On Quantum Secure Compressing Pseudorandom Functions

Ritam Bhaumik[1], Benoît Cogliati[2], Jordan Ethan[3], Ashwin Jha[3]

[1]EPFL, Switzerland
[2]Thales DIS France SAS, Meudon, France
[3]CISPA Helmholtz Center for Information Security, Saarbrücken, Germany
ritam.bhaumik@epfl.ch, benoit.cogliati@gmail.com, jordan.ethan@cispa.de, ashwin.jha@cispa.de

Abstract. In this paper we characterize all $2n$-bit-to-n-bit Pseudorandom Functions (PRFs) constructed with the minimum number of calls to n-bit-to-n-bit PRFs and arbitrary number of linear functions. First, we show that all two-round constructions are either classically insecure, or vulnerable to quantum period-finding attacks. Second, we categorize three-round constructions depending on their vulnerability to these types of attacks. This allows us to identify classes of constructions that could be proven secure. We then proceed to show the security of the following three candidates against any quantum distinguisher that asks at most $2^{n/4}$ (possibly superposition) queries

$$\begin{aligned}\mathsf{TNT}(x_1, x_2) &:= f_3(x_2 \oplus f_2(x_2 \oplus f_1(x_1)))\\ \mathsf{LRQ}(x_1, x_2) &:= f_2(x_2) \oplus f_3(x_2 \oplus f_1(x_1))\\ \mathsf{LRWQ}(x_1, x_2) &:= f_3(f_1(x_1) \oplus f_2(x_2)).\end{aligned}$$

Note that the first construction is a classically secure tweakable block cipher due to Bao et al., and the third construction is shown to be quantum secure tweakable block cipher by Hosoyamada and Iwata with similar query limits. Of note is our proof framework, an adaptation of Chung et al.'s rigorous formulation of Zhandry's compressed oracle technique in indistinguishability setup, which could be of independent interests. This framework gives very compact and mostly classical looking proofs as compared to Hosoyamada and Iwata interpretation of Zhandry's compressed oracle.

Keywords: QPRF, TNT, LRWQ, compressed oracle, Simon's algorithm

1 Introduction

Quantum Security. In the past two decades, post-quantum security has attracted a lot of attention, especially in public-key security. As for symmetric cryptography, the consensus used to be that the main threat would come from the speed-up in exhaustive key search provided by Grover's algorithm. Hence, a doubling of the key length would be sufficient to reach security against quantum distinguishers. However, a long line of papers (see e.g. [6,7,8,9,10,13,18,20,21,22,23]) has proven that this was not sufficient, as quantum distinguishers were able to be significantly more efficient than Grover's search for some constructions. This has renewed the interest in formally proving the post-quantum security of symmetric modes of operation or generic constructions [4,5,12,14,16,17,19,26,28].

Pseudorandom Functions. One of the most studied primitive in symmetric-key cryptography is the block cipher. Thanks to the classical PRP-PRF Switching Lemma, block ciphers are known to be secure PRFs in the classical setting as long as the number of adversarial queries is small in front of $2^{n/2}$, where n denotes the block size. In the quantum setting, this bound degrades to $2^{n/3}$ [27], which can be seen as the quantum equivalent of the so-called birthday bound. Block ciphers can also be used to build other primitives, such as authenticated encryption schemes, or message authentication codes, that are secure in the classical sense. Among these primitives, $2n$-bit-to-n-bit PRFs are a key component in building higher-level optimally-secure (in the classical sense) schemes. Indeed, combining a universal $2n$-bit hash function with a $2n$-bit-to-n-bit PRF yields an n-bit secure variable-input-length PRF, which can be used to create an optimally secure authenticated encryption scheme using the SIV construction [25]. While these composition results do not exist yet in the quantum world, constructing a (quantum secure) contracting PRF from a block cipher is a key component in building more sophisticated algorithms. A first step in this direction has been taken by Hosoyamada and Iwata. Indeed, after developing a variant of Zhandry's compressed oracle [28] in [14], they have proven that the LRWQ construction

$$\begin{aligned}\{0,1\}^n \times \{0,1\}^n &\longrightarrow \{0,1\}^n \\ (x_1, x_2) &\longmapsto \mathsf{LRWQ}(x_1, x_2) := f_3(f_1(x_1) \oplus f_2(x_2)),\end{aligned}$$

where F_1, F_2, F_3 are random n-bit functions, is a (quantum) secure PRF as long as the number of queries is small in front of $2^{n/4}$ in [17]. Since this construction uses three PRF calls, two natural questions arise from this result:

- can a construction using only two PRF calls be proven secure?
- does there exist any other secure construction using three PRF calls?

It is worth noting that these questions have conclusively affirmative answers (see fixed-length $\mathsf{CBC\text{-}MAC}$ [3]) in the classical setting. In this paper, we aim to answer the two questions in the quantum settings.

1.1 Our Contributions

Our first contribution is the systematical study of all possible $2n$-bit-to-n-bit PRFs that are built using two or three PRF calls, and only linear function, as depicted in Fig. 1. In section 2, we start by introducing our notation, and describing the three main attack strategies that we will rely on. Then, in section 3, we prove that all the 2-call constructions are either classically broken, or vulnerable to a quantum period-finding distinguisher. Furthermore, we identify classes of 3-call constructions that are insecure, and categorize candidates that may be secure.

Our second contribution is to prove the security of the following constructions:

$$\begin{aligned}\mathsf{TNT}(x_1, x_2) &:= f_3(x_2 \oplus f_2(x_2 \oplus f_1(x_1)))\\ \mathsf{LRQ}(x_1, x_2) &:= f_2(x_2) \oplus f_3(x_2 \oplus f_1(x_1))\\ \mathsf{LRWQ}(x_1, x_2) &:= f_3(f_1(x_1) \oplus f_2(x_2)).\end{aligned}$$

In section 4 we adapt the rigorous formulation of Zhandry's compressed oracle technique [28] by Chung et al. [11] in the indistinguishability setting. Using this framework, in section 5 we prove that all three constructions are secure as long as the number of adversarial queries is small in front of $2^{n/4}$. As a byproduct, we also prove that the TNT construction [1] is quantum-secure against chosen plaintext attacks as long as the number of adversarial queries is small in front of $2^{n/6}$ by combining our main result with [17, Theorem 3]. We note that the combination of Hosoyamada and Iwata's proof strategy and Chung et al. framework leads to compact proofs that look mostly classical in nature. As a comparison, we derive a similar security bound for LRWQ as Hosoyamada and Iwata [17], albeit without the heavy computations from [17].

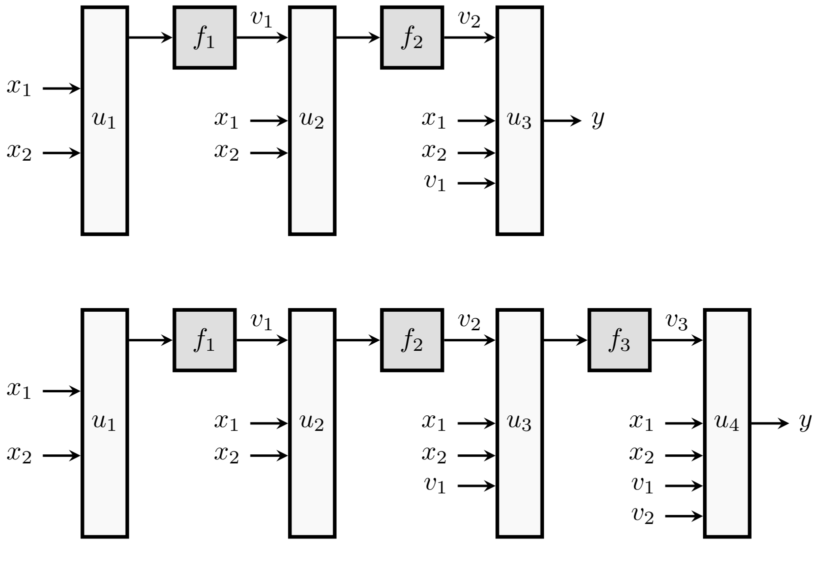

Fig. 1: Graphical representation of the generic $2n$-bit-to-n-bit PRF construction with two (top) and three (bottom) n-bit-to-n-bit PRF calls and linear functions. In this figure f_1, f_2, and f_3 are n-bit-to-n-bit PRFs, u_1, u_2, u_3, and u_4 are GF(2^n)-linear functions, and all wires are n-bit wide.

2 Preliminaries

The set of all binary strings, including the empty string $\perp$, is denoted $\{0,1\}^*$. For some $x, y \in \{0,1\}^*$, $x\|y$ denotes the concatenation of X and Y. For some positive integer m: $[m]$ denotes the set $\{1,\ldots,m\}$, and $\{0,1\}^m$ denotes the set of all m-bit binary strings. Throughout this paper, we fix a positive integer n as the block length. The set $\{0,1\}^n$ can be viewed as the binary field $\mathrm{GF}(2^n)$ by fixing a degree n primitive polynomial. We use $\oplus$ and $\odot$ to denote the field addition (XOR) and field multiplication, respectively, over the finite field $\mathrm{GF}(2^n)$. For $x, y \in \mathrm{GF}(2^n)$, we sometimes also write xy to denote $x \odot y$.

2.1 Security Definitions

In this paper, a *distinguisher* is a quantum algorithm that accesses one or more oracles. The exact model of computation, and the nature and modeling of such algorithms and oracles are not strictly necessary for the first part of this paper. So, we postpone a rigorous formalism to a latter section (see section 4). For now, it suffices to know that we deal with quantum algorithms having access to some oracle(s). We denote the event that a distinguisher $\mathscr{A}$ outputs a bit b after it runs relative to an oracle $\mathcal{O}$ by $\mathscr{A}^{\mathcal{O}} = b$.

Pseudorandom Function. Let $F : \mathcal{K} \times \{0,1\}^m \to \{0,1\}^n$ be a keyed function, indexed with keys from $\mathcal{K}$. The pseudorandom function (or PRF) advantage of some distinguisher $\mathscr{A}$ against F is defined as

$$\mathbf{Adv}_F^{\mathsf{prf}}(\mathscr{A}) := \left|\Pr\left(\mathscr{A}^{F_K} = 1\right) - \Pr\left(\mathscr{A}^{f} = 1\right)\right|, \tag{1}$$

where K is drawn uniformly at random from $\mathcal{K}$, and $f : \{0,1\}^m \to \{0,1\}^n$ is a uniform random function.

Pseudorandom Permutation. Let $E : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$ be a keyed permutation, indexed with keys from $\mathcal{K}$. The pseudorandom permutation (or PRP) advantage of some distinguisher $\mathscr{A}$ against E is defined as

$$\mathbf{Adv}_E^{\mathsf{prf}}(\mathscr{A}) := \left|\Pr\left(\mathscr{A}^{E_K} = 1\right) - \Pr\left(\mathscr{A}^{\pi} = 1\right)\right|, \tag{2}$$

where K is drawn uniformly at random from $\mathcal{K}$, and p is a uniform random permutation of $\{0,1\}^n$.

2.2 Some Useful Attack Strategies

Throughout this paper, we often employ the following attack strategies to construct generic distinguishers against various constructions.

Proposition 1 (Zero-Sum Four-Cycle). *Let $f_1, f_2 : \{0,1\}^n \to \{0,1\}^n$ be two length preserving functions and let (α_1, α_2) and (β_1, β_2) be two arbitrary two dimensional vectors over* $\mathrm{GF}(2^n)$. *Consider the function $F : \{0,1\}^{2n} \to \{0,1\}^n$ defined by the mapping $(x_1, x_2) \mapsto f_1(\alpha_1 x_1 \oplus \alpha_2 x_2) \oplus f_2(\beta_1 x_1 \oplus \beta_2 x_2)$. Then, there exists four distinct pairs $(x_1^1, x_2^1), \ldots, (x_1^4, x_2^4) \in \{0,1\}^{2n}$ such that, $F(x_1^1, x_2^1) \oplus F(x_1^2, x_2^2) \oplus F(x_1^3, x_2^3) \oplus F(x_1^4, x_2^4) = 0$.*

Proof. First, assume that (β_1, β_2) is dependent on (α_1, α_2). In this case one can always find four distinct pairs $(x_1^1, x_2^1), (x_1^2, x_2^2), (x_1^3, x_2^3), (x_1^4, x_2^4) \in \{0,1\}^{2n}$ such that

$$\alpha_1 x_1^1 \oplus \alpha_2 x_2^1 = \alpha_1 x_1^2 \oplus \alpha_2 x_2^2, \qquad \alpha_1 x_1^3 \oplus \alpha_2 x_2^3 = \alpha_1 x_1^4 \oplus \alpha_2 x_2^4.$$

Since (β_1, β_2) is dependent on (α_1, α_2), this straightaway implies that

$$\beta_1 x_1^1 \oplus \beta_2 x_2^1 = \beta_1 x_1^2 \oplus \beta_2 x_2^2, \qquad \beta_1 x_1^3 \oplus \beta_2 x_2^3 = \beta_1 x_1^4 \oplus \beta_2 x_2^4,$$

whence we get the first part of the proposition, as $F(x_1^1, x_2^1) = F(x_1^2, x_2^2)$ and $F(x_1^3, x_2^3) = F(x_1^4, x_2^4)$. Now, assume that (α_1, α_2) is independent of (β_1, β_2), which implies that the mapping

$$(x_1, x_2) \overset{\varphi}{\longmapsto} (\alpha_1 x_1 \oplus \alpha_2 x_2, \beta_1 x_1 \oplus \beta_2 x_2)$$

is a bijection. Fix some $y_1 \neq y_1' \in \mathrm{GF}(2^n)$ and $y_2 \neq y_2' \in \mathrm{GF}(2^n)$, and compute

$$\begin{aligned} (x_1^1, x_2^1) &= \varphi^{-1}(y_1, y_2) & \qquad (x_1^2, x_2^2) &= \varphi^{-1}(y_1', y_2) \\ (x_1^3, x_2^3) &= \varphi^{-1}(y_1', y_2') & \qquad (x_1^4, x_2^4) &= \varphi^{-1}(y_1, y_2'), \end{aligned}$$

so that $F(x_1^1, x_2^1) \oplus F(x_1^2, x_2^2) = f_1(y_1) \oplus f_1(y_1') = F(x_1^3, x_2^3) \oplus F(x_1^4, x_2^4)$. This proves the second part of the proposition. □

One can extend Proposition 1 to Proposition 2 in a straightforward manner.

Proposition 2 (Generalized Zero-Sum Four-Cycle). *Let $f_1, f_2, f_3 : \{0,1\}^n \to \{0,1\}^n$ be three length preserving functions and let (α_1, α_2), (β_1, β_2), and (γ_1, γ_2) be three arbitrary two dimensional vectors over* $\mathrm{GF}(2^n)$. *Consider the function $F : \{0,1\}^{2n} \to \{0,1\}^n$ defined by the mapping*

$$(x_1, x_2) \mapsto f_1(\alpha_1 x_1 \oplus \alpha_2 x_2) \oplus f_2(\beta_1 x_1 \oplus \beta_2 x_2) \oplus f_3(\gamma_1 x_1 \oplus \gamma_2 x_2).$$

Then, there exists four distinct pairs $(x_1^1, x_2^1), \ldots, (x_1^4, x_2^4) \in \{0,1\}^{2n}$ such that,

$$F(x_1^1, x_2^1) \oplus F(x_1^2, x_2^2) \oplus F(x_1^3, x_2^3) \oplus F(x_1^4, x_2^4) = 0.$$

Proof. First, consider the case where (β_1, β_2) and (γ_1, γ_2) are dependent on (α_1, α_2). In this case, one can always find four distinct pairs $(x_1^1, x_2^1), (x_1^2, x_2^2), (x_1^3, x_2^3), (x_1^4, x_2^4) \in \{0,1\}^{2n}$ such that

$$\alpha_1 x_1^1 \oplus \alpha_2 x_2^1 = \alpha_1 x_1^2 \oplus \alpha_2 x_2^2, \qquad \alpha_1 x_1^3 \oplus \alpha_2 x_2^3 = \alpha_1 x_1^4 \oplus \alpha_2 x_2^4.$$

This straightaway implies that

$$\begin{aligned} \beta_1 x_1^1 \oplus \beta_2 x_2^1 &= \beta_1 x_1^2 \oplus \beta_2 x_2^2 \qquad & \gamma_1 x_1^1 \oplus \gamma_2 x_2^1 &= \gamma_1 x_1^2 \oplus \gamma_2 x_2^2 \\ \beta_1 x_1^3 \oplus \beta_2 x_2^3 &= \beta_1 x_1^4 \oplus \beta_2 x_2^4 \qquad & \gamma_1 x_1^3 \oplus \gamma_2 x_2^3 &= \gamma_1 x_1^4 \oplus \gamma_2 x_2^4 \end{aligned}$$

since (β_1, β_2) and (γ_1, γ_2) are dependent on (α_1, α_2). This proves the first part of the proposition.

Now, assume that (α_1, α_2) and (β_1, β_2) are independent, but (γ_1, γ_2) is a linear combination of (α_1, α_2) and (β_1, β_2). In other words, we have

$$(\gamma_1, \gamma_2) = (a\alpha_1 \oplus b\beta_1, a\alpha_2 \oplus b\beta_2) \tag{3}$$

for some $\{a, b\} \neq \{0\}$. Now, we can fix some $(y_1, y_2) \neq (y_1', y_2') \in \mathrm{GF}(2^n) \times \mathrm{GF}(2^n)$, such that

$$ay_1 \oplus by_2 = ay_1' \oplus by_2'. \tag{4}$$

Since, (α_1, α_2) is independent of (β_1, β_2), the mapping $(x_1, x_2) \overset{\varphi}{\mapsto} (\alpha_1 x_1 \oplus \alpha_2 x_2, \beta_1 x_1 \oplus \beta_2 x_2)$ is bijective. Let

$$\begin{aligned} (x_1^1, x_2^1) &= \varphi^{-1}(y_1, y_2) \qquad & (x_1^2, x_2^2) &= \varphi^{-1}(y_1', y_2) \\ (x_1^3, x_2^3) &= \varphi^{-1}(y_1', y_2') \qquad & (x_1^4, x_2^4) &= \varphi^{-1}(y_1, y_2') \end{aligned}$$

From (3) and (4), we have

$$\begin{aligned} \gamma_1 x_1^1 \oplus \gamma_2 x_2^1 &= \gamma_1 x_1^3 \oplus \gamma_2 x_2^3 \\ \gamma_1 x_1^2 \oplus \gamma_2 x_2^2 &= \gamma_1 x_1^4 \oplus \gamma_2 x_2^4 \end{aligned}$$

This proves the second part of the proposition. □

Note that, Proposition 1 is a special case of Proposition 2, where f_3 is a constant function.

Proposition 3 (Period Finding). *For any $f_1, f_2, f_3 : \{0,1\}^n \to \{0,1\}^n$, suppose $F : \{0,1\}^{2n} \to \{0,1\}^n$ is defined by the mapping $(x_1, x_2) \mapsto f_3(x_2 \oplus f_1(x_1)) \oplus f_2(x_1)$. Then, for any $x_1^0 \neq x_1^1 \in \{0,1\}^n$, the function $G_{x_1^0, x_1^1} : \{0,1\}^n \to \{0,1\}^n$ defined by the mapping $x_2 \mapsto F(x_1^0, x_2) \oplus F(x_1^1, x_2)$ is periodic and the period $s(x_1^0, x_1^1) = f_1(x_1^0) \oplus f_1(x_1^1)$.*

Proof. For any $x_2 \in \{0,1\}^n$, we have

$$\begin{aligned} G_{x_1^0, x_1^1}(x_2 \oplus s(x_1^0, x_1^1)) &= F(x_1^0, x_2 \oplus s(x_1^0, x_1^1)) \oplus F(x_1^1, x_2 \oplus s(x_1^0, x_1^1)) \\ &= f_3(x_2 \oplus f_1(x_1^0) \oplus f_1(x_1^1) \oplus f_1(x_1^0)) \\ &\qquad\quad \oplus f_3(x_2 \oplus f_1(x_1^0) \oplus f_1(x_1^1) \oplus f_1(x_1^1)) \\ &= F(x_1^0, x_2) \oplus F(x_1^1, x_2) = G_{x_1^0, x_1^1}(x_2). \end{aligned}$$

While the first two Propositions are interesting even in the classical setting, Proposition 3 is mainly useful in the quantum setting. Specifically, it facilitates the application of Simon's algorithm (see [24] for details). We often employ Proposition 3 in conjunction with the following useful result [20] due to Kaplan et al., which greatly extends the scope of Simon's algorithm.

Let $f : \{0,1\}^n \to \{0,1\}^n$ be a random function with some period $s \neq 0$. In [20], Kaplan et al. define

$$\epsilon(f, s) := \max_{t \in \{0,1\}^n \setminus \{0,s\}} \Pr_{f,x} \left(f(x) = f(x \oplus t) \right) \tag{5}$$

Theorem 1 ([20], Theorem 1). *Let $f : \{0,1\}^n \to \{0,1\}^n$ be a random function with some period $s \neq 0$. If $\epsilon(f, s) \leq p_0 < 1$, then Simon's algorithm returns s with cn queries, with probability at least $1 - \left(2\left(\frac{1+p_0}{2}\right)^c\right)^n$.*

Note that choosing $c > 3/(1 - p_0)$ ensures that the error decreases exponentially with n. Thus, it is sufficient to show that $\epsilon(f, s) < 1$. Specifically, it is well-known that $\epsilon(f, s) = \Theta(n2^{-n})$ when f is a random function. Then, Simon's algorithm returns the period with probability close to 1.

