A Note on Quantum-Secure PRPs

Mark Zhandry

NTT Research

arXiv:1611.05564v3 [cs.CR] 2 Apr 2025

We show how to construct pseudorandom permutations (PRPs) that remain secure even if the adversary can query the permutation, both in the forward and reverse directions, on a quantum superposition of inputs. Such quantum-secure PRPs have found numerous applications in cryptography and complexity theory. Our construction combines a quantum-secure pseudorandom *function* together with constructions of *classical* format preserving encryption. By combining known results, we show how to construct quantum-secure PRP in this model whose security relies only on the existence of one-way functions.

1 Introduction

Pseudorandom permutations (PRPs), a formalization of block ciphers, are one of the most widely used cryptographic building blocks, as they underlie most symmetric key encryption used today. A PRP is a classical, efficiently computable keyed permutation that looks like a truly random permutation to anyone that is only given oracle access to the function. Additionally, given the key it is also possible to efficiently invert the permutation. A celebrated foundational result is that PRPs can be built from a much weaker tool — a one-way function, which is a classical function that is easy to compute but hard to invert.

Enter quantum computers. In this work, we consider a very strong *quantum* adversary model for PRPs. Namely, we allow the adversary to not only poses a quantum computer, but also make quantum superposition queries to the permutation, both in the forward and reverse direction. Such PRPs are a very natural object in the quantum setting, and have found numerous applications (see Section 1.1 below for examples).

We investigate the following open question raised by Zhandry [Zha12]: whether or not such strong PRPs can still be built from (quantum resistant) one-way functions as in the classical case. We resolve this question positively:

Theorem 1.1. *Assuming quantum resistant one-way functions exist, so do quantum-secure PRPs.*

Theorem 1.1 follows by combining a number of known results. In particular, our main insight is to show that certain constructions of *format-preserving* encryption yield quantum-secure PRPs.

Acknowledgments. We would like to thank Scott Aaronson and Lijie Chen, both for needing a quantum-secure PRP in one of their results and for encouraging us to finally write this paper. Without these motivations, the result would likely have remained unpublished for some time.

1.1 Applications of Quantum PRPs.

To the best of our knowledge, the first proposed applications of quantum-secure PRPs are symmetric-key encryption secure in a strong quantum query model by Gagliardoni, Hülsing, and Schaffner [GHS16], and an efficient oracle separation for SZK and BQP by Aaronson and Chen [AC17].

Subsequent to initially making our work public, quantum PRPs have been used in a number of important applications. Cryptographic applications include those of Zhandry [Zha21] for analyzing

Mark Zhandry: mzhandry@gmail.com, This paper was initially written while at Princeton University, but the idea had been in my head since I was a PhD student at Stanford University.

the post-quantum security of the Sponge hash function, and of Bos, Hülsing, Renes, and van Vredendaal [BHRvV21] to study the post-quantum security of the XMSS signature scheme.

Quantum-secure PRPs have been used in a number of works on quantum pseudorandomness. For example, Behera, Brakerski, Sattath, and Shmueli [BBSS23] use quantum-secure PRPs to construct pseudorandomness with proofs of deletion and Lu, Qin, Song, Yao, and Zhao [LQS+25] use them to construct pseudorandom scramblers. Aaronson et al. [ABF+24], Giurgica-Tiron and Bouland [GTB23], and Arnon-Friedman, Brakerski, and Vidick [AFBV23] use such PRPs to study quantum pseudo-entanglement. Chia and Hung [CH22] use quantum-secure PRPs to classically verify quantum depth. They were recently used by Ananth, Gulati, Kaleoglu, and Lin [AGKL24] to construct pseudorandom isometries. Finally, in a very recent breakthrough work, quantum-secure PRPs were used by Huang and Ma [MH25] to construct pseudorandom unitaries. Through our work, these results can all be based on quantum-immune one-way functions.

1.2 Other Related Work

Superposition security. When considering classical cryptosystems in the quantum setting, one option is to keep the classical security experiment, but allow the adversary local quantum computation. A stronger security notion, however, is to update the security experiment itself to allow quantum queries. Such a stronger notion captures a wider class of attacks, and is often necessary if the protocol is to be used as part of a higher-level quantum protocol.

There have been numerous works considering such superposition security models. The previously mentioned work of [Zha12] considers the case of quantum-secure pseudorandom *functions*. Other examples include MPC [DFNS14, ECKM20, LSZ20], message authentication/signatures [BZ13a, BZ13b, KLLN16, GYZ17], and encryption [BZ13b, BJ15, GHS16, AMRS20].

Quantum security of PRPs. The quantum security of Feistel networks remains a largely open, very challenging problem. Kuwakado and Morii [KM10] show that 3-round Feistel is insecure under forward-only quantum queries, in contrast to the classical setting where 3 rounds employing a suitable round function *is* sufficient [LR88]. Hosoyamada and Iwata [HI19] claimed to prove that 4-round Feistel is quantum-secure under forward-only quantum queries, but it was very recently discovered that there was a bug in their proof [BCEJ24]. For non-adaptive forward-only queries, [BCEJ24] show that 4-round Feistel is still secure, but the adaptive query setting remains open. There are no positive results for Feistel networks in any number of rounds when allowing reverse queries. Our result remains the only provably secure PRP allowing inverse queries.

Subsequent to the initial publication of our work, [Son17] sketched in a blog post how to construct quantum-secure PRPs using the rapid mixing of the Thorpe shuffle. Their main idea and construction are a special case of Theorem 1.1: namely, the rapid mixing of the Thorpe shuffle gives a format preserving encryption scheme sufficient for realizing quantum-secure PRPs.

1.3 Our Techniques

On adapting the classical approach. The classical blueprint for constructing PRPs from one-way functions is usually described as follows.

- Håstad, Impagliazzo, Levin, and Luby [HILL99] show how to use one-way functions to build pseudorandom generators (PRGs).
- In turn, Goldreich, Goldwasser, and Micali [GGM86] show how to use pseudorandom generators to build pseudorandom functions (PRFs), which are a relaxed notion of PRPs where the function is not required to be a permutation[1].
- Finally, Luby and Rackoff [LR88] show that by plugging PRFs into a 3-round (respectively 4-round) Feistel Network, one obtains a PRP secure for forward-only queries (resp. forward and inverse queries).

[1] There is also no efficient inverse function.

