Pseudorandom Isometries

Prabhanjan Ananth[1], Aditya Gulati[1], Fatih Kaleoglu[1], and Yao-Ting Lin[1]

UCSB, USA
prabhanjan@cs.ucsb.edu, adityagulati@ucsb.edu, kaleoglu@ucsb.edu, yao-ting_lin@ucsb.edu

Abstract. We introduce a new notion called $\mathcal{Q}$-secure pseudorandom isometries (PRI). A pseudorandom isometry is an efficient quantum circuit that maps an n-qubit state to an $(n+m)$-qubit state in an isometric manner. In terms of security, we require that the output of a q-fold PRI on ρ, for $\rho \in \mathcal{Q}$, for any polynomial q, should be computationally indistinguishable from the output of a q-fold Haar isometry on ρ.
By fine-tuning $\mathcal{Q}$, we recover many existing notions of pseudorandomness. We present a construction of PRIs and assuming post-quantum one-way functions, we prove the security of $\mathcal{Q}$-secure pseudorandom isometries (PRI) for different interesting settings of $\mathcal{Q}$.
We also demonstrate many cryptographic applications of PRIs, including, length extension theorems for quantum pseudorandomness notions, message authentication schemes for quantum states, multi-copy secure public and private encryption schemes, and succinct quantum commitments.

1 Introduction

Pseudorandomness has played an important role in theoretical computer science. In classical cryptography, the notions of pseudorandom generators and functions have been foundational, with applications to traditional and advanced encryption schemes, signatures, secure computation, secret sharing schemes, and proof systems. On the other hand, we have only just begun to scratch the surface of understanding the implications pseudorandomness holds for quantum cryptography, and there is still a vast uncharted territory waiting to be explored.
When defining pseudorandomness in the quantum world, there are two broad directions one can consider.

Quantum States. Firstly, we can study pseudorandomness in the context of quantum states. Ji, Liu, and Song (JLS) [JLS18] proposed the notion of a pseudorandom quantum state generator, which is an efficient quantum circuit that on input a secret key k produces a quantum state (referred to as a pseudorandom quantum state) that is computationally indistinguishable from a Haar state as long as k is picked uniformly at random and moreover, the distinguisher is given many copies of the state. JLS and the followup works by Brakerski and Shmueli [BS19, BS20b] presented constructions of pseudorandom quantum state generators from

one-way functions. Ananth, Qian, and Yuen [AQY22] defined the notion of a pseudorandom function-like quantum state generator, which is similar to pseudorandom quantum state generators, except that the same key can be used to generate multiple pseudorandom quantum states. These two notions have many applications, including in quantum gravity theory [BFV20, ABF+23], quantum machine learning [HBC+22], quantum complexity [Kre21], and quantum cryptography [AQY22, MY22]. Other notions of pseudorandomness for quantum states have also been recently explored [ABF+23, ABK+23, GLG+23].

Quantum Operations. Secondly, we can consider pseudorandomness in the context of quantum operations. This direction is relatively less explored. One prominent example, proposed in the same work of [JLS18], is the notion of pseudorandom unitaries, which are efficient quantum circuits such that any efficient distinguisher should not be able to distinguish whether they are given oracle access to a pseudorandom unitary or a Haar unitary. Establishing the feasibility of pseudorandom unitaries could have ramifications for quantum gravity theory (as noted under open problems in [GLG+23]), quantum complexity theory [Kre21], and cryptography [GJMZ23]. Unfortunately, to date, we do not have any provably secure construction of pseudorandom unitaries, although some candidates have been proposed in [JLS18]. A recent independent work by by Lu, Qin, Song, Yao, and Zhao [LQS+23] takes an important step towards formulating and investigating the feasibility of pseudorandomness of quantum operations. They define a notion called pseudorandom state scramblers that isometrically maps a quantum state $|\psi\rangle$ into another state $|\psi'\rangle$ such that t copies of $|\psi'\rangle$, where t is a polynomial, is computationally indistinguishable from t copies of a Haar state. They establish its feasibility based on post-quantum one-way functions. In the same work, they also explored cryptographic applications of pseudorandom state scramblers.

Although pseudorandom state scramblers can be instantiated from one-way functions, the definition inherently allows for scrambling only a single state. On the other extreme, pseudorandom unitaries allow for scrambling polynomially many states but unfortunately, establishing their feasibility remains an important open problem. Thus, we pose the following question:

Is there a pseudorandomness notion that can scramble polynomially many states and can be provably instantiated based on well studied cryptographic assumptions?

Our Work in a Nutshell. We address the above question in this work. Our contribution is three-fold:

1. New definitions: We introduce a new notion called $\mathcal{Q}$-secure pseudorandom isometries that can be leveraged to scramble many quantum states coming from the set $\mathcal{Q}$.
2. Construction: We present a construction of pseudorandom isometries and investigate its security for different settings of $\mathcal{Q}$.

3. Applications: Finally, we explore many cryptographic applications of pseudorandom isometries.

1.1 Our Results

Roughly speaking, a pseudorandom isometry is an efficient quantum circuit, denoted by PRI_k, parameterized by a key[1] $k \in \{0,1\}^\lambda$ that takes as input an n-qubit state and outputs an $(n+m)$-qubit state with the guarantee that PRI_k is functionally equivalent to an isometry. In terms of security, we require that any efficient distinguisher should not be able to distinguish whether they are given oracle access to PRI_k or a Haar isometry[2] $\mathcal{I}$. We consider a more fine-grained version of this definition in this work, where we could fine-tune the set of allowable queries.

More precisely, we introduce a concept called $(n, n+m)$-$\mathcal{Q}$-*secure- pseudorandom isometries* (PRIs). Let us first consider a simplified version of this definition. Suppose $n(\lambda), q(\lambda)$ are polynomials and $\mathcal{Q}_{n,q,\lambda}$ is a subset of nq-qubit (mixed) states. Let $\mathcal{Q} = \{\mathcal{Q}_{n,q,\lambda}\}_{\lambda\in\mathbb{N}}$. The definition states that it should be computationally infeasible to distinguish the following two distributions: for any polynomials q,

- $\left(\rho,\ \mathsf{PRI}_k^{\otimes q}(\rho)\right)$,
- $\left(\rho,\ \mathcal{I}^{\otimes q}(\rho)\,(\mathcal{I}^\dagger)^{\otimes q}\right)$,

where $\rho \in \mathcal{Q}_{n,q,\lambda}$ and $\mathcal{I}$ is a Haar isometry.

Let us consider some examples.

1. If $\mathcal{Q}_{n,q,\lambda} = \{|0^n\rangle^{\otimes q}\}$ then this notion implies a pseudorandom state generator (PRSG) [JLS18].
2. If $\mathcal{Q}_{n,q,\lambda}$ consists of all possible q computational basis states then this notion implies a pseudorandom function-like state generator (PRFSG) [AQY22, AGQY22].
3. If $\mathcal{Q}_{n,q,\lambda}$ consists of q-fold tensor of all possible n-qubit states then this notion implies a pseudorandom state scrambler (PSS) [LQS+23].

We can generalize this definition even further. Specifically, we allow the adversary to hold an auxiliary register that is entangled with the register on which the q-fold isometry (PRI_k or Haar) is applied and we could require the stronger security property that the above indistinguishability should hold even in this setting.

In more detail, ρ is now an $(nq+\ell)$-qubit state and the distinguisher is given either of the following:

- $\left(\rho, \left(I_\ell \otimes \mathsf{PRI}_k^{\otimes q}\right)(\rho)\right)$,
- $\left(\rho, \left(I_\ell \otimes \mathcal{I}_k^{\otimes q}\right)\rho\left(I_\ell \otimes \mathcal{I}_k^{\dagger\otimes q}\right)\right)$

where I_ℓ is an ℓ-qubit identity operator. We can correspondingly define $\mathcal{Q}$ to be instead parameterized by n, q, ℓ, λ, and we require $\rho \in \mathcal{Q}_{n,q,\ell,\lambda}$.

The above generalization captures the notion of pseudorandom isometries (discussed in the beginning of Section 1.1) against selective queries.

[1] We denote λ to be the security parameter.

[2] The Haar distribution of isometries is defined as follows: first, sample a unitary from the Haar measure, and then set the isometry, that on input a quantum state $|\psi\rangle$, first initializes an ancilla register containing zeroes and then applies the Haar unitary on $|\psi\rangle$ and the ancilla register.

Specifically, if PRI_k is a $\mathcal{Q}$-secure pseudorandom isometry (according to the above-generalized definition), where $\mathcal{Q}$ is the set of all possible $nq+\ell$-qubit states then indeed it is infeasible for an efficient distinguisher making selective queries[3] to distinguish whether it has oracle access to PRI_k or a Haar isometry oracle.
Thus, by fine-tuning $\mathcal{Q}$, we recover many notions of pseudorandomness in the context of both quantum states and operations.

Construction. We first study the feasibility of PRIs.
We present a construction of PRIs and investigate its security for different settings of $\mathcal{Q}$. On input an n-qubit state $|\psi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x |x\rangle$, define $\mathsf{PRI}_k |\psi\rangle$ as follows:

$$\mathsf{PRI}_k |\psi\rangle = \frac{1}{\sqrt{2^m}} \sum_{x\in\{0,1\}^n, y\in\{0,1\}^m} \alpha_x \cdot \omega_p^{f_{k_1}(x||y)} |g_{k_2}(x||y)\rangle$$

In the above construction, we parse k as a concatenation of two λ_1-bit strings k_1 and k_2, where $\lambda = 2\lambda_1$. The first key k_1 would serve as a key for a pseudorandom function $f : \{0,1\}^{\lambda_1} \times \{0,1\}^{n+m} \to \mathbb{Z}_p$, where $p \sim 2^{\lambda_1}$ is an integer. The second key k_2 would serve as a key for a pseudorandom permutation $g : \{0,1\}^{\lambda_1} \times \{0,1\}^{n+m} \to \{0,1\}^{n+m}$. Both f and g should satisfy quantum query security. Moreover, both of them can be instantiated from post-quantum one-way functions [Zha12, Zha16]. We require n to be a polynomial in λ, larger than λ, and similarly, we set m to be a polynomial in λ, larger than λ.
The above construction was first studied by [BBSS23, ABF+23], perhaps surprisingly, in completely different contexts. Brakerski, Behera, Sattath, and Shmueli [BBSS23] introduced a new notion of PRSG and PRFSG and instantiated these two notions using the above construction. Aaronson, Bouland, Fefferman, Ghosh, Vazirani, Zhang, and Zhou [ABF+23] introduced the notion of pseudo-entanglement and instantiated this notion using the above construction. An important property of this construction is that it is *invertible*, that is, given the key k, it is efficient to implement Inv_k such that $\mathsf{Inv}_k\mathsf{PRI}_k$ is the identity map.
It is natural to wonder if it is possible to modify the above construction to have binary phase as against p^{th} roots of unity, for a large p. There is some recent evidence to believe since [HBK23] showed that pseudorandom unitaries cannot just have real entries.

Security. We look at different possible settings of $\mathcal{Q}$ and study their security[4].

I. Haar states. Our main contribution is showing that the output of PRI_k on many copies of many n-qubit Haar states, namely, $(|\psi_1\rangle^{\otimes t}, \ldots,$

[3] Roughly speaking, the selective query setting is one where all the queries are made at the same time. In contrast, in the adaptive query setting, each query could depend on the previous queries and answers.

[4] We only consider a simplified version of these settings here and in the technical sections, we consider the most general version.

$|\psi_s\rangle^{\otimes t}$) with t being a polynomial and $|\psi_1\rangle, \ldots, |\psi_s\rangle$ are Haar states, is computationally indistinguishable from a Haar isometry on ($|\psi_1\rangle^{\otimes t}, \ldots,$ $|\psi_s\rangle^{\otimes t}$). Moreover, the computational indistinguishability should hold even if ($|\psi_1\rangle^{\otimes t}, \ldots, |\psi_s\rangle^{\otimes t}$) is given to the QPT adversary. In other words, PRI_k can be used to map maximally mixed states on smaller dimensional symmetric subspaces onto pseudorandom states on larger dimensional symmetric subspaces. We consider the following setting:

- Let $t(\lambda)$ and $s(\lambda)$ be two polynomials. Let $q = s \cdot t$ and $\ell = n \cdot q$.
- We define $\mathcal{Q}_{\mathsf{Haar}} = \{\mathcal{Q}_{n,q,\ell,\lambda}\}_{\lambda\in\mathbb{N}}$, where $\mathcal{Q}_{n,q,\ell,\lambda}$ is defined as follows[5]:

$$\mathcal{Q}_{n,q,\ell,\lambda} = \left\{ \mathbb{E}_{|\psi_1\rangle,\ldots,|\psi_s\rangle\leftarrow\mathscr{H}_n} \left[\bigotimes_{i=1}^{s} |\psi_i\rangle\langle\psi_i|^{\otimes t} \otimes \bigotimes_{i=1}^{s} |\psi_i\rangle\langle\psi_i|^{\otimes t} \right] \right\}$$

  Recall that the first ℓ qubits (in the above case, it is the first t red-colored copies of n-qubit Haar states $|\psi_1\rangle, \ldots, |\psi_s\rangle$) are not touched. On the next q n-qubit states (colored in blue), either $\mathsf{PRI}_k^{\otimes q}$ or $\mathcal{I}^{\otimes q}$ is applied.