3 Characterizing 2n-to-n-bit Functions

Our first goal is to identify the minimum number of secret random functions and arbitrary linear functions, required to construct a secure 2n-to-n-bit PRF. Actually, we go a step further and characterize all the secure (and interesting) PRFs with minimum number of calls. Since, LRWQ [17] by Hosoyamada and Iwata, can also be considered as a secure PRF, we already have an upper bound of three calls. So we limit ourselves to at most three calls constructions. The attacks presented here are apparent enough to verify that the query complexity is at most polynomial in n to achieve a constant PRF advantage. So, for the sake of simplicity, we skip computing the exact query complexity and attack advantage for the attacks. Further, to start off, we observe that functions based on just one random function are trivially broken in the classical sense as well. So, we skip them from our discussions, and move on to two or more random functions.

Let $f_1, f_2, f_3; \{0,1\}^n \to \{0,1\}^n$, be three independent secret random functions. Let $\alpha = (\alpha_1, \alpha_2) \in \{0,1\}^{2n}$ and $\beta = (\beta_1, \beta_2, \beta_3) \in \{0,1\}^{3n}$, $\gamma = (\gamma_1, \gamma_2, \gamma_3, \gamma_4) \in \{0,1\}^{4n}$, $\delta = (\delta_1, \delta_2, \delta_3, \delta_4, \delta_5) \in \{0,1\}^{5n}$ be some public parameters.

3.1 Constructions Based on Two Calls

For a 3 × 4 matrix

$$A = \begin{pmatrix} \alpha_1 & \alpha_2 & 0 & 0 \\ \beta_1 & \beta_2 & \beta_3 & 0 \\ \gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 \end{pmatrix}$$

our candidate function $F_{A,f_1,f_2} : \{0,1\}^{2n} \to \{0,1\}^n$ indexed by A, f_1, and f_2 is described below.
On input $(x_1, x_2) \in \{0,1\}^{2n}$:

1. $u_1(x_1, x_2) = \alpha_1 x_1 \oplus \alpha_2 x_2$
2. $v_1(x_1, x_2) = f_1(u_1(x_1, x_2))$
3. $u_2(x_1, x_2, v_1) = \beta_1 x_1 \oplus \beta_2 x_2 \oplus \beta_3 v_1$
4. $v_2(x_1, x_2) = f_2(u_2(x_1, x_2, v_1))$
5. $u_3(x_1, x_2, v_1, v_2) = \gamma_1 x_1 \oplus \gamma_2 x_2 \oplus \gamma_3 v_1 \oplus \gamma_4 v_2$
6. $F_{A,f_1,f_2}(x_1, x_2) = y = u_3(x_1, x_2, v_1, v_2)$

With a slight abuse of notation, we simply write u_i and v_j to denote $u_i(\cdot)$ $v_j(\cdot)$ for all $i \in [3]$ and $j \in [2]$, whenever the input is known from the context, or the stated fact is independent of the inputs. With this slight simplification, we can represent the entire function using the following system of equations,

$$A \cdot \begin{pmatrix} x_1 \\ x_2 \\ v_1 \\ v_2 \end{pmatrix} = \begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix}$$

First, notice that some straightforward simplifications can be done with respect to A:

1. Without loss of generality, we assume that $\gamma_1 = \gamma_2 = 0$, since the adversary can easily create $u_3' = u_3 \oplus \gamma_1 x_1 \oplus \gamma_2 x_2$ for any pair of inputs $(x_1, x_2) \in \{0,1\}^{2n}$.
2. We assume that each row of A is non-zero. Otherwise, there exists $i \in [3]$ such that $u_i = 0$, whence either F is independent of f_1 or f_2, or it is a constant.
3. We assume that each column of A is non-zero as well. Otherwise, for all $i \in [3]$, u_i is independent of one of x_1, x_2, v_1, and v_2, whence F is independent of f_1 or f_2 or it is independent of one of its inputs.
4. We can multiply any row by a non-zero constant. Indeed, for the first two rows, multiplying the input of a uniformly random function by a non-zero constant does not change the distribution of the outputs. For the final row, the adversary can multiply the outputs of the construction by any constant.

Using the above simplifications, from now on we can assume that $\gamma_4 = 1$ by normalizing the final row by γ_4^{-1}. Given these initial simplifications, we do the characterization of F_{A,f_1,f_2} into three cases:

Case 1: $\beta_1 = \beta_2 = 0$. Then, according to our simplification $\beta_3 = 1$. Therefore,

$$F(x_1, x_2) = (\gamma_3 f_1(u_1)) \oplus (f_2(f_1(u_1))).$$

Using Proposition 1, we can find $(x_1, x_2) \neq (x_1', x_2')$ such that $F(u_1(x_1, x_2)) \oplus F(u_1(x_1', x_2')) = 0$. That gives a classical collision attack.

CASE 2: ($\beta_1 \neq 0$ OR $\beta_2 \neq 0$) AND $\alpha_1\beta_2 = \alpha_2\beta_1$. Then, there exists a non-zero $c \in \mathrm{GF}(2^n)$, such that $(\beta_1, \beta_2) = (c\alpha_1, c\alpha_2)$. So for every pair of inputs $(x_1, x_2) \neq (x'_1, x'_2)$, such that $\alpha_1 x_1 \oplus \alpha_2 x_2 = \alpha_1 x'_1 \oplus \alpha_2 x'_2$, we must have $\beta_1 x_1 \oplus \beta_2 x_2 = \beta_1 x'_1 \oplus \beta_2 x'_2$. Therefore, $u_1(x_1, x_2) = u_1(x'_1, x'_2)$ and $u_2(x_1, x_2, v_1) = u_2(x'_1, x'_2, v_1)$ which implies that $u_3(x_1, x_2, v_1, v_2) = u_3(x'_1, x'_2, v_1, v_2)$. This clearly gives a collision attack on the construction for inputs (x_1, x_2) and (x'_1, x'_2).

CASE 3: ($\beta_1 \neq 0$ OR $\beta_2 \neq 0$) AND $\alpha_1\beta_2 \neq \alpha_2\beta_1$. Then the construction is reduced to,

$$F(x_1, x_2) = \gamma_3 f_1(\alpha_1 x_1 \oplus \alpha_2 x_2) \oplus f_2\left(\beta_1 x_1 \oplus \beta_2 x_2 \oplus \beta_3 f_1(\alpha_1 x_1 \oplus \alpha_2 x_2)\right).$$

Let $f'_1 = \gamma_3 f_1$, and $f''_1 = \beta_3 f_1$, and $u'_2(x_1, x_2) = \beta_1 x_1 \oplus \beta_2 x_2$. Then, the above construction reduces to

$$F(x_1, x_2) = f'_1(u_1(x_1, x_2)) \oplus f_2\left(u'_2(x_1, x_2) \oplus f''_1(u_1(x_1, x_2))\right).$$

Using Proposition 3, we can come up with a periodic function, and hence using Theorem 1, we can find the period in polynomial number of queries.

This concludes the characterization of two call constructions. Through our analysis, we have established that two calls are not sufficient to construct a $2n$-to-n-bit quantum secure PRF.

3.2 Constructions Based on Three Calls

For a 4×5 matrix

$$A = \begin{pmatrix} \alpha_1 & \alpha_2 & 0 & 0 & 0 \\ \beta_1 & \beta_2 & \beta_3 & 0 & 0 \\ \gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 & 0 \\ \delta_1 & \delta_2 & \delta_3 & \delta_4 & \delta_5 \end{pmatrix}$$

our candidate function $F_{A,f_1,f_2,f_3} : \{0,1\}^{2n} \to \{0,1\}^n$ indexed by A, f_1, f_2, and f_3 is described below.
On input $(x_1, x_2) \in \{0,1\}^{2n}$:

1. $u_1(x_1, x_2) = \alpha_1 x_1 \oplus \alpha_2 x_2$
2. $v_1(x_1, x_2) = f_1(u_1(x_1, x_2))$
3. $u_2(x_1, x_2, v_1) = \beta_1 x_1 \oplus \beta_2 x_2 \oplus \beta_3 v_1$
4. $v_2(x_1, x_2) = f_2(u_2(x_1, x_2, v_1))$
5. $u_3(x_1, x_2, v_1, v_2) = \gamma_1 x_1 \oplus \gamma_2 x_2 \oplus \gamma_3 v_1 \oplus \gamma_4 v_2$
6. $v_3(x_1, x_2) = f_3(u_3(x_1, x_2, v_1, v_2))$
7. $u_4(x_1, x_2, v_1, v_2, v_3) = \delta_1 x_1 \oplus \delta_2 x_2 \oplus \delta_3 v_1 \oplus \delta_4 v_2 \oplus \delta_5 v_3$
8. $F_{A,f_1,f_2,f_3}(x_1, x_2) = y = u_4(x_1, x_2, v_1, v_2, v_3)$

With similar simplifications as in the case of two call analysis, we can represent the entire function using the following system of equations,

$$A \cdot \begin{pmatrix} x_1 \\ x_2 \\ v_1 \\ v_2 \\ v_3 \end{pmatrix} = \begin{pmatrix} u_1 \\ u_2 \\ u_3 \\ u_4 \end{pmatrix} \tag{6}$$

Further, we can make the same initial simplifying assumptions, as made in case of two call constructions, namely

- $\delta_1 = \delta_2 = 0$;
- each row of the matrix is non-zero; and
- each column of the matrix is non-zero.

Further, from now on we assume that $\delta_5 = 1$. Moreover, we claim that the following preconditions are necessary to get a secure construction:

Precondition 1: (α_1, α_2) should be independent of (β_1, β_2).

Precondition 2: $\gamma_4 \neq 0$ or

(a) (α_1, α_2) should be independent of (γ_1, γ_2); and

(b) $(\beta_1, \beta_2, \beta_3)$ should be independent of $(\gamma_1, \gamma_2, \gamma_3)$.

Precondition 3: $\begin{pmatrix} \beta_3 & \gamma_3 \\ \gamma_4 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

Indeed, in Proposition 4, we show that the construction is susceptible to efficient (quantum) attack if any one of the three conditions are violated.

Proposition 4. *The Precondition 1, 2, and 3, as stated above are necessary for F_{A,f_1,f_2,f_3} to be a quantum secure PRF.*

Proof. First consider the Precondition 1. Our analysis is divided into two cases.

- If $\alpha_1\gamma_2 = \alpha_2\gamma_1$, then we can construct a collision attack on F using a similar argument as used in Case 2 for two call constructions.
- Otherwise, the function $(x_1, x_2) \mapsto (\alpha_1 x_1 \oplus \alpha_2 x_2, \gamma_1 x_1 \oplus \gamma_2 x_2)$ is a bijection. Moreover, there exists $c \neq 0$ such that, $(\alpha_1, \alpha_2) = (c\beta_1, c\beta_2)$. Let $u_3'(x_1, x_2) = \gamma_1 x_1 \oplus \gamma_2 x_2$. Then we can rewrite $F(x_1, x_2)$ as

$$\delta_3 f_1(u_1) \oplus \delta_2 f_2(cu_1 \oplus \beta_3 f_1(u_1)) \oplus f_3\left(u_3' \oplus \gamma_3 f_1(u_1) \oplus \gamma_4 f_2(cu_1 \oplus \beta_3 f_1(u_1))\right).$$

We define $F_1, F_2 : \{0,1\}^n \to \{0,1\}^n$ by

$$F_1(u_1) = \delta_3 f_1(u_1) \oplus \delta_2 f_2(cu_1 \oplus \beta_3 f_1(u_1)),$$
$$F_2(u_1) = \gamma_3 f_1(u_1) \oplus \gamma_4 f_2(cu_1 \oplus \beta_3 f_1(u_1)),$$

This reduces $F(x_1, x_2)$ to $F_1(x_1) \oplus f_3(x_2 \oplus F_2(x_1))$, which, as we show in Proposition 3, is susceptible to period finding, and hence hence distinguishable in polynomial number of queries using Theorem 1.

Next, we take Precondition 2. Without loss of generality, assume that Precondition 1 holds, otherwise a similar attack will work in this case as well (irrespective of $\gamma_4 = 0$ or not). First, consider the case when (α_1, α_2) and (γ_1, γ_2) are dependent. Then, there exists $c \neq 0$ such that $(c\alpha_1, c\alpha_2) = (\gamma_1, \gamma_2)$. Let $u_2' = \beta_1 x_1 \oplus \beta_2 x_2$, then we can rewrite $F(x_1, x_2)$ as

$$\delta_3 f_1(u_1) \oplus \delta_2 f_2(u_2' \oplus \beta_3 f_1(u_1)) \oplus f_3\left(cu_1 \oplus \gamma_3 f_1(u_1)\right).$$

We define $F_1, F_2 : \{0,1\}^n \to \{0,1\}^n$ by

$$F_1(u_1) = \delta_3 f_1(u_1) \oplus f_3\left(cu_1 \oplus \gamma_3 f_1(u_1)\right), \qquad F_2(u_1) = \beta_3 f_1(u_1).$$

This reduces $F(x_1, x_2)$ to $F_1(u_1) \oplus \delta_3 f_2(u_2' \oplus F_2(u_1))$, which is susceptible to period finding (using Proposition 3 and Theorem 1). For the case when $(\beta_1, \beta_2, \beta_3)$ and $(\gamma_1, \gamma_2, \gamma_3)$ are dependent, we can argue similarly that the resulting construction is susceptible to period finding.

Finally, we consider Precondition 3. In this case, the adversary can deduce and to some extent manipulate u_1, u_2, u_3 (since he knows the parameters). More precisely, we can rewrite $F(x_1, x_2)$ as

$$F(x_1, x_2) = \delta_3 f_1(\alpha_1 x_1 \oplus \alpha_2 x_2) \oplus \delta_4 f_2(\beta_1 x_1 \oplus \beta_2 x_2) \oplus \delta_5 f_3(\gamma_1 x_1 \oplus \gamma_2 x_2).$$

Using Proposition 2, we can find four queries whose outputs sum to 0. This gives a simple classical distinguisher. □

Onwards, using our simplifications and preconditions, we can rewrite the three call system given in (6) as

$$\begin{pmatrix} \alpha_1 & \alpha_2 & 0 & 0 & 0 \\ \beta_1 & \beta_2 & \beta_3 & 0 & 0 \\ \gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 & 0 \\ 0 & 0 & \delta_3 & \delta_4 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ v_1 \\ v_2 \\ v_3 \end{pmatrix} = \begin{pmatrix} u_1 \\ u_2 \\ u_3 \\ u_4 \end{pmatrix} \tag{7}$$

In the following discussion, we divide our analysis into two cases:

Case 1: $\gamma_4 = 0$. Without loss of generality assume $\delta_4 = 1$, and consider the three sub cases below.

(a) $\beta_3 = 0$. By Precondition 3, we must have $\gamma_3 \neq 0$. For simplicity assume $\gamma_3 = 1$. Moreover, notice that Precondition 1 implies that without loss of generality,

$$\begin{pmatrix} \alpha_1 & \alpha_2 \\ \beta_1 & \beta_2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Next, note that $\gamma_2 \neq 0$, otherwise this violates Precondition 2. Therefore, we are left with the following general matrix,

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ \gamma_1 & \gamma_2 & 1 & 0 & 0 \\ 0 & 0 & \delta_3 & 1 & 1 \end{pmatrix} \tag{8}$$

where the blue colored elements indicate strictly non-zero values only. We further, simplify the above matrix, by setting $\gamma_1 = \delta_3 = 0$, and $\gamma_2 = 1$. This simplification stems from the point of view of efficiency. A simple XOR is always preferable to a finite field multiplication followed by an XOR. Finally, we arrive to the following matrix:

$$A_{\mathsf{LRQ}} := \begin{pmatrix} 1\,0\,0\,0\,0 \\ 0\,1\,0\,0\,0 \\ 0\,1\,1\,0\,0 \\ 0\,0\,0\,1\,1 \end{pmatrix} \tag{9}$$

and the resulting construction is defined as

$$\mathsf{LRQ}(x_1, x_2) := f_2(x_2) \oplus f_3(x_2 \oplus f_1(x_1)) \tag{10}$$

(b) $\gamma_3 = 0$. By Precondition 3, we must have $\beta_3 \neq 0$. For simplicity, assume $\beta_3 = 1$. Moreover, notice that Precondition 2 implies that without loss of generality,

$$\begin{pmatrix} \alpha_1 & \alpha_2 \\ \gamma_1 & \gamma_2 \end{pmatrix} = \begin{pmatrix} 1\,0 \\ 0\,1 \end{pmatrix}$$

Next , note that we must have $\beta_2 \neq 0$, otherwise this violates Precondition 1. Therefore, we are left with the following general matrix,

$$\begin{pmatrix} 1 & 0 & 0 & 0\,0 \\ \beta_1 & \beta_2 & 1 & 0\,0 \\ 0 & 1 & 0 & 0\,0 \\ 0 & 0 & \delta_3 & 1\,1 \end{pmatrix} \tag{11}$$

On further simplification, by setting $\beta_1 = \delta_3 = 0$ and $\beta_2 = 1$, we observe that this corresponds to the same construction as (9) up to a relabeling of functions.

(c) $\beta_3, \gamma_3 \neq 0$. Without loss of generality assume that $\beta_3 = 1$. Then, we are left with the following general matrix,

$$\begin{pmatrix} \alpha_1 & \alpha_2 & 0 & 0\,0 \\ \beta_1 & \beta_2 & 1 & 0\,0 \\ \gamma_1 & \gamma_2 & \gamma_3 & 0\,0 \\ 0 & 0 & \delta_3 & 1\,1 \end{pmatrix} \tag{12}$$

where the red colored submatrix represents the fact that it satisfies Precondition 1 and 2, i.e., we must have (α_1, α_2) independent of (β_1, β_2) and (γ_1, γ_2), and $(\beta_1, \beta_2, 1)$ independent of $(\gamma_1, \gamma_2, \gamma_3)$. Using similar simplifying arguments as before, and preserving isomorphism up to relabeling of functions, we arrive at the following interesting matrices

$$A_{\mathsf{CSUMQ}} := \begin{pmatrix} 1\,0\,0\,0\,0 \\ 0\,1\,1\,0\,0 \\ 1\,1\,1\,0\,0 \\ 0\,0\,0\,1\,1 \end{pmatrix}, \qquad A_{\mathsf{LMQ}} := \begin{pmatrix} 1\,1\,0\,0\,0 \\ 0\,1\,1\,0\,0 \\ 1\,0\,1\,0\,0 \\ 0\,0\,0\,1\,1 \end{pmatrix} \tag{13}$$

and the resulting constructions are defined as

$$\mathsf{CSUMQ}(x_1, x_2) := f_2(x_2 \oplus f_1(x_1)) \oplus f_3(x_2 \oplus x_1 \oplus f_1(x_1)) \tag{14}$$

$$\mathsf{LMQ}(x_1, x_2) := f_2(x_2 \oplus f_1(x_1 \oplus x_2)) \oplus f_3(x_1 \oplus f_1(x_1 \oplus x_2)) \tag{15}$$

Case 2: $\gamma_4 \neq 0$. Without loss of generality, assume that $\gamma_4 = 1$. Consider the following three sub cases:

(a) $\beta_3 = \gamma_3 = 0$. Then, using Precondition 1, we are left with the following general matrix,

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ \gamma_1 & \gamma_2 & 0 & 1 & 0 \\ 0 & 0 & \delta_3 & \delta_4 & 1 \end{pmatrix} \tag{16}$$

where blue colored elements indicate strictly non-zero values only. The condition $\gamma_1 \neq 0$ can be easily argued as follows: Suppose, $\gamma_1 = 0$. Then, using Proposition 1, one can find four queries such that the outputs sum to 0, resulting in a classical distinguishing attack. Similarly, $\delta_3 \neq 0$, since each column must have one non-zero entry. Further, by setting $\gamma_2 = \delta_4 = 0$ and $\gamma_1 = \delta_3 = 1$, we arrive at the same construction as in (9) up to a relabeling of functions and input variables.

