution $H_j^{t,Q}$.

- For $q \in \{1, 2, ..., j\}$, $|s_q\rangle \leftarrow \mu$ and $|s'_q\rangle \leftarrow \mu$.
- For $q \in \{j+1, j+2, ..., Q\}$, $|s_q\rangle \leftarrow \mu$ and $h_q \leftarrow G$.
- Output $\{(|s_q\rangle, |s'_q\rangle)^{\otimes t}\}_{q\in\{1,...,j\}}$ and $\{(|s_q\rangle, h_q|s_q\rangle)^{\otimes t}\}_{q\in\{j+1,...,Q\}}$.

It is clear that $D'_{\mathrm{HaarPR},0} = H_0^{t,Q}$ and $D'_{\mathrm{HaarPR},1} = H_Q^{t,Q}$. We claim that for any QPT adversary $\mathcal{A}$, any polynomials Q, t, and any $j \in [Q]$

$$\left|\Pr[1 \leftarrow \mathcal{A}(H_{j-1}^{t,Q})] - \Pr[1 \leftarrow \mathcal{A}(H_j^{t,Q})]\right| \leq \mathsf{negl}(\lambda).$$

To show it, assume that there exist a QPT $\mathcal{A}$, polynomials Q, t, p, and $j \in [Q]$ such that

$$\left|\Pr[1 \leftarrow \mathcal{A}(H_{j-1}^{t,Q})] - \Pr[1 \leftarrow \mathcal{A}(H_j^{t,Q})]\right| \geq \frac{1}{p(\lambda)}$$

for infinitely many λ. Then we can construct a QPT adversary $\mathcal{B}$ that breaks the security of the Haar-PR QGA as follows.

1. The challenger $\mathcal{C}$ chooses $b \leftarrow \{0, 1\}$.
2. If $b = 0$, $\mathcal{C}$ chooses $|s\rangle \leftarrow \mu$ and $h \leftarrow G$. and sends $(|s\rangle, h|s\rangle)^{\otimes t}$ to $\mathcal{B}$. If $b = 1$, $\mathcal{C}$ chooses $|s\rangle, |s'\rangle \leftarrow \mu$, and sends $(|s\rangle, |s'\rangle)^{\otimes t}$ to $\mathcal{B}$.
3. $\mathcal{B}$ prepares $\{(|s_q\rangle, |s'_q\rangle)^{\otimes t})\}_{q\in\{1,...,j-1\}}$ and $\{|s_q\rangle, h_q|s_q\rangle)^{\otimes t}\}_{q\in\{j+1,...,Q\}}$ by using t-designs. It then runs $\mathcal{A}$ on input $\{(|s_q\rangle, |s'_q\rangle)^{\otimes t})\}_{q\in\{1,...,j-1\}}$, the received state, and $\{|s_q\rangle, h_q|s_q\rangle)^{\otimes t}\}_{q\in\{j+1,...,Q\}}$, and outputs its output. Here, all $|s_q\rangle, |s'_q\rangle$ are t-designs.

We have

$$\left|\Pr[1 \leftarrow \mathcal{B} \mid b=0] - \Pr[1 \leftarrow \mathcal{A}(H_{j-1}^{t,Q})]\right| \leq \mathsf{negl}(\lambda),$$
$$\left|\Pr[1 \leftarrow \mathcal{B} \mid b=1] - \Pr[1 \leftarrow \mathcal{A}(H_{j}^{t,Q})]\right| \leq \mathsf{negl}(\lambda).$$

Therefore, we have

$$\begin{aligned}
&|\Pr[1 \leftarrow \mathcal{B} \mid b=0] - \Pr[1 \leftarrow \mathcal{B} \mid b=1]| \\
&\geq \left|\Pr[1 \leftarrow \mathcal{A}(H_{j-1}^{t,Q})] - \Pr[1 \leftarrow \mathcal{A}(H_{j}^{t,Q})]\right| - \mathsf{negl}(\lambda) \\
&\geq \frac{1}{p(\lambda)} - \mathsf{negl}(\lambda)
\end{aligned}$$

for infinitely many λ, which means that the Haar-PR QGA is broken. □

We also define a natural quantum analogue of *Decisional Diffie-Hellman (DDH)*.

Definition 3.13 (DDH QGAs). *A QGA (G, S) is called* Decisional Diffie-Hellman (DDH) *if the following two distributions are computationally indistinguishable for any polynomials Q and t:*

$$D_{\mathrm{DDH},0} : |s_0\rangle \leftarrow S, \tilde{g}, g \leftarrow G;\ \textit{return}\ \{(|s_0\rangle, \tilde{g}\,|s_0\rangle, g\,|s_0\rangle, \tilde{g}g\,|s_0\rangle)^{\otimes t}\}_{q\in[Q]}$$
$$D_{\mathrm{DDH},1} : |s_0\rangle \leftarrow S, \tilde{g}, g, h \leftarrow G;\ \textit{return}\ \{(|s_0\rangle, \tilde{g}\,|s_0\rangle, g\,|s_0\rangle, h\,|s_0\rangle)^{\otimes t}\}_{q\in[Q]}.$$

We next give another variant of DDH, which we call *Haar Decisional Diffie-Hellman (Haar-DDH)*. We will use it for the case that G is non-commutative.

Definition 3.14 (Haar-DDH QGAs). *A QGA (G, S) is called* Haar-Decisional Diffie-Hellman (Haar-DDH) *if the following two distributions are computationally indistinguishable for any polynomials Q and t:*

$$D_{\mathrm{HaarDDH},0} : g \leftarrow G,\ \textit{for}\ q\in[Q]\ |s_q\rangle \leftarrow \mu;\ \textit{return}\ \{(|s_q\rangle, g\,|s_q\rangle)^{\otimes t}\}_{q\in[Q]}$$
$$D_{\mathrm{HaarDDH},1} : \textit{for}\ q\in[Q]\ |s_q\rangle \leftarrow \mu, h_q \leftarrow G;\ \textit{return}\ \{(|s_q\rangle, h_q\,|s_q\rangle)^{\otimes t}\}_{q\in[Q]}.$$

3.4 Naor-Reingold QGAs

We also introduce an assumption that is a key for our construction of PRFSGs from pseudorandom QGAs. We dub it as *Naor-Reingold (NR)* QGAs because this assumption will be used to show the pseudorandomness of the Naor-Reingold-style PRFSGs.

Definition 3.15 (NR QGAs). *A QGA (G, S) is called* Naor-Reingold (NR) *if the following two distributions are computationally indistinguishable for any polynomial Q and t:*

$$D_{\mathrm{NR},0} : |s_0\rangle \leftarrow S, \tilde{g} \leftarrow G,\ \textit{for}\ q\in[Q]\ g_q \leftarrow G;\ \textit{return}\ \{(g_q\,|s_0\rangle, \tilde{g}g_q\,|s_0\rangle)^{\otimes t}\}_{q\in[Q]}$$
$$D_{\mathrm{NR},1} : |s_0\rangle \leftarrow S,\ \textit{for}\ q\in[Q]\ g_q \leftarrow G, h_q \leftarrow G;\ \textit{return}\ \{(g_q\,|s_0\rangle, h_q\,|s_0\rangle)^{\otimes t}\}_{q\in[Q]}.$$

If we consider classical group actions with special properties, the NR-GA follows from the pseudorandomness of group actions. (See Appendix B for the details.) In the case of QGA, we will face several problems since we cannot use algebraic structures; G might not be a group, and S is not closed. Fortunately, the NR property of QGA follows from its PR, Haar-PR, and Haar-DDH properties.

Lemma 3.16. *If a QGA is PR, Haar-PR, and Haar-DDH, then it is NR.*

Proof. To show the lemma, we introduce an intermediate distribution D'_{NR} defined as follows:

$$D'_{\mathrm{NR}}: \text{ for } q \in [Q] \ |s_q\rangle \leftarrow \mu, \tilde{h}_q \leftarrow G; \text{ return } \{(|s_q\rangle, \tilde{h}_q |s_q\rangle)^{\otimes t}\}_{q\in[Q]}.$$

We show that $D_{\mathrm{NR},0} \approx_c D'_{\mathrm{NR}} \approx_c D_{\mathrm{NR},1}$ under our assumptions.

