



Quantum Group Action

Tomoyuki Morimae¹ , Keita Xagawa² and Shogo Yamada¹

¹ Yukawa Institute for Theoretical Physics, Kyoto University, Kyoto, Japan

² Technology Innovation Institute, Abu Dhabi, United Arab Emirates

Abstract. In quantum cryptography, there could be a new world, *Microcrypt*, where cryptography is possible but one-way functions (OWFs) do not exist. Many quantum analogues of OWFs and pseudorandom generators (PRGs) that are potentially weaker than OWFs have been introduced, and their useful applications have been demonstrated. However, Microcrypt still lacks enough foundations on which they are based compared with the classical cryptographic world. 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 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 $\star : G \times S \rightarrow S$. We introduce a quantum analogue of group actions, which we call *quantum group actions* (QGAs), where G is a subgroup 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. As an application, we construct classical-query pseudorandom function-like state generators (PRFSGs) based on these assumptions. 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. We also show that those assumptions are implied by non-adaptive pseudorandom unitaries (PRUs). Because classical group actions are instantiated with many concrete mathematical hardness assumptions, our QGAs could also have concrete (even OWFs-free) instantiations. We provide some candidate instantiations based on random circuits and IQP circuits.

Keywords: Quantum group action · Pseudorandom function-like state generator

1 Introduction

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

In contrast, recent studies have demonstrated that OWFs are not necessarily a minimal assumption in quantum cryptography: there may be a new world, called *Microcrypt*, in

E-mail: tomoyuki.morimae@yukawa.kyoto-u.ac.jp (Tomoyuki Morimae), keita.xagawa@tii.ae (Keita Xagawa), shogo.yamada@yukawa.kyoto-u.ac.jp (Shogo Yamada)



which OWFs do not exist but cryptography remains possible. Many fundamental primitives have been introduced, including pseudorandom unitaries (PRUs) [JLS18], pseudorandom function-like state generators (PRFSGs) [AQY22, AGQY22], unpredictable state generators (UPSGs) [MY24], pseudorandom state generators (PRSGs) [JLS18], one-way state generators (OWSGs) [MY22], EFI pairs [BCQ23], and one-way puzzles (OWPuzzs) [KT24]. These primitives may be weaker than OWFs [Kre21, KQST23, LMW24], while still implying useful applications such as commitments [MY22, AQY22, BCQ23, Yan22], multi-party computation [MY22, AQY22], message authentication codes (MACs) [AQY22, MY24], secret-key encryption [AQY22, MY24], digital signatures [MY22], and private-key quantum money [JLS18].

In classical cryptography, many hardness assumptions have been formulated for concrete mathematical problems, such as the discrete logarithm (DL) and decisional Diffie–Hellman (DDH) problems over groups arising from finite fields or elliptic curves [DH76, Mil86, Kob87, JD11, CLM⁺18]. These concrete assumptions are then abstracted into generic hardness assumptions, such as the DL and DDH assumptions over group actions [BY91, JQSY19, ADMP20]. Cryptographic primitives and applications are subsequently constructed from these generic assumptions.

In contrast, our understanding of the foundations of Microcrypt remains extremely limited. PRUs can be constructed from OWFs [MH25], and PRUs in turn imply PRFSGs, UPSGs, PRSGs, OWSGs, EFI pairs, and OWPuzzs. Consequently, all these primitives can be constructed using OWFs; see Figure 2. However, few “OWF-free” concrete or abstract mathematical hardness assumptions are known from which these primitives can be constructed directly.¹

1.1 Our Results

Our contributions are summarized as follows.

- We introduce several generic hardness assumptions intended to connect concrete mathematical hardness assumptions with cryptographic applications. As we explain in more detail below, these assumptions are based on a quantum analogue of cryptographic group actions [BY91, Cou06, JQSY19, ADMP20], which we call *quantum group actions* (QGAs). Classical cryptographic group actions admit many concrete instantiations [JD11, CLM⁺18, DD24]. Likewise, QGAs may admit concrete, potentially OWF-free instantiations based directly on natural quantum analogues of classical hard problems, without first constructing classical cryptographic primitives from OWFs.
- From QGAs satisfying suitable pseudorandomness properties, we construct classical-query PRFSGs, which are quantum analogues of PRFs. A PRFSG is a quantum polynomial-time (QPT) algorithm `StateGen` that takes a classical key k and a bit string x as input and outputs a quantum state $|\phi_k(x)\rangle$. Informally, security requires that no QPT adversary can distinguish oracle access to `StateGen`($k, \cdot$) for a uniformly random key k from access to an oracle that returns Haar-random states, which we call the Haar oracle.² PRFSGs imply nearly all known Microcrypt primitives, including UPSGs, PRSGs, OWSGs, OWPuzzs, and EFI pairs. They also yield applications such as secret-key encryption (SKE), message authentication codes (MACs), private-key quantum money, commitments, multi-party computation, and digital signatures

¹Here, “OWF-free” means that the assumption or construction can plausibly be instantiated without using OWFs, or primitives constructed from OWFs, as building blocks; it does not necessarily mean that the assumption is known not to imply OWFs. Several recent works have pursued this direction; see Subsection 1.2.

²More precisely, for each x , the oracle samples a Haar-random state $|\psi_x\rangle$ and returns a fresh copy of $|\psi_x\rangle$ whenever x is queried.

with bounded-polynomial-time security. The PRFSGs constructed in this paper are, however, secure only against classical queries.³ Whether quantum-query-secure PRFSGs, or even PRUs, can be constructed from QGAs remains open.

- We also show that QGAs satisfying the required pseudorandomness properties can be constructed from PRUs. A PRU is a family of keyed unitaries such that no QPT adversary can distinguish oracle access to a randomly keyed unitary from oracle access to a Haar-random unitary. In fact, we prove the slightly stronger result that these QGAs can be constructed from *non-adaptive* PRUs, whose security is required only against adversaries that make their oracle queries non-adaptively. Because non-adaptive PRUs appear to be weaker than adaptive PRUs, this result suggests that our QGA assumptions may also be weaker than adaptive PRUs. Whether QGAs imply PRUs remains open.
- We propose candidate QGA instantiations based on random quantum circuits and instantaneous quantum polynomial-time (IQP) circuits [BJS11, BMS16]. These candidates are intended to be OWF-free: their sampling algorithms are defined directly using random quantum circuits rather than by first constructing classical pseudorandom functions or other primitives from OWFs. For the IQP-based candidates, the acting group G is commutative, which may be advantageous for further cryptographic applications.

As a supplementary result, we also show in Appendix A that QGAs satisfying specific pseudorandom properties imply secret-key encryption. Since this construction is a simple additional application of our QGA assumptions rather than a main contribution of this work, we defer it to Appendix A.

We next describe these results in more detail.

1.1.1 (Quantum) Group Actions.

Our quantum assumptions are based on a “quantization” of group actions. We first briefly review group actions, and then give a summary of our quantum group actions.

Group actions. A group action $(G, S, \star)$ consists of a group G , a set S , and an operation $\star: G \times S \rightarrow S$ such that $g_1 \star (g_2 \star s) = (g_1 g_2) \star s$ for all $g_1, g_2 \in G$ and $s \in S$, and such that the identity element $e \in G$ satisfies $e \star s = s$ for every $s \in S$. Cryptographic group actions [BY91, Cou06, JQSY19, ADMP20] are group actions endowed with computational hardness assumptions.

For example, a *one-way group action* [BY91] is a group action for which, given a fixed element $s_0 \in S$ and $t := g \star s_0$ for a uniformly random $g \leftarrow G$,⁴ it is computationally hard to find any g' satisfying $g' \star s_0 = t$. One-way group actions abstract several well-studied cryptographic assumptions, including discrete-logarithm assumptions [DH76], isogeny-based assumptions [JD11, CLM⁺18], and code-based assumptions [DD24]. They have applications to identification schemes, digital signatures, and commitments [BY91].

A *pseudorandom group action* [JQSY19, ADMP20] is a group action for which $g \star s_0$, with $g \leftarrow G$, is computationally indistinguishable from an independently sampled $u \leftarrow S$.⁵ A *weakly pseudorandom group action* [ADMP20] is a group action for which $(s_i, g \star s_i)_{i \in [Q]}$ and $(s_i, s'_i)_{i \in [Q]}$ are computationally indistinguishable, where $g \leftarrow G$ and $s_1, \dots, s_Q, s'_1, \dots, s'_Q \leftarrow S$. Weakly pseudorandom group actions abstract several well-studied cryptographic assumptions, including the decisional Diffie–Hellman (DDH)

³The resulting IND-CPA SKE and EUF-CMA MACs are likewise secure only against classical queries.

⁴Throughout this paper, $a \leftarrow A$ denotes that a is sampled uniformly at random from the finite set A .

⁵This notion is nontrivial when the distribution of $g \star s_0$ does not already coincide with the uniform distribution over S ; see Subsection B.1.

assumption [DH76] and isogeny-based assumptions [CLM⁺18]. They also yield applications such as key exchange, smooth projective hashing, dual-mode public-key encryption (PKE), two-message statistically sender-private oblivious transfer (OT), and pseudorandom functions (PRFs) [BY91, ADMP20, JQSY19, Cou06].

Quantum group actions. We introduce a quantum analogue of cryptographic group actions, which we call *quantum group actions (QGAs)*.⁶ A QGA $(G, S, \star)$ is a tuple of a group G , a set S , and an operation $\star$: G is a subgroup of unitary operators and S is a set of quantum states. The action $\star$ is just the application of a unitary in G on a state in S . Then the property $g_1(g_2|s\rangle) = (g_1g_2)|s\rangle$ is trivially satisfied for any $g_1, g_2 \in G$ and $|s\rangle \in S$.

We introduce a quantum analogue of cryptographic group actions, which we call *quantum group actions (QGAs)*.⁷ A QGA $(G, S, \star)$ consists of a group G , a set S , and an action $\star$, where G is a subgroup of unitary operators and S is a set of quantum states preserved by the action of G . For $g \in G$ and $|s\rangle \in S$, the action $g \star |s\rangle$ is simply the application of the unitary g to $|s\rangle$. Consequently, $g_1 \star (g_2 \star |s\rangle) = (g_1g_2) \star |s\rangle$ for all $g_1, g_2 \in G$ and $|s\rangle \in S$. Since the action is simply unitary application, we usually omit $\star$ and write $g|s\rangle$ instead of $g \star |s\rangle$.

For cryptographic applications, we equip G with an efficient sampling algorithm **SampG**. Strictly speaking, **SampG** outputs a classical description $[g]$ of a unitary $g \in G$. The distribution induced by **SampG** need not be uniform over G , and its support need not coincide with G or be closed under composition. For readability, throughout the introduction we use the shorthand $g \leftarrow \text{SampG}$ to mean that $[g]$ is generated by **SampG** and the corresponding unitary g is used.

We similarly introduce an efficient generation algorithm **GenS** for states in S , which generates a quantum analogue of a fixed element $s_0 \in S$. Strictly speaking, **GenS** outputs a classical description $[|s\rangle]$ of a preparation circuit for a state $|s\rangle \in S$. This description allows any polynomial number of fresh copies of $|s\rangle$ to be prepared efficiently. Throughout the introduction, we use the shorthand $|s\rangle \leftarrow \text{GenS}$ to denote this procedure and the resulting state.

Some of our security definitions additionally use Haar-random states. We write $|s\rangle \leftarrow \mu$ when $|s\rangle$ is sampled according to the Haar measure μ over the pure-state space. Although exact Haar-random states are used in the idealized security definitions, the reductions require only finitely many moments; accordingly, Haar-random states can be replaced there by efficiently generated approximate t -designs of suitable orders and approximation errors.

We endow QGAs with several computational hardness assumptions. In particular, we introduce several pseudorandomness properties for QGAs and show that suitable combinations of these properties imply classical-query PRFSGs and can be obtained from PRUs.

1.1.2 Construction of PRFSGs.

To provide intuition for our construction of pseudorandom function-like state generators (PRFSGs) from pseudorandom quantum group actions (QGAs), we first review the classical Naor–Reingold construction of pseudorandom functions (PRFs) from group actions [NR04].

Naor–Reingold PRFs, decisional Diffie–Hellman (DDH), and weak pseudorandomness. The Naor–Reingold PRF can be instantiated from a group action as follows [NR04, BKW20, ADMP20, MOT20]. The key of the PRF f_k is $k := (g_0, g_1, \dots, g_\ell)$

⁶A quantum variant of group actions where S is the set of quantum states was introduced in [Zha24] and studied recently in [MZ25]. See Subsection 1.2.

⁷A different quantum variant of group actions, in which S is a set of quantum states, was introduced in [Zha24] and subsequently studied in [MZ25]; see Subsection 1.2.

where $g_i \leftarrow \$ G$ for every $i \in \{0, 1, \dots, \ell\}$. For an input $x := (x_1, \dots, x_\ell) \in \{0, 1\}^\ell$, define

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

where s_0 is a fixed element of S .

Roughly speaking, the security of this construction follows from the computational indistinguishability⁸

$$\left\{ (g_i \star s_0, (\tilde{g}g_i) \star s_0)_{i \in [Q]} : \tilde{g} \leftarrow \$ G, \forall i \in [Q] g_i \leftarrow \$ G \right\} \quad (2)$$

$$\approx_c \left\{ (g_i \star s_0, h_i \star s_0)_{i \in [Q]} : \forall i \in [Q] g_i, h_i \leftarrow \$ G \right\}, \quad (3)$$

which we call the *Naor–Reingold (NR) assumption*. Here, Q is polynomially bounded in the security parameter. By applying the NR assumption repeatedly, one can show that the outputs of f_k are computationally indistinguishable from those of $f'_k(x) := g_x \star s_0$, where an independent $g_x \leftarrow \$ G$ is sampled for each input x [NR04].

Naor and Reingold [NR04] showed that the NR assumption follows from the decisional Diffie–Hellman (DDH) assumption. For a group action, the DDH assumption requires

$$(s_0, \tilde{g} \star s_0, g \star s_0, (\tilde{g}g) \star s_0) \approx_c (s_0, \tilde{g} \star s_0, g \star s_0, h \star s_0), \quad (4)$$

where s_0 is a fixed element of S and $\tilde{g}, g, h \leftarrow \$ G$ independently.

Suppose that G additionally has the structure of a commutative ring with operations $(\cdot, +)$, and that S has a binary operation $\circ$ satisfying $x(g \star s_0) \circ (g' \star s_0) = (g + g') \star s_0$. In this setting, the DDH assumption tightly implies the NR assumption because the samples can be rerandomized [NR04, BMR10].⁹

Boneh, Kogan, and Woo [BKW20] considered the case in which G is a *commutative group* and showed, via a hybrid argument, that the DDH assumption implies the NR assumption. Alamedi, De Feo, Montgomery, and Patrnanabis [ADMP20] took a different approach by introducing *weak pseudorandomness*.¹⁰ This property requires the computational indistinguishability

$$\left\{ (s_i, \tilde{g} \star s_i)_{i \in [Q]} : \tilde{g} \leftarrow \$ G, \forall i \in [Q], s_i \leftarrow \$ S \right\} \approx_c \left\{ (s_i, s'_i)_{i \in [Q]} : \forall i \in [Q], s_i, s'_i \leftarrow \$ S \right\}. \quad (5)$$

If the group action is regular (and hence transitive)¹¹ then, for any fixed $s_0 \in S$, the distribution of $g_i \star s_0$ for a uniformly random $g_i \leftarrow \$ G$ is uniform over S . Therefore, replacing s_i and s'_i with $g_i \star s_0$ and $h_i \star s_0$, respectively, where $g_i, h_i \leftarrow \$ G$, transforms the weak-pseudorandomness experiment into the NR experiment. Consequently, weak pseudorandomness is tightly equivalent to the NR assumption in this setting.