(b) $\beta_3 = 0$ and $\gamma_3 \neq 0$. Then, using Precondition 1, we are left with the following general matrix,

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ \gamma_1 & \gamma_2 & \gamma_3 & 1 & 0 \\ 0 & 0 & \delta_3 & \delta_4 & 1 \end{pmatrix} \tag{17}$$

where blue colored elements indicate strictly non-zero values only. By setting $\gamma_1 = \gamma_2 = \delta_3 = \delta_4 = 0$ and $\gamma_3 = 1$, we arrive at the following matrix

$$A_{\mathsf{LRWQ}} := \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \tag{18}$$

which corresponds to the LRWQ construction [17] by Hosoyamada and Iwata. The function is defined as

$$\mathsf{LRWQ}(x_1, x_2) := f_3\left(f_1(x_1) \oplus f_2(x_2)\right) \tag{19}$$

(c) $\gamma_3 = 0$ and $\beta_3 \neq 0$. Without loss of generality, we assume that $\beta_3 = 1$. Then, using Precondition 1, we are left with the following general matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ \gamma_1 & \gamma_2 & 0 & 1 & 0 \\ 0 & 0 & \delta_3 & \delta_4 & 1 \end{pmatrix} \tag{20}$$

where red colored elements indicate that they cannot all be 0. This can be easily argued by looking at the resulting construction. Suppose, $\gamma_1 = \gamma_2 = 0$. Then, the second and third calls can be clubbed together (since the output of the second call is directly fed into the third call), resulting in a reduction to an equivalent two call construction, which is already shown to be insecure. Now, using the simplification steps, we get the following two matrices

$$A_{\mathsf{EDMQ}} := \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \qquad A_{\mathsf{TNT}} := \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \tag{21}$$

where the second matrix, i.e., A_{TNT} corresponds to the TNT construction [2] by Bao et al. The corresponding constructions are defined as follows:

$$\mathsf{EDMQ}(x_1, x_2) := f_3(x_1 \oplus f_2(x_2 \oplus f_1(x_1))) \tag{22}$$

$$\mathsf{TNT}(x_1, x_2) := f_3(x_2 \oplus f_2(x_2 \oplus f_1(x_1))) \tag{23}$$

(d) $\beta_3, \gamma_3 \neq 0$. In this case, using $\mathsf{Precondition\ 1}$, we can have the following general matrix,

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & \beta_3 & 0 & 0 \\ \gamma_1 & \gamma_2 & \gamma_3 & 1 & 0 \\ 0 & 0 & \delta_3 & \delta_4 & 1 \end{pmatrix} \tag{24}$$

where blue colored elements indicate strictly non-zero values only. Further, by setting $\gamma_1 = \gamma_2 = \delta_3 = \delta_4 = 0$, and $\beta_3 = \gamma_3 = 1$, we get

$$A_{\mathsf{EDMDQ}} := \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \tag{25}$$

and the corresponding construction is defined as

$$\mathsf{EDMDQ}(x_1, x_2) := f_3(f_1(x_1) \oplus f_2(x_2 \oplus f_1(x_1))) \tag{26}$$

A Summary of Interesting Candidates. In Table 1, we summarize the definitions and special features of the seven candidate PRF constructions. Three of the seven candidates, namely, LRQ, LRWQ [17], and TNT [2], are special as they can act as a tweakable permutation when the underlying primitives are permutations. Further, they are also among the most favorable candidates in terms of desirable implementation features like XOR counts, parallelizability, and state size. So, we concentrate on proving the security of these three candidates. In this paper, we mainly consider the PRF security of these constructions. However, the TPRP security can be easily recovered using a well-known switching result [14,15] due to Hososyamada and Iwata.[1]

Table 1: Summary of the possibly secure PRF candidates with minimum number of random function calls.

Candidate	Definition	Memory	XORs	Invertible	Parallel
LRQ	$f_2(x_2) \oplus f_3(x_2 \oplus f_1(x_1))$	$2n$	2	✓	✓
CSUMQ	$f_2(x_2 \oplus f_1(x_1)) \oplus f_3(x_2 \oplus x_1 \oplus f_1(x_1))$	$2n$	3	×	✓
LMQ	$f_2(x_2 \oplus f_1(x_1 \oplus x_2)) \oplus f_3(x_1 \oplus f_1(x_1 \oplus x_2))$	$2n$	4	×	✓
LRWQ [17]	$f_3(f_1(x_1) \oplus f_2(x_2))$	$2n$	1	✓	✓
EDMQ	$f_3(x_1 \oplus f_2(x_2 \oplus f_1(x_1)))$	n	2	×	×
TNT [2]	$f_3(x_2 \oplus f_2(x_2 \oplus f_1(x_1)))$	n	2	✓	×
EDMDQ	$f_3(f_1(x_1) \oplus f_2(x_2 \oplus f_1(x_1)))$	n	2	×	×

4 Quantum Proof Framework

Let $\mathcal{Y}$ denote $\{0,1\}^n$. Let $B_C := \{|y\rangle \mid y \in \mathcal{Y}\}$ denote the computational basis of the n-qubit space $\mathbb{C}^{2^n}$. For each $y \in \mathcal{Y}$ let $\widehat{y}$ denote the group homomorphism $z \mapsto (-1)^{y \cdot z}$ from $\mathcal{Y}$ to $\{1,-1\}$ (the latter a group under multiplication). Then $\widehat{\mathcal{Y}} := \{\widehat{y} \mid y \in \mathcal{Y}\}$ forms a group under the group operation $\widehat{y} + \widehat{z} := \widehat{y \oplus z}$ (where $\oplus$ denote bitwise XOR, the group operation in $\mathcal{Y}$); we call $\widehat{\mathcal{Y}}$ the *dual group* of $\mathcal{Y}$. (The definition of the group operation for $\widehat{\mathcal{Y}}$ also implies that $y \mapsto \widehat{y}$ is a group isomorphism from $\mathcal{Y}$ to $\widehat{\mathcal{Y}}$.)

For each $\widehat{y} \in \widehat{\mathcal{Y}}$ define

$$\left|\widehat{y}\right\rangle := \frac{1}{2^{n/2}} \sum_{z \in \mathcal{Y}} \widehat{y}(z) \, |z\rangle = \frac{1}{2^{n/2}} \sum_{z \in \mathcal{Y}} (-1)^{y \cdot z} \, |z\rangle \, .$$

Then $B_F := \{\left|\widehat{y}\right\rangle \mid \widehat{y} \in \widehat{\mathcal{Y}}\}$ also constitutes a basis of $\mathbb{C}^{2^n}$; we call it the *Fourier basis*. The reverse basis transformation from the Fourier basis to the computational basis is given by

$$|y\rangle := \frac{1}{2^{n/2}} \sum_{\widehat{z} \in \widehat{\mathcal{Y}}} \widehat{z}(y) \left|\widehat{z}\right\rangle = \frac{1}{2^{n/2}} \sum_{\widehat{z} \in \widehat{\mathcal{Y}}} (-1)^{z \cdot y} \left|\widehat{z}\right\rangle \, .$$

Next, let $\mathcal{Z}$ denote the set $\mathcal{Y} \cup \{\perp\}$ for a special symbol $\perp$; similarly $\widehat{\mathcal{Z}}$ will denote $\widehat{\mathcal{Y}} \cup \{\perp\}$. We also choose a corresponding norm-1 vector $|\perp\rangle$ orthogonal

[1] Remark that the TPRP security would only hold against unidirectional quantum distinguishers.

to $\mathbb{C}^{2^n}$, so that the span of both $\overline{B_C} := \{|y\rangle \mid y \in \mathcal{Z}\}$ and $\overline{B_F} := \{\,\left|\widehat{y}\right\rangle \mid \widehat{y} \in \widehat{\mathcal{Z}}\}$ is $\mathbb{C}^{2^n+1}$; we'll call $\overline{B_C}$ and $\overline{B_F}$ the computational basis and Fourier basis respectively of the extended space $\mathbb{C}^{2^n+1}$.

Functions and Databases. Let $\mathcal{X}$ denote $\{0,1\}^m$ for some arbitrary m, and let $\mathcal{F}$ denote the set of m-bit-to-n-bit classical functions $f : \mathcal{X} \longrightarrow \mathcal{Y}$. The *quantum truth table* of f is defined as

$$|f\rangle := \bigotimes_{x \in \mathcal{X}} |x\rangle \, |f(x)\rangle \, .$$

Let $\widehat{\mathcal{F}}$ denote the set of *Fourier* functions $\widehat{f} : \mathcal{X} \longrightarrow \widehat{\mathcal{Y}}$. The quantum truth table of $\widehat{f}$ is defined similarly as

$$\left|\widehat{f}\,\right\rangle := \bigotimes_{x \in \mathcal{X}} |x\rangle \, \left|\widehat{f}(x)\right\rangle .$$

For a subset $\mathcal{S} \subseteq \mathcal{X}$, a function $f : \mathcal{S} \longrightarrow \mathcal{Y}$ will be called a *partial function* from $\mathcal{X}$ to $\mathcal{Y}$. A partial function f can be extended to a function $d_f : \mathcal{X} \longrightarrow \mathcal{Z}$ by defining $d_f(y) = \perp$ for all $y \in \mathcal{X} \setminus \mathcal{S}$. We call d_f the *database* representing f, with $\perp$ denoting the cells where f is not defined. (When f is a full function, d_f coincides with f.) The database will also be represented as a quantum truth table

$$|d_f\rangle := \bigotimes_{x \in \mathcal{X}} |x\rangle \, |d_f(x)\rangle \, .$$

Similarly we define partial Fourier functions $\widehat{f} : \mathcal{S} \longrightarrow \widehat{\mathcal{Y}}$, databases $d_{\widehat{f}} : \mathcal{X} \longrightarrow \widehat{\mathcal{Z}}$ representing partial Fourier functions, and their quantum truth tables $\left|d_{\widehat{f}}\right\rangle$. When f and $\widehat{f}$ are clear from context, we'll find it convenient to drop the subscripts and write d_f and $d_{\widehat{f}}$ simply as d and $\widehat{d}$ respectively. We'll write $\mathcal{D}$ (resp. $\widehat{\mathcal{D}}$) to denote the set of all databases $d : \mathcal{X} \longrightarrow \mathcal{Z}$ (resp. all Fourier databases $\widehat{d} : \mathcal{X} \longrightarrow \widehat{\mathcal{Z}}$). When convenient we will treat a database d as a relation on $\mathcal{X} \times \mathcal{Y}$ and write $(x, y) \in \mathcal{D}$ to denote $d(x) = y$; $|d|$ will then denote the size of this relation, i.e., the size of $\{x \in \mathcal{X} \mid d(x) \in \mathcal{Y}\}$.

Our notation allows us to define an easy correspondence between classical functions and Fourier functions: for any function $f \in \mathcal{F}$, let $\widehat{f} \in \widehat{\mathcal{F}}$ be defined as the map $x \mapsto \widehat{f(x)}$. Then we have

$$\left|\widehat{f}\,\right\rangle = \frac{1}{2^{n2^m/2}} \sum_{g \in \mathcal{F}} (-1)^{f \cdot g} \, |g\rangle \, , \tag{27}$$

where $f \cdot g$ is defined as $\sum_{x \in \mathcal{X}} f(x) \cdot g(x)$. (For a proof of (27) see App. B.) Thus, $\{|f\rangle \mid f \in \mathcal{F}\}$ and $\{\,\left|\widehat{f}\,\right\rangle \mid \widehat{f} \in \widehat{\mathcal{F}}\}$ span the same space (isomorphic to $\mathbb{C}^{2^{n2^m}}$). Similarly we can show that $\{|d\rangle \mid d \in \mathcal{D}\}$ and $\{\,\left|\widehat{d}\,\right\rangle \mid \widehat{d} \in \widehat{\mathcal{D}}\}$ span the same space isomorphic to $\mathbb{C}^{(2^n+1)^{2^m}}$; we call this space the *database space* $\mathbb{D}$.

Letting $\mathbf{0}$ denote the constant 0^n function and observing that $\mathbf{0} \cdot g = 0$ for any $g \in \mathcal{F}$, we have

$$\left|\widehat{\mathbf{0}}\right\rangle = \frac{1}{2^{n2^m/2}} \sum_{g \in \mathcal{F}} |g\rangle \,,$$

the uniform superposition over all functions in $\mathcal{F}$.

The Fourier Oracle. Given a truth-table representation $\left|f\right\rangle$ of a function $f \in \mathcal{F}$, the standard oracle acts on the adversary registers $|x\rangle\,|y\rangle$ and the truth-table registers $\left|f\right\rangle$ as

$$\mathsf{stO}\,|x\rangle\,|y\rangle \otimes \left|f\right\rangle = |x\rangle\,\left|y \oplus f(x)\right\rangle \otimes \left|f\right\rangle .$$

If we first put the adversary's response register and the truth-table register in the Fourier basis first, we have

$$\mathsf{stO}\,|x\rangle\,\left|\widehat{y}\right\rangle \otimes \left|\widehat{f}\,\right\rangle = |x\rangle\,\left|\widehat{y}\right\rangle \otimes \left|\widehat{f} + \widehat{\delta}_{xy}\right\rangle , \tag{28}$$

where δ_{xy} is the function in $\mathcal{F}$ defined as

$$\begin{aligned} \delta_{xy}(z) &= y, && \text{when } z = x, \\ &= 0, && \text{otherwise,} \end{aligned}$$

and the operations $\oplus$ in $\mathcal{F}$ and $+$ in $\widehat{\mathcal{F}}$ are defined point-wise. (For a proof of (28) see App. B.) We define the operator $\mathsf{O}_{x\widehat{y}}$ on the truth-table register as

$$\mathsf{O}_{x\widehat{y}}\left|\widehat{f}\,\right\rangle := \left|\widehat{f} + \widehat{\delta}_{xy}\right\rangle .$$

Then we can write

$$\mathsf{stO}\,|x\rangle\,\left|\widehat{y}\right\rangle \otimes \left|\widehat{f}\,\right\rangle = |x\rangle\,\left|\widehat{y}\right\rangle \otimes \mathsf{O}_{x\widehat{y}}\left|\widehat{f}\,\right\rangle .$$

The Compressed Oracle. The *cell compression* unitary comp_0 on $\mathbb{C}^{2^n+1}$ is defined on the basis $\overline{B_F}$ as

$$\mathsf{comp}_0 := |\bot\rangle\langle\widehat{0}| + |\widehat{0}\rangle\langle\bot| + \sum_{\widehat{y} \in \widehat{\mathcal{Y}} \setminus \{\widehat{0}\}} |\widehat{y}\rangle\langle\widehat{y}| .$$

Then, for any $\left|\widehat{y}\right\rangle \in \overline{B_F}$, we have

$$\begin{aligned} \mathsf{comp}_0\left|\widehat{y}\right\rangle &= |\bot\rangle , && \text{when } \widehat{y} = \widehat{0}, \\ &= \left|\widehat{0}\right\rangle , && \text{when } \widehat{y} = \bot, \\ &= \left|\widehat{y}\right\rangle , && \text{otherwise.} \end{aligned}$$

For any r let I_r denote the identity operation over r qubits. Then the *database compression* unitary comp on $\mathbb{D}$ is defined as

$$\mathsf{comp} := \bigotimes_{\mathcal{X}} (I_m \otimes \mathsf{comp}_0).$$

The *compressed oracle* cO is defined jointly on the adversary's registers and the oracle's database registers as

$$\mathsf{cO} := (I_{m+n} \otimes \mathsf{comp}) \circ \mathsf{stO} \circ (I_{m+n} \otimes \mathsf{comp}).$$

For a database $\widehat{d}$ we have

$$\mathsf{cO}\,|x\rangle\,\left|\widehat{y}\right\rangle \otimes \left|\widehat{d}\,\right\rangle = |x\rangle\,\left|\widehat{y}\right\rangle \otimes \mathsf{cO}_{x\widehat{y}}\,\left|\widehat{d}\,\right\rangle,$$

where $\mathsf{cO}_{x\widehat{y}} := \mathsf{comp} \circ \mathsf{O}_{x\widehat{y}} \circ \mathsf{comp}$.

Domain-Restricted Databases. For a subset $\widetilde{\mathcal{X}}$ of $\mathcal{X}$ we will write $\mathcal{D}|_{\widetilde{\mathcal{X}}}$ to denote the set of databases restricted to $\widetilde{\mathcal{X}}$, defined equivalently as $\{d|_{\widetilde{\mathcal{X}}} \mid d \in \mathcal{D}\}$ or the set of databases $d : \widetilde{\mathcal{X}} \longrightarrow \mathcal{Z}$. While this is technically equivalent to a partial function from $\mathcal{X}$ to $\mathcal{Z}$, we emphasise the distinction that in the case of a domain-restricted database, we do not expect it to be queried on any $x \notin \widetilde{\mathcal{X}}$.

Since $\mathcal{D}$ is a basis of the database space $\mathbb{D}$, a domain-restricted database space will span a subspace of $\mathbb{D}$ isomorphic to $\mathbb{C}^{(2^n+1)^{|\widetilde{\mathcal{X}}|}}$; usually we won't need to refer to this space explicitly. We continue to represent elements of $\widetilde{\mathcal{X}}$ as m-bit numbers.

Transition Capacity. For a domain-restricted database-set $\mathcal{D}|_{\widetilde{\mathcal{X}}}$, a subset $\mathcal{P} \subseteq \mathcal{D}|_{\widetilde{\mathcal{X}}}$ will be called a *database property* on $\mathcal{D}|_{\widetilde{\mathcal{X}}}$. We also define the projection

$$\mathit{\Pi}_{\mathcal{P}} := \sum_{d \in \mathcal{P}} |d\rangle\langle d|\,.$$

For a database $d \in \mathcal{D}|_{\widetilde{\mathcal{X}}}$ and an $x \in \widetilde{\mathcal{X}}$ define

$$d|^{x} := \{d' \in \mathcal{D}|_{\widetilde{\mathcal{X}}} \mid d'(x') = d(x') \forall x' \in \widetilde{\mathcal{X}} \setminus \{x\}\}.$$

In other words, $d|^{x}$ is the set of databases in $\mathcal{D}|_{\widetilde{\mathcal{X}}}$ which are identical to d except (possibly) at x. (Note that since d (resp. x) is also in $\mathcal{D}$ (resp. $\mathcal{X}$), $d|^{x}$ is only well-defined when we specify $\mathcal{D}|_{\widetilde{\mathcal{X}}}$ as well; however, since $\mathcal{D}|_{\widetilde{\mathcal{X}}}$ will usually be clear from the context, for notational convenience we leave the dependence of $d|^{x}$ on $\mathcal{D}|_{\widetilde{\mathcal{X}}}$ implicit.)

For two properties $\mathcal{P}$ and $\mathcal{P}'$, the *transition capacity* from $\mathcal{P}$ to $\mathcal{P}'$ is defined as

$$[\![\mathcal{P} \hookrightarrow \mathcal{P}']\!] := \max_{x \in \widetilde{\mathcal{X}}, \widehat{y} \in \widehat{\mathcal{Y}}, d \in \mathcal{D}|_{\widetilde{\mathcal{X}}}} \left\| \mathit{\Pi}_{\mathcal{P}' \cap d|^{x}} \circ \mathsf{cO}_{x\widehat{y}} \circ \mathit{\Pi}_{\mathcal{P} \cap d|^{x}} \right\|.$$

The transition capacity $[\![\mathcal{P} \hookrightarrow \mathcal{P}']\!]$ is roughly a measure of an upper bound for how likely it can be that a database in $\mathcal{P}$ will transition into a database in $\mathcal{P}'$ after a single query to cO.

For any property $\mathcal{P}$ let $\bar{\mathit{\Pi}}_{\mathcal{P}} := I_{m+n} \otimes \mathit{\Pi}_{\mathcal{P}}$. We adapt the following useful proposition from an intermediate result in [11, Proof of Lemma 5.6]. (For a proof see App. C.)

Proposition 5. *For any pair of properties $\mathcal{P}$ and $\mathcal{P}'$,*

$$[\![\mathcal{P} \hookrightarrow \mathcal{P}']\!] \geq \left\| \bar{\Pi}_{\mathcal{P}'} \circ \mathsf{cO} \circ \bar{\Pi}_{\mathcal{P}} \right\|.$$

For a property $\mathcal{P} \subseteq \mathcal{D}|_{\widetilde{\mathcal{X}}}$, let $\mathcal{P}^c$ denote its negation, i.e., $\mathcal{D}|_{\widetilde{\mathcal{X}}} \setminus \mathcal{P}$. Then we have the following lemma, adapted from [11, Theorem 5.17]. (For a proof see App. D.)

Lemma 1 (Transition Capacity Bound). *Let $\mathcal{P}, \mathcal{P}'$ be properties on $\mathcal{D}|_{\widetilde{\mathcal{X}}}$ such that for every $x \in \widetilde{\mathcal{X}}$ and $d \in \mathcal{D}|_{\widetilde{\mathcal{X}}}$, we can find a set $\mathcal{S}_{x,d}^{\mathcal{P}^c \hookrightarrow \mathcal{P}'} \subseteq \mathcal{Y}$ satisfying*

$$\mathcal{P}' \cap d|^x \subseteq \{d' \in d|^x \mid d'(x) \in \mathcal{S}_{x,d}^{\mathcal{P}^c \hookrightarrow \mathcal{P}'}\} \subseteq \mathcal{P} \cap d|^x. \tag{29}$$

In other words, for any database $d' \in d|^x$,

$$d' \in \mathcal{P}' \implies d'(x) \in \mathcal{S}_{x,d}^{\mathcal{P}^c \hookrightarrow \mathcal{P}'} \implies d' \in \mathcal{P}.$$

Then we have

$$[\![\mathcal{P}^c \hookrightarrow \mathcal{P}']\!] \leq \max_{x \in \widetilde{\mathcal{X}}, d \in \mathcal{D}|_{\widetilde{\mathcal{X}}}} \sqrt{\frac{10 |\mathcal{S}_{x,d}^{\mathcal{P}^c \hookrightarrow \mathcal{P}'}|}{2^n}}.$$

Size-restricted Properties. For a domain-restricted database-set $\mathcal{D}|_{\widetilde{\mathcal{X}}}$, a property $\mathcal{P} \subseteq \mathcal{D}|_{\widetilde{\mathcal{X}}}$, and some $i \leq |\widetilde{\mathcal{X}}|$, we define

$$\mathcal{P}_{[\leq i]} := \{d \in \mathcal{P} \mid |d| \leq i\}.$$

Then the transition capacity $[\![\mathcal{P}^c_{[\leq i-1]} \hookrightarrow \mathcal{P}_{[\leq i]}]\!]$ is a measure of the maximum probability of a database outside $\mathcal{P}$ with at most $i-1$ entries changing to a database in $\mathcal{P}$ after a single application $\mathsf{cO}_{x\widehat{y}}$. (Note that $\mathcal{P}^c_{[\leq i-1]}$ denotes the size-restriction of $\mathcal{P}^c$, and not the complement of $\mathcal{P}_{[\leq i-1]}$.)