Proof of $D_{\mathrm{NR},0} \approx_c D'_{\mathrm{NR}}$. We first show that $D_{\mathrm{NR},0} \approx_c D'_{\mathrm{NR}}$ if QGA is PR and Haar-DDH. Let us consider the following distribution:

$$D'_{\mathrm{NR},0}: \tilde{g} \leftarrow G, \text{ for } q \in [Q] \ |s_q\rangle \leftarrow \mu; \text{ return } \{(|s_q\rangle, \tilde{g} |s_q\rangle)^{\otimes t}\}_{q\in[Q]}.$$

As in Claim 3.17 below, we have $D_{\mathrm{NR},0} \approx_c D'_{\mathrm{NR},0}$ if QGA is PR. We also have $D'_{\mathrm{NR},0} \approx_c D'_{\mathrm{NR}}$, which directly follows from the Haar-DDH assumption (Definition 3.14). Hence, we have $D_{\mathrm{NR},0} \approx_c D'_{\mathrm{NR}}$. □

Claim 3.17. If QGA is PR, then $D_{\mathrm{NR},0} \approx_c D'_{\mathrm{NR},0}$.

Proof of Claim 3.17. Assuming that QGA is PR, we know that $D'_{\mathrm{pr},0}$ and $D'_{\mathrm{pr},1}$ are computationally indistinguishable due to Lemma 3.8. To show $D_{\mathrm{NR},0} \approx_c D'_{\mathrm{NR},0}$, it is enough to show that we can efficiently convert samples from $D'_{\mathrm{pr},0}$ and $D'_{\mathrm{pr},1}$ into $D_{\mathrm{NR},0}$ and $D'_{\mathrm{NR},0}$, respectively, in an oblivious way. Suppose that we are given samples $\{|y_q\rangle^{\otimes 2t}\}_{q\in[Q]}$ from $D'_{\mathrm{pr},0}$ or $D'_{\mathrm{pr},1}$, where $|y_q\rangle = h_q |s_0\rangle$ for $D_{\mathrm{pr},0}$ and $|y_q\rangle = |s_q\rangle$ for $D_{\mathrm{pr},1}$. To prepare samples for $D_{\mathrm{NR},0}$ or $D'_{\mathrm{NR},0}$, we choose $\tilde{g} \leftarrow G$ and compute $(|y_q\rangle, \tilde{g} |y_q\rangle)^{\otimes t}$ for $q \in [Q]$. If the input distribution is $D_{\mathrm{pr},0}$, then the output distribution is $D_{\mathrm{NR},0}$. On the other hand, if the input distribution is $D_{\mathrm{pr},1}$, then the output distribution is $D'_{\mathrm{NR},0}$. □

Proof of $D'_{\mathrm{NR}} \approx_c D_{\mathrm{NR},1}$. We then show $D'_{\mathrm{NR}} \approx_c D_{\mathrm{NR},1}$ if QGA is PR and Haar-PR. We consider the following distribution:

$$D'_{\mathrm{NR},1}: \text{ for } q \in [Q] \ |s_q\rangle \leftarrow \mu, |s'_q\rangle \leftarrow \mu; \text{ return } \{(|s_q\rangle, |s'_q\rangle)^{\otimes t}\}_{q\in[Q]}.$$

The following claim (Claim 3.18) shows that $D_{\mathrm{NR},1} \approx_c D'_{\mathrm{NR},1}$ if QGA is PR. Lemma 3.12 shows that, if QGA is Harr-PR, then we have that $D'_{\mathrm{NR}} \approx_c D'_{\mathrm{NR},1}$. This completes the proof. □

Claim 3.18. If QGA is PR, then $D_{\mathrm{NR},1} \approx_c D'_{\mathrm{NR},1}$.

Proof of Claim 3.18. We construct an efficient quantum algorithm that converts samples from $D'_{\mathrm{pr},0}$ and $D'_{\mathrm{pr},1}$ in Lemma 3.8 and into samples from $D_{\mathrm{NR},1}$ and $D'_{\mathrm{NR},1}$, respectively. Suppose that we are given samples $\{|y_q\rangle^{\otimes t}\}_{q\in[2Q]}$ from $D'_{\mathrm{pr},0}$ or $D'_{\mathrm{pr},1}$, where $|y_q\rangle = h_q |s_0\rangle$ for $D_{\mathrm{pr},0}$ and $|y_q\rangle = |s_q\rangle$ for $D_{\mathrm{pr},1}$. The converter outputs $\{(|y_{2q-1}\rangle, |y_{2q}\rangle)^{\otimes t}\}_{q\in[Q]}$ by rearranging samples. If the input distribution is $D_{\mathrm{pr},0}$, then the output distribution is $D_{\mathrm{NR},1}$. On the other hand, if the input distribution is $D_{\mathrm{pr},1}$, then the output distribution is D'_{NR} as we wanted. □

Wrapping up the lemmas and claims, we have shown that $D_{\mathrm{NR},0} \approx_c D'_{\mathrm{NR}} \approx_c D_{\mathrm{NR},1}$ in Lemma 3.16. □

If G is *commutative*, then we only need the DDH assumption as Boneh et al. [BKW20].

Lemma 3.19. *Let (G, S) be a QGA. If G is commutative and (G, S) is DDH, then (G, S) is NR.*

Proof. For $i = 0, \ldots, Q$, we consider the following hybrid distributions $\bar{D}_i$ of $\{(|\phi_q\rangle, |\psi_q\rangle)^{\otimes t}\}_{q\in[Q]}$:

- $\tilde{g} \leftarrow G$ and $|s_0\rangle \leftarrow S$.
- For $j = 1, \ldots, i$, $|\phi_q\rangle := g_q|s_0\rangle$ and $|\psi_q\rangle := h_q|s_0\rangle$, where $g_q, h_q \leftarrow G$.
- For $j = i+1, \ldots, Q$, $|\phi_q\rangle := g_q|s_0\rangle$ and $|\psi_q\rangle := \tilde{g}h_q|s_0\rangle$, where $g_q, h_q \leftarrow G$.

By using the following claim, we have $\bar{D}_0 \approx_c \bar{D}_1 \approx_c \cdots \approx_c \bar{D}_Q$ if the DDH assumption holds. □

Claim 3.20. Let (G, S) be a QGA. If G is commutative and (G, S) is DDH, then, for $i = 1, \ldots, Q$, $\bar{D}_{i-1} \approx_c \bar{D}_i$ holds.

Proof. Suppose that there exists $\mathcal{A}$ distinguishing $\bar{D}_{i-1}$ from $\bar{D}_i$. We construct an adversary $\mathcal{B}$ against the DDH assumption as follows:

- Given a sample $(|s_0\rangle, \tilde{g}|s_0\rangle, g|s_0\rangle, h|s_0\rangle)^{\otimes tQ}$, where $h = \tilde{g}g$ or random, $\mathcal{B}$ prepares a sample $\{(|\phi_q\rangle, |\psi_q\rangle)^{\otimes t}\}_{q\in[Q]}$ as follows:
  - for $q = 1, \ldots, i-1$, take random $g_q, h_q \leftarrow G$ and set $(|\phi_q\rangle, |\psi_q\rangle) := (g_q|s_0\rangle, h_q|s_0\rangle)$;
  - for $q = i$, set $(|\phi_q\rangle, |\psi_q\rangle) = (g|s_0\rangle, h|s_0\rangle)$;
  - for $q = i+1, \ldots, Q$, take random $g_q \leftarrow G$ and set $(|\phi_q\rangle, |\psi_q\rangle) = (g_q|s_0\rangle, g_q\tilde{g}|s_0\rangle)$.
- It runs $\mathcal{A}$ on input $\{(|\phi_q\rangle, |\psi_q\rangle)^{\otimes t}\}_{j\in[Q]}$ and outputs $\mathcal{A}$'s decision.

We note that, due to commutativity of G, the last $Q - i$ samples are equivalent to $(g_q|s_0\rangle, \tilde{g}g_q|s_0\rangle)$. If $h = \tilde{g}g$, then $(|\phi_i\rangle, |\psi_i\rangle) = (g|s_0\rangle, \tilde{g}g|s_0\rangle)$ and $\mathcal{B}$ perfectly simulates the distribution $\bar{D}_{i-1}$ since G is a group and the distribution of If h is random, then $\mathcal{B}$ perfectly simulates the distribution $\bar{D}_i$. Thus, $\mathcal{B}$'s advantage is equivalent to $\mathcal{A}$'s advantage distinguishing $\bar{D}_{i-1}$ and $\bar{D}_i$. □

4 Construction of (Classical-Query) PRFSGs

4.1 Construction

We construct a Naor-Reingold-style PRFSG from QGA (that is secure against classical queries) in this section.

Theorem 4.1. *Let (G, S) be a QGA. If (G, S) is PR and NR, then the following* $(\mathsf{KeyGen}, \mathsf{StateGen})$ *is a PRFSG whose input space is* $\{0,1\}^\ell$.