The obvious idea for constructing a quantum-secure PRP is to try to "upgrade" each step above to work quantumly:

- **Quantum immune one-way functions to quantum immune PRGs.** Fortunately, the classical proof of security in [HILL99] can be lifted to the quantum setting. Intuitively, the classical security proof does not make any assumptions about the model of the adversary, and so works equally well when the adversary is classical or quantum. This result seems to be folklore, but is mentioned in [Aar09, AC12, Zha12].

- **Quantum immune PRGs to quantum-secure PRFs.** Here, unfortunately, the classical model *does* restrict the model of the adversary, as the adversary's queries are assumed to be classical in the classical proof. The classical proof in [GGM86] crucially uses the fact that the adversary only sees a polynomial number of *classical* evaluations of the function. It is therefore no longer valid for proving security against quantum queries, who see superpositions over exponentially-many points. Fortunately, Zhandry [Zha12] gives a new and very different proof that does show the security of the GGM PRF against quantum algorithms making quantum queries.

- **Quantum-secure PRFs to quantum-secure PRPs.** Here again the classical model restricts the model of the adversary, so the classical proof in [LR88] is no longer valid. The classical security proof works as follows. In the first step, the PRF in the Feistel network is replaced with a truly random function. If we allow quantum queries to the PRP, we will need the PRF to be secure against quantum queries, but otherwise translating this step to the quantum setting is straightforward. The next step, however, is problematic. The next step is to show that the Feistel network, when instantiated with a truly random function, becomes indistinguishable from a truly random permutation. Unfortunately, as with the GGM security proof above, the proof in the classical setting crucially relies on the fact that the adversary only ever gets to see a polynomial number of points, and completely breaks down if the adversary gets to "see" all exponentially many points. As shown by Kuwakado and Morii [KM10], the 3-round Feistel network is insecure under quantum queries to only the forward directly, despite 3-rounds being sufficient for classical forward queries. It is entirely possible that with more rounds Feistel networks become indisitnguishable from random permutation under quantum queries, but no quantum security proof for Feistel networks is known[2], and any result along these lines would likely require a substantial reworking of Luby and Rackoff's analysis.

We will therefore devise a new approach to solving the third step above. Our construction is a simple combination of prior work. At a very high level, in any construction of a PRP from a PRF (quantum-secure or otherwise), the first step to prove security is to replace the PRF with a truly random function, invoking PRF security to show that change is indistinguishable. The second step is to take the resulting random object, and show that it "looks like" a truly random permutation. Importantly, this second step no longer utilizes the adversary's computational bounds, only the implied bounds on the number of queries. Essentially, what [LR88] show is that Feistel networks "look like" random permutations to algorithms making a bounded number of classical queries.

An analogous quantum statement for Feistel networks requires making query complexity arguments that seem beyond the reach of current techniques. Our key insight is that, in the second step, if the *truth table* of the permutation (using a truly random function in place of the PRF) is statistically close to that of a random permutation, then this suffices for quantum security, even in the presence of quantum adversaries. Equivalently, if the construction (after replacing the PRF with a truly random function) is indistinguishable against algorithms that make *classical* queries, but are allowed to query the *entire domain*, then quantum security follows. Note that for this insight, it is crucial that we consider the information-theoretic object obtained by replacing the round-function PRF with a truly random function. Indeed, prior to replacing the PRF, the truth table *cannot* look like a uniform permutation since there is not nearly enough entropy in the PRP key.

"Full domain" security is extremely strong, and it is well-known that the basic balanced Feistel networks such analyzed in [LR88] do not achieve such security. Indeed, a k-round Feistel network on n bits consists of k independent random "round" functions from $n/2$ bits to $n/2$ bits. After replacing

[2]See Related Works below in Section 1.2.

the round functions with truly random functions, each round function has $(n/2) \times 2^{n/2}$ bits of entropy. The total entropy of the network is therefore at most $k \times (n/2)2^{(n/2)}$. On the other hand a random permutation will have roughly $n \times 2^n$ bits of entropy, far more than a k round network can have for any polynomial k.

Fortunately, full domain PRPs have been widely studied in classical cryptography, under completely different motivations, namely in the context of *format preserving encryption* [BRRS09]. A core tool in format preserving encryption is a PRP where the domain can be very small, possibly even polynomial. The challenge here is that, once the domain is polynomial, a polynomial-time adversary can query the function on the entire domain. For this reason, the balanced Feistel network cannot work in this regime, since they *cannot* maintain security once queried on the entire domain. A fascinating line of work [Mor05, GP07, BRRS09, SS12, HMR12, RY13, MR14] has shown how to build PRPs that (1) support small potentially polynomial-sized domains, and (2) support adversaries querying on the entire domain. By plugging in these results, we obtain a quantum-secure PRP from any quantum-secure PRF, and hence from any one-way function.

Now, in these works, since the domain is small, the overall construction can remain polynomial-time even if the run-time has a rather poor dependence on the domain size. Thus, small-domain full-domain PRPs are not necesarily enough to give large-domain quantum-secure PRPs. However, in the interest of achieving practical constructions, the above sequence of works has shown that the dependence of the run-time on the domain size can be made essentially logarithmic. Thus, we can "scale up" these constructions to the case of exponentially-large domains (that is, polynomial bit-length), and achieve a PRP secure against quantum queries even in the large-domain case, and the run-time remains polynomial.

2 Preliminaries

A function $\epsilon = \epsilon(\lambda)$ is negligible if it is smaller than any inverse polynomial. A *classical* algorithm is said to be efficient if it runs in probabilistic polynomial time.

This work will make minimal use of quantum formalism. Nonetheless, for completeness we recall the basics of quantum computation and quantum oracle queries. The following is taken more or less verbatim from [BZ13b].

Quantum Computation. We give a short introduction to quantum computation. A quantum system A is a complex Hilbert space $\mathcal{H}$ together with and inner product $\langle \cdot | \cdot \rangle$. The state of a quantum system is given by a vector $|\psi\rangle$ of unit norm ($\langle \psi | \psi \rangle = 1$). Given quantum systems $\mathcal{H}_1$ and $\mathcal{H}_2$, the joint quantum system is given by the tensor product $\mathcal{H}_1 \otimes \mathcal{H}_2$. Given $|\psi_1\rangle \in \mathcal{H}_1$ and $|\psi_2\rangle \in \mathcal{H}_2$, the product state is given by $|\psi_1\rangle|\psi_2\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$. Given a quantum state $|\psi\rangle$ and an orthonormal basis $B = \{|b_0\rangle, ..., |b_{d-1}\rangle\}$ for $\mathcal{H}$, a measurement of $|\psi\rangle$ in the basis B results in the value i with probability $|\langle b_i | \psi \rangle|^2$, and the quantum state collapses to the basis vector $|b_i\rangle$. If $|\psi\rangle$ is actually a state in a joint system $\mathcal{H} \otimes \mathcal{H}'$, then $|\psi\rangle$ can be written as

$$|\psi\rangle = \sum_{i=0}^{d-1} \alpha_i \, |b_i\rangle |\psi_i'\rangle$$

for some complex values α_i and states $|\psi_i'\rangle$ over $\mathcal{H}'$. Then, the measurement over $\mathcal{H}$ obtains the value i with probability $|\alpha_i|^2$ and in this case the resulting quantum state is $|b_i\rangle|\psi_i'\rangle$.