Let $\perp := \{d_\perp\}$ denote the *empty* property (where $d_\perp$ is the empty database, i.e., the constant-$\perp$ function). Then for $\mathcal{P}$ such that $d_\perp \notin \mathcal{P}$, $\perp = \mathcal{P}_{[\leq 0]}$. We define

$$\left(\perp \overset{q}{\rightsquigarrow} \mathcal{P}\right) := \sum_{i=1}^{q} [\![\mathcal{P}^c_{[\leq i-1]} \hookrightarrow \mathcal{P}_{[\leq i]}]\!],$$

the *q-query transition bound* from $\perp$ to $\mathcal{P}$. In other words, $\left(\perp \overset{q}{\rightsquigarrow} \mathcal{P}\right)$ is a measure of the probability that the empty database changes into a database in $\mathcal{P}$ *at any point* during q successive queries. We point out that this is different from the q-query transition capacity defined in [11], which only considers a transition after *exactly* q queries.

Two-Domain Systems. Fix two domains $\widetilde{\mathcal{X}}_0, \widetilde{\mathcal{X}}_1 \subseteq \mathcal{X}$, and define $\mathcal{D}_0 := \mathcal{D}|_{\widetilde{\mathcal{X}}_0}$ and $\mathcal{D}_1 := \mathcal{D}|_{\widetilde{\mathcal{X}}_1}$. Consider properties $\mathcal{B}_0 \subseteq \mathcal{D}_0 \setminus \perp$ and $\mathcal{B}_1 \subseteq \mathcal{D}_1 \setminus \perp$, and define $\mathcal{G}_0 := \mathcal{D}_0 \setminus \mathcal{B}_0$ and $\mathcal{G}_1 := \mathcal{D}_1 \setminus \mathcal{B}_1$. In addition let $\mathcal{I} \subseteq \mathcal{X}$ be an additional domain called the *input domain*, along with two injective input-preparation maps $p_0 : \mathcal{I} \longrightarrow \widetilde{\mathcal{X}}_0$ and $p_1 : \mathcal{I} \longrightarrow \widetilde{\mathcal{X}}_1$ that cast an input from $\mathcal{I}$ into their respective domains. Let the oracles cO_0 and cO_1 be defined as

$$\mathsf{cO}_0 \left|x\right\rangle \left|\widehat{y}\right\rangle \otimes \left|\widehat{d_0}\right\rangle = \left|x\right\rangle \left|\widehat{y}\right\rangle \otimes \mathsf{cO}_{p_0(x)\widehat{y}} \left|\widehat{d_0}\right\rangle ,$$
$$\mathsf{cO}_1 \left|x\right\rangle \left|\widehat{y}\right\rangle \otimes \left|\widehat{d_1}\right\rangle = \left|x\right\rangle \left|\widehat{y}\right\rangle \otimes \mathsf{cO}_{p_1(x)\widehat{y}} \left|\widehat{d_1}\right\rangle ,$$

for any $x \in \mathcal{I}$, $\widehat{y} \in \widehat{\mathcal{Y}}$, $d_0 \in \mathcal{D}_0$ and $d_1 \in \mathcal{D}_1$. Let $I_{\mathbb{D}}$ denote the identity over $\mathbb{D}$ (which is also the identity over the subspaces of $\mathbb{D}$ spanned by $\mathcal{D}_0$ and $\mathcal{D}_1$). Finally, denoting $\left|\psi_\perp\right\rangle := \left|0\right\rangle \left|\widehat{0}\right\rangle \otimes \left|d_\perp\right\rangle$, define

$$\mathcal{T}_0^q(U_0, \dots, U_q) := \Big\| (U_q \otimes I_{\mathbb{D}}) \circ \mathsf{cO}_0 \circ (U_{q-1} \otimes I_{\mathbb{D}}) \circ \mathsf{cO}_0 \circ \dots$$
$$\circ\, \mathsf{cO}_0 \circ (U_1 \otimes I_{\mathbb{D}}) \circ \mathsf{cO}_0 \circ (U_0 \otimes I_{\mathbb{D}}) \left|\psi_\perp\right\rangle \Big\| ,$$
$$\mathcal{T}_1^q(U_0, \dots, U_q) := \Big\| (U_q \otimes I_{\mathbb{D}}) \circ \mathsf{cO}_1 \circ (U_{q-1} \otimes I_{\mathbb{D}}) \circ \mathsf{cO}_1 \circ \dots$$
$$\circ\, \mathsf{cO}_1 \circ (U_1 \otimes I_{\mathbb{D}}) \circ \mathsf{cO}_1 \circ (U_0 \otimes I_{\mathbb{D}}) \left|\psi_\perp\right\rangle \Big\| ,$$

for unitaries $U_0, \dots, U_q$ acting on $m + n$ qubits.

The central tool of our proof technique will be the following result, adapted from [17, Proposition 3].

Lemma 2 (Two-Domain Distance Lemma). *Suppose we can find a map* $h : \mathcal{G}_0 \longrightarrow \mathcal{G}_1$ *such that the following hold:*

- *h is a bijection from $\mathcal{G}_0$ to $\mathcal{G}_1$ (and hence $|\mathcal{G}_0| = |\mathcal{G}_1|$);*
- *For every $i \in [q-1] \cup \{0\}$, $h|_{\mathcal{G}_{0[\leq i]}}$ is a bijection from $\mathcal{G}_{0[\leq i]}$ to $\mathcal{G}_{1[\leq i]}$ (and hence $|\mathcal{G}_{0[\leq i]}| = |\mathcal{G}_{1[\leq i]}|$);*
- *For every $i \in [q]$, $x \in \mathcal{I}$, $\widehat{y} \in \widehat{\mathcal{Y}}$, $d \in \mathcal{G}_{0[\leq i-1]}$, and $d' \in \mathcal{G}_{0[\leq i]}$,*

$$\left\langle d' \middle| \mathsf{cO}_{p_0(x)\widehat{y}} \middle| d \right\rangle = \left\langle h(d') \middle| \mathsf{cO}_{p_1(x)\widehat{y}} \middle| h(d) \right\rangle .$$

Then we have

$$\sup_{U_0, \dots, U_q} \left| \mathcal{T}_0^q(U_0, \dots, U_q) - \mathcal{T}_1^q(U_0, \dots, U_q) \right| \leq \Big(\perp \overset{q}{\rightsquigarrow} \mathcal{B}_0 \Big)_0 + \Big(\perp \overset{q}{\rightsquigarrow} \mathcal{B}_1 \Big)_1 ,$$

where the transition bounds $\Big(\perp \overset{q}{\rightsquigarrow} \cdot \Big)_0$ and $\Big(\perp \overset{q}{\rightsquigarrow} \cdot \Big)_1$ are defined for queries to cO_0 and cO_1 respectively, and the supremum is taken over all unitaries $U_0, \dots, U_q$ acting on $m + n$ qubits.

When the oracle in use is clear from the context, we will drop the subscripts for the transition bounds and simply write both as $\Big(\perp \overset{q}{\rightsquigarrow} \cdot \Big)$. We'll also keep the input-preparation maps implicit when there's not scope for ambiguity.

Proof. Fix $U_0, \dots, U_q$, and let $\mathcal{T}_0$ and $\mathcal{T}_1$ denote $\mathcal{T}_0^q(U_0, \dots, U_q)$ and $\mathcal{T}_1^q(U_0, \dots, U_q)$ respectively. We'll use the shorthand notation $\ddot{U}_i := U_i \otimes I_{\mathbb{D}}$ for any $i \in [0..q]$. Let $|\psi_0\rangle := \ddot{U}_0 |\psi_\perp\rangle = (U_0 |0\rangle \left|\widehat{0}\right\rangle) \otimes |d_\perp\rangle$. For each $i \in [q]$ define $W_{i,0} := \ddot{U}_i \circ \mathsf{cO}_0$, $W_{i,1} := \ddot{U}_i \circ \mathsf{cO}_1$. Then we can write

$$\begin{aligned} \mathcal{T}_0 &:= \Big\| W_{q,0} \circ W_{q-1,0} \circ \dots \circ W_{1,0} |\psi_0\rangle \Big\|, \\ \mathcal{T}_1 &:= \Big\| W_{q,1} \circ W_{q-1,1} \circ \dots \circ W_{1,1} |\psi_0\rangle \Big\|. \end{aligned}$$

For each $i \in [q]$ define

$$\begin{aligned} W_{i,0}^b &:= \bar{\Pi}_{\mathcal{B}_{0[\leq i]}} \circ W_{i,0}, & W_{i,1}^b &:= \bar{\Pi}_{\mathcal{B}_{1[\leq i]}} \circ W_{i,1}, \\ W_{i,0}^g &:= \bar{\Pi}_{\mathcal{G}_{0[\leq i]}} \circ W_{i,0}, & W_{i,1}^g &:= \bar{\Pi}_{\mathcal{G}_{1[\leq i]}} \circ W_{i,1}. \end{aligned}$$

Then we can write

$$W_{i,0} = W_{i,0}^b + W_{i,0}^g, \quad W_{i,1} = W_{i,1}^b + W_{i,1}^g.$$

For each $i \in [q]$ further define

$$\begin{aligned} |\psi_{i,0}\rangle &:= W_{i,0} \circ \dots \circ W_{1,0} |\psi_0\rangle, & |\psi_{i,1}\rangle &:= W_{i,1} \circ \dots \circ W_{1,1} |\psi_0\rangle, \\ \left|\psi_{i,0}^g\right\rangle &:= W_{i,0}^g \circ \dots \circ W_{1,0}^g |\psi_0\rangle, & \left|\psi_{i,1}^g\right\rangle &:= W_{i,1}^g \circ \dots \circ W_{1,1}^g |\psi_0\rangle. \end{aligned}$$

Claim. For every $i \in [q]$,

$$\left\| |\psi_{i,0}\rangle - \left|\psi_{i,0}^g\right\rangle \right\| \leq \Big(\perp \overset{i}{\rightsquigarrow} \mathcal{B}_0\Big)_0, \qquad \left\| |\psi_{i,1}\rangle - \left|\psi_{i,1}^g\right\rangle \right\| \leq \Big(\perp \overset{i}{\rightsquigarrow} \mathcal{B}_1\Big)_1.$$

Proof (of Claim). We will show the first inequality by induction, and claim the second one by symmetry. For the base case of $i = 1$, we have

$$\left\| |\psi_{1,0}\rangle - \left|\psi_{1,0}^g\right\rangle \right\| = \left\| W_{1,0} |\psi_0\rangle - W_{1,0}^g |\psi_0\rangle \right\| = \left\| W_{1,0}^b |\psi_0\rangle \right\|.$$

Since $d_\perp \in \mathcal{G}_0$, and $\ddot{U}_1$ commutes with $\bar{\Pi}_{\mathcal{B}_{0[\leq 1]}}$, we have

$$\begin{aligned} \left\| W_{1,0}^b |\psi_0\rangle \right\| &= \left\| \bar{\Pi}_{\mathcal{B}_{0[\leq 1]}} \circ W_{1,0} \circ \bar{\Pi}_{\mathcal{G}_{0[\leq 0]}} |\psi_0\rangle \right\| \\ &= \Big\| \bar{\Pi}_{\mathcal{B}_{0[\leq 1]}} \circ \ddot{U}_1 \circ \mathsf{cO}_0 \circ \bar{\Pi}_{\mathcal{G}_{0[\leq 0]}} |\psi_0\rangle \Big\| \\ &= \Big\| \ddot{U}_1 \circ \bar{\Pi}_{\mathcal{B}_{0[\leq 1]}} \circ \mathsf{cO}_0 \circ \bar{\Pi}_{\mathcal{G}_{0[\leq 0]}} |\psi_0\rangle \Big\| \\ &\leq \left\| \bar{\Pi}_{\mathcal{B}_{0[\leq 1]}} \circ \mathsf{cO}_0 \circ \bar{\Pi}_{\mathcal{G}_{0[\leq 0]}} \right\| \leq \llbracket \mathcal{G}_{0[\leq 0]} \hookrightarrow \mathcal{B}_{0[\leq 1]} \rrbracket_0 = \Big(\perp \overset{1}{\rightsquigarrow} \mathcal{B}_0\Big)_0, \end{aligned}$$

where the last inequality in the last line follows from Proposition 5. This proves the base case. Our induction hypothesis will be that for some $i \geq 2$,

$$\left\| |\psi_{i-1,0}\rangle - \left|\psi_{i-1,0}^g\right\rangle \right\| \leq \Big(\perp \overset{i-1}{\rightsquigarrow} \mathcal{B}_0\Big)_0.$$

Then we have

$$\begin{aligned}\big\| |\psi_{i,0}\rangle - |\psi^g_{i,0}\rangle \big\| &= \big\| W_{i,0} |\psi_{i-1,0}\rangle - W^g_{i,0} |\psi^g_{i-1,0}\rangle \big\| \\ &= \big\| W_{i,0} |\psi_{i-1,0}\rangle - W_{i,0} |\psi^g_{i-1,0}\rangle + W_{i,0} |\psi^g_{i-1,0}\rangle - W^g_{i,0} |\psi^g_{i-1,0}\rangle \big\| \\ &= \big\| W_{i,0}(|\psi_{i-1,0}\rangle - |\psi^g_{i-1,0}\rangle) + (W_{i,0} - W^g_{i,0}) |\psi^g_{i-1,0}\rangle \big\| \\ &\le \big\| W_{i,0}(|\psi_{i-1,0}\rangle - |\psi^g_{i-1,0}\rangle) \big\| + \big\| W^b_{i,0} |\psi^g_{i-1,0}\rangle \big\| \\ &\le \big\| |\psi_{i-1,0}\rangle - |\psi^g_{i-1,0}\rangle \big\| + \big\| \bar{\mathit{\Pi}}_{\mathcal{B}_{0[\le i]}} \circ W_{i,0} |\psi^g_{i-1,0}\rangle \big\|. \end{aligned}$$

By definition of $|\psi^g_{i-1,0}\rangle$, it is in the column space of $\bar{\mathit{\Pi}}_{\mathcal{G}_{0[\le i-1]}}$. Thus, by reasoning as in the base case above, we have

$$\big\| \bar{\mathit{\Pi}}_{\mathcal{B}_{0[\le i]}} \circ W_{i,0} |\psi^g_{i-1,0}\rangle \big\| \le \big\| \bar{\mathit{\Pi}}_{\mathcal{B}_{0[\le i]}} \circ \mathsf{cO}_0 \circ \bar{\mathit{\Pi}}_{\mathcal{G}_{0[\le i-1]}} \big\| \le \llbracket \mathcal{G}_{0[\le i-1]} \hookrightarrow \mathcal{B}_{0[\le i]} \rrbracket_0 .$$

Using the above inequality and the induction hypothesis we get

$$\begin{aligned}\big\| |\psi_{i,0}\rangle - |\psi^g_{i,0}\rangle \big\| &\le \big\| |\psi_{i-1,0}\rangle - |\psi^g_{i-1,0}\rangle \big\| + \big\| \bar{\mathit{\Pi}}_{\mathcal{B}_{0[\le i]}} \circ W_{i,0} |\psi^g_{i-1,0}\rangle \big\| \\ &\le \Big(\perp \overset{i-1}{\rightsquigarrow} \mathcal{B}_0 \Big)_0 + \llbracket \mathcal{G}_{0[\le i-1]} \hookrightarrow \mathcal{B}_{0[\le i]} \rrbracket_0 = \Big(\perp \overset{i}{\rightsquigarrow} \mathcal{B}_0 \Big)_0 , \end{aligned}$$

thus completing the proof of the first inequality in the claim. The second inequality follows by symmetry. □

For any $x \in \mathcal{I}, \widehat{y} \in \widehat{\mathcal{Y}}, d \in \mathcal{D}_0$, let $|\varphi_{x,\widehat{y},d}\rangle$ denote the basis state $|x\rangle\,|\widehat{y}\rangle \otimes |d\rangle$, and let $|\varphi_{x,\widehat{y},h(d)}\rangle$ denote the basis state $|x\rangle\,|\widehat{y}\rangle \otimes |h(d)\rangle$. We next observe that for any $x, \widehat{y}$, any $i \in [q]$, and any $d \in \mathcal{G}_{0[\le i]}$,

$$\langle \varphi_{x,\widehat{y},d} | \psi^g_{i,0} \rangle = \langle \varphi_{x,\widehat{y},h(d)} | \psi^g_{i,1} \rangle . \tag{30}$$

This can be shown inductively by carefully tracking the coefficients on both sides and using the third condition of the lemma statement. (For a detailed proof see App. B.) Using this observation we can show that for any $i \in [q]$,

$$\big\| \psi^g_{i,0} \big\| = \sqrt{\sum_{x,\widehat{y},d \in \mathcal{G}_{0[\le i]}} \langle \varphi_{x,\widehat{y},d} | \psi^g_{i,0} \rangle^2} = \sqrt{\sum_{x,\widehat{y},d' \in \mathcal{G}_{1[\le i]}} \langle \varphi_{x,\widehat{y},d'} | \psi^g_{i,1} \rangle^2} = \big\| \psi^g_{i,1} \big\| . \tag{31}$$

Thus we have

$$\begin{aligned}\big| \mathcal{T}_0 - \mathcal{T}_1 \big| &= \big| \| |\psi_{q,0}\rangle \| - \| |\psi_{q,1}\rangle \| \big| \\ &\le \Big| \| |\psi_{q,0}\rangle \| - \| |\psi^g_{q,0}\rangle \| \Big| + \Big| \| |\psi_{q,1}\rangle \| - \| |\psi^g_{q,1}\rangle \| \Big| + \Big| \| |\psi^g_{q,0}\rangle \| - \| |\psi^g_{q,1}\rangle \| \Big| \\ &= \Big| \| |\psi_{q,0}\rangle \| - \| |\psi^g_{q,0}\rangle \| \Big| + \Big| \| |\psi_{q,1}\rangle \| - \| |\psi^g_{q,1}\rangle \| & (32) \\ &\le \big\| |\psi_{q,0}\rangle - |\psi^g_{q,0}\rangle \big\| + \big\| |\psi_{q,1}\rangle - |\psi^g_{q,1}\rangle \big\| & (33) \\ &\le \Big(\perp \overset{q}{\rightsquigarrow} \mathcal{B}_0 \Big)_0 + \Big(\perp \overset{q}{\rightsquigarrow} \mathcal{B}_1 \Big)_1 , & (34) \end{aligned}$$

where (32) follows from (31), (33) uses the triangle inequality for norms, and (34) follows from the claim. Since the bound above is free of $U_0, \ldots, U_q$, taking supremum over $U_0, \ldots, U_q$ completes the proof the lemma. □

5 Post-Quantum PRF Security of TNT, LRQ and LRWQ

Equipped with the quantum proof machinery developed in section 4, we now delve into the security proofs for the three PRF candidates, namely, TNT, LRQ, and LRWQ.

5.1 Security of TNT

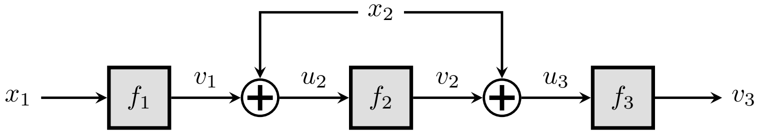

Fig. 2: The TNT construction by Bao et al. [2].

In this section, we analyse the post-quantum security of TNT (see Fig. 2), defined as

$$g_{\mathsf{re}}^{\mathsf{TNT}}(x_1, x_2) := f_3(f_2(f_1(x_1) \oplus x_2) \oplus x_2)$$

for three n-bit-to-n-bit random functions f_1, f_2, f_3. We want to bound the distinguishing advantage between $g_{\mathsf{re}}^{\mathsf{TNT}}$ (the *real world*) and a $2n$-bit-to-n-bit random function g_{id} (the *ideal world*).

Theorem 2. *Let $\mathscr{A}$ be a (q, τ)-quantum adversary distinguishing g_{re}^{TNT} from g_{id}. Then there exists $(O(q), \tau_i)$-quantum distinguishers $\mathscr{B}_i$ against f_i, such that*

$$\mathbf{Adv}_{TNT}^{\mathsf{qprf}}(\mathscr{A}) \leq \sum_{i=1}^{3} \mathbf{Adv}_{f_i}^{\mathsf{qprp}}(\mathscr{B}_i) + 4\sqrt{\frac{10q^4}{2^n}},$$

where $\tau_i \in \widetilde{O}(\tau + q^2)$, for all $i \in \{1, 2, 3\}$.

Formulation of the Proof. As a first step, we observe that in order to establish Theorem 2, it is enough to show that when f_1, f_2, f_3 are perfect PRF's,

$$\mathbf{Adv}_{\mathsf{TNT}}^{\mathsf{qprf}}(\mathscr{A}) \leq 4\sqrt{\frac{10q^4}{2^n}}.$$

We will look at a slightly modified representation of the game. Let $\mathcal{X} := \{0,1\}^{3n+2}$, and let $f : \mathcal{X} \longrightarrow \mathcal{Y}$ be a $(3n+2)$-bit-to-n-bit random function, such that for each $x, x' \in \mathcal{Y}$,

$$f_1(x) = f(00\|x\|0^{2n}), \qquad f_2(x) = f(01\|x\|0^{2n}),$$
$$f_3(x) = f(10\|x\|0^{2n}), \qquad g_{\mathsf{id}}(x_1, x_2) = f(11\|x\|x'\|0^n).$$

The distinctness of the first two bits ensures that $f_1, f_2, f_3, g_{\mathsf{id}}$ are all independent. Thus, this game is identical to the one we began with. Next, we replace g_{id} by g^*_{id}, defined as

$$g^*_{\mathsf{id}}(x_1, x_2) := f(11\|x_1\|x_2\|f_2(f_1(x_1) \oplus x_2) \oplus x_2),$$

where we also call f_1 and f_2 in the ideal world. Since $f_2(f_1(x_1) \oplus x_2) \oplus x_2$ is a function of x_1 and x_2, g^*_{id} is still a random function of $x_1\|x_2$, making this game to behave identically with the one we started with.