We prove the following.

Theorem 1 (Informal). *Assuming post-quantum one-way functions exist,* PRI_k *is a* $\mathcal{Q}_{\mathsf{Haar}}$*-secure pseudorandom isometry.*

This setting is reminiscent of the *weak* pseudorandom functions [DN02, ABG+14] studied in the classical cryptography literature, where we require the pseudorandomness to hold only on inputs chosen from the uniform distribution on binary strings.

Application: Length Extension Theorem. As an application, we demonstrate a length extension theorem for PRSGs and PRFSGs. Specifically, we show how to extend the output length of both these pseudorandomness notions assuming PRIs secure against Haar queries[6]. Specifically, we show the following.

Theorem 2 (Length Extension Theorem; Informal). *Assuming* $\mathcal{Q}_{\mathsf{Haar}}$*-secure pseudorandom isometry, mapping* n *qubits to* $n+m$ *qubits, and an* n*-qubit* PRSG*, there exists an* $n+m$*-qubit* PRSG*.*
Similarly, assuming a $\mathcal{Q}_{\mathsf{Haar}}$*-secure pseudorandom isometry, mapping* n *qubits to* $n+m$ *qubits, and* n*-qubit* PRFSG*, there exists an* $(n+m)$*-qubit* PRFSG*.*

Prior to our work, the only known length extension theorem was by Gunn, Ju, Ma, and Zhandry [GJMZ23] who demonstrated a method to increase the output length of pseudorandom states and pseudorandom unitaries but at the cost of reducing the number of copies given to the adversary. That is, the resulting PRSG in their transformation is only

[5] $\mathscr{H}_n$ denotes the Haar distribution on n-qubit Haar states.

[6] An $(n, n+m)$-pseudorandom isometry secure against any $\mathcal{Q}$ trivially gives a PRSG or PRFSG on $n+m$ qubits. However, our length extension theorem requires the underlying PRI to only be secure against Haar queries.

secure if the adversary is given one copy. On the other hand, in the above theorem, the number of copies of the PRSG is preserved in the above transformation.

II. Many copies of an n-qubit state. We also consider the setting where we have multiple copies of a single state. Specifically, we consider the following setting:

- Let $q = q(\lambda)$ be a polynomial. Let $\ell = n \cdot q$.
- We define $\mathcal{Q}_{\mathsf{Single}} = \{\mathcal{Q}_{n,q,\ell,\lambda}\}_{\lambda\in\mathbb{N}}$, where $\mathcal{Q}_{n,q,\ell,\lambda}$ is defined as follows:

$$\mathcal{Q}_{n,q,\ell,\lambda} = \left\{ |\psi\rangle^{\otimes q} \otimes |\psi\rangle^{\otimes q} \ : \ |\psi\rangle \in \mathcal{S}(\mathbb{C}^{2^n}) \right\}$$

We prove the following.

Theorem 3 (Informal). *Assuming post-quantum one-way functions exist,* PRI_k *is a* $\mathcal{Q}_{\mathsf{Single}}$*-secure pseudorandom isometry.*

Informally, the above theorem ensures that even if an efficient distinguisher is given polynomially many copies of $|\psi\rangle$, for an arbitrary n-qubit state $|\psi\rangle$, it should not be able to efficiently distinguish q copies of $\mathsf{PRI}_k |\psi\rangle$ versus q copies of $\mathcal{I} |\psi\rangle$, for any polynomial $q(\lambda)$.

Application: Pseudorandom State Scramblers.
A recent work [LQS+23] shows how to isometrically scramble a state such that many copies of the scrambled state should be computationally indistinguishable from many copies of a Haar state. Our notion of $\mathcal{Q}_{\mathsf{Single}}$-secure pseudorandom isometry is equivalent to pseudorandom state scramblers. Thus, we have the following.

Theorem 4 (Informal). $\mathcal{Q}_{\mathsf{Single}}$*-secure pseudorandom isometry exists if and only if pseudorandom state scramblers exist.*

The work of [LQS+23] presents an instantiation of pseudorandom scramblers from post-quantum one-way functions. While our result does not give anything new for pseudorandom scramblers in terms of assumptions, we argue that our construction and analysis are (in our eyes) much simpler than [LQS+23]. In addition to pseudorandom permutations and functions, they also use rotation unitaries in the construction. Their analysis also relies on novel and sophistical tools such as Kac random walks whereas our analysis is more elementary.

Application: Multi-Copy Secure Public-Key Encryption.
There is a simple technique to encrypt a quantum state, say $|\psi\rangle$: apply a quantum one-time pad on $|\psi\rangle$ and then encrypt the one-time pad keys using a post-quantum encryption scheme. However, the disadvantage of this construction is that the security is not guaranteed to hold if the adversary receives many copies of the ciphertext state. A natural idea is to apply a unitary t-design on $|\psi\rangle$ rather than a quantum one-time pad but this again only guarantees security if the adversary receives at most t queries. On the other hand, we formalize a security notion called multi-copy secure public-key and private-key encryption schemes, where the security should hold even if the adversary receives arbitrary polynomially many copies of the ciphertext.

Theorem 5 (Informal). *Assuming $\mathcal{Q}_{\mathsf{Single}}$-secure pseudorandom isometry*[7]*, there exists multi-copy secure private-key and public-key encryption schemes.*

The investigation of multi-copy security was independently conducted by [LQS+23]. However, they only studied multi-copy security in the context of one-time encryption schemes whereas we introduce the definition of multi-copy security for private-key and public-key encryption schemes and establish their feasibility for the first time.

Conjecture. Unfortunately, we currently do not know how to prove that PRI_k is a $\mathcal{Q}$-secure pseudorandom isometry for every $\mathcal{Q}$. We leave the investigation of this question as an interesting open problem.

Conjecture 1. For every $\mathcal{Q} = \{\mathcal{Q}_{n,q,\ell,\lambda}\}_{\lambda\in\mathbb{N}}$, where $\mathcal{Q}_{n,q,\ell,\lambda}$ consists of nq-qubit states, PRI_k is a $\mathcal{Q}$-secure pseudorandom isometry.

Other Applications. We explore other applications of PRIs that were not covered before.

Application: Quantum MACs. We explore novel notions of message authentication codes (MAC) for quantum states. Roughly speaking, in a MAC for quantum states, there is a signing algorithm using a signing key sk that on input a state, say $|\psi\rangle$, outputs a tag that can be verified using the same signing key sk. Intuitively, we require that any adversary who receives tags on message states of their choice should not be able to produce a tag on a challenge message state. For the notion to be meaningful, we require that the challenge message state should be orthogonal (or small fidelity) to all the message states seen so far.
There are different settings we consider:

- In the first setting, the verification algorithm gets as input multiple copies of the message state $|\psi\rangle$ and the tag state. In this case, we require the probability that the adversary should succeed is negligible.
- In the second setting, the verification algorithm gets as input many copies of the message state but only a single copy of the tag. In this case, we weaken the security by only requiring that the adversary should only be able to succeed with inverse polynomial probability.
- Finally, we consider the setting where we restrict the type of message states that can be signed. Specifically, we impose the condition that for every message state $|\psi\rangle$, there is a circuit C that on input an all-zero state outputs $|\psi\rangle$. Moreover this circuit C is known to the verification algorithm. In this case, we require that the adversary only be able to succeed with negligible probability.

We show how to achieve all of the above three settings using PRIs.

Application: Length Extension Theorem. Previously, we explored a length extension theorem where we showed how to generically increase

[7] We additionally require that the pseudorandom isometry satisfy an invertibility condition. We define this more formally in the technical sections.

the output length of pseudorandom (function-like) state generators assuming only PRIs secure against Haar queries. We explore a qualitatively different method to extend the output length of pseudorandom states. Specifically, we show the following.

Theorem 6 (Informal). *Assuming the existence of $(n, n+m)$-secure pseudorandom isometry and an $(2n)$-output PRSG secure against $o(m)$ queries, there exists a $(2n+m)$-output PRSG secure against the same number of queries. Moreover, the key of the resulting PRSG is a concatenation of the $(2n)$-output PRSG and the $(n, n+m)$-secure PRI.*

One might be tempted to conclude that a unitary $o(m)$-design can be used to get the above result. The main issue with using a $o(m)$-design is that it increases the key size significantly [BCH+21]. However, in the above theorem, if we start with a PRI with short keys (i.e., $\lambda \ll m$) then the above transformation gets a PRSG with a much larger stretch without increasing the key size by much. [8]

1.2 Technical Overview

Haar Unitaries: Observations Before we talk about proving security of our construction, we point out some useful properties of Haar unitaries. Note that Haar isometries are closely related to Haar unitaries since the former can be implemented by appending suitably many zeroes[9] followed by a Haar random unitary.

Behavior on Orthogonal Inputs. In the classical world, a random function f with polynomial output length is indistinguishable from the corresponding random permutation g against a query-bounded black-box adversary $\mathcal{A}$. One can prove this fact in three simple steps:

1. Without loss of generality one can assume $\mathcal{A}$ only makes distinct queries $\{x_1, \ldots, x_q\}$.
2. f is perfectly indistinguishable from g conditioned on the fact that $f(x_i) \neq f(x_j)$ for $i \neq j$.
3. If the number q is polynomial, then the probability that f has a collision on $\{x_1, \ldots, x_q\}$ is negligible.

Now consider the quantum analogue of the same problem. Namely, consider two oracles O_1, O_2 that can only be queried on classical inputs, where: (1) O_1 on input x outputs $\mathcal{U}|x\rangle$, where $\mathcal{U}$ is a Haar unitary; and (2) O_2 for each distinct input x, outputs an i.i.d. Haar-random state $|\psi_x\rangle$. Our goal is to show that O_1, O_2 are indistinguishable against a query-bounded quantum adversary $\mathcal{A}$. If we try to replicate the classical proof above, we run into problems: we can no longer assume distinct queries due to the principle of no-cloning, and we need to generalize step 3 in a non-trivial to an almost-orthogonality argument. Instead, we consider an alternative proof for the classical case.

Fix the set of queries $\{x_1, \ldots, x_q\}$ and for $0 \leq i \leq q$ define a hybrid oracle O_i as follows:

[8] The proofs can be found in the full version https://eprint.iacr.org/2023/1741.

[9] The state being appended and the position of the new qubits is not important.

- For $1 \leq j \leq q$, if $x_j \in \{x_1, \ldots, x_{q-1}\}$, then output consistently as the previous instance of the same query.
- Otherwise, for $1 \leq j \leq i$: On input x_j, sample $y_j \notin \{y_1, \ldots, y_{j-1}\}$ uniformly at random and output y_j. For $i+1 \leq j \leq q$, sample an i.i.d. random answer y_j and output y_j.

Now, one can argue that O_i is perfectly indistinguishable from O_{i+1} conditioned on the answer y_{i+1} sampled by O_i satisfying $y_{i+1} \notin \{y_1, \ldots, y_i\}$. It turns out this argument is more easily generalizable to the quantum case, where we can define oracle $\widetilde{O}_i$ as answering $x_1, \ldots, x_i$ using a random isometry and answering $x_{i+1}, \ldots, x_q$ using i.i.d. Haar-random states (while maintaining consistency). Indistinguishability of $\widetilde{O}_i$ and $\widetilde{O}_{i+1}$ follows from an analysis comparing the dimensions of the subspaces the hybrid oracles sample outputs from.

Almost-Invariance Property. The security definition for a pseudorandom unitary, and similarly isometry, can be cumbersome to work with. Let us focus on the information-theoretic setting first, i.e. when there is no computational assumption on the adversary besides a query bound. We investigate what it means for a candidate pseudorandom unitary F_k to be information theoretically indistinguishable from a Haar unitary $\mathcal{U}$ for different query sets $\mathcal{Q}$; in other words, we consider *statistical $\mathcal{Q}$-security* of F_k. Rather than attempting to directly calculate the trace distance between the output of F_k on a given query ρ and the output of a Haar unitary $\mathcal{U}$ on the same input, which may look significantly different for different values of ρ, we are naturally drawn to look for a simpler condition that suffices for security.