A unitary transformation over a d-dimensional Hilbert space $\mathcal{H}$ is a $d \times d$ matrix $\mathbf{U}$ such that $\mathbf{U}\mathbf{U}^\dagger = \mathbf{I}_d$, where $\mathbf{U}^\dagger$ represents the conjugate transpose. A quantum algorithm operates on a product space $\mathcal{H}_{in} \otimes \mathcal{H}_{out} \otimes \mathcal{H}_{work}$ and consists of n unitary transformations $\mathbf{U}_1, ..., \mathbf{U}_n$ in this space. $\mathcal{H}_{in}$ represents the input to the algorithm, $\mathcal{H}_{out}$ the output, and $\mathcal{H}_{work}$ the work space. A classical input x to the quantum algorithm is converted to the quantum state $|x, 0, 0\rangle$. Then, the unitary transformations are applied one-by-one, resulting in the final state

$$|\psi_x\rangle = \mathbf{U}_n ... \mathbf{U}_1 |x, 0, 0\rangle \ .$$

The final state is then measured, obtaining the tuple (a, b, c) with probability $|\langle a, b, c | \psi_x \rangle|^2$. The output of the algorithm is b. We say that a quantum algorithm is efficient if each of the unitary matrices

$\mathbf{U}_i$ come from some fixed basis set, and n, the number of unitary matrices, is polynomial in the size of the input.

Quantum-accessible Oracles. We will implement an oracle $O : \mathcal{X} \to \mathcal{Y}$ by a unitary transformation $\mathbf{O}$ where

$$\mathbf{O}|x, y, z\rangle = |x, y + O(x), z\rangle$$

where $+ : \mathcal{X} \times \mathcal{X} \to \mathcal{X}$ is some group operation on $\mathcal{X}$. Suppose we have a quantum algorithm that makes quantum queries to oracles $O_1, ..., O_q$. Let $|\psi_0\rangle$ be the input state of the algorithm, and let $\mathbf{U}_0, ..., \mathbf{U}_q$ be the unitary transformations applied between queries. Note that the transformations $\mathbf{U}_i$ are themselves possibly the products of many simpler unitary transformations. The final state of the algorithm will be

$$\mathbf{U}_q\mathbf{O}_q...\mathbf{U}_1\mathbf{O}_1\mathbf{U}_0|\psi_0\rangle \ .$$

We can also have an algorithm make classical queries to O_i. In this case, the input to the oracle is measured before applying the transformation $\mathbf{O}_i$. We call a quantum oracle algorithm efficient if the number of queries q is a polyomial, and each of the transformations $\mathbf{U}_i$ between queries can be written as the product polynomially many unitary transformations from some fixed basis set.

Conventions for this paper. For this paper, all cryptographic primitives discussed will be implemented by efficient *classical* algorithms. We will use $\mathsf{ClassicComp}$ and $\mathsf{QuantComp}$ to distinguish between classical and quantum adversaries, and we will use $\mathsf{ClassicQuery}$ and $\mathsf{QuantQuery}$ to distinguish between adversaries making classical or quantum queries.

2.1 Cryptographic Primitives

All algorithms and adversaries will take as input a security parameter λ. We will use the convention that λ is specified in binary, and algorithms are efficient if they run in time polynomial in λ (which is exponential in the bit-length of λ).

Definition 2.1. A $\mathsf{ClassicComp}$- (resp. $\mathsf{QuantComp}$-) *one-way* function is an efficient classical function $\mathsf{OWF} : \{0,1\}^\lambda \to \{0,1\}^*$ such that, for any efficient classical (resp. quantum) adversary $\mathcal{A}$, the probability that $\mathcal{A}$ inverts OWF on a random input is negligible. That is, there exists a negligible $\mathsf{negl}(\lambda)$ such that

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

Definition 2.2. For a pair $(\mathsf{Comp}, \mathsf{Query}) \in \{(\mathsf{ClassicComp}, \mathsf{ClassicQuery}), (\mathsf{QuantComp}, \mathsf{ClassicQuery}), (\mathsf{QuantComp}, \mathsf{QuantQuery})\}$,[3] A $(\mathsf{Comp}, \mathsf{Query})$-*pseudorandom function* (PRF), is a family of efficient classical functions $\mathsf{PRF}_{m,n} : \{0,1\}^\lambda \times \{0,1\}^m \to \{0,1\}^n$ such that the following holds. For any polynomially bounded $m = m(\lambda)$ and $n = n(\lambda)$, and any efficient adversary $\mathcal{A}$, $\mathcal{A}$ cannot distinguish $\mathsf{PRF}_{m,n}(k, \cdot)$ for a random $k \leftarrow \{0,1\}^\lambda$ from a truly random function $O : \{0,1\}^m \to \{0,1\}^n$. That is, there exists a negligible $\mathsf{negl}(\lambda)$ such that

$$\left|\Pr[\mathcal{A}^{\mathsf{PRF}_{m,n}(k,\cdot)}(\lambda) = 1 : k \leftarrow \{0,1\}^\lambda] - \Pr[\mathcal{A}^{O(\cdot)}(\lambda) = 1]\right| < \mathsf{negl}(\lambda) \ .$$

Here, O is chosen at random from the set of all functions from $\{0,1\}^m$ into $\{0,1\}^n$. If $(\mathsf{Comp}, \mathsf{Query}) = (\mathsf{ClassicComp}, \mathsf{ClassicQuery})$, $\mathcal{A}$ is restricted to being an efficient classical algorithm making classical queries to O. If $\mathsf{Comp} = \mathsf{QuantComp}$, then $\mathcal{A}$ is allowed to be a quantum algorithm. In this case, if $\mathsf{Query} = \mathsf{ClassicQuery}$, $\mathcal{A}$, despite being quantum, is still required to make classical queries. If $\mathsf{Query} = \mathsf{QuantQuery}$, $\mathcal{A}$ is allowed to make quantum queries to O.

