Post-Quantum Security of Block Cipher Constructions

Gorjan Alagic[1], Chen Bai[2], Christian Majenz[3], and Kaiyan Shi[4]

[1] QuICS, University of Maryland/NIST
galagic.umd.edu
[2] Dept. of Computer Science, Virginia Tech
cbai1@vt.edu
[3] Dept. of Applied Mathematics and Computer Science, Technical University of Denmark
chmaj@dtu.dk
[4] Dept. of Computer Science, University of Maryland
kshi12@umd.edu

Abstract. Block ciphers are versatile cryptographic ingredients that are used in a wide range of applications ranging from secure Internet communications to disk encryption. While post-quantum security of public-key cryptography has received significant attention, the case of symmetric-key cryptography (and block ciphers in particular) remains a largely unexplored topic. In this work, we set the foundations for a theory of post-quantum security for block ciphers and associated constructions. Leveraging our new techniques, we provide the first post-quantum security proofs for the key-length extension scheme FX, the tweakable block ciphers LRW and XEX, and most block cipher encryption and authentication modes. Our techniques can be used for security proofs in both the plain model and the quantum ideal cipher model. Our work takes significant initial steps in establishing a rigorous understanding of the post-quantum security of practical symmetric-key cryptography.

Table of Contents

1 Introduction . . . 3
1.1 Background . . . 3
1.2 This work . . . 3
1.3 Technical summary of results . . . 4
1.4 Related Work . . . 7
2 Preliminaries . . . 7
3 Ideal Cipher Resampling . . . 8
4 Post-Quantum Security of FX . . . 9
4.1 The construction . . . 9
4.2 Post-Quantum Security . . . 9
4.3 Tightness . . . 15
4.4 Application . . . 15
The PRIDE cipher. . . . 16
5 Tweakable Block Ciphers . . . 16
5.1 Definitions . . . 16
5.2 Post-Quantum Security of LRW using the Hybrid Technique . . . 19
5.3 Tightness . . . 20
6 Block Cipher Modes . . . 20
6.1 Definitions . . . 20
6.2 PRP-PQ Security of an Ideal Cipher . . . 21
6.3 Security of Block Cipher Modes . . . 22
General Theorem . . . 22
Applications of Theorem 7 and Theorem 8. . . . 27
6.4 Security of LRW and XEX2 using Theorem 7 . . . 29
6.5 Comparison of LRW Security Bound . . . 29
A Proofs of the new resampling lemma . . . 34
A.1 Proof of Lemma 2 . . . 34
B More Details on Post-Quantum Security of FX . . . 37
B.1 Proof of Proposition 1 . . . 37
B.2 Handling Inverse Queries . . . 38
C Detailed Attacks on LRW and XEX2 . . . 42
C.1 Classical Distinguishing Attacks . . . 42
Birthday Collision Attack . . . 42
Even-Mansour Attack . . . 43
C.2 Classical Complete Key-Search Attack . . . 44
C.3 Quantum Complete Key Recovery Attack (shorter cipher key) . . . 44
C.4 Quantum Complete Key Recovery Attack (longer cipher key) . . . 45
D Post-Quantum Security Proof of LRW in Theorem 5 . . . 46
E Quantum Oracle Constructions in the Proof of Theorem 6 . . . 54
F Post-Quantum Lower Bounds for Modes . . . 55

1 Introduction

1.1 Background

Block ciphers. A block cipher is a keyed family of efficiently-implementable permutations of $\{0,1\}^n$. A block cipher π is secure if, for a uniformly random key k, the permutation π_k is indistinguishable from random to adversaries that can make forward and inverse queries to π_k. The most well-known example of a block cipher is the Advanced Encryption Standard (AES) [DBN+01], which is a fundamental ingredient in secure Internet communications and much more.

Block ciphers are ubiquitous in real-world cryptography. They are versatile ingredients that can be adapted to a variety of cryptographic applications. Their security can be increased via simple key-length extension schemes like FX [KR96,KR01]. They can also be expanded into an exponentially-large family of ciphers via tweakable constructions like LRW and XEX2 [LRW02,Rog13]. Finally, by means of *block cipher modes*, block ciphers can be used to construct a multitude of symmetric-key encryption and/or authentication schemes, with a wide range of options for both security and performance (see, e.g., [Dwo01,Dwo07,Dwo10a,GLL17]). In applications, block cipher modes are ubiquitous in secure communications, while tweakable ciphers are commonly used in disk encryption schemes.

Post-quantum security. The impact of large-scale quantum computation on the security of block ciphers and associated cryptographic constructions is not fully understood. While Shor's algorithm [Sho94] spurred intense scrutiny of the impact of quantum computers on public-key cryptography, post-quantum security of symmetric-key cryptography has received scant attention. While there are no known dramatic quantum attacks against currently-deployed symmetric-key schemes, there are important reasons to understand this setting in general (and the block cipher case in particular), as we now briefly explain.

First, it is *in principle* possible that some symmetric-key schemes in use today are not post-quantum secure[5]. Second, many symmetric-key constructions rely crucially on security proofs, and only a handful of such proofs for post-quantum security are known (mainly for Even-Mansour-type constructions [ABKM22,ABK+24,BEM24] and the Ascon scheme [Hos25]). Finally, fine-grained bounds in proofs often inform parameter selection when deploying symmetric-key schemes, and such bounds are essentially unavailable in the post-quantum case. Instead, practitioners typically assume that one can simply double the key length to avoid Grover search. However, the few results we do have indicate that this is sometimes overkill [ABKM22] and could in principle even be insufficient [BSS22].

1.2 This work

In this work, we set the foundations for a theory of post-quantum security for block ciphers and associated constructions. We then apply our techniques to give the first post-quantum security proofs for a variety of schemes, including key-length extension schemes, tweakable block ciphers, and block cipher modes. Our work takes significant initial steps in establishing a rigorous understanding of the post-quantum security of practical symmetric-key cryptography.

Our techniques can be used for security proofs both in the *plain model* (i.e., without any special assumptions or idealizations) as well as the *ideal cipher model* (ICM), a commonly used model in relevant classical proofs. In the ICM, one assumes that a *perfect* block cipher π was sampled (i.e., π_k is a uniformly random permutation for all k), and all parties have oracle access to it. In the traditional classical setting, this oracle access allows anyone to make queries of the form

$$(x,k) \mapsto \pi_k(x) \qquad \text{and} \qquad (x,k) \mapsto \pi_k^{-1}(x)\,. \tag{1}$$

In a post-quantum setting, however, adversaries in possession of a quantum computer will be able to execute the circuits of AES in superposition. It is thus natural to also grant quantum adversaries such access in the ideal cipher setting, via black-box unitaries

$$|k\rangle\,|x\rangle\,|y\rangle \mapsto |k\rangle\,|x\rangle\,|y \oplus \pi_k(x)\rangle \qquad \text{and} \qquad |k\rangle\,|x\rangle\,|y\rangle \mapsto |k\rangle\,|x\rangle\,|y \oplus \pi_k^{-1}(x)\rangle\,. \tag{2}$$

[5] One can easily construct relatively natural examples of schemes that are secure against classical computers but not against quantum computers. However, we doubt that this holds for any currently-deployed schemes.

The resulting model is called the quantum ideal cipher model (or QICM)[6] [CHL+25,SS19]. Proving results in the QICM has turned out to be quite difficult. Classical techniques are based on transcripts and do not translate to this setting. While Zhandry's compressed oracle [Zha19] does offer a somewhat analogous quantum lower bound method, it only applies to *random function oracles*, and extending it to permutations and ideal ciphers has proved challenging. Moreover, the post-quantum setting involves mixed query types: the ideal cipher is queried both *classically* (through the construction) and *quantumly* (directly by the adversary). This is the right post-quantum model: the construction is always a classical cipher implemented by the honest party on a classical computer using knowledge of the actual secret keys, while the block cipher is a public algorithm. Moreover, correct modeling of the construction oracle makes a crucial difference in security, as many commonly-used ciphers are *insecure* if the construction can be queried quantumly [KLLN16], but *secure* if the construction can only be queried classically [ABKM22].

In this paper, we only consider the model in which the ideal cipher is quantumly-accessible and any constructions involving the secret key are only classically-accessible. We refer to this model as the post-quantum model. In previous literature, this model was sometimes referred to as the Q1 model [BHNP+19,HS18,JST21,KLLN16], in contrast with the (unrealistic) Q2 model where all oracles can be queried quantumly.

Our results are summarized as follows. We give a more technical summary further below, including the precise security bounds we establish.

1. **QICM resampling.** We give a general *resampling lemma* that can be used to ascertain the ability of a quantum adversary to detect modifications to the ideal cipher (e.g., in a simulation as part of a proof). Previous resampling lemmas only held for random functions and permutations [ABKM22,ABK+24,GHHM21,Hos25]. This new tool can be combined with an adaptation of a proof approach of [ABKM22] to yield a powerful technique for QICM security proofs. We apply this technique to establish further results below.
2. **FX construction.** We prove post-quantum security of the FX key-length extension scheme in the QICM. This problem has evaded analysis for a number of years (a 2021 result only held for non-adaptive adversaries [JST21]). The bound we give for the number of queries needed to achieve a constant distinguishing probability is tight. A straightforward application of our result establishs post-quantum security for the lightweight cipher PRINCE [BCG+12].
3. **Tweakable ciphers.** We prove security of two widely-used tweakable block ciphers (LRW and XEX2) in both the plain model and in the QICM (with different bounds). We note that XEX2 is the basis of the XTS-AES disk encryption scheme used by most operating systems.
4. **Block cipher modes.** Finally, we observe that the security proofs of most block cipher modes (including all modes used in secure Internet traffic) translate easily to the post-quantum setting. Moreover, one can translate classical security bounds to post-quantum ones simply by replacing the appropriate strong pseudorandomness advantage term with its post-quantum analogue.

1.3 Technical summary of results

A technical summary of our main results is as follows.

A proof technique for the QICM. The first proof of post-quantum security of a block cipher construction was for the plain Even-Mansour construction [ABKM22]. Since then, the technique of [ABKM22] has been extended to show security of tweakable Even-Mansour [ABK+24], the Ascon lightweight cipher [Hos25], key-alternating ciphers [BEM24,BBC+25]. The technique has even been adapted to give certain proofs in the quantum Haar-random oracle model [HY24].

At a high level, the technique of [ABKM22] can be described as follows. The goal is to show indistinguishability between (i.) a pair of "real" oracles $(E_{(k)}, |E\rangle)$ and (ii.) an "ideal" uncorrelated pair $(R, |E\rangle)$. In both worlds, the first oracle is classical and the second oracle is quantum. Starting with a real-world q-query sequence

$$|E\rangle, E_{(k)}, |E\rangle, E_{(k)}, \ldots, |E\rangle, E_{(k)} \tag{3}$$

[6] The ICM (resp., QICM) is the natural block cipher analogue of the well-known Random Oracle Model (ROM, resp., QROM), which is often used to model hash functions in security proofs.

we switch the classical queries to the ideal case, one-by-one. A naive j-th hybrid would then be

$$\underbrace{|E\rangle, R, \ldots, |E\rangle, R}_{j}, \underbrace{|E\rangle, E_{(k)}, \ldots, |E\rangle, E_{(k)}}_{q-j}. \tag{4}$$

Unfortunately, this does not work: showing indistinguishability of hybrids $j-1$ and j would require first showing that the adversary cannot extract the key k during the last $q-j$ queries; indeed, with knowledge of k one easily notices the switch in past queries. This leads to a circular argument.

Instead, when switching classical queries to the ideal case, we also modify E (for all remaining queries) in a small number of locations, and then reset these modifications at a later stage:

$$\underbrace{|E\rangle, R, \ldots, |E\rangle, R}_{j}, \underbrace{|E^{[j]}\rangle, E^{[j]}_{(k)}, \ldots, |E^{[j]}\rangle, E^{[j]}_{(k)}}_{q-j}. \tag{5}$$

where $E^{[j]}$ denotes the quantum oracle with roughly j modified locations. Making such modifications necessitates the use of a particular technical ingredient: a *resampling lemma*[7]. Such a lemma states that an adversary cannot detect such modifications unless it has made a very large number of quantum queries to E prior to the modification being made.

Ideal cipher resampling. In this work, we develop the above technique in the case where E is an ideal cipher. This enables us to give the first full post-quantum security proofs for a variety of block cipher constructions. The key technical advance is a resampling lemma for the ideal cipher model. Consider the advantage of a computationally unbounded distinguisher $\mathcal{D}$ in the following three-phase experiment.

1. An ideal cipher $E : \{0,1\}^m \times \{0,1\}^n \to \{0,1\}^n$ is sampled, and $\mathcal{D}$ gets (two-way) quantum-query access to E. Then $\mathcal{D}$ (adaptively) selects and outputs a description of a distribution M.
2. A sample (k, s_0, s_1) is drawn from M, and $E_k(s_0)$ and $E_k(s_1)$ are swapped ($b = 1$) or not ($b = 0$).
3. Now $\mathcal{D}$ continues with access to (the possibly modified) E, and must eventually output a guess b' for the value of b.

We show that the guessing advantage of $\mathcal{D}$ is at most $4\sqrt{q \cdot 2^{n-h}}$ where h is the min-entropy of M and q is the number of queries made by $\mathcal{D}$ *in phase 1*. Note that the bound does not depend on the number of queries made in phase 3.

The full technical statement of this resampling lemma is given in Section 3, with proofs in Section A. Using this lemma and the hybrid technique described above, we are able to show the security of several constructions, discussed below.

FX construction. The FX construction [KR96,KR01] transforms a block cipher $E : \{0,1\}^m \times \{0,1\}^n \to \{0,1\}^n$ with key length m into another block cipher with the same block size but a longer key, as follows.

$$\mathsf{FX}^E_{k_0,k_1,k_2}(x) = E_{k_0}(x \oplus k_1) \oplus k_2 \tag{6}$$

Here $k_0 \leftarrow \{0,1\}^m$ and the marginal distributions of $k_1, k_2 \in \{0,1\}^n$ are uniform. For post-quantum security in the QICM, the relevant quantity is the distinguishing advantage

$$\mathsf{Adv}^{\mathsf{FX}}_{\mathcal{A}} := \left| \Pr_{E,k_0,k_1,k_2}\left[\mathcal{A}^{\mathsf{FX}[E],|E\rangle} = 1\right] - \Pr_{R,E}\left[\mathcal{A}^{R,|E\rangle} = 1\right] \right| \tag{7}$$

of an (unbounded) adversary $\mathcal{A}$ in distinguishing FX from a random permutation R using q_C classical queries, while making q_Q quantum queries to E. Both forward and inverse queries are allowed. In Section 4, we show that

$$\mathsf{Adv}^{\mathsf{FX}}_{\mathcal{A}} \le 4(q_C\sqrt{q_Q} + q_Q\sqrt{q_C}) \cdot 2^{-(m+n)/2} \qquad \text{for } q_C \ll 2^n \tag{8}$$

$$\mathsf{Adv}^{\mathsf{FX}}_{\mathcal{A}} \le q_Q^2 \cdot 2^{-m} \qquad \text{for } q_C \approx 2^n \tag{9}$$

[7] One also needs a *reprogramming lemma* (to reset these modifications at a later stage) but this is a relatively straightforward quantum search lower bound [ABKM22].

For calculating the number of queries required for constant success probability, our bounds are tight. For small q_C as well as $q_C \approx 2^n$ (i.e., the full codebook case), Grover search for remaining keys matches the bound. For $q_C \approx 2^{n/3}$, BHT collision-finding [KM12] also matches our bound.