Accordingly, we show that F_k is statistically $\mathcal{Q}$-secure if and only if for every $\rho \in \mathcal{Q}$ which describes q queries to F_k, we have that $F_k^{\otimes q} \rho (F_k^\dagger)^{\otimes q}$ changes only negligibly (in trace distance) under the action of q-fold Haar unitary $\mathcal{U}^{\otimes q}(\cdot)(\mathcal{U}^\dagger)^{\otimes q}$. We prove this fact for any quantum channel Φ (in particular for $\Phi(\cdot) = F_k(\cdot)F_k^\dagger$) as long as Φ is a mixture of unitary maps, and the proof follows by the unitary invariance of the Haar measure.

We note that the argument above can be easily generalized to a pseudorandom isometry (PRI), since an isometry can be decomposed into appending zeroes followed by applying a unitary.

Next, we will describe our construction, then discuss its security and applications in more detail.

Construction We describe how to naturally arrive at our construction of pseudorandom isometry, which was recently studied by [BBSS23, ABF+23] in different contexts. Given an input state $|\psi\rangle = \sum \alpha_x |x\rangle$, we will first apply an isometry $\widetilde{I}$ to get a state $|\varphi\rangle = \sum \theta_z |z\rangle$, followed by unitary operations. A commonly used technique to scramble a given input state $|\varphi\rangle$ is to apply a random binary function f with a phase kickback [JLS18], i.e. apply the unitary $O_f |\psi\rangle = \sum (-1)^{f(z)} \theta_z |z\rangle$. The action of O_f on a mixed state q-query input $\rho = \sum_{\vec{z},\vec{z}'} \beta_{\vec{z},\vec{z}'} |\vec{z}\rangle \langle \vec{z}'|$ can

be calculated as

$$\mathop{\mathbb{E}}_{f}\left[O_f^{\otimes q}\rho(O_f^\dagger)^{\otimes q}\right] = \mathop{\mathbb{E}}_{f}\left[\sum_{\vec{z},\vec{z}'}(-1)^{\sum_i f(z_i)+f(z_i')}\beta_{\vec{z},\vec{z}'}\left|\vec{z}\right\rangle\left\langle\vec{z}'\right|\right]$$
$$= \sum_{\vec{z},\vec{z}'}\beta_{\vec{z},\vec{z}'}\left|\vec{z}\right\rangle\left\langle\vec{z}'\right|\mathop{\mathbb{E}}_{f}\left[(-1)^{\sum_i f(z_i)+f(z_i')}\right].$$

Observe that if $\vec{z}$ and $\vec{z}'$ are related by a permutation[10], then $(-1)^{\sum_i f(z_i)+f(z_i')} = 1$. Otherwise, if there exists z, which occurs odd number of times in $\vec{z}$ and even number of times in $\vec{z}'$ (or vice versa), we get $(-1)^{\sum_i f(z_i)+f(z_i')} = 0$. Ideally we would like all terms $\left|\vec{z}\right\rangle\left\langle\vec{z}'\right|$ to vanish when $\vec{z}$ and $\vec{z}'$ are not related by a permutation. We can easily fix this by switching to p-th root of unity phase kickback, i.e. apply $\widetilde{O}_f$ for a random function f with codomain $\mathbb{Z}_p$, where $\widetilde{O}_f\left|\psi\right\rangle = \sum_x \omega_p^{f(x)}\left|x\right\rangle$ and $\omega_p = e^{2\pi i/p}$. As long as $q \ll p$ (e.g. q is polynomial and p is super-polynomial), we get that

$$\mathop{\mathbb{E}}_{f}\left[\widetilde{O}_f^{\otimes q}\rho(\widetilde{O}_f^\dagger)^{\otimes q}\right] = \sum_{\substack{\vec{z},\vec{z}' \\ \exists\sigma:\ \vec{z}'=\sigma(\vec{z})}}\beta_{\vec{z},\vec{z}'}\left|\vec{z}\right\rangle\left\langle\vec{z}'\right|.$$

Now we would like to scramble the remaining terms $\left|\vec{z}\right\rangle\left\langle\vec{z}'\right|$ in the equation above. A natural try is to apply a random permutation π in the computational basis, denoted by O_π as a unitary operation. Such an operation would scramble the term above as $O_\pi^{\otimes q}\left|\vec{z}\right\rangle\left\langle\vec{z}'\right|(O_\pi^\dagger)^{\otimes q}$, which only depends on σ as long as $\vec{z}$ has distinct entries. Hence, to achieve maximal scrambling we would like $\left|\varphi\right\rangle$ to have negligible weight on states $\left|\vec{z}\right\rangle$ with collisions of the form $z_i = z_j$.
In order to make sure that the weight on $\left|\vec{z}\right\rangle$ with distinct entries is close to 1, we pick $\widetilde{I}$ to append a uniform superposition of strings[11], which brings us to the information-theoretic inefficient construction

$$G_{(f,\pi)}\left|\psi\right\rangle = \frac{1}{\sqrt{2^m}}\sum_{x\in\{0,1\}^n, y\in\{0,1\}^m}\alpha_x\cdot\omega_p^{f(x||y)}\left|\pi(x||y)\right\rangle, \tag{1}$$

To make the construction efficient, we instantiate f and g with a post-quantum pseudorandom function and a post-quantum pseudorandom permutation, respectively, hence reaching our construction

$$F_{(k_1,k_2)}\left|\psi\right\rangle = \frac{1}{\sqrt{2^m}}\sum_{x\in\{0,1\}^n, y\in\{0,1\}^m}\alpha_x\cdot\omega_p^{f_{k_1}(x||y)}\left|g_{k_2}(x||y)\right\rangle.$$

Security Proof As a first step, we argue that a QPT adversary cannot distinguish the PRF (f_{k_1}) and the PRP (g_{k_2}) from a random function and a random permutation, respectively. To show this we use a $2q$-wise

[10] This condition will later be referred to as $\vec{z}$ and $\vec{z}'$ having the same *type*.
[11] Note that this step crucially relies on the fact that we are constructing a pseudorandom isometry, not a pseudorandom unitary.

independent hash function as an intermediate hybrid for f_{k_1} to get an efficient reduction, following [Zha12] who showed that such a hash function is indistinguishable from a random function under q queries. Combining this with [Zha16] who showed how to instantiate the PRP (g_{k_2}) from post-quantum one-way functions, we successfully invoke computational assumptions.

Now that we have invoked the computational assumptions as per the existence of quantum-secure PRF and PRP, we are left with the information theoretic construction given by $G_{(f,\pi)}$ (eq. (1)), which is parametrized by a random function f and a random permutation π. Below, we write $\rho \in \mathcal{Q}$ as a short-hand to mean $\rho \in \mathcal{Q}_{n,q,\ell,\lambda}$ for some $\lambda \in \mathbb{N}$. To show that $G_{(f,\pi)}$ is *statistically* $\mathcal{Q}$-secure for different query sets $\mathcal{Q}$, we will show that the output of $G_{(f,\pi)}$ under any query $\rho \in \mathcal{Q}$ is *almost-invariant* under q-fold Haar unitary as per our second observation above. We achieve this in two steps:

Step 1: Find a particular mixed state ρ_{uni}, to be defined later, which is almost-invariant under q-fold Haar unitary. Conclude that if the output of $G_{(f,\pi)}$ under any query $\rho \in \mathcal{Q}$ is negligibly close (in trace distance) to ρ_{uni}, then it is q-fold Haar almost invariant, hence $G_{(f,\pi)}$ satisfies statistical $\mathcal{Q}$-security.

Step 2: For 3 different instantiations of $\mathcal{Q}$, prove that the condition in Step 1 is satisfied, hence $G_{(f,\pi)}$ is statistically $\mathcal{Q}$-secure.

Note that our proof-strategy outlined above is a top-down approach, and the first two steps can be viewed as reducing the problem of PRI-security to a simpler condition that is easier to check for different query sets, and is independent of the action of Haar isometry on $\mathcal{Q}$. In Step 3, we show instantiations of $\mathcal{Q}$ that satisfy the simpler condition. Next, we delve into the details of each step.

Step 1: An Almost-Invariant State: ρ_{uni}. Having established q-fold Haar almost-invariance as a sufficient condition for statistical security of $G_{(f,\pi)}$, it is natural to ask the question:

Can we find a state ρ^* which is both:
(a) close to the output of $G_{(f,\pi)}$ on certain inputs, and
(b) q-fold Haar almost-invariant?

This would allow us to use negligible closeness to ρ^* as a sufficient condition for q-fold Haar almost-invariance, hence for statistical security of $G_{(f,\pi)}$. We start by analyzing condition (a).

We restrict our attention to queries with a particular, yet quite general, structure. Namely, suppose $\mathcal{Q} = \{\mathcal{Q}_{n,q,\ell,\lambda}\}$ is such that every $\rho \in \mathcal{Q}$ is a mixture of pure states of the form $\bigotimes_{i=1}^{s} |\psi_i\rangle^{\otimes t}$, where $q = st$. In other words, the adversary makes queries in the form of s states with t-copies each, or formally queries from the s-fold tensor product of symmetric subspaces, denoted by $\mathcal{H} = \left(\vee^t \mathbb{C}^N\right)^s$. For such inputs, the output of the isometry will belong to the corresponding tensor product of symmetric subspaces $\mathcal{H}' := \left(\vee^t \mathbb{C}^{NM}\right)^s$, where $N = 2^n$ and $M = 2^m$. It is known [Har13] that $\mathcal{H}$ is spanned by s-fold tensor product of *type states* $|\psi_{T_1,\ldots,T_s}\rangle = \bigotimes_{i=1}^{s} |\mathsf{type}_{T_i}\rangle$, where $|\mathsf{type}_{T_i}\rangle$ is a uniform superposition over computational basis states $|\vec{x}\rangle \in \mathbb{C}^{Nt}$ of the same *type* (T_i), where

$\vec{x}$ and $\vec{y}$ are said to have the same type if $\vec{y} = \sigma\vec{x}$ for some permutation $\sigma \in S_t$ over t elements.
To understand the action of $G_{(f,\pi)}$ on $\mathcal{Q}$, we consider its action on a basis state $|\psi_{T_1,\ldots,T_s}\rangle$ of $\mathcal{H}$. We first look at the action of a random isometry $\mathcal{I}$ on $|\psi_{T_1,\ldots,T_s}\rangle$ and see that

$$\mathop{\mathbb{E}}_{\mathcal{I}}\left[\mathcal{I}^{\otimes q}\,|\psi_{T_1,\ldots,T_s}\rangle\langle\psi_{T_1,\ldots,T_s}|\,\mathcal{I}^{\otimes q}\right] = \mathop{\mathbb{E}}_{T'_1,\ldots,T'_s}\left[|\psi_{T'_1,\ldots,T'_s}\rangle\langle\psi_{T'_1,\ldots,T'_s}|\right]$$

is maximally mixed over $\mathcal{H}'$, where $T'_1,\ldots,T'_s$ are types over $\mathbb{C}^{NMt}$. The same fact is not quite true for $G_{(f,\pi)}$ due to cross terms. Nonetheless, such terms cancel out whenever $(T_1,\ldots,T_s)$ form a set of *unique* types, denoted by $(T_1,\ldots,T_s) \in \mathcal{T}_{\mathsf{uni}^n_{s,t}}$, meaning collectively they span st distinct computational basis states $|x\rangle \in \mathbb{C}^N$, thanks to the nice algebraic structure of the image of f, i.e. $\mathbb{Z}_p$. As a result, we get

$$\begin{aligned}&\mathop{\mathbb{E}}_{f,\pi}\left[G^{\otimes q}_{(f,\pi)}\,|\psi_{T_1,\ldots,T_s}\rangle\langle\psi_{T_1,\ldots,T_s}|\,G^{\otimes q}_{(f,\pi)}\right]\\ &= \mathop{\mathbb{E}}_{(T'_1,\ldots,T'_s)\leftarrow\mathcal{T}_{\mathsf{uni}^{n+m}_{s,t}}}\left[|\psi_{T'_1,\ldots,T'_s}\rangle\langle\psi_{T'_1,\ldots,T'_s}|\right] =: \rho_{\mathsf{uni}} \qquad (2)\end{aligned}$$

for any $(T_1,\ldots,T_s) \in \mathcal{T}_{\mathsf{uni}^n_{s,t}}$. Fortunately, ρ_{uni} satisfies[12] property (b) as well. The reason is that the q-fold unique type states $|\psi_{T_1,\ldots,T_s}\rangle$ constitute the vast majority[13] of the basis for $\mathcal{H}'$, so that ρ_{uni} is negligibly close to the maximally mixed state over $\mathcal{H}'$, which is invariant under q-fold unitary operations. Therefore, if $G^{\otimes q}_{(f,\pi)}\rho(G^{\dagger}_{(f,\pi)})^{\otimes q}$ is negligible close to ρ_{uni}, then it is q-fold Haar almost-invariant, hence we have a simpler sufficient condition to check for PRI security as desired. Note that so far we have ignored the ℓ-qubit (purification) register held by the adversary, but the arguments generalize without trouble.