We will often abuse notation when m and n are clear from context and write PRF to denote $\mathsf{PRF}_{m,n}$.

[3] Note that it does not make sense to consider classical adversary's that make quantum queries.

We note that PRFs domains and co-domains are *monotone*, in the sense that a PRF on for large domain and range gives a PRF for small domain and range, simply by hard-coding some bits of the inputs and discarding some bits of the output. Therefore, if a PRF is secure for large domain/range sizes (say, polynomial m and n), it can also easily be made secure for small domain and range sizes (say, logarithmic or polylogarithmic m and n).

We recall the following theorem, combining the results [GGM86, HILL99, Zha12].

Theorem 2.3 (Combination of [GGM86, HILL99, Zha12])**.** *If* $\mathsf{ClassicComp}$*-one-way functions exist, then so do* $(\mathsf{ClassicComp}, \mathsf{ClassicQuery})$*-PRFs. Moreover, if* $\mathsf{QuantComp}$*-one-way functions exist, then so do* $(\mathsf{QuantComp}, \mathsf{QuantQuery})$*-PRFs.*

The classical version follows from [GGM86, HILL99]. The reductions in those works are actually independent of the computational model, so the proofs also show that $\mathsf{QuantComp}$-one-way functions imply $(\mathsf{QuantComp}, \mathsf{ClassicQuery})$-PRFs. The analysis does not extend to the $\mathsf{QuantQuery}$ setting. Instead, the work of [Zha12] shows how to modify the proof to get the quantum part of Theorem 2.3.

3 Pseudorandom Permutations

Definition 3.1. For a pair $(\mathsf{Comp}, \mathsf{Query}) \in \{(\mathsf{ClassicComp}, \mathsf{ClassicQuery}), (\mathsf{QuantComp}, \mathsf{ClassicQuery}), (\mathsf{QuantComp}, \mathsf{QuantQuery})\}$ and $\mathsf{Dom} \in \{\mathsf{LargeDom}, \mathsf{AnyDom}\}$, a $(\mathsf{Comp}, \mathsf{Query}, \mathsf{Dom})$-*pseudorandom permutation* (PRP), is a family of efficient classical function pairs $\mathsf{PRP}_o : \{0,1\}^\lambda \times \{0,1\}^o \to \{0,1\}^o$ and $\mathsf{PRP}_o^{-1} : \{0,1\}^\lambda \times \{0,1\}^o \to \{0,1\}^o$ such that the following holds.

- First, for every key k and integer o, the functions $\mathsf{PRP}_o(k,\cdot)$ and $\mathsf{PRP}_o^{-1}(k,\cdot)$ are inverses of each other. That is, $\mathsf{PRP}_o^{-1}(k, \mathsf{PRP}_o(k,x)) = x$ for all o, k, x. This implies that $\mathsf{PRP}_o(k,\cdot)$ is a permutation.
- Second, for any polynomially-bounded $o = o(\lambda)$ and any efficient adversary $\mathcal{A}$, $\mathcal{A}$ cannot distinguish $\mathsf{PRP}_o(k,\cdot)$ for a random $k \leftarrow \{0,1\}^\lambda$ from a truly random *permutation* $P : \{0,1\}^o \to \{0,1\}^o$. We consider the strong variant where $\mathcal{A}$ has access to both P and P^{-1}. That is, there exists a negligible $\mathsf{negl}(\lambda)$ such that

$$\left|\Pr[\mathcal{A}^{\mathsf{PRP}_o(k,\cdot),\mathsf{PRP}_o^{-1}(k,\cdot)}(\lambda) = 1 : k \leftarrow \{0,1\}^\lambda] - \Pr[\mathcal{A}^{P(\cdot),P^{-1}(\cdot)}(\lambda) = 1]\right| < \mathsf{negl}(\lambda) \ .$$

  Here, P is chosen at random from the set of all permutations on $\{0,1\}^o$. If $(\mathsf{Comp}, \mathsf{Query}) = (\mathsf{ClassicComp}, \mathsf{ClassicQuery})$, $\mathcal{A}$ is restricted to being an efficient classical algorithm making classical queries to P, P^{-1}. If $\mathsf{Comp} = \mathsf{QuantComp}$, then $\mathcal{A}$ is allowed to be a quantum algorithm. In this case, if $\mathsf{Query} = \mathsf{ClassicQuery}$, $\mathcal{A}$, despite being quantum, is still required to make classical queries. If $\mathsf{Query} = \mathsf{QuantQuery}$, $\mathcal{A}$ is allowed to make quantum queries to P, P^{-1}.
- Finally, if $\mathsf{Dom} = \mathsf{LargeDom}$, we only require security to hold for o that are upper- and lower-bounded by a polynomial. If $\mathsf{Dom} = \mathsf{AnyDom}$, we allow for arbitrary polynomially-upper-bounded o (so o could be, for example, logarithmic in this case). Note that a PRP for domain $\{0,1\}^o$ does not give a PRP for domain $\{0,1\}^{o'}$ for $o' < o$ by fixing bits, since PRP_o is not guaranteed to be a permutation on $\{0,1\}^{o'}$. Therefore, we make a distinction between PRPs that only work for sufficiently large domains ($\mathsf{LargeDom}$), and those that remain secure for both large and small domains (AnyDom).

We will often abuse notation when o is clear from context and write PRP to denote PRP_o.

3.1 Function to Permutation Converters

In this section, we define a information theoretic object called a *function to permutation converter* (FPC), which roughly takes a random function and transforms it into a random permutation. Such FPCs are implicitly used in many constructions of PRPs, and basically every construction of a PRP from general one-way functions.