This setup allows us to use a single database $d_f : \mathcal{X} \longrightarrow \mathcal{Z}$ to keep track of f_1, f_2, f_3, and g^*_{id}; we refer to this database as d_{re} in the real world (tracking f_1, f_2, and f_3) and d_{id} in the ideal world (tracking f_1, f_2, and g^*_{id}). Let $\mathcal{D}_{\mathsf{re}}$ (resp. $\mathcal{D}_{\mathsf{id}}$) be the set of all possible choices for d_{re} (resp. d_{id}).

Let $[x]_1$ denote $00\|x\|0^{2n}$, $[x]_2$ denote $01\|x\|0^{2n}$, and $[x]_3$ denote $10\|x\|0^{2n}$. Define $\widetilde{\mathcal{X}}_{\mathsf{re}} := \{[x]_1, [x]_2, [x]_3 \mid x \in \mathcal{Y}\}$ and $\widetilde{\mathcal{X}}_{\mathsf{id}} := \{[x]_1, [x]_2, 11\|x\|x'\|y \mid x, x', y \in \mathcal{Y}\}$. Then it is easy to see that $\mathcal{D}_{\mathsf{re}} = \mathcal{D}|_{\widetilde{\mathcal{X}}_{\mathsf{re}}}$ and $\mathcal{D}_{\mathsf{id}} = \mathcal{D}|_{\widetilde{\mathcal{X}}_{\mathsf{id}}}$. Thus we can represent our game as a two-domain system, with the labels re and id replacing 0 and 1 from Sect. 4; we extend this convention to the rest of the notation developed in Sect. 4 to avoid defining everything all over again. Then we can say

$$\mathbf{Adv}^{\mathsf{qprf}}_{\mathsf{TNT}}(\mathscr{A}) \leq \sup_{U_0,\ldots,U_q} \left| \mathcal{T}^{3q}_{\mathsf{re}}(U_0, \ldots, U_q) - \mathcal{T}^{3q}_{\mathsf{id}}(U_0, \ldots, U_q) \right|,$$

since there are $3q$ calls to f (and hence to cO) during the game.

Let $\mathcal{B}_{\mathsf{re}}$ be the set of databases d_{re} satisfying the following condition: we can find $x_1, v_1, x'_1, v'_1, x_2, v_2, x'_2, v'_2, v_3 \in \mathcal{Y}$ such that

– $([x_1]_1, v_1), ([x'_1]_1, v'_1), ([v_1 \oplus x_2]_2, v_2), ([v'_1 \oplus x'_2]_2, v'_2) \in d_{\mathsf{re}}$;
– $v_2 \oplus x_2 = v'_2 \oplus x'_2$;
– $([v_2 \oplus x_2]_3, v_3) \in d_{\mathsf{re}}$.

Next, let $\mathcal{B}_{\mathsf{id}}$ be the set of databases d_{id} satisfying the following condition: we can find $x_1, v_1, x'_1, v'_1, x_2, v_2, x'_2, v'_2, v_3 \in \mathcal{Y}$ such that

– $([x_1]_1, v_1), ([x'_1]_1, v'_1), ([v_1 \oplus x_2]_2, v_2), ([v'_1 \oplus x'_2]_2, v'_2) \in d_{\mathsf{id}}$;
– $v_2 \oplus x_2 = v'_2 \oplus x'_2$;
– One of $(11\|x_1\|x_2\|(v_2 \oplus x_2), v_3)$ and $(11\|x'_1\|x'_2\|(v_2 \oplus x_2), v_3) \in d_{\mathsf{id}}$.

Let $\mathcal{G}_{\mathsf{re}} := \mathcal{D}_{\mathsf{re}} \setminus \mathcal{B}_{\mathsf{re}}$ and $\mathcal{G}_{\mathsf{id}} := \mathcal{D}_{\mathsf{id}} \setminus \mathcal{B}_{\mathsf{id}}$. Thus the above definitions mean that in both $\mathcal{G}_{\mathsf{re}}$ and $\mathcal{G}_{\mathsf{id}}$, each $u_3 := v_2 \oplus x_2$ is associated with a unique pair (x_1, x_2). Then we can define the bijection $h : \mathcal{G}_{\mathsf{re}} \longrightarrow \mathcal{G}_{\mathsf{id}}$ as follows: for each d_{re} we define $d_{\mathsf{id}} := h(d_{\mathsf{re}})$ such that

– for each $x_1 \in \mathcal{Y}$, $d_{\mathsf{id}}([x_1]_1) = d_{\mathsf{re}}([x_1]_1)$;
– for each $u_2 \in \mathcal{Y}$, $d_{\mathsf{id}}([u_2]_2) = d_{\mathsf{re}}([u_2]_2)$;
– for each $x_1, x_2 \in \mathcal{Y}$ and the associated u_3, $d_{\mathsf{id}}(11\|x_1\|x_2\|u_3) = d_{\mathsf{re}}([u_3]_3)$.

Then h satisfies the conditions of Lemma 2. To complete the proof of Theorem 2, we just need to show that

$$\left(\bot \overset{3q}{\rightsquigarrow} \mathcal{B}_{\mathsf{re}}\right) + \left(\bot \overset{3q}{\rightsquigarrow} \mathcal{B}_{\mathsf{id}}\right) \leq 4\sqrt{\frac{10q^4}{2^n}}.$$

Sequence of Actions. Each query by the adversary to its oracle results in a sequence of three queries to f, one each to f_1, f_2, and one to f_3 in the real world or g^*_{id} in the ideal world, in that order. We view the query response phase as a sequence of $3q$ (possibly duplicate) *actions* and analyze the transition capacity at each action.

Action of f_1: For $i \in \{3k+1 : 0 \leq k \leq q-1\}$, we first look at the transition capacity $[\![\mathcal{B}^c_{\mathsf{re}[\leq i-1]} \hookrightarrow \mathcal{B}_{\mathsf{re}[\leq i]}]\!]$. For any d_{re} with $|d_{\mathsf{re}}| \leq i-1$ and any $x \in \mathcal{Y}$, we have

$$\mathcal{S}^{\mathcal{B}^c_{\mathsf{re}} \hookrightarrow \mathcal{B}_{\mathsf{re}}}_{x,d} = \{d_{\mathsf{re}}([u_2]_2) \oplus u_2 \oplus u_3 \mid d_{\mathsf{re}}([u_2]_2) \neq \perp, d_{\mathsf{re}}([u_3]_3) \neq \perp\}\,.$$

There are at most $\lceil (i-1)/3 \rceil^2$ choices for the pair (u_2, u_3), so $|\mathcal{S}^{\mathcal{B}^c_{\mathsf{re}} \hookrightarrow \mathcal{B}_{\mathsf{re}}}_{x,d}| \leq \lceil (i-1)/3 \rceil^2 \leq q^2$, and from there using Lemma 1 we have

$$[\![\mathcal{B}^c_{\mathsf{re}[\leq i-1]} \hookrightarrow \mathcal{B}_{\mathsf{re}[\leq i]}]\!] \leq \sqrt{\frac{10q^2}{2^n}}, \qquad \forall\, i \in \{3k+1 : 0 \leq k \leq q-1\}. \tag{35}$$

By the same arguments we can also show that

$$[\![\mathcal{B}^c_{\mathsf{id}[\leq i-1]} \hookrightarrow \mathcal{B}_{\mathsf{id}[\leq i]}]\!] \leq \sqrt{\frac{10q^2}{2^n}}, \qquad \forall\, i \in \{3k+1 : 0 \leq k \leq q-1\}. \tag{36}$$

Action of f_2: Next we look at the transition capacity $[\![\mathcal{B}^c_{\mathsf{re}[\leq i-1]} \hookrightarrow \mathcal{B}_{\mathsf{re}[\leq i]}]\!]$ for $i \in \{3k+2 : 0 \leq k \leq q-1\}$. For any d_{re} with $|d_{\mathsf{re}}| \leq i-1$ and any $x \in \mathcal{Y}$, we have

$$\mathcal{S}^{\mathcal{B}^c_{\mathsf{re}} \hookrightarrow \mathcal{B}_{\mathsf{re}}}_{x,d} := \{d_{\mathsf{re}}([x_1]_1) \oplus x \oplus u_3 \mid d_{\mathsf{re}}([x_1]_1) \neq \perp, d_{\mathsf{re}}([u_3]_3) \neq \perp\}.$$

Again, there are at most $\lceil (i-1)/3 \rceil^2$ choices for the pair (x_1, u_3), and arguing as before we have

$$[\![\mathcal{B}^c_{\mathsf{re}[\leq i-1]} \hookrightarrow \mathcal{B}_{\mathsf{re}[\leq i]}]\!] \leq \sqrt{\frac{10q^2}{2^n}}, \qquad \forall\, i \in \{3k+2 : 0 \leq k \leq q-1\}. \tag{37}$$

By the same arguments we can also show that

$$[\![\mathcal{B}^c_{\mathsf{id}[\leq i-1]} \hookrightarrow \mathcal{B}_{\mathsf{id}[\leq i]}]\!] \leq \sqrt{\frac{10q^2}{2^n}}, \qquad \forall\, i \in \{3k+2 : 0 \leq k \leq q-1\}. \tag{38}$$

Action of f_3 (resp. g^*_{ID}): Finally, for $i \in \{3k : 1 \leq k \leq q\}$, for any d_{re} with $|d_{\mathsf{re}}| \leq i-1$ (resp. any d_{id} with $|d_{\mathsf{id}}| \leq i-1$) and any $x \in \mathcal{Y}$, since the property $\mathcal{B}_{\mathsf{re}}$ (resp. $\mathcal{B}_{\mathsf{id}}$) does not depend on $d_{\mathsf{re}}([x]_3)$ (resp. $d_{\mathsf{id}}(11\|x_1\|x_2\|x)$), we have $\mathcal{S}^{\mathcal{B}^c_{\mathsf{re}} \hookrightarrow \mathcal{B}_{\mathsf{re}}}_{x,d} = \emptyset$ (resp. $\mathcal{S}^{\mathcal{B}^c_{\mathsf{id}} \hookrightarrow \mathcal{B}_{\mathsf{id}}}_{x,d} = \emptyset$). Thus,

$$[\![\mathcal{B}^c_{\mathsf{re}[\leq i-1]} \hookrightarrow \mathcal{B}_{\mathsf{re}[\leq i]}]\!] = 0, \qquad \forall\, i \in \{3k : 1 \leq k \leq q\}, \tag{39}$$

and also,

$$[\![\mathcal{B}^{\mathsf{c}}_{\mathsf{id}[\leq i-1]} \hookrightarrow \mathcal{B}_{\mathsf{id}[\leq i]}]\!] = 0, \qquad \forall\, i \in \{3k : 1 \leq k \leq q\}. \tag{40}$$

From (35)-(40), we get

$$\left(\perp \overset{3q}{\rightsquigarrow} \mathcal{B}_{\mathsf{re}}\right) \leq 2\sqrt{\frac{10q^4}{2^n}}, \qquad \left(\perp \overset{3q}{\rightsquigarrow} \mathcal{B}_{\mathsf{id}}\right) \leq 2\sqrt{\frac{10q^4}{2^n}}. \tag{41}$$

Adding the two inequalities completes the proof of Theorem 2.

5.2 Security of LRQ

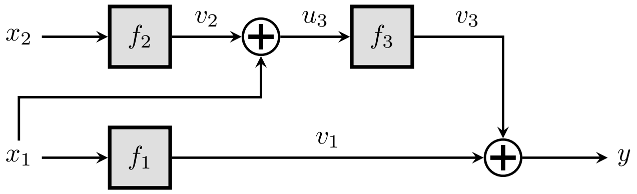

Fig. 3: The LRQ construction.

In this section, we analyze the post-quantum security of LRQ (see Fig. 3), defined as

$$g^{\mathsf{LRQ}}_{\mathsf{re}}(x_1, x_2) := f_1(x_1) \oplus f_3(x_1 \oplus f_2(x_2)).$$

Note that, we have swapped the labels, x_1 with x_2, and f_1 with f_2. This is just an administrative step to aid our proof. The construction remains exactly the same as before up to relabeling.

Theorem 3. *Let $\mathscr{A}$ be a (q, τ)-quantum adversary distinguishing $g^{\mathsf{LRQ}}_{\mathsf{re}}$ from g_{id}. Then there exists $(O(q), \tau_i)$-quantum distinguishers $\mathscr{B}_i$ against f_i, such that*

$$\mathbf{Adv}^{\mathsf{qprf}}_{\mathsf{LRQ}}(\mathscr{A}) \leq \sum_{i=1}^{3} \mathbf{Adv}^{\mathsf{qprp}}_{f_i}(\mathscr{B}_i) + 2\sqrt{\frac{10q^4}{2^n}},$$

where $\tau_i \in \widetilde{O}(\tau + q^2)$, for all $i \in \{1, 2, 3\}$.

Since the proof follows the same approach of the proof of Theorem 2, we will skip some details of the formulation which are very similar to the earlier proof and can be surmised from the context.

Formulation of the Proof. As before we will simulate all the random functions using a single random function $f : \{0,1\}^{3n+2} \to \{0,1\}^n$. For each $x \in \mathcal{Y}$,

$$f_1(x) = f(00\|x\|0^{2n}), \qquad f_2(x) = f(01\|x\|0^{2n}),$$

$$f_3(x) = f(10\|x\|0^{2n}), \qquad g^*_{\mathsf{id}}(x_1, x_2) = f(11\|x_1\|x_2\|x_1 \oplus f_2(x_2)).$$

Here we replace g_{id} with the map $(x_1, x_2) \mapsto g^*_{\mathsf{id}}(x_1, x_2) \oplus f_1(x_1)$. Since g^*_{id} is a random function of (x_1, x_2) and is independent from f_1, $g^*_{\mathsf{id}}(x_1, x_2) \oplus f_1(x_1)$ is identically distributed with $g_{\mathsf{id}}(x_1, x_2)$.

Let $\mathcal{D}_{\mathsf{re}}, \mathcal{D}_{\mathsf{id}}, \widetilde{\mathcal{X}}_{\mathsf{re}}, \widetilde{\mathcal{X}}_{\mathsf{id}}$ be as before. Let $\mathcal{B}_{\mathsf{re}}$ be the set of databases d_{re} satisfying the following condition: we can find $x_1, v_1, x'_1, v'_1, x_2, v_2, x'_2, v'_2, v_3 \in \mathcal{Y}$ such that

– $([x_1]_1, v_1), ([x'_1]_1, v'_1), ([x_2]_2, v_2), ([x'_2]_2, v'_2) \in d_{\mathsf{re}}$;
– $v_2 \oplus x_1 = v'_2 \oplus x'_1$;
– $([v_2 \oplus x_1]_3, v_3) \in d_{\mathsf{re}}$.

Next, let $\mathcal{B}_{\mathsf{id}}$ be the set of databases d_{id} satisfying the following condition: we can find $x_1, v_1, x'_1, v'_1, x_2, v_2, x'_2, v'_2, v_3 \in \mathcal{Y}$ such that

– $([x_1]_1, v_1), ([x'_1]_1, v'_1), ([x_2]_2, v_2), ([x'_2]_2, v'_2) \in d_{\mathsf{id}}$;
– $v_2 \oplus x_1 = v'_2 \oplus x'_1$;
– One of $(11\|x_1\|x_2\|(v_2 \oplus x_1), v_3)$ and $(11\|x'_1\|x'_2\|(v_2 \oplus x_1), v_3) \in d_{\mathsf{id}}$.

As before et $\mathcal{G}_{\mathsf{re}} := \mathcal{D}_{\mathsf{re}} \setminus \mathcal{B}_{\mathsf{re}}$ and $\mathcal{G}_{\mathsf{id}} := \mathcal{D}_{\mathsf{id}} \setminus \mathcal{B}_{\mathsf{id}}$. Thus the above definitions mean that in both $\mathcal{G}_{\mathsf{re}}$ and $\mathcal{G}_{\mathsf{id}}$, each $u_3 := v_2 \oplus x_1$ is associated with a unique pair (x_1, x_2). Then we can define the bijection $h : \mathcal{G}_{\mathsf{re}} \longrightarrow \mathcal{G}_{\mathsf{id}}$ as follows: for each d_{re} we define $d_{\mathsf{id}} := h(d_{\mathsf{re}})$ such that

– for each $x_1 \in \mathcal{Y}$, $d_{\mathsf{id}}([x_1]_1) = d_{\mathsf{re}}([x_1]_1)$;
– for each $x_2 \in \mathcal{Y}$, $d_{\mathsf{id}}([x_2]_2) = d_{\mathsf{re}}([x_2]_2)$;
– for each $x_1, x_2 \in \mathcal{Y}$ and the associated u_3, $d_{\mathsf{id}}(11\|x_1\|x_2\|u_3) = d_{\mathsf{re}}([u_3]_3)$.

Then h satisfies the conditions of Lemma 2. To complete the proof of Theorem 3, we just need to show that

$$\left(\perp \overset{3q}{\rightsquigarrow} \mathcal{B}_{\mathsf{re}}\right) + \left(\perp \overset{3q}{\rightsquigarrow} \mathcal{B}_{\mathsf{id}}\right) \leq 2\sqrt{\frac{10q^4}{2^n}}.$$

Sequence of Actions. As before, we deal with three main actions, one each corresponding to f_1, f_2, and f_3 or g^*_{id}.

Action of f_1: For $i \in \{3k+1 : 0 \leq k \leq q-1\}$, for any d_{re} with $|d_{\mathsf{re}}| \leq i-1$ and any $x \in \mathcal{Y}$, since the property $\mathcal{B}_{\mathsf{re}}$ does not depend on $d_{\mathsf{re}}([x]_1)$, we have $\mathcal{S}^{\mathcal{B}^c_{\mathsf{re}} \hookrightarrow \mathcal{B}_{\mathsf{re}}}_{x,d} = \emptyset$. Thus,

$$[\![\mathcal{B}^c_{\mathsf{re}[\leq i-1]} \hookrightarrow \mathcal{B}_{\mathsf{re}[\leq i]}]\!] = 0, \qquad \forall\, i \in \{3k+1 : 0 \leq k \leq q-1\}. \tag{42}$$

By the same arguments

$$[\![\mathcal{B}^c_{\mathsf{id}[\leq i-1]} \hookrightarrow \mathcal{B}_{\mathsf{id}[\leq i]}]\!] = 0, \qquad \forall\, i \in \{3k+1 : 0 \leq k \leq q-1\}. \tag{43}$$

Action of f_2: Next we look at the transition capacity $[\![\mathcal{B}^c_{\mathsf{re}[\leq i-1]} \hookrightarrow \mathcal{B}_{\mathsf{re}[\leq i]}]\!]$ for $i \in \{3k+2 : 0 \leq k \leq q-1\}$. For any d_{re} with $|d_{\mathsf{re}}| \leq i-1$ and any $x \in \mathcal{Y}$, we have

$$\mathcal{S}_{x,d}^{\mathcal{B}_{\mathsf{re}}^c \hookrightarrow \mathcal{B}_{\mathsf{re}}} := \{x_1 \oplus u_3 \mid d_{\mathsf{re}}([x_1]_1) \neq \bot, d_{\mathsf{re}}([u_3]_3) \neq \bot\}.$$

There are at most $\lceil (i-1)/3 \rceil^2$ choices for the pair (x_1, u_3), so from Lemma 1 we have

$$[\![\mathcal{B}^c_{\mathsf{re}[\leq i-1]} \hookrightarrow \mathcal{B}_{\mathsf{re}[\leq i]}]\!] \leq \sqrt{\frac{10q^2}{2^n}}, \qquad \forall\ i \in \{3k+2 : 0 \leq k \leq q-1\}. \tag{44}$$

By the same arguments

$$[\![\mathcal{B}^c_{\mathsf{id}[\leq i-1]} \hookrightarrow \mathcal{B}_{\mathsf{id}[\leq i]}]\!] \leq \sqrt{\frac{10q^2}{2^n}}, \qquad \forall\ i \in \{3k+2 : 0 \leq k \leq q-1\}. \tag{45}$$

Action of f_3 (resp. g^*_{ID}): Finally, for $i \in \{3k : 1 \leq k \leq q\}$, for any d_{re} with $|d_{\mathsf{re}}| \leq i-1$ (resp. any d_{id} with $|d_{\mathsf{id}}| \leq i-1$) and any $x \in \mathcal{Y}$, since the property $\mathcal{B}_{\mathsf{re}}$ (resp. $\mathcal{B}_{\mathsf{id}}$) does not depend on $d_{\mathsf{re}}([x]_3)$ (resp. $d_{\mathsf{id}}(11\|x_1\|x_2\|x)$), we have $\mathcal{S}_{x,d}^{\mathcal{B}_{\mathsf{re}}^c \hookrightarrow \mathcal{B}_{\mathsf{re}}} = \emptyset$ (resp. $\mathcal{S}_{x,d}^{\mathcal{B}_{\mathsf{id}}^c \hookrightarrow \mathcal{B}_{\mathsf{id}}} = \emptyset$). Thus,

$$[\![\mathcal{B}^c_{\mathsf{re}[\leq i-1]} \hookrightarrow \mathcal{B}_{\mathsf{re}[\leq i]}]\!] = 0, \qquad \forall\ i \in \{3k : 1 \leq k \leq q\}, \tag{46}$$

and also,

$$[\![\mathcal{B}^c_{\mathsf{id}[\leq i-1]} \hookrightarrow \mathcal{B}_{\mathsf{id}[\leq i]}]\!] = 0, \qquad \forall\ i \in \{3k : 1 \leq k \leq q\}. \tag{47}$$

From (42)-(47), we get

$$\left(\bot \overset{3q}{\rightsquigarrow} \mathcal{B}_{\mathsf{re}}\right) \leq \sqrt{\frac{10q^4}{2^n}}, \qquad \left(\bot \overset{3q}{\rightsquigarrow} \mathcal{B}_{\mathsf{id}}\right) \leq \sqrt{\frac{10q^4}{2^n}}. \tag{48}$$

Adding the two inequalities completes the proof of Theorem 3.