Although Alamedi et al. focused on the case in which G is commutative, their approach extends to noncommutative groups. We also note that we will not need some properties of G assumed by Boneh, Kogan, and Woo [BKW20] when we employ pseudorandom group actions. See Appendix B for details.

Construction of PRFSGs. Motivated by the classical Naor–Reingold construction, we construct a PRFSG from a QGA. Our construction is summarized in Figure 1. Let $(G, S, \star)$ be a QGA.¹²

⁸Here, $\approx_c$ denotes computational indistinguishability between the two distribution ensembles.

⁹Some non-commutative settings related to matrix DDH assumptions have also been studied [LW09, EHK⁺13, ABP15].

¹⁰More precisely, they require the permutation $\pi_{\tilde{g}} : s \mapsto \tilde{g} \star s$ to be a weak pseudorandom permutation.

¹¹A group action is *transitive* if, for every $s_1, s_2 \in S$, there exists a $g \in G$ such that $s_2 = g \star s_1$. A group action is *regular* if it is both transitive and free, where freeness means that $g \star s = s$ for some $s \in S$ implies that g is the identity element. See Definition 23 in Appendix B.

¹²Because the action is simply the application of a unitary to a state, we omit $\star$ below and write $g|s\rangle$ for $g \star |s\rangle$.

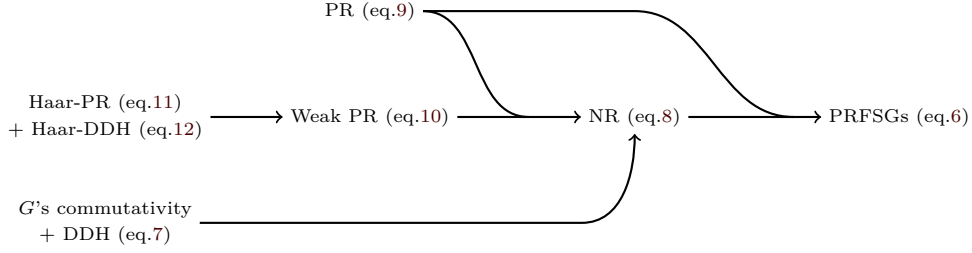


Figure 1: Diagram for our construction.

We define the PRFSG $\text{StateGen}(k, x) \rightarrow |\phi_k(x)\rangle$ as follows: Its key is $k := (g_0, g_1, \dots, g_\ell, |s_0\rangle)$, where $g_i \leftarrow \text{SampG}$ for every $i \in \{0, 1, \dots, \ell\}$ and $|s_0\rangle \leftarrow \text{GenS}$ is a fixed, efficiently preparable state in S . For an input $x = (x_1, \dots, x_\ell) \in \{0, 1\}^\ell$, the output state is defined by¹³

$$|\phi_k(x)\rangle := (g_\ell^{x_\ell} \cdots g_1^{x_1} g_0) |s_0\rangle. \quad (6)$$

The remaining question is which hardness assumptions on the QGA suffice to guarantee the security of **StateGen** as a PRFSG. A direct quantum analogue of the DDH assumption would require the computational indistinguishability

$$(|s_0\rangle, \tilde{g}|s_0\rangle, g|s_0\rangle, \tilde{g}g|s_0\rangle) \approx_c (|s_0\rangle, \tilde{g}|s_0\rangle, g|s_0\rangle, h|s_0\rangle), \quad (7)$$

where $|s_0\rangle \leftarrow \text{GenS}$ and $\tilde{g}, g, h \leftarrow \text{SampG}$ independently. Similarly, the quantum analogue of the NR assumption informally requires the following computational indistinguishability.¹⁴

$$\begin{aligned} \{ (g_i|s_0\rangle, \tilde{g}g_i|s_0\rangle)_{i \in [Q]} : \tilde{g} \leftarrow \text{SampG}, \forall i \in [Q] \ g_i \leftarrow \text{SampG} \} \\ \approx_c \{ (g_i|s_0\rangle, h_i|s_0\rangle)_{i \in [Q]} : \forall i \in [Q] \ g_i, h_i \leftarrow \text{SampG} \}. \end{aligned} \quad (8)$$

Unfortunately, when G lacks additional algebraic structure, such as commutativity, neither this direct analogue of the DDH assumption nor a direct analogue of weak pseudorandomness appears sufficient to imply the quantum NR assumption. We therefore seek simple and plausible assumptions on QGAs that together imply the quantum NR assumption.

Moreover, unlike in the classical setting, the quantum NR assumption in Equation 8 alone is insufficient to construct PRFSGs. In the classical Naor–Reingold construction, repeated applications of the NR assumption show that the outputs of f_k are computationally indistinguishable from those of $f'_k(x) := g_x \star s_0$, where an independent $g_x \leftarrow G$ is sampled for each input x . If the classical group action is transitive, then $g_x \star s_0$ is uniformly distributed over S when g_x is sampled uniformly from G . In the quantum setting, by contrast, the distribution induced by $g_x|s_0\rangle$ for $g_x \leftarrow \text{SampG}$ need not be the uniform distribution over any efficiently sampleable state space S' .¹⁵ We therefore additionally require that $g_x|s_0\rangle$, for $g_x \leftarrow \text{SampG}$, be computationally indistinguishable from a Haar-random state.

We call this property *pseudorandomness (PR)*. Informally, it requires

$$(|s_0\rangle, h|s_0\rangle) \approx_c (|s_0\rangle, |s'\rangle), \quad (9)$$

¹³Ananth, Gulati, and Lin [AGL24] gave a similar construction of selectively secure PRFSGs in the common-Haar-state model, inspired by the Goldreich–Goldwasser–Micali (GGM) construction [GGM86].

¹⁴Formally, the adversary receives polynomially many copies of each state. Thus, for every polynomially bounded t , each pair in the two ensembles below should be replaced by $(g_i|s_0\rangle, \tilde{g}g_i|s_0\rangle)^{\otimes t}$ and $(g_i|s_0\rangle, h_i|s_0\rangle)^{\otimes t}$, respectively. However, in this introduction, we suppress the number of copies for readability.

¹⁵The state space S' may differ from S .

where $|s_0\rangle \leftarrow \text{GenS}$, $h \leftarrow \text{SampG}$, and $|s'\rangle \leftarrow \mu$ is Haar-random.¹⁶ Combining the quantum NR assumption in Equation 8 with the PR assumption yields our PRFSG construction.

It remains to determine how the quantum NR assumption can be obtained from simpler assumptions. In the classical setting, the NR assumption follows from weak pseudorandomness as defined in Equation 5 [ADMP20]. A natural quantum analogue would require

$$\begin{aligned} & \{(|s_i\rangle, \tilde{g}|s_i\rangle)_{i \in [Q]} : \tilde{g} \leftarrow \text{SampG}, \forall i \in [Q] \ |s_i\rangle \leftarrow \mu\} \\ & \approx_c \{(|s_i\rangle, |s'_i\rangle)_{i \in [Q]} : \forall i \in [Q] \ |s_i\rangle, |s'_i\rangle \leftarrow \mu\}. \end{aligned} \quad (10)$$

In the classical setting, weak pseudorandomness is equivalent to the NR assumption under the transitivity condition discussed above. In the quantum setting, however, the Haar-random states in Equation 10 need not have the same distribution as states of the form $g|s_0\rangle$ for $g \leftarrow \text{SampG}$. Consequently, Equation 10 alone does not yield the quantum NR assumption in Equation 8. Combining it with the PR assumption in Equation 9, however, allows us to bridge this distributional gap and recover the quantum NR assumption.

Our next goal is therefore to establish the quantum analogue of weak pseudorandomness in Equation 10. For this purpose, we introduce two assumptions that we believe to be natural and plausible. The first is *Haar-pseudorandomness (Haar-PR)*, which informally requires

$$(|s\rangle, h|s\rangle) \approx_c (|s\rangle, |s'\rangle), \quad (11)$$

where $|s\rangle, |s'\rangle \leftarrow \mu$ independently and $h \leftarrow \text{SampG}$.¹⁷ Importantly, PR and Haar-PR are not equivalent in general. In the PR experiment of Equation 9, the state $h|s_0\rangle$ is generated by applying a sampled unitary to a fixed efficiently preparable state and need not be Haar-distributed. In the Haar-PR experiment of Equation 11, by contrast, the “input” state itself is Haar-random.

The second assumption is a multi-sample quantum analogue of the DDH assumption over Haar-random states. We call this property *Haar-decisional Diffie–Hellman (Haar-DDH)*. Informally, it requires

$$\begin{aligned} & \{(|s_i\rangle, g|s_i\rangle)_{i \in [Q]} : g \leftarrow \text{SampG}, \forall i \in [Q] \ |s_i\rangle \leftarrow \mu\} \\ & \approx_c \{(|s_i\rangle, h_i|s_i\rangle)_{i \in [Q]} : \forall i \in [Q] \ |s_i\rangle \leftarrow \mu, h_i \leftarrow \text{SampG}\}. \end{aligned} \quad (12)$$

Together, the Haar-PR and Haar-DDH assumptions imply the quantum analogue of weak pseudorandomness in Equation 10. Combining this property with PR yields the quantum NR assumption in Equation 8. Finally, the quantum NR and PR assumptions together establish the security of our Naor–Reingold-style PRFSG construction. See Figure 1 for the diagram.

PRFSGs are generally defined to be secure against quantum-query adversaries [AQY22, AGQY22]; namely, their security must hold against every quantum polynomial-time (QPT) adversary that may query the input x in superposition. Our proof, however, establishes security only against *classical-query* adversaries, and several barriers prevent our current techniques from extending to quantum queries; see Subsection 4.2. Constructing quantum-query-secure PRFSGs, or even PRUs, from QGAs or other OWF-free assumptions remains an open problem.

In the classical setting, PRFs can be constructed from pseudorandom group actions, as shown by Ji et al. [JQSY19]. By contrast, we do not know how to construct PRFSGs from PR QGAs or Haar-PR QGAs alone. In particular, Ji et al. [JQSY19, Section 7.2] follow

¹⁶Formally, the adversary receives an arbitrary polynomial number of copies of each state. We suppress the number of copies throughout the introduction.

¹⁷The adversary may receive an arbitrary polynomial number of copies of each state. By contrast, when the number of copies is bounded by a constant, a statistical construction is known [AGL24, Section 4].

the Goldreich–Goldwasser–Micali (GGM) paradigm [GGM84], together with its quantum-security extensions by Zhandry [Zha12a] and Song and Yun [SY17]. They construct a keyed length-doubling pseudorandom generator $\text{PRG}_k: G \rightarrow G \times G$ using a pseudorandom group action, hash functions, and a sampling algorithm. We do not know how to realize an analogous length-doubling PRG from QGA assumptions in the quantum-state setting. More generally, it remains open whether PRFSGs can be constructed from PRSGs.¹⁸

1.1.3 Relations Between QGAs and Other Primitives.

Pseudorandom state generators (PRSGs) from PR QGAs. As explained above, pseudorandomness for QGAs requires

$$(|s_0\rangle, h|s_0\rangle)^{\otimes t} \approx_c (|s_0\rangle, |s'\rangle)^{\otimes t}$$

for every polynomially bounded t , where $|s_0\rangle \leftarrow \text{GenS}$, $h \leftarrow \text{SampG}$, and $|s'\rangle \leftarrow \mu$ is Haar-random. As an additional result, we observe that a PR QGA directly yields a PRSG.

Lemma 1. *Pseudorandom quantum group actions (PR QGAs) imply pseudorandom state generators (PRSGs).*

One-way state generators (OWSGs) from one-way QGAs. It is also natural to define a quantum analogue of one-way group actions. In the security game for a classical one-way group action, the adversary receives the classical elements s and $g \star s$. In the corresponding security game for a one-way QGA, the adversary receives $|s\rangle^{\otimes t}$ and $(g|s\rangle)^{\otimes t}$ for every polynomially bounded t . We obtain the following implication.

Lemma 2. *One-way QGAs imply pure one-way state generators (OWSGs).*

QGAs from pseudorandom unitaries (PRUs). We construct QGAs from pseudorandom unitaries (PRUs) by letting the sampler for G output a uniformly random key k , which serves as a classical description of the unitary U_k , and by letting the generation algorithm for S output $|0^\lambda\rangle$ as the initial state.

Lemma 3. *Pseudorandom unitaries (PRUs) imply PR, Haar-PR, and Haar-DDH QGAs.*

See Section 5 for the proofs.

Candidate instantiations of QGAs. Finally, we discuss several candidate QGA instantiations. We conjecture that QGAs based on random quantum circuits satisfy PR, Haar-PR, and Haar-DDH. For the IQP-based candidates, the acting group G is commutative, which may be advantageous for further cryptographic applications. See Section 6 for details.

Summary of results. Figure 2 summarizes the new and known relations between cryptographic primitives and QGAs, distinguishing primitives with classical-query security from those with quantum-query security. As illustrated in the figure, our results may open a new avenue for connecting quantum cryptographic applications to concrete OWF-free hardness assumptions.

¹⁸PRFSGs with $O(\log \lambda)$ -bit inputs can be constructed from PRSGs [AQY22], but the problem remains open for PRFSGs with $\text{poly}(\lambda)$ -bit inputs.

1.2 Related Works

As discussed above, an important goal in this area is to base Microcrypt primitives on plausible concrete or abstract OWF-free hardness assumptions. During the preparation of this manuscript, the following three works pursuing this goal appeared.

Khurana and Tomer [KT25] constructed one-way puzzles (OWPuzzs) from hardness assumptions underlying sampling-based quantum advantage [BFNV19, AA11, TD04, BJS11, BMS16, FKM⁺18], together with the mild complexity assumption, $\mathbf{P}^{\#P} \not\subseteq (io)\mathbf{BQP}/qpoly$.

Hiroka and Morimae [HM25] and Cavalar, Goldin, Gray, and Hall [CGGH25] constructed OWPuzzs from the quantum average-case hardness of the GapK problem. GapK is a promise problem that asks whether a given bit string x has low Kolmogorov complexity. Its quantum average-case hardness requires that instances be sampled from a quantum-polynomial-time sampleable distribution and that no quantum-polynomial-time algorithm can solve the problem. Their assumptions are more concrete and have previously been studied outside cryptography, particularly in the contexts of quantum advantage and classical meta-complexity.

On the other hand, our work constructs the stronger primitive of PRFSGs, which in turn imply UPSGs, PRSGs, OWSGs, private-key quantum money, IND-CPA SKE, EUF-CMA MACs, OWPuzzs, and EFI pairs. An interesting open problem is whether our QGA assumptions can be instantiated from concrete assumptions related to quantum advantage or meta-complexity.