Definition 3.2. Let $\mathsf{Query} \in \{\mathsf{ClassicQuery}, \mathsf{QuantQuery}\}$, $\mathsf{Dom} \in \{\mathsf{LargeDom}, \mathsf{AnyDom}\}$. Fix a family $\mathcal{Q}$ of functions over o, λ. An $(\mathsf{Query}, \mathsf{Dom}, \mathcal{Q})$-FPC is a sequence of pairs of efficient classical oracle algorithms $\mathsf{F}_o, \mathsf{R}_o$ where:

- $\mathsf{F}_o, \mathsf{R}_o$ take as input λ and string $x \in \{0,1\}^o$, and output a string $y \in \{0,1\}^o$
- There exist polynomials $m(o,\lambda), n(o,\lambda)$ such that $\mathsf{F}_o, \mathsf{R}_o$ make queries to a function $O : \{0,1\}^m \to \{0,1\}^n$.
- $\mathsf{F}_o, \mathsf{R}_o$ are efficient, running in time $\mathsf{poly}(o,\lambda)$. In particular, they make at most $\mathsf{poly}(o,\lambda)$ queries to O.
- $\mathsf{F}_o, \mathsf{R}_o$ are inverses: $\mathsf{R}_o^O(\lambda, \mathsf{F}_o^O(\lambda, x)) = x$ for all $x \in \{0,1\}^o$ and all oracles O.
- $\mathsf{F}_o, \mathsf{R}_o$ are indistinguishable from a random permutation and its inverse, given query access. That is, let $o(\lambda)$ be any polynomially bounded function. If $\mathsf{Dom} = \mathsf{LargeDom}$, we will restrict to o being lower-bounded by a polynomial as well. Let $q(\lambda) = q(o(\lambda), \lambda)$ be any function in $\mathcal{Q}$. Let $\mathcal{A}$ be any (possibly inefficient) adversary that makes at most q queries to its oracles, where if $\mathsf{Query} = \mathsf{QuantQuery}$ the queries are allowed to quantum, and if $\mathsf{Query} = \mathsf{ClassicQuery}$, the queries are restricted to being classical. Then there exists a negligible $\mathsf{negl}(\lambda)$ such that:

$$\left|\Pr[\mathcal{A}^{\mathsf{F}_o^O(\lambda,\cdot),\mathsf{R}_o^O(\lambda,\cdot)}(\lambda) = 1] - \Pr[\mathcal{A}^{P,P^{-1}}(\lambda) = 1]\right| < \mathsf{negl}(\lambda) \ .$$

3.2 The Main Lemma

Here we prove that FPCs are sufficient to build PRPs.

Lemma 3.3. *Let $\mathcal{Q}$ be the set of all polynomials. If* $(\mathsf{Comp}, \mathsf{Query})$*-PRFs exist and* $(\mathsf{Query}, \mathsf{Dom}, \mathcal{Q})$*-FPCs exist, then* $(\mathsf{Comp}, \mathsf{Query}, \mathsf{Dom})$*-PRPs exist.*

We note that the $(\mathsf{Comp}, \mathsf{Query}, \mathsf{Dom}) = (\mathsf{ClassicComp}, \mathsf{ClassicQuery}, \mathsf{Dom})$ version of this lemma is implicit in essentially all constructions of classically secure PRPs from general PRFs. The proof is a straightforward adaptation to handle quantum queries.

Proof. We prove the $(\mathsf{QuantComp}, \mathsf{QuantQuery}, \mathsf{AnyDom})$ version, the other versions being similar. The construction is simple: $\mathsf{PRP}_o(k,x) = \mathsf{F}_o^{\mathsf{PRF}_{m,n}(k,\cdot)}(\lambda, x)$ and $\mathsf{PRP}_o^{-1}(k,x) = \mathsf{R}_o^{\mathsf{PRF}_{m,n}(k,\cdot)}(\lambda, x)$ where $\lambda = |k|$.

Security is proved by a sequence of hybrids.

Hybrid 0. This is the case where the adversary is given the oracles $P(x) = \mathsf{F}_o^{\mathsf{PRF}_{m,n}(k,\cdot)}(\lambda, x)$ and $P^{-1}(x) = \mathsf{R}_o^{\mathsf{PRF}_{m,n}(k,\cdot)}(\lambda, x)$.

Hybrid 1. In this case, we switch PRF to be random, so that the adversary is given the oracles $P(x) = \mathsf{F}_o^{O(\cdot)}(\lambda, x)$ and $P^{-1}(x) = \mathsf{R}_o^{O(\cdot)}(\lambda, x)$ for a random function $O : \{0,1\}^m \to \{0,1\}^n$.

Suppose $\mathcal{A}$ distinguishes **Hybrid 0** from **Hybrid 1** with non-negligible probability. Then we can construct a PRF adversary $\mathcal{B}^O(\lambda) = \mathcal{A}^{\mathsf{F}_o^O(\lambda,\cdot),\mathsf{R}_o^O(\lambda,\cdot)}(\lambda)$. If $O(\cdot) = \mathsf{PRF}_{m,n}(k,\cdot)$ for a random k, then the view of $\mathcal{A}$ is identical to **Hybrid 0**. Likewise, if $O(\cdot)$ is a truly random function, then the view of $\mathcal{A}$ is identical to **Hybrid 1**. Moreover, $\mathcal{B}$ can answer any quantum query made by $\mathcal{A}$ by making a polynomial number of quantum queries to its own oracle. Therefore, $\mathcal{B}$ is an efficient quantum algorithm. Moreover, its advantage in breaking the security of PRF is identical to $\mathcal{A}$'s distinguishing advantage between **Hybrid 0** and **Hybrid 1**. This contradicts our assumption that PRF is $(\mathsf{QuantComp}, \mathsf{QuantQuery})$ secure.

Therefore, **Hybrid 0** and **Hybrid 1** are indistinguishable, except with negligible probability.

Hybrid 2. In this hybrid, the adversary is given truly random permutation oracles P, P^{-1}. Indistinguishability between **Hybrid 1** and **Hybrid 2** follows immediately from the $(\mathsf{QuantQuery}, \mathsf{AnyDom}, \mathcal{Q})$ security of F, R.

Thus, **Hybrid 0** and **Hybrid 2** are indistinguishable, demonstrating the security of PRP. □

3.3 Constructions of FPCs

From Theorem 2.3, we already have PRFs from one-way functions. It remains to demonstrate a suitable FPC. Luby and Rackoff's [LR88] proof essentially shows the following:

Lemma 3.4 (Implicit in [LR88])**.** *Let $\mathcal{Q}$ be the set of polynomial-bounded functions. Then* (ClassicQuery, LargeDom, $\mathcal{Q}$)*-FPCs exist.*

This gives us the following corollary, showing that (large-domain) PRPs secure against classical queries exist:

Corollary 3.5. *For* Comp $\in \{$ClassicComp, QuantComp$\}$*, if* Comp*-one-way functions exist, then* (Comp, ClassicQuery, LargeDom)*-PRPs exist.*

Proof. Assuming Comp-one-way functions exist, by Theorem 2.3, so do (Comp, ClassicQuery)-PRFs. Lemma 3.4 shows the existence of (ClassicQuery, LargeDom, $\mathcal{Q}$)-FPCs, where $\mathcal{Q}$ is the set of polynomially-bounded functions. Plugging the PRF and FPC into Lemma 3.3 with Query = ClassicQuery and Dom = LargeDom then gives the desired (Comp, ClassicQuery, LargeDom)-PRPs. □

Luby Rackoff's construction uses Feistel networks. If we could show that Feistel networks are also (QuantQuery, LargeDom, $\mathcal{Q}$)-FPCs, then we would immediately get (QuantComp, QuantQuery, LargeDom)-PRPs from any QuantComp-one-way function as desired. Unfortunately, we do not know how to show this. It is known that more rounds are necessary than in the classical setting [KM10], but it is unknown whether any number of rounds are sufficient quantumly. We therefore leave the quantum security of the Feistel network as an important open question.