In contrast, in the classical ideal cipher model, the FX construction is tightly secure (i.e., indistinguishable from an independent uniformly random permutation) with distinguishing advantage [KR01]

$$\mathsf{Adv}^{\mathsf{FX}}_{\mathcal{A}} \leq \frac{q_{\mathsf{FX}} \cdot q_E}{2^{m+n}}. \tag{10}$$

against an adversary making q_{FX} queries to FX_K and q_E queries to the ideal cipher E.

Applications to lightweight ciphers. A relatively straightforward application of our lower bound for FX establishes post-quantum security of the PRINCE [BCG+12] cipher in the QICM. The security of PRINCE is derived from the security of a primitive $\widetilde{\mathsf{FX}}$ which is closely related to standard FX. Specifically, let H be an $(m-1)$-dimensional subspace of $\mathbb{F}_2$, choose nonzero $\alpha \in \mathbb{F}_2^m$ not in H, and define

$$\widetilde{\mathsf{FX}}_{k_0,k_1,k_2}(x) \;=\; \begin{cases} \mathsf{FX}_{k_0,k_1,k_2}(x), & \text{if } k_0 \in H, \\ \mathsf{FX}^{-1}_{k_0 \oplus \alpha,\, k_1,\, k_2}(x), & \text{if } k_0 \in \alpha \oplus H. \end{cases}$$

The post-quantum security of $\widetilde{\mathsf{FX}}$ then follows directly from the same security for FX.

Another application of our FX analysis is PRIDE. Since PRIDE instantiates FX with the constraint $k_1 = k_2$, the relevant construction in the QICM is $\mathsf{FX}_{k_0,\,k_1,\,k_1}(x)$, which is already covered by our general proof. Because our analysis relies only on the marginal uniformity of the keys, this special case fits directly within our framework. As in Section 4.4, the post-quantum security of PRIDE follows immediately from our FX result.

Tweakable ciphers. As a second major application of our technique for the QICM, we establish post-quantum security of two tweakable block ciphers: LRW and XEX2 in Section 5. Tweakable block ciphers like LRW have a variety of applications, e.g., to modes for authentication and authenticated encryption [Rog04]. The XEX2 cipher forms the core of the widely-used and standardized XTS-AES disk encryption scheme [P1606,Dwo10b].

The LRW construction is defined by

$$\mathsf{LRW}^{E,h}_{k,k'}(\tau, x) = E_k(x \oplus h_{k'}(\tau)) \oplus h_{k'}(\tau)\,. \tag{11}$$

Here, τ is a tweak parameter, h is an XOR-universal hash function, and E is a block cipher. XEX2 is defined similarly, except that (roughly speaking) E'_k (for independent k') is used in place of h. Our post-quantum bound for distinguishing LRW from an ideal tweakable cipher is similar to that for FX, but with an additional additive term of $6q_C^2 \cdot 2^{-n}$. This corresponds to a (purely classical) collision attack that is possible against LRW but not against FX. For XEX2, our bound is $q_Q^2 \cdot 2^{-m} + 3q_C^2 \cdot 2^{-n}$, and is derived from Theorem 1 below.

In the classical setting, LRW achieves birthday-bound security. In the ideal cipher model, its distinguishing advantage is bounded by approximately $2^{-n/2} + 2^{-m/2}$. Prior work [LRW02,JN20] establishes that any classical adversary requires $q = O(2^{n/2})$ queries to distinguish LRW from an ideal tweakable cipher, and this bound is tight due to the existence of matching collision-based attacks. Similarly, the standardized XEX2 construction used in XTS-AES [P1619] has been extensively analyzed [CSR+08,LM08,Rog13], exhibiting comparable birthday-bound security in the classical model.

In the post-quantum setting, our additional term $q_C^2 \cdot 2^{-n}$ in the bound corresponds directly to the classical collision attack that also limits LRW 's classical security. The remaining terms in our bound arise from the inherent quantum speedups in key search and collision finding.

Block cipher modes. In Section 6, we give the following general lifting theorem for establishing post-quantum security of block cipher modes.

Theorem 1 (informal). *Let Exp be a security experiment and Con a construction instantiated with a block cipher E. Then the post-quantum security of Con is bounded as follows:*

$$\mathit{Adv}^{\mathit{Exp\text{-}PQ}}_{\mathit{Con}[E]}(q,t) \leq \mathit{Adv}^{\mathit{SPRP\text{-}PQ}}_{E}(q',t) + \delta(q), \tag{12}$$

where q' is the number of E-queries made by Con and the challenger, (q,t) denotes the (query, time)-complexity of the quantum adversary, and $\delta(q)$ is the classical information-theoretic security of Con.

While this lifting theorem is straightforward to prove, it offers a useful and rather general observation for establishing post-quantum security for a wide variety of block cipher modes, including CBC, ECBC, CMAC, GCM, and GCM-SST. It can also be applied in the QICM, with the SPRP advantage term becoming $(q')^2/2^m$, corresponding to a lower bound for quantum key search. This also yields lower bounds for LRW and XEX2, although, in these cases, better bounds are available using the hybrid technique discussed above. Some lower bounds computed via Theorem 1 are given in Section F.

We remark that, while Theorem 1 can be applied to FX, LRW, and XEX2 in the ideal cipher model, the specialized bounds we establish using the hybrid technique are far better.

1.4 Related Work

We focus on related work concerning post-quantum (i.e, Q1-model) security of keyed symmetric ciphers. We first discuss lower bounds, and then attacks. Since our results are query lower bounds, we will account separately for offline computation time and queries to the "offline primitive" (e.g., a public random permutation). Some cryptanalytic works do not make this distinction.

Alagic et al. [ABKM22] established a tight lower bound for Even-Mansour using the hybrid technique discussed above. These methods were then extended to prove security of tweakable Even-Mansour [ABK+24]. Recently, these techniques were also used to prove results about the security of key-alternating Feistel [BBC+25], multi-round Even-Mansour [BEM24], and Ascon [Hos25].

All ciphers under consideration can be attacked by first making (a small number of) classical queries, and then performing Grover search on the offline primitive for the full key. Kuwakado and Morii observed that BHT collision-finding [BHT97] can be used to perform key recovery for Even-Mansour using $O(2^{n/3})$ classical and quantum queries (and the same amount of time and space) [KM12]. Bonnetain et al. improved on this with the offline Simon algorithm, achieving the same query complexity but only using polynomial quantum space [BHN+19].

The offline-Simon algorithm also applies to key recovery on the FX, demanding $O(2^{(m+n)/3})$ classical queries while maintaining $\mathsf{poly}(n)$ classical memory. Additionally, the earlier meet-in-the-middle attack [HS18] on the FX requires $O(2^{3(m+n)/7})$ classical queries and $O(2^{(m+n)/7})$ classical memory. Bonnetain et al. [BSS22] propose the first general quantum key-recovery attack in the post-quantum setting on a symmetric block cipher, offering a super quadratic speedup compared to the best classical attacks. Their work extends the offline-Simon algorithm to attack the 2XOR Cascade construction [GT12], achieving a 2.5× quantum speedup in the exponent over the best-known classical attack.

2 Preliminaries

Notations and definitions. Sampling an element s uniformly at random from a set S is denoted by $s \leftarrow S$. We let $\mathcal{P}(n)$ denote the set of all permutations on $\{0,1\}^n$. A block cipher $E : \{0,1\}^m \times \{0,1\}^n \to \{0,1\}^n$ is a keyed permutation, i.e., $E_k(\cdot) = E(k,\cdot)$ is a permutation of $\{0,1\}^n$ for all $k \in \{0,1\}^m$. We also define the *swap operator* $\mathsf{swap}_{a,b} : \mathcal{X} \to \mathcal{X}$ as

$$\mathsf{swap}_{a,b}(x) = \begin{cases} a, & \text{if } x = b, \\ b, & \text{if } x = a, \\ x, & \text{otherwise.} \end{cases} \tag{13}$$

That is, $\mathsf{swap}_{a,b}$ exchanges a and b and leaves all other elements unchanged.

For an oracle $\mathcal{O}$, we write $\pm\mathcal{O}$ to denote two-directional access, i.e., the adversary gets access to both $\mathcal{O}$ and $\mathcal{O}^{-1}$. Given a function $F : \{0,1\}^t \to \{0,1\}^\ell$, we let $|F\rangle$ denote the appropriate quantum oracle $|x\rangle|y\rangle \to |x\rangle|y \oplus F(x)\rangle$ for making quantum queries to F. So, for example, the notation $\mathcal{A}^{F,|\pm P\rangle}$ denotes an algorithm $\mathcal{A}$ that can make classical queries to a function F (forward only) and quantum queries to a permutation P (in both the forward and inverse direction).

A reprogramming lemma. For a function $F : \{0,1\}^\ell \to \{0,1\}^n$ and a set $B \subset \{0,1\}^\ell \times \{0,1\}^n$ such that each $x \in \{0,1\}^\ell$ is the first element of at most one tuple in B, define

$$F^{(B)}(x) := \begin{cases} y & \text{if } (x,y) \in B \\ F(x) & \text{otherwise.} \end{cases} \tag{14}$$

The following is taken verbatim from [ABKM22, Lemma 3]:

Lemma 1 (Reprogramming Lemma). *Let $\mathcal{D}$ be a quantum distinguisher in the following experiment:*

Phase 1: *$\mathcal{D}$ outputs descriptions of a function $F_0 = F : \{0,1\}^\ell \to \{0,1\}^n$ and a randomized algorithm $\mathcal{B}$ whose output is a set $B \subset \{0,1\}^\ell \times \{0,1\}^n$ where each $x \in \{0,1\}^\ell$ is the first element of at most one tuple in B. Let $B_1 = \{x \mid \exists y : (x,y) \in B\}$ and $\varepsilon = \max_{x \in \{0,1\}^\ell} \{\Pr_{B \leftarrow \mathcal{B}}[x \in B_1]\}$.*

Phase 2: *$\mathcal{B}$ is run to obtain B. Let $F_1 = F^{(B)}$. A uniform bit b is chosen, and $\mathcal{D}$ is given quantum access to F_b.*

Phase 3: *$\mathcal{D}$ loses access to F_b, and receives the randomness r used to invoke $\mathcal{B}$ in phase 2. Then $\mathcal{D}$ outputs a guess b'.*

For any $\mathcal{D}$ making q queries in expectation when its oracle is F_0, it holds that

$$|\Pr[\mathcal{D} \text{ outputs } 1 \mid b = 1] - \Pr[\mathcal{D} \text{ outputs } 1 \mid b = 0]| \leq 2q \cdot \sqrt{\varepsilon}\,. \tag{15}$$

3 Ideal Cipher Resampling

The hybrid technique described in Section 1.3 is rather general, and could in principle be applied to a wide variety of settings. One particular setting of interest is the Quantum Ideal Cipher Model, where the oracle $|E\rangle$ gives quantum oracle access to the ideal cipher, and the oracle $E_{(k)}$ gives classical oracle access to some construction based on E (e.g., a tweakable cipher.) The main technical ingredient that is then required is an appropriate resampling lemma. We now briefly introduce the Quantum Ideal Cipher Model (QICM) and state our new resampling lemma for that model.

Quantum Ideal Cipher Model. The QICM was first discussed in [HY18]. Define $\mathcal{E}(m,n)$ to be the space of all keyed permutations where the key $k \in \{0,1\}^m$ and the input $x \in \{0,1\}^n$. In the quantum ideal cipher model, we treat the underlying block cipher as an ideal cipher $E \leftarrow \mathcal{E}(m,n)$, meaning that for each key k, the function E_k is a random permutation. Additionally, adversaries have quantum-computational capabilities in this model, and are thus allowed to make both forward and backward quantum queries to the ideal cipher.

In the security notions mentioned above, we consider algorithms having only classical access to secretly keyed primitives. When we consider constructions of keyed primitives (e.g., a tweakable block cipher) from public primitives (e.g., a random permutation), however, we provide the distinguisher with *quantum* oracle access to the public primitive. Thus, for example, a quantum distinguisher in the QICM can apply the unitary operators

$$|k\rangle\,|x\rangle\,|y\rangle \mapsto |k\rangle\,|x\rangle\,|E_k(x) \oplus y\rangle \tag{16}$$

$$|k\rangle\,|x\rangle\,|y\rangle \mapsto |k\rangle\,|x\rangle\,|E_k^{-1}(x) \oplus y\rangle \tag{17}$$

to quantum registers of the adversary's choice. We will denote an algorithm $\mathcal{A}$ with such access to a block cipher E by $\mathcal{A}^{|\pm E\rangle}$.

A resampling lemma for the QICM. We first give a resampling lemma for the ideal cipher model, generalizing a lemma of Hosoyamada [Hos25, Lemma 3]. Our generalization differs from [Hos25] in that it works in the QICM rather than the random permutation model, and in that it allows an arbitrary (distinguisher-chosen) distribution of the key and resampling points, rather than restricting to uniform sampling.

Lemma 2. *Let $\mathcal{D} = (\mathcal{D}_0, \mathcal{D}_1)$ be a quantum distinguisher interacting with the following experiment:*

Phase 1: *Choose a uniform ideal cipher $E \in \mathcal{E}(m,n)$ and give $\mathcal{D}$ quantum access to E and E^{-1}. Then $\mathcal{D}_0$ outputs a distribution D over $\{0,1\}^{m+2n}$.*

Phase 2: *Sample $(k_0, s_0, s_1) \in \{0,1\}^m \times \{0,1\}^n \times \{0,1\}^n$ according to D. Define $E^{(0)} = E$ and $E^{(1)}$ as*

$$E^{(1)}_{k^*}(x) = \begin{cases} E_{k^*}(x), & \text{if } k^* \neq k_0, \\ E_{k^*} \circ \mathsf{swap}_{s_0,\,s_1}(x), & \text{if } k^* = k_0, \end{cases} \tag{18}$$

where $\mathsf{swap}_{s_0,\,s_1}$ is the transposition swapping s_0 and s_1. A uniform bit $b \in \{0,1\}$ is chosen, and $\mathcal{D}$ is given k_0, s_0, s_1 along with quantum access to $E^{(b)}$. Finally, $\mathcal{D}$ outputs a guess b'.

For a distribution D on $\{0,1\}^{m+2n}$, define

$$\varepsilon \;=\; \max_{(k_0^*,s_0^*,s_1^*)\in\{0,1\}^{m+2n}} D(k_0^*, s_0^*, s_1^*)\,. \tag{19}$$

Then for any distinguisher $\mathcal{D}$ making at most q queries to E in Phase 1, it holds that

$$|\Pr[\mathcal{D}\ \textit{outputs}\ 1 \mid b=1] - \Pr[\mathcal{D}\ \textit{outputs}\ 1 \mid b=0]| \;\le\; 4\sqrt{2^n \cdot q \cdot \varepsilon}\,. \tag{20}$$

The proof follows the approach of [ABKM22,Hos25], which proceeds by bounding the trace distance between the quantum states produced after Phase 1 in the original case ($b=0$) and the reprogrammed case ($b=1$). Crucially, the distinguishing advantage depends only on the queries made in Phase 1: the swap operation itself does not alter the distribution of E globally, and so unless the adversary has queried the resampled points during Phase 1, the two cases are identically distributed. The proof of Lemma 2 is given in Appendix A.1.

4 Post-Quantum Security of FX

4.1 The construction

The FX key-length extension construction was analyzed in [KR96,KR01]. It is defined as follows.