- $\mathsf{KeyGen}(1^\lambda) \to k$: *Sample $g_0, g_1, ..., g_\ell \leftarrow G$ and $|s_0\rangle \leftarrow S$. Output $k := (g_0, g_1, ..., g_\ell, |s_0\rangle)$. (Note that $|s_0\rangle$ here is not a physical quantum state but its classical description.)*
- $\mathsf{StateGen}(k, x) \to |\phi_k(x)\rangle$: *Parse $k = (g_0, g_1, ..., g_\ell, |s_0\rangle)$ and $x = (x[1], \ldots, x[\ell]) \in \{0,1\}^\ell$. Output*

$$|\phi_k(x)\rangle := g_\ell^{x[\ell]} g_{\ell-1}^{x[\ell-1]} \cdots g_1^{x[1]} g_0 \, |s_0\rangle \, . \tag{23}$$

From Lemma 3.16 and Lemma 3.19, we obtain the following corollaries.

Corollary 4.2. *If a QGA is PR, Haar-PR, and Haar-DDH, then the above construction is a PRFSG.*

Corollary 4.3. *If a QGA is DDH and G is commutative, then the above construction is a PRFSG.*

To show Theorem 4.1, we define three games Real, Hybrid, and Ideal defined as follows:

- Real: This is the PRFSG security game whose oracle is $\mathsf{StateGen}(k,\cdot)$. That is, the challenger $\mathcal{C}$ chooses $k \leftarrow \mathsf{KeyGen}(1^\lambda)$ and runs $\mathcal{A}$ with the oracle $\mathsf{StateGen}(k,\cdot)$, which takes $x \in \{0,1\}^\ell$ as input and returns $|\phi_k(x)\rangle$. $\mathcal{C}$ outputs $\mathcal{A}$'s decision.
- Hybrid: This is the PRFSG security game whose oracle is defined as follows: On query x, if it is not queried before, then the oracle samples $h_x \leftarrow G$ and returns $h_x |s_0\rangle$; otherwise, it returns stored $h_x |s_0\rangle$.
- Ideal: This is the PRFSG security game whose oracle is $\mathcal{O}_{\mathrm{Haar}}$ defined as follows: On query x, if it is not queried before, then $\mathcal{O}_{\mathrm{Haar}}$ samples $|s_x\rangle \leftarrow \mu$ and returns $|s_x\rangle$; otherwise, it returns $|s_x\rangle$.

Lemma 4.4 below shows that Real is computationally indistinguishable from Hybrid if QGA is NR. The proof is obtained by following the proofs in Naor and Reingold [NR04] and Alamati et al. [ADMP20]. It is easy to show that Hybrid and Ideal are computationally indistinguishable if QGA is PR (Lemma 4.6). Thus, we obtain Theorem 4.1. The lemmas follow.

Lemma 4.4. Real *and* Hybrid *are computationally indistinguishable if QGA is NR.*

Proof. We define the following hybrid games Game_j for $j = 0,\dots,\ell$: The challenger samples $|s_0\rangle \leftarrow S$, $g_0 \leftarrow G$, and $g_i \leftarrow G$ for $i \in [j+1,\ell]$. Let q-th adversary's query be $x_q = (x_q[1],\dots,x_q[\ell]) \in \{0,1\}^\ell$. The challenger returns a quantum state $|f_{j,q}\rangle$ defined as follows:

1. If $j = 0$, then the challenger let $|y_q\rangle = g_0 |s_0\rangle$.
2. Otherwise
   - if there exists $q' < q$ satisfying $(x_q[1],\dots,x_q[j]) = (x_{q'}[1],\dots,x_{q'}[j])$, then $|y_q\rangle = |y_{q'}\rangle$;
   - otherwise, it samples $g_q \leftarrow G$ and $|y_q\rangle \coloneqq g_q |s_0\rangle$.
3. Return $|f_{j,q}\rangle \coloneqq g_\ell^{x_q[\ell]} \cdots g_{j+1}^{x_q[j+1]} |y_q\rangle$.

It is easy to verify Game_0 and Game_ℓ are Real and Hybrid, respectively. The following claim shows $\mathsf{Game}_0 \approx_c \mathsf{Game}_1 \approx_c \cdots \approx_c \mathsf{Game}_\ell$ if the QGA is NR. □

Claim 4.5. For $j = 0,\dots,\ell-1$, Game_j and Game_{j+1} are computationally indistinguishable if the QGA is NR.

Proof. The definition of NR QGAs implies that $D_{\mathrm{NR},0} \approx_c D_{\mathrm{NR},1}$ under our hypothesis. Thus, it is enough to construct a reduction algorithm $\mathcal{B}$ distinguishing $D_{\mathrm{NR},0}$ and $D_{\mathrm{NR},1}$ by using an adversary $\mathcal{A}$ distinguishing Game_j and Game_{j+1}. Our reduction algorithm is defined as follows:

1. $\mathcal{B}$ is given $\{(|y_q\rangle, |z_q\rangle)^{\otimes Q}\}_{q\in[Q]}$, where $(|y_q\rangle, |z_q\rangle) = (g_q |s_0\rangle, \tilde{g} g_q |s_0\rangle)$ in $D_{\mathrm{NR},0}$ or $(g_q |s_0\rangle, h_q |s_0\rangle)$ in $D_{\mathrm{NR},1}$. It prepares $g_{j+2},\dots,g_\ell \leftarrow G$. It initializes $c = 1$.
2. Receiving a q-th query x_q from $\mathcal{A}$, it checks if there exists $q' < q$ satisfying $(x_q[1],\dots,x_q[j]) = (x_{q'}[1],\dots,x_{q'}[j])$. If so, it uses previously-defined consistent quantum states, that is, sets $|\tilde{y}_q\rangle \coloneqq |\tilde{y}_{q'}\rangle$ and $|\tilde{z}_q\rangle \coloneqq |\tilde{z}_{q'}\rangle$. Otherwise, it picks new quantum states from the pool, that is, sets $|\tilde{y}_q\rangle \coloneqq |y_c\rangle$ and $|\tilde{z}_q\rangle = |z_c\rangle$ and increments c. It then answers

$$|f_{j,q}\rangle \coloneqq \begin{cases} g_\ell^{x_q[\ell]} \cdots g_{j+2}^{x_q[j+2]} |\tilde{y}_q\rangle & \text{if } x_q[j+1] = 0 \\ g_\ell^{x_q[\ell]} \cdots g_{j+2}^{x_q[j+2]} |\tilde{z}_q\rangle & \text{if } x_q[j+1] = 1. \end{cases}$$

3. $\mathcal{B}$ outputs $\mathcal{A}$'s decision.

If the given samples follow $D_{\mathrm{NR},0}$, then the above simulation perfectly simulates Game_j by considering $\tilde{g}$ as g_{j+1}. If the given samples follow $D_{\mathrm{NR},1}$, then the above simulation perfectly simulates Game_{j+1} since g_q's and h_q's in $D_{\mathrm{NR},1}$ are chosen independently. Thus, the claim follows. □

Lemma 4.6. Hybrid *and* Ideal *are computationally indistinguishable if QGA is PR.*

Proof. This lemma immediately follows from Lemma 3.8. □

4.2 On Quantum-Query PRFSGs

As remarked in Remark 2.8, we only consider classical-query PRFSGs (Definition 2.6). Currently, we fail to show either positive results that our NR-type PRFSG is secure against quantum queries or negative results, that is, the separation of classical-query and quantum-query PRFSGs. We discuss barriers for positive or negative results in the following.

Barriers for positive results. We tried to show our NR-type PRFSG is secure against *quantum* queries, but we faced some problems. For example, we can consider the quantum-query version of Hybrid and Ideal. Can we show the computational indistinguishability between them from PR QGAs?

For simplicity, we consider the case of small input space $\{0,1\}^\ell$ with $\ell = O(\log(\lambda))$.[19] We identify $\{0,1\}^\ell$ with $[2^\ell]$. If we consider PRFs, then classical-query PRFs against a quantum adversary is also quantum-query PRFs. This is because a classical-query adversary can ask all inputs $1,\dots,2^\ell$ to its oracle and simulate answers on quantum queries. However, in the case of PRFSGs, we do not have such implications. A classical-query adversary can obtain all states $|s_x\rangle$, which is $|\phi_k(x)\rangle$ or $|\psi_x\rangle$, for all $x \in [2^\ell]$. How can we simulate the answers to quantum queries?

For example, if we implement a mapping $|x\rangle \mapsto |x\rangle |s_x\rangle$ by using a controlled swap, then the results will be as follows:

$$\begin{aligned}&|x\rangle |0^n\rangle \otimes (|s_1\rangle^{\otimes Q} \otimes \cdots \otimes |s_{2^\ell}\rangle^{\otimes Q})\\ &\quad \mapsto_{\text{controlled swap}} |x\rangle |s_x\rangle \otimes (|s_1\rangle^{\otimes Q} \otimes \cdots \otimes |0^n\rangle |s_x\rangle^{\otimes (Q-1)} \otimes \cdots \otimes |s_{2^\ell}\rangle^{\otimes Q}).\end{aligned}$$

Unfortunately, these operations produce an entanglement between the states for the adversary and the reduction algorithm $\mathcal{B}$ and our attempt fails.