Step 2: Closeness to ρ_{uni}. In the final step of our security proof, we show that $G_{(f,\pi)}$ is statistically $\mathcal{Q}$-secure for three instantiations of $\mathcal{Q}$ by showing that the output of $G_{(f,\pi)}$ is close to ρ_{uni} in each case.

Distinct Types: By *eq.* (2), it follows that $G_{(f,\pi)}$ is $\mathcal{Q}$-secure for[14] $\mathcal{Q} = \mathcal{T}_{\mathsf{uni}^n_{s,t}}$. We can generalize this to *distinct* type states $|\psi_{T_1,\ldots,T_s}\rangle$, which are defined by the condition that the computational basis states spanned by the types T_i are mutually disjoint, denoted by $(T_1,\ldots,T_s) \in \mathcal{T}_{\mathsf{dis}^n_{s,t}}$. Note that $\mathcal{T}_{\mathsf{uni}^n_{s,t}} \subset \mathcal{T}_{\mathsf{dis}^n_{s,t}}$ since for types $(T_1,\ldots,T_s) \in \mathcal{T}_{\mathsf{dis}^n_{s,t}}$ each T_j may contain repetitions. Fortunately, a careful analysis shows that the output of $G_{(f,\pi)}$ on a distinct type state acquires a nice form and is close to ρ_{uni} as well. Intuitively, the reason for this is that the first step in our construction appends a random string $\vec{a}$ to the input query, and

[12] We note that $\rho_{\mathsf{uni}} = \rho_{\mathsf{uni}_{s,t}}$ is parametrized by s,t in the tecnhical sections, which we omit here for simplicity of notation.
[13] This follows from the fact that a random type will contain no repetitions with overwhelming probability as long as $t = \mathsf{poly}(\lambda)$.
[14] The reader may observe that we can also consider the convex closure of $\mathcal{T}_{\mathsf{uni}^n_{s,t}}$.

after this step the internal collisions in $\mathcal{T}_{\mathsf{dis}^n_{s,t}}$ get eliminated except with negligible weight. Accordingly, we get security for the query set

$$\mathcal{Q}_{\mathsf{distinct}_{t,s}} = \left\{ \bigotimes_{i=1}^{s} |\mathsf{type}_{T_i}\rangle\langle\mathsf{type}_{T_i}| : (T_1, \cdots, T_s) \in \mathcal{T}_{\mathsf{dis}^n_{s,t}} \right\}.$$

As a corollary, we conclude that our construction is secure against computational basis queries.

Many Copies of an n-Qubit State: Next, we show security for many copies of the same pure state, defined by the query set

$$\mathcal{Q}_{\mathsf{Single}} = \left\{ |\psi\rangle^{\otimes t} \otimes |\psi\rangle^{\otimes t} \ : \ |\psi\rangle \in \mathcal{S}(\mathbb{C}^{2^n}) \right\},$$

which allows for the adversary to keep t copies of the state that are not fed into the PRI, with $\ell = q = t$. We can write the input state in the type-basis of the symmetric subspace as

$$|\psi\rangle\langle\psi|^{\otimes t} = \sum_{T,T'} \alpha_{T,T'} |\mathsf{type}_T\rangle\langle\mathsf{type}_{T'}|.$$

Thanks to the algebraic structure of $\mathbb{Z}_p$, the terms with $T \neq T'$ vanish under the application of $G^{\otimes q}_{(f,\pi)}(\cdot)(G^{\dagger}_{(f,\pi)})^{\otimes q}$. The rest of the terms are approximately mapped to ρ_{uni} as we showed in $\mathcal{Q}_{\mathsf{distinct}_{t,s}}$-security above (by taking $s = 1$). Hence, the result follows.

Haar States: Finally, we consider the case when the query contains a collection of s i.i.d. Haar states, with t copies of each kept by the adversary and t copies given as input to the PRI, i.e. the query set is

$$\mathcal{Q}_{\mathsf{Haar}} = \left\{ \mathbb{E}_{|\psi_1\rangle,\ldots,|\psi_s\rangle \leftarrow \mathscr{H}_n} \left[\bigotimes_{i=1}^{s} |\psi_i\rangle\langle\psi_i|^{\otimes t} \otimes \bigotimes_{i=1}^{s} |\psi_i\rangle\langle\psi_i|^{\otimes t} \right] \right\}.$$

Note that without the red part, the security would simply follow by taking an expectation over unique types in eq. (2). Since the adversary will keep t copies of each Haar state to herself, she holds an entangled register (purification) to the query register, hence we need to work more. We first recall that the query $\rho_{\mathsf{Haar}} \in \mathcal{Q}_{\mathsf{Haar}}$ is negligibly close to the uniform mixture of unique s-fold type states (for $2t$ copies). We combine this with the useful expression

$$|\mathsf{type}_T\rangle\langle\mathsf{type}_T| = \frac{1}{(2t)!} \sum_{\sigma \in S_{2t}} \sum_{\substack{\vec{v} \in [N]^{2t} \\ \mathsf{type}(\vec{v}) = T}} |\vec{v}\rangle\langle\sigma(\vec{v})|. \tag{3}$$

to express the output as

$$\rho \propto \mathop{\mathbb{E}}_{\substack{(f,\pi) \\ T_1,\ldots,T_s \\ (\vec{x_1},\cdots,\vec{x_s}) \in (T_1,\cdots,T_s) \\ \sigma_1,\cdots,\sigma_s \in S_{2t}}} \left[\bigotimes_{i=1}^{s} \left(\left(I_{nt} \otimes \left(G_{(f,\pi)} \right)^{\otimes t} \right) |\vec{x_i}\rangle\langle\sigma_i(\vec{x_i})| \right. \right.$$

$$\cdot \left(I_{nt} \otimes \left(G^{\dagger}_{(f,\pi)} \right)^{\otimes t} \right) \Big) \Big] .$$

Above, due to the nice structure of $G_{(f,\pi)}$, the only terms that do not vanish are those with permutations σ_i that act separately on the first and the last n qubits, i.e. $\sigma_i(\vec{x_i}) = \sigma_i^1(\vec{x_i^1})||\sigma_i^2(\vec{x_i^2})$ with $\sigma_i^b \in S_n, x_i^b \in \{0,1\}^n$. With this observation, and using eq. (3) in reverse, we see that the q-fold application of $G_{(f,\pi)}$ effectively *unentangles* the state, which was the only barrier against security.

Applications We discuss applications of PRIs, giving an overview of Section 4.

Multi-Copy Secure Encryption. As a first application, we achieve multi-copy secure public-key and private-key encryption for quantum messages. Multi-copy security is defined via a chosen-plaintext attack (CPA) with the modification that the CPA adversary gets polynomially many copies of the ciphertext in the security experiment. This modification only affects security in the quantum setting due to the no-cloning principle, with the ciphertexts being quantum states. We note that using t-designs one can achieve multi-copy security if the number of copies is fixed a-priori before the construction, whereas using PRI we can achieve it for *arbitrary* polynomially many copies. Multi-copy security was independently studied by [LQS+23] albeit in the one-time setting.
We will focus on the public-key setting, for the private-key setting is similar. Formally, we would like an encryption scheme $(\mathsf{Setup}, \mathsf{Enc}, \mathsf{Dec})$ with the property that no QPT adversary, given $\rho^{\otimes t}$, where $\rho \leftarrow \mathsf{Enc}(|\psi_b\rangle)$, can distinguish the cases $b = 0$ and $b = 1$ with non-negligible advantage, for any quantum messages $|\psi_0\rangle, |\psi_1\rangle$. In the construction, we will use a post-quantum public-key encryption scheme $(\mathsf{setup}, \mathsf{enc}, \mathsf{dec})$ and a secure pseudorandom isometry PRI. The public-secret keys are those generated by $\mathsf{setup}(1^\lambda)$. To encrypt a quantum message $|\psi\rangle$, we sample a PRI key k and output (ct, φ), where ct is encryption of k using enc, and $\varphi \leftarrow \mathsf{PRI}_k(|\psi\rangle)$. Note that for correctness we need the ability to efficiently invert the PRI, which is a property satisfied by our PRI construction.
To show security, we deploy a standard hybrid argument where we invoke the security of $(\mathsf{setup}, \mathsf{enc}, \mathsf{dec})$ as well as the $\mathcal{Q}_{\mathsf{Single}}$-security of PRI. This suffices since we only run PRI on copies of the same pure-state input (the quantum message).

Succinct Commitments. [GJMZ23] showed how to achieve succinct quantum commitments using pseudorandom unitaries (PRU) by first achieving one-time secure quantum encryption, and then showing that one-time secure quantum encryption implies succinct commitments. We adapt their approach to achieve succinct quantum commitments from PRIs. [LQS+23] uses the work of [GJMZ23] in a similar fashion to achieve succinct commitments from quantum pseudorandom state scramblers.
To one-time encrypt a quantum message, we apply in order: (1) inverse Schur transform, (2) PRI, and (3) Schur transform. Note that in contrast

with [GJMZ23], the Schur transforms in (1) and (3) have different dimensions. The security proof follows that of [GJMZ23] closely and relies on Schur's Lemma.

Quantum MACs. We show how to achieve a restricted version of quantum message authentication codes (QMACs) using an invertible pseudorandom isometry PRI. We face definitional challenges in this task.
Similar to an injective function, an isometry does not have a unique inverse[15]. We discuss this and give a natural definition of the inverse in Section 2.1.
There is extensive literature [BCG+02, DNS12, GYZ17, AM17] on *one-time*, private-key quantum state authentications, i.e., the honest parties can detect whether the signed quantum state has been tempered. However, defining *many-time* security, such as existentially unforgeable security under a chosen-message attack, is quite challenging. In particular, defining QMACs is non-trivial for several reasons, explicitly pointed out by [AGM18]. Firstly, one needs to carefully define what constitutes a *forgery*, and secondly, verification may require multiple copies of the message and/or the tag. We give a new syntax which differs from the classical setting in that the verification algorithm outputs a message instead of Accept/Reject.
In our construction, the signing algorithm simply applies PRI to the quantum message, whereas the verification applies the inverse of PRI. Given this syntax, we show that our construction satisfies three different security notions:

- In the first setting, the verification algorithm is run polynomially many times in parallel on fresh (message, tag) pairs, and the outputs of the verifier is compared with the message using a SWAP test. We argue that during a forgery, each swap test succeeds with constant probability, hence the forgery succeeds with exponentially small probability due to independent repetition of SWAP tests.
- In the second setting, the verification is run once on the tag, and the output is compared to polynomially many copies of the message using a generalized SWAP test called *the permutation test* [BBD+97, KNY08, GHMW15, BS20a]. The upside of this security notion is that it requires only one copy of the tag, yet the downside is that the it yields inverse polynomial security rather than negligible security.
- In the third setting, the adversary is asked to output the description of an invertible quantum circuit that generates the forgery message on input $|0^n\rangle$, together with the tag. In this setting, the verification is run on the tag, and the inverse of the circuit is computed on the output to see if the outcome is $|0^n\rangle$. We show that negligible security in this setting follows as a direct consequence of PRI security.

Now we will describe the security proof for the first and the second settings. Firstly, we can replace the PRI with a Haar isometry $\mathcal{I}$ using PRI security. Next, suppose the adversary $\mathcal{A}$ makes q queries $|\psi_1\rangle, \ldots, |\psi_q\rangle$ to the signing oracle, receiving tags $|v_1\rangle, \ldots, |v_q\rangle$ in return. Let the forgery

[15] We remind the reader that the map $\mathcal{I}^\dagger$ is not a physical map (quantum channel) for a general isometry $\mathcal{I}$.

output by $\mathcal{A}$ be $(|\psi^*\rangle, |\phi^*\rangle)$. It is forced by definition that $|\psi^*\rangle$ is orthogonal to $V := \mathsf{span}(|\psi_1\rangle, \ldots, |\psi_q\rangle)$. From $\mathcal{A}$'s point of view, $\mathcal{I}|\psi^*\rangle$ is a Haar-random state sampled from $V^\perp$. Therefore, any $|\phi^*\rangle \in V$ will be mapped to a state orthogonal to $|\psi^*\rangle$ by the verification, whereas a forgery satisfying $|\phi^*\rangle \in V^\perp$ is as good as any other such forgery. Putting these together, a straightforward calculation using the fact that $\dim V \leq q \ll 2^\lambda$ suffices for the proof in both settings.