Definition 1 (FX construction). *Let m and n be positive integers. Let $E : \{0,1\}^m \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher. The FX construction is defined as*

$$FX_K^E(x) = E_{k_0}(x \oplus k_1) \oplus k_2\,, \tag{21}$$

where $K = (k_0, k_1, k_2)$ with $k_0 \leftarrow \{0,1\}^m$ sampled independently and uniformly, and the marginal distributions of $k_1, k_2 \in \{0,1\}^n$ are uniform. For the remainder of this paper, we use $\mathcal{K}$ to denote this distribution over K.

4.2 Post-Quantum Security

We now state and prove a post-quantum security bound for FX (Definition 1). As in the classical case discussed above, we are concerned with the maximum distinguishing advantage between FX and an independent uniformly random permutation in the ideal-cipher model.

Theorem 2. *Let $\mathcal{A}$ be an adversary making q_C classical queries to its first oracle and q_Q quantum queries to its second oracle. Then*

$$\begin{aligned}\Bigg|\Pr_{(k_0,k_1,k_2)\leftarrow\{0,1\}^{m+2n};\ E\leftarrow\mathcal{E}(m,n)}\left[\mathcal{A}^{\pm FX_K[E],|\pm E\rangle}=1\right] \\ - \Pr_{R\leftarrow\mathcal{P}(n);E\leftarrow\mathcal{E}(m,n)}\left[\mathcal{A}^{\pm R,|\pm E\rangle}=1\right]\Bigg| \\ \le \frac{4}{\sqrt{2^m(2^n-q_C+1)}}\cdot q_C\sqrt{q_Q} + \frac{2}{\sqrt{2^{m+n}}}q_Q\sqrt{q_C}.\end{aligned}$$

Proof. For a general adversary, whether a particular classical query is made in the forward or inverse direction can be chosen in an arbitrary, adaptive manner. Without loss of generality, we consider adversaries who fix this order in advance; this incurs a factor 2 cost in the total number of queries. Our proof will proceed using a hybrid-by-classical-queries approach. We will now give the proof in the case where every classical query is in the forward direction. The case where the relevant classical query is in the inverse direction is handled analogously, and we omit the detailed proof.

We begin by setting down a way of modifying a given cipher based on a choice of key and a list of classical queries to an FX oracle. Let $E \in \mathcal{E}(m,n)$, $K = (k_0,k_1,k_2) \leftarrow \mathcal{K}$, and fix a list $\{(x_1,y_1),(x_2,y_2),\ldots,(x_{q_C},y_{q_C})\}$. Each pair (x_i,y_i) represents an input–output pair of a classical query.

Repeated queries are not allowed, i.e., $x_i \neq x_{i'}$ for all $i \neq i'$. For any $j \leq q_C$, let T_j be the list containing the first j queries. The "modified cipher" after j-many queries is denoted $E^{T_j,K}$, and is given by

$$E_{k^*}^{T_j,K}(x) = \begin{cases} E_{k^*}(x) & \text{if } k^* \neq k_0 \\ E_{k_0}^{T_j,K}(x) & \text{if } k^* = k_0. \end{cases} \tag{22}$$

where $E_{k_0}^{T_j,K}$ is defined as follows. First, define $E^{T_0,K} = E$, and for all $j \in [1, q_C]$,

$$E_{k_0}^{T_j,K}(x) = \mathsf{swap}_{E_{k_0}^{T_{j-1},K}(x_j \oplus k_1),\, y_j \oplus k_2} \circ E_{k_0}^{T_{j-1},K}(x)\,. \tag{23}$$

Note that the above definition differs from prior work [ABKM22,ABK+24], [BBC+25]. Specifically, $E^{T_i,K}$ is now constructed recursively based on $E^{T_{i-1},K}$, whereas in previous work, it was not. Roughly speaking, $E^{T_j,K}$ denotes a slight modification of E that remains consistent with the transcript T_j, as stated in Proposition 1. The proof is straightforward and we omit the routine details.

Proposition 1. *For any $E \in \mathcal{E}(m,n)$, $K = (k_0, k_1, k_2) \leftarrow \mathcal{K}$, $j \in \{1, \ldots, q_C\}$, transcript $T_j = \{(x_1, y_1), \ldots, (x_j, y_j)\}$ without repetition, and any $i \in \{1, \ldots, j\}$, it holds that*

$$E_{k_0}^{T_j,K}(x_i \oplus k_1) \oplus k_2 = y_i.$$

For compactness, we occasionally write E^j in place of $E^{T_j,K}$ when T_j and K are understood from the context. We also set $E^0 = E$.

We now define a sequence

$$\mathbf{H}_0, \mathbf{H}_0^1, \mathbf{H}_0^2, \mathbf{H}_0^3, \mathbf{H}_1, \mathbf{H}_1^1, \ldots, \mathbf{H}_{q_C}^3 \tag{24}$$

of hybrid experiments. Each experiment begins with sampling uniform $R \in \mathcal{P}(n)$ and $E \in \mathcal{E}(m,n)$, and a uniform key $K = (k_0, k_1, k_2) \leftarrow \mathcal{K}$. The remaining steps of each hybrid are as follows.

Experiment $\mathbf{H}_j$.

1. Run $\mathcal{A}$, answering its classical queries using R and quantum queries using E, stopping immediately *before* its $(j+1)^{\text{st}}$ classical query. Let T_j be the list of classical queries so far.
2. For the remainder of the execution of $\mathcal{A}$, answer its classical queries by $\mathsf{FX}_K[E^{T_j,K}]$ and its quantum queries by $E^{T_j,K}$.

Experiment $\mathbf{H}_j^1$.

1. Run $\mathcal{A}$, answering its classical queries using R and its quantum queries using E, until $\mathcal{A}$ makes its $(j+1)^{\text{st}}$ classical query, which we assume to be in the forward direction. Let T_j be the list of classical queries so far.
2. Define set $S = \{0,1\}^n \backslash \{x_1 \oplus k_1, \cdots, x_j \oplus k_1\}$. Choose uniform $s \in S$, and define $E^{(1)}$ as

$$E_{k^*}^{(1)}(x) = \begin{cases} E_{k^*}(x) & \text{if } k^* \neq k_0 \\ \left(E_{k_0} \circ \mathsf{swap}_{k_1 \oplus x_{j+1},\, s}\right)(x) & \text{if } k^* = k_0. \end{cases}$$

   Continue running $\mathcal{A}$, answering its remaining classical queries (including the $(j+1)^{\text{st}}$) using $\mathsf{FX}_K[(E^{(1)})^{T_j,K}]$, and its quantum queries using $(E^{(1)})^{T_j,K}$.

Experiment $\mathbf{H}_j^2$.

1. Run $\mathcal{A}$, answering its classical queries using R and its quantum queries using E, until $\mathcal{A}$ makes its $(j+1)^{\text{st}}$ classical query, which we assume to be in the forward direction. Let T_{j+1} be the list of classical queries so far, and T_j the subset consisting of the first j queries.
2. Answer query $j+1$ as in $\mathbf{H}_j^1$, i.e., with $(j+1)^{\text{st}}$ query using $y_{j+1} := \mathsf{FX}_K[(E^{(1)})^{T_j,K}](x_{j+1})$. Then construct $E^{j+1} \equiv E^{T_{j+1},K}$ as defined adaptively as in Equation 22. Continue running $\mathcal{A}$, answering its remaining classical queries using $\mathsf{FX}_K[E^{T_{j+1},K}]$, and its quantum queries using $E^{T_{j+1},K}$.

Experiment $\mathbf{H}_j^3$.

1. Run $\mathcal{A}$, answering its classical queries using R and its quantum queries using E, stopping immediately *after* its $(j+1)^{\text{st}}$ classical query. Let T_{j+1} be the set of classical queries so far.

2. For the remainder of the execution of $\mathcal{A}$, answer its classical queries using $\mathsf{FX}_K\left[E^{T_{j+1},K}\right]$ and its quantum queries using $E^{T_{j+1},K}$, i.e. $|E^{j+1}\rangle$.

We can compactly represent the hybrids $\left\{\mathbf{H}_j, \mathbf{H}_j^1, \mathbf{H}_j^2, \mathbf{H}_j^3, \mathbf{H}_{j+1}\right\}$ as the experiments in which $\mathcal{A}$'s queries are answered using the following oracle sequences. Let $(E^{(1)})^j$ denote $(E_{k_0}^{(1)})^{T_j,K}$.

$$
\begin{aligned}
\mathbf{H}_j &: |E\rangle, R, |E\rangle, \cdots, R, |E\rangle, \mathsf{FX}_K[\quad E^j \quad], |E^j\rangle \quad, \mathsf{FX}_K\left[E^j\right], |E^j\rangle, \cdots \\
\mathbf{H}_j^1 &: |E\rangle, R, |E\rangle, \cdots, R, |E\rangle, \mathsf{FX}_K[(E^{(1)})^j], |(E^{(1)})^j\rangle, \mathsf{FX}_K[(E^{(1)})^j], (E^{(1)})^j, \cdot \\
\mathbf{H}_j^2 &: |E\rangle, R, |E\rangle, \cdots, R, |E\rangle, \mathsf{FX}_K[(E^{(1)})^j], |E^{j+1}\rangle \quad, \mathsf{FX}_K[E^{j+1}], |E^{j+1}\rangle, \cdots \\
\mathbf{H}_j^3 &: |E\rangle, R, |E\rangle, \cdots, R, |E\rangle, \quad R \quad, |E^{j+1}\rangle \quad, \mathsf{FX}_K[E^{j+1}], |E^{j+1}\rangle, \cdots \\
\mathbf{H}_{j+1} &: \underbrace{|E\rangle, R, |E\rangle, \cdots, R, |E\rangle}_{j \text{ classical queries}}, \underbrace{\quad R \quad, |E\rangle}_{(j+1)^{\text{st}} \text{ classical query}}, \underbrace{\mathsf{FX}_K[E^{j+1}], |E^{j+1}\rangle, \cdots}_{q_C - j - 1 \text{ classical queries}}.
\end{aligned}
$$

Then we establish the following bounds on the distinguishability of $\mathbf{H}_j$ and $\mathbf{H}_{j+1}$, step by step, for $0 \le j < q_C$:

$$
\begin{aligned}
&\text{Lemma 3:} \quad \left|\Pr[\mathcal{A}(\mathbf{H}_j) = 1] - \Pr[\mathcal{A}(\mathbf{H}_j^1) = 1]\right| \le 4\sqrt{\frac{q_Q}{2^m(2^n - j)}} \\
&\text{Lemma 4:} \quad \mathbf{H}_j^1 = \mathbf{H}_j^2 \\
&\text{Lemma 5:} \quad \mathbf{H}_j^2 = \mathbf{H}_j^3 \\
&\text{Lemma 6:} \quad \left|\Pr[\mathcal{A}(\mathbf{H}_j^3) = 1] - \Pr[\mathcal{A}(\mathbf{H}_{j+1}) = 1]\right| \le 2 \cdot q_{Q,j+1}\sqrt{\frac{2(j+1)}{2^{m+n}}},
\end{aligned}
$$

where $q_{Q,j+1}$ is the expected number of queries $\mathcal{A}$ makes to P in the $(j+1)^{\text{st}}$ stage, i.e., the stage between the $(j+1)^{\text{st}}$ and $(j+2)^{\text{nd}}$ classical queries.

Using the above, we have

$$
\begin{aligned}
&\left|\Pr[\mathcal{A}(\mathbf{H}_0) = 1] - \Pr[\mathcal{A}(\mathbf{H}_{q_C}) = 1]\right| \\
&\le \sum_{j=0}^{q_C-1}\left(4\sqrt{\frac{q_Q}{2^m(2^n - j)}} + 2 \cdot q_{Q,j+1}\sqrt{\frac{2(j+1)}{2^{m+n}}}\right) \\
&\le \sum_{j=0}^{q_C-1}\left(4\sqrt{\frac{q_Q}{2^m(2^n - j)}} + 2 \cdot q_{Q,j+1}\sqrt{\frac{2q_C}{2^{m+n}}}\right) \\
&\le \frac{4}{\sqrt{2^m(2^n - q_C + 1)}} \cdot q_C\sqrt{q_Q} + \frac{2}{\sqrt{2^{m+n}}} q_Q\sqrt{q_C}. \qquad (25)
\end{aligned}
$$

□

Remark. When $q_C < \frac{3}{4}2^n$, our bound can be simplified to

$$
\frac{8}{\sqrt{2^{m+n}}}\left(q_C\sqrt{q_Q} + q_Q\sqrt{q_C}\right).
$$

As q_C approaches 2^n (in particular when $q_C = 2^n$), the bound above is no longer tight. In this case, as explained in Section 6.2, the distinguishing problem between (R, E) and (FX_K, E) is equivalent to the UNIQUE-SEARCH problem on k_0. By Corollary 2, this yields an advantage of $\frac{q_Q^2}{2^m}$.

We now prove Lemma 3, Lemma 4, Lemma 5 and Lemma 6.

Lemma 3. *For $j = 0, \ldots, q_C$,*

$$
\left|\Pr[\mathcal{A}(\mathbf{H}_j) = 1] - \Pr[\mathcal{A}(\mathbf{H}_j^1) = 1]\right| \le 4\sqrt{\frac{q_Q}{2^m(2^n - j)}}.
$$

Proof. In this lemma, we bound the distinguishability of $\mathbf{H}_j$ and $\mathbf{H}_j^1$.

$$\begin{aligned}
\mathbf{H}_j &: \ |E\rangle, R, |E\rangle, \cdots, R, |E\rangle, \mathsf{FX}_K[\ \ E^j\ \ ], |E^j\rangle \qquad, \mathsf{FX}_K\left[E^j\right], |E^j\rangle, \cdots \\
\mathbf{H}_j^1 &: \ |E\rangle, R, |E\rangle, \cdots, R, |E\rangle, \mathsf{FX}_K[(E^{(1)})^j], |(E^{(1)})^j\rangle, \mathsf{FX}_K[(E^{(1)})^j], (E^{(1)})^j, \cdots
\end{aligned}$$

Let $\mathcal{A}$ be a distinguisher between $\mathbf{H}_j$ and $\mathbf{H}_j^1$. We construct from $\mathcal{A}$ a distinguisher $\mathcal{D}$ for the resampling experiment of Lemma 2. $\mathcal{D}$ does:

Phase 1: $\mathcal{D}$ is given quantum access to an ideal cipher E. It samples a uniform $R \leftarrow \mathcal{P}_n$ and then runs $\mathcal{A}$, answering its quantum queries with E and its classical queries with R (in the appropriate directions), until $\mathcal{A}$ submits its $(j+1)^{\text{st}}$ classical query x_{j+1}. At that point, $\mathcal{D}$ has a list $T_j = \{(x_1, y_1), \cdots, (x_j, y_j)\}$ of the queries/answers $\mathcal{A}$ has made to its classical oracle thus far. Next, $\mathcal{D}$ constructs a distribution D on $\{0,1\}^{m+2n}$ and its sampling algorithm Π. To sample a tuple $(a_0, z_0, z_1) \leftarrow D$, Π does the following:
1 : Sample uniform $a_0 \in \{0,1\}^m$ and $z_0 \in \{0,1\}^n$.
2 : Construct $S = \{0,1\}^n \backslash \{z_0 \oplus x_1 \oplus x_{j+1}, \cdots, z_0 \oplus x_j \oplus x_{j+1}\}$.
3 : Sample uniform $z_1 \in S$, and output (a_0, z_0, z_1).