Barriers for negative results. Zhandry showed that if there exists a classical-query PRF, then there is a classical-query PRF insecure against quantum-query attacks [Zha12a, Theorem 3.1]. One would consider we can show its analogy for PRFSGs by mimicking his proof. Unfortunately, this strategy does not work because of the following reasons.

We briefly review Zhandry's strategy: Suppose that there exists a PRF PRF whose input space is $[N]$, where $N = 2^{\omega(\log(\lambda))}$. (Otherwise, there is no separation as we explained in the above.) We then define a new PRF whose input space is $[N']$, where N' is a power of 2 larger than $4N^2$. The new key is a pair of the original key k and a random prime $a \in (N/2, N]$. The new PRF is defined as $\mathsf{PRF}'\colon ((k,a),x) \mapsto \mathsf{PRF}(k, x \bmod a)$, which has a secret period a. Zhandry then showed that 1) if PRF is classical-query secure, then PRF' is also and 2) if PRF is quantum-query secure, then PRF' is *not*,

[19] If $\ell = \omega(\log(\lambda))$, we then invoke the small-range distribution argument in Zhandry [Zha12b].

which implies there exists a PRF that is classical-query secure but quantum-query insecure. To show 2), Zhandry constructed a quantum-query adversary breaking the security of PRF'. Roughly speaking, using the period-finding algorithm in Boneh and Lipton [BL95], the adversary can find a period a in polynomial time with a probability of at least $1/2$. The Boneh-Lipton period-finding algorithm uses a sufficiently large number W and prepare a quantum state $\frac{1}{\sqrt{W}}\sum_{x,s\in\mathbb{Z}_W}\exp(2\pi ixs/W)\,|s\rangle\,|\mathsf{PRF}'_{k,a}(x)\rangle = \frac{1}{\sqrt{W}}\sum_{x,s\in\mathbb{Z}_W}\exp(2\pi ixs/W)\,|s\rangle\,|\mathsf{PRF}_k(x \bmod a)\rangle$. We note that the success probability of the algorithm strongly depends on the distinctness of $\mathsf{PRF}(k,0),\ldots,\mathsf{PRF}(k,a-1)$ and good measurements. The distinctness follows from the quantum-query security of PRF. The measurement is done by using the computational basis.

In the case of PRFSGs, we can construct an analogue of a new PRF in the same way. While the distinctness follows from the quantum-query security of PRFSG, we fail to give the measurement to distinguish a independent samples $|\psi_1\rangle,\ldots,|\psi_a\rangle$ from the Haar measure.

5 Candidates of QGA

In this section, we provide some examples of candidate constructions of QGAs. The one is taken from random quantum circuits. The other candidates are inspired by Instantaneous quantum polynomial (IQP) circuits [BMS16, BJS11]. Those ones feature a commutativity of two unitaries taken by G.

Definition 5.1 (Candidate 1: Random circuit QGA). *We define*

- $G(1^\lambda)\to[g]$: *Output a random quantum circuit g.*
- $S(1^\lambda)\to[|s\rangle]$: *Output* $|s\rangle\coloneqq|0^\lambda\rangle$.

Random quantum circuits are conjectured to be PRUs [AQY22], while PR, Haar-PR, and Haar-DDH QGA seem to be incomparable with PRUs.

Inspired by IQP, we conjecture that the following two QGAs are PR, Haar-PR, and Haar-DDH.

Definition 5.2 (Candidate 2: IQP QGA with random Z-diagonal circuit). *We define an IQP QGA (G,S) as follows:*

- $G(1^\lambda)\to[g]$: *Take a random Z-diagonal circuit D* [20] *and output a description $[D]$. This defines $g=H^{\otimes\lambda}\cdot D\cdot H^{\otimes\lambda}$.*
- $S(1^\lambda)\to[|s\rangle]$: *Output* $|s\rangle\coloneqq|0^\lambda\rangle$.

Definition 5.3 (Candidate 3: IQP QGA with random sparse polynomials). *Let $d\in[1,\lambda]$ and polynomial $w=w(\lambda)$. Let $\mathcal{D}_{d,w}$ be*

$$\mathcal{D}_{d,w}\coloneqq\left\{\begin{array}{l}D\colon\ |x_1,\ldots,x_\lambda\rangle\to(-1)^{f(x_1,\ldots,x_\lambda)}\,|x_1,\ldots,x_\lambda\rangle\\ |\ f\in\mathbb{F}_2[x_1,\ldots,x_\lambda],\deg(f)\le d,\mathrm{term}(f)\le w\end{array}\right\},$$

where deg *is a total degree of f and* term *is a number of terms of f. We then define a set of IQP circuits with respect to $\mathcal{D}$:*

$$\mathcal{G}_{d,w}\coloneqq\{H^{\otimes\lambda}\cdot D\cdot H^{\otimes\lambda}\mid D\in\mathcal{D}_{d,w}\}.$$

We define an IQP QGA (G,S) as follows:

[20] E.g., a random circuit with gates $\{T, CS\}$ [BMS16].

- $G(1^\lambda) \to [g]$: *Take a random sample* $D \leftarrow \mathcal{D}_{d,w}$ *and output a description* $[D]$. *This defines* $g = H^{\otimes\lambda} \cdot D \cdot H^{\otimes\lambda}$.
- $S(1^\lambda) \to [|s\rangle]$: *Output* $|s\rangle \coloneqq |0^\lambda\rangle$.

Candidates 2 and 3 differ the way to choose the Z-digaonal circuit D. We note that $gh = hg$ holds for any $g = H^{\otimes\lambda} D_g H^{\otimes\lambda}$ and $h = H^{\otimes\lambda} D_h H^{\otimes\lambda}$ chosen by G in both candidates.

IQP random circuits are not PRUs. In fact, if the adversary queries $H^{\otimes\lambda}|0^\lambda\rangle$ to the oracle, the oracle always returns $H^{\otimes\lambda}|0^\lambda\rangle$ if the oracle is the IQP oracle, but such probability is exponentially small if the oracle is the Haar random unitary oracle.[21] Currently, we do not know that IQP random circuits are PR QGAs; It is shown that the state $\sum_x (-1)^{f(x)}|x\rangle$ with random f is Haar random [BS20]. We do not find any evidence that IQP random circuits are not Haar-PR or DDH QGAs.

Acknowledgements. TM is supported by JST CREST JPMJCR23I3, JST Moonshot R&D JPMJMS2061-5-1-1, JST FOREST, MEXT QLEAP, the Grant-in Aid for Transformative Research Areas (A) 21H05183, and the Grant-in-Aid for Scientific Research (A) No.22H00522.

References

[AA11] Scott Aaronson and Alex Arkhipov. The computational complexity of linear optics. In Lance Fortnow and Salil P. Vadhan, editors, *43rd ACM STOC*, pages 333–342. ACM Press, June 2011. (Cited on page 9.)

[ABF+16] Gorjan Alagic, Anne Broadbent, Bill Fefferman, Tommaso Gagliardoni, Christian Schaffner, and Michael St. Jules. Computational security of quantum encryption. In Anderson C. A. Nascimento and Paulo Barreto, editors, *ICITS 16*, volume 10015 of *LNCS*, pages 47–71. Springer, Heidelberg, August 2016. (Cited on page 27.)

[ABP15] Michel Abdalla, Fabrice Benhamouda, and Alain Passelègue. An algebraic framework for pseudorandom functions and applications to related-key security. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *CRYPTO 2015, Part I*, volume 9215 of *LNCS*, pages 388–409. Springer, Heidelberg, August 2015. (Cited on page 5.)

[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 3, 4, 5, 6, 19, 29, 30, 31, 32.)

[AGL24] Prabhanjan Ananth, Aditya Gulati, and Yao-Ting Lin. Cryptography in the common Haar state model: Feasibility results and separations. Cryptology ePrint Archive, Paper 2024/1043, 2024. To appear TCC 2024. (Cited on page 6, 7, 15.)

[AGQY22] Prabhanjan Ananth, Aditya Gulati, Luowen Qian, and Henry Yuen. Pseudorandom (function-like) quantum state generators: New definitions and applications. In Eike Kiltz and Vinod Vaikuntanathan, editors, *TCC 2022, Part I*, volume 13747 of *LNCS*, pages 237–265. Springer, Heidelberg, November 2022. (Cited on page 3, 7, 8, 11.)

[21] We thank Shogo Yamada for pointing out it.

[AQY22] Prabhanjan Ananth, Luowen Qian, and Henry Yuen. Cryptography from pseudorandom quantum states. In Yevgeniy Dodis and Thomas Shrimpton, editors, *CRYPTO 2022, Part I*, volume 13507 of *LNCS*, pages 208–236. Springer, Heidelberg, August 2022. (Cited on page 3, 7, 8, 10, 11, 21.)