Comparison with Mutreja and Zhandry (CRYPTO 2025). Mutreja and Zhandry [MZ25], following the earlier framework of Zhandry [Zha25], study *quantum state group actions* in which a group acts on a set of quantum states. They investigate concrete constructions and cryptographic problems associated with such actions, including both vulnerable constructions with sufficiently many copies and secure ones. Their constructions are unconditional or based on assumptions such as LWE or the quantum random-oracle model, and provide a unified perspective on quantum-money and key-distribution protocols.

Our work has a complementary objective. We model the acting group directly as a subgroup of unitary operators and develop generic hardness assumptions for QGAs in Microcrypt, including PR, Haar-PR, Haar-DDH, and NR. We then use these assumptions to construct classical-query pseudorandom function-like state generators (PRFSGs). Thus, Mutreja and Zhandry primarily analyze concrete quantum-state actions, their bounded-copy security, and the cryptographic problems supported by their additional structure, whereas our goal is to provide an assumption framework connecting candidate unitary ensembles to generic cryptographic applications.

Comparison with Bostanci, Haferkamp, Hangleiter, and Poremba (TQC 2025). Bostanci et al. [BHHP25] introduce Hamiltonian phase states (HPSs), generated by random IQP circuits, and conjecture their one-wayness and pseudorandomness. Their construction can be viewed as a concrete instantiation of our IQP-based QGA framework, where the HPS circuit distribution specifies the sampler **SampG** for the acting unitaries. Up to an efficiently invertible fixed Hadamard transform, their search and decision HPS assumptions correspond closely to the one-wayness and PR assumptions for this IQP-based QGA.

The two works are complementary: Bostanci et al. analyze a specific, efficiently implementable IQP ensemble and provide supporting evidence such as worst-case-to-average-case reductions and approximate state-design properties, whereas we develop a generic group-action framework connecting unitary ensembles to cryptographic applications. Our framework additionally introduces action-level notions such as Haar-PR, Haar-DDH, and NR.

2 Preliminaries

2.1 Basic Notations

We use the standard notations from quantum information and cryptography. 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 $\{1, 2, \dots, Q\}$. 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. We write μ_m and μ_m^U to denote the Haar measure over m -qubit space and over m -qubit unitaries, respectively. In what follows, we assume that the length of quantum states is $m(\lambda)$ qubits, where m is a polynomial. We often drop the subscription m from μ_m and μ_m^U if m is clear in the context. For a distribution or measure D , $y \leftarrow D$ means that we take a sample y by following D .

2.2 Quantum Cryptographic Primitives

We review quantum cryptographic primitives in the literature.

Definition 1 (Pseudorandom State Generators (PRSGs) [JLS18]). A pseudorandom state generator (PRSG) is a tuple $(\text{KeyGen}, \text{StateGen})$ of algorithms such that

- $\text{KeyGen}(1^\lambda) \rightarrow k$: 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.
- $\text{StateGen}(k) \rightarrow |\phi_k\rangle$: 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 ,

$$\left| \Pr_{k \leftarrow \text{KeyGen}(1^\lambda)} [1 \leftarrow \mathcal{A}(1^\lambda, |\phi_k\rangle^{\otimes t})] - \Pr_{|\psi\rangle \leftarrow \mu} [1 \leftarrow \mathcal{A}(1^\lambda, |\psi\rangle^{\otimes t})] \right| \leq \text{negl}(\lambda). \quad (13)$$

Definition 2 (One-Way State Generators (OWSGs) [MY22, MY24]). A one-way state generator (OWSG) is a tuple $(\text{KeyGen}, \text{StateGen}, \text{Ver})$ of algorithms such that

- $\text{KeyGen}(1^\lambda) \rightarrow k$: 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.
- $\text{StateGen}(k) \rightarrow \phi_k$: It is a QPT algorithm that, on input a classical string k , outputs a quantum state ϕ_k .
- $\text{Ver}(k', \phi_k) \rightarrow \top/\perp$: It is a QPT algorithm that, on input a classical string k' and a quantum state ϕ_k , outputs $\top$ or $\perp$.

We require the following correctness and one-wayness.

Correctness.

$$\Pr[\top \leftarrow \text{Ver}(k, \phi_k) : k \leftarrow \text{KeyGen}(1^\lambda), \phi_k \leftarrow \text{StateGen}(k)] \geq 1 - \text{negl}(\lambda). \quad (14)$$

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

$$\Pr[\top \leftarrow \text{Ver}(k', \phi_k) : k \leftarrow \text{KeyGen}(1^\lambda), \phi_k \leftarrow \text{StateGen}(k), k' \leftarrow \mathcal{A}(1^\lambda, \phi_k^{\otimes t})] \leq \text{negl}(\lambda). \quad (15)$$

Remark 1. If all $|\phi_k\rangle$ are pure and $\Pr[\top \leftarrow \text{Ver}(k, |\phi_k\rangle)] \geq 1 - \text{negl}(\lambda)$ 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 $\perp$.

Definition 3 (Weak OWSGs [MY24]). The definition of weak one-way state generators (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

$$\Pr[\top \leftarrow \text{Ver}(k', \phi_k) : k \leftarrow \text{KeyGen}(1^\lambda), \phi_k \leftarrow \text{StateGen}(k), k' \leftarrow \mathcal{A}(1^\lambda, \phi_k^{\otimes t})] \leq 1 - \frac{1}{p(\lambda)}. \quad (16)$$

Remark 2. It is shown in Theorem 3.7 of [MY24] that OWSGs exist if and only if weak OWSGs exist.

Definition 4 (Pseudorandom Function-Like State Generators (PRFSGs) [AQY22]). A pseudorandom function-like state generator (PRFSG) is a tuple $(\text{KeyGen}, \text{StateGen})$ of algorithms such that

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

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

$$\left| \Pr_{k \leftarrow \text{KeyGen}(1^\lambda)}[1 \leftarrow \mathcal{A}^{\text{StateGen}(k, \cdot)}(1^\lambda)] - \Pr[1 \leftarrow \mathcal{A}^{\mathcal{O}_{\text{Haar}}}(1^\lambda)] \right| \leq \text{negl}(\lambda). \quad (17)$$

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

1. Sample $|\psi_x\rangle \leftarrow \mu$ for each x .
2. When x is queried, return $|\psi_x\rangle$.

Definition 5 (Classical-Query PRFSGs). A pseudorandom function-like state generator (PRFSG) is called a classical-query PRFSG if it is secure against only adversaries that query the oracle classically.

Remark 3. 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.

Definition 6 ((Non-adaptive) Pseudorandom Unitaries (PRUs) [JLS18, MPSY24]). Let $\mathcal{K}_\lambda$ denote the key space at most $\text{poly}(\lambda)$ bits. A family $\{\{U_k\}_{k \in \mathcal{K}_\lambda}\}_{\lambda \in \mathbb{N}}$ of unitaries is a pseudorandom unitary (PRU) if it satisfies the following:

- Efficient generation: there exists a QPT algorithm G that implements U_k on input k . Namely, for any $m(\lambda)$ -qubit state $|\psi\rangle$, $G(k, |\psi\rangle)$ outputs $U_k |\psi\rangle$.

- Indistinguishability from Haar random unitary: For any QPT algorithm $\mathcal{A}^{(\cdot)}$,

$$\left| \Pr_{k \leftarrow \mathcal{U}(\mathcal{K}_\lambda)}[1 \leftarrow \mathcal{A}^{U_k}] - \Pr_{U \leftarrow \mu_U}[1 \leftarrow \mathcal{A}^U] \right| \leq \text{negl}(\lambda), \quad (18)$$

where $\mathcal{U}(\mathcal{K}_\lambda)$ denotes the uniform distribution over $\mathcal{K}_\lambda$.

If the indistinguishability holds only for adversaries with non-adaptive queries (i.e., $U^{\otimes \text{poly}(\lambda)}$ can be queried only at once), we say that $\{\{U_k\}_{k \in \mathcal{K}_\lambda}\}_{\lambda \in \mathbb{N}}$ is a non-adaptive PRU.

2.3 Design and Haar Measure

The following lemma shows that there exists an efficient approximate quantum t -design that approximates the Haar measure over states.

Lemma 4 ([Kre21, Lemma 8 and Fact 9] based on [BHH16], adapted). *For each $n, t \in \mathbb{N}$ and $\epsilon > 0$, there exists a $\text{poly}(n, t, \log \frac{1}{\epsilon})$ -time quantum algorithm $\mathcal{S}_{n,t,\epsilon}$ that outputs an n -qubit state such that for any quantum algorithm $\mathcal{A}$,*

$$(1 - \epsilon) \Pr_{|\psi\rangle \leftarrow \mu_n} [1 \leftarrow \mathcal{A}(|\psi\rangle^{\otimes t})] \leq \Pr_{|\psi\rangle \leftarrow \mathcal{S}_{n,t,\epsilon}} [1 \leftarrow \mathcal{A}(|\psi\rangle^{\otimes t})] \leq (1 + \epsilon) \Pr_{|\psi\rangle \leftarrow \mu_n} [1 \leftarrow \mathcal{A}(|\psi\rangle^{\otimes t})]. \quad (19)$$

We will use the Haar measure for definitions and use efficient approximate quantum t -designs for the security proof. An exception is symmetric-key encryption in [Appendix A](#), where we use the efficient approximate quantum t -designs for constructions.

The next lemma says that two independent samples from the Haar measure is almost orthogonal.

Lemma 5.

$$\mathbb{E}_{|\psi\rangle, |\phi\rangle \leftarrow \mu_n} |\langle \psi | \phi \rangle|^2 = \frac{1}{2^n}. \quad (20)$$

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

$$\mathbb{E}_{|\psi\rangle, |\phi\rangle \leftarrow \mu_n} |\langle \psi | \phi \rangle|^2 = \mathbb{E}_{|\phi\rangle \leftarrow \mu_n} \langle \phi | [\mathbb{E}_{|\psi\rangle \leftarrow \mu_n} |\psi\rangle \langle \psi|] | \phi \rangle = \frac{1}{2^n}. \quad (21)$$

□

3 Quantum Group Actions and Hardness Assumptions

In this section, we define quantum group actions (QGAs) and their properties. (For a review of classical group actions, see [Appendix B](#).) We also introduce several hardness assumptions for QGAs, including one-wayness and various notions of pseudorandomness.

3.1 Quantum Group Actions

We first define quantum group actions (QGAs), which are a quantum analogue of group actions.

Definition 7 (Quantum Group Actions (QGAs)). A quantum group action (QGA) is a pair (G, S) of a group G and a set S such that

- G : a subgroup of λ -qubit unitary operators.
- S : a set of λ -qubit states.

We require that for any $g \in G$ and $\phi \in S$, $g\phi g^\dagger \in S$.

Remark 4. For notational simplicity, we present our definitions and results using pure states. However, all of our results extend straightforwardly to mixed states.

We define effective QGA, which is a quantum analogue of effective group actions [ADMP20].

Definition 8 (Effective Quantum Group Actions (EQGAs)). We say that a QGA (G, S) is *effective* if there are two algorithms **SampG** and **GenS** such that

- **SampG** $(1^\lambda) \rightarrow [g]$: It is a QPT algorithm that takes 1^λ as input, and outputs an efficient classical description $[g]$ of a unitary operator $g \in G$. An efficient classical description $[g]$ of g means, for example, a classical description of a $\text{poly}(\lambda)$ -size quantum circuit that implements g .
- **GenS** $(1^\lambda) \rightarrow [|s\rangle]$: It is a QPT algorithm that takes 1^λ as input, and outputs an efficient classical description $[|s\rangle]$ of a quantum state $|s\rangle \in S$. An efficient classical description $[|s\rangle]$ of $|s\rangle$ means, for example, a classical description of a $\text{poly}(\lambda)$ -size quantum circuit that prepares $|s\rangle$.

Remark 5. Note that neither **SampG** nor **GenS** is required to be deterministic. Consequently, different executions of **SampG** (respectively, **GenS**) may output different descriptions $[g]$ (respectively, $[|s\rangle]$).

Remark 6. Unlike effective group actions [ADMP20] (see Subsection B.1), we do not require **SampG** to sample uniformly from the entire group G . In particular, if we define

$$\text{Supp}(\text{SampG}) := \{g \in G : [g] \leftarrow \text{SampG}(1^\lambda) \text{ with nonzero probability}\},$$

then we do not require $\text{Supp}(\text{SampG}) = G$. The reason is that our cryptographic definitions do not depend on the distribution of g itself, but only on the distribution of the resulting state $g|s\rangle$. For example, our pseudorandomness notions will be defined via the computational indistinguishability between states generated as $g|s\rangle$, where $[g] \leftarrow \text{SampG}(1^\lambda)$, and Haar-random states. Therefore, requiring **SampG** to sample uniformly from all of G is unnecessary for our purposes. A similar relaxation is possible even in classical effective group actions. There, pseudorandomness is defined by comparing the distribution of $g \star s_0$ with the uniform distribution over the state space S , and the distribution of g itself need not be uniform over G . Indeed, some lattice-based constructions consider non-uniform sampling procedures, e.g., [BBCK24].

Remark 7. For simplicity, we often write $[g]$ and $[|s\rangle]$ simply as g and $|s\rangle$, respectively, whenever no confusion can arise. Moreover, throughout the remainder of the paper, all QGAs are assumed to be effective. Accordingly, we omit the qualifier “effective” and simply write QGA.

3.2 One-Way QGAs

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

Definition 9 (One-Way Quantum Group Actions (OW QGAs)). A QGA (G, S) with $(\text{SampG}, \text{GenS})$ is called *one-way (OW)* if for any QPT adversary $\mathcal{A}$ and any polynomial t , $\Pr[\mathcal{T} \leftarrow \mathcal{C}] \leq \text{negl}(\lambda)$ is satisfied in the following security game.

1. The challenger $\mathcal{C}$ runs $|s\rangle \leftarrow \text{SampG}(1^\lambda)$ and $g \leftarrow \text{SampG}(1^\lambda)$.
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' .¹⁹

¹⁹ $[g']$ could be outside of G .

4. $\mathcal{C}$ projects $g|s\rangle$ onto $g'|s\rangle$. If the projection is successful, $\mathcal{C}$ outputs $\top$. Otherwise, it outputs $\perp$.