PRS Length Extension. We show how to generically extend the length of a Haar-random state using a small amount of randomness assuming the existence of PRIs. Formally, we show that if PRI is a secure $(n, n+m)$-pseudorandom isometry, then given t copies of a $2n$-qubit Haar-random state $|\theta\rangle$, the state $(I_n \otimes \mathsf{PRI}_k)^{\otimes t} |\theta\rangle^{\otimes t}$, obtained by applying PRI_k to the last n qubits, is computationally indistinguishable from t copies of a $(2n+m)$-qubit Haar-random state $|\gamma\rangle^{\otimes t}$.
In the proof, we can replace PRI with a random isometry $\mathcal{I}$ up to negligible loss invoking security. After writing $|\theta\rangle\langle\theta|^{\otimes t}$ as a uniform mixture of type states, we obtain the expression

$$\rho' = \mathop{\mathbb{E}}_{T,\mathcal{I}} \left[(I_n \otimes \mathcal{I})^{\otimes t} |\mathsf{type}_T\rangle\langle\mathsf{type}_T| (I_n \otimes \mathcal{I}^\dagger)^{\otimes t} \right],$$

where by a collision-bound we can assume (up to a negligible loss) that T is sampled as a *good* type, meaning if it contains strings $\{x_1||y_1 \ldots x_t||y_t\}$, then $x_i \neq x_j$ and $y_i \neq y_j$ for $i \neq j$. For such good types T, we can show that the state ρ' is close to the uniform mixture of type states $|\mathsf{type}_{T'}\rangle\langle\mathsf{type}_{T'}|$ spanning states of the form $|\vec{x}\rangle|\vec{z}\rangle$, where $\vec{z} \in \{0,1\}^{(n+m)t}$ is a random vector with pairwise distinct coordinates. This is because the mapping $(I_n \otimes \mathcal{I})^{\otimes t}$ *scrambles* $\vec{y}$ and leaves $\vec{x}$ untouched. In the proof we use our (first) observation about how t-fold Haar unitary acts on orthogonal inputs.
For technical reasons, our loss in this step is proportional to $t!$, which necessitates the assumption that t must be sublinear in the security parameter (e.g. $t = \mathsf{poly}\log(\lambda)$. In more detail, we expand ρ' by expressing the type state $|\mathsf{type}_T\rangle$ as superposition of computational basis states pairwise related by a permutation to get

$$\begin{aligned}\rho' &= \frac{1}{t!} \sum_{\sigma,\pi \in S_t} |\sigma(\vec{x})\rangle\langle\pi(\vec{x})| \otimes \mathop{\mathbb{E}}_{\mathcal{I}}[\mathcal{I}^{\otimes t} |\sigma(\vec{y})\rangle\langle\pi(\vec{y})| (\mathcal{I}^\dagger)^{\otimes t}] \\ &= \frac{1}{t!} \sum_{\sigma,\pi \in S_t} |\sigma(\vec{x})\rangle\langle\pi(\vec{x})| \otimes P_\sigma \mathop{\mathbb{E}}_{\mathcal{I}}[\mathcal{I}^{\otimes t} |\vec{y}\rangle\langle\vec{y}| (\mathcal{I}^\dagger)^{\otimes t}] P_\pi^\dagger,\end{aligned}$$

where we used the fact that the permutation operators P_σ, P_π commute[16] with the t-fold isometry $\mathcal{I}^{\otimes t}$. We can show that the term between the permutation operators $P_\sigma, P_\pi^\dagger$ is maximally scrambled for any given σ, π, which can be combined with a union bound over σ, π that yields a factor of $t!$ in the loss. Unfortunately we do not know how to relate the

[16] Technically the permutation operator acts on a larger Hilbert space after applying the isometry, but it applies the same permutation to the order of t copies.

terms across different σ, π to avoid this loss. Finally, the uniform mixture we obtained is negligibly close to the distribution of $|\gamma\rangle^{\otimes t}$ by another collision-bound.

2 Pseudorandom Isometry: Definition

For a given class of inputs $\mathcal{Q}$, we propose the following definition of $\mathcal{Q}$-secure psuedorandom isometries. Throughout the rest of the paper, for a polynomial $p(\cdot)$, we denote p to be $p(\lambda)$, where λ is the security parameter.

Definition 1 ($\mathcal{Q}$-Secure Pseudorandom Isometry (PRI)). *Let n, m, q, ℓ be polynomials in λ. Suppose $\mathcal{Q} = \{\mathcal{Q}_{n,q,\ell,\lambda}\}_{\lambda\in\mathbb{N}}$, where $\mathcal{Q}_{n,q,\ell,\lambda} \subseteq \mathcal{D}(\mathbb{C}^{2^{nq+\ell}})$. We say that $\mathsf{PRI} = \{F_\lambda\}_{\lambda\in\mathbb{N}}$ is an $(n, n+m)$-$\mathcal{Q}$-secure pseudorandom isometry if the following holds:*

- *For every $k \in \{0,1\}^\lambda$, $F_\lambda(k,\cdot)$ is a QPT algorithm implementing a quantum channel such that it is functionally equivalent to $\mathcal{I}_k$, where $\mathcal{I}_k$ is an isometry that maps n qubits to $n+m$ qubits.*
- *For sufficiently large $\lambda \in \mathbb{N}$, any QPT distinguisher $\mathcal{A}$, the following holds: for every $\rho \in \mathcal{Q}_{n,q,\ell,\lambda}$,*

$$\left|\Pr\left[\mathcal{A}\left(\left(I_\ell \otimes F_k^{\otimes q}\right)(\rho)\right) = 1\right] - \Pr\left[\mathcal{A}\left(\left(I_\ell \otimes \mathcal{I}^{\otimes q}\right)(\rho)\right) = 1\right]\right| \leq \mathsf{negl}(\lambda),$$

where:

- *$\mathcal{I}(\cdot)$ is the channel implementing a Haar-random isometry that takes an n-qubit input $|\psi\rangle$ and outputs an $(n+m)$-qubit output $\mathcal{I}(|\psi\rangle)$,*
- *I_ℓ is an identity operator on ℓ qubits.*

We sometimes write $\mathcal{Q}$-secure with m, n being implicit. We consider the following set of queries. We color the part of the query given to I_ℓ with red and color the part of the query given to F_k or $\mathcal{I}$ with blue.

Computational basis queries. We define $\mathcal{Q}^{(\mathsf{Comp})}_{n,q,\ell,\lambda}$ as follows.

$$\mathcal{Q}^{(\mathsf{Comp})}_{n,q,\ell,\lambda} = \mathcal{D}(\mathbb{C}^{2^\ell}) \otimes \{(|x_1\rangle\langle x_1| \otimes \ldots \otimes |x_q\rangle\langle x_q|) \ : \ x_1, \ldots, x_q \in \{0,1\}^n\}.$$

Let $n(\cdot), q(\cdot), \ell(\cdot)$ be polynomials. We also define $\mathcal{Q}_{\mathsf{Comp}}$ (implicitly parameterized by $n(\cdot), q(\cdot), \ell(\cdot)$) to be $\mathcal{Q}_{\mathsf{Comp}} = \left\{\mathcal{Q}^{(\mathsf{Comp})}_{n,q,\ell,\lambda}\right\}_{\lambda\in\mathbb{N}}$.

Multiple copies of a single pure state. We define $\mathcal{Q}^{(\mathsf{Single})}_{n,q,\ell,\lambda}$ as follows:

$$\mathcal{Q}^{(\mathsf{Single})}_{n,q,\ell,\lambda} = \mathcal{D}(\mathbb{C}^{2^\ell}) \otimes \left\{\left(|\psi\rangle\langle\psi|^{\otimes q}\right) \ : |\psi\rangle \text{ is an } n\text{-qubit pure state}\right\}.$$

Let $n(\cdot), q(\cdot), \ell(\cdot)$ be polynomials. We also define $\mathcal{Q}_{\mathsf{Single}}$ (implicitly parameterized by $n(\cdot), q(\cdot), \ell(\cdot)$) to be $\mathcal{Q}_{\mathsf{Single}} = \left\{\mathcal{Q}^{(\mathsf{Single})}_{n,q,\ell,\lambda}\right\}_{\lambda\in\mathbb{N}}$.

Haar queries. We first define $\mathcal{Q}^{(\mathsf{Haar})}_{n,s,t,\ell',\lambda}$ as follows, for some polynomials $s(\cdot), t(\cdot), \ell'(\cdot)$,

$$\mathcal{Q}^{(\mathsf{Haar})}_{n,s,t,\ell',\lambda} = \mathcal{D}(\mathbb{C}^{2^{\ell'(\lambda)}}) \otimes \left\{ \mathop{\mathbb{E}}_{|\psi_1\rangle,\ldots,|\psi_{s(\lambda)}\rangle \leftarrow \mathscr{H}_n} \left[\bigotimes_{i=1}^{s(\lambda)} |\psi_i\rangle\langle\psi_i|^{\otimes t(\lambda)} \otimes \bigotimes_{i=1}^{s(\lambda)} |\psi_i\rangle\langle\psi_i|^{\otimes t(\lambda)} \right] \right\}.$$

Next, we define $\mathcal{Q}^{(\mathsf{Haar})}_{n,q,\ell,\lambda}$ as follows

$$\mathcal{Q}^{(\mathsf{Haar})}_{n,q,\ell,\lambda} = \bigcup_{\substack{s,t,\ell' \\ \text{such that } q=st \\ \text{and } \ell=\ell'+st}} \mathcal{Q}^{(\mathsf{Haar})}_{n,s,t,\ell',\lambda}.$$

Let $n(\cdot), q(\cdot), \ell(\cdot)$ be polynomials. We also define $\mathcal{Q}_{\mathsf{Haar}}$ (implicitly parameterized by $n(\cdot), q(\cdot), \ell(\cdot)$) to be $\mathcal{Q}_{\mathsf{Haar}} = \left\{ \mathcal{Q}^{(\mathsf{Haar})}_{n,q,\ell,\lambda} \right\}_{\lambda\in\mathbb{N}}$.

Distinct Querries We define a class of states

$$\mathcal{Q}^{(\mathsf{distinct})}_{n,t,s,\ell,\lambda} := \mathcal{D}(\mathbb{C}^{2^{\ell'(\lambda)}}) \otimes \{ \bigotimes_{i=1}^{s} |\mathsf{type}_{T_i}\rangle\langle\mathsf{type}_{T_i}| : (T_1, \cdots, T_s) \in \mathcal{T}_{\mathsf{dis}^n_{s,t}} \}.$$

Next, we define the following class:

$$\mathcal{Q}^{(\mathsf{distinct})}_{n,q,\ell,\lambda} := \bigcup_{\substack{s,t \\ \text{such that } q=st}} \mathcal{Q}^{(\mathsf{distinct})}_{n,t,s,\ell,\lambda}.$$

We define $\mathcal{Q}_{(\mathsf{distinct})} := \{\mathcal{Q}^{(\mathsf{distinct})}_{n,q,\ell,\lambda}\}_{\lambda\in\mathbb{N}}$.

Selective PRI. Above, we considered the security of PRI in the setting where the queries came from a specific query set. However, we can consider an alternate definition where the indistinguishability holds against computationally bounded adversaries making a single parallel query to an oracle that is either PRI or Haar. We term such a PRI to be a selectively secure PRI.

Definition 2 (Selective Pseudorandom Isometry). $\mathsf{PRI} = \{F_\lambda\}_{\lambda\in\mathbb{N}}$ *is an* $(n, n+m)$*-selective pseudorandom isometry if the following holds:*

- *For every* $k \in \{0,1\}^\lambda$, $F_\lambda(k,\cdot)$ *is a QPT algorithm such that it is functionally equivalent to* $\mathcal{I}_k$*, where* $\mathcal{I}_k$ *is an isometry that maps* n *qubits to* $n+m$ *qubits.*
- *For sufficiently large* $\lambda \in \mathbb{N}$*, for any* $q = \mathsf{poly}(\lambda)$*, any QPT distinguisher* $\mathcal{A}$ *making* 1 *query to the oracle, the following holds:*

$$\left| \Pr\left[\mathcal{A}^{(F_\lambda(k,\cdot))^{\otimes q}} = 1\right] - \Pr\left[\mathcal{A}^{(\mathcal{I}(\cdot))^{\otimes q}} = 1\right] \right| \leq \mathsf{negl}(\lambda),$$

where:

- $F_\lambda(k,\cdot)$ *takes as input* $|\psi\rangle$ *and outputs* $F_\lambda(k,|\psi\rangle)$
- $\mathcal{I}(\cdot)$ *is a Haar-random isometry that takes as* n*-qubit input* $|\psi\rangle$ *and outputs an* $(n+m)$*-qubit output* $\mathcal{I}(|\psi\rangle)$.

The following claim is immediate.

Claim. Let $n(\cdot), m(\cdot)$ be two polynomials. Suppose PRI is an $(n, n+m)$-$\mathcal{Q}_{n,q,\ell}$-secure pseudorandom isometry for every polynomial $q(\cdot), \ell(\cdot)$, and, $\mathcal{Q}_{n,q,\ell} = \{\mathcal{Q}_{n,q,\ell,\lambda}\}_{\lambda\in\mathbb{N}}$, where $\mathcal{Q}_{n,q,\ell,\lambda} = \mathcal{D}(\mathbb{C}^{2^{nq+\ell}})$. Then, PRI is a selective pseudorandom isometry.

Similarly, the other direction is true as well.