[BCDD+24] Alessandro Budroni, Jesús-Javier Chi-Domínguez, Giuseppe D'Alconzo, Antonio J. Di Scala, and Mukul Kulkarni. Don't use it twice! Solving relaxed linear code equivalence problems. Cryptology ePrint Archive, Paper 2024/244, 2024. To appear ASIACRYPT 2024. (Cited on page 4.)

[BCQ23] Zvika Brakerski, Ran Canetti, and Luowen Qian. On the computational hardness needed for quantum cryptography. ITCS 2023, 2023. (Cited on page 3.)

[BDJR97] Mihir Bellare, Anand Desai, Eric Jokipii, and Phillip Rogaway. A concrete security treatment of symmetric encryption. In *38th FOCS*, pages 394–403. IEEE Computer Society Press, October 1997. (Cited on page 27.)

[BFNV19] Adam Bouland, Bill Fefferman, Chinmay Nirkhe, and Umesh Vazirani. On the complexity and verification of quantum random circuit sampling. *Nature Physics*, 15:159–163, 2019. (Cited on page 9.)

[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 27, 29.)

[BJS11] Michael J. Bremner, Richard Jozsa, and Dan J. Shepherd. Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 467:459–472, 2011. (Cited on page 9, 21.)

[BKW20] Dan Boneh, Dmitry Kogan, and Katharine Woo. Oblivious pseudorandom functions from isogenies. In Shiho Moriai and Huaxiong Wang, editors, *ASIACRYPT 2020, Part II*, volume 12492 of *LNCS*, pages 520–550. Springer, Heidelberg, December 2020. (Cited on page 4, 5, 17, 29, 31, 32.)

[BL95] Dan Boneh and Richard J. Lipton. Quantum cryptanalysis of hidden linear functions (extended abstract). In Don Coppersmith, editor, *CRYPTO'95*, volume 963 of *LNCS*, pages 424–437. Springer, Heidelberg, August 1995. (Cited on page 21.)

[BMR10] Dan Boneh, Hart William Montgomery, and Ananth Raghunathan. Algebraic pseudorandom functions with improved efficiency from the augmented cascade. In Ehab Al-Shaer, Angelos D. Keromytis, and Vitaly Shmatikov, editors, *ACM CCS 2010*, pages 131–140. ACM Press, October 2010. (Cited on page 5.)

[BMS16] Michael J. Bremner, Ashley Montanaro, and Dan J. Shepherd. Average-case complexity versus approximate simulation of commuting quantum computations. *Physical Review Letters*, 117:080501, 2016. (Cited on page 9, 21.)

[BS20] Zvika Brakerski and Omri Shmueli. Scalable pseudorandom quantum states. In Daniele Micciancio and Thomas Ristenpart, editors, *CRYPTO 2020, Part II*, volume 12171 of *LNCS*, pages 417–440. Springer, Heidelberg, August 2020. (Cited on page 22.)

[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 3, 4.)

[CCS24] Boyang Chen, Andrea Coladangelo, and Or Sattath. The power of a single haar random state: constructing and separating quantum pseudorandomness, 2024. (Cited on page 15.)

[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 3, 4.)

[Cou06] Jean-Marc Couveignes. Hard homogeneous spaces. Cryptology ePrint Archive, Paper 2006/291, 2006. https://eprint.iacr.org/2006/291. (Cited on page 3, 4.)

[DD24] Giuseppe D'Alconzo and Antonio J. Di Scala. Representations of group actions and their applications in cryptography. *Finite Fields and Their Applications*, 99:102476, 2024. (Cited on page 3, 4.)

[DH76] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976. (Cited on page 4.)

[EHK+13] Alex Escala, Gottfried Herold, Eike Kiltz, Carla Ràfols, and Jorge Villar. An algebraic framework for Diffie-Hellman assumptions. In Ran Canetti and Juan A. Garay, editors, *CRYPTO 2013, Part II*, volume 8043 of *LNCS*, pages 129–147. Springer, Heidelberg, August 2013. (Cited on page 5.)

[FKM+18] Keisuke Fujii, Hirotada Kobayashi, Tomoyuki Morimae, Harumichi Nishimura, Seiichiro Tani, and Shuhei Tamate. Impossibility of classically simulating one-clean-qubit model with multiplicative error. *Physical Review Letters*, 120:200502, 2018. (Cited on page 9.)

[GGM84] Oded Goldreich, Shafi Goldwasser, and Silvio Micali. How to construct random functions (extended abstract). In *25th FOCS*, pages 464–479. IEEE Computer Society Press, October 1984. (Cited on page 7.)

[GGM86] Oded Goldreich, Shafi Goldwasser, and Silvio Micali. How to construct random functions. *Journal of the ACM*, 33(4):792–807, 1986. (Cited on page 6.)

[HM24a] Taiga Hiroka and Tomoyuki Morimae. Quantum cryptography from meta-complexity, 2024. (Cited on page 9.)

[HM24b] Hsin-Yuan Huang and Fermi Ma. Talk at simons institute, 2024. (Cited on page 3, 8.)

[IL89] Russell Impagliazzo and Michael Luby. One-way functions are essential for complexity based cryptography (extended abstract). In *30th FOCS*, pages 230–235. IEEE Computer Society Press, October / November 1989. (Cited on page 3.)

[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 3, 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 3, 8, 9.)

[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 3, 4, 7.)

[KQST23] William Kretschmer, Luowen Qian, Makrand Sinha, and Avishay Tal. Quantum cryptography in algorithmica. In Barna Saha and Rocco A. Servedio, editors, *55th ACM STOC*, pages 1589–1602. ACM Press, June 2023. (Cited on page 3.)

[Kre21] W. Kretschmer. Quantum pseudorandomness and classical complexity. *TQC 2021*, 2021. (Cited on page 3, 8, 11.)

[KT24a] Dakshita Khurana and Kabir Tomer. Commitments from quantum one-wayness. In Bojan Mohar, Igor Shinkar, and Ryan O'Donnell, editors, *56th STOC*, pages 968–978. ACM, 2024. (Cited on page 3, 8.)

[KT24b] Dakshita Khurana and Kabir Tomer. Founding quantum cryptography on quantum advantage, or, towards cryptography from #P-hardness. Cryptology ePrint Archive, Paper 2024/1490, 2024. (Cited on page 9.)

[LMW24] Alex Lombardi, Fermi Ma, and John Wright. A one-query lower bound for unitary synthesis and breaking quantum cryptography. In Bojan Mohar, Igor Shinkar, and Ryan O'Donnell, editors, *56th STOC*, pages 979–990. ACM, 2024. (Cited on page 3.)

[LW09] Allison B. Lewko and Brent Waters. Efficient pseudorandom functions from the decisional linear assumption and weaker variants. In Ehab Al-Shaer, Somesh Jha, and Angelos D. Keromytis, editors, *ACM CCS 2009*, pages 112–120. ACM Press, November 2009. (Cited on page 5.)

[MOT20] Tomoki Moriya, Hiroshi Onuki, and Tsuyoshi Takagi. SiGamal: A supersingular isogeny-based PKE and its application to a PRF. In Shiho Moriai and Huaxiong Wang, editors, *ASIACRYPT 2020, Part II*, volume 12492 of *LNCS*, pages 551–580. Springer, Heidelberg, December 2020. (Cited on page 4.)

[MY22] Tomoyuki Morimae and Takashi Yamakawa. Quantum commitments and signatures without one-way functions. In Yevgeniy Dodis and Thomas Shrimpton, editors, *CRYPTO 2022, Part I*, volume 13507 of *LNCS*, pages 269–295. Springer, Heidelberg, August 2022. (Cited on page 3, 10.)

[MY24] Tomoyuki Morimae and Takashi Yamakawa. One-wayness in quantum cryptography. In Frédéric Magniez and Alex Bredariol Grilo, editors, *TQC 2024*, volume 310 of *LIPIcs*,

pages 4:1–4:21. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2024. See also https://eprint.iacr.org/2022/1336. (Cited on page 8, 10, 13.)

[MYY24] Tomoyuki Morimae, Shogo Yamada, and Takashi Yamakawa. Quantum unpredictability. Cryptology ePrint Archive, Paper 2024/701, 2024. To appear ASIACRYPT 2024. (Cited on page 3, 8, 27, 29.)

[NR04] Moni Naor and Omer Reingold. Number-theoretic constructions of efficient pseudo-random functions. *J. ACM*, 51(2):231–262, 2004. (Cited on page 4, 5, 19.)

[TD04] B. M. Terhal and D. P. DiVincenzo. Adaptive quantum computation, constant-depth circuits and arthur-merlin games. *Quant. Inf. Comput.*, 4(2):134–145, 2004. (Cited on page 9.)