Lemma 6. *If one-way quantum group action (OW QGAs) exist then one-way state generators (OWSGs) exist.*

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

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

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

$$\sum_{|s\rangle, g} \Pr[|s\rangle \leftarrow \text{GenS}(1^\lambda)] \Pr[g \leftarrow \text{SampG}(1^\lambda)] \left(\sum_{[|s'\rangle], [g']} \Pr[(|s'\rangle, [g']) \leftarrow \mathcal{A}(1^\lambda, (|s\rangle \otimes g|s\rangle)^{\otimes t})] \cdot \frac{1 + |\langle s|(g')^\dagger g|s\rangle|^2}{2} \right) \quad (22)$$

$$\geq 1 - \frac{1}{p(\lambda)}, \quad (23)$$

which means that

$$\sum_{|s\rangle, g} \Pr[|s\rangle \leftarrow \text{GenS}(1^\lambda)] \Pr[g \leftarrow \text{SampG}(1^\lambda)] \left(\sum_{[|s'\rangle], [g']} \Pr[(|s'\rangle, [g']) \leftarrow \mathcal{A}(1^\lambda, (|s\rangle \otimes g|s\rangle)^{\otimes t})] \cdot |\langle s|(g')^\dagger g|s\rangle|^2 \right) \quad (24)$$

$$\geq 1 - \frac{2}{p(\lambda)}. \quad (25)$$

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

3.3 Pseudorandom QGAs

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

Definition 10 (Pseudorandom Quantum Group Actions (PR QGAs)). We say that a QGA (G, S) with $(\text{SampG}, \text{GenS})$ is *pseudorandom (PR)* if the following two distributions are computationally indistinguishable for any polynomial t :

$$\text{PR}_0 : \text{return } (|s_0\rangle, h|s_0\rangle)^{\otimes t}, \text{ where } |s_0\rangle \leftarrow \text{GenS}(1^\lambda), h \leftarrow \text{SampG}(1^\lambda),$$

$$\text{PR}_1 : \text{return } (|s_0\rangle, h|s\rangle)^{\otimes t}, \text{ where } |s_0\rangle \leftarrow \text{GenS}(1^\lambda), |s\rangle \leftarrow \mu.$$

It is easy to see that PR QGAs can be constructed from PRUs by setting $|s_0\rangle$ to be a fixed state, say, $|0\dots 0\rangle$, and considering $h \leftarrow \text{SampG}(1^\lambda)$ as sampling k and outputting U_k .

Lemma 7. *If pseudorandom unitaries (PRUs) exist, then pseudorandom quantum group action (PR QGAs) exist.*

We can show that the multiple samples are also pseudorandom.

Lemma 8. *Let (G, S) be a pseudorandom quantum group action (PR QGA) with $(\text{SampG}, \text{GenS})$. Then the following two distributions are computationally indistinguishable for any polynomials Q and t :*

mPR_0 : return $\{(h_q|s_0)\}^{\otimes t}_{q \in [Q]}$, where $|s_0\rangle \leftarrow \text{GenS}(1^\lambda)$ and $h_q \leftarrow \text{SampG}(1^\lambda)$ for $q \in [Q]$,
 mPR_1 : return $\{|s_q\rangle^{\otimes t}\}_{q \in [Q]}$, where $|s_q\rangle \leftarrow \mu$ for $q \in [Q]$.

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

- $|s_0\rangle \leftarrow \text{GenS}(1^\lambda)$
- For $q \in \{1, 2, \dots, j\}$, $|s_q\rangle \leftarrow \mu$.
- For $q \in \{j+1, \dots, Q\}$, $h_q \leftarrow \text{SampG}(1^\lambda)$.
- Output $\{|s_q\rangle^{\otimes t}\}_{q \in \{1, \dots, j\}}$ and $\{(h_q|s_0)\}^{\otimes t}_{q \in \{j+1, \dots, Q\}}$.

It is clear that $\text{mPR}_0 = H_0^{t,Q}$ and $\text{mPR}_1 = H_Q^{t,Q}$. We claim that for any QPT adversary $\mathcal{A}$, any polynomials Q, t , and any $j \in [Q]$

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

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 $|s_0\rangle \leftarrow \text{GenS}(1^\lambda)$ and $b \leftarrow \{0, 1\}$.
2. If $b = 0$, $\mathcal{C}$ chooses $h \leftarrow \text{SampG}(1^\lambda)$ 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 $\{(h_q|s_0)\}^{\otimes t}_{q \in \{j+1, \dots, Q\}}$, and outputs $\mathcal{A}$'s output. Here, all $|s_q\rangle$ are approximate quantum t -designs and each $h_q \leftarrow \text{SampG}(1^\lambda)$. (From Lemma 4, we can replace Haar random states with approximate quantum t -design states.) Note that $\mathcal{B}$ can efficiently generate the $\{(h_q|s_0)\}^{\otimes t}_{q \in \{j+1, \dots, Q\}}$ because $\mathcal{B}$ receives $|s_0\rangle^{\otimes Qt}$ from $\mathcal{C}$.

We have

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

Therefore, we have

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

for infinitely many λ , which means that the PR QGA is broken. $\square$

It is obvious that PR QGAs directly imply PRSGs.

Lemma 9. *If pseudorandom quantum group actions (PR QGAs) exist, then pseudorandom state generators (PRSGs) exist.*

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

- $\text{KeyGen}(1^\lambda) \rightarrow k : \text{Run } |s\rangle \leftarrow \text{GenS}(1^\lambda) \text{ and } g \leftarrow \text{SampG}(1^\lambda). \text{ Output } k := (|s\rangle, g).$
- $\text{StateGen}(1^\lambda, k) \rightarrow |\phi_k\rangle : \text{Parse } k = (|s\rangle, g). \text{ Output } |\phi_k\rangle := g|s\rangle.$

It is clear that this satisfies the security of PRSGs. $\square$

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 11 (Haar-Pseudorandom Quantum Group Actions (Haar-PR QGAs)). A QGA (G, S) with $(\text{SampG}, \text{GenS})$ is called *Haar-pseudorandom* (*Haar-PR*) if the following two distributions are computationally indistinguishable for any polynomial t :

$$\begin{aligned} \text{HaarPR}_0 & : \text{return } (|s\rangle, h|s\rangle)^{\otimes t}, \text{ where } |s\rangle \leftarrow \mu, h \leftarrow \text{SampG}(1^\lambda), \\ \text{HaarPR}_1 & : \text{return } (|s\rangle, |s'\rangle)^{\otimes t}, \text{ where } |s\rangle \leftarrow \mu, |s'\rangle \leftarrow \mu. \end{aligned}$$

Remark 8. Haar-PR QGAs can be considered as a computational version of the statistical construction of PRSGs in the common Haar state model [AGL24, CCS25].

Similarly to PR QGAs, Haar-PR QGAs can also be constructed from PRUs.

Lemma 10. *If pseudorandom unitaries (PRUs) exist, then Haar-pseudorandom quantum group actions (Haar-PR QGAs) exist.*

We can show that the multiple samples are also pseudorandom as in the case of PR QGAs Lemma 8.

Lemma 11. *Let (G, S) be a Haar-pseudorandom quantum group action (Haar-PR QGA) with $(\text{SampG}, \text{GenS})$. Then the following two distributions are computationally indistinguishable for any polynomials Q and t :*

$$\begin{aligned} \text{mHaarPR}_0 & : \text{return } \{(|s_q\rangle, h_q|s_q\rangle)^{\otimes t}\}_{q \in [Q]}, \text{ where } |s_q\rangle \leftarrow \mu, h_q \leftarrow \text{SampG}(1^\lambda) \text{ for } q \in [Q], \\ \text{mHaarPR}_1 & : \text{return } \{(|s_q\rangle, |s'_q\rangle)^{\otimes t}\}_{q \in [Q]}, \text{ where } |s_q\rangle \leftarrow \mu, |s'_q\rangle \leftarrow \mu \text{ for } q \in [Q]. \end{aligned}$$

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

- For $q \in \{1, 2, \dots, j\}$, $|s_q\rangle \leftarrow \mu$ and $|s'_q\rangle \leftarrow \mu$.
- For $q \in \{j+1, j+2, \dots, Q\}$, $|s_q\rangle \leftarrow \mu$ and $h_q \leftarrow \text{SampG}(1^\lambda)$.

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

It is clear that $\text{mHaarPR}_0 = H_0^{t,Q}$ and $\text{mHaarPR}_1 = H_Q^{t,Q}$. We claim that for any QPT adversary $\mathcal{A}$, any polynomials Q, t , and any $j \in [Q]$

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

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 $h \leftarrow \text{SampG}(1^\lambda)$, 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 $\{(|s_q\rangle, |s'_q\rangle)^{\otimes t}\}_{q \in \{1, \dots, j-1\}}$ and $\{(|s_q\rangle, h_q|s_q\rangle)^{\otimes t}\}_{q \in \{j+1, \dots, Q\}}$ by using t -designs. It then runs $\mathcal{A}$ on input $\{(|s_q\rangle, |s'_q\rangle)^{\otimes t}\}_{q \in \{1, \dots, j-1\}}$, the received state, and $\{(|s_q\rangle, h_q|s_q\rangle)^{\otimes t}\}_{q \in \{j+1, \dots, Q\}}$, and outputs its output. Here, all $|s_q\rangle, |s'_q\rangle$ are t -designs.

We have

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

Therefore, we have

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

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

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

Definition 12 (Decisional Diffie-Hellman Quantum Group Actions (DDH QGAs)). A QGA (G, S) with $(\text{SampG}, \text{GenS})$ is called *Decisional Diffie-Hellman (DDH)* if the following two distributions are computationally indistinguishable for any polynomial t :

DDH_0 : return $(|s_0\rangle, \tilde{g}|s_0\rangle, g|s_0\rangle, \tilde{g}g|s_0\rangle)^{\otimes t}$, where $|s_0\rangle \leftarrow \text{GenS}(1^\lambda)$ and $\tilde{g}, g \leftarrow \text{SampG}(1^\lambda)$,
 DDH_1 : return $(|s_0\rangle, \tilde{g}|s_0\rangle, g|s_0\rangle, h|s_0\rangle)^{\otimes t}$, where $|s_0\rangle \leftarrow \text{GenS}(1^\lambda)$ and $\tilde{g}, g, h \leftarrow \text{SampG}(1^\lambda)$.

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 13 (Haar-Decisional Diffie-Hellman Quantum Group Actions (Haar-DDH QGAs)). A QGA (G, S) with $(\text{SampG}, \text{GenS})$ is called *Haar-Decisional Diffie-Hellman (Haar-DDH)* if the following two distributions are computationally indistinguishable for any polynomials Q and t :

HaarDDH_0 : return $\{(|s_q\rangle, \tilde{g}|s_q\rangle)^{\otimes t}\}_{q \in [Q]}$, where $\tilde{g} \leftarrow \text{SampG}(1^\lambda)$ and $|s_q\rangle \leftarrow \mu$ for $q \in [Q]$,
 HaarDDH_1 : return $\{(|s_q\rangle, h_q|s_q\rangle)^{\otimes t}\}_{q \in [Q]}$, where $|s_q\rangle \leftarrow \mu, h_q \leftarrow \text{SampG}(1^\lambda)$ for $q \in [Q]$.

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 14 (Naor-Reingold Quantum Group Actions (NR QGAs)). A QGA (G, S) with $(\text{SampG}, \text{GenS})$ is called *Naor-Reingold (NR)* if the following two distributions are computationally indistinguishable for any polynomial Q and t :

NR_0 : return $\{(g_q|s_0), \tilde{g}g_q|s_0)\}^{\otimes t}_{q \in [Q]}$, where $|s_0\rangle \leftarrow \text{GenS}(1^\lambda)$, $\tilde{g} \leftarrow \text{SampG}(1^\lambda)$, and $g_q \leftarrow \text{SampG}(1^\lambda)$ for $q \in [Q]$;

NR_1 : return $\{(g_q|s_0), h_q|s_0)\}^{\otimes t}_{q \in [Q]}$, where $|s_0\rangle \leftarrow \text{GenS}(1^\lambda)$ and $g_q, h_q \leftarrow \text{SampG}(1^\lambda)$ for $q \in [Q]$.

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 QGAs, we will face several problems since we cannot use algebraic structures; G and S might not be closed. Fortunately, the NR property of QGA follows from its PR, Haar-PR, and Haar-DDH properties as follows:

Theorem 1. *If a quantum group action (QGA) is pseudorandom (PR), Haar-pseudorandom (Haar-PR), and Haar-decisional Diffie-Hellman (Haar-DDH), then it is Naor-Reingold (NR).*

Proof. To show the lemma, we introduce three intermediate distributions H_1, H_2, H_3 defined as follows, where we recap NR_0 and NR_1 for comparisons:

NR_0 : return $\{(g_q|s_0), \tilde{g}g_q|s_0)\}^{\otimes t}_{q \in [Q]}$, where $|s_0\rangle \leftarrow \text{GenS}(1^\lambda)$, $\tilde{g} \leftarrow \text{SampG}(1^\lambda)$, and $g_q \leftarrow \text{SampG}(1^\lambda)$ for $q \in [Q]$;

H_1 : return $\{(|s_q\rangle, \tilde{g}|s_q\rangle)\}^{\otimes t}_{q \in [Q]}$, where $\tilde{g} \leftarrow \text{SampG}(1^\lambda)$ and $|s_q\rangle \leftarrow \mu$ for $q \in [Q]$;

H_2 : return $\{(|s_q\rangle, h_q|s_q\rangle)\}^{\otimes t}_{q \in [Q]}$, where $|s_q\rangle \leftarrow \mu$ and $h_q \leftarrow \text{SampG}(1^\lambda)$ for $q \in [Q]$;

H_3 : return $\{(|s_q\rangle, |s'_q\rangle)\}^{\otimes t}_{q \in [Q]}$, where $|s_q\rangle, |s'_q\rangle \leftarrow \mu$ for $q \in [Q]$;

NR_1 : return $\{(g_q|s_0), h_q|s_0)\}^{\otimes t}_{q \in [Q]}$, where $|s_0\rangle \leftarrow \text{GenS}(1^\lambda)$ and $g_q, h_q \leftarrow \text{SampG}(1^\lambda)$ for $q \in [Q]$.

The following four lemmas show that $\text{NR}_0 \approx_c H_1 \approx_c H_2 \approx_c H_3 \approx_c \text{NR}_1$ under our assumptions and this completes the proof. $\square$

Lemma 12. *If QGA is pseudorandom (PR), then $\text{NR}_0 \approx_c H_1$.*

Proof. Assuming that QGA is PR, we know that mPR_0 and mPR_1 are computationally indistinguishable due to [Lemma 8](#). To show $\text{NR}_0 \approx_c H_1$, it is enough to show that we can efficiently convert samples from mPR_0 and mPR_1 into NR_0 and H_1 in an oblivious way, respectively. Suppose that we are given samples $\{|y_q\rangle^{\otimes 2t}\}_{q \in [Q]}$ from mPR_0 or mPR_1 , where $|y_q\rangle = h_q|s_0\rangle$ for mPR_0 and $|y_q\rangle = |s_q\rangle$ for mPR_1 . To prepare samples for NR_0 or H_1 , we choose $\tilde{g} \leftarrow \text{SampG}(1^\lambda)$ and output $\{(|y_q\rangle, \tilde{g}|y_q\rangle)\}^{\otimes t}_{q \in [Q]}$. If the input distribution is mPR_0 , then the output distribution is NR_0 . On the other hand, if the input distribution is PR_1 , then the output distribution is H_1 . This completes the proof. $\square$

Lemma 13. *If QGA is Haar-decisional Diffie-Hellman (Haar-DDH), then $H_1 \approx_c H_2$.*

Proof. This directly follows from the Haar-DDH assumption ([Definition 13](#)). $\square$

Lemma 14. *If QGA is Haar-pseudorandom (Haar-PR), then $H_2 \approx_c H_3$.*

Proof. This directly follows from the multi-instance version of Haar-PR (Lemma 11). $\square$

Lemma 15. *If QGA is pseudorandom (PR), then $H_3 \approx_c \text{NR}_1$.*

Proof. We construct an efficient quantum algorithm that converts samples from mPR_0 and mPR_1 in Lemma 8 and into samples from NR_1 and H_3 , respectively. Suppose that we are given samples $\{|y_q\rangle^{\otimes t}\}_{q \in [2Q]}$ from mPR_0 or mPR_1 , where $|y_q\rangle = h_q|s_0\rangle$ for mPR_0 and $|y_q\rangle = |s_q\rangle$ for mPR_1 . We just output $\{(|y_{2q-1}\rangle, |y_{2q}\rangle)^{\otimes t}\}_{q \in [Q]}$ by rearranging samples. If the input distribution is mPR_0 , then the output distribution is NR_1 . On the other hand, if the input distribution is mPR_1 , then the output distribution is H_3 as we wanted. $\square$

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

Theorem 2. *Let (G, S) be a QGA with $(\text{SampG}, \text{GenS})$. If G is commutative and (G, S) is decisional Diffie-Hellman (DDH), then (G, S) is Naor-Reingold (NR).*

Proof. For $i = 0, \dots, Q$, we consider the following hybrid distributions H_i :

- $\tilde{g} \leftarrow \text{SampG}(1^\lambda)$ and $|s_0\rangle \leftarrow \text{GenS}(1^\lambda)$.
- For $j = 1, \dots, i$, $|\phi_j\rangle := g_j|s_0\rangle$ and $|\psi_j\rangle := h_j|s_0\rangle$, where $g_j, h_j \leftarrow \text{SampG}(1^\lambda)$.
- For $j = i + 1, \dots, Q$, $|\phi_j\rangle := g_j|s_0\rangle$ and $|\psi_j\rangle := \tilde{g}g_j|s_0\rangle$, where $g_j \leftarrow \text{SampG}(1^\lambda)$.
- Output $\{(|\phi_q\rangle, |\psi_q\rangle)^{\otimes t}\}_{q \in [Q]}$.