Claim. Let $n(\cdot), m(\cdot)$ be two polynomials. Suppose PRI is an $(n, n+m)$-secure pseudorandom isometry. Then PRI is a $(n, n+m)$-$\mathcal{Q}_{n,q,\ell}$-secure pseudorandom isometry for every polynomial $q(\cdot), \ell(\cdot)$, and, $\mathcal{Q}_{n,q,\ell} = \{\mathcal{Q}_{n,q,\ell,\lambda}\}_{\lambda\in\mathbb{N}}$, where $\mathcal{Q}_{n,q,\ell,\lambda} = \mathcal{D}(\mathbb{C}^{2^{nq+\ell}})$.

Adapive PRI. We also define an adaptive version of the pseudorandom isometries below. In this definition, the adversary can make an arbitrary number of queries to the oracle.

Definition 3 (Adaptive Pseudorandom Isometry). $\mathsf{PRI} = \{F_\lambda\}_{\lambda\in\mathbb{N}}$ *is an* $(n, n+m)$*-adaptive pseudorandom isometry if the following holds:*

- *For every* $k \in \{0,1\}^\lambda$, $F_\lambda(k,\cdot)$ *is a QPT algorithm such that it is functionally equivalent to* $\mathcal{I}_k$*, where* $\mathcal{I}_k$ *is an isometry that maps* n *qubits to* $n+m$ *qubits.*
- *For sufficiently large* $\lambda \in \mathbb{N}$*, for any* $t = \mathsf{poly}(\lambda)$*, any QPT distinguisher* $\mathcal{A}$ *making* t *queries to the oracle, the following holds:*

$$\left|\Pr\left[\mathcal{A}^{F_\lambda(k,\cdot)} = 1\right] - \Pr\left[\mathcal{A}^{\mathcal{I}(\cdot)} = 1\right]\right| \leq \mathsf{negl}(\lambda),$$

where:

- $F_\lambda(k,\cdot)$ *takes as input* $|\psi\rangle$ *and outputs* $F_\lambda(k,|\psi\rangle)$
- $\mathcal{I}(\cdot)$ *is a Haar-random isometry that takes as* n*-qubit input* $|\psi\rangle$ *and outputs an* $(n+m)$*-qubit output* $\mathcal{I}(|\psi\rangle)$.

Observations. It should be immediate that pseudorandom unitaries, introduced in [JLS18], imply adaptive PRI, which in turn implies selectively secure PRI. Whether pseudorandom isometries are separated from pseudorandom unitaries or there is a transformation from the former to the latter is an interesting direction to explore.
If we weaken our definition of pseudorandom isometries further, where we a priori fix the number of queries made by the adversary and allow the description of the pseudorandom isometry to depend on this then this notion is implied by unitary t-designs [AE07, BHH16].
In terms of implications of pseudorandom isometries to other notions of pseudorandomness in the quantum world, we note that pseudorandom isometries imply both PRSGs and PRFSGs.

2.1 Invertibility

Invertible Pseudorandom Isometries. In applications, we need a stronger notion of *invertible* pseudorandom isometries.

Definition 4 (Invertible $\mathcal{Q}$-Secure Pseudorandom Isometry). *We say that* $\mathsf{PRI} = \{F_\lambda\}_{\lambda\in\mathbb{N}}$ *is an invertible* $(n, n+m)$*-*$\mathcal{Q}$*-secure pseudorandom isometry if first and foremost, it is a* $\mathcal{Q}$*-secure pseudorandom isometry (Definition 1) and secondly, there is a QPT algorithm* Inv *with the following guarantee: for every* $|\psi\rangle \in \mathcal{S}\left(\mathbb{C}^{2^n}\right)$ *and* $k \in \{0,1\}^\lambda$*,*

$$\mathrm{TD}(|\psi\rangle\langle\psi|, \mathsf{Inv}(k, F_\lambda(k, |\psi\rangle))) = \mathsf{negl}(\lambda).$$

Remark 1. Similarly, we can define invertible versions of $\mathcal{Q}$-secure PRIs and selectively secure PRIs. Also, note that for $|\phi\rangle$ which is orthogonal to the range of $F_\lambda(k,\cdot)$, being invertible has no guarantee on $\mathsf{Inv}(k, |\phi\rangle)$.

Inverse of Isometries. For a (fixed) isometry $\mathcal{I}$ maps n-qubit states to $(n+m)$-qubit states, the "inverse" of $\mathcal{I}$ is not unique. However, under the view of *Stinespring dilation*, it is possible to naturally define a quantum channel $\mathcal{I}^{-1}$ such that $\mathcal{I}^{-1} \circ (\mathcal{I}|\psi\rangle\langle\psi|\mathcal{I}^\dagger) = |\psi\rangle\langle\psi|$ for every $|\psi\rangle \in \mathcal{S}\left(\mathbb{C}^{2^n}\right)$.[17] Consider an arbitrary unitary $U_\mathcal{I}$ on $n+m$ qubits such that $U_\mathcal{I}$ is *consistent* with $\mathcal{I}$, that is, $U_\mathcal{I}|\psi\rangle|0^m\rangle_{\mathsf{Aux}} = \mathcal{I}|\psi\rangle$ for every $|\psi\rangle \in \mathcal{S}\left(\mathbb{C}^{2^n}\right)$. One can easily verify that $\mathrm{Tr}_{\mathsf{Aux}}\left(U_\mathcal{I}^\dagger \mathcal{I}|\psi\rangle\langle\psi|\mathcal{I}^\dagger U_\mathcal{I}\right) = |\psi\rangle\langle\psi|$ for every $|\psi\rangle \in \mathcal{S}\left(\mathbb{C}^{2^n}\right)$. Furthermore, one can even provide a distribution over such unitaries. This yields the following candidate definition: let $\mu_\mathcal{I}$ be some distribution over unitaries that are consistent with $\mathcal{I}$, the inverse of $\mathcal{I}$ can be defined as

$$\mathcal{I}^{-1}(X) = \mathop{\mathbb{E}}_{U_\mathcal{I}\leftarrow\mu_\mathcal{I}} \mathrm{Tr}_{\mathsf{Aux}}\left(U_\mathcal{I}^\dagger X U_\mathcal{I}\right).$$

Since we focus on Haar isometries in this work, we'll choose the distribution $\mu_\mathcal{I}$ to be Haar random conditioned on being consistent with $\mathcal{I}$. Formally, we have the following definition.

Definition 5 (Inverse of Isometries). *Let* $\mathcal{I}$ *be an isometry from* n *qubits to* $n+m$ *qubits. The inverse of* $\mathcal{I}$ *is a quantum channel from* $n+m$ *qubits to* n *qubits defined to be*

$$\mathcal{I}^{-1}(X) := \mathop{\mathbb{E}}_{U\leftarrow\overline{\mathscr{H}_{n+m}}|_\mathcal{I}} \mathrm{Tr}_{\mathsf{Aux}}\left(U^\dagger X U\right),$$

for any $X \in \mathcal{L}(\mathbb{C}^{2^{n+m}})$*, where register* Aux *refers to the last* m *qubits and* $\overline{\mathscr{H}_{n+m}}|_\mathcal{I}$ *denotes the Haar measure over* $(n+m)$*-qubit unitaries* U *conditioned on* $U|\psi\rangle|0^m\rangle_{\mathsf{Aux}} = \mathcal{I}|\psi\rangle$ *for any* $|\psi\rangle \in \mathcal{S}\left(\mathbb{C}^{2^n}\right)$.

The inverse of a Haar isometry satisfies the following:

[17] The readers should not confuse $\mathcal{I}^\dagger$, the conjugate transpose of $\mathcal{I}$, with the channel $\mathcal{I}^{-1}$.

Fact 7. *Let $\mathcal{I}$ be a Haar isometry from n qubits to $n+m$ qubits. Then the joint distribution of $(\mathcal{I}, \mathcal{I}^{-1})$ is identically distributed to the following procedures: (1) Sample $U \leftarrow \mathscr{H}_{n+m}$. (2) Define $\mathcal{I}$ to be the first 2^n columns of U. That is, $\mathcal{I}$ satisfies $\mathcal{I}|\psi\rangle = U|\psi\rangle|0^m\rangle_{\mathsf{Aux}}$ for any $|\psi\rangle \in \mathcal{S}\left(\mathbb{C}^{2^n}\right)$. (3) Define $\mathcal{I}^{-1}(X) := \mathrm{Tr}_{\mathsf{Aux}}(U^\dagger X U)$.*

Strong Invertible Adaptive PRI. In order to achieve more applications, we define the following stronger security definition in which the adversary is given the inversion oracle.

Definition 6 (Strong Invertible Adaptive Pseudorandom Isometry). *$\mathsf{PRI} = \{F_\lambda\}_{\lambda\in\mathbb{N}}$ is a strong invertible $(n, n+m)$-pseudorandom isometry if it satisfies the following conditions for every $\lambda \in \mathbb{N}$:*

- *For every $k \in \{0,1\}^\lambda$, $F(k,\cdot)$ is a QPT algorithm such that it is functionally equivalent to $\mathcal{I}_k$, where $\mathcal{I}_k$ is an isometry that maps n qubits to $n+m$ qubits.*
- *For every $k \in \{0,1\}^\lambda$, $\mathsf{Inv}(k,\cdot)$ is a QPT algorithm such that it is functionally equivalent to $\mathcal{I}_k^{-1}$, where $\mathcal{I}_k^{-1}$ is the inverse of $\mathcal{I}_k$ (Definition 5) that maps $n+m$ qubits to n qubits.*
- *For any polynomial $t = \mathsf{poly}(\lambda)$, any QPT distinguisher $\mathcal{A}$ making a total of t queries to the oracles, the following holds:*

$$\left|\Pr_{k\leftarrow\{0,1\}^\lambda}\left[\mathcal{A}^{F(k,\cdot),\mathsf{Inv}(k,\cdot)}=1\right] - \Pr_{\mathcal{I}\leftarrow\mathscr{H}_{n,n+m}}\left[\mathcal{A}^{\mathcal{I}(\cdot),\mathcal{I}^{-1}(\cdot)}=1\right]\right| \leq \mathsf{negl}(\lambda).$$

3 Construction

Let $m(\cdot), n(\cdot)$ be polynomials. Let $p = p(\lambda)$ be a λ-bit integer. Let $\lambda = 2\lambda_1$. We use the following tools in the construction of PRI.

- $f : \{0,1\}^{\lambda_1} \times \{0,1\}^{n(\lambda_1)+m(\lambda_1)} \to \mathbb{Z}_p$ is a quantum-query secure pseudorandom function (QPRF).
- $g : \{0,1\}^{\lambda_1} \times \{0,1\}^{n(\lambda_1)+m(\lambda_1)} \to \{0,1\}^{n(\lambda_1)+m(\lambda_1)}$ is a quantum-query secure pseudorandom permutation (QPRP).

We present the construction of psuedorandom isometry $\{F_\lambda\}_{\lambda\in\mathbb{N}}$ in Figure 1. Note that the construction presented is functionally equivalent to an isometry even though it performs a partial trace.

3.1 Main Results

Our construction is secure against inputs of the form: (1) distinct type state, (2) multiple copies of the same pure state, (3) i.i.d. Haar states. We state the formal theorem below:

Theorem 8 (Main Theorem). *Let $n, m, s, t, \ell, q = \mathsf{poly}(\lambda)$. Let $\mathcal{Q}^{(\mathsf{distinct})}_{n,t,s,\ell,\lambda}$, $\mathcal{Q}^{(\mathsf{Haar})}_{n,q,\ell,\lambda}$ and $\mathcal{Q}^{(\mathsf{Single})}_{n,q,\ell,\lambda}$ be as defined in Section 2, then, assuming the existence of post-quantum one-way functions, the construction of PRI given in Figure 1 is $\mathcal{Q}$-secure for $\mathcal{Q} \in \left\{\mathcal{Q}^{(\mathsf{distinct})}_{n,t,s,\ell,\lambda}, \mathcal{Q}^{(\mathsf{Haar})}_{n,q,\ell,\lambda}, \mathcal{Q}^{(\mathsf{Single})}_{n,q,\ell,\lambda}\right\}$.*

On input a key $k \in \{0,1\}^\lambda$ and an n-qubit register $\mathbf{X}$. We define the operation of $F_\lambda(k,\cdot)$ as follows.

- Parse the key k as $k_1||k_2$, where $k_1 \in \{0,1\}^{\lambda_1}$ is a QPRF key and $k_2 \in \{0,1\}^{\lambda_1}$ is a QPRP key.
- Append an m-qubit register $\mathbf{Z}$ initalized with $|0^m\rangle_{\mathbf{Z}}$ to register $\mathbf{X}$.
- Apply $H^{\otimes m}$ to register $\mathbf{Z}$.
- Apply $O_{f_{k_1}}$ to registers $\mathbf{X}$ and $\mathbf{Z}$.
- Apply $O_{g_{k_2}}$ to registers $\mathbf{X}$ and $\mathbf{Z}$.