Instead, we observe that if $q = 2^o$, then even a classical algorithm can query the entire domain of F_o, obtaining the entire truth table for the function (as well as its inverse R_o). Then it can simulate any query, quantum or otherwise. Thus, in this regime, there is no distinction between classical and quantum FPCs. Note that this regime still makes sense even though an adversary making 2^o queries is inefficient, since FPC security is defined for computationally unbounded adversaries. This motivates the following definition:

Definition 3.6. The family $(\mathsf{F}_o, \mathsf{R}_o)$ is a Dom-Full Domain FPC if there exists a set $\mathcal{Q}$ containing a function $q(o, \lambda)$ such that $q(o, \lambda) \geq 2^o$, such that $(\mathsf{F}_o, \mathsf{R}_o)$ is a (ClassicQuery, Dom, $\mathcal{Q}$)-FPC.

Lemma 3.7. *Any* Dom*-Full Domain FPC is also a* (QuantQuery, Dom, $\mathcal{Q}$)*-FPC, for* any *class of functions* $\mathcal{Q}$*.*

Proof. Let $\mathcal{A}$ be any (possibly inefficient) algorithm making quantum queries to a Dom-Full Domain FPC, and consider the quantity

$$\epsilon(\lambda) := \left|\Pr[\mathcal{A}^{\mathsf{F}_o^O(\lambda,\cdot),\mathsf{R}_o^O(\lambda,\cdot)}(\lambda) = 1] - \Pr[\mathcal{A}^{P,P^{-1}}(\lambda) = 1]\right| \ .$$

Our goal is to show that ϵ must be negligible, regardless of how many (quantum) queries $\mathcal{A}$ makes. Now let $\mathcal{B}$ be the following inefficient classical query algorithm: using 2^o queries, it queries the entire domain of its oracle. $\mathcal{B}$ then uses the query responses to build the truth table T for its oracle. It then runs $\mathcal{A}^{T,T^{-1}}$, where the oracle T is a quantum-accessible classical oracle defined by the truth table T, and T^{-1} is its (quantumly-accessible) inverse. $\mathcal{B}$ outputs whatever $\mathcal{A}$ outputs. The oracle T seen by $\mathcal{A}$ is exactly the same as the oracle seen by $\mathcal{B}$. Hence, we have that

$$\left|\Pr[\mathcal{B}^{\mathsf{F}_o^O(\lambda,\cdot),\mathsf{R}_o^O(\lambda,\cdot)}(\lambda) = 1] - \Pr[\mathcal{B}^{P,P^{-1}}(\lambda) = 1]\right| = \epsilon(\lambda) \ .$$

Since Dom-Full Domain security applies to algorithms making 2^o queries, and hence applies to $\mathcal{B}$, we have that ϵ is negligible, as desired. □

Next, we observe that the card shuffles at the heart of constructions of format preserving encryption give us Full-Domain FPCs. The following is adapted from [Mor05, GP07, SS12, HMR12, RY13, MR14].

Lemma 3.8 (Implicit in [Mor05, GP07, SS12, HMR12, RY13, MR14])**.** AnyDom*-Full Domain FPCs exist.*

The main difference between these various works is how efficient the constructions are. The goal of these works is to use Lemma 3.8 to give the following improvement to Corollary 3.5, namely achieving security for arbitrary domains, which we adapt here:

Corollary 3.9. *For* $\mathsf{Comp} \in \{\mathsf{ClassicComp}, \mathsf{QuantComp}\}$*, if* Comp*-one-way functions exist, then* $(\mathsf{Comp}, \mathsf{ClassicQuery}, \mathsf{AnyDom})$*-PRPs exist.*

Proof. The proof is identical to Corollary 3.5, but with with $\mathsf{LargeDom}$ replaced with AnyDom and Lemma 3.4 replaced with Lemma 3.8. □

3.4 Putting it All Together

Combining Theorem 2.3 with Lemmas 3.3, 3.7, and 3.8, quantum-secure PRPs exist, giving a slightly more precise version of Theorem 1.1:

Theorem 3.10. *If* $\mathsf{QuantComp}$*-one-way functions exist, then so do* $(\mathsf{QuantComp}, \mathsf{QuantQuery}, \mathsf{AnyDom})$*-PRPs.*

Proof. Assuming $\mathsf{QuantComp}$-one-way functions exist, by Theorem 2.3, so do $(\mathsf{QuantComp}, \mathsf{QuantQuery})$-PRFs. Lemma 3.8 shows the existence of AnyDom-Full Domain FPCs, which by Lemma 3.7 are also $(\mathsf{QuantQuery}, \mathsf{Dom}, \mathcal{Q})$-FPCs for any class of functions $\mathcal{Q}$; therefore set $\mathcal{Q}$ to be the set of all polynomials. Plugging the PRF and FPC into Lemma 3.3 with $\mathsf{Query} = \mathsf{QuantQuery}$ and $\mathsf{Dom} = \mathsf{AnyDom}$ then gives the desired $(\mathsf{QuantComp}, \mathsf{QuantQuery}, \mathsf{AnyDom})$-PRPs. □

References

[Aar09] Scott Aaronson. Quantum Copy-Protection and Quantum Money. *Proceedings of the 24th Annual IEEE Conference on Computaitonal Complexity (CCC)*, 2009. https://doi.org/10.1109/CCC.2009.42.

[ABF+24] Scott Aaronson, Adam Bouland, Bill Fefferman, Soumik Ghosh, Umesh V. Vazirani, Chenyi Zhang, and Zixin Zhou. Quantum pseudoentanglement. In Venkatesan Guruswami, editor, *ITCS 2024: 15th Innovations in Theoretical Computer Science Conference*, volume 287, pages 2:1–2:21, Berkeley, CA, USA, January 30 – February 2, 2024. Leibniz International Proceedings in Informatics (LIPIcs). https://doi.org/10.4230/LIPIcs.ITCS.2024.2.