We have $H_0 = \text{NR}_0$ and $H_Q = \text{NR}_1$. By using the following lemma, we have $H_0 \approx_c H_1 \approx_c \dots \approx_c H_Q$. $\square$

Lemma 16. *Let (G, S) be a QGA with $(\text{SampG}, \text{GenS})$. If G is commutative and (G, S) is decisional Diffie-Hellman (DDH), then, for $i = 1, \dots, Q$, $H_{i-1} \approx_c H_i$ holds.*

Proof. Suppose that there exists $\mathcal{A}$ distinguishing H_{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 $q = 1, \dots, i - 1$, take random $g_q, h_q \leftarrow \text{SampG}(1^\lambda)$ 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 $q = i + 1, \dots, Q$, take random $g_q \leftarrow \text{SampG}(1^\lambda)$ 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 $\{(|\phi_q\rangle, |\psi_q\rangle)^{\otimes t}\}_{q \in [Q]}$ 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 H_{i-1} . If h is random, then $\mathcal{B}$ perfectly simulates the distribution H_i . Thus, $\mathcal{B}$'s advantage is equivalent to $\mathcal{A}$'s advantage distinguishing H_{i-1} and H_i . $\square$

4 Construction of (Classical-Query) PRFSGs

4.1 Construction

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

Theorem 3. *Let (G, S) be a QGA with $(\text{SampG}, \text{GenS})$. If (G, S) is pseudorandom (PR) and Naor-Reingold (NR), then the following $(\text{KeyGen}, \text{StateGen})$ is a pseudorandom function-like state generator (PRFSG) whose input space is $\{0, 1\}^\ell$.*

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

$$|\phi_k(x)\rangle := g_\ell^{x[\ell]} g_{\ell-1}^{x[\ell-1]} \dots g_1^{x[1]} g_0 |s_0\rangle. \quad (26)$$

From Theorem 1 and Theorem 2, we obtain the following corollaries.

Corollary 1. *If a QGA is pseudorandom (PR), Haar-pseudorandom (Haar-PR), and Haar-decisional Diffie-Hellman (Haar-DDH), then the above construction is a PRFSG.*

Corollary 2. *If a QGA is pseudorandom (PR) and decisional Diffie-Hellman (DDH) and G is commutative, then the above construction is a PRFSG.*

To show Theorem 3, we define three games Real, Hybrid, and Ideal defined as follows:

- **Real:** This is the PRFSG security game whose oracle is $\text{StateGen}(k, \cdot)$. That is, the challenger $\mathcal{C}$ chooses $k \leftarrow \text{KeyGen}(1^\lambda)$ and runs $\mathcal{A}$ with the oracle $\text{StateGen}(k, \cdot)$, which takes a classical string $x \in \{0, 1\}^\ell$ 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 $h_x \leftarrow \text{SampG}(1^\lambda)$ 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 $\mathcal{O}_{\text{Haar}}$ defined as follows: On query x , if it is not queried before, then $\mathcal{O}_{\text{Haar}}$ samples $|s_x\rangle \leftarrow \mu$ and returns $|s_x\rangle$; otherwise, it returns $|s_x\rangle$.

Lemma 17 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 18). Thus, we obtain Theorem 3. The lemmas follow.

Lemma 17. *Real and Hybrid are computationally indistinguishable if QGA is Naor-Reingold (NR).*

Proof. We define the following hybrid games Game_j for $j = 0, \dots, \ell$: The challenger samples $|s_0\rangle \leftarrow \text{GenS}(1^\lambda)$, $g_0 \leftarrow \text{SampG}(1^\lambda)$, and $g_i \leftarrow \text{SampG}(1^\lambda)$ 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 $g_q \leftarrow \text{SampG}(1^\lambda)$ and $|y_q\rangle := g_q|s_0\rangle$.

3. Return $|f_{j,q}\rangle := g_\ell^{x_q[\ell]} \dots g_{j+1}^{x_q[j+1]} |y_q\rangle$.

We note that if the query is repeated, then the challenger returns the same answer correctly. It is easy to verify Game_0 and Game_ℓ are Real and Hybrid, respectively. In what follows, we show that $\text{Game}_0 \approx_c \text{Game}_1 \approx_c \dots \approx_c \text{Game}_\ell$ if the QGA is NR.

Fix $j \in \{0, \dots, \ell - 1\}$ and consider the computational indistinguishability between Game_j and Game_{j+1} . Let Q be the number of the adversary's queries. The definition of NR QGAs implies that $\text{NR}_0 \approx_c \text{NR}_1$ (Definition 14) where we will set the number of copies t as Q . Thus, it is enough to construct a reduction algorithm $\mathcal{B}$ distinguishing NR_0 and 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 NR_0 or $(g_q|s_0\rangle, h_q|s_0\rangle)$ in NR_1 . It prepares $g_{j+2}, \dots, g_\ell \leftarrow \text{SampG}(1^\lambda)$. 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 $|\tilde{y}_q\rangle := |\tilde{y}_{q'}\rangle$ and $|\tilde{z}_q\rangle := |\tilde{z}_{q'}\rangle$. (This is possible since we have Q copies.) Otherwise, it picks new quantum states from the pool, that is, sets $|\tilde{y}_q\rangle := |y_c\rangle$ and $|\tilde{z}_q\rangle := |z_c\rangle$ and increments c . It then answers

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

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

If the given samples follow NR_0 , then the above simulation perfectly simulates Game_j by letting $\tilde{g} := g_{j+1}$. If the given samples follow NR_1 , then the above simulation perfectly simulates Game_{j+1} since g_q 's and h_q 's in NR_1 are chosen independently. Thus, we have $\text{Game}_j \approx_c \text{Game}_{j+1}$ if the QGA is NR. $\square$

Lemma 18. *Hybrid and Ideal are computationally indistinguishable if QGA is pseudorandom (PR).*

Proof. This lemma immediately follows from the pseudorandomness of multiple samples in Lemma 8, where we need to set the number of copies t as Q . $\square$

4.2 On Quantum-Query PRFSGs

As remarked in Remark 3, we only consider classical-query pseudorandom function-like state generators (PRFSGs) (Definition 4). Currently, we fail to show either positive results that our Naor-Reingold-type PRFSG is secure against quantum queries or negative results, that is, the separation of classical-query and quantum-query PRFSGs. We discuss barriers to positive or negative results in the following.

Barriers to positive results. We tried to show our Naor-Reingold-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 pseudorandom (PR) QGAs?

For simplicity, we consider the case of small input space $\{0, 1\}^\ell$ with $\ell = O(\log(\lambda))$.²⁰ We identify $\{0, 1\}^\ell$ with $[2^\ell]$. If we consider PRFs, then classical-query PRFs against a quantum adversary are 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:

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

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

Barriers to 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 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 $\text{PRF}' : ((k, a), x) \mapsto \text{PRF}(k, x \bmod a)$, 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*, 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 prepares a quantum state $\frac{1}{\sqrt{W}} \sum_{x,s \in \mathbb{Z}_W} \exp(2\pi i x s / W) |s\rangle |\text{PRF}'_{k,a}(x)\rangle = \frac{1}{\sqrt{W}} \sum_{x,s \in \mathbb{Z}_W} \exp(2\pi i x s / W) |s\rangle |\text{PRF}_k(x \bmod a)\rangle$. We note that the success probability of the algorithm strongly depends on the distinctness of $\text{PRF}(k, 0), \dots, \text{PRF}(k, a-1)$ 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 a new PRFSG' from PRFSG in the same way. While the distinctness follows from the quantum-query security of PRFSG, we fail to construct the measurement to distinguish a independent samples $|\psi_1\rangle, \dots, |\psi_a\rangle$ from the Haar measure.

5 Constructions of QGAs from PRUs

In this section, we show that pseudorandom unitaries (PRUs) in Definition 6 imply QGAs which are pseudorandom (PR), Haar-pseudorandom (Haar-PR), and Haar-decisional Diffie-Hellman (Haar-DDH). We construct it as follows:

²⁰If $\ell = \omega(\log(\lambda))$, we then invoke the small-range distribution argument in Zhandry [Zha12b].

Definition 15. Let $\{\{U_k\}_{k \in \mathcal{K}_\lambda}\}_{\lambda \in \mathbb{N}}$ be a non-adaptive PRU. We define effective QGA (G, S) with $(\text{SampG}, \text{GenS})$ as follows:

- G : a set of unitary operations.
- S : a set of m -qubits states.
- $\text{SampG}(1^\lambda) \rightarrow [g]$: Choose $k \leftarrow \mathcal{K}_\lambda$ and set $g := U_k$.
- $\text{GenS}(1^\lambda) \rightarrow [|s\rangle]$: Output $|0\dots 0\rangle$.

Our goal is to show the following:

Theorem 4. *If non-adaptive PRUs exist, then (G, S) in Definition 15 is PR, Haar-PR, and Haar-DDH.*

We show that it is PR, Haar-PR, and Haar-DDH in Subsection 5.1, Subsection 5.2, and Subsection 5.3, respectively.

We will use the following lemma.

Lemma 19 ([AGKL24]). *Let $m, t, Q \in \mathbb{N}$. Suppose that $|\phi_1\rangle, \dots, |\phi_Q\rangle$ are m -qubit states which are orthogonal to each other. Then,*

$$\left\| \mathbb{E}_{|\psi_1\rangle, \dots, |\psi_Q\rangle \leftarrow \mu_m} \bigotimes_{q \in [Q]} |\psi_q\rangle \langle \psi_q|^{\otimes t} - \mathbb{E}_{U \leftarrow \mu_m^U} \bigotimes_{q \in [Q]} (U |\phi_q\rangle \langle \phi_q| U^\dagger)^{\otimes t} \right\|_1 \leq O\left(\frac{Qt^2}{2^m}\right). \quad (27)$$

5.1 PR

First, we show that the QGA in Definition 15 is PR.

Lemma 20. *If non-adaptive PRUs exist, then (G, S) in Definition 15 is pseudorandom (PR).*

Proof of Lemma 20. Let t be a polynomial. Consider the following states:

$$\begin{aligned} \rho_0 &:= \mathbb{E}_{k \leftarrow \mathcal{K}_\lambda} |0\dots 0\rangle \langle 0\dots 0|^{\otimes t} \otimes (U_k |0\dots 0\rangle \langle 0\dots 0| U_k^\dagger)^{\otimes t}, \\ \rho_1 &:= \mathbb{E}_{U \leftarrow \mu^U} |0\dots 0\rangle \langle 0\dots 0|^{\otimes t} \otimes (U |0\dots 0\rangle \langle 0\dots 0| U^\dagger)^{\otimes t}, \\ \rho_2 &:= \mathbb{E}_{|s\rangle \leftarrow \mu} |0\dots 0\rangle \langle 0\dots 0|^{\otimes t} \otimes |s\rangle \langle s|^{\otimes t}. \end{aligned}$$

Note that ρ_0 and ρ_2 are equal to the output of PR_0 and PR_1 in Definition 10, respectively since $\text{GenS}(1^\lambda)$ outputs $|0\dots 0\rangle$ with probability 1. Since $\{U_k\}_k$ is a non-adaptive PRU, ρ_0 and ρ_1 are computationally indistinguishable. Moreover, it is clear that $\rho_1 = \rho_2$ since $U |0\dots 0\rangle$ is a Haar random state. Thus, ρ_0 is computationally indistinguishable from ρ_2 , which concludes the proof. $\square$

5.2 Haar-PR

Next, we show that the QGA in Definition 15 is Haar-PR.

Lemma 21. *If non-adaptive PRUs exist, then (G, S) in Definition 15 is Haar-pseudorandom (Haar-PR).*

Proof of Lemma 21. Let t be a polynomial. Consider the following states:

$$\begin{aligned}\rho_0 &:= \mathbb{E}_{k \leftarrow \mathcal{K}_\lambda, |s\rangle \leftarrow \mu} |s\rangle \langle s|^{\otimes t} \otimes (U_k |s\rangle \langle s| U_k^\dagger)^{\otimes t}, \\ \rho_1 &:= \mathbb{E}_{U \leftarrow \mu^U, |s\rangle \leftarrow \mu} |s\rangle \langle s|^{\otimes t} \otimes (U |s\rangle \langle s| U^\dagger)^{\otimes t}, \\ \rho_2 &:= \mathbb{E}_{|s\rangle, |s'\rangle \leftarrow \mu} |s\rangle \langle s|^{\otimes t} \otimes |s'\rangle \langle s'|^{\otimes t}.\end{aligned}$$

Note that ρ_0 and ρ_2 are equal to the output of HaarPR_0 and HaarPR_1 in Definition 11, respectively. Since $\{U_k\}_k$ is a non-adaptive PRU, ρ_0 and ρ_1 are computationally indistinguishable. Moreover, it is clear that $\rho_1 = \rho_2$ since $U |s\rangle$ is an independent Haar random state. Thus, ρ_0 is computationally indistinguishable from ρ_2 , which concludes the proof. $\square$

5.3 Haar-DDH

Finally, we show that the QGA in Definition 15 is Haar-DDH.