5.3 Security of LRWQ

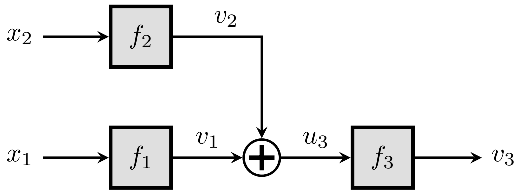

Fig. 4: The LRWQ construction by Hosoyamada et al. [17].

In this section, we analyze the post-quantum security of LRWQ (see Fig. 4), defined as

$$g_{\mathsf{re}}^{\mathsf{LRWQ}}(x_1, x_2) := f_3(f_1(x_1) \oplus f_2(x_2)).$$

Theorem 4. *Let $\mathscr{A}$ be a (q,τ)-quantum adversary distinguishing $g_{\mathsf{re}}^{\mathsf{LRWQ}}$ from g_{id}. Then there exists $(O(q),\tau_i)$-quantum distinguishers $\mathscr{B}_i$ against f_i, such that*

$$\mathbf{Adv}_{\mathsf{LRWQ}}^{\mathsf{qprf}}(\mathscr{A}) \leq \sum_{i=1}^{3} \mathbf{Adv}_{f_i}^{\mathsf{qprp}}(\mathscr{B}_i) + 4\sqrt{\frac{10q^4}{2^n}},$$

where $\tau_i \in \widetilde{O}(\tau + q^2)$, for all $i \in \{1,2,3\}$.

Formulation of the Proof. As before we will simulate all the random functions using a single random function $f : \{0,1\}^{3n+2} \to \{0,1\}^n$. For each $x \in \mathcal{Y}$,

$$f_1(x) = f(00\|x\|0^{2n}), \qquad f_2(x) = f(01\|x\|0^{2n}),$$
$$f_3(x) = f(10\|x\|0^{2n}), \qquad g_{\mathsf{id}}^*(x_1,x_2) = f(11\|x_1\|x_2\|f_1(x_1) \oplus f_2(x_2)).$$

Using a similar argument as before we can conclude that this game behaves identical with the standard PRF game.

Let $\mathcal{D}_{\mathsf{re}}, \mathcal{D}_{\mathsf{id}}, \widetilde{\mathcal{X}}_{\mathsf{re}}, \widetilde{\mathcal{X}}_{\mathsf{id}}$ be as before. Let $\mathcal{B}_{\mathsf{re}}$ be the set of databases d_{re} satisfying the following condition: we can find $x_1, v_1, x_1', v_1', x_2, v_2, x_2', v_2', v_3 \in \mathcal{Y}$ such that

- $([x_1]_1, v_1), ([x_1']_1, v_1'), ([x_2]_2, v_2), ([x_2']_2, v_2') \in d_{\mathsf{re}}$;
- $v_1 \oplus v_2 = v_1' \oplus v_2'$;
- $([v_1 \oplus v_2]_3, v_3) \in d_{\mathsf{re}}$.

Next, let $\mathcal{B}_{\mathsf{id}}$ be the set of databases d_{id} satisfying the following condition: we can find $x_1, v_1, x_1', v_1', x_2, v_2, x_2', v_2', y \in \mathcal{Y}$ such that

- $([x_1]_1, v_1), ([x_1']_1, v_1'), ([x_2]_2, v_2), ([x_2']_2, v_2') \in d_{\mathsf{re}}$;
- $v_1 \oplus v_2 = v_1' \oplus v_2'$;
- One of $(11\|x_1\|x_2\|(v_1 \oplus v_2), v_3)$ and $(11\|x_1'\|x_2'\|(v_1 \oplus v_2), v_3) \in d_{\mathsf{id}}$.

As before et $\mathcal{G}_{\mathsf{re}} := \mathcal{D}_{\mathsf{re}} \setminus \mathcal{B}_{\mathsf{re}}$ and $\mathcal{G}_{\mathsf{id}} := \mathcal{D}_{\mathsf{id}} \setminus \mathcal{B}_{\mathsf{id}}$. Thus the above definitions mean that in both $\mathcal{G}_{\mathsf{re}}$ and $\mathcal{G}_{\mathsf{id}}$, each $u_3 := v_1 \oplus v_2$ is associated with a unique pair (x_1, x_2). Then we can define the bijection $h : \mathcal{G}_{\mathsf{re}} \longrightarrow \mathcal{G}_{\mathsf{id}}$ as follows: for each d_{re} we define $d_{\mathsf{id}} := h(d_{\mathsf{re}})$ such that

- for each $x_1 \in \mathcal{Y}$, $d_{\mathsf{id}}([x_1]_1) = d_{\mathsf{re}}([x_1]_1)$;
- for each $x_2 \in \mathcal{Y}$, $d_{\mathsf{id}}([x_2]_2) = d_{\mathsf{re}}([x_2]_2)$;
- for each $x_1, x_2 \in \mathcal{Y}$ and the associated u_3, $d_{\mathsf{id}}(11\|x_1\|x_2\|u_3) = d_{\mathsf{re}}([u_3]_3)$.

Then h satisfies the conditions of Lemma 2. To complete the proof of Theorem 4, we just need to show that

$$\left(\perp \overset{3q}{\rightsquigarrow} \mathcal{B}_{\mathsf{re}}\right) + \left(\perp \overset{3q}{\rightsquigarrow} \mathcal{B}_{\mathsf{id}}\right) \leq 4\sqrt{\frac{10q^4}{2^n}}.$$

Sequence of Actions. As before, we deal with three main actions, one each corresponding to f_1, f_2, and f_3 or g^*_{id}.

Action of f_1: For $i \in \{3k+1 : 0 \le k \le q-1\}$, we first look at the transition capacity $[\![\mathcal{B}^c_{\mathsf{re}[\le i-1]} \hookrightarrow \mathcal{B}_{\mathsf{re}[\le i]}]\!]$. For any d_{re} with $|d_{\mathsf{re}}| \le i-1$ and any $x \in \mathcal{Y}$, we have

$$\mathcal{S}_{x,d}^{\mathcal{B}^c_{\mathsf{re}} \hookrightarrow \mathcal{B}_{\mathsf{re}}} = \{d_{\mathsf{re}}([x_2]_2) \oplus u_3 \mid d_{\mathsf{re}}([x_2]_2) \neq \perp, d_{\mathsf{re}}([u_3]_3) \neq \perp\}\,.$$

There are at most $\lceil (i-1)/3 \rceil^2$ choices for the pair (x_2, u_3), so $|\mathcal{S}_{x,d}^{\mathcal{B}^c_{\mathsf{re}} \hookrightarrow \mathcal{B}_{\mathsf{re}}}| \le \lceil (i-1)/3 \rceil^2 \le q^2$, and from there using Lemma 1 we have

$$[\![\mathcal{B}^c_{\mathsf{re}[\le i-1]} \hookrightarrow \mathcal{B}_{\mathsf{re}[\le i]}]\!] \le \sqrt{\frac{10q^2}{2^n}}, \qquad \forall\, i \in \{3k+1 : 0 \le k \le q-1\}. \tag{49}$$

By the same arguments

$$[\![\mathcal{B}^c_{\mathsf{id}[\le i-1]} \hookrightarrow \mathcal{B}_{\mathsf{id}[\le i]}]\!] \le \sqrt{\frac{10q^2}{2^n}}, \qquad \forall\, i \in \{3k+1 : 0 \le k \le q-1\}. \tag{50}$$

Action of f_2: Next we look at the transition capacity $[\![\mathcal{B}^c_{\mathsf{re}[\le i-1]} \hookrightarrow \mathcal{B}_{\mathsf{re}[\le i]}]\!]$ for $i \in \{3k+2 : 0 \le k \le q-1\}$. For any d_{re} with $|d_{\mathsf{re}}| \le i-1$ and any $x \in \mathcal{Y}$, we have

$$\mathcal{S}_{x,d}^{\mathcal{B}^c_{\mathsf{re}} \hookrightarrow \mathcal{B}_{\mathsf{re}}} := \{d_{\mathsf{re}}([x_1]_1) \oplus u_3 \mid d_{\mathsf{re}}([x_1]_1) \neq \perp, d_{\mathsf{re}}([u_3]_3) \neq \perp\}.$$

Again, there are at most $\lceil (i-1)/3 \rceil^2$ choices for the pair (x_1, u_3), and arguing as before we have

$$[\![\mathcal{B}^c_{\mathsf{re}[\le i-1]} \hookrightarrow \mathcal{B}_{\mathsf{re}[\le i]}]\!] \le \sqrt{\frac{10q^2}{2^n}}, \qquad \forall\, i \in \{3k+2 : 0 \le k \le q-1\}. \tag{51}$$

By the same arguments

$$[\![\mathcal{B}^c_{\mathsf{id}[\le i-1]} \hookrightarrow \mathcal{B}_{\mathsf{id}[\le i]}]\!] \le \sqrt{\frac{10q^2}{2^n}}, \qquad \forall\, i \in \{3k+2 : 0 \le k \le q-1\}. \tag{52}$$

Action of f_3 (resp. g^*_{ID}): Finally, for $i \in \{3k : 1 \le k \le q\}$, for any d_{re} with $|d_{\mathsf{re}}| \le i-1$ (resp. any d_{id} with $|d_{\mathsf{id}}| \le i-1$) and any $x \in \mathcal{Y}$, since the property $\mathcal{B}_{\mathsf{re}}$ (resp. $\mathcal{B}_{\mathsf{id}}$) does not depend on $d_{\mathsf{re}}([x]_3)$ (resp. $d_{\mathsf{id}}(11\|x_1\|x_2\|x)$), we have $\mathcal{S}_{x,d}^{\mathcal{B}^c_{\mathsf{re}} \hookrightarrow \mathcal{B}_{\mathsf{re}}} = \emptyset$ (resp. $\mathcal{S}_{x,d}^{\mathcal{B}^c_{\mathsf{id}} \hookrightarrow \mathcal{B}_{\mathsf{id}}} = \emptyset$). Thus,

$$[\![\mathcal{B}^c_{\mathsf{re}[\le i-1]} \hookrightarrow \mathcal{B}_{\mathsf{re}[\le i]}]\!] = 0, \qquad \forall\, i \in \{3k : 1 \le k \le q\}, \tag{53}$$

and also,

$$[\![\mathcal{B}^c_{\mathsf{id}[\le i-1]} \hookrightarrow \mathcal{B}_{\mathsf{id}[\le i]}]\!] = 0, \qquad \forall\, i \in \{3k : 1 \le k \le q\}. \tag{54}$$

From (49)-(54), we get

$$\left(\perp \overset{3q}{\rightsquigarrow} \mathcal{B}_{\mathsf{re}}\right) \le 2\sqrt{\frac{10q^4}{2^n}}, \qquad \left(\perp \overset{3q}{\rightsquigarrow} \mathcal{B}_{\mathsf{id}}\right) \le 2\sqrt{\frac{10q^4}{2^n}}. \tag{55}$$

Adding the two inequalities completes the proof of Theorem 4.

6 Conclusion

In this work, we show that 2n-bit-to-n-bit compressing PRFs that are built using two n-bit-to-n-bit PRF calls are insecure in the quantum setting. Furthermore, we identify classes of constructions using three PRF calls that are also broken. Among the constructions that may be secure, we select TNT, LRQ, and LRWQ, as they are the most efficient invertible ones, which allows them to also be used as tweakable block ciphers. We then prove their PRF security against quantum distinguishers that use less than $2^{n/4}$ queries.

We leave the issue of improving the security bound of these constructions to $2^{n/3}$ adversarial queries as an interesting open problem.

Acknowledgments

The authors would like to thank all the anonymous reviewers who reviewed and provided valuable comments on this paper. This work was carried out under the framework of the French-German-Center for Cybersecurity, a collaboration of CISPA and LORIA. Part of this work was written while Benoît Cogliati and Ritam Bhaumik were respectively employed by the CISPA Helmholtz Center for Information Security and Inria Paris, where the latter received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement no. 714294 - acronym QUASYModo).

References

1. Zhenzhen Bao, Chun Guo, Jian Guo, and Ling Song. TNT: How to tweak a block cipher. In Anne Canteaut and Yuval Ishai, editors, *EUROCRYPT 2020, Part II*, volume 12106 of *LNCS*, pages 641–673. Springer, Heidelberg, May 2020.
2. Zhenzhen Bao, Chun Guo, Jian Guo, and Ling Song. TNT: how to tweak a block cipher. In Anne Canteaut and Yuval Ishai, editors, *Advances in Cryptology - EUROCRYPT 2020, Proceedings, Part II*, volume 12106 of *Lecture Notes in Computer Science*, pages 641–673. Springer, 2020.
3. Mihir Bellare, Joe Kilian, and Phillip Rogaway. The security of the cipher block chaining message authentication code. *Journal of Computer and System Sciences*, 61(3):362–399, 2000.
4. Ritam Bhaumik, Xavier Bonnetain, André Chailloux, Gaëtan Leurent, María Naya-Plasencia, André Schrottenloher, and Yannick Seurin. Qcb: Efficient quantum-secure authenticated encryption. In Mehdi Tibouchi and Huaxiong Wang, editors, *Advances in Cryptology – ASIACRYPT 2021*, pages 668–698, Cham, 2021. Springer International Publishing.
5. Dan Boneh and Mark Zhandry. Quantum-secure message authentication codes. In Thomas Johansson and Phong Q. Nguyen, editors, *EUROCRYPT 2013*, volume 7881 of *LNCS*, pages 592–608. Springer, Heidelberg, May 2013.
6. Xavier Bonnetain and María Naya-Plasencia. Hidden shift quantum cryptanalysis and implications. In Thomas Peyrin and Steven Galbraith, editors, *ASIACRYPT 2018, Part I*, volume 11272 of *LNCS*, pages 560–592. Springer, Heidelberg, December 2018.

7. Xavier Bonnetain, María Naya-Plasencia, and André Schrottenloher. On quantum slide attacks. In Kenneth G. Paterson and Douglas Stebila, editors, *SAC 2019*, volume 11959 of *LNCS*, pages 492–519. Springer, Heidelberg, August 2019.
8. Xavier Bonnetain, María Naya-Plasencia, and André Schrottenloher. Quantum security analysis of AES. *IACR Trans. Symm. Cryptol.*, 2019(2):55–93, 2019.
9. Xavier Bonnetain, André Schrottenloher, and Ferdinand Sibleyras. Beyond quadratic speedups in quantum attacks on symmetric schemes. In Orr Dunkelman and Stefan Dziembowski, editors, *EUROCRYPT 2022, Part III*, volume 13277 of *LNCS*, pages 315–344. Springer, Heidelberg, May / June 2022.
10. André Chailloux, María Naya-Plasencia, and André Schrottenloher. An efficient quantum collision search algorithm and implications on symmetric cryptography. In Tsuyoshi Takagi and Thomas Peyrin, editors, *ASIACRYPT 2017, Part II*, volume 10625 of *LNCS*, pages 211–240. Springer, Heidelberg, December 2017.
11. Kai-Min Chung, Serge Fehr, Yu-Hsuan Huang, and Tai-Ning Liao. On the compressed-oracle technique, and post-quantum security of proofs of sequential work. In Anne Canteaut and François-Xavier Standaert, editors, *EUROCRYPT 2021, Part II*, volume 12697 of *LNCS*, pages 598–629. Springer, Heidelberg, October 2021.
12. Jan Czajkowski, Andreas Hülsing, and Christian Schaffner. Quantum indistinguishability of random sponges. In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Part II*, volume 11693 of *LNCS*, pages 296–325. Springer, Heidelberg, August 2019.
13. Lorenzo Grassi, María Naya-Plasencia, and André Schrottenloher. Quantum algorithms for the k-xor problem. In Thomas Peyrin and Steven Galbraith, editors, *ASIACRYPT 2018, Part I*, volume 11272 of *LNCS*, pages 527–559. Springer, Heidelberg, December 2018.
14. Akinori Hosoyamada and Tetsu Iwata. 4-round Luby-Rackoff construction is a qPRP. In Steven D. Galbraith and Shiho Moriai, editors, *ASIACRYPT 2019, Part I*, volume 11921 of *LNCS*, pages 145–174. Springer, Heidelberg, December 2019.
15. Akinori Hosoyamada and Tetsu Iwata. 4-round luby-rackoff construction is a qprp: Tight quantum security bound. Cryptology ePrint Archive, Report 2019/243, 2019. `https://eprint.iacr.org/2019/243`.
16. Akinori Hosoyamada and Tetsu Iwata. On tight quantum security of HMAC and NMAC in the quantum random oracle model. In Tal Malkin and Chris Peikert, editors, *CRYPTO 2021, Part I*, volume 12825 of *LNCS*, pages 585–615, Virtual Event, August 2021. Springer, Heidelberg.
17. Akinori Hosoyamada and Tetsu Iwata. Provably quantum-secure tweakable block ciphers. *IACR Trans. Symm. Cryptol.*, 2021(1):337–377, 2021.
18. Akinori Hosoyamada, Yu Sasaki, and Keita Xagawa. Quantum multicollision-finding algorithm. In Tsuyoshi Takagi and Thomas Peyrin, editors, *ASIACRYPT 2017, Part II*, volume 10625 of *LNCS*, pages 179–210. Springer, Heidelberg, December 2017.
19. Akinori Hosoyamada and Kan Yasuda. Building quantum-one-way functions from block ciphers: Davies-Meyer and Merkle-Damgård constructions. In Thomas Peyrin and Steven Galbraith, editors, *ASIACRYPT 2018, Part I*, volume 11272 of *LNCS*, pages 275–304. Springer, Heidelberg, December 2018.
20. Marc Kaplan, Gaëtan Leurent, Anthony Leverrier, and María Naya-Plasencia. Breaking symmetric cryptosystems using quantum period finding. In Matthew Robshaw and Jonathan Katz, editors, *CRYPTO 2016, Part II*, volume 9815 of *LNCS*, pages 207–237. Springer, Heidelberg, August 2016.

21. Marc Kaplan, Gaëtan Leurent, Anthony Leverrier, and María Naya-Plasencia. Quantum differential and linear cryptanalysis. *IACR Trans. Symm. Cryptol.*, 2016(1):71–94, 2016. `https://tosc.iacr.org/index.php/ToSC/article/view/536`.
22. 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.
23. Hidenori Kuwakado and Masakatu Morii. Security on the quantum-type even-mansour cipher. In *2012 International Symposium on Information Theory and its Applications*, pages 312–316, 2012.
24. Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information (10th Anniversary edition)*. Cambridge University Press, 2016.
25. Phillip Rogaway and Thomas Shrimpton. A provable-security treatment of the key-wrap problem. In Serge Vaudenay, editor, *EUROCRYPT 2006*, volume 4004 of *LNCS*, pages 373–390. Springer, Heidelberg, May / June 2006.
26. Fang Song and Aaram Yun. Quantum security of NMAC and related constructions - PRF domain extension against quantum attacks. In Jonathan Katz and Hovav Shacham, editors, *CRYPTO 2017, Part II*, volume 10402 of *LNCS*, pages 283–309. Springer, Heidelberg, August 2017.
27. Mark Zhandry. A note on the quantum collision and set equality problems. *Quantum Inf. Comput.*, 15(7&8):557–567, 2015.
28. Mark Zhandry. How to record quantum queries, and applications to quantum indifferentiability. In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Part II*, volume 11693 of *LNCS*, pages 239–268. Springer, Heidelberg, August 2019.