Explicitly, $F_\lambda(k,\cdot)$ maps the basis vector $|x\rangle_{\mathbf{X}}$ to

$$\frac{1}{\sqrt{2^m}} \sum_{z\in\{0,1\}^m} \omega_p^{f(k_1,x||z)} |g(k_2,x||z)\rangle_{\mathbf{XZ}} .$$

Fig. 1. Description of F_λ.

Although we are not able to prove stronger security of our construction, we observe that our construction naturally mimics the steps of sampling a Haar isometry by truncating columns of a Haar unitary. We have the following conjecture.

Conjecture 2. Assuming the existence of post-quantum one-way functions, the construction of PRI given in Figure 1 is a strong invertible adaptive PRI (Definition 6)

4 Applications

We explore the cryptographic applications of pseudorandom isometries. Notably, some applications in this section only require invertible $\mathcal{Q}$-secure (Definition 4), for classes of $\mathcal{Q}$ which can be initiated by post-quantum one-way functions, as we showed in Section 3.
In Section 4.2, we present quantum message authentication codes. In Section 4.3, we present length extension theorems.

4.1 PRI implies PRSG and PRFSG

Theorem 9 (PRI implies PRSG and PRFSG). *Assuming $(n, n+m)$-$\mathcal{Q}_{\mathsf{Comp}}$-pseudorandom isometries exist, there exist an $(n+m)$-PRSG and a selectively-secure $(n, n+m)$-PRFSG.*

4.2 Quantum Message Authentication Codes

The scheme of authenticating *quantum messages* was first studied by Barnum et al. [BCG+02] in which they considered *one-time private-key* authentication schemes. The definition in [BCG+02] is generalized in the following works [DNS12, GYZ17]. In particular, Garg, Yuen, and

Zhandry [GYZ17] defined the notion of *total authentication*, which is tailored for one-time (information-theoretic) security. They showed that total authentication implies unforgeability (in certain settings[18]) and *key reusability* — conditioned on successful verification of an authentication scheme that satisfies total authentication, the key can be reused by the honest parties. Moreover, they constructed a total-authenticating scheme from unitary 8-designs. Later, the works of [Por17, AM17] independently improved the construction by using only unitary 2-designs to achieve total authentication.

In the fully classical setting, many-time security of an authentication scheme is defined via *unforgeability* — no efficient adversary can forge an un-queried message-tag pair. A message authentication code (MAC) is a common primitive that satisfies the desired properties. However, consider MACs for classical messages: when the adversary is allowed to query the signing oracle in superposition [BZ13, AMRS20], defining the *freshness* of the forgery is already nontrivial. For quantum message authentication schemes, it is well-known that authentication implies encryption [BCG+02]. Furthermore, due to the quantum nature of no-cloning and entanglement, it is challenging to define a general many-time security notion [AGM18, AGM21]. Nevertheless, we consider a strict version of MACs for quantum messages in this subsection. We'll focus on several weak yet nontrivial notions of unforgeability and show how to achieve them using PRIs.

Syntax. A message authentication codes (MAC) scheme for quantum messages of length $n(\lambda)$ is a triple of algorithms $(\mathsf{Setup}, \mathsf{Sign}, \mathsf{Ver})$.

- $\mathsf{Setup}(1^\lambda)$: on input the security parameter λ, output a key $k \leftarrow \{0,1\}^\lambda$.
- $\mathsf{Sign}(k, |\psi\rangle)$: on input $k \in \{0,1\}^\lambda$ and a quantum message $|\psi\rangle \in \mathcal{S}\left(\mathbb{C}^{2^n}\right)$, output a quantum tag[19] $|\phi\rangle \in \mathcal{S}\left(\mathbb{C}^{2^s}\right)$ where $s(\lambda) = \mathsf{poly}(\lambda)$ is the tag length.
- $\mathsf{Ver}(k, |\phi\rangle)$: on input $k \in \{0,1\}^\lambda$ and a quantum tag $|\phi\rangle \in \mathcal{S}\left(\mathbb{C}^{2^s}\right)$, output a mixed quantum state $\rho \in \mathcal{D}(\mathbb{C}^{2^n})$.

Definition 7 (Correctness). *There exists a negligible function $\varepsilon(\cdot)$ such that for every $\lambda \in \mathbb{N}$, $k \in \{0,1\}^\lambda$, and quantum message $|\psi\rangle \in \mathcal{S}\left(\mathbb{C}^{2^n}\right)$,*

$$\mathrm{TD}(\mathsf{Ver}(k, \mathsf{Sign}(k, |\psi\rangle)), |\psi\rangle\langle\psi|) \leq \varepsilon(\lambda).$$

Security Definitions. Defining security for MACs for quantum states is quite challenging, as discussed in prior works, notably in [AGM18].

[18] In more detail, they show total authentication implies unforgeability for MACs for classical messages with security against a single superposition message query.

[19] We emphasize that here we explicitly require the tag to be a pure state. We can relax this condition to allow for the signature algorithm to output a state that is close to a pure state without changing the notion much.

Nonetheless, our goal is to present some reasonable, although restrictive, definitions of MACs for quantum states whose feasibility can be established based on the existence of pseudorandom isometries. We believe that our results shed light on the interesting connection between pseudorandom isometries and MACs for quantum states and we leave the exploration of presenting the most general definition of MACs for quantum states (which in our eyes is an interesting research direction by itself!) for future works.

When the adversary is only asked to output a single copy of the (quantum) forgery, it is unclear how to achieve negligible security error. For example, if the verification is done by simply applying a SWAP test[20], then the success probability of the forger is at least $1/2$. In the following, we introduce several notions capturing unforgeability. First, in order to boost security, a straightforward way is to simply ask the adversary to send $t = \mathsf{poly}(\lambda)$ copies of the forgery message and tag.

Definition 8 (Many-Copies-Unforgeability). *Let $t = \mathsf{poly}(\lambda)$. For every polynomial $q(\cdot)$ and every non-uniform QPT adversary, there exists a function $\varepsilon(\cdot)$ such that for sufficiently large $\lambda \in \mathbb{N}$, the adversary wins with probability at most $\varepsilon(\lambda)$ in the following security game:*

1. *Challenger samples $k \leftarrow \{0,1\}^\lambda$.*
2. *The adversary sends $|\psi_1\rangle, \ldots, |\psi_q\rangle \in \mathcal{S}\left(\mathbb{C}^{2^n}\right)$ and receives $\mathsf{Sign}(k, |\psi_i\rangle)$ for $i = 1, \ldots, q$.*
3. *The adversary outputs $(|\psi^*\rangle \otimes |\phi^*\rangle)^{\otimes t}$ where $|\psi^*\rangle \in \mathcal{S}\left(\mathbb{C}^{2^n}\right)$ is orthogonal to $|\psi_i\rangle$ for $i = 1, \ldots, q$.*
4. *Challenger runs $\mathsf{SwapTest}(|\psi^*\rangle\langle\psi^*|, \mathsf{Ver}(k, |\phi^*\rangle))$ t times in parallel. The adversary wins if and only if every SWAP test outputs 1.*

Remark 2. We note that, in general, the forgery message and the tag could be entangled. Here, we focus on a restricted case in which the message and tag are required to be a product state. We leave the exploration of stronger security notions for future works.

In some cases, it is unsatisfactory to ask the adversary to output multiple copies of the forgery tag due to the no-cloning theorem and in this case, we can consider the following definition in which the adversary needs to output multiple copies of the forgery message but only a single copy of the forgery tag. The winning condition of the adversary is defined by passing the generalized SWAP test — called the *permutation test* [BBD+97, KNY08, GHMW15, BS20a].

Lemma 1 (Permutation Test). *The permutation test is an efficient quantum circuit $\mathsf{PermTest}$ that takes as input $\rho \in \mathcal{D}((\mathbb{C}^d)^{\otimes t})$, outputs 1 with probability $p := \mathrm{Tr}(\Pi^{d,t}_{\mathsf{sym}}\rho)$, and outputs 0 with probability $1 - p$.*

Definition 9 ($(\mathsf{PermTest}, t, \varepsilon)$-unforgeability). *For every polynomial $q(\cdot)$ and every non-uniform QPT adversary, there exists a function $\varepsilon(\cdot)$ such that for sufficiently large $\lambda \in \mathbb{N}$, the adversary wins with probability at most $\varepsilon(\lambda)$ in the following security game:*

[20] The SWAP test is an efficient quantum circuit that takes as input two density matrices ρ, σ of the same dimension and output 1 with probability $\frac{1+\mathrm{Tr}(\rho\sigma)}{2}$.

1. *Challenger samples* $k \leftarrow \{0,1\}^\lambda$.
2. *The adversary sends* $|\psi_1\rangle, \ldots, |\psi_q\rangle \in \mathcal{S}\left(\mathbb{C}^{2^n}\right)$ *and receives* $\mathsf{Sign}(k, |\psi_i\rangle)$ *for* $i = 1, \ldots, q$.
3. *The adversary outputs* $|\psi^*\rangle^{\otimes t} \otimes |\phi^*\rangle$ *where* $|\psi^*\rangle \in \mathcal{S}\left(\mathbb{C}^{2^n}\right)$ *and is orthogonal to* $|\psi_i\rangle$ *for* $i = 1, \ldots, q$.
4. *The adversary wins if* $\mathsf{PermTest}(|\psi^*\rangle\langle\psi^*|^{\otimes t} \otimes \mathsf{Ver}(k, |\phi^*\rangle)) = 1$.

Finally, suppose $\mathsf{Sign}(k, \cdot)$ is an isometry for every $k \in \{0,1\}^\lambda$. We consider another definition in which we ask the adversary to send the classical description of the quantum circuit that generates the forgery message and only one copy of the corresponding tag.

Definition 10 (Uncompute-Unforgeability). *For every polynomial* $q(\cdot)$ *and every non-uniform QPT adversary, there exists a negligible function* $\varepsilon(\cdot)$ *such that for every* $\lambda \in \mathbb{N}$*, the adversary wins with probability at most* $\varepsilon(\lambda)$ *in the following security game:*

1. *Challenger samples* $k \leftarrow \{0,1\}^\lambda$.
2. *The adversary sends* $|\psi_1\rangle, \ldots, |\psi_q\rangle \in \mathcal{S}\left(\mathbb{C}^{2^n}\right)$ *and receives* $\mathsf{Sign}(k, |\psi_i\rangle)$ *for* $i = 1, \ldots, q$.
3. *The adversary outputs a pair* $(C, |\phi^*\rangle)$ *where* C *is the classical description of a quantum circuit containing no measurements such that* $C|0^n\rangle$ *is orthogonal to* $|\psi_i\rangle$ *for* $i = 1, \ldots, q$.
4. *Challenger applies* $C^\dagger\mathsf{Ver}(k, \cdot)$ *on* $|\phi^*\rangle$ *and performs a measurement on all qubits in the computational basis. The adversary wins if and only if the measurement outcome is* 0^n.

Let $\mathsf{PRI} = \{F_\lambda\}_{\lambda\in\mathbb{N}}$ be a strong invertible adaptive $(n, n+m)$-PRI (Definition 6) where $n(\cdot), m(\cdot)$ are polynomials. We construct a MAC for quantum messages from PRI.

Construction 10 (MAC for quantum messages)**.**

1. $\mathsf{Sign}(k, |\psi\rangle)$: *on input* $k \in \{0,1\}^\lambda$ *and a message* $|\psi\rangle \in \mathcal{S}\left(\mathbb{C}^{2^n}\right)$*, output* $F_\lambda(k, |\psi\rangle) \in \mathcal{S}\left(\mathbb{C}^{2^{m+n}}\right)$.
2. $\mathsf{Ver}(k, |\phi\rangle)$: *on input* $k \in \{0,1\}^\lambda$ *and a tag* $|\phi\rangle \in \mathcal{S}\left(\mathbb{C}^{2^{m+n}}\right)$*, output* $\mathsf{Inv}(k, |\phi\rangle)$.

The correctness of Construction 10 follows from the invertibility of PRI.

Theorem 11. *For every* $t \in \mathbb{N}$*, Construction 10 satisfies* $(\mathsf{PermTest}, t, O(1/t))$*-unforgeability.*

Theorem 12. *Construction 10 satisfies uncompute-unforgeability.*

4.3 Length Extension of Pseudorandom States

We introduce methods to increase the *length* of pseudorandom quantum states while preserving the *number of copies*. In the classical setting, the length extension of pseudorandom strings can be accomplished by repeatedly applying PRGs. On the other hand, since pseudorandom random states are necessarily (highly) pure and entangled [JLS18, AQY22], no such method was known that would not decrease the number of copies.