[Yan22] Jun Yan. General properties of quantum bit commitments (extended abstract). In Shweta Agrawal and Dongdai Lin, editors, *ASIACRYPT 2022, Part IV*, volume 13794 of *LNCS*, pages 628–657. Springer, Heidelberg, December 2022. (Cited on page 3.)

[Zha12a] Mark Zhandry. How to construct quantum random functions. In *53rd FOCS*, pages 679–687. IEEE Computer Society Press, October 2012. (Cited on page 20.)

[Zha12b] Mark Zhandry. Secure identity-based encryption in the quantum random oracle model. In Reihaneh Safavi-Naini and Ran Canetti, editors, *CRYPTO 2012*, volume 7417 of *LNCS*, pages 758–775. Springer, Heidelberg, August 2012. (Cited on page 20.)

Appendix

A Haar-PR and Haar-Haar-DDH imply SKE

Preliminaries. We first review the definitions of SKE. Our IND-CPA definition is "real-or-fixed" style[22]. It is easy to show that this security implies left-or-right IND-CPA security[23]. via a hybrid argument. It is also easy to show that left-or-right IND-CPA security implies find-then-guess IND-CPA securities[24] defined in [BJ15, ABF+16, MYY24] by following the proof in [BDJR97].

Definition A.1 (Classical-message SKE). *A symmetric-key encryption (SKE) scheme for ℓ-bit classical messages consists of three algorithms* $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ *such that*

- $\mathsf{KeyGen}(1^\lambda) \to K$: *This is a QPT algorithm that takes the security parameter 1^λ as input and outputs a* classical *secret key K.*
- $\mathsf{Enc}(K, b) \to \mathsf{ct}$: *This is a QPT algorithm that takes K and a message $b \in \{0,1\}^\ell$ and outputs a* quantum *ciphertext* ct.
- $\mathsf{Dec}(K, \mathsf{ct}) \to b'/\bot$: *This is a QPT algorithm that takes K and a quantum ciphertext* ct *and outputs a classical message $b' \in \{0,1\}^\ell$ or a rejection symbol $\bot$.*

Definition A.2 (IND-CPA-secure 1-bit SKE). *We say that a SKE scheme* $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ *is* IND-CPA-secure 1-bit SKE *if it satisfies the following two properties:*

- *Correctness: We have*

$$\Pr_{K \leftarrow \mathsf{KeyGen}(1^\lambda)}[\mathsf{Dec}(K, \mathsf{Enc}(K, 0)) = 0] = 1,$$
$$\Pr_{K \leftarrow \mathsf{KeyGen}(1^\lambda)}[\mathsf{Dec}(K, \mathsf{Enc}(K, 1)) = 1] \geq 1/5.$$

- *IND-CPA security: We call SKE* indistinguishable against chosen-plaintext attacks (IND-CPA secure) *if the following holds: For any QPT adversary $\mathcal{A}$,*

$$\left| \Pr_{K \leftarrow \mathsf{KeyGen}(1^\lambda)}[1 \leftarrow \mathcal{A}^{\mathsf{Enc}(K,\cdot)}(1^\lambda)] - \Pr_{K \leftarrow \mathsf{KeyGen}(1^\lambda)}[1 \leftarrow \mathcal{A}^{\mathsf{Enc}(K,1)}(1^\lambda)] \right| \leq \mathsf{negl}(\lambda),$$

  where $\mathcal{A}$ queries the encryption oracles $\mathsf{Enc}(K, \cdot)$ or $\mathsf{Enc}(K, 1)$ only classically.

Definition A.3 (IND-CPA-secure multi-bit SKE). *We say that a SKE scheme* $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ *is* IND-CPA-secure multi-bit SKE *if it satisfies the following two properties:*

- *Correctness: for any $m \in \{0,1\}^\ell$,*

$$\Pr_{K \leftarrow \mathsf{KeyGen}(1^\lambda)}[\mathsf{Dec}(K, \mathsf{Enc}(K, m)) = m] \geq 1 - \mathsf{negl}(\lambda).$$

[22] An adversary has access to the oracle that takes an input x and returns an encryption of x or a fixed element x' depending on fixed $b \in \{0,1\}$ and guesses b.

[23] An adversary has access to the oracle that takes two inputs x_0, x_1 and returns an encryption of x_b with fixed $b \in \{0,1\}$ and guesses b.

[24] An adversary has access to the oracle that takes an input x and returns an encryption of x and distinguish an encryption of x_0^* or x_1^*.

- *IND-CPA security: We call SKE* indistinguishable against chosen-plaintext attacks (IND-CPA secure) *if the following holds: For any QPT adversary $\mathcal{A}$,*

$$\left|\Pr_{K\leftarrow\mathsf{KeyGen}(1^\lambda)}[1\leftarrow\mathcal{A}^{\mathsf{Enc}(K,\cdot)}(1^\lambda)]-\Pr_{K\leftarrow\mathsf{KeyGen}(1^\lambda)}[1\leftarrow\mathcal{A}^{\mathsf{Enc}(K,1^\ell)}(1^\lambda)]\right|\leq\mathsf{negl}(\lambda),$$

where $\mathcal{A}$ queries the encryption oracles $\mathsf{Enc}(K,\cdot)$ or $\mathsf{Enc}(K,1^\ell)$ only classically.

Lemma A.4. *Suppose that there exists an IND-CPA-secure 1-bit SKE $(\mathsf{KeyGen},\mathsf{Enc},\mathsf{Dec})$. Let $t=t(\lambda)=\omega(\log(\lambda))$ and $\ell=\ell(\lambda)$ be polynomials. We define the following new SKE scheme:*

- KeyGen' : *Run $\mathsf{KeyGen}(1^\lambda)$ $t\ell$-times and obtain $K_1,\dots,K_{t\ell}$. Output $K'=(K_1,\dots,K_{t\ell})$.*
- $\mathsf{Enc}'(K',m)$: *Let $m=(m_1,\dots,m_\ell)\in\{0,1\}^\ell$. For $i\in[\ell]$ and $j\in[t]$, generate $\mathsf{ct}_{(i-1)t+j}\leftarrow\mathsf{Enc}(K_{(i-1)t+j},m_i)$. Output $\mathsf{ct}'=(\mathsf{ct}_1,\dots,\mathsf{ct}_{t\ell})$.*
- $\mathsf{Dec}'(K',\mathsf{ct}')$: *For $i\in[\ell]$ and $j\in[t]$, let $m_{(i-1)t+j}\leftarrow\mathsf{Dec}(K_{(i-1)t+j},\mathsf{ct}_{(i-1)t+j})$. For $i\in[\ell]$, if $m_{(i-1)t+j}=0$ for all $j\in[t]$, then set $m'_i=0$; otherwise, set $m'_i=1$. Output $m'=(m'_1,\dots,m'_\ell)$.*

This new SKE $(\mathsf{KeyGen}',\mathsf{Enc}',\mathsf{Dec}')$ is IND-CPA-secure multi-bit SKE with plaintext space $\{0,1\}^\ell$.

Proof. The correctness of the new multi-bit SKE follows from that of the underlying 1-bit SKE: If $m_i=0$, then the new decryption algorithm always outputs $m'_i=0$. If $m_i=1$, then the new decryption algorithm outputs $m'_i=1$ with probability at least $1-(1-1/5)^t=1-(4/5)^{\omega(\log(\lambda))}=1-\delta(\lambda)$ for some negligible function $\delta(\lambda)$. Thus, for any $m\in\{0,1\}^\ell$, we have

$$\begin{aligned}\Pr_{K'\leftarrow\mathsf{KeyGen}'(1^\lambda)}[\mathsf{Dec}'(K',\mathsf{Enc}'(K',m))=m]&\geq 1-\Pr_{K'\leftarrow\mathsf{KeyGen}'(1^\lambda)}[\exists i\in[\ell]:1=m_i\neq m'_i=0]\\&\geq 1-\ell\cdot\delta(\lambda)\\&=1-\mathsf{negl}(\lambda)\end{aligned}$$

as we wanted.