Phase 2: $\mathcal{D}$ is given $(k_0, s_0, s_1) \leftarrow D$ and quantum oracle access to a cipher $E^{(b)}$. Then $\mathcal{D}$ sets $k_1 = x_{j+1} \oplus s_0$, $k_2 \leftarrow \mathcal{K}_{|k_0,k_1}$[8] and $K = (k_0, k_1, k_2)$. It then continues running $\mathcal{A}$, answering its remaining classical queries (including the $(j+1)^{\text{st}}$) using $\mathsf{FX}_K[(E^{(b)})^{T_j,K}]$, and its remaining quantum queries using $(E^{(b)})^{T_j,K}$. $\mathcal{D}$ outputs whatever $\mathcal{A}$ does.

Defining $S^\perp = \{x_1 \oplus k_1, \cdots x_j \oplus k_1\}$, we have $s_1 \in \{0,1\}^n \setminus S^\perp$ from algorithm Π. In phase 1, distinguisher $\mathcal{D}$ perfectly simulates experiments $\mathbf{H}_j$ and $\mathbf{H}_j^1$ for $\mathcal{A}$ until the point where $\mathcal{A}$ makes its $(j+1)^{\text{st}}$ classical query. In phase 2, we first note that k_1 is uniform since s_0 is uniform and independent of x_{j+1}. If $b = 0$, $\mathcal{D}$ gets access to $E^{(0)} = E$ in phase 2. Since $\mathcal{D}$ answers all quantum queries using $(E^{(0)})^{T_j,K}$ and all classical queries using $\mathsf{FX}_K[(E^{(0)})^{T_j,K}]$, we see that $\mathcal{D}$ perfectly simulates $\mathbf{H}_j$ for $\mathcal{A}$ in that case. If, on the other hand, $b = 1$ in phase 2, then $\mathcal{D}$ gets access to $E^{(1)}$, where

$$E_{k^*}^{(1)}(x) = \begin{cases} E_{k^*}(x) & \text{if } k^* \neq k_0 \\ E_{k_0} \circ \mathsf{swap}_{s_0,\, s_1}(x) & \text{if } k^* = k_0\,. \end{cases}$$

Since $k_1 \coloneqq s_0 \oplus x_{j+1}$, it holds that

$$E_{k^*}^{(1)}(x) = \begin{cases} E_{k^*}(x) & \text{if } k^* \neq k_0 \\ E_{k_0} \circ \mathsf{swap}_{k_1 \oplus x_{j+1},\, s_1}(x) & \text{if } k^* = k_0\,. \end{cases}$$

Moreover, the fact that s_0 (and hence $s_0 \oplus x_{j+1}$), k_0 and k_2 are uniform implies that $\mathcal{D}$ perfectly simulates $\mathbf{H}_j^1$ for $\mathcal{A}$. Applying Lemma 2 thus gives

$$\left|\Pr[\mathcal{A}(\mathbf{H}_j) = 1] - \Pr[\mathcal{A}(\mathbf{H}_j^1) = 1]\right| \leq 4\sqrt{q_Q \cdot \varepsilon \cdot 2^n},$$

where,

$$\varepsilon = \max_{(k_0^*, s_0^*, s_1^*) \in \{0,1\}^{m+2n}} D(k_0, s_0, s_1) = \frac{1}{2^{m+n}(2^n - j)}.$$

Therefore, we have

$$\left|\Pr[\mathcal{A}(\mathbf{H}_j) = 1] - \Pr[\mathcal{A}(\mathbf{H}_j^1) = 1]\right| \leq 4\sqrt{\frac{q_Q}{2^m(2^n - j)}}.$$

□

Lemma 4. *For $j = 0, \ldots, q_C$, $\mathbf{H}_j^1 = \mathbf{H}_j^2$.*

[8] This denotes the conditional distribution of k_2 given (k_0, k_1). Note that while this conditional distribution may depend on (k_0, k_1), the induced marginal distribution of k_2 is uniform by definition of $\mathcal{K}$.

Proof.

$$\mathbf{H}_j^1 : \ |E\rangle, R, |E\rangle, \cdots, R, |E\rangle, \mathsf{FX}_K[(E^{(1)})^j], |(E^{(1)})^j\rangle, \mathsf{FX}_K[(E^{(1)})^j], (E^{(1)})^j, \cdots$$
$$\mathbf{H}_j^2 : \ |E\rangle, R, |E\rangle, \cdots, R, |E\rangle, \mathsf{FX}_K[(E^{(1)})^j], |E^{j+1}\rangle \quad , \mathsf{FX}_K[E^{j+1}], |E^{j+1}\rangle, \cdots.$$

We first prove the following proposition.

Proposition 2. *For any $K = (k_0, k_1, k_2) \leftarrow \mathcal{K}$, $j \in \{1, \ldots, q_C\}$, $i \in \{1, \ldots, j\}$, and all $r \in \{0, \ldots, j\}$*

$$(E_{k_0}^{(1)})^{T_r, K}(x_i \oplus k_1) \ = \ E_{k_0}^{T_r, K}(x_i \oplus k_1),$$

when $s \notin \{x_1 \oplus k_1, \cdots x_j \oplus k_1\}$.

Proof. We will do a proof by induction on r. We start by the base case $r = 0$. We note that since the classical queries are not repeated, $x_{j+1} \oplus k_1 \notin \{x_1 \oplus k_1, \cdots x_j \oplus k_1\}$. Additionally since $s \notin \{x_1 \oplus k_1, \cdots x_j \oplus k_1\}$, we have that for all $i \in \{1, \cdots, j\}$

$$\begin{aligned}(E_{k_0}^{(1)})^{T_0, K}(x_i \oplus k_1) := E_{k_0}^{(1)}(x_i \oplus k_1) &= E_{k_0} \circ \mathsf{swap}_{x_{j+1} \oplus k_1, \, s}(x_i \oplus k_1) \\ &= E_{k_0}(x_i \oplus k_1).\end{aligned}$$

Assume for some $r - 1 \geq 0$ that

$$(E_{k_0}^{(1)})^{T_{r-1}, K}(x_i \oplus k_1) = E_{k_0}^{T_{r-1}, K}(x_i \oplus k_1).$$

Then by the definition,

$$\begin{aligned}(E_{k_0}^{(1)})^{T_r, K}(x_i \oplus k_1) &= \mathsf{swap}_{(E_{k_0}^{(1)})^{T_{r-1}, K}(x_r \oplus k_1), \, y_r \oplus k_2} \circ (E_{k_0}^{(1)})^{T_{r-1}, K}(x_i \oplus k_1) \\ &= \mathsf{swap}_{E_{k_0}^{T_{r-1}, K}(x_r \oplus k_1), \, y_r \oplus k_2} \circ E_{k_0}^{T_{r-1}, K}(x_i \oplus k_1) \\ &= E_{k_0}^{T_r, K}(x_i \oplus k_1).\end{aligned}$$

By induction, the proposition holds for all $r \in \{0, \ldots, j\}$. □

In particular, for all $i \in \{1, \ldots, j\}$,

$$(E_{k_0}^{(1)})^{T_{i-1}, K}(x_i \oplus k_1) = E_{k_0}^{T_{i-1}, K}(x_i \oplus k_1).$$

To prove $\mathbf{H}_j^1$ and $\mathbf{H}_j^2$ are identical, it suffices to show that the quantum oracles $(E^{(1)})^j$ and E^{j+1} are identical. Note that $(E_{k^*}^{(1)})^j = E_{k^*}^{j+1}$ for all $k^* \neq k_0$, we only need to consider the case where $k^* = k_0$.

In both $\mathbf{H}_j^1$ and $\mathbf{H}_j^2$, the response to the $(j+1)^{\text{st}}$ classical query is:

$$\begin{aligned}y_{j+1} \stackrel{\text{def}}{=} \mathsf{FX}_K[(E^{(1)})^{T_j, K}](x_{j+1}) &= (E_{k_0}^{(1)})^{T_j, K}(x_{j+1} \oplus k_1) \oplus k_2 \\ &= \left(\prod_{i=j}^{1} \mathsf{swap}_{(E_{k_0}^{(1)})^{T_{i-1}, K}(x_i \oplus k_1), \, y_i \oplus k_2} \right) \circ E_{k_0}^{(1)}(x_{j+1} \oplus k_1) \oplus k_2 \\ &= \left(\prod_{i=j}^{1} \mathsf{swap}_{(E_{k_0})^{T_{i-1}, K}(x_i \oplus k_1), \, y_i \oplus k_2} \right) \circ E_{k_0}(s) \oplus k_2 = E_{k_0}^{T_j, K}(s) \oplus k_2,\end{aligned}$$

where the fourth equality comes from Proposition 2. We use "$\prod$" to denote sequential composition of operations, i.e., $\prod_{i=1}^{n} f_i = f_1 \circ \cdots \circ f_n$. By rearranging $s = \left(E_{k_0}^{T_j, K}\right)^{-1}(y_{j+1} \oplus k_2)$, it follows that for any $x \in \{0,1\}^n$,

$$\begin{aligned}&(E_{k_0}^{(1)})^j(x) \\ &= \mathsf{swap}_{(E_{k_0}^{(1)})^{j-1}(x_j \oplus k_1), \, y_j \oplus k_2} \circ \cdot \circ \mathsf{swap}_{E_{k_0}^{(1)}(x_1 \oplus k_1), \, y_1 \oplus k_2} \circ E_{k_0} \circ \mathsf{swap}_{x_{j+1} \oplus k_1, \, s}(x) \\ &= \mathsf{swap}_{E_{k_0}^{j-1}(x_j \oplus k_1), \, y_j \oplus k_2} \circ \cdots \circ \mathsf{swap}_{E_{k_0}(x_1 \oplus k_1), \, y_1 \oplus k_2} \circ E_{k_0} \circ \mathsf{swap}_{x_{j+1} \oplus k_1, \, s}(x) \\ &= E_{k_0}^j \circ \mathsf{swap}_{x_{j+1} \oplus k_1, \, (E_{k_0}^j)^{-1}(y_{j+1} \oplus k_2)}(x) \\ &= \mathsf{swap}_{E_{k_0}^j(x_{j+1} \oplus k_1), \, y_{j+1} \oplus k_2} \circ E_{k_0}^j(x) = E_{k_0}^{j+1}(x),\end{aligned}$$

where the second equality comes from Proposition 2. This concludes the proof that $(E^{(1)})^j \equiv E^{j+1}$. It follows that $\mathbf{H}_j^1 = \mathbf{H}_j^2$. □

Lemma 5. *For $j = 0, \ldots, q_C$, $\mathbf{H}_j^2 = \mathbf{H}_j^3$.*

Proof.

$$\begin{aligned}
\mathbf{H}_j^2 &: \ |E\rangle, R, |E\rangle, \cdots, R, |E\rangle, \mathsf{FX}_K[(E^{(1)})^j], |E^{j+1}\rangle \quad, \mathsf{FX}_K[E^{j+1}], |E^{j+1}\rangle, \cdots \\
\mathbf{H}_j^3 &: \ |E\rangle, R, |E\rangle, \cdots, R, |E\rangle, \qquad R \qquad, |E^{j+1}\rangle \quad, \mathsf{FX}_K[E^{j+1}], |E^{j+1}\rangle, \cdots .
\end{aligned}$$

We observe that $\mathbf{H}_j^2$ and $\mathbf{H}_j^3$ differ only in the response to the $(j+1)^{\text{st}}$ classical query. In $\mathbf{H}_j^2$, this query is answered using

$$y_{j+1} \ = \ \mathsf{FX}_K\big[(E^{(1)})^{T_j,K}\big](x_{j+1}) \ = \ E_{k_0}^{T_j,K}(s) \oplus k_2,$$

as shown in Lemma 4. In contrast, in $\mathbf{H}_j^3$ the same query is answered with $y_{j+1} = R(x_{j+1})$.

Next, we prove that y_{j+1} is distributed the same in both $\mathbf{H}_j^2$ and $\mathbf{H}_j^3$. Recall Proposition 1, we have

$$y_i \ = \ E_{k_0}^{T_j,K}(x_i \oplus k_1) \oplus k_2, \quad \forall i \in [1, j],$$

and since $s \in \{0,1\}^n \setminus \{x_1 \oplus k_1, \ldots, x_j \oplus k_1\}$, it follows that in $\mathbf{H}_j^2$,

$$y_{j+1} = E_{k_0}^{T_j,K}(s) \oplus k_2 \in \{0,1\}^n \setminus \{y_1, \ldots, y_j\}.$$

Moreover, because $E_{k_0}^{T_j,K}$ is a permutation, the mapping

$$x_i \oplus k_1 \ \mapsto \ y_i = E_{k_0}^{T_j,K}(x_i \oplus k_1) \oplus k_2$$

is injective. Since s is chosen uniformly from $\{0,1\}^n \setminus \{x_1 \oplus k_1, \ldots, x_j \oplus k_1\}$ and k_2 is uniform, the output y_{j+1} is uniformly distributed over $\{0,1\}^n \setminus \{y_1, \ldots, y_j\}$ in $\mathbf{H}_j^2$. In $\mathbf{H}_j^3$, since classical queries are not repeated, $y_{j+1} = R(x_{j+1})$ is also uniformly distributed over $\{0,1\}^n \setminus \{y_1, \ldots, y_j\}$. Thus, the distribution of y_{j+1} conditioned on all previous queries is identical in the two hybrids.

Moreover, in both $\mathbf{H}_j^2$ and $\mathbf{H}_j^3$, the construction of E^{j+1} follows exactly the same procedure, i.e., from the first $j+1$ classical input–output pairs and E as specified in Equation 22. Consequently, the two hybrids yield identical distributions, and hence $\mathbf{H}_j^2 = \mathbf{H}_j^3$. □

Lemma 6. *For $j = 0, \ldots, q_C - 1$,*

$$\Pr[\mathcal{A}(\mathbf{H}_j^3) = 1] - \Pr[\mathcal{A}(\mathbf{H}_{j+1}) = 1]| \le 2 \cdot q_{Q,j+1} \sqrt{\frac{2(j+1)}{2^{m+n}}},$$

where $q_{Q,j+1}$ is the expected number of queries $\mathcal{A}$ makes to P in the $(j+1)^{st}$ stage in the ideal world (i.e., in $\mathbf{H}_{q_C}$).

Proof. Let $\mathcal{A}$ be a distinguisher between $\mathbf{H}_j^3$ and $\mathbf{H}_{j+1}$. We construct a distinguisher $\mathcal{D}$ for the experiment from Lemma 1:

Phase 1: $\mathcal{D}$ samples uniform $E \in \mathcal{E}(m,n)$ and $R \in \mathcal{P}(n)$. It then runs $\mathcal{A}$, answering its quantum queries using R and its classical queries using E, until after it responds to $\mathcal{A}$'s $(j+1)^{\text{st}}$ classical query. Let $T_{j+1} = \{(x_i, y_i)\}_{i=1}^{j+1}$ be the list of classical queries by $\mathcal{A}$ thus far. $\mathcal{D}$ defines $F(a, k_0, x) := E_{k_0}^a(x)$ for $a \in \{1, -1\}$.
It also defines the following randomized algorithm $\mathcal{B}$: sample $K \leftarrow \mathcal{K}$ and write $K = (k_0^*, k_1^*, k_2^*)$. Then it computes the set B of input/output pairs to be reprogrammed so that $F^{(B)}(a, k_0^*, x) = \left(E_{k_0^*}^{T_{j+1},K}\right)^a(x)$ for all a, k_0^*, x. Finally, $\mathcal{D}$ outputs $(F, \mathcal{B})$.