[AC12] Scott Aaronson and Paul Christiano. Quantum money from hidden subspaces. In Howard J. Karloff and Toniann Pitassi, editors, *44th Annual ACM Symposium on Theory of Computing*, pages 41–60, New York, NY, USA, May 19–22, 2012. ACM Press. https://doi.org/10.1145/2213977.2213983.

[AC17] Scott Aaronson and Lijie Chen. Complexity-theoretic foundations of quantum supremacy experiments. In *Proceedings of the 32nd Computational Complexity Conference*, CCC '17, Dagstuhl, DEU, 2017. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik. https://doi.org/10.4230/LIPIcs.CCC.2017.22.

[AFBV23] Rotem Arnon-Friedman, Zvika Brakerski, and Thomas Vidick. Computational entanglement theory, 2023. https://arxiv.org/abs/2310.02783.

[AGKL24] Prabhanjan Ananth, Aditya Gulati, Fatih Kaleoglu, and Yao-Ting Lin. Pseudorandom isometries. In Marc Joye and Gregor Leander, editors, *Advances in Cryptology – EUROCRYPT 2024, Part IV*, volume 14654 of *Lecture Notes in Computer Science*, pages 226–254, Zurich, Switzerland, May 26–30, 2024. Springer, Cham, Switzerland. https://doi.org/10.1007/978-3-031-58737-5_9.

[AMRS20] Gorjan Alagic, Christian Majenz, Alexander Russell, and Fang Song. Quantum-access-secure message authentication via blind-unforgeability. In Anne Canteaut and Yuval Ishai, editors, *Advances in Cryptology – EUROCRYPT 2020, Part III*, volume 12107 of *Lecture Notes in Computer Science*, pages 788–817, Zagreb, Croatia, May 10–14, 2020. Springer, Cham, Switzerland. https://doi.org/10.1007/978-3-030-45727-3_27.

[BBSS23] Amit Behera, Zvika Brakerski, Or Sattath, and Omri Shmueli. Pseudorandomness with proof of destruction and applications. In Guy N. Rothblum and Hoeteck Wee, editors, *TCC 2023: 21st Theory of Cryptography Conference, Part IV*, volume 14372 of *Lecture Notes in Computer Science*, pages 125–154, Taipei, Taiwan, November 29 – December 2, 2023. Springer, Cham, Switzerland. https://doi.org/10.1007/978-3-031-48624-1_5.

[BCEJ24] Ritam Bhaumik, Benoît Cogliati, Jordan Ethan, and Ashwin Jha. Mind the bad norms: Revisiting compressed oracle-based quantum indistinguishability proofs. In *Advances in Cryptology – ASIACRYPT 2024: 30th International Conference on the Theory and Application of Cryptology and Information Security, Kolkata, India, December 9–13, 2024, Proceedings, Part IX*, page 215–247, Berlin, Heidelberg, 2024. Springer-Verlag. https://doi.org/10.1007/978-981-96-0947-5_8.

[BHRvV21] Joppe W. Bos, Andreas Hülsing, Joost Renes, and Christine van Vredendaal. Rapidly verifiable XMSS signatures. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2021(1):137–168, 2021. https://doi.org/10.46586/tches.v2021.i1.137-168.

[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, *Advances in Cryptology – CRYPTO 2015, Part II*, volume 9216 of *Lecture Notes in Computer Science*, pages 609–629, Santa Barbara, CA, USA, August 16–20, 2015. Springer Berlin Heidelberg, Germany. https://doi.org/10.1007/978-3-662-48000-7_30.

[BRRS09] Mihir Bellare, Thomas Ristenpart, Phillip Rogaway, and Till Stegers. Format-preserving encryption. In Michael J. Jacobson, Jr., Vincent Rijmen, and Reihaneh Safavi-Naini, editors, *SAC 2009: 16th Annual International Workshop on Selected Areas in Cryptography*, volume 5867 of *Lecture Notes in Computer Science*, pages 295–312, Calgary, Alberta, Canada, August 13–14, 2009. Springer Berlin Heidelberg, Germany. https://doi.org/10.1007/978-3-642-05445-7_19.

[BZ13a] Dan Boneh and Mark Zhandry. Quantum-secure message authentication codes. In Thomas Johansson and Phong Q. Nguyen, editors, *Advances in Cryptology – EUROCRYPT 2013*, volume 7881 of *Lecture Notes in Computer Science*, pages 592–608, Athens, Greece, May 26–30, 2013. Springer Berlin Heidelberg, Germany. https://doi.org/10.1007/978-3-642-38348-9_35.

[BZ13b] Dan Boneh and Mark Zhandry. Secure signatures and chosen ciphertext security in a quantum computing world. In Ran Canetti and Juan A. Garay, editors, *Advances in Cryptology – CRYPTO 2013, Part II*, volume 8043 of *Lecture Notes in Computer Science*, pages 361–379, Santa Barbara, CA, USA, August 18–22, 2013. Springer Berlin Heidelberg, Germany. https://doi.org/10.1007/978-3-642-40084-1_21.

[CH22] Nai-Hui Chia and Shih-Han Hung. Classical verification of quantum depth, 2022. https://arxiv.org/abs/2205.04656.

[DFNS14] Ivan Damgård, Jakob Funder, Jesper Buus Nielsen, and Louis Salvail. Superposition attacks on cryptographic protocols. In Carles Padró, editor, *ICITS 13: 7th International Conference on Information Theoretic Security*, volume 8317 of *Lecture Notes in Computer Science*, pages 142–161, Singapore, 2014. Springer, Cham, Switzerland. https://doi.org/10.1007/978-3-319-04268-8_9.

[ECKM20] Ehsan Ebrahimi, Céline Chevalier, Marc Kaplan, and Michele Minelli. Superposition attack on OT protocols. Cryptology ePrint Archive, Report 2020/798, 2020. https://eprint.iacr.org/2020/798.

[GGM86] Oded Goldreich, Shafi Goldwasser, and Silvio Micali. How to construct random functions. *Journal of the ACM*, 33(4):792–807, October 1986. https://doi.org/10.1145/6490.6503.

[GHS16] Tommaso Gagliardoni, Andreas Hülsing, and Christian Schaffner. Semantic security and indistinguishability in the quantum world. In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology – CRYPTO 2016, Part III*, volume 9816 of *Lecture Notes in Computer Science*, pages 60–89, Santa Barbara, CA, USA, August 14–18, 2016. Springer Berlin Heidelberg, Germany. https://doi.org/10.1007/978-3-662-53015-3_3.