The IND-CPA security of the new multi-bit SKE immediately follows from that of the underlying 1-bit SKE via a hybrid argument. □

Construction. We can construct a simple IND-CPA-secure 1-bit SKE from the HaarPR and Haar-DDH assumptions:

Theorem A.5. *Let (G,S) be a HaarPR and Haar-DDH QGA. Then, the following SKE is IND-CPA-secure 1-bit SKE.*

- $\mathsf{KeyGen}(1^\lambda)$: *Generate $g\leftarrow G(1^\lambda)$ and output $K=g$.*
- $\mathsf{Enc}(K,b)$: *If $b=0$, then generate $|s\rangle\leftarrow\mu$ by using a 1-design and output a ciphertext $\mathsf{ct}=(|s\rangle,g|s\rangle)$. If $b=1$, then generate $|s\rangle,|s'\rangle\leftarrow\mu$ by using a 1-design and output $\mathsf{ct}=(|s\rangle,|s'\rangle)$*
- $\mathsf{Dec}(K,\mathsf{ct})$: *Let $\mathsf{ct}=(|\phi\rangle,|\psi\rangle)$. Compute $g\otimes I$ on ct and run the SWAP test between registers. Output the result of the SWAP test.*

Proof of correctness. If $b = 0$, then $|\psi\rangle = g|s\rangle$, then the registers after applying $g \otimes I$ is $(g|s\rangle, g|s\rangle)$. Thus, the SWAP test always outputs 0. On the other hand, if $b = 1$, then $|\psi\rangle = |s'\rangle$ is independent of $|\phi\rangle = |s\rangle$. Thus,

$$\Pr[\mathsf{Dec}(K, \mathsf{Enc}(K, 1)) = 0] \leq \mathbb{E}_{g\leftarrow G,|s\rangle,|s'\rangle\leftarrow\mu}\left[\frac{1 + |\langle s'|g|s\rangle|^2}{2}\right] + \mathsf{negl}(\lambda) \tag{24}$$

$$\leq \mathbb{E}_{|s\rangle,|s'\rangle\leftarrow\mu}\left[\frac{1 + |\langle s'|s\rangle|^2}{2}\right] + \mathsf{negl}(\lambda) \tag{25}$$

$$\leq (1 + 1/2)/2 + \mathsf{negl}(\lambda) \leq 4/5, \tag{26}$$

where we used Lemma 2.9 for Equation (24), the fact that, for any g, the distribution of $g|s\rangle \leftarrow \mu$ is equivalent to that of $g|s\rangle \leftarrow \mu$ for Equation (25), and Lemma 2.10 for Equation (26). □

Proof of IND-CPA security. If the QGA is Haar-PR, then $D'_{\mathrm{HaarPR},0} \approx_c D'_{\mathrm{HaarPR},1}$ holds in Lemma 3.12. Notice that $D'_{\mathrm{HaarPR},0} = D_{\mathrm{HaarDDH},1}$ in Definition 3.14. Thus, if the underlying QGA is Haar-PR and Haar-DDH, then $D'_{\mathrm{HaarPR},1} \approx_c D_{\mathrm{HaarDDH},0}$, where

$$D'_{\mathrm{HaarPR},1} : \text{for } q \in [Q]\ |s_q\rangle \leftarrow \mu, |s'_q\rangle \leftarrow \mu;\ \text{return } \{(|s_q\rangle, |s'_q\rangle)^{\otimes t}\}_{q\in[Q]},$$
$$D_{\mathrm{HaarDDH},0} : g \leftarrow G,\ \text{for } q \in [Q]\ |s_q\rangle \leftarrow \mu;\ \text{return } \{(|s_q\rangle, g|s_q\rangle)^{\otimes t}\}_{q\in[Q]}.$$

Let $\mathcal{A}$ be an adversary against the IND-CPA security and let Q be the number of queries $\mathcal{A}$ making. We construct a reduction algorithm $\mathcal{B}$ distinguishing $D'_{\mathrm{HaarPR},1}$ and $D_{\mathrm{HaarDDH},0}$ with $t = 1$ as follows:

1. Receive samples $\{(|s_q\rangle, |s'_q\rangle)\}_{q\in[Q]}$ as input, where $|s'_q\rangle$ is $g|s_q\rangle$ with $g \leftarrow G$ or chosen from μ.
2. Run $\mathcal{A}$ and simulate the oracle as follows:
   - If the i-th query is 0, then return $\mathsf{ct}_i = (|s_q\rangle, |s'_q\rangle)$.
   - If the i-th query is 1, then generate two independent samples $|\phi\rangle, |\psi\rangle$ by using 1-design and return $\mathsf{ct}_i = (|\phi\rangle, |\psi\rangle)$.
3. Output $\mathcal{A}$'s decision.

If the input samples are chosen from $D_{\mathrm{HaarDDH},0}$, then $\mathcal{B}$ perfectly simulates the encryption oracle $\mathsf{Enc}(K, \cdot)$, where $K = g \leftarrow G$. On the other hand, if the input samples are chosen from $D'_{\mathrm{HaarPR},1}$, then $\mathcal{B}$ statistically simulates the encryption oracle $\mathsf{Enc}(K, 1)$. Thus, $\mathcal{B}$'s advantage is statistically close to that of $\mathcal{A}$ against IND-CPA security. This completes the proof. □

Since an IND-CPA-secure multi-bit SKE implies an IND-CPA-secure *quantum-message* SKE [BJ15] (and the formal proof in [MYY24, Appendix A]), we have the following corollary.

Corollary A.6. *Let (G, S) be a HaarPR and Haar-DDH QGA. Then, an IND-CPA-secure quantum-message SKE exists.*

B Discussion on Naor-Reingold-style PRFs from Group Actions

Here, we discuss how to weaken algebraic structures of group actions in the existing proofs [BKW20, ADMP20]. We first briefly review group actions and their notions. We then discuss the existing proofs by Boneh et al. [BKW20] and Alamati et al. [ADMP20].

B.1 Preliminaries

We first review the definition of group actions.

Definition B.1 (Group action). *Let G be a group with an identity element 1_G and let S be a set. Let $\star\colon G \times S \to S$ be a map. We say that $(G, S, \star)$ is a group action if the map satisfies the following two properties:*

1. *Identity: For any $s \in S$, we have $1_G \star s = s$.*
2. *Compatibility: For any $g, h \in G$ and any $s \in S$, it holds that $(gh) \star s = g \star (h \star s)$.*

We next review the standard notions of group actions.

Definition B.2 (Properties of group actions).

1. *Transitive: $(G, S, \star)$ is said to be* transitive *if for arbitrary $s_1, s_2 \in S$, there exists a group element $g \in G$ satisfying $s_2 = g \star s_1$.*
2. *Faithful: $(G, S, \star)$ is said to be* faithful *if for each group element $g \in G$, either $g = 1_G$ or there exists an element $s \in S$ satisfying $s \neq g \star s$. In other words, a group action is* faithful *if $g = 1_G$ if and only if $s = g \star s$ for all $s \in S$.*
3. *Free: $(G, S, \star)$ is called* free *if for each group element $g \in G$, if there exists some element $s \in S$ satisfying $s = g \star s$ then $g = 1_G$. Note that if group action is free, then it is also faithful.*
4. *Regular: $(G, S, \star)$ is said to be* regular *if it is transitive and free.*

For an element $s \in S$, we consider a mapping $f_s\colon g \in G \mapsto g \star s \in S$. We also consider, for an element $g \in G$, a mapping $L_g\colon s \in S \mapsto g \star s \in S$. We note that, for any $s \in S$, if a group action is *transitive* (or *free*, resp.), then f_s is subjective (or injective, resp.). We also note that, if a group action is *faithful*, then for any $g \neq h \in G$, $L_g \neq L_h$.

Lemma B.3. *Suppose that G is finite and a group action $(G, S, \star)$ is* transitive and faithful. *Then, for any $s_0 \in S$, then the distribution of $s_i \leftarrow S$ is equivalent to that of $g_i \star s_0$ with $g_i \leftarrow G$.*

Proof. The proof is easily obtained by considering a subgroup $H = \{g : g \star s_0 = s_0\}$ and left cosets $\{gH\}$ induced by H and using the facts in above. □

We then review *effective group actions* in [ADMP20].

Definition B.4 (Effective group actions (EGAs) [ADMP20, Definition 3.4]). *We say that a group action $(G, S, \star)$ is* effective *if the following properties are satisfied:*

1. *The group G is finite and there exist efficient algorithms for:*
   (a) *Membership testing, that is, to decide if a given bit-string represents a valid group element in G or not.*
   (b) *Equality testing, that is, to decide if two bit-strings represent the same group element in G or not.*
   (c) *Sampling, that is, to sample an element g from a distribution that is statistically close to the uniform over G.*

(d) *Operation, that is, to compute gh from $g, h \in G$.*

(e) *Inversion, that is, to compute g^{-1} from $g \in G$.*

2. *The set X is finite and there exist efficient algorithms for:*

   (a) *Membership testing, that is, to decide if a given bit-string represents a valid set element in S or not.*

   (b) *Unique representation, that is, given any $s \in S$, to compute a string $\hat{s}$ that canonically represents s.*

3. *Origin: There exists an element $s_0 \in S$, called the origin, such that its representation is known in public.*

4. *Operation $\star$: There exists an efficient algorithm that takes $g \in G$ and $s \in S$ and outputs $g \star s$.*

We next define several computational assumptions of group actions.

Definition B.5 (Assumptions).