Phase 2: $\mathcal{B}$ is run to generate B, and $\mathcal{D}$ is given quantum access to an oracle F_b. $\mathcal{D}$ resumes running $\mathcal{A}$, answering its quantum queries using F_b. Phase 2 ends before $\mathcal{A}$ makes its next (i.e., $(j+2)^{\text{nd}}$) classical query.

Phase 3: $\mathcal{D}$ is given the randomness used by $\mathcal{B}$ to generate k. It resumes running $\mathcal{A}$, answering its classical queries using $\mathsf{FX}_K[E^{T_{j+1},K}]$ and its quantum queries using $E^{T_{j+1},K}$. Finally, it outputs whatever $\mathcal{A}$ outputs.

It is immediate that if $b = 0$ (i.e., $\mathcal{D}$'s oracle in phase 2 is $F_0 = F$), then $\mathcal{A}$'s output is identically distributed to its output in $\mathbf{H}_{j+1}$, whereas if $b = 1$ (i.e., $\mathcal{D}$'s oracle in phase 2 is $F_1 = F^{(B)}$), then $\mathcal{A}$'s output is identically distributed to its output in $\mathbf{H}^3_j$. It follows that $|\Pr[\mathcal{A}(\mathbf{H}^3_j) = 1] - \Pr[\mathcal{A}(\mathbf{H}_{j+1}) = 1]|$ is equal to the distinguishing advantage of $\mathcal{D}$ in the reprogramming experiment of Lemma 1. To bound this quantity, we bound the parameter ε and the expected number of queries made by $\mathcal{D}$ in phase 2 (when $F = F_0$).

The value of ε can be bounded using the definition of $E^{T_{j+1},K}_{k^*_0}$ and the fact that $F^{(B)}(a, k^*_0, x) = \left(E^{T_{j+1},K}_{k^*_0}\right)^a(x)$. Fixing E and T_{j+1}, the probability that any particular input (a, k^*_0, x) is reprogrammed is at most the probability (over k) that it lies in the set

$$\left\{ \begin{array}{c} (1, k_0, x_i \oplus k_1), \left(1, k_0, E^{-1}_{k_0}(y_i \oplus k_2)\right), \\ (-1, k_0, E_{k_0}(x_i \oplus k_1)), (-1, k_0, y_i \oplus k_2) \end{array} \right\}^{j+1}_{i=1}.$$

We compute the probability that $(a, k^*_0, x) = (1, k_0, x_i \oplus k_1)$ for some fixed i. As k_0 and k_1 are uniform,

$$\Pr_k[(a, k^*_0, x) = (1, k_0, x_i \oplus k_1)] = \begin{cases} 2^{-(m+n)} & a = 1 \\ 0 & a = -1 \end{cases}.$$

A similar bound holds for the other possibilities. By distinguishing the cases $a = 1$ and $a = -1$ and applying a union bound, we get $\varepsilon \le 2(j+1)/2^{m+n}$.

The expected number of queries made by $\mathcal{D}$ in phase 2 when $F = F_0$ is equal to the expected number of queries made by $\mathcal{A}$ in its $(j+1)^{\text{st}}$ stage in $\mathbf{H}_{j+1}$. Since $\mathbf{H}_{j+1}$ and $\mathbf{H}_{q_C}$ are identical until after the $(j+1)^{\text{st}}$ stage is complete, this is precisely $q_{Q,j+1}$. □

Remark. Our proof covers the case $k_1 = k_2$. Since $\mathcal{K}$ allows arbitrary dependence between k_1 and k_2 as long as their marginals are uniform, choosing $k_2 = k_1$ is simply a valid (fully correlated) instantiation of $\mathcal{K}$. Our analysis never relies on k_1 and k_2 being distinct, so all arguments apply unchanged.

4.3 Tightness

Let q_C represent the number of online classical queries and q_Q denote the number of offline quantum computations. Different attacks with corresponding trade-off are presented in Table 1.

Typical attacks involve full-key recovery, which classically requires 2^{m+n} offline queries, while quantumly, it requires only $2^{(m+n)/2}$ offline queries using Grover's algorithm. The Grover+BHT attack employs Grover's algorithm to recover the cipher key k_0 and uses the BHT/Kuwakado–Morii [KM12] to determine the whitening keys k_1 and k_2. It requires $q_Q = 2^{m/2+n/3}$ quantum queries and $q_C = 2^{n/3}$ classical queries. Details of this attack is similar to that on LRW, which is provided in Appendix C. The resources used align with $\frac{2}{\sqrt{2^{m+n}}} q_Q \sqrt{q_C}$ in the security bound established in Theorem 2.

In Meet-in-the-Middle attack [HS18], $q_C \cdot q_Q^6 = 2^{3(m+n)}$ classical online queries are required under the condition that only polynomially many qubits are available, by using the multi-target preimage search [CNPS17]. This attack was later improved by the offline-Simon attack [BHNP+19], which combines quantum search with quantum period finding, with a trade-off $q_C \cdot q_Q^2 = 2^{m+n}$, which also matches $\frac{2}{\sqrt{2^{m+n}}} q_Q \sqrt{q_C}$ term in the security bound.

4.4 Application

In this section, we present post-quantum security analyses of lightweight block ciphers that instantiate the FX construction, namely PRINCE and PRIDE, as applications of our framework.

PRINCE [BCG+12] is a lightweight block cipher designed for ultra-low latency applications, particularly in pervasive and embedded computing. Its distinguishing feature is the α-reflection property, which makes encryption and decryption nearly identical, thereby enabling very efficient hardware implementations. Concretely, PRINCE is based on $\mathsf{PRINCE}_{\text{core}}$, which can be viewed as a $\widetilde{\mathsf{FX}}$ construction, namely the α-reflection variant of the classical FX design.

Reference	Tradeoff between q_C and q_Q
Classical [Din15]	$q = 2^{m+n}$
Grover	$q_Q = 2^{\frac{m+n}{2}}, q_c = \text{constant}$
Grover + BHT [KM12]	$q_Q = 2^{\frac{m}{2}+\frac{n}{3}}, q_C = 2^{\frac{n}{3}}$
Meet-in-the-Middle [HS18]	$q_C \cdot q_Q^6 = 2^{3(m+n)}, q_C \leq \{2^n, 2^{3(m+n)/7}\}$
Offline-Simon [BHNP+19]	$q_C \cdot q_Q^2 = 2^{m+n}, q_C \leq 2^n$

Table 1. Tradeoffs for quantum attacks on the FX construction.

The α-reflection property ensures that this permutation can be inverted with minimal overhead. The classical security of this design is analyzed in Section 4.1 of [BCG+12].

The classical security of PRINCE is analyzed in the ideal cipher model via the primitive $\widetilde{\mathsf{FX}}$, the α-reflection variant of the standard FX construction. Let $\mathbb{F}_2^m$ denote the m-dimensional vector space over $\mathbb{F}_2$. Let H be an $(m-1)$-dimensional linear subspace of $\mathbb{F}_2^m$, and let $\alpha \in \mathbb{F}_2^m$ be a fixed nonzero element with $\alpha \notin H$. Thus, $\mathbb{F}_2^m$ is partitioned as $H \cup (\alpha \oplus H)$. Define

$$\widetilde{\mathsf{FX}}_{k_0,k_1,k_2}(x) \;=\; \begin{cases} \mathsf{FX}_{k_0,k_1,k_2}(x), & \text{if } k_0 \in H, \\ \mathsf{FX}^{-1}_{k_0 \oplus \alpha,\, k_1,\, k_2}(x), & \text{if } k_0 \in \alpha \oplus H. \end{cases}$$

[BCG+12, Corollary 1] shows that $\widetilde{\mathsf{FX}}$ achieves the same level of security as the original FX construction, in the pure classical setting.

Corollary 1 ([BCG+12]). $Adv^{\mathsf{SPRP\text{-}IC}}_{\mathsf{FX}}(q_{\mathsf{FX}}, q_E) = Adv^{\mathsf{SPRP\text{-}IC}}_{\widetilde{\mathsf{FX}}}(q_{\widetilde{\mathsf{FX}}}, q_E)$.

The classical proof of Corollary 1 carries over directly to the post-quantum setting. Together with Theorem 2, this implies the post-quantum security of $\widetilde{\mathsf{FX}}$, and hence the post-quantum security of PRINCE in the QICM, i.e., where $\mathsf{PRINCE}_{\text{core}}$ is replaced by an ideal cipher to which everyone has quantum access.

The PRIDE cipher. The classical security of PRIDE is analyzed via the standard FX construction, instantiated with the ARX-based core $\mathsf{PRIDE}_{\text{core}}$. In the specification of PRIDE, the master key is split into two halves, where one half is used for input/output whitening and the other half drives the round function of $\mathsf{PRIDE}_{\text{core}}$. Concretely, in the ideal cipher model where $\mathsf{PRIDE}_{\text{core}}$ is replaced by an ideal cipher E, PRIDE can be expressed as the special case $\mathsf{FX}k_0, k_1, k_0$ of the general FX construction, i.e.,

$$\mathsf{PRIDE}(k_0, k_1; x) = k_1 \oplus E_{k_0}(x \oplus k_1).$$

The classical security analysis of this design is provided in Section 5 of [ADK+14]. The post-quantum security of PRIDE follows directly from Theorem 2.

5 Tweakable Block Ciphers

5.1 Definitions

Definition 2 (Tweakable Permutation). *Let $\mathcal{T}$ be a tweak space. $\widetilde{\Pi} : \mathcal{T} \times \{0,1\}^n \to \{0,1\}^n$ is a tweakable permutation, where for each tweak $\tau \in \mathcal{T}$, $\widetilde{\Pi}(\tau, \cdot) \xleftarrow{\$} \mathcal{P}_n$ is an independently and randomly chosen permutation on $\{0,1\}^n$. We also define $\mathcal{E}(\mathcal{T}, n)$ to be the set of all such tweakable permutations. Additionally, we denote the "inverse" oracle as $\widetilde{\Pi}^{-1}(\tau, \cdot) := \widetilde{\Pi}_\tau^{-1}(\cdot)$ for some $\tau \in \mathcal{T}$.*

Definition 3 (Distinguishing Advantage). *Let $G : \{0,1\}^m \times \mathcal{T} \times \{0,1\}^n \longrightarrow \{0,1\}^n$ be a family of efficient, keyed permutations and $G^{-1} : \{0,1\}^m \times \mathcal{T} \times \{0,1\}^n \longrightarrow \{0,1\}^n$ be its corresponding decryption*

oracle. Consider an adversary $\mathcal{A}$ (which can be either quantum or classical) with time complexity $T_{\mathcal{A}}$. The advantage of $\mathcal{A}$ in attacking G is measured by

$$\mathsf{Adv}_G(\mathcal{A},q) := \left| \Pr_{k\leftarrow\{0,1\}^m}\left[\mathcal{A}^{G_k(\cdot,\cdot),G_k^{-1}(\cdot,\cdot)}=1\right] - \Pr_{\widetilde{\Pi}\leftarrow\mathcal{E}(\mathcal{T},n)}\left[\mathcal{A}^{\widetilde{\Pi}(\cdot,\cdot),\widetilde{\Pi}^{-1}(\cdot,\cdot)}=1\right]\right|,$$

where the probabilities are also taken over the randomness of $\mathcal{A}$, and $\mathcal{A}$ is allowed to make q ***classical*** *queries to the oracles within a time bound of t.*

Definition 4 (SPRP(-PQ) Security of Tweakable Block Cipher). *Let $G : \{0,1\}^m \times \mathcal{T} \times \{0,1\}^n \longrightarrow \{0,1\}^n$ be a tweakable block cipher. The (Post-Quantum) strong pseudorandom permutation security of G is measured by the maximum advantage over all (quantum) adversaries $\mathcal{A}$:*

$$\begin{aligned}\mathsf{Adv}_G^{\mathsf{SPRP(-PQ)}}(q,t) &= \max_{\mathcal{A}:T_{\mathcal{A}}\le t}\mathsf{Adv}_G(\mathcal{A},q)\\ &= \max_{\mathcal{A}:T_{\mathcal{A}}\le t}\left|\Pr_{k\leftarrow\{0,1\}^m}\left[\mathcal{A}^{G_k(\cdot,\cdot),G_k^{-1}(\cdot,\cdot)}=1\right] - \Pr_{\widetilde{\Pi}\leftarrow\mathcal{E}(\mathcal{T},n)}\left[\mathcal{A}^{\widetilde{\Pi}(\cdot,\cdot),\widetilde{\Pi}^{-1}(\cdot,\cdot)}=1\right]\right|.\end{aligned}$$

Here, the probabilities are additionally over the randomness of $\mathcal{A}$, and the adversary $\mathcal{A}$ is allowed up to q classical queries to the oracles within a time bound t. $\widetilde{\Pi}$ is an ideal tweakable block cipher, where $\widetilde{\Pi}(\tau,\cdot)$ is a random permutation, and $\tau \xleftarrow{\$} \mathcal{T}$.

Remark. Definition 4 provides a general definition of distinguishing advantage. However, when considering the SPRP-PQ-security of a construction in the QICM, where the underlying block cipher E is an ideal cipher, which can only be accessed through oracle queries rather than a public description; we provide adversaries with these additional oracles, $|E(\cdot,\cdot)\rangle$ and $|E^{-1}(\cdot,\cdot)\rangle$. Formally, if we consider the SPRP-PQ-security of a construction $G[E__]$ where the cipher E is accessible exclusively through oracle queries, then the security is measured as below:

$$\mathsf{Adv}^{\mathsf{SPRP\text{-}PQ}}_{G[E__]}(q,t) = \max_{\mathcal{A}}\left|\Pr_{k\leftarrow\{0,1\}^m}[\mathcal{A}^{G[E_k],G^{-1}[E_k^{-1}],|E\rangle,|E^{-1}\rangle}=1] - \Pr_{\widetilde{\Pi}\leftarrow\mathcal{E}(\mathcal{T},n)}\left[\mathcal{A}^{\widetilde{\Pi},\widetilde{\Pi}^{-1},|E\rangle,|E^{-1}\rangle}=1\right]\right|.$$

Definition 5 (XOR-Universality). *A family of functions $h = \{h_k : \{0,1\}^n \to \{0,1\}^n\}_{k\in\mathcal{K}}$ is called ε-XOR universal if for a randomly drawn key $k \in \mathcal{K}$, $\forall x,y,z \in \{0,1\}^n$ and $x \neq y$,*

$$\Pr_{k\xleftarrow{\$}\mathcal{K}}[h_k(x)\oplus h_k(y)=z] \le \varepsilon.$$

If $\varepsilon = \frac{1}{2^n}$, h is simply called XOR universal.

Definition 6 (Uniformity). *A family of functions h is uniform if $\forall x,y \in \{0,1\}^n$,*

$$\Pr_{k\xleftarrow{\$}\mathcal{K}}[h_k(x)=y] = \frac{1}{2^n}.$$

Remark. We note that, for these properties to hold, it is necessary that $|k| \ge n$. This further implies that for all x,y, there exists at least one k such that $h_k(x)=y$.