[GP07] Louis Granboulan and Thomas Pornin. Perfect block ciphers with small blocks. In Alex Biryukov, editor, *Fast Software Encryption – FSE 2007*, volume 4593 of *Lecture Notes in Computer Science*, pages 452–465, Luxembourg, Luxembourg, March 26–28, 2007. Springer Berlin Heidelberg, Germany. https://doi.org/10.1007/978-3-540-74619-5_28.

[GTB23] Tudor Giurgica-Tiron and Adam Bouland. Pseudorandomness from subset states, 2023. https://arxiv.org/abs/2312.09206.

[GYZ17] Sumegha Garg, Henry Yuen, and Mark Zhandry. New security notions and feasibility results for authentication of quantum data. In Jonathan Katz and Hovav Shacham, editors, *Advances in Cryptology – CRYPTO 2017, Part II*, volume 10402 of *Lecture Notes in Computer Science*, pages 342–371, Santa Barbara, CA, USA, August 20–24, 2017. Springer, Cham, Switzerland. https://doi.org/10.1007/978-3-319-63715-0_12.

[HI19] Akinori Hosoyamada and Tetsu Iwata. 4-round Luby-Rackoff construction is a qPRP. In Steven D. Galbraith and Shiho Moriai, editors, *Advances in Cryptology – ASIACRYPT 2019, Part I*, volume 11921 of *Lecture Notes in Computer Science*, pages 145–174, Kobe, Japan, December 8–12, 2019. Springer, Cham, Switzerland. https://doi.org/10.1007/978-3-030-34578-5_6.

[HILL99] Johan Håstad, Russell Impagliazzo, Leonid A. Levin, and Michael Luby. A pseudorandom generator from any one-way function. *SIAM Journal on Computing*, 28(4):1364–1396, 1999. https://doi.org/10.1137/S0097539793244708.

[HMR12] Viet Tung Hoang, Ben Morris, and Phillip Rogaway. An enciphering scheme based on a card shuffle. In Reihaneh Safavi-Naini and Ran Canetti, editors, *Advances in Cryptology – CRYPTO 2012*, volume 7417 of *Lecture Notes in Computer Science*, pages 1–13, Santa Barbara, CA, USA, August 19–23, 2012. Springer Berlin Heidelberg, Germany. https://doi.org/10.1007/978-3-642-32009-5_1.

[KLLN16] Marc Kaplan, Gaëtan Leurent, Anthony Leverrier, and María Naya-Plasencia. Breaking symmetric cryptosystems using quantum period finding. In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology – CRYPTO 2016, Part II*, volume 9815 of *Lecture Notes in Computer Science*, pages 207–237, Santa Barbara, CA, USA, August 14–18, 2016. Springer Berlin Heidelberg, Germany. https://doi.org/10.1007/978-3-662-53008-5_8.

[KM10] Hidenori Kuwakado and Masakatu Morii. Quantum distinguisher between the 3-round feistel cipher and the random permutation. In *2010 IEEE International Symposium on Information Theory*, pages 2682–2685, 2010. https://doi.org/10.1109/ISIT.2010.5513654.

[LQS+25] Chuhan Lu, Minglong Qin, Fang Song, Penghui Yao, and Mingnan Zhao. Quantum pseudorandom scramblers. In Elette Boyle and Mohammad Mahmoody, editors, *Theory of Cryptography: 22nd International Conference, TCC 2024, Milan, Italy, December 2–6, 2024, Proceedings, Part II*, pages 3–35, Cham, 2025. Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-78017-2_1.

[LR88] Michael Luby and Charles Rackoff. How to construct pseudorandom permutations from pseudorandom functions. *SIAM Journal on Computing*, 17(2), 1988. https://doi.org/10.1137/0217022.

[LSZ20] Qipeng Liu, Amit Sahai, and Mark Zhandry. Quantum immune one-time memories. Cryptology ePrint Archive, Report 2020/871, 2020. https://eprint.iacr.org/2020/871.

[MH25] Fermi Ma and Hsin-Yuan Huang. How to construct random unitaries. In *STOC 2025 (to appear)*, 2025. https://arxiv.org/abs/2410.10116.

[Mor05] Ben Morris. The mixing time of the Thorp shuffle. In Harold N. Gabow and Ronald Fagin, editors, *37th Annual ACM Symposium on Theory of Computing*, pages 403–412, Baltimore, MA, USA, May 22–24, 2005. ACM Press. https://doi.org/10.1145/1060590.1060651.

[MR14] Ben Morris and Phillip Rogaway. Sometimes-recurse shuffle - almost-random permutations in logarithmic expected time. In Phong Q. Nguyen and Elisabeth Oswald, editors, *Advances in Cryptology – EUROCRYPT 2014*, volume 8441 of *Lecture Notes in Computer Science*, pages 311–326, Copenhagen, Denmark, May 11–15, 2014. Springer Berlin Heidelberg, Germany. https://doi.org/10.1007/978-3-642-55220-5_18.

[RY13] Thomas Ristenpart and Scott Yilek. The mix-and-cut shuffle: Small-domain encryption secure against N queries. In Ran Canetti and Juan A. Garay, editors, *Advances in Cryptology – CRYPTO 2013, Part I*, volume 8042 of *Lecture Notes in Computer Science*, pages 392–409, Santa Barbara, CA, USA, August 18–22, 2013. Springer Berlin Heidelberg, Germany. https://doi.org/10.1007/978-3-642-40041-4_22.

[Son17] Fang Song. Quantum-secure pseudorandom permutations, 2017. Blog post: https://qcc.fangsong.info/2017-06-quantumprp.

[SS12] Emil Stefanov and Elaine Shi. FastPRP: Fast pseudo-random permutations for small domains. Cryptology ePrint Archive, Report 2012/254, 2012. https://eprint.iacr.org/2012/254.

[Zha12] Mark Zhandry. How to construct quantum random functions. In *53rd Annual Symposium on Foundations of Computer Science*, pages 679–687, New Brunswick, NJ, USA, October 20–23, 2012. IEEE Computer Society Press. https://doi.org/10.1109/FOCS.2012.37.

[Zha21] Mark Zhandry. Redeeming reset indifferentiability and applications to post-quantum security. In Mehdi Tibouchi and Huaxiong Wang, editors, *Advances in Cryptology – ASIACRYPT 2021, Part I*, volume 13090 of *Lecture Notes in Computer Science*, pages 518–548, Singapore, December 6–10, 2021. Springer, Cham, Switzerland. https://doi.org/10.1007/978-3-030-92062-3_18.