A Linear Algebra Results

Operator Norm. For any finite set $\mathcal{X}$, $\mathbb{C}[\mathcal{X}]$ will denote the span of the orthonormal basis $B := \{|x\rangle \mid x \in \mathcal{X}\}$, which is a Hilbert space of dimension $|\mathcal{X}|$. (We will interchangeably write $\mathbb{C}[B]$ to denote the same Hilbert space.) For a linear operator $A : \mathbb{C}[\mathcal{X}_0] \longrightarrow \mathbb{C}[\mathcal{X}_1]$, we define the *operator norm* of A as

$$\|A\| = \sup_{|\psi\rangle \in \mathbb{C}[\mathcal{X}_1], \| |\psi\rangle \| = 1} \|A\,|\psi\rangle\|,$$

where the norm on the right hand side is the norm over the Hilbert space $\mathbb{C}[\mathcal{X}_1]$. If

$$A = \sum_{i=1}^{r} \sigma_i \,|x_i\rangle\langle y_i|$$

is the singular value decomposition of A (where r is the rank of A and $x_1, \ldots, x_r \in \mathcal{X}_1, y_1, \ldots, y_r \in \mathcal{X}_0$), then we have

$$\|A\| = \max_i \sigma_i.$$

For four finite sets $\mathcal{X}_0$, $\mathcal{X}_1$, $\mathcal{X}_0'$, and $\mathcal{X}_1'$, let $A : \mathbb{C}[\mathcal{X}_0] \longrightarrow \mathbb{C}[\mathcal{X}_1]$ and $A' : \mathbb{C}[\mathcal{X}_0'] \longrightarrow \mathbb{C}[\mathcal{X}_1']$ be linear operators with singular value decompositions

$$A = \sum_{i=1}^{r} \sigma_i \,|x_i\rangle\langle y_i| \text{ and } A' = \sum_{i'=1}^{r'} \sigma'_{i'} \,|x'_{i'}\rangle\langle y'_{i'}|\,.$$

Then we have

$$\begin{aligned} A \otimes A' &= \left(\sum_{i=1}^{r} \sigma_i \,|x_i\rangle\langle y_i| \right) \otimes \left(\sum_{i'=1}^{r'} \sigma'_{i'} \,|x'_{i'}\rangle\langle y'_{i'}| \right) \\ &= \sum_{i,i'} \sigma_i \sigma'_{i'} \left(|x_i\rangle\langle y_i| \otimes |x'_{i'}\rangle\langle y'_{i'}| \right) \\ &= \sum_{i,i'} \sigma_i \sigma'_{i'} \left(|x_i\rangle \otimes |x'_{i'}\rangle \right) \left(\langle y_i| \otimes \langle y'_{i'}| \right). \end{aligned}$$

Since $|x_1\rangle, \ldots, |x_r\rangle$ are independent and orthonormal and $|x'_1\rangle, \ldots, |x'_{r'}\rangle$ are independent and orthonormal, $\{|x_i\rangle \otimes |x'_{i'}\rangle \mid 1 \leq i \leq r, 1 \leq i' \leq r'\}$ also forms a set of independent and orthonormal vectors in the tensor product space $\mathbb{C}[\mathcal{X}_1] \otimes \mathbb{C}[\mathcal{X}_1']$, and similarly, $\{|y_i\rangle \otimes |y'_{i'}\rangle \mid 1 \leq i \leq r, 1 \leq i' \leq r'\}$ also forms a set of independent and orthonormal vectors in the tensor product space $\mathbb{C}[\mathcal{X}_0] \otimes \mathbb{C}[\mathcal{X}_0']$. Thus,

$$A \otimes A' = \sum_{i,i'} \sigma_i \sigma'_{i'} \left(|x_i\rangle \otimes |x'_{i'}\rangle \right) \left(\langle y_i| \otimes \langle y'_{i'}| \right)$$

is a singular value decomposition of $A \otimes A'$, and consequently

$$\|A \otimes A'\| = \max_{i,i'} \sigma_i \sigma'_{i'} = \left(\max_i \sigma_i \right) \cdot \left(\max_{i'} \sigma'_{i'} \right) = \|A\| \cdot \|A'\|.$$

Frobenius Norm. The *Frobenius Norm* of the operator A is defined as

$$\|A\|_F := \sqrt{\sum_{x\in\mathcal{X}_1} \|A\,|x\rangle\|^2} = \sqrt{\sum_{x\in\mathcal{X}_1, y\in\mathcal{X}_0} \left|\,\langle y|A|x\rangle\,\right|^2}.$$

We can relate the two norms as follows: for any $|\psi\rangle \in \mathbb{C}[\mathcal{X}_1]$, we have

$$\begin{aligned}
\|A\,|\psi\rangle\| &= \left\|A \sum_{x\in\mathcal{X}_1} |x\rangle\langle x|\;|\psi\rangle\right\| \\
&\leq \sum_{x\in\mathcal{X}_1} \|\langle x|\psi\rangle\, A\,|x\rangle\| && \text{(Triangle Inequality)} \\
&= \sum_{x\in\mathcal{X}_1} |\,\langle x|\psi\rangle\,| \cdot \|A\,|x\rangle\| \\
&\leq \sqrt{\sum_{x\in\mathcal{X}_1} |\,\langle x|\psi\rangle\,|^2} \cdot \sqrt{\sum_{x\in\mathcal{X}_1} \|A\,|x\rangle\|^2} && \text{(Cauchy-Schwarz)} \\
&= \|\psi\| \cdot \|A\|_F.
\end{aligned}$$

This gives the inequality

$$\|A\| = \sup_{\||\psi\rangle\|=1} \|A\,|\psi\rangle\| \leq \|A\|_F.$$

Control Registers. Consider a linear operator $A : \mathbb{C}[\mathcal{X}] \otimes \mathbb{C}[\mathcal{X}_0'] \longrightarrow \mathbb{C}[\mathcal{X}] \otimes \mathbb{C}[\mathcal{X}_1']$, and a set of linear operators $\{A_x : \mathbb{C}[\mathcal{X}_0'] \longrightarrow \mathbb{C}[\mathcal{X}_1'] \mid x \in \mathcal{X}\}$, such that for every $x \in \mathcal{X}$ and every $|\psi\rangle \in \mathbb{C}[\mathcal{X}_0']$, we have

$$A(|x\rangle \otimes |\psi\rangle) = |x\rangle \otimes A_x\,|\psi\rangle\,.$$

Then the register containing the part of the input corresponding to $\mathbb{C}[\mathcal{X}]$ is called the *control register* of A. For any $|\phi\rangle \in \mathbb{C}[\mathcal{X}]$ and any $|\psi\rangle \in \mathbb{C}[\mathcal{X}_0']$, we have

$$\begin{aligned}
\|A(|\phi\rangle \otimes |\psi\rangle)\| &= \left\|\sum_{x\in\mathcal{X}} \langle x|\phi\rangle\, A(|x\rangle \otimes |\psi\rangle)\right\| \\
&= \left\|\sum_{x\in\mathcal{X}} \langle x|\phi\rangle\,|x\rangle \otimes A_x\,|\psi\rangle\right\| \\
&= \left\|\sum_{x\in\mathcal{X}, y\in\mathcal{X}_0'} \langle x|\phi\rangle\,\langle y|\psi\rangle\,|x\rangle \otimes A_x\,|y\rangle\right\| \\
&= \left\|\sum_{x\in\mathcal{X}, y\in\mathcal{X}_0', z\in\mathcal{X}_1'} \langle x|\phi\rangle\,\langle y|\psi\rangle\,\langle z|A_x|y\rangle\,|x\rangle \otimes |z\rangle\right\| \\
&= \left\|\sum_{x\in\mathcal{X}, z\in\mathcal{X}_1'} \langle x|\phi\rangle \left(\sum_{y\in\mathcal{X}_0'} \langle y|\psi\rangle\,\langle z|A_x|y\rangle\right) |x\rangle \otimes |z\rangle\right\|
\end{aligned}$$

$$
\begin{aligned}
&= \sqrt{\sum_{x\in\mathcal{X}, z\in\mathcal{X}'_1} |\left\langle x|\phi\right\rangle|^2 \cdot \left|\sum_{y\in\mathcal{X}'_0} \left\langle y|\psi\right\rangle \left\langle z|A_x|y\right\rangle\right|^2} \\
&= \sqrt{\sum_{x\in\mathcal{X}} |\left\langle x|\phi\right\rangle|^2 \cdot \sum_{z\in\mathcal{X}'_1}\left|\sum_{y\in\mathcal{X}'_0} \left\langle y|\psi\right\rangle \left\langle z|A_x|y\right\rangle\right|^2} \\
&= \sqrt{\sum_{x\in\mathcal{X}} |\left\langle x|\phi\right\rangle|^2 \cdot \left\|\sum_{z\in\mathcal{X}'_1}\left(\sum_{y\in\mathcal{X}'_0} \left\langle y|\psi\right\rangle \left\langle z|A_x|y\right\rangle\right)\left|z\right\rangle\right\|^2} \\
&= \sqrt{\sum_{x\in\mathcal{X}} |\left\langle x|\phi\right\rangle|^2 \cdot \left\|\sum_{y\in\mathcal{X}'_0} \left\langle y|\psi\right\rangle \left(\sum_{z\in\mathcal{X}'_1} \left\langle z|A_x|y\right\rangle\left|z\right\rangle\right)\right\|^2} \\
&= \sqrt{\sum_{x\in\mathcal{X}} |\left\langle x|\phi\right\rangle|^2 \cdot \left\|\sum_{y\in\mathcal{X}'_0} \left\langle y|\psi\right\rangle A_x\left|y\right\rangle\right\|^2} \\
&= \sqrt{\sum_{x\in\mathcal{X}} |\left\langle x|\phi\right\rangle|^2 \cdot \|A_x\left|\psi\right\rangle\|^2} \\
&\leq \sqrt{\sum_{x\in\mathcal{X}} |\left\langle x|\phi\right\rangle|^2} \cdot \max_{x\in\mathcal{X}}\|A_x\left|\psi\right\rangle\| = \max_{x\in\mathcal{X}}\|A_x\left|\psi\right\rangle\|.
\end{aligned}
$$

This gives the useful inequality

$$
\|A\| \leq \max_{x\in\mathcal{X}}\|A_x\|. \tag{56}
$$

B Miscellaneous Proofs

Proof of Equation (27)**.** From the definition of $\left|\widehat{f}\,\right\rangle$, we have

$$
\begin{aligned}
\left|\widehat{f}\,\right\rangle &= \bigotimes_{x\in\mathcal{X}} \left|x\right\rangle \left|\widehat{f}(x)\right\rangle \\
&= \bigotimes_{x\in\mathcal{X}} \left|x\right\rangle \left|\widehat{f(x)}\right\rangle \\
&= \bigotimes_{x\in\mathcal{X}} \left(\frac{1}{2^{n/2}}\sum_{y\in\mathcal{Y}}(-1)^{f(x)\cdot y}\left|x\right\rangle\left|y\right\rangle\right) \\
&= \frac{1}{2^{n2^m/2}} \sum_{y_0,\ldots,y_{2^n-1}\in\mathcal{Y}} \left[\bigotimes_{x\in\mathcal{X}}(-1)^{f(x)\cdot y_x}\left|x\right\rangle\left|y_x\right\rangle\right]
\end{aligned}
$$

$$
\begin{aligned}
&= \frac{1}{2^{n2^m/2}} \sum_{g\in\mathcal{F}} \left[\bigotimes_{x\in\mathcal{X}} (-1)^{f(x)\cdot g(x)} \left|x\right\rangle \left|g(x)\right\rangle \right] \\
&= \frac{1}{2^{n2^m/2}} \sum_{g\in\mathcal{F}} (-1)^{f\cdot g} \left|g\right\rangle ,
\end{aligned}
$$

as claimed. □

Proof of Equation (28)**.** Substituting the definitions of $\left|\widehat{y}\right\rangle$ and $\left|\widehat{f}\,\right\rangle$ in the oracle equation of stO gives

$$
\begin{aligned}
&\mathsf{stO}\left|x\right\rangle \left|\widehat{y}\right\rangle \otimes \left|\widehat{f}\,\right\rangle \\
&= \mathsf{stO}\left|x\right\rangle \frac{1}{2^{n/2}} \left(\sum_{z\in\mathcal{Y}} (-1)^{y\cdot z} \left|z\right\rangle \right) \otimes \left[\frac{1}{2^{n2^m/2}} \sum_{g\in\mathcal{F}} (-1)^{f\cdot g} \left|g\right\rangle \right] \\
&= \frac{1}{2^{n(2^m+1)/2}} \sum_{z\in\mathcal{Y}} \sum_{g\in\mathcal{F}} (-1)^{y\cdot z\oplus f\cdot g} \left(\mathsf{stO}\left|x\right\rangle \left|z\right\rangle \otimes \left|g\right\rangle\right) \\
&= \frac{1}{2^{n(2^m+1)/2}} \sum_{z\in\mathcal{Y}} \sum_{g\in\mathcal{F}} (-1)^{y\cdot z\oplus f\cdot g} \left|x\right\rangle \left|z\oplus g(x)\right\rangle \otimes \left|g\right\rangle \\
&= \frac{1}{2^{n(2^m+1)/2}} \sum_{z'\in\mathcal{Y}} \sum_{g\in\mathcal{F}} (-1)^{y\cdot(z'\oplus g(x))\oplus f\cdot g} \left|x\right\rangle \left|z'\right\rangle \otimes \left|g\right\rangle \\
&= \frac{1}{2^{n(2^m+1)/2}} \sum_{z'\in\mathcal{Y}} \sum_{g\in\mathcal{F}} (-1)^{y\cdot z'\oplus(f\oplus\delta_{xy})\cdot g} \left|x\right\rangle \left|z'\right\rangle \otimes \left|g\right\rangle \\
&= \left|x\right\rangle \frac{1}{2^{n/2}} \left(\sum_{z'\in\mathcal{Y}} (-1)^{y\cdot z'} \left|z'\right\rangle \right) \otimes \left[\frac{1}{2^{n2^m/2}} \sum_{g\in\mathcal{F}} (-1)^{(f\oplus\delta_{xy})\cdot g} \left|g\right\rangle \right] \\
&= \left|x\right\rangle \left|\widehat{y}\right\rangle \otimes \left|\widehat{f\oplus\delta_{xy}}\right\rangle = \left|x\right\rangle \left|\widehat{y}\right\rangle \otimes \left|\widehat{f}+\widehat{\delta}_{xy}\right\rangle ,
\end{aligned}
$$

as required. □

Proof of Observation (30)**.** We can prove this by induction on i. For the base case of $i=1$, considering some $d\in\mathcal{G}_{0[\leq 1]}$, we have

$$
\left|\psi^{g}_{1,0}\right\rangle = W^{g}_{1,0}\left|\psi_0\right\rangle = \bar{\mathit{\Pi}}_{\mathcal{G}_{0[\leq 1]}} \circ \ddot{U}_1 \circ \mathsf{cO}_0 \circ \ddot{U}_0 \left|\psi_\perp\right\rangle .
$$

Let $\left|\gamma_{x,\widehat{y}}\right\rangle$ denote the basis state $\left|x\right\rangle\left|\widehat{y}\right\rangle$. Then we have

$$
\begin{aligned}
&\ddot{U}_1 \circ \mathsf{cO}_0 \circ \ddot{U}_0 \left|\psi_\perp\right\rangle \\
&= \sum_{x,\widehat{y}} \ddot{U}_1 \circ \mathsf{cO}_0 \circ \ddot{U}_0 \left|\gamma_{0,\widehat{0}}\right\rangle \otimes \left|d_\perp\right\rangle \\
&= \sum_{x,\widehat{y}} \left\langle\gamma_{x,\widehat{y}}\middle|U_0\middle|\gamma_{0,\widehat{0}}\right\rangle \ddot{U}_1 \circ \mathsf{cO}_0 \left|\gamma_{x,\widehat{y}}\right\rangle \otimes \left|d_\perp\right\rangle
\end{aligned}
$$

$$
\begin{aligned}
&= \sum_{x,\widehat{y}} \left\langle \gamma_{x,\widehat{y}} \middle| U_0 \middle| \gamma_{0,\widehat{0}} \right\rangle \ddot{U}_1 \left(\left| \gamma_{x,\widehat{y}} \right\rangle \otimes \mathsf{cO}_{p_0(x)\widehat{y}} \left| d_\perp \right\rangle \right) \\
&= \sum_{x,\widehat{y},d\in\mathcal{D}_0} \left\langle \gamma_{x,\widehat{y}} \middle| U_0 \middle| \gamma_{0,\widehat{0}} \right\rangle \left\langle d \middle| \mathsf{cO}_{p_0(x)\widehat{y}} \middle| d_\perp \right\rangle \ddot{U}_1 \left| \gamma_{x,\widehat{y}} \right\rangle \otimes \left| d \right\rangle \\
&= \sum_{x,x',\widehat{y},\widehat{y}',d\in\mathcal{D}_0} \left\langle \gamma_{x,\widehat{y}} \middle| U_0 \middle| \gamma_{0,\widehat{0}} \right\rangle \left\langle d \middle| \mathsf{cO}_{p_0(x)\widehat{y}} \middle| d_\perp \right\rangle \left\langle \gamma_{x',\widehat{y}'} \middle| U_1 \middle| \gamma_{x,\widehat{y}} \right\rangle \left| \gamma_{x',\widehat{y}'} \right\rangle \otimes \left| d \right\rangle ,
\end{aligned}
$$

where x, x' vary over $\mathcal{I}$, and $\widehat{y}, \widehat{y}'$ vary over $\widehat{\mathcal{Y}}$ in all the sums. Thus,

$$
\begin{aligned}
&\bar{\Pi}_{\mathcal{G}_{0[\leq 1]}} \circ U_1 \circ \mathsf{cO}_0 \circ \ddot{U}_0 \left| \psi_\perp \right\rangle \\
&= \sum_{x,x',\widehat{y},\widehat{y}',d\in\mathcal{G}_{0[\leq 1]}} \left\langle \gamma_{x,\widehat{y}} \middle| U_0 \middle| \gamma_{0,\widehat{0}} \right\rangle \left\langle d \middle| \mathsf{cO}_{p_0(x)\widehat{y}} \middle| d_\perp \right\rangle \left\langle \gamma_{x',\widehat{y}'} \middle| U_1 \middle| \gamma_{x,\widehat{y}} \right\rangle \left| \varphi_{x',\widehat{y}',d} \right\rangle ,
\end{aligned}
$$

which gives, for any $x' \in \mathcal{I}$, $\widehat{y} \in \widehat{\mathcal{Y}}$, and $d \in \mathcal{G}_{0[\leq 1]}$,

$$
\left\langle \varphi_{x',\widehat{y}',d} \middle| \psi^g_{1,0} \right\rangle = \sum_{x,\widehat{y}} \left\langle \gamma_{x,\widehat{y}} \middle| U_0 \middle| \gamma_{0,\widehat{0}} \right\rangle \left\langle d \middle| \mathsf{cO}_{p_0(x)\widehat{y}} \middle| d_\perp \right\rangle \left\langle \gamma_{x',\widehat{y}'} \middle| U_1 \middle| \gamma_{x,\widehat{y}} \right\rangle .
$$

Similarly, we can show that

$$
\left\langle \varphi_{x',\widehat{y}',h(d)} \middle| \psi^g_{1,1} \right\rangle = \sum_{x,\widehat{y}} \left\langle \gamma_{x,\widehat{y}} \middle| U_0 \middle| \gamma_{0,\widehat{0}} \right\rangle \left\langle h(d) \middle| \mathsf{cO}_{p_1(x)\widehat{y}} \middle| d_\perp \right\rangle \left\langle \gamma_{x',\widehat{y}'} \middle| U_1 \middle| \gamma_{x,\widehat{y}} \right\rangle .
$$

Since $\mathcal{G}_{0[\leq 0]} = \mathcal{G}_{1[\leq 0]} = \{d_\perp\}$, we have $h(d_\perp) = d_\perp$, and the third condition of the lemma gives us $\left\langle \varphi_{x',\widehat{y}',d} \middle| \psi^g_{1,0} \right\rangle = \left\langle \varphi_{x',\widehat{y}',h(d)} \middle| \psi^g_{1,1} \right\rangle$, thus establishing the base case.

Our induction hypothesis will be that for some $i \geq 2$, for all $x, \in \mathcal{I}$, $\widehat{y} \in \widehat{\mathcal{Y}}$, and $d \in \mathcal{G}_{0[\leq i-1]}$,

$$
\left\langle \varphi_{x,\widehat{y},d} \middle| \psi^g_{i-1,0} \right\rangle = \left\langle \varphi_{x,\widehat{y},h(d)} \middle| \psi^g_{i-1,1} \right\rangle =: \alpha_{x,\widehat{y},d}.
$$

Then (since $h|_{\mathcal{G}_{0[\leq i-1]}}$ is bijective) we have

$$
\begin{aligned}
\left| \psi^g_{i-1,0} \right\rangle &= \sum_{x,\widehat{y},d\in\mathcal{G}_{0[\leq i-1]}} \alpha_{x,\widehat{y},d} \left| \varphi_{x,\widehat{y},d} \right\rangle , \\
\left| \psi^g_{i-1,1} \right\rangle &= \sum_{x,\widehat{y},d'\in\mathcal{G}_{1[\leq i-1]}} \left\langle \varphi_{x,\widehat{y},d'} \middle| \psi^g_{i-1,1} \right\rangle \left| \varphi_{x,\widehat{y},d'} \right\rangle , \\
&= \sum_{x,\widehat{y},d\in\mathcal{G}_{0[\leq i-1]}} \alpha_{x,\widehat{y},d} \left| \varphi_{x,\widehat{y},h(d)} \right\rangle .
\end{aligned}
$$