Definition 7 (LRW construction [LRW02]). *Let m and n be positive integers. Let $E : \{0,1\}^m \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher. Let h be a hash function. The LRW construction is defined as*

$$\mathsf{LRW}^{E,h}_{k,k'}(\tau,x) = E_k(x\oplus h_{k'}(\tau))\oplus h_{k'}(\tau),$$

where $k \xleftarrow{\$} \{0,1\}^m$ is the block cipher key and $k' \xleftarrow{\$} \{0,1\}^\kappa$ is the tweak key, $x \in \{0,1\}^n$ is the input, $\tau \in \{0,1\}^*$ is the tweak, and h is a hash function. For simpler notation, we write $\mathsf{LRW}^{E,h}_{k,k'}(\tau,x)$ as $\mathsf{LRW}_{k,k'}(\tau,x)$, when E and h are clear from the context.

Theorem 3 (Classical security of LRW [LRW02,Min06]). *Let h be an ε-XOR-universal hash function. Then for $\mathsf{LRW}^{E,h}$ construction,*

$$\mathsf{Adv}^{\mathsf{SPRP}}_{\mathsf{LRW}}(q,t) \leq \mathsf{Adv}^{\mathsf{SPRP}}_{E}(q,t) + q^2\varepsilon,$$

where q is the number of queries to $\mathsf{LRW}_{k,k'}(\cdot,\cdot)$ within a time bound t.

We note that the security of XEX2 is not analyzed via the hybrid argument in this section. Instead, its bound is derived later using the more general theorem presented in Theorem 7.

Definition 8 (XEX2 construction [Rog13]). *Let m and n be positive integers. Let $E : \{0,1\}^m \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher, and let $\alpha \in \mathbb{F}^*_{2^n}$. The tweakable block cipher construction XEX2 is*

$$\mathit{XEX2}^{E,\alpha}_{k,k'}(x,i,j) = E_k(x \oplus \Delta_{i,j,k'}) \oplus \Delta_{i,j,k'},$$

where $\Delta_{i,j,k'} = \alpha^j \times_* E_{k'}(i)$. Here, $\times_*$ denotes multiplication in the finite field $\mathbb{F}_{2^n} \setminus \{0^n\}$. The key of XEX2 consists of the block cipher keys $k, k' \xleftarrow{\$} \{0,1\}^m$. Furthermore, $x, i \in \{0,1\}^n$, and $j \in [0, 2^{20}-1]$.

We include a classical security analysis for completeness here. To facilitate the (classical and post-quantum) security analysis of XEX2, we define an inefficient idealized variant of XEX2, where $E_{k'}$ is replaced with a random permutation π, which is then considered part of the key.

Definition 9 (XEX2 with idealized hash). *The tweakable block cipher construction $\mathsf{XEX2}^{\mathrm{ideal-hash}}$ is*

$$\mathit{XEX2}^{E,\alpha}_{k,\pi}(x,i,j) = E_k(x \oplus \Delta_{i,j}) \oplus \Delta_{i,j},$$

where $\Delta_{i,j} = \alpha^j \times_* \pi(i)$. The key of $\mathsf{XEX2}^{\mathrm{ideal-hash}}$ consists of the block cipher key $k \xleftarrow{\$} \{0,1\}^m$ and the permutation $\pi \in S_{2^n}$, while the remaining parameters are as in Definition 8.

Observe that $\mathsf{XEX2}^{\mathrm{ideal-hash}}$ is the LRW construction with the hash function family

$$h^{\mathsf{XEX2}^{\mathrm{ideal-hash}}}_{\pi}(i,j) = \Delta_{i,j} = \alpha^j \times_* \pi(i).$$

Clearly, XEX2 and $\mathsf{XEX2}^{\mathrm{ideal-hash}}$ are indistinguishable for an SPRP adversary, up to the SPRP security of E.

Proposition 3. *The security of XEX2 and $\mathsf{XEX2}^{\mathrm{ideal-hash}}$ is related as follows.*

$$\mathsf{Adv}^{\mathsf{SPRP}}_{\mathit{XEX2}}(q,t) \leq \mathsf{Adv}^{\mathsf{SPRP}}_{E}(q,t) + \mathsf{Adv}^{\mathsf{SPRP}}_{\mathsf{XEX2}^{\mathrm{ideal-hash}}}(q,t).$$

This inequality holds for various adversarial models, including classical, post-quantum and quantum-access.

Next, we show that the hash function in $\mathsf{XEX2}^{\mathrm{ideal-hash}}$ is ε-XOR universal for negligible ε.

Lemma 7. *The hash function family $h^{\mathsf{XEX2}^{\mathrm{ideal-hash}}}$ is $\frac{1}{2^n-1}$-XOR universal.*

Proof. We bound

$$\max_{z \in \{0,1\}^n, (i_1,j_1) \neq (i_2,j_2)} \Pr_{\pi}[\pi(i_1) \times_* \alpha^{j_1} \oplus \pi(i_2) \times_* \alpha^{j_2} = z]$$

If $i_1 \neq i_2$, since π is a random permutation, the values $\pi(i_1)$ and $\pi(i_2)$ are distinct random elements from $\mathrm{GF}(2^n)$, implying that the XOR expression is uniformly distributed over the set $\mathsf{GF}(2^n) \setminus \{\alpha^{j_1} \oplus \alpha^{j_2}\}$. In this case, the probability expression above us thus bounded by $1/(2^n-1)$. When $i_1 = i_2$ and $j_1 \neq j_2$, the probability expression becomes:

$$\begin{aligned}
&\Pr_{\pi}[\pi(i_1) \times_* \alpha^{j_1} \oplus \pi(i_1) \times_* \alpha^{j_2} = z] \\
&= \Pr_{\pi}[\pi(i_1) \times_* (\alpha^{j_1} \oplus \alpha^{j_2}) = z] \\
&= \Pr_{\pi}[\pi(i_1) = z \times_* (\alpha^{j_1} \oplus \alpha^{j_2})^{-1}].
\end{aligned}$$

Since π is a random permutation, the value $\pi(i_1)$ is uniformly distributed, and thus $\varepsilon \leq \frac{1}{2^n-1}$. □

We now obtain the classical security of XEX2.

Theorem 4 (Classical security of XEX2 [Rog13]). *Fix $n \geq 1$ and let $\alpha \in \mathbb{F}_{2^n}^*$ be base elements. Fix a block cipher $E : \{0,1\}^m \times \{0,1\}^n \to \{0,1\}^n$. Then*

$$\mathsf{Adv}^{\mathsf{SPRP}}_{\mathsf{XEX2}}(q,t) \leq 2\mathsf{Adv}^{\mathsf{SPRP}}_{E}(q,t) + \frac{q^2}{2^n - 1},$$

where q is the number of queries to XEX2, within a time bound t.

Proof. Immediate by combining Theorem 3, Proposition 3, and Lemma 7. □

The tweakable block cipher XEX2 is employed in the NIST-standardized XTS-AES [P1619], with AES as the underlying block cipher. However, the application-level security goals of XTS remain poorly understood [CSR+08,Rog13]. Another variant, which we denote by XEX, uses a single key ($k = k'$). Discussions on whether to employ a single key or two separate keys are explored in [CSR+08,LM08], with no definitive conclusion reached.

Applications of LRW and XEX2. LRW is implemented as LRW-AES Encryption in earlier drafts of IEEE P1619 [P1606], utilizing AES as the block cipher E and the hash function used is $h_{k'}(\tau) = k' \times_* \tau$, where $\times_*$ represents the group multiplication in $\mathbb{F}_{2^n}^*$. For a single 128-bit block, the block cipher key k is 128, 192, or 256 bits, while the hash key k' is 128 bits. The tweak τ is 128 bits, and E operates on 128-bit (tweakable) blocks.

This LRW-AES was later replaced by XTS-AES in the final IEEE P1619 standard [P1619], with a constraint that the data unit length for any XTS-AES implementation must not exceed 2^{20} AES blocks [Dwo10a]. Initially, LRW was considered slower than XTS due to the full multiplication over $\mathsf{GF}(2^n)$ required for each tweak update, but this is no longer the case [IM19]. The input or output data may consist of multiple 128-bit blocks followed by a partial block of less than 128 bits.

In the XTS-AES Encryption procedure [P1619] for a single 128-bit block, the keys k and k' are either 128 bits or 256 bits. The tweak is represented by i, a 128-bit value, and j, a sequential number of the 128-bit block within the data unit.

5.2 Post-Quantum Security of LRW using the Hybrid Technique

Theorem 5. *Let LRW be as in Definition 7 and let $\mathcal{A}$ be an adversary making q_C classical queries to its first oracle and $q_Q \geq 1$ quantum queries to its second oracle. Assuming h is XOR-universal and uniform, it holds that in the ideal cipher model,*

$$\left| \Pr_{\substack{k \leftarrow \{0,1\}^m; k' \leftarrow \{0,1\}^\kappa \\ E \leftarrow \mathcal{E}(m,n)}} \left[\mathcal{A}^{\pm \mathsf{LRW}_{k,k'}[E__],|\pm E\rangle} = 1 \right] - \Pr_{\substack{\widetilde{\Pi} \leftarrow \mathcal{E}(\mathcal{T},n); \\ E \leftarrow \mathcal{E}(m,n)}} \left[\mathcal{A}^{\pm \widetilde{\Pi},|\pm E\rangle} = 1 \right] \right| \leq \frac{6q_C^2}{2^n} + \frac{4}{2^{(m+n)/2}} \left(q_C \sqrt{q_Q} + q_Q \sqrt{q_C} \right).$$

Proof. The proof follows a procedure similar to that of the post-quantum security proof for FX (Theorem 2). However, in LRW, we introduce bad events related to collisions, defined as $\mathsf{Bad}_j = \mathsf{Bad}_{j,1} \wedge \mathsf{Bad}_{j,2}$, where j indicates the jth stage of the hybrid:

- $\mathsf{Bad}_{j,1}$: A collision occurs in the set $\{x_1 \oplus h_{k'}(\tau_1), \ldots, x_j \oplus h_{k'}(\tau_j)\}$,
- $\mathsf{Bad}_{j,2}$: A collision occurs in the set $\{y_1 \oplus h_{k'}(\tau_1), \ldots, y_j \oplus h_{k'}(\tau_j)\}$.

Using the hybrid technique, we analyze under the condition that these bad events do not occur:

$$\begin{aligned}
&|\Pr[\mathcal{A}(\mathbf{H}_0) = 1] - \Pr[\mathcal{A}(\mathbf{H}_{q_C}) = 1]| \\
&= |\Pr[\mathcal{A}(\mathbf{H}_0) = 1] - \Pr[\mathcal{A}(\mathbf{H}_{q_C}) = 1 \wedge \neg \mathsf{Bad}_{q_C}] - \Pr[\mathcal{A}(\mathbf{H}_{q_C}) = 1 \wedge \mathsf{Bad}_{q_C}]| \\
&\leq |\Pr[\mathcal{A}(\mathbf{H}_0) = 1] - \Pr[\mathcal{A}(\mathbf{H}_{q_C}) = 1 \wedge \neg \mathsf{Bad}_{q_C}]| + \Pr[\mathsf{Bad}_{q_C}] \\
&\leq \sum_{j=0}^{q_C - 1} |\Pr[\mathcal{A}(\mathbf{H}_j) = 1 \wedge \neg \mathsf{Bad}_j] - \Pr[\mathcal{A}(\mathbf{H}_{j+1}) = 1 \wedge \neg \mathsf{Bad}_{j+1}]| + \Pr[\mathsf{Bad}_{q_C}].
\end{aligned}$$

This way to introducing bad events was first employed in [Hos25]. Detailed proof for LRW is in Appendix D. □

5.3 Tightness

We summarize the best-known attacks on standardized LRW and XEX2, with detailed presentations provided in Appendix C:

- Classical Distinguishing Attack: The best-known distinguishing attacks on LRW and XEX2, which aim to differentiate them from a block cipher, exploit either birthday collisions or Even-Mansour-related structures. These attacks generally require only $O(2^{n/2})$ online queries. This matches the $q_C^2 \cdot 2^{-n}$ term in the security bound.
- Classical Complete Key Recovery Attack: Distinguishing attacks are first employed to identify the tweak key, followed by an exhaustive key search for the cipher key. This process requires a total of $O(2^{n/2} + 2^m)$ online queries and $O(2^m)$ offline queries.
- Quantum Complete Key Recovery Attack (shorter cipher key): The offline-Simon attack [BHNP+19] satisfies the trade-off $q_C q_Q^2 = 2^{m+n}$. For block ciphers with shorter key lengths ($m \leq 2n$), this attack, recognized as the best known attack, recovers the secret key using approximately $\widetilde{O}(2^{(m+n)/3})$ online (classical) and $\widetilde{O}(2^{(m+n)/3})$ offline (quantum) queries. Up to poly-logarithmic factors, this aligns with the term $\sqrt{q_C}\, q_Q \cdot 2^{(m+n)/2}$ in our security bound.
- Quantum Complete Key Recovery Attack (longer cipher key): For longer key lengths ($m > 2n$), we can combine Grover's algorithm with the Kuwakado-Morii attack [KM12]. The query complexity is $q_Q = O(2^{m/2+n/3})$ and $q_C = O(2^{n/3})$. Notably, this matches the offline-Simon attack's trade-off, satisfying $q_Q^2 q_C = O(2^{(m+n)/2})$. Alternatively, we can apply Grover's algorithm alone to recover both the cipher key and tweak key, resulting in $q_Q = O(2^{(m+n)/2})$. The choice of attack depends on whether we prioritize minimizing quantum or classical queries. Similarly, it aligns with the term $\sqrt{q_C}\, q_Q \cdot 2^{(m+n)/2}$ in our security bound.

6 Block Cipher Modes

6.1 Definitions

Definition 10 (Distinguishing Advantage). *Let $E : \{0,1\}^m \times \{0,1\}^n \to \{0,1\}^n$ be an efficient, keyed permutation. Consider an adversary $\mathcal{A}$ (which can be either quantum or classical). The advantage of $\mathcal{A}$ in attacking E is measured by*

$$\mathsf{Adv}_E(\mathcal{A}) := \left| \Pr_{k \leftarrow \{0,1\}^m}[\mathcal{A}^{E_k(\cdot), E_k^{-1}(\cdot)} = 1] - \Pr_{P \leftarrow \mathcal{P}_n}[\mathcal{A}^{P(\cdot), P^{-1}(\cdot)} = 1] \right|,$$

where the probabilities are also taken over the randomness of $\mathcal{A}$.

For the rest of the paper, we define $T_{\mathcal{A}}$ as the time an adversary $\mathcal{A}$ spends and $Q_{\mathcal{A}}$ as the number of **classical** queries that $\mathcal{A}$ makes to the oracles.

Definition 11 (SPRP(-PQ) Security). *Let $E : \{0,1\}^m \times \{0,1\}^n \to \{0,1\}^n$ be an efficient keyed permutation. The (PQ) strong pseudorandom permutation security of E is measured by the maximum advantage over all (quantum) adversaries $\mathcal{A}$:*

$$\begin{aligned}\mathsf{Adv}_E^{\mathsf{SPRP(-PQ)}}(q,t) &:= \max_{\substack{\mathcal{A}: T_{\mathcal{A}} \leq t; \\ Q_{\mathcal{A}} \leq q}} \mathsf{Adv}_E(\mathcal{A}) \\ &= \max_{\substack{\mathcal{A}: T_{\mathcal{A}} \leq t; \\ Q_{\mathcal{A}} \leq q}} \left| \Pr_{k \leftarrow \{0,1\}^m}[\mathcal{A}^{E_k(\cdot), E_k^{-1}(\cdot)} = 1] - \Pr_{P \leftarrow \mathcal{P}_n}[\mathcal{A}^{P(\cdot), P^{-1}(\cdot)} = 1] \right|,\end{aligned}$$

where the probabilities are also taken over the randomness of $\mathcal{A}$.