Theorem 13 (Length Extension Theorem). *Assuming $\mathcal{Q}_{\mathsf{Haar}}$-secure pseudorandom isometry, mapping n qubits to $n+m$ qubits, and an n-qubit* PRSG*, there exists an $(n+m)$-*PRSG*. Similarly, assuming $\mathcal{Q}_{\mathsf{Haar}}$-secure pseudorandom isometry, mapping n qubits to $n+m$ qubits, and classical-accessible selectively-secure (ℓ, n)-*PRFSG*, there exists an classical-accessible selectively-secure $(\ell, n+m)$-*PRFSG*.*

Theorem 14 (Another Length Extension Theorem). *Let $\{F_\lambda\}_{\lambda\in\mathbb{N}}$ be an $(n, n+m)$-*PRI*, $t = t(\lambda)$,*

$$\rho := \mathop{\mathbb{E}}_{|\theta\rangle\leftarrow\mathscr{H}_{2^n}, k\in\{0,1\}^\lambda} \left[(I_n \otimes F_k)^{\otimes t} |\theta\rangle\langle\theta|^{\otimes t} (I_n \otimes F_k^\dagger)^{\otimes t} \right],$$

where F_k means $F_\lambda(k,\cdot)$ and I_n is the identity operator on n qubits, and

$$\sigma := \mathop{\mathbb{E}}_{|\gamma\rangle\leftarrow\mathscr{H}_{2^{n+m}}} \left[|\gamma\rangle\langle\gamma|^{\otimes t} \right].$$

Then any non-uniform QPT adversary has at most $O(t!t^2/2^{n+m} + t^2/2^n)$ advantage in distinguishing ρ from σ.

Acknowledgements

We thank Fermi Ma for useful discussions.

References

[ABF+23] Scott Aaronson, Adam Bouland, Bill Fefferman, Soumik Ghosh, Umesh Vazirani, Chenyi Zhang, and Zixin Zhou. *Quantum Pseudoentanglement*. 2023. arXiv: 2211.00747 [quant-ph] (cit. on pp. 2, 4, 9).

[ABG+14] Adi Akavia, Andrej Bogdanov, Siyao Guo, Akshay Kamath, and Alon Rosen. "Candidate weak pseudorandom functions in $\mathsf{AC}^0 \circ \mathsf{Mod}_2$". In: *Proceedings of the 5th conference on Innovations in theoretical computer science*. 2014, pp. 251–260 (cit. on p. 5).

[ABK+23] Rahul Arvind, Kishor Bharti, Jun Yong Khoo, Dax Enshan Koh, and Jian Feng Kong. "A quantum tug of war between randomness and symmetries on homogeneous spaces". In: *arXiv preprint arXiv:2309.05253* (2023) (cit. on p. 2).

[AE07] Andris Ambainis and Joseph Emerson. "Quantum t-designs: t-wise independence in the quantum world". In: *Twenty-Second Annual IEEE Conference on Computational Complexity (CCC'07)*. IEEE. 2007, pp. 129–140 (cit. on p. 19).

[AGM18] Gorjan Alagic, Tommaso Gagliardoni, and Christian Majenz. "Unforgeable quantum encryption". In: *Annual international conference on the theory and applications of cryptographic techniques*. Springer. 2018, pp. 489–519 (cit. on pp. 15, 23).

[AGM21] Gorjan Alagic, Tommaso Gagliardoni, and Christian Majenz. "Can you sign a quantum state?" In: *Quantum* 5 (Dec. 2021), p. 603. ISSN: 2521-327X. DOI: 10.22331/q-2021-12-16-603. URL: https://doi.org/10.22331/q-2021-12-16-603 (cit. on p. 23).

[AGQY22] Prabhanjan Ananth, Aditya Gulati, Luowen Qian, and Henry Yuen. "Pseudorandom (Function-Like) Quantum State Generators: New Definitions and Applications". In: *Theory of Cryptography Conference*. Springer. 2022, pp. 237–265 (cit. on p. 3).

[AM17] Gorjan Alagic and Christian Majenz. "Quantum non-malleability and authentication". In: *Advances in Cryptology–CRYPTO 2017: 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20–24, 2017, Proceedings, Part II 37*. Springer. 2017, pp. 310–341 (cit. on pp. 15, 23).

[AMRS20] Gorjan Alagic, Christian Majenz, Alexander Russell, and Fang Song. "Quantum-access-secure message authentication via blind-unforgeability". In: *Advances in Cryptology–EUROCRYPT 2020: 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10–14, 2020, Proceedings, Part III 39*. Springer. 2020, pp. 788–817 (cit. on p. 23).

[AQY22] Prabhanjan Ananth, Luowen Qian, and Henry Yuen. "Cryptography from Pseudorandom Quantum States." In: *CRYPTO*. 2022 (cit. on pp. 2, 3, 25).

[BBD+97] Adriano Barenco, Andre Berthiaume, David Deutsch, Artur Ekert, Richard Jozsa, and Chiara Macchiavello. "Stabilization of quantum computations by symmetrization". In: *SIAM Journal on Computing* 26.5 (1997), pp. 1541–1557 (cit. on pp. 15, 24).

[BBSS23] Amit Behera, Zvika Brakerski, Or Sattath, and Omri Shmueli. "Pseudorandomness with proof of destruction and applications". In: *Cryptology ePrint Archive* (2023) (cit. on pp. 4, 9).

[BCG+02] Howard Barnum, Claude Crépeau, Daniel Gottesman, Adam Smith, and Alain Tapp. "Authentication of quantum messages". In: *The 43rd Annual IEEE Symposium on Foundations of Computer Science, 2002.*

Proceedings. IEEE. 2002, pp. 449–458 (cit. on pp. 15, 22, 23).

[BCH+21] Fernando GSL Brandão, Wissam Chemissany, Nicholas Hunter-Jones, Richard Kueng, and John Preskill. "Models of quantum complexity growth". In: *PRX Quantum* 2.3 (2021), p. 030316 (cit. on p. 8).

[BFV20] Adam Bouland, Bill Fefferman, and Umesh V. Vazirani. "Computational Pseudorandomness, the Wormhole Growth Paradox, and Constraints on the AdS/CFT Duality (Abstract)". In: *11th Innovations in Theoretical Computer Science Conference, ITCS 2020, January 12-14, 2020, Seattle, Washington, USA*. Ed. by Thomas Vidick. Vol. 151. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020, 63:1–63:2. DOI: 10.4230/LIPIcs.ITCS.2020.63 (cit. on p. 2).

[BHH16] Fernando GSL Brandao, Aram W Harrow, and Michał Horodecki. "Local random quantum circuits are approximate polynomial-designs". In: *Communications in Mathematical Physics* 346 (2016), pp. 397–434 (cit. on p. 19).

[BS19] Zvika Brakerski and Omri Shmueli. "(Pseudo) Random Quantum States with Binary Phase". In: *Theory of Cryptography - 17th International Conference, TCC 2019, Nuremberg, Germany, December 1-5, 2019, Proceedings, Part I*. Ed. by Dennis Hofheinz and Alon Rosen. Vol. 11891. Lecture Notes in Computer Science. Springer, 2019, pp. 229–250. DOI: 10.1007/978-3-030-36030-6_10 (cit. on p. 1).

[BS20a] Amit Behera and Or Sattath. "Almost public quantum coins". In: *arXiv preprint arXiv:2002.12438* (2020) (cit. on pp. 15, 24).

[BS20b] Zvika Brakerski and Omri Shmueli. "Scalable Pseudorandom Quantum States". In: *Advances in Cryptology - CRYPTO 2020 - 40th Annual International Cryptology Conference, CRYPTO 2020, Santa Barbara, CA, USA, August 17-21, 2020, Proceedings, Part II*. Ed. by Daniele Micciancio and Thomas Ristenpart. Vol. 12171. Lecture Notes in Computer Science. Springer, 2020, pp. 417–440. DOI: 10.1007/978-3-030-56880-1_15 (cit. on p. 1).

[BZ13] Dan Boneh and Mark Zhandry. "Quantum-secure message authentication codes". In: *Advances in Cryptology–EUROCRYPT 2013: 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013.*

Proceedings 32. Springer. 2013, pp. 592–608 (cit. on p. 23).

[DN02] Ivan Damgård and Jesper Buus Nielsen. "Expanding pseudorandom functions; or: From known-plaintext security to chosen-plaintext security". In: *Annual International Cryptology Conference*. Springer. 2002, pp. 449–464 (cit. on p. 5).

[DNS12] Frédéric Dupuis, Jesper Buus Nielsen, and Louis Salvail. "Actively secure two-party evaluation of any quantum operation". In: *Annual Cryptology Conference*. Springer. 2012, pp. 794–811 (cit. on pp. 15, 22).

[GHMW15] Gus Gutoski, Patrick Hayden, Kevin Milner, and Mark M. Wilde. "Quantum Interactive Proofs and the Complexity of Separability Testing". In: *Theory of Computing* 11.3 (2015), pp. 59–103. DOI: 10.4086/toc.2015.v011a003. URL: https://theoryofcomputing.org/articles/v011a003 (cit. on pp. 15, 24).

[GJMZ23] Sam Gunn, Nathan Ju, Fermi Ma, and Mark Zhandry. "Commitments to quantum states". In: *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*. 2023, pp. 1579–1588 (cit. on pp. 2, 5, 14, 15).

[GLG+23] Andi Gu, Lorenzo Leone, Soumik Ghosh, Jens Eisert, Susanne Yelin, and Yihui Quek. "A little magic means a lot". In: *arXiv preprint arXiv:2308.16228* (2023) (cit. on p. 2).

[GYZ17] Sumegha Garg, Henry Yuen, and Mark Zhandry. "New security notions and feasibility results for authentication of quantum data". In: *Advances in Cryptology–CRYPTO 2017: 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20–24, 2017, Proceedings, Part II 37*. Springer. 2017, pp. 342–371 (cit. on pp. 15, 22, 23).

[Har13] Aram W Harrow. "The church of the symmetric subspace". In: *arXiv preprint arXiv:1308.6595* (2013) (cit. on p. 11).

[HBC+22] Hsin-Yuan Huang, Michael Broughton, Jordan Cotler, Sitan Chen, Jerry Li, Masoud Mohseni, Hartmut Neven, Ryan Babbush, Richard Kueng, John Preskill, et al. "Quantum advantage in learning from experiments". In: *Science* 376.6598 (2022), pp. 1182–1186 (cit. on p. 2).

[HBK23] Tobias Haug, Kishor Bharti, and Dax Enshan Koh. "Pseudorandom unitaries are neither real nor sparse

nor noise-robust". In: *arXiv preprint arXiv:2306.11677* (2023) (cit. on p. 4).

[JLS18] Zhengfeng Ji, Yi-Kai Liu, and Fang Song. "Pseudorandom Quantum States". In: *Advances in Cryptology - CRYPTO 2018 - 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2018, Proceedings, Part III*. Ed. by Hovav Shacham and Alexandra Boldyreva. Vol. 10993. Lecture Notes in Computer Science. Springer, 2018, pp. 126–152. DOI: 10.1007/978-3-319-96878-0_5 (cit. on pp. 1–3, 9, 19, 25).

[KNY08] Masaru Kada, Harumichi Nishimura, and Tomoyuki Yamakami. "The efficiency of quantum identity testing of multiple states". In: *Journal of Physics A: Mathematical and Theoretical* 41.39 (2008), p. 395309 (cit. on pp. 15, 24).

[Kre21] William Kretschmer. "Quantum Pseudorandomness and Classical Complexity". In: *16th Conference on the Theory of Quantum Computation, Communication and Cryptography, TQC 2021, July 5-8, 2021, Virtual Conference*. Ed. by Min-Hsiu Hsieh. Vol. 197. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021, 2:1–2:20. DOI: 10.4230/LIPIcs.TQC.2021.2 (cit. on p. 2).

[LQS+23] Chuhan Lu, Minglong Qin, Fang Song, Penghui Yao, and Mingnan Zhao. "Quantum Pseudorandom Scramblers". In: *arXiv preprint arXiv:2309.08941* (2023) (cit. on pp. 2, 3, 6, 7, 14).

[MY22] Tomoyuki Morimae and Takashi Yamakawa. "Quantum commitments and signatures without one-way functions". In: *CRYPTO*. 2022 (cit. on p. 2).

[Por17] Christopher Portmann. "Quantum authentication with key recycling". In: *Advances in Cryptology–EUROCRYPT 2017: 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30–May 4, 2017, Proceedings, Part III 36*. Springer. 2017, pp. 339–368 (cit. on p. 23).

[Zha12] Mark Zhandry. *Secure Identity-Based Encryption in the Quantum Random Oracle Model*. Cryptology ePrint Archive, Paper 2012/076. https://eprint.iacr.org/2012/076. 2012. URL: https://eprint.iacr.org/2012/076 (cit. on pp. 4, 11).

[Zha16] Mark Zhandry. "A note on quantum-secure PRPs". In: *arXiv preprint arXiv:1611.05564* (2016) (cit. on pp. 4, 11).