This gives

$$
\begin{aligned}
\left| \psi^g_{i,0} \right\rangle &= W^g_{i,0} \left| \psi^g_{i-1,0} \right\rangle \\
&= \bar{\Pi}_{\mathcal{G}_{0[\leq i]}} \circ \ddot{U}_i \circ \mathsf{cO}_0 \left| \psi^g_{i-1,0} \right\rangle
\end{aligned}
$$

$$
\begin{aligned}
&= \sum_{x,\widehat{y},d\in\mathcal{G}_{0[\leq i-1]}} \alpha_{x,\widehat{y},d}\ \bar{\mathit{\Pi}}_{\mathcal{G}_{0[\leq i]}} \circ \ddot{U}_i \circ \mathsf{cO}_0 \left|\gamma_{x,\widehat{y}}\right\rangle \otimes |d\rangle \\
&= \sum_{x,\widehat{y},d\in\mathcal{G}_{0[\leq i-1]}} \alpha_{x,\widehat{y},d}\ \bar{\mathit{\Pi}}_{\mathcal{G}_{0[\leq i]}} \circ \ddot{U}_i \left(\left|\gamma_{x,\widehat{y}}\right\rangle \otimes \mathsf{cO}_{p_0(x)\widehat{y}} |d\rangle \right) \\
&= \sum_{\substack{x,\widehat{y},d'\in\mathcal{D}_0,\\ d\in\mathcal{G}_{0[\leq i-1]}}} \alpha_{x,\widehat{y},d} \left\langle d' \middle| \mathsf{cO}_{p_0(x)\widehat{y}} \middle| d \right\rangle \bar{\mathit{\Pi}}_{\mathcal{G}_{0[\leq i]}} \circ \ddot{U}_i \left|\gamma_{x,\widehat{y}}\right\rangle \otimes |d'\rangle \\
&= \sum_{\substack{x,x',\widehat{y},\widehat{y}',d'\in\mathcal{D}_0,\\ d\in\mathcal{G}_{0[\leq i-1]}}} \alpha_{x,\widehat{y},d} \left\langle d' \middle| \mathsf{cO}_{p_0(x)\widehat{y}} \middle| d \right\rangle \left\langle \gamma_{x',\widehat{y}'} \middle| U_i \middle| \gamma_{x,\widehat{y}} \right\rangle \bar{\mathit{\Pi}}_{\mathcal{G}_{0[\leq i]}} \left|\varphi_{x',\widehat{y}',d'}\right\rangle \\
&= \sum_{\substack{x,x',\widehat{y},\widehat{y}',d'\in\mathcal{G}_{0[\leq i]},\\ d\in\mathcal{G}_{0[\leq i-1]}}} \alpha_{x,\widehat{y},d} \left\langle d' \middle| \mathsf{cO}_{p_0(x)\widehat{y}} \middle| d \right\rangle \left\langle \gamma_{x',\widehat{y}'} \middle| U_i \middle| \gamma_{x,\widehat{y}} \right\rangle \left|\varphi_{x',\widehat{y}',d'}\right\rangle,
\end{aligned}
$$

so that for any $x' \in \mathcal{I}$, $\widehat{y} \in \widehat{\mathcal{Y}}$, and $d' \in \mathcal{G}_{0[\leq i]}$, we have

$$
\left\langle \varphi_{x',\widehat{y}',d'} \middle| \psi^g_{i,0} \right\rangle = \sum_{x,\widehat{y},d\in\mathcal{G}_{0[\leq i-1]}} \alpha_{x,\widehat{y},d} \left\langle d' \middle| \mathsf{cO}_{p_0(x)\widehat{y}} \middle| d \right\rangle \left\langle \gamma_{x',\widehat{y}'} \middle| U_i \middle| \gamma_{x,\widehat{y}} \right\rangle.
$$

Similarly, we can show that

$$
\left\langle \varphi_{x',\widehat{y}',h(d')} \middle| \psi^g_{i,1} \right\rangle = \sum_{x,\widehat{y},d\in\mathcal{G}_{0[\leq i-1]}} \alpha_{x,\widehat{y},d} \left\langle h(d') \middle| \mathsf{cO}_{p_1(x)\widehat{y}} \middle| h(d) \right\rangle \left\langle \gamma_{x',\widehat{y}'} \middle| U_i \middle| \gamma_{x,\widehat{y}} \right\rangle.
$$

Then the third condition of Lemma 2 gives us

$$
\left\langle \varphi_{x',\widehat{y}',d'} \middle| \psi^g_{i,0} \right\rangle = \left\langle \varphi_{x',\widehat{y}',h(d')} \middle| \psi^g_{i,1} \right\rangle,
$$

thus completing the proof of the observation by induction. □

Proof of (31)**.** Using Observation (30) we get

$$
\begin{aligned}
\left\| \psi^g_{i,0} \right\| &= \left\| \sum_{x,\widehat{y},d\in\mathcal{G}_{0[\leq i]}} \left\langle \varphi_{x,\widehat{y},d} \middle| \psi^g_{i,0} \right\rangle \left|\varphi_{x,\widehat{y},d}\right\rangle \right\| \\
&= \sqrt{\sum_{x,\widehat{y},d\in\mathcal{G}_{0[\leq i]}} \left\langle \varphi_{x,\widehat{y},d} \middle| \psi^g_{i,0} \right\rangle^2} \\
&= \sqrt{\sum_{x,\widehat{y},d\in\mathcal{G}_{0[\leq i]}} \left\langle \varphi_{x,\widehat{y},h(d)} \middle| \psi^g_{i,1} \right\rangle^2} \\
&= \sqrt{\sum_{x,\widehat{y},d'\in\mathcal{G}_{1[\leq i]}} \left\langle \varphi_{x,\widehat{y},d'} \middle| \psi^g_{i,1} \right\rangle^2} \\
&= \left\| \sum_{x,\widehat{y},d'\in\mathcal{G}_{1[\leq i]}} \left\langle \varphi_{x,\widehat{y},d'} \middle| \psi^g_{i,1} \right\rangle \left|\varphi_{x,\widehat{y},d'}\right\rangle \right\| = \left\| \psi^g_{i,1} \right\|,
\end{aligned}
$$

as claimed. □

C Proof of Proposition 5

Proposition 5. *For any pair of properties $\mathcal{P}$ and $\mathcal{P}'$,*

$$[\![\mathcal{P} \hookrightarrow \mathcal{P}']\!] \geq \left\| \bar{\mathit{\Pi}}_{\mathcal{P}'} \circ \mathit{cO} \circ \bar{\mathit{\Pi}}_{\mathcal{P}} \right\|.$$

Proof. We first observe that

$$\left\| \bar{\mathit{\Pi}}_{\mathcal{P}'} \circ \mathsf{cO} \circ \bar{\mathit{\Pi}}_{\mathcal{P}} \right\| \leq \max_{x \in \widetilde{\mathcal{X}}, \widehat{y} \in \widehat{\mathcal{Y}}} \| \mathit{\Pi}_{\mathcal{P}'} \circ \mathsf{cO}_{x\widehat{y}} \circ \mathit{\Pi}_{\mathcal{P}} \| \tag{57}$$

by (56). Fix any $x, \widehat{y}$, and d. Then, by the definition of $d|^x$, for any $|\mathit{\Delta}\rangle \in \mathbb{C}[d|^x]$, we have $\mathsf{cO}_{x\widehat{y}} \ |\mathit{\Delta}\rangle \in \mathbb{C}[d|^x]$, i.e., $\mathsf{cO}_{x\widehat{y}}$ is a unitary on $\mathbb{C}[d|^x]$. Thus, for any $|\mathit{\Delta}\rangle \in \mathbb{C}[d|^x]$,

$$\begin{aligned} \mathit{\Pi}_{\mathcal{P}'} \circ \mathsf{cO}_{x\widehat{y}} \circ \mathit{\Pi}_{\mathcal{P}} |\mathit{\Delta}\rangle &= \mathit{\Pi}_{\mathcal{P}'} \circ \mathsf{cO}_{x\widehat{y}} \circ \mathit{\Pi}_{\mathcal{P} \cap d|^x} |\mathit{\Delta}\rangle \\ &= \mathit{\Pi}_{\mathcal{P}' \cap d|^x} \circ \mathsf{cO}_{x\widehat{y}} \circ \mathit{\Pi}_{\mathcal{P} \cap d|^x} |\mathit{\Delta}\rangle , \end{aligned}$$

where for the last equality we use the fact that $\mathit{\Pi}_{\mathcal{P} \cap d|^x} |\mathit{\Delta}\rangle \in \mathbb{C}[d|^x]$, and thus $\mathsf{cO}_{x\widehat{y}} \circ \mathit{\Pi}_{\mathcal{P} \cap d|^x} |\mathit{\Delta}\rangle \in \mathbb{C}[d|^x]$. Thus, for any $x, \widehat{y}$, we have

$$\begin{aligned} \| \mathit{\Pi}_{\mathcal{P}'} \circ \mathsf{cO}_{x\widehat{y}} \circ \mathit{\Pi}_{\mathcal{P}} \| &= \sup_{|\mathit{\Delta}\rangle \in \mathbb{C}[\mathcal{D}|_{\widetilde{\mathcal{X}}}]} \| \mathit{\Pi}_{\mathcal{P}'} \circ \mathsf{cO}_{x\widehat{y}} \circ \mathit{\Pi}_{\mathcal{P}} |\mathit{\Delta}\rangle \| \\ &= \max_{d \in \mathcal{D}|_{\widetilde{\mathcal{X}}}} \sup_{|\mathit{\Delta}\rangle \in \mathbb{C}[d|^x]} \| \mathit{\Pi}_{\mathcal{P}'} \circ \mathsf{cO}_{x\widehat{y}} \circ \mathit{\Pi}_{\mathcal{P}} |\mathit{\Delta}\rangle \| \\ &= \max_{d \in \mathcal{D}|_{\widetilde{\mathcal{X}}}} \sup_{|\mathit{\Delta}\rangle \in \mathbb{C}[d|^x]} \left\| \mathit{\Pi}_{\mathcal{P}' \cap d|^x} \circ \mathsf{cO}_{x\widehat{y}} \circ \mathit{\Pi}_{\mathcal{P} \cap d|^x} |\mathit{\Delta}\rangle \right\| \\ &= \max_{d \in \mathcal{D}|_{\widetilde{\mathcal{X}}}} \left\| \mathit{\Pi}_{\mathcal{P}' \cap d|^x} \circ \mathsf{cO}_{x\widehat{y}} \circ \mathit{\Pi}_{\mathcal{P} \cap d|^x} \right\|, \end{aligned} \tag{58}$$

where for the last equality we observe that $\mathit{\Pi}_{\mathcal{P}' \cap d|^x} \circ \mathsf{cO}_{x\widehat{y}} \circ \mathit{\Pi}_{\mathcal{P} \cap d|^x}$ takes any state orthogonal to $\mathbb{C}[d|^x]$ to 0, so for any $|\mathit{\Delta}\rangle \in \mathbb{C}[\mathcal{D}|_{\widetilde{\mathcal{X}}}]$ we have $|\mathit{\Delta}'\rangle := \mathit{\Pi}_{d|^x} |\mathit{\Delta}\rangle \in \mathbb{C}[d|^x]$ such that

$$\left\| \mathit{\Pi}_{\mathcal{P}' \cap d|^x} \circ \mathsf{cO}_{x\widehat{y}} \circ \mathit{\Pi}_{\mathcal{P} \cap d|^x} |\mathit{\Delta}\rangle \right\| \leq \left\| \mathit{\Pi}_{\mathcal{P}' \cap d|^x} \circ \mathsf{cO}_{x\widehat{y}} \circ \mathit{\Pi}_{\mathcal{P} \cap d|^x} |\mathit{\Delta}'\rangle \right\|.$$

Plugging (58) in (57) gives

$$\left\| \bar{\mathit{\Pi}}_{\mathcal{P}'} \circ \mathsf{cO} \circ \bar{\mathit{\Pi}}_{\mathcal{P}} \right\| \leq \max_{x \in \widetilde{\mathcal{X}}, \widehat{y} \in \widehat{\mathcal{Y}}, d \in \mathcal{D}|_{\widetilde{\mathcal{X}}}} \left\| \mathit{\Pi}_{\mathcal{P}' \cap d|^x} \circ \mathsf{cO}_{x\widehat{y}} \circ \mathit{\Pi}_{\mathcal{P} \cap d|^x} \right\| = [\![\mathcal{P} \hookrightarrow \mathcal{P}']\!],$$

thus establishing the proposition. □

D Proof of Lemma 1

Before proving Lemma 1, we introduce some more setup and borrow a counting result from [11]. We begin by singling out the unitary that acts on the cell $|d(x)\rangle$ when $\mathsf{cO}_{x\widehat{y}}$ acts on $|d\rangle$. Let $\mathsf{V}_{\widehat{y}}$ be the unitary defined on the basis $\mathcal{B}_F$ as

$$\mathsf{V}_{\widehat{y}} |\widehat{z}\rangle := |\widehat{z} + \widehat{y}\rangle = \left| \widehat{z \oplus y} \right\rangle .$$

Then we can write

$$\mathsf{O}_{x\widehat{y}} = \bigotimes_{\widetilde{\mathcal{X}}} \left[\, |x\rangle\langle x| \otimes \mathsf{V}_{\widehat{y}} + (I_m - |x\rangle\langle x|\,) \otimes I_n \right],$$

which applies the same cell unitary $|x\rangle\langle x| \otimes \mathsf{V}_{\widehat{y}} + (I_m - |x\rangle\langle x|\,) \otimes I_n$ to every cell. For the cell $|x\rangle\,|d(x)\rangle$, this cell unitary is identical to $I_m \otimes \mathsf{V}_{\widehat{y}}$, while for all other cells it is identical to I_{m+n}. Thus we can more simply write

$$\mathsf{O}_{x\widehat{y}} = I_{m+n} \otimes \ldots \otimes I_{m+n} \otimes (I_m \otimes \mathsf{V}_{\widehat{y}}) \otimes I_{m+n} \otimes \ldots \otimes I_{m+n}.$$

We extend $\mathsf{V}_{\widehat{y}}$ to $\overline{\mathcal{B}_F}$ by defining

$$\mathsf{V}_{\widehat{y}}\,|\bot\rangle = |\bot\rangle\,.$$

Next we define

$$\mathsf{cV}_{\widehat{y}} := \mathsf{comp}_0 \circ \mathsf{V}_{\widehat{y}} \circ \mathsf{comp}_0.$$

Recalling that

$$\mathsf{comp} = \bigotimes_{\widetilde{\mathcal{X}}} (I_m \otimes \mathsf{comp}_0),$$

we have

$$\begin{aligned} \mathsf{cO}_{x\widehat{y}} &= \mathsf{comp} \circ \mathsf{O}_{x\widehat{y}} \circ \mathsf{comp} \\ &= \bigotimes_{\widetilde{\mathcal{X}}} \left[\, |x\rangle\langle x| \otimes \mathsf{cV}_{\widehat{y}} + (I_m - |x\rangle\langle x|\,) \otimes I_n \right] \\ &= I_{m+n} \otimes \ldots \otimes I_{m+n} \otimes (I_m \otimes \mathsf{cV}_{\widehat{y}}) \otimes I_{m+n} \otimes \ldots \otimes I_{m+n}. \end{aligned}$$

Note that even though $\mathsf{O}_{x\widehat{y}}$ and $\mathsf{cO}_{x\widehat{y}}$ are defined on the entire $\mathbb{C}[\mathcal{D}]$ and not just $\mathbb{C}[\mathcal{D}|_{\widetilde{\mathcal{X}}}]$, in these calculations we continue to ignore the cells with labels outside $\widetilde{\mathcal{X}}$; since we are only dealing with databases restricted to $\widetilde{\mathcal{X}}$, the other cells will always remain empty at the beginning of each oracle call and will get set back to empty at the end of each oracle call, and hence won't affect our computations.

The transition matrix of $\mathsf{cV}_{\widehat{y}}$ is described in detail in [11, Lemma 4.3] (and is in fact also implicitly derived in [14, Proposition 2]). For our purposes it will be sufficient to borrow [11, Sect. 4.3, Eq. 8], which states that for any subset $\mathcal{S}$ of $\mathcal{Y}$,

$$\sum_{w\in\mathcal{S}, z\in\overline{\mathcal{Y}}, z\neq w} |\,\langle w|\mathsf{cV}_{\widehat{y}}|z\rangle\,|^2 \leq \frac{10|\mathcal{S}|}{2^n}.$$

Note that the condition $\mathcal{S} \subseteq \mathcal{Y}$ is important, as this result may not hold when $\bot \in \mathcal{S}$. Using this result, we can now proceed to prove Lemma 1.

Lemma 1 (Transition Capacity Bound). *Let $\mathcal{P}, \mathcal{P}'$ be properties on $\mathcal{D}|_{\widetilde{\mathcal{X}}}$ such that for every $x \in \widetilde{\mathcal{X}}$ and $d \in \mathcal{D}|_{\widetilde{\mathcal{X}}}$, we can find a set $\mathcal{S}_{x,d}^{\mathcal{P}^c \hookrightarrow \mathcal{P}'} \subseteq \mathcal{Y}$ satisfying*

$$\mathcal{P}' \cap d|^x \subseteq \{d' \in d|^x \mid d'(x) \in \mathcal{S}_{x,d}^{\mathcal{P}^c \hookrightarrow \mathcal{P}'}\} \subseteq \mathcal{P} \cap d|^x. \tag{59}$$

In other words, for any database $d' \in d|^x$,

$$d' \in \mathcal{P}' \implies d'(x) \in \mathcal{S}_{x,d}^{\mathcal{P}^c \hookrightarrow \mathcal{P}'} \implies d' \in \mathcal{P}.$$

Then we have

$$[\![\mathcal{P}^c \hookrightarrow \mathcal{P}']\!] \leq \max_{x \in \widetilde{\mathcal{X}}, d \in \mathcal{D}|_{\widetilde{\mathcal{X}}}} \sqrt{\frac{10|\mathcal{S}_{x,d}^{\mathcal{P}^c \hookrightarrow \mathcal{P}'}|}{2^n}}.$$

Proof. Fix $x \in \widetilde{\mathcal{X}}$ and $d \in \mathcal{D}|_{\widetilde{\mathcal{X}}}$. Let $\mathcal{S}$ denote $\mathcal{S}_{x,d}^{\mathcal{P}^c \hookrightarrow \mathcal{P}'}$, and $\varPi_{\mathcal{S}}$ denote the projection onto $\mathcal{S}$, defined by

$$\varPi_{\mathcal{S}} := \sum_{y \in \mathcal{S}} |y\rangle\langle y| \, .$$

Let $\mathcal{P}_\dagger$ denote the property $\{d' \in d|^x \mid d'(x) \in \mathcal{S}_{x,d}^{\mathcal{P}^c \hookrightarrow \mathcal{P}'}\}$. Then we have

$$\varPi_{\mathcal{P}_\dagger} = \sum_{d \in \mathcal{P}_\dagger} |d\rangle\langle d| = \bigotimes_{x' \in \widetilde{\mathcal{X}}} \left[|x\rangle\langle x| \otimes \varPi_{\mathcal{S}} + \sum_{x' \neq x} |x'\rangle\langle x'| \otimes |d(x')\rangle\langle d(x')| \right].$$

Since $\mathcal{P}' \cap d|^x \subseteq \mathcal{P}_\dagger$, we have $\varPi_{\mathcal{P}' \cap d|^x} \circ \varPi_{\mathcal{P}_\dagger} = \varPi_{\mathcal{P}' \cap d|^x}$. Moreover, since $\mathcal{P}^c \cap d|^x \subseteq \mathcal{P}_\dagger^c$, we have $\varPi_{\mathcal{P}_\dagger^c} \circ \varPi_{\mathcal{P}^c \cap d|^x} = \varPi_{\mathcal{P}^c \cap d|^x}$. Then for any $\widehat{y} \in \widehat{\mathcal{Y}}$ we have

$$\begin{aligned}
\left\| \varPi_{\mathcal{P}' \cap d|^x} \circ \mathsf{cO}_{x\widehat{y}} \circ \varPi_{\mathcal{P}^c \cap d|^x} \right\| &= \left\| \varPi_{\mathcal{P}' \cap d|^x} \circ \varPi_{\mathcal{P}_\dagger} \circ \mathsf{cO}_{x\widehat{y}} \circ \varPi_{\mathcal{P}_\dagger^c} \circ \varPi_{\mathcal{P}^c \cap d|^x} \right\| \\
&\leq \left\| \varPi_{\mathcal{P}_\dagger} \circ \mathsf{cO}_{x\widehat{y}} \circ \varPi_{\mathcal{P}_\dagger^c} \right\|.
\end{aligned}$$

Applying $\varPi_{\mathcal{P}_\dagger} \circ \mathsf{cO}_{x\widehat{y}} \circ \varPi_{\mathcal{P}_\dagger^c}$ to a database is equivalent to applying $\varPi_{\mathcal{S}} \circ \mathsf{cV}_{\widehat{y}} \circ (I_n - \varPi_{\mathcal{S}})$ to the cell labelled x and I_{m+n} to all other cells. Thus,

$$\begin{aligned}
\left\| \varPi_{\mathcal{P}' \cap d|^x} \circ \mathsf{cO}_{x\widehat{y}} \circ \varPi_{\mathcal{P}^c \cap d|^x} \right\| &\leq \| \varPi_{\mathcal{S}} \circ \mathsf{cV}_{\widehat{y}} \circ (I_n - \varPi_{\mathcal{S}}) \| \\
&\leq \| \varPi_{\mathcal{S}} \circ \mathsf{cV}_{\widehat{y}} \circ (I_n - \varPi_{\mathcal{S}}) \|_F \\
&= \sqrt{\sum_{w,z \in \overline{\mathcal{Y}}} \left| \langle w | \varPi_{\mathcal{S}} \circ \mathsf{cV}_{\widehat{y}} \circ (I_n - \varPi_{\mathcal{S}}) | z \rangle \right|^2} \\
&= \sqrt{\sum_{w \in \mathcal{S}, z \notin \mathcal{S}} \left| \langle w | \mathsf{cV}_{\widehat{y}} | z \rangle \right|^2} \\
&\leq \sqrt{\sum_{w \in \mathcal{S}, z \in \overline{\mathcal{Y}}, z \neq w} \left| \langle w | \mathsf{cV}_{\widehat{y}} | z \rangle \right|^2} \leq \sqrt{\frac{10|\mathcal{S}|}{2^n}},
\end{aligned}$$

where we can apply the last inequality because $\mathcal{S} \subseteq \mathcal{Y}$. Thus we have

$$\begin{aligned}
[\![\mathcal{P}^c \hookrightarrow \mathcal{P}']\!] &= \max_{x \in \widetilde{\mathcal{X}}, \widehat{y} \in \widehat{\mathcal{Y}}, d \in \mathcal{D}|_{\widetilde{\mathcal{X}}}} \left\| \varPi_{\mathcal{P}' \cap d|^x} \circ \mathsf{cO}_{x\widehat{y}} \circ \varPi_{\mathcal{P}^c \cap d|^x} \right\| \\
&\leq \max_{x \in \widetilde{\mathcal{X}}, d \in \mathcal{D}|_{\widetilde{\mathcal{X}}}} \sqrt{\frac{10|\mathcal{S}_{x,d}^{\mathcal{P}^c \hookrightarrow \mathcal{P}'}|}{2^n}},
\end{aligned}$$

thus completing the proof. □