Definition 12 (PRF(-PQ) Security). *Let $E : \{0,1\}^m \times \{0,1\}^* \to \{0,1\}^*$ be an efficient keyed function. The (PQ) pseudorandom function security of E is measured by the maximum advantage over all (quantum) adversaries $\mathcal{A}$:*

$$\mathsf{Adv}_E^{\mathsf{PRF(-PQ)}}(q,t) := \max_{\substack{\mathcal{A}: T_{\mathcal{A}} \leq t; \\ Q_{\mathcal{A}} \leq q}} \left| \Pr_{k \leftarrow \{0,1\}^m}[\mathcal{A}^{E_k(\cdot)} = 1] - \Pr_f[\mathcal{A}^{f(\cdot)} = 1] \right|,$$

where f is chosen uniformly from the set of functions mapping $\{0,1\}^*$ to $\{0,1\}^*$; the probabilities are also taken over the randomness of $\mathcal{A}$.

6.2 PRP-PQ Security of an Ideal Cipher

We consider quantum information-theoretic adversaries that are not constrained by computational resources, such as time or the number of available qubits. The only restriction is on the number of queries that the adversary can make to its oracles.

Definition 13. *Let E be the ideal cipher in the quantum ideal cipher model, and let $\mathcal{A}$ be a quantum adversary. The advantage of $\mathcal{A}$ in attacking E is measured by:*

$$\mathsf{Adv}_E(\mathcal{A}) := \left| \Pr_{k \leftarrow \{0,1\}^m} \left[\mathcal{A}^{E_k(\cdot), E_k^{-1}(\cdot), |E(\cdot,\cdot)\rangle, |E^{-1}(\cdot,\cdot)\rangle} = 1 \right] - \Pr_{P \leftarrow \mathcal{P}_n} \left[\mathcal{A}^{P, P^{-1}, |E\rangle, |E^{-1}\rangle} = 1 \right] \right|.$$

For simplicity of presentation, we sometimes later will omit the inverse oracles when considering SPRP(-PQ)-security. Similarly, SPRP-PQ security of an ideal cipher E is the maximum advantage taken over all possible quantum adversaries $\mathcal{A}$:

$$\mathsf{Adv}_E^{\mathsf{SPRP\text{-}PQ}}(q_1, q_2) := \max_{\substack{\mathcal{A}: Q_{1,\mathcal{A}} \le q_1; \\ Q_{2,\mathcal{A}} \le q_2}} \mathsf{Adv}_E(\mathcal{A}),$$

where $Q_{1,\mathcal{A}}$ and $Q_{2,\mathcal{A}}$ represent the queries that $\mathcal{A}$ makes to $E_k^{\pm}(\cdot)$ and $|E^{\pm}(\cdot,\cdot)\rangle$, respectively.

We emphasize that no block cipher can offer greater security than an ideal cipher. Now we start examining the SPRP-PQ security of an ideal cipher. To establish a bound on the distinguishing probability, we reduce to the UNIQUE-SEARCH problem from the distinguishing problem.

Definition 14. *(UNIQUE-SEARCH$_n$) Given a function $f : \{0,1\}^n \to \{0,1\}$, such that f maps at most one element to 1, output YES if $f^{-1}(1)$ is non-empty and NO otherwise.*

Theorem 6. *Let E be an ideal cipher (in the quantum ideal cipher model) and assume an adversary $\mathcal{A}$ making q_C classical queries to E_k and q_Q quantum queries to E. Then it holds that*

$$\begin{aligned} \mathsf{Adv}_E^{\mathsf{SPRP\text{-}PQ\text{-}IC}}(q_C, q_Q) &= \max_{\mathcal{A}} \left| \Pr_{k \leftarrow \{0,1\}^m} [\mathcal{A}^{E_k, |E\rangle} = 1] - \Pr_{P \leftarrow \mathcal{P}_n} [\mathcal{A}^{P, |E\rangle} = 1] \right| \\ &\le \max_{\mathcal{A}'} \mathsf{Adv}_f^{\mathsf{UNIQUE\text{-}SEARCH}}(\mathcal{A}'). \end{aligned}$$

Proof. Given an adversary $\mathcal{A}$ that attacks E, we now construct an adversary $\mathcal{A}'^{|f\rangle}$ attacking UNIQUE-SEARCH problem:

1. $\mathcal{A}'$ generates a permutation $P \in \mathcal{P}_n$ and an ideal block cipher $E \in \mathcal{E}(m,n)$.
2. $\mathcal{A}'$ then constructs a function E' by querying its own oracle f:

$$E'(k,\tau) = \begin{cases} P(\tau) & \text{if } f(k) = 1 \\ E(k,\tau) & \text{if } f(k) \neq 1 \end{cases}.$$

   $\mathcal{A}'$ subsequently provides $\mathcal{A}$ with classical oracle access to P, P^{-1}, as well as quantum oracle access to E', E'^{-1}. The construction of these quantum oracles is detailed in Section E.
3. $\mathcal{A}'$ outputs what $\mathcal{A}$ outputs.

We now argue that if $\mathcal{A}$ successfully distinguishes between having oracle access to $(P, |E\rangle)$ or $(E_k, |E\rangle)$, then $\mathcal{A}'$ can successfully attack the UNIQUE-SEARCH problem, specifically determining whether f^{-1} is empty or not. We will present our argument by considering the following cases:

YES case. There exists a k^* such that $f(k^*) = 1$, which implies that $E'(k^*, \tau) = P(\tau)$ for any t. From the perspective of $\mathcal{A}$, for this specific k^*, the behavior of the second oracle E' when queried with $(k^*, \cdot)$ matches the behavior of the first oracle P when queried with $(\cdot)$. This situation is equivalent to what $\mathcal{A}$ expects to observe in the interaction with the oracles $(E_k, |E\rangle)$, i.e. $\mathcal{A}^{E_k, |E\rangle}$.

NO case. There does not exist any k such that $f(k) = 1$, which implies that for all k and any τ, we have $E'(k,\tau) = E(k,\tau)$. Consequently, from the perspective of $\mathcal{A}$, the interaction with the oracles $(P, |E'\rangle)$ is just $(P, |E\rangle)$, which gives $\mathcal{A}^{P, |E\rangle}$.

Therefore, if $\mathcal{A}$ can distinguish the real world $\left(\mathcal{A}^{E_k,|E\rangle}\right)$ and the ideal world $\left(\mathcal{A}^{P,|E\rangle}\right)$, then $\mathcal{A}'$ can distinguish YES and NO case in UNIQUE-SEARCH:

$$\mathsf{Adv}_f^{\text{UNIQUE-SEARCH}}(\mathcal{A}') \geq \mathsf{Adv}_E(\mathcal{A}).$$

We note that the number of queries $\mathcal{A}'$ makes to f is determined only by q_Q, as specified by the construction of E'. □

The UNIQUE-SEARCH bound against quantum adversaries [BBBV97] yields:

Corollary 2. *Let E be an ideal cipher (in QICM) and assume an adversary $\mathcal{A}$ making q_C queries to E_k and q_Q **quantum** queries to E. Then it holds that*

$$\mathit{Adv}_E^{\mathit{SPRP\text{-}PQ\text{-}IC}}(q_C, q_Q) \leq \frac{q_Q^2}{2^m}.$$

We note that the bound is optimal, and Grover's search is the matching algorithm, which involves querying E $2^{m/2}$ times to find the key. It is evident from the bound that only q_Q, i.e., the number of queries to E, is involved. This implies that the security lower bound stays the same in the Q2 model, in which the adversary can query both of its oracles quantumly.

6.3 Security of Block Cipher Modes

General Theorem Construction Con. We begin by defining a polynomial-time algorithm, denoted as Con, which uses a (black-box) permutation as input to produce a specific construction. This permutation can take on different forms: when the construction is instantiated with a specific block cipher E, we denote it as $\mathsf{Con}[E_]$. Then with a key $k \leftarrow \{0,1\}^m$ is uniformly sampled first, E_k then serves as the (black-box) permutation, denoted as $\mathsf{Con}[E_k]$. For Con that is invertible, we denote its inverse as DeCon and with different underlying permutations, it is denoted as $\mathsf{DeCon}\left[E_k^{-1}\right]$ and $\mathsf{DeCon}\left[P^{-1}\right]$.

To illustrate, consider Con as the CBC-MAC construction. When the permutation is instantiated with a block cipher E, the construction first samples a uniformly random key $k \leftarrow \{0,1\}^m$ and uses it as the block cipher key for E, which gives $\mathsf{Con}[E_k] = \mathsf{CBC\text{-}MAC}[E_k]$. The output of this construction is given by:

$$\mathsf{CBC\text{-}MAC}[E_k](x_1, \ldots, x_\ell) = E_k(E_k(\ldots E_k(E_k(x_1) \oplus x_2) \oplus \ldots) \oplus x_\ell).$$

Alternatively, when the permutation-like oracle is instantiated as a true random permutation P, the construction is denoted by $\mathsf{Con}[P] = \mathsf{CBC\text{-}MAC}[P]$. In this scenario, the block cipher E_k is replaced entirely by the permutation P within the construction, resulting in the following definition:

$$\mathsf{CBC\text{-}MAC}[P](x_1, \ldots, x_\ell) = P(P(\ldots P(P(x_1) \oplus x_2) \oplus \ldots) \oplus x_\ell).$$

Experiment Exp. The security of a cryptographic scheme Con is typically analyzed through a well-defined probabilistic experiment, denoted as Exp. This experiment captures the interaction between an adversary $\mathcal{A}$ and a challenger, modeled as a classical polynomial-time algorithm. The challenger has access to certain resources, such as a black-box permutation oracle, which it can query as needed during the experiment. The goal of the adversary $\mathcal{A}$ is to exploit these interactions and the oracle queries to either compromise a specific security property of Con or extract secret information. The experiment $\mathsf{Exp}(\mathcal{A})$ proceeds as follows:

1. **Initialization and Oracle Access**: The challenger Chall is possible to be given access to one or more oracles, such as black-box permutation oracles, which it may use to process information or respond to the adversary's queries. Chall may also grant the adversary direct access to some oracles under predefined rules. Con can also obtain oracle access to these oracles. We assume that the number of queries to these oracles only depends on the number of queries the adversary makes to the construction Con.
2. **Interaction with the Adversary**: The challenger Chall and the adversary $\mathcal{A}$ engage in a protocol where information is exchanged. The adversary may send queries or responses to the challenger, aiming to gather information or manipulate the interaction to achieve its goals. The interaction is always classical.

3. **Output of the Experiment**: After a sequence of interactions and oracle queries, the challenger outputs a single bit $b \in \{0,1\}$. This bit represents the outcome of the experiment, where its distribution reflects the adversary's success in breaking the scheme Con or achieving a specific objective.

The success of the adversary $\mathcal{A}$ is quantified by the probability that it achieves a favorable outcome in Exp. This is measured in terms of the adversary's **advantage**, denoted as $\mathsf{Adv}^{\mathsf{Exp}}_{\mathsf{Con}}(\mathcal{A})$. The advantage reflects the extent to which the adversary outperforms random guessing in achieving its goals. Finally, the security of the scheme Con is determined by evaluating the maximum advantage achievable by any adversary $\mathcal{A}$. This is expressed as:

$$\mathsf{Adv}^{\mathsf{Exp}}_{\mathsf{Con}}(\cdot) = \max_{\mathcal{A}} \mathsf{Adv}^{\mathsf{Exp}}_{\mathsf{Con}}(\mathcal{A}).$$

Here are some example experiments. The PRF experiment is a standard framework to evaluate the pseudorandom function PRF security of a construction Con. This experiment proceeds as follows:

1. **Initialization and Oracle Access**: The challenger initializes the experiment by setting up the construction $\mathsf{Con}_k(\cdot)$, where $k \in \{0,1\}^\kappa$ is a secret key sampled uniformly at random. A bit $d \xleftarrow{\$} \{0,1\}$ is sampled uniformly at random. This bit determines the behavior of the oracle provided to the adversary $\mathcal{A}$:
   - If $d = 0$, the challenger grants $\mathcal{A}$ access to the oracle implementing the function $\mathsf{Con}_k(\cdot)$.
   - If $d = 1$, for each query m from $\mathcal{A}$, the challenger responds with a value $y \xleftarrow{\$} \mathcal{Y}$ sampled uniformly at random from the output range $\mathcal{Y}$, independent of m, mimicking a random oracle.
2. **Interaction with the Adversary**: The adversary $\mathcal{A}$ is allowed to interact with the oracle provided by the challenger. It may issue a sequence of queries m and receive corresponding responses, either from $\mathsf{Con}_k(\cdot)$ (if $d = 0$) or the random oracle (if $d = 1$).
3. **Output of the Experiment**: After a sequence of interactions, $\mathcal{A}$ outputs a bit d', representing its guess about whether the oracle is $\mathsf{Con}_k(\cdot)$ ($d = 0$) or a random oracle ($d = 1$). The challenger then computes the output of the experiment as a bit $b = \overline{d \oplus d'}$, where $b = 1$ indicates that $\mathcal{A}$ correctly distinguished the oracle type and $b = 0$ indicates that $\mathcal{A}$ guessed incorrectly.

The adversary's goal is to maximize the probability of outputting the correct guess, $d' = d$, thus making $b = 1$. The PRF security of the construction Con is defined as the maximum distinguishing advantage over all adversaries $\mathcal{A}$ running within the given resource constraints (q), denoted as $\mathsf{Adv}^{\mathsf{PRF}}_{\mathsf{Con}}(q)$.

The distinguishing advantage of the adversary $\mathcal{A}$ in the PRF experiment is defined as:

$$\mathsf{Adv}^{\mathsf{PRF}}_{\mathsf{Con}}(\mathcal{A}) = \left| \Pr[b = 1] - \frac{1}{2} \right|.$$

The PRF security of the construction Con is then defined as the maximum distinguishing advantage over all adversaries $\mathcal{A}$ running within the given resource constraints (q, t):

$$\mathsf{Adv}^{\mathsf{PRF}}_{\mathsf{Con}}(q, t) = \max_{\mathcal{A}} \mathsf{Adv}^{\mathsf{PRF}}_{\mathsf{Con}}(\mathcal{A}).$$

Consider another example, the $\mathsf{Forgery}$ experiment. The $\mathsf{Forgery}$ experiment evaluates the unforgeability of a construction Con, demonstrating that Con is a MAC (Message Authentication Code). It is structured as follows:

1. **Initialization and Oracle Access**: The challenger initializes the experiment by setting up the construction $\mathsf{Con}_k(\cdot)$, where $k \in \{0,1\}^\kappa$ is a secret key sampled uniformly at random. The oracle $\mathsf{Con}_k(\cdot)$ is made available to the adversary $\mathcal{A}$.
2. **Interaction with the Adversary**: The adversary $\mathcal{A}$ interacts with the oracle $\mathsf{Con}_k(\cdot)$. On a query m, the oracle computes the tag $\mathsf{tag} = \mathsf{Con}_k(m)$ and returns tag to $\mathcal{A}$.
3. **Output of the Experiment**: After a sequence of interactions, $\mathcal{A}$ outputs a pair (m, tag). Let $\mathcal{Q}$ denote the set of all queries that $\mathcal{A}$ asked its oracle. The challenger outputs $b = 1$ if and only if $\mathsf{Con}_k(m) = \mathsf{tag}$ and $m \notin \mathcal{Q}$, the adversary produces a valid tag for a message m that it has not queried during the interaction. Otherwise, the challenger outputs 0.