Lemma 22. *If non-adaptive PRUs exist, then (G, S) in Definition 15 is Haar-decisional Diffie-Hellman (Haar-DDH).*

Proof of Lemma 22. Let t and Q be polynomials. Define $|\phi_1\rangle, \dots, |\phi_Q\rangle$ as orthogonal states. Consider the following states:

$$\begin{aligned}\rho_0 &:= \mathbb{E}_{\substack{k \leftarrow \mathcal{K}_\lambda, \\ |s_1\rangle, \dots, |s_Q\rangle \leftarrow \mu}} \bigotimes_{q \in [Q]} \left(|s_q\rangle \langle s_q|^{\otimes t} \otimes (U_k |s_q\rangle \langle s_q| U_k^\dagger)^{\otimes t} \right), \\ \rho_1 &:= \mathbb{E}_{\substack{U \leftarrow \mu^U, \\ |s_1\rangle, \dots, |s_Q\rangle \leftarrow \mu}} \bigotimes_{q \in [Q]} \left(|s_q\rangle \langle s_q|^{\otimes t} \otimes (U |s_q\rangle \langle s_q| U^\dagger)^{\otimes t} \right), \\ \rho_2 &:= \mathbb{E}_{U, V \leftarrow \mu^U} \bigotimes_{q \in [Q]} \left((V | \phi_q\rangle \langle \phi_q| V^\dagger)^{\otimes t} \otimes (UV | \phi_q\rangle \langle \phi_q| V^\dagger U^\dagger)^{\otimes t} \right), \\ \rho_3 &:= \mathbb{E}_{V, W \leftarrow \mu^U} \bigotimes_{q \in [Q]} \left((V | \phi_q\rangle \langle \phi_q| V^\dagger)^{\otimes t} \otimes (W | \phi_q\rangle \langle \phi_q| W^\dagger)^{\otimes t} \right), \\ \rho_4 &:= \mathbb{E}_{\substack{|s_1\rangle, \dots, |s_Q\rangle \leftarrow \mu, \\ |s'_1\rangle, \dots, |s'_Q\rangle \leftarrow \mu}} \bigotimes_{q \in [Q]} \left(|s_q\rangle \langle s_q|^{\otimes t} \otimes |s'_q\rangle \langle s'_q|^{\otimes t} \right), \\ \rho_5 &:= \mathbb{E}_{\substack{U_1, \dots, U_Q \leftarrow \mu^U, \\ |s_1\rangle, \dots, |s_Q\rangle \leftarrow \mu}} \bigotimes_{q \in [Q]} \left(|s_q\rangle \langle s_q|^{\otimes t} \otimes (U_q |s_q\rangle \langle s_q| U_q^\dagger)^{\otimes t} \right), \\ \rho_6 &:= \mathbb{E}_{\substack{k_1, \dots, k_Q \leftarrow \mathcal{K}_\lambda, \\ |s_1\rangle, \dots, |s_Q\rangle \leftarrow \mu}} \bigotimes_{q \in [Q]} \left(|s_q\rangle \langle s_q|^{\otimes t} \otimes (U_{k_q} |s_q\rangle \langle s_q| U_{k_q}^\dagger)^{\otimes t} \right).\end{aligned}$$

Note that ρ_0 and ρ_6 are equal to HaarPR_0 and HaarPR_1 in Definition 13, respectively. Thus, our goal is to show ρ_0 and ρ_6 are computationally indistinguishable. We show it as follows:

- ρ_0 and ρ_1 are computationally indistinguishable since $\{U_k\}_k$ is a non-adaptive PRU.
- ρ_1 and ρ_2 are statistically indistinguishable from Lemma 19.
- $\rho_2 = \rho_3$ from the left and right invariance of the Haar measure.

- ρ_3 and ρ_4 are statistically indistinguishable from [Lemma 19](#).
- $\rho_4 = \rho_5$ from the left and right invariance of the Haar measure.
- ρ_5 and ρ_6 are computationally indistinguishable since $\{U_k\}_k$ is a non-adaptive PRU.

□

6 Candidates of QGA

In this section, we advocate 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 in G .

6.1 Non-commutative QGA candidate

The first candidate is based on a random quantum circuit. We conjecture that this QGA satisfies pseudorandom (PR), Haar-pseudorandom (Haar-PR), and Haar-decisional Diffie-Hellman (Haar-DDH).

Definition 16 (Candidate 1: Random-circuit QGA). We define an effective QGA (G, S) with $(\text{SampG}, \text{GenS})$ as follows:

- G : a set of all quantum circuits.
- S : the state space of a λ -qubit system.
- $\text{SampG}(1^\lambda) \rightarrow [g]$: Output a random quantum circuit g .
- $\text{GenS}(1^\lambda) \rightarrow [|s]\rangle$: Output $|s\rangle := |0^\lambda\rangle$.

Note that random quantum circuits are conjectured to be pseudorandom unitaries (PRUs) [\[AQY22, ABGL25\]](#) since sufficiently deep random circuits are approximate unitary t -designs [\[BHH16, HM23\]](#). As we shown in [Section 5](#), a PRU instantiates a PR, Haar-PR, and Haar-DDH QGA. Thus, our conjecture holds if random quantum circuits are PRUs.

6.2 Commutative QGA candidate

Inspired by Instantaneous Quantum Polynomial (IQP), we conjecture that the following two *commutative* QGAs are PR, Haar-PR, and Haar-DDH. Let us denote the group of all IQP circuits by

$$G_{\text{IQP}} := \{H^{\otimes \lambda} D H^{\otimes \lambda} \mid D \text{ is a } Z\text{-diagonal circuit}\}.$$

We note that G_{IQP} is commutative, that is, $gh = hg$ holds for any $g = H^{\otimes \lambda} D_g H^{\otimes \lambda}$ and $h = H^{\otimes \lambda} D_h H^{\otimes \lambda}$.

Definition 17 (Candidate 2: IQP QGA with random Z -diagonal circuit). We define an IQP QGA (G, S) with $(\text{SampG}, \text{GenS})$ as follows:

- G : the group consisting of all IQP circuits, G_{IQP} .
- S : the state space of a λ -qubit system.
- $\text{SampG}(1^\lambda) \rightarrow [g]$: Take a random Z -diagonal circuit D ²¹ and output a description $[D]$. This defines $g = H^{\otimes \lambda} \cdot D \cdot H^{\otimes \lambda}$.

²¹E.g., a random circuit with gates $\{T, CS\}$ [\[BMS16\]](#).

- $\text{GenS}(1^\lambda) \rightarrow [|s\rangle] : \text{Output } |s\rangle := |0^\lambda\rangle$.

Definition 18 (Candidate 3: IQP QGA with random sparse polynomials). Let $d \in [1, \lambda]$ and polynomial $w = w(\lambda)$. Let $\mathcal{D}_{d,w}$ be

$$\mathcal{D}_{d,w} := \left\{ D: |x_1, \dots, x_\lambda\rangle \mapsto (-1)^{f(x_1, \dots, x_\lambda)} |x_1, \dots, x_\lambda\rangle \mid f \in \mathbb{F}_2[x_1, \dots, x_\lambda], \deg(f) \leq d, \text{term}(f) \leq w \right\},$$

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

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

We define an IQP QGA (G, S) with $(\text{SampG}, \text{GenS})$ as follows:

- G : the group consisting of all IQP circuits, G_{IQP} .
- S : the state space of a λ -qubit system.
- $\text{SampG}(1^\lambda) \rightarrow [g]$: Take a random sample $D \leftarrow \mathcal{D}_{d,w}$ and output a description $[D]$. This defines $g = H^{\otimes \lambda} \cdot D \cdot H^{\otimes \lambda}$.
- $\text{GenS}(1^\lambda) \rightarrow [|s\rangle]$: Output $|s\rangle := |0^\lambda\rangle$.

Candidates 2 and 3 differ in the way to choose the Z -diagonal circuit D .

Remark 9. We note that SampG takes a random sample within a restricted subset of G and the product of g and h chosen by SampG may be outside of the support of SampG , while it is in G .

On the relation between IQP QGAs and PRUs: 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.

We do not think small modifications of IQP random circuits will not realize PRUs because of the following reason: There are only two known constructions of PRUs. One is [BHHP25] where PRUs are constructed from the $FHFHFC$ circuit. (Here F is a Z -diagonal circuit, H is the Hadamard gate, and C is a Clifford gate.) The other one is [MPSY24, MH25] where PRUs are constructed from the PFC circuit. (Here P is the permutation of basis.) These circuits are clearly “far from” the IQP circuit, and making them closer to IQP seems to be very challenging.

As we already saw in the previous section, PRUs imply non-commutative QGAs. But, we do not know how to construct *commutative* QGAs from PRUs, and leave it as an open problem.

6.3 On the security of IQP-like QGAs

We discuss why we conjecture that our IQP-like QGAs satisfy PR, Haar-PR, and Haar-DDH. Here we focus on Candidate 3, since it is more restrictive than Candidate 2.

Pseudorandom (PR): Our starting point is the pseudorandomness of random binary phase states. For a Boolean function $f: \{0, 1\}^\lambda \rightarrow \{0, 1\}$, consider the state

$$|\psi_f\rangle := 2^{-\lambda/2} \sum_{x \in \{0, 1\}^\lambda} (-1)^{f(x)} |x\rangle.$$

It is known that when f is chosen uniformly at random, $|\psi_f\rangle$ is statistically close to Haar-random states for any polynomial number of copies; more quantitatively, it forms an approximate t -design with error $4t^2/2^\lambda$ [BS19, Theorem 1.2]. Moreover, by combining this observation with the standard fact that $2t$ -wise independent functions fool all tests using at most t copies ([Zha12a, Fact 2]), one obtains the same approximate t -design guarantee when f is sampled from a $2t$ -wise independent family [BS19, Section 3.2].

Candidate 3 can be viewed as a restricted version of this construction: Instead of sampling a completely random Boolean function, we sample a sparse polynomial f_D and consider the IQP-type state

$$H^{\otimes \lambda} \cdot D \cdot H^{\otimes \lambda} |0^\lambda\rangle = H^{\otimes \lambda} \cdot 2^{-\lambda/2} \sum_x (-1)^{f_D(x)} |x\rangle.$$

The main question is whether the restricted family of sparse polynomials still has enough pseudorandomness to make the corresponding binary phase states computationally indistinguishable from Haar-random states.

There is, of course, a limitation when the degree is too small. In particular, if the degree d of f_D is constant, then the polynomial f_D can be learned from $O(\lambda^d)$ copies [ABDY23, Section 7.1 of the arXiv ver.]. This prevents pseudorandomness for constant d . However, to the best of our knowledge, this is the strongest known attack on such states. When $d = \omega(1)$, for example $d = \log^2 \lambda$, $\sqrt{\lambda}$, $\lambda/2$, or λ , the known learning attacks require super-polynomially many copies. We therefore conjecture that for sufficiently large super-constant d and appropriate polynomial sparsity w , the states generated by Candidate 3 are computationally indistinguishable from Haar-random states for any polynomial number of copies. This is precisely the intuition behind the PR property of our IQP-like QGA.

Haar-Pseudorandom (Haar-PR): We next discuss Haar-PR. Under our Definition 11, the Haar-PR experiment compares

$$\begin{aligned} \text{HaarPR}_0 &: \text{return } (|s\rangle, h|s\rangle)^{\otimes t}, \text{ where } |s\rangle \leftarrow \mu, h \leftarrow \text{SampG}(1^\lambda), \\ \text{HaarPR}_1 &: \text{return } (|s\rangle, |s'\rangle)^{\otimes t}, \text{ where } |s\rangle \leftarrow \mu, |s'\rangle \leftarrow \mu. \end{aligned}$$

The first component $|s\rangle$ is Haar-random and independent of h in both experiments. Hence the only nontrivial issue is whether $h|s\rangle$ is computationally indistinguishable from an independent Haar-random state. This is exactly the same pseudorandomness intuition as above. In other words, Haar-PR should be viewed here as a Haar-randomly padded version of PR. The extra Haar-random state does not reveal information about the sampled IQP circuit, and the security reduces heuristically to the pseudorandomness of the IQP-generated state $h|s\rangle$.

Consequently, we conjecture that Candidate 3 satisfies Haar-PR under the same parameter regime as PR, namely when the degree d is sufficiently large so that no efficient learner can recover useful information about f_D from polynomially many copies. We emphasize that this is a conjectural assumption rather than a theorem. Unlike the case of fully random or $2t$ -wise independent phase functions, sparse polynomial families do not currently come with an information-theoretic design guarantee. Our claim is that they provide a natural and structured candidate for computational pseudorandomness.

Haar-decisional Diffie-Hellman (Haar-DDH): Finally, we discuss Haar-DDH. Recall that the Haar-DDH experiment in Definition 13 compares

$$\begin{aligned} \text{HaarDDH}_0 &: \text{return } \{(|s_q\rangle, \tilde{g}|s_q\rangle)^{\otimes t}\}_{q \in [Q]}, \text{ where } \tilde{g} \leftarrow \text{SampG}(1^\lambda) \text{ and } |s_q\rangle \leftarrow \mu \text{ for } q \in [Q], \\ \text{HaarDDH}_1 &: \text{return } \{(|s_q\rangle, h_q|s_q\rangle)^{\otimes t}\}_{q \in [Q]}, \text{ where } |s_q\rangle \leftarrow \mu, h_q \leftarrow \text{SampG}(1^\lambda) \text{ for } q \in [Q]. \end{aligned}$$

The two experiments differ only in whether the same sampled IQP circuit is applied to all Haar-random input states or an independently sampled circuit is used for each input. For every fixed unitary g , Haar invariance implies that $g|s_q\rangle$ is Haar-random whenever $|s_q\rangle$ is Haar-random. Therefore, the marginal distribution of each output state ($\tilde{g}|s_q\rangle$ or $h_q|s_q\rangle$) is identical in the two experiments.

This observation alone does not establish Haar-DDH, since each pair $(|s_q\rangle, \tilde{g}|s_q\rangle)$ may contain $\tilde{g}$ -dependent correlations. Moreover, when the same $\tilde{g}$ is reused, such information may be correlated across different values. A Haar-DDH adversary should exploit these input–output correlations to determine whether the transformations are induced by one common sparse polynomial or by independently sampled polynomials.

The learning result of [ABDY23, Section 7.1 of the arXiv ver.] does not directly apply here, which learns the polynomial from copies of a binary-phase state generated from a fixed initial state, whereas Haar-DDH provides Haar-random input–output pairs. To the best of our knowledge, no efficient algorithm is known for detecting a common high-degree sparse polynomial from the latter type of samples.

We therefore conjecture that, for suitable super-constant degree d and polynomial sparsity w , the correlations caused by reusing one sampled IQP circuit are computationally hidden. We emphasize that this does not follow from PR or Haar-PR and should be regarded as a separate conjectural assumption.

6.4 Concurrent work by Bostanci et al. [BHHP25]:

Concurrently, Bostanci et al. [BHHP25] introduced Hamiltonian phase states (HPSs) and conjectured their one-wayness and pseudorandomness. Their assumptions can be viewed as the one-wayness and PR assumptions for a concrete instantiation of our IQP QGA in Candidate 2.

More precisely, their diagonal unitary is of the form

$$D_{A,\theta} = \exp \left(i \sum_{i=1}^m \theta_i \bigotimes_{j=1}^n Z^{A_{ij}} \right),$$

where $A \leftarrow \mathbb{F}_2^{m \times n}$ and angles $\theta_i \leftarrow \{2\pi k/q : k \in \{0, 1, \dots, q-1\}\}$ are sampled randomly. By instantiating **SampG** in Candidate 2 with this distribution, the sampled group element is $g_{A,\theta} = H^{\otimes \lambda} D_{A,\theta} H^{\otimes \lambda}$. Since **GenS** outputs $|0^\lambda\rangle$, the corresponding QGA state is $g_{A,\theta} |0^\lambda\rangle = H^{\otimes \lambda} D_{A,\theta} |+\rangle$, which is an HPS followed by the fixed unitary $H^{\otimes \lambda}$. Because this fixed unitary is efficiently invertible and preserves the Haar measure, it does not affect either one-wayness or pseudorandomness. Thus, the search and decision HPS assumptions closely correspond to the one-wayness and PR assumptions, respectively, for this instantiation of Candidate 2. (Candidate 3 is a further restricted instantiation of Candidate 2 based on binary phases determined by sparse polynomials; it is therefore different from the more general discretized phase distribution used for HPSs.)