1. *Pseudorandom: A GA is called* pseudorandom (PR) *if*

$$\{(s_0, g \star s_0) : g \leftarrow G\} \approx_c \{(s_0, s_1) : s_1 \leftarrow S\}.$$

2. *Weakly pseudorandom: A GA is called* weakly pseudorandom (wPR) *if for any polynomial $Q = Q(\lambda)$,*

$$\{(s_i, g \star s_i) : g \leftarrow G, s_i \leftarrow S\} \approx_c \{(s_i, s_i') : s_i, s_i' \leftarrow S\}.$$

3. *Decisional Diffie-Hellman (DDH): A GA is called* Decisional Diffie-Hellman (DDH) *if*

$$\{(s_0, \tilde{g} \star s_0, g \star s_0, (\tilde{g}g) \star s_0) : \tilde{g}, g \leftarrow G\} \approx_c \{(s_0, \tilde{g} \star s_0, g \star s_0, h \star s_0) : \tilde{g}, g, h \leftarrow G\}.$$

4. *Naor-Reingold (NR): A GA is called* Naor-Reingold (NR) *if for any polynomial $Q = Q(\lambda)$,*

$$\{(g_i \star s_0, (\tilde{g}g_i) \star s_0) : \tilde{g}, g_i \leftarrow G\} \approx_c \{(g_i \star s_0, h_i \star s_0) : g_i, h_i \leftarrow G\}.$$

NR-style PRF. Let $(G, S, \star)$ be an EGA. We define $f \colon G^{\ell+1} \times \{0,1\}^\ell \to S$ as

$$f_{g_0,\ldots,g_\ell}(x_1, \ldots, x_\ell) \coloneqq (g_\ell^{x_\ell} \cdot \cdots \cdot g_1^{x_1} \cdot g_0) \star s_0.$$

We say that this function is PRF is this f is computationally indistinguishable with a random function $f' \colon x \in \{0,1\}^\ell \mapsto s_x \in S$, where $s_x \leftarrow S$ for each $x \in \{0,1\}^\ell$.

By adopting the proof for the NR-style PRFSG (Theorem 4.1), we obtain the following theorem for the NR-style PRF f:

Theorem B.6. *Let $(G, S, \star)$ be an EGA. If it is PR and NR, then the function f is a PRF.*

We then review the proofs in [BKW20] and [ADMP20] and weaken the requirements of them.

B.2 BKW20 Proof

Boneh et al. [BKW20] assumed that a group action is transitive and faithful and G is commutative.

Theorem B.7 ([BKW20, Section 8], adapted). *Let $(G, S, \star)$ be an EGA. Suppose that the EGA is transitive and faithful and G is commutative. If the EGA is DDH, then the function f is a PRF.*

The following lemma (Lemma B.9) shows that if G is commutative and the EGA is DDH, then it is NR. Combining the lemma with Theorem B.6, we obtain the following corollary.

Corollary B.8. *Let $(G, S, \star)$ be an EGA. If G is commutative, and the EGA is PR and DDH, then the function f is a PRF.*

Lemma B.9. *Let $(G, S, \star)$ be an EGA. If G is commutative and the EGA is DDH, then the EGA is NR.*

Proof. Let us consider hybrid distributions $\bar{D}_i$: For $j = 1, \ldots, i$, $(a_i, b_i) = (g_i \star s_0, h_i \star s_0)$ and $j = i+1, \ldots, Q$, $(a_i, b_i) = (g_i \star s_0, \tilde{g} g_i \star s_0)$. By using the following claim, we have $\bar{D}_0 \approx_c \bar{D}_1 \approx_c \cdots \approx_c \bar{D}_Q$ if the DDH assumption holds. □

Claim B.10. If $(G, S, \star)$ is an EGA, G is commutative, and the DDH assumptions hold, for $i = 1, \ldots, Q$, $\bar{D}_{i-1} \approx_c \bar{D}_i$ holds.

Proof. Suppose that there exists $\mathcal{A}$ distinguishing $\bar{D}_{i-1}$ from $\bar{D}_i$. We construct an adversary $\mathcal{B}$ against the DDH assumption as follows:

- Given a sample $(s_0, \tilde{g} \star s_0, g \star s_0, h \star s_0)$, where $h = \tilde{g} g$ or random, $\mathcal{B}$ prepares a sample $\{(a_j, b_j)\}_{j \in [Q]}$ as follows:
  - for $j = 1, \ldots, i-1$, take random $g_j, h_j \leftarrow G$ and set $(a_j, b_j) := (g_j \star s_0, h_j \star s_0)$;
  - for $j = i$, set $(a_j, b_j) = (g \star s_0, h \star s_0)$;
  - for $j = i+1, \ldots, Q$, take random $g_j \leftarrow G$ and set $(a_j, b_j) = (g_j \star s_0, g_j \tilde{g} \star s_0)$.
- It runs $\mathcal{A}$ on input $\{(a_j, b_j)\}_{j \in [Q]}$ and outputs $\mathcal{A}$'s decision.

We note that, due to commutativity of G, the last $Q - i$ samples are equivalent to $(g_j \star s_0, \tilde{g} g_j \star s_0)$. If $h = \tilde{g} g$, then $(a_j, b_j) = (g \star s_0, (\tilde{g} g) \star s_0)$ and $\mathcal{B}$ perfectly simulates the distribution $\bar{D}_{i-1}$ since G is a group and the distribution of If h is random, then $\mathcal{B}$ perfectly simulates the distribution $\bar{D}_i$. Thus, $\mathcal{B}$'s advantage is equivalent to $\mathcal{A}$'s advantage distinguishing $\bar{D}_{i-1}$ and $\bar{D}_i$. □

B.3 ADMP20 Proof

Alamati et al. [ADMP20] assumed that a group action is weakly pseudorandom and G is regular and commutative.

Theorem B.11 ([ADMP20, Section 3.1 and Section 4.4], adapted). *Let $(G, S, \star)$ be an EGA. Suppose that the EGA is regular and G is commutative.*[25] *If the EGA is weakly pseudorandom, then the function f is a PRF.*

[25] [ADMP20, Section 3.1 and Section 4.4]

As in our discussion in the introduction, we do not require commutativity of G. It is easy to show that if the EGA is wPR and PR, then the EGA is NR (Lemma B.13 below). In addition, due to Lemma B.3, if the EGA is wPR and G is transitive and faithful, then the EGA is NR (Corollary B.14). Thus, we obtain the following corollary of Theorem B.6.

Corollary B.12. *Let $(G, S, \star)$ be an EGA.*

- *If it is PR and wPR, then the function f is a PRF.*
- *If it is wPR and G is transitive and faithful, then the function f is a PRF.*

Lemma B.13. *Let $(G, S, \star)$ be an EGA. If it is wPR and PR, then it is NR.*

Proof. It is easy to see that if the EGA is PR, then we can replace "$s_i \leftarrow S$" with "$g_i \star s_0$ with $g_i \leftarrow G$". Thus, we have that

$$\{(s_i, g \star s_i) : g \leftarrow G, s_i \leftarrow S\}_{i\in[Q]} \approx_c \{(g_i \star s_0, gg_i \star s_0) : g, g_i \leftarrow G\}_{i\in[Q]} \tag{27}$$
$$\{(s_i, h_i \star s_i) : h_i \leftarrow G, s_i \leftarrow S\}_{i\in[Q]} \approx_c \{(g_i \star s_0, h_i g_i \star s_0) : h_i, g_i \leftarrow G\}_{i\in[Q]}. \tag{28}$$

We obtain that

$$\begin{aligned}
&\{(g_i \star s_0, gg_i \star s_0) : g, g_i \leftarrow G\}_{i\in[Q]} \\
&\approx_c \{(s_i, g \star s_i) : g \leftarrow G, s_i \leftarrow S\}_{i\in[Q]} && \text{(from Equation (27))} \\
&\approx_c \{(s_i, s_i') : s_i, s_i' \leftarrow S\}_{i\in[Q]} && \text{(from wPR)} \\
&\approx_c \{(s_i, h_i \star s_i) : h_i \leftarrow G, s_i \leftarrow S\}_{i\in[Q]} && \text{(from wPR)} \\
&\approx_c \{(g_i \star s_0, h_i g_i \star s_0) : h_i, g_i \leftarrow G\}_{i\in[Q]} && \text{(from Equation (28))} \\
&\equiv \{(g_i \star s_0, h_i \star s_0) : h_i, g_i \leftarrow G\}_{i\in[Q]} && (G \text{ is a group}),
\end{aligned}$$

where we apply wPR Q-times to obtain third computational indistinguishability. □

Recall that if G is transitive and faithful, then an EGA $(G, S, \star)$ is perfectly PR (Lemma B.3). Thus, we obtain the following corollary.

Corollary B.14. *Let $(G, S, \star)$ be an EGA. If G is transitive and faithful, and the EGA is wPR, then the EGA is NR.*