The two works have complementary goals. Bostanci et al. study this specific IQP ensemble in detail and provide additional evidence for their assumptions, including random self-reducibility in certain parameter regimes. In contrast, our goal is to provide a generic group-action framework that separates the underlying group, state space, sampler, and hardness assumptions. Our framework also introduces action-level notions such as Haar-PR, Haar-DDH, and NR, which are not directly captured by the search and decision HPS assumptions.

Bostanci et al. also construct quantum trapdoor functions, which imply weakly secure public-key encryption with quantum public keys, from their assumptions. Their construction can also be instantiated from an IQP QGA satisfying the corresponding one-wayness

and pseudorandomness properties, by applying essentially the same construction. Conversely, our main focus is on deriving applications such as classical-query PRF-like state generators generically from QGA assumptions.

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. doi:[10.1145/1993636.1993682](https://doi.org/10.1145/1993636.1993682).
- [ABDY23] Srinivasan Arunachalam, Sergey Bravyi, Arkopal Dutt, and Theodore J. Yoder. Optimal algorithms for learning quantum phase states. In Omar Fawzi and Michael Walter, editors, *TQC 2023*, volume 266 of *LIPICs*, pages 3:1–3:24, Dagstuhl, Germany, 2023. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. doi:[10.4230/LIPICs.TQC.2023.3](https://doi.org/10.4230/LIPICs.TQC.2023.3).
- [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, Cham, August 2016. doi:[10.1007/978-3-319-49175-2_3](https://doi.org/10.1007/978-3-319-49175-2_3).
- [ABGL25] Prabhanjan Ananth, John Bostanci, Aditya Gulati, and Yao-Ting Lin. Pseudorandom unitaries in the haar random oracle model. In Yael Tauman Kalai and Seny F. Kamara, editors, *CRYPTO 2025, Part II*, volume 16001 of *LNCS*, pages 301–333. Springer, Cham, August 2025. doi:[10.1007/978-3-032-01878-6_10](https://doi.org/10.1007/978-3-032-01878-6_10).
- [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, Berlin, Heidelberg, August 2015. doi:[10.1007/978-3-662-47989-6_19](https://doi.org/10.1007/978-3-662-47989-6_19).
- [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, Cham, December 2020. doi:[10.1007/978-3-030-64834-3_14](https://doi.org/10.1007/978-3-030-64834-3_14).
- [AGKL24] Prabhanjan Ananth, Aditya Gulati, Fatih Kaleoglu, and Yao-Ting Lin. Pseudorandom isometries. In Marc Joye and Gregor Leander, editors, *EUROCRYPT 2024, Part IV*, volume 14654 of *LNCS*, pages 226–254. Springer, Cham, May 2024. doi:[10.1007/978-3-031-58737-5_9](https://doi.org/10.1007/978-3-031-58737-5_9).
- [AGL24] Prabhanjan Ananth, Aditya Gulati, and Yao-Ting Lin. Cryptography in the common Haar state model: Feasibility results and separations. In Elette Boyle and Mohammad Mahmoody, editors, *TCC 2024, Part II*, volume 15365 of *LNCS*, pages 94–125. Springer, Cham, December 2024. doi:[10.1007/978-3-031-78017-2_4](https://doi.org/10.1007/978-3-031-78017-2_4).
- [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, Cham, November 2022. doi:[10.1007/978-3-031-22318-1_9](https://doi.org/10.1007/978-3-031-22318-1_9).

- [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, Cham, August 2022. doi:[10.1007/978-3-031-15802-5_8](https://doi.org/10.1007/978-3-031-15802-5_8).
- [BBCK24] Benjamin Benčina, Alessandro Budroni, Jesús-Javier Chi-Domínguez, and Mukul Kulkarni. Properties of lattice isomorphism as a cryptographic group action. In Markku-Juhani Saariinen and Daniel Smith-Tone, editors, *Post-Quantum Cryptography - 15th International Workshop, PQCrypto 2024, Part I*, pages 170–201. Springer, Cham, June 2024. doi:[10.1007/978-3-031-62743-9_6](https://doi.org/10.1007/978-3-031-62743-9_6).
- [BCQ23] Zvika Brakerski, Ran Canetti, and Luowen Qian. On the computational hardness needed for quantum cryptography. *ITCS 2023*, 2023. doi:[10.4230/LIPIcs.ITCS.2023.24](https://doi.org/10.4230/LIPIcs.ITCS.2023.24).
- [BDJR97] Mihir Bellare, Anand Desai, Eric Joriki, and Phillip Rogaway. A concrete security treatment of symmetric encryption. In *38th FOCS*, pages 394–403. IEEE Computer Society Press, October 1997. doi:[10.1109/SFCS.1997.646128](https://doi.org/10.1109/SFCS.1997.646128).
- [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. doi:[10.1038/s41567-018-0318-2](https://doi.org/10.1038/s41567-018-0318-2).
- [BHH16] Fernando G. S. L. Brandão, Aram W. Harrow, and Michał Horodecki. Local random quantum circuits are approximate polynomial-designs. *Commun. Math. Phys.*, 346:397–434, 2016. doi:[10.1007/s00220-016-2706-8](https://doi.org/10.1007/s00220-016-2706-8).
- [BHHP25] John Bostanci, Jonas Haferkamp, Dominik Hangleiter, and Alexander Poremba. Efficient Quantum Pseudorandomness from Hamiltonian Phase States. In Bill Fefferman, editor, *TQC 2025*, volume 350 of *LIPIcs*, pages 9:1–9:18, Dagstuhl, Germany, 2025. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. doi:[10.4230/LIPIcs.TQC.2025.9](https://doi.org/10.4230/LIPIcs.TQC.2025.9).
- [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, Berlin, Heidelberg, August 2015. doi:[10.1007/978-3-662-48000-7_30](https://doi.org/10.1007/978-3-662-48000-7_30).
- [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. doi:[10.1098/rspa.2010.0301](https://doi.org/10.1098/rspa.2010.0301).
- [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, Cham, December 2020. doi:[10.1007/978-3-030-64834-3_18](https://doi.org/10.1007/978-3-030-64834-3_18).
- [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, Berlin, Heidelberg, August 1995. doi:[10.1007/3-540-44750-4_34](https://doi.org/10.1007/3-540-44750-4_34).

- [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. doi:[10.1145/1866307.1866323](https://doi.org/10.1145/1866307.1866323).
- [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. doi:[10.1103/PhysRevLett.117.080501](https://doi.org/10.1103/PhysRevLett.117.080501).
- [BS19] Zvika Brakerski and Omri Shmueli. (Pseudo) random quantum states with binary phase. In Dennis Hofheinz and Alon Rosen, editors, *TCC 2019, Part I*, volume 11891 of *LNCS*, pages 229–250. Springer, Cham, December 2019. doi:[10.1007/978-3-030-36030-6_10](https://doi.org/10.1007/978-3-030-36030-6_10).
- [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, Berlin, Heidelberg, August 1991. doi:[10.1007/3-540-38424-3_7](https://doi.org/10.1007/3-540-38424-3_7).
- [CCS25] Boyang Chen, Andrea Coladangelo, and Or Sattath. The power of a single haar random state: Constructing and separating quantum pseudorandomness. In Serge Fehr and Pierre-Alain Fouque, editors, *EUROCRYPT 2025, Part VII*, volume 15607 of *LNCS*, pages 108–137. Springer, Cham, May 2025. doi:[10.1007/978-3-031-91098-2_5](https://doi.org/10.1007/978-3-031-91098-2_5).
- [CGGH25] Bruno Pasqualotto Cavalar, Eli Goldin, Matthew Gray, and Peter Hall. A meta-complexity characterization of quantum cryptography. In Serge Fehr and Pierre-Alain Fouque, editors, *EUROCRYPT 2025, Part VII*, volume 15607 of *LNCS*, pages 82–107. Springer, Cham, May 2025. doi:[10.1007/978-3-031-91098-2_4](https://doi.org/10.1007/978-3-031-91098-2_4).
- [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, Cham, December 2018. doi:[10.1007/978-3-030-03332-3_15](https://doi.org/10.1007/978-3-030-03332-3_15).
- [Cou06] Jean-Marc Couveignes. Hard homogeneous spaces. Cryptology ePrint Archive, Paper 2006/291, 2006. URL: <https://eprint.iacr.org/2006/291>.
- [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. doi:[10.1016/j.ffa.2024.102476](https://doi.org/10.1016/j.ffa.2024.102476).
- [DH76] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976. doi:[10.1109/TIT.1976.1055638](https://doi.org/10.1109/TIT.1976.1055638).
- [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, Berlin, Heidelberg, August 2013. doi:[10.1007/978-3-642-40084-1_8](https://doi.org/10.1007/978-3-642-40084-1_8).

- [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. doi:[10.1103/PhysRevLett.120.200502](https://doi.org/10.1103/PhysRevLett.120.200502).
- [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. doi:[10.1109/SFCS.1984.715949](https://doi.org/10.1109/SFCS.1984.715949).
- [GGM86] Oded Goldreich, Shafi Goldwasser, and Silvio Micali. How to construct random functions. *Journal of the ACM*, 33(4):792–807, 1986. doi:[10.1145/6490.6503](https://doi.org/10.1145/6490.6503).
- [HM23] Aram W. Harrow and Saeed Mehraban. Approximate unitary t -designs by short random quantum circuits using nearest-neighbor and long-range gates. *Commun. Math. Phys.*, 401:1531–1626, 2023. doi:[10.1007/s00220-016-2706-8](https://doi.org/10.1007/s00220-016-2706-8).
- [HM25] Taiga Hiroka and Tomoyuki Morimae. Quantum cryptography and meta-complexity. In Yael Tauman Kalai and Seny F. Kamara, editors, *CRYPTO 2025, Part II*, volume 16001 of *LNCS*, pages 545–574. Springer, Cham, August 2025. doi:[10.1007/978-3-032-01878-6_18](https://doi.org/10.1007/978-3-032-01878-6_18).
- [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. doi:[10.1109/SFCS.1989.63483](https://doi.org/10.1109/SFCS.1989.63483).
- [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, Berlin, Heidelberg, November / December 2011. doi:[10.1007/978-3-642-25405-5_2](https://doi.org/10.1007/978-3-642-25405-5_2).
- [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, Cham, August 2018. doi:[10.1007/978-3-319-96878-0_5](https://doi.org/10.1007/978-3-319-96878-0_5).
- [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, Cham, December 2019. doi:[10.1007/978-3-030-36030-6_11](https://doi.org/10.1007/978-3-030-36030-6_11).
- [Kob87] Neal Koblitz. Elliptic curve cryptosystems. *Math. Comp.*, 48(177):203–209, 1987. doi:[10.2307/2007884](https://doi.org/10.2307/2007884).
- [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. doi:[10.1145/3564246.3585225](https://doi.org/10.1145/3564246.3585225).
- [Kre21] William Kretschmer. Quantum pseudorandomness and classical complexity. *TQC 2021*, 2021. doi:[10.4230/LIPICS.TQC.2021.2](https://doi.org/10.4230/LIPICS.TQC.2021.2).
- [KT24] Dakshita Khurana and Kabir Tomer. Commitments from quantum one-wayness. In Bojan Mohar, Igor Shinkar, and Ryan O’Donnell, editors, *56th ACM STOC*, pages 968–978. ACM Press, June 2024. doi:[10.1145/3618260.3649654](https://doi.org/10.1145/3618260.3649654).

- [KT25] Dakshita Khurana and Kabir Tomer. Founding quantum cryptography on quantum advantage, or, towards cryptography from $\#P$ hardness. In Michal Koucký and Nikhil Bansal, editors, *57th ACM STOC*, pages 178–188. ACM Press, June 2025. doi:10.1145/3717823.3718145.
- [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 ACM STOC*, pages 979–990. ACM Press, June 2024. doi:10.1145/3618260.3649650.
- [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. doi:10.1145/1653662.1653677.
- [MH25] Fermi Ma and Hsin-Yuan Huang. How to construct random unitaries. In Michal Koucký and Nikhil Bansal, editors, *57th ACM STOC*, pages 806–809. ACM Press, June 2025. doi:10.1145/3717823.3718254.
- [Mil86] Victor S. Miller. Use of elliptic curves in cryptography. In Hugh C. Williams, editor, *CRYPTO’85*, volume 218 of *LNCS*, pages 417–426. Springer, Berlin, Heidelberg, August 1986. doi:10.1007/3-540-39799-X_31.
- [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, Cham, December 2020. doi:10.1007/978-3-030-64834-3_19.
- [MPSY24] Tony Metger, Alexander Poremba, Makrand Sinha, and Henry Yuen. Simple constructions of linear-depth t -designs and pseudorandom unitaries. In *65th FOCS*, pages 485–492. IEEE Computer Society Press, October 2024. doi:10.1109/FOCS61266.2024.00038.
- [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, Cham, August 2022. doi:10.1007/978-3-031-15802-5_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>. doi:10.4230/LIPICs.TQC.2024.4.
- [MY24] Tomoyuki Morimae, Shogo Yamada, and Takashi Yamakawa. Quantum unpredictability. In Kai-Min Chung and Yu Sasaki, editors, *ASIACRYPT 2024, Part IX*, volume 15492 of *LNCS*, pages 3–32. Springer, Singapore, December 2024. doi:10.1007/978-981-96-0947-5_1.
- [MZ25] Saachi Mutreja and Mark Zhandry. Quantum state group actions. In Yael Tauman Kalai and Seny F. Kamara, editors, *CRYPTO 2025, Part II*, volume 16001 of *LNCS*, pages 449–480. Springer, Cham, August 2025. doi:10.1007/978-3-032-01878-6_15.
- [NR04] Moni Naor and Omer Reingold. Number-theoretic constructions of efficient pseudo-random functions. *Journal of the ACM*, 51(2):231–262, 2004. doi:10.1145/972639.972643.

- [SY17] Fang Song and Aaram Yun. Quantum security of NMAC and related constructions - PRF domain extension against quantum attacks. In Jonathan Katz and Hovav Shacham, editors, *CRYPTO 2017, Part II*, volume 10402 of *LNCS*, pages 283–309. Springer, Cham, August 2017. [doi:10.1007/978-3-319-63715-0_10](https://doi.org/10.1007/978-3-319-63715-0_10).
- [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. [doi:10.26421/QIC4.2-5](https://doi.org/10.26421/QIC4.2-5).
- [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, Cham, December 2022. [doi:10.1007/978-3-031-22972-5_22](https://doi.org/10.1007/978-3-031-22972-5_22).
- [Zha12a] Mark Zhandry. How to construct quantum random functions. In *53rd FOCS*, pages 679–687. IEEE Computer Society Press, October 2012. [doi:10.1109/FOCS.2012.37](https://doi.org/10.1109/FOCS.2012.37).
- [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, Berlin, Heidelberg, August 2012. [doi:10.1007/978-3-642-32009-5_44](https://doi.org/10.1007/978-3-642-32009-5_44).
- [Zha24] Mark Zhandry. Quantum money from Abelian group actions. In Venkatesan Guruswami, editor, *ITCS 2024*, volume 287 of *LIPICs*, pages 101:1–101:23, Dagstuhl, Germany, 2024. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. [doi:10.4230/LIPICs.ITCS.2024.101](https://doi.org/10.4230/LIPICs.ITCS.2024.101).
- [Zha25] Mark Zhandry. Quantum money from Abelian group actions. *TheoretCS*, 4, 2025. [doi:10.46298/theoretics.25.18](https://doi.org/10.46298/theoretics.25.18).

A Haar-PR and Haar-DDH imply SKE

Preliminaries. We first review the definitions of symmetric-key encryption (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 security²³ via a hybrid argument. It is also easy to show that left-or-right IND-CPA security implies find-then-guess IND-CPA securities²⁴ defined in [BJ15, ABF⁺16, MYY24] by following the proof in [BDJR97].

Definition 19 (Classical-Message Symmetric-Key Encryption (SKE)). A symmetric-key encryption (SKE) scheme for ℓ -bit classical messages consists of three algorithms (KeyGen, Enc, Dec) such that

- $\text{KeyGen}(1^\lambda) \rightarrow K$: This is a QPT algorithm that takes the security parameter 1^λ as input and outputs a *classical* secret key K .
- $\text{Enc}(K, b) \rightarrow \text{ct}$: This is a QPT algorithm that takes K and a message $b \in \{0, 1\}^\ell$ and outputs a *quantum* ciphertext ct .

²²An 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 .

²³An 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 .

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

- $\text{Dec}(K, \text{ct}) \rightarrow b'/\perp$: 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 $\perp$.

Definition 20 (IND-CPA-secure 1-bit SKE). We say that a SKE scheme $(\text{KeyGen}, \text{Enc}, \text{Dec})$ is *IND-CPA-secure 1-bit SKE* if it satisfies the following two properties:

- Correctness: We have

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

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

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

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

Definition 21 (IND-CPA-secure multi-bit SKE). We say that a SKE scheme $(\text{KeyGen}, \text{Enc}, \text{Dec})$ is *IND-CPA-secure multi-bit SKE* if it satisfies the following two properties:

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

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

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

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

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

Lemma 23. Suppose that there exists an IND-CPA-secure 1-bit SKE $(\text{KeyGen}, \text{Enc}, \text{Dec})$. Let $t = t(\lambda) = \omega(\log(\lambda))$ and $\ell = \ell(\lambda)$ be polynomials. We define the following new SKE scheme:

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

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

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. $\square$

Construction. Let (G, S) with $(\text{SampG}, \text{GenS})$ be an effective quantum group action, where S is a set of λ -qubits states. Let $\epsilon = \epsilon(\lambda)$ be some negligible function. We use ϵ -approximate quantum 1- or 2-designs, $\mathcal{S}_{\lambda,1,\epsilon}$ and $\mathcal{S}_{\lambda,2,\epsilon}$ in Lemma 4. By using those, we can construct a simple IND-CPA-secure 1-bit SKE from the HaarPR and Haar-DDH assumptions:

Theorem 5. *Let (G, S) with $(\text{SampG}, \text{GenS})$ be a Haar-pseudorandom (Haar-PR) and Haar-decisional Diffie-Hellman (Haar-DDH) QGA. Then, the following SKE is IND-CPA-secure 1-bit SKE.*

- $\text{KeyGen}(1^\lambda)$: Generate $g \leftarrow \text{SampG}(1^\lambda)$ and output $K := g$.
- $\text{Enc}(K, b)$: If $b = 0$, then prepare $|s\rangle^{\otimes 2}$ by using $\mathcal{S}_{\lambda,2,\epsilon}$ and output a ciphertext $\text{ct} := (|s\rangle, g|s\rangle)$. If $b = 1$, then generate $|s\rangle, |s'\rangle \leftarrow \mathcal{S}_{\lambda,1,\epsilon}$ by using a 1-design and output $\text{ct} := (|s\rangle, |s'\rangle)$.
- $\text{Dec}(K, \text{ct})$: Let $\text{ct} = (|\phi\rangle, |\psi\rangle)$. 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,

$$\Pr[\text{Dec}(K, \text{Enc}(K, 1)) = 0] \leq \mathbb{E}_{g \leftarrow \text{SampG}(1^\lambda), |s\rangle, |s'\rangle \leftarrow \mu} \left[\frac{1 + |\langle s' | g|s \rangle|^2}{2} \right] + \text{negl}(\lambda) \quad (28)$$

$$\leq \mathbb{E}_{|s\rangle, |s'\rangle \leftarrow \mu} \left[\frac{1 + |\langle s' | s \rangle|^2}{2} \right] + \text{negl}(\lambda) \quad (29)$$

$$\leq (1 + 1/2)/2 + \text{negl}(\lambda) \leq 4/5, \quad (30)$$

where we used

- Lemma 4 and the assumption that ϵ is negligible for Equation 28,
- the fact that, for any g , the distribution of $g|s\rangle \leftarrow \mu$ is equivalent to that of $|s\rangle \leftarrow \mu$ for Equation 29,
- and Lemma 5 for Equation 30.

$\square$

Proof of IND-CPA security. If the QGA is Haar-PR, then $\text{mHaarPR}_0 \approx_c \text{mHaarPR}_1$ holds in Lemma 11. Notice that $\text{mHaarPR}_0 = \text{HaarDDH}_1$ in Definition 13. Thus, if the underlying QGA is Haar-PR and Haar-DDH, then $\text{mHaarPR}_1 \approx_c \text{HaarDDH}_0$, where

mHaarPR_1 : return $\{|s_q\rangle, |s'_q\rangle\}_{q \in [Q]}^{\otimes t}$, where $|s_q\rangle, |s'_q\rangle \leftarrow \mu$ for $q \in [Q]$,

HaarDDH_0 : return $\{|s_q\rangle, g|s_q\rangle\}_{q \in [Q]}^{\otimes t}$, where $g \leftarrow \text{SampG}(1^\lambda)$ and $|s_q\rangle \leftarrow \mu$ for $q \in [Q]$.

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 mHaarPR_1 and 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 $g \leftarrow \text{SampG}(1^\lambda)$ or chosen from μ .
2. Run $\mathcal{A}$ and simulate the oracle as follows:
 - If the i -th query is 0, then return $\text{ct}_i := (|s_q\rangle, |s'_q\rangle)$.
 - If the i -th query is 1, then generate two independent samples $|\phi\rangle, |\psi\rangle$ by using 1-design and return $\text{ct}_i := (|\phi\rangle, |\psi\rangle)$.
3. Output $\mathcal{A}$'s decision.

If the input samples are chosen from HaarDDH_0 , then $\mathcal{B}$ statistically simulates the encryption oracle $\text{Enc}(K, \cdot)$, where $K = g \leftarrow \text{SampG}(1^\lambda)$, because of [Lemma 4](#). On the other hand, if the input samples are chosen from mHaarPR_1 , then $\mathcal{B}$ statistically simulates the encryption oracle $\text{Enc}(K, 1)$ because of [Lemma 4](#). Thus, $\mathcal{B}$'s advantage is statistically close to that of $\mathcal{A}$ against IND-CPA security. This completes the proof. $\square$

Since an IND-CPA-secure multi-bit SKE implies an IND-CPA-secure *quantum-message* SKE [[BJ15](#)] (and the formal proof in [[MY24](#), Appendix A of the ePrint version]), we have the following corollary.

Corollary 3. *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 Alapati et al. [[ADMP20](#)].

B.1 Preliminaries

We first review the definition and notions of group actions. For further details, see textbooks of abstract algebra or group theory.

Definition 22 (Group action). Let G be a group with an identity element 1_G and let S be a set. Let $\star: G \times S \rightarrow S$ 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 23 (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 $f_s: g \in G \mapsto g \star s \in S$. We also consider, for an element $g \in G$, a mapping $L_g: s \in S \mapsto g \star s \in S$. We note that, for any $s \in S$, if a group action is *transitive* (or *free*, resp.), then f_s is surjective (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 24. *Suppose that G is finite and a group action $(G, S, \star)$ is transitive. Then, for any $s_0 \in S$, the distribution of $g \star s_0$ with $g \leftarrow \$ G$ is the uniform distribution over S .*

Proof. Let $H := \{g \in G : g \star s_0 = s_0\}$ be the stabilizer of s_0 . Since the action is transitive, the map $\phi_{s_0}: g \mapsto g \star s_0$ is surjective. Moreover, for any $g_1, g_2 \in G$, $g_1 \star s_0 = g_2 \star s_0$ holds if and only if $g_2^{-1}g_1 \in H$. The latter holds if and only if $g_1H = g_2H$. Hence each element of S has exactly $|H|$ preimages under ϕ_{s_0} . Therefore, for every $s \in S$, $\Pr_g[g \star s_0 = s] = |H|/|G|$. This implies that $g \star s_0$ is uniformly distributed over S . $\square$

Since a group action is transitive if it is regular, we obtain the following corollary.

Corollary 4. *Suppose that G is finite and a group action $(G, S, \star)$ is regular, that is, transitive and free. 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 $g_i \leftarrow \$ G$.*

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

Definition 24 (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 .²⁵
 - (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 S 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.²⁶

²⁵We generalize this sampling algorithm as **SampG** in the definition of effective QGA.

²⁶We generalize this sampling algorithm as **SampS** in the definition of effective QGA.

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 25 (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 $Q = Q(\lambda)$,

$$\left\{ (s_i, \tilde{g} \star s_i)_{i \in [Q]} : \forall i \in [Q] \begin{array}{l} \tilde{g} \leftarrow_{\$} G, \\ s_i \leftarrow_{\$} S \end{array} \right\} \approx_c \{(s_i, s'_i)_{i \in [Q]} : s_i, s'_i \leftarrow_{\$} S\}.$$

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 $Q = Q(\lambda)$,

$$\left\{ (g_i \star s_0, (\tilde{g}g_i) \star s_0)_{i \in [Q]} : \forall i \in [Q] \begin{array}{l} \tilde{g} \leftarrow_{\$} G, \\ g_i \leftarrow_{\$} G \end{array} \right\} \approx_c \{(g_i \star s_0, h_i \star s_0)_{i \in [Q]} : g_i, h_i \leftarrow_{\$} G\}.$$

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

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

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

By adopting the proof for the NR-style PRFSG ([Theorem 3](#)), we obtain the following theorem for the NR-style PRF f :

Theorem 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 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 25](#)) shows that if G is commutative and the EGA is DDH, then it is NR. Combining the lemma with [Theorem 6](#), we obtain the following corollary.

Corollary 5. *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.*

This means that we can replace the two conditions of EGA, transitivity and faithfulness, to construct PRF with pseudorandomness of EGA. We additionally note that a GA is PR if it is transitive (Lemma 24). Thus, we can simply remove faithfulness from the original theorem.

Lemma 25. *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 H_i :

- For $j = 1, \dots, i$, $(a_j, b_j) := (g_j \star s_0, h_j \star s_0)$;
- For $j = i + 1, \dots, Q$, $(a_j, b_j) := (g_j \star s_0, (\tilde{g}g_j) \star s_0)$,
- Output $(a_j, b_j)_{j \in [Q]}$.

where $\tilde{g} \leftarrow \$ G$ and $g_j, h_j \leftarrow \$ G$ for $j \in [Q]$. By using the following claim, we have $H_0 \approx_c H_1 \approx_c \dots \approx_c H_Q$ if the DDH assumption holds. $\square$

Claim. *If $(G, S, \star)$ is an EGA, G is commutative, and the DDH assumptions hold, for $i = 1, \dots, Q$, $H_{i-1} \approx_c H_i$ holds.*

Proof. Suppose that there exists $\mathcal{A}$ distinguishing H_{i-1} from H_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 $j = 1, \dots, i-1$, 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 $j = i + 1, \dots, Q$, 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 H_{i-1} since G is a group and the distribution of h is random, then $\mathcal{B}$ perfectly simulates the distribution H_i . Thus, $\mathcal{B}$'s advantage is equivalent to $\mathcal{A}$'s advantage distinguishing H_{i-1} and H_i . $\square$

B.3 ADMP20 Proof

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

Theorem 8 ([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.²⁷ If the EGA is wPR, then the function f is a PRF.*

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 26 below). In addition, due to Lemma 24, if the EGA is transitive and wPR, then the EGA is NR (Lemma 27). Thus, we obtain the following corollary of Theorem 6.

Corollary 6. *Let $(G, S, \star)$ be an EGA.*

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

²⁷[ADMP20, Section 3.1 and Section 4.4]

- If it is transitive and wPR, then the function f is a PRF.

The two lemmas follow:

Lemma 26. *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

$$\begin{aligned} & \left\{ (s_i, \tilde{g} \star s_i)_{i \in [Q]} : \forall i \in [Q] \ s_i \leftarrow S, \tilde{g} \leftarrow G \right\} \\ & \approx_c \left\{ (g_i \star s_0, (\tilde{g}g_i) \star s_0)_{i \in [Q]} : \forall i \in [Q] \ g_i \leftarrow G, \tilde{g} \leftarrow G \right\}, \quad (31) \end{aligned}$$

$$\begin{aligned} & \{(s_i, h_i \star s_i)_{i \in [Q]} : \forall i \in [Q] \ h_i \leftarrow G, s_i \leftarrow S\} \\ & \approx_c \{(g_i \star s_0, (h_i g_i) \star s_0)_{i \in [Q]} : \forall i \in [Q] \ h_i, g_i \leftarrow G\}. \quad (32) \end{aligned}$$

We obtain that

$$\begin{aligned} & \left\{ (g_i \star s_0, (\tilde{g}g_i) \star s_0)_{i \in [Q]} : \forall i \in [Q] \ g_i \leftarrow G, \tilde{g} \leftarrow G \right\} \\ & \approx_c \left\{ (s_i, \tilde{g} \star s_i)_{i \in [Q]} : \forall i \in [Q] \ s_i \leftarrow S, \tilde{g} \leftarrow G \right\} && \text{(from Equation 31)} \\ & \approx_c \{(s_i, s'_i)_{i \in [Q]} : \forall i \in [Q] \ s_i, s'_i \leftarrow S\} && \text{(from wPR)} \\ & \approx_c \{(s_i, h_i \star s_i)_{i \in [Q]} : \forall i \in [Q] \ h_i \leftarrow G, s_i \leftarrow S\} && \text{(from wPR)} \\ & \approx_c \{(g_i \star s_0, (h_i g_i) \star s_0)_{i \in [Q]} : \forall i \in [Q] \ h_i, g_i \leftarrow G\} && \text{(from Equation 32)} \\ & \equiv \{(g_i \star s_0, h_i \star s_0)_{i \in [Q]} : \forall i \in [Q] \ h_i, g_i \leftarrow G\} && (G \text{ is a group}), \end{aligned}$$

where we apply wPR Q -times to obtain third computational indistinguishability. $\square$

Recall that if an EGA is transitive, then it is perfectly PR (Lemma 24). Thus, we obtain the following lemma.

Lemma 27. *Let $(G, S, \star)$ be an EGA. If the EGA is transitive and wPR, then it is NR.*