The adversary's goal is to maximize the probability of producing a valid, unqueried message-tag pair (m, tag) such that the experiment outputs 1. The unforgeability of the construction Con is quantified by the adversary's advantage:

$$\mathsf{Adv}^{\mathsf{Forgery}}_{\mathsf{Con}}(\mathcal{A}) = \Pr[b = 1].$$

The unforgeability of Con is then defined as the maximum advantage over all adversaries $\mathcal{A}$ constrained by a certain number of queries q and time t:

$$\mathsf{Adv}^{\mathsf{Forgery}}_{\mathsf{Con}}(q, t) = \max_{\mathcal{A}} \mathsf{Adv}^{\mathsf{Forgery}}_{\mathsf{Con}}(\mathcal{A}).$$

For $\mathsf{Forgery}$ experiment with decryption oracle access, denoted as $\mathsf{Forgery}\pm$, it is structured as follows for a construction Con:

1. **Initialization and Oracle Access**: The challenger Chall initializes the experiment by setting up the construction $\mathsf{Con}_k(\cdot)$ and $\mathsf{DeCon}_k(\cdot)$, where $k \in \{0,1\}^\kappa$ is a secret key sampled uniformly at random. Both oracles are made available to the adversary $\mathcal{A}$.
2. **Interaction with the Adversary**: The adversary $\mathcal{A}$ interacts with the oracle $\mathsf{Con}_k(\cdot)$ and $\mathsf{DeCon}_k(\cdot)$. When $\mathsf{Con}_k(\cdot)$ is queried on a query m, the oracle computes the tag $\mathsf{tag} = \mathsf{Con}_k(m)$ and returns t to $\mathcal{A}$. When $\mathsf{DeCon}_k(\cdot)$ is queried on a query t, the oracle computes the tag $m = \mathsf{DeCon}_k(t)$ and returns m to $\mathcal{A}$.
3. **Output of the Experiment**: Same as in $\mathsf{Forgery}$ experiment.

General Theorem. We now focus on a collection of constructions whose security is analyzed in a typical reduction-based approach. The classical security of the construction $\mathsf{Con}[E__]$, for a particular block cipher E in a specific experiment Exp, is established through the following steps:

1. **Reduction to the Block Cipher SPRP Security:** Replace the block cipher E_k with a truly random permutation $P \xleftarrow{\$} \mathcal{P}_n$, incurring a loss equivalent to the SPRP security of E.
2. **Information-Theoretic Security of $\mathsf{Con}[\mathsf{P}]$:** When E is replaced by P, it can be shown that the construction $\mathsf{Con}[P]$ achieves a certain level of security in an information-theoretic sense. This means that the security is determined solely by the number of queries q made to the construction oracle $\mathsf{Con}[P]$ and its inverse, independent of the adversary's computational power.

Therefore, the final security of $\mathsf{Con}[E__]$ in a given experiment Exp against a classical probabilistic adversary making q queries in time t is given by:

$$\mathsf{Adv}^{\mathsf{Exp}}_{\mathsf{Con}[E__]}(q, t) \leq \mathsf{Adv}^{\mathsf{SPRP}}_{E}(q', t) + \delta(q),$$

Here, $q' = f(q)$, a function of q, represents the number of queries made by Con and Chall to $E__(\cdot)$. Additionally, t denotes the computational resources required for the reduction to the security of the underlying block cipher.

This approach combines the underlying computational security of the block cipher E and the inherent information-theoretic security of the construction when using a random permutation P. When Con is instantiated with a specific block cipher E, we can extend the classical security analysis of Con in a given experiment Exp to establish its post-quantum security in the same experiment Exp as follows:

Theorem 7. *Let Exp be a security experiment, and let Con be a construction as defined above, instantiated with a block cipher E. Then the post-quantum security of Con is bounded as follows:*

$$\mathsf{Adv}^{\mathsf{Exp\text{-}PQ}}_{\mathsf{Con}[E__]}(q, t) \leq \mathsf{Adv}^{\mathsf{SPRP\text{-}PQ}}_{E}(q', t) + \delta(q),$$

where q is the number of queries made to the keyed construction and its inverses, $\mathsf{Con}[E_k](\cdot)$ and $\mathsf{DeCon}\left[E_k^{-1}\right](\cdot)$; $q' = f(q)$ represents the number of queries made by Con and the challenger Chall to $E__(\cdot)$; t denote the time resources available to quantum adversaries in the experiments Exp. $\delta(q)$ is the classical-model information-theoretic security of Con instantiated with an ideal block cipher.

Proof. Suppose $\mathcal{A}$ is a quantum adversary attacking $\mathsf{Con}[E__]$ in a specified experiment Exp. The corresponding security is:

$$\begin{aligned}\mathsf{Adv}^{\mathsf{Exp\text{-}PQ}}_{\mathsf{Con}[E__]}(q,t) &= \max_{\mathcal{A}} \mathsf{Adv}^{\mathsf{Exp\text{-}PQ}}_{\mathsf{Con}[E__]}(\mathcal{A}) \\ &= \max_{\mathcal{A}} \left| \Pr_{k\leftarrow\{0,1\}^m}\left[\mathsf{Exp}\left(\mathcal{A}^{\mathsf{Con}[E_k],\mathsf{DeCon}\left[E_k^{-1}\right]}\right)=1\right] - \Pr_{P\leftarrow\mathcal{P}_n}\left[\mathsf{Exp}\left(\mathcal{A}^{P,P^{-1}}\right)=1\right]\right|.\end{aligned}$$

We then consider a special class of quantum adversaries, denoted as $\mathcal{B}$. As defined in Definition 10, $\mathcal{B}$ has classical oracle access to $\mathcal{O}$ and $\mathcal{O}^{-1}$, where $\mathcal{O}$ represents either $E_k(\cdot)$ or $P(\cdot)$. The goal of $\mathcal{B}$ is to simulate a complete interaction between a specific adversary $\mathcal{A}$ and the challenger in the experiment Exp as follows:

1. **Construct Oracles:** $\mathcal{B}$ constructs the oracles $\mathsf{Con}[\mathcal{O}]$ and $\mathsf{DeCon}\left[\mathcal{O}^{-1}\right]$ based on its own access to $\mathcal{O}$ and $\mathcal{O}^{-1}$.
2. **Simulate Interaction:** $\mathcal{B}$ invokes the specific adversary $\mathcal{A}$ and runs it in the experiment Exp while acting as the challenger; $\mathcal{B}$ also provides $\mathcal{A}$ with the constructed oracles $\mathsf{Con}[\mathcal{O}]$ and $\mathsf{DeCon}\left[\mathcal{O}^{-1}\right]$ when necessary.
3. **Output Result:** $\mathcal{B}$ outputs a bit: 1 if $\mathcal{A}$ succeeds in the experiment Exp, and 0 otherwise.

We note that for certain specific experiments Exp, where the adversary $\mathcal{A}$ is tasked with distinguishing whether the construction is based on E or P, in the final step, $\mathcal{B}$ simply outputs whatever $\mathcal{A}$ outputs. From the reduction, it is clear that

$$\begin{aligned}\mathsf{Adv}_E(\mathcal{B}) &= \left| \Pr_{k\leftarrow\{0,1\}^m}\left[\mathcal{B}^{E_k(\cdot),E_k^{-1}(\cdot)}=1\right] - \Pr_{P\leftarrow\mathcal{P}_n}\left[\mathcal{B}^{P(\cdot),P^{-1}(\cdot)}=1\right]\right| \\ &\geq \left| \Pr_{k\leftarrow\{0,1\}^m}\left[\mathsf{Exp}\left(\mathcal{A}^{\mathsf{Con}[E_k],\mathsf{DeCon}\left[E_k^{-1}\right]}\right)=1\right] - \Pr_{k\leftarrow\{0,1\}^m}\left[\mathsf{Exp}\left(\mathcal{A}^{\mathsf{Con}[P],\mathsf{DeCon}\left[P^{-1}\right]}\right)=1\right]\right|.\end{aligned} \tag{26}$$

We also note that after replacing E_k with P, the distinguishing advantage of $\mathcal{A}$ attacking $\mathsf{Con}[E_k]$ with classical oracle access is given by

$$\left| \Pr_{k\leftarrow\{0,1\}^m}\left[\mathsf{Exp}\left(\mathcal{A}^{\mathsf{Con}[P],\mathsf{DeCon}\left[P^{-1}\right]}\right)=1\right] - \Pr_{P\leftarrow\mathcal{P}_n}\left[\mathsf{Exp}\left(\mathcal{A}^{P,P^{-1}}\right)=1\right]\right| \leq \delta(q), \tag{27}$$

which is information-theoretic. This indicates that even if $\mathcal{A}$ possesses local quantum capabilities, as long as it has only classical oracle access, the distinguishing advantage remains bounded by $\delta(q)$.

By combining the above three equations, we obtain:

$$\begin{aligned}&\mathsf{Adv}^{\mathsf{Exp\text{-}PQ}}_{\mathsf{Con}[E__]}(\mathcal{A}) \\ &\leq \left| \Pr_{k\leftarrow\{0,1\}^m}\left[\mathsf{Exp}\left(\mathcal{A}^{\mathsf{Con}[E_k],\mathsf{DeCon}\left[E_k^{-1}\right]}\right)=1\right] - \Pr_{k\leftarrow\{0,1\}^m}\left[\mathsf{Exp}\left(\mathcal{A}^{\mathsf{Con}[P],\mathsf{DeCon}\left[P^{-1}\right]}\right)=1\right]\right| \\ &\quad + \left| \Pr_{k\leftarrow\{0,1\}^m}\left[\mathsf{Exp}\left(\mathcal{A}^{\mathsf{Con}[P],\mathsf{DeCon}\left[P^{-1}\right]}\right)=1\right] - \Pr_{P\leftarrow\mathcal{P}_n}\left[\mathsf{Exp}\left(\mathcal{A}^{P,P^{-1}}\right)=1\right]\right| \\ &\leq \mathsf{Adv}_E(\mathcal{B}) + \delta(q).\end{aligned} \tag{28}$$

By taking the maximum over adversaries $\mathcal{A}$, which is equivalent to taking the maximum over adversaries $\mathcal{B}$, it follows that:

$$\begin{aligned}\mathsf{Adv}^{\mathsf{Exp\text{-}PQ}}_{\mathsf{Con}[E__]}(q,t) &\leq \max_{\mathcal{B}} \mathsf{Adv}_E(\mathcal{B}) + \delta(q) \\ &= \mathsf{Adv}^{\mathsf{SPRP\text{-}PQ}}_E(q',t) + \delta(q).\end{aligned}$$

□

Remark. The current statement applies directly only to constructions Con based on a block cipher E with a single key. For constructions where E uses multiple (say c) independently sampled keys, the argument can be extended with minor modifications:

$$\mathsf{Adv}^{\mathsf{Exp}}_{\mathsf{Con}[E__]}(q,t) \leq c\cdot\mathsf{Adv}^{\mathsf{SPRP}}_E(q',t) + \delta(q) \Longrightarrow \mathsf{Adv}^{\mathsf{Exp\text{-}PQ}}_{\mathsf{Con}[E__]}(q,t) \leq c\cdot\mathsf{Adv}^{\mathsf{SPRP\text{-}PQ}}_E(q',t) + \delta(q).$$

We also examine the security of $\mathsf{Con}[E__]$ in the QICM. As discussed in Section 3, in this model, E is treated as an ideal cipher, and $\mathsf{Con}[E__]$ is constructed using such E. Unlike the previous version, here, the challenger Chall and Con are only granted **classical** oracle access to the *ideal cipher* $E(\cdot,\cdot)$, rather than access to the full scripts as in the previous version. The number of queries they make is recorded as q'_C. The adversary $\mathcal{A}$, however, is granted **quantum** oracle access to $E(\cdot,\cdot)$, recorded as q_Q, in addition to **classical** oracle access to $\mathsf{Con}[E_k]$ and $\mathsf{DeCon}\left[E_k^{-1}\right]$, recorded as q_C. It is important to note that, in this model, we consider adversaries with unbounded computational power. Thus, we are effectively analyzing the security of $\mathsf{Con}[E__]$ in the post-quantum model.

Theorem 8. *Let Exp be a security experiment, and let Con be a construction as defined before. Then the post-quantum security of $\mathsf{Con}[E__]$ in the ideal cipher model is given by:*

$$\begin{aligned}\mathsf{Adv}^{\mathsf{Exp\text{-}PQ\text{-}IC}}_{\mathsf{Con}[E__]}(q_C,q_Q) &\le \mathsf{Adv}^{\mathsf{SPRP\text{-}PQ\text{-}IC}}_{E}(q'_C,q_Q)+\delta(q_C)\\ &= \frac{q_Q^2}{2^n}+\delta(q_C)\end{aligned}$$

where q_C, q'_C and q_Q is defined as above; t denote the time resources available to quantum adversaries in the experiments Exp. $\delta(q_C)$ is the classical-model info-theoretic security of Con instantiated with an ideal block cipher.

Proof. Suppose $\mathcal{A}$ is a quantum adversary attacking $\mathsf{Con}[E__]$ in a specified experiment Exp in the quantum ideal cipher model. The corresponding security is:

$$\begin{aligned}&\mathsf{Adv}_{\mathsf{Con}[E__]}(q_C,q_Q)\\ &=\max_{\mathcal{A}}\left|\Pr_{\substack{k\leftarrow\{0,1\}^m\\ E\leftarrow\mathcal{E}(m,n)}}\left[\mathsf{Exp}\left(\mathcal{A}^{\mathsf{Con}[E_k],\mathsf{DeCon}\left[E_k^{-1}\right],E}\right)=1\right]-\Pr_{\substack{P\leftarrow\mathcal{P}_n\\ E\leftarrow\mathcal{E}(m,n)}}\left[\mathsf{Exp}\left(\mathcal{A}^{P,P^{-1},E}\right)=1\right]\right|.\end{aligned}$$

We note that the presence of an additional oracle $E(\cdot,\cdot)$ does not affect the validity of Equation 26. Additionally, Equation 27 also remains valid in the presence of the extra oracle E, as the oracles $\mathsf{Con}[P]$, $\mathsf{DeCon}\left[P^{-1}\right]$, P, P^{-1} operate independently from E:

$$\begin{aligned}\Pr_{\substack{k\leftarrow\{0,1\}^m\\ E\leftarrow\mathcal{E}(m,n)}}\left[\mathsf{Exp}\left(\mathcal{A}^{\mathsf{Con}[P],\mathsf{DeCon}\left[P^{-1}\right],E}\right)=1\right] &= \Pr_{k\leftarrow\{0,1\}^m}\left[\mathsf{Exp}\left(\mathcal{A}^{\mathsf{Con}[P],\mathsf{DeCon}\left[P^{-1}\right]}\right)=1\right]\\ \Pr_{\substack{P\leftarrow\mathcal{P}_n\\ E\leftarrow\mathcal{E}(m,n)}}\left[\mathsf{Exp}\left(\mathcal{A}^{P,P^{-1},E}\right)=1\right] &= \Pr_{P\leftarrow\mathcal{P}_n}\left[\mathsf{Exp}\left(\mathcal{A}^{P,P^{-1}}\right)=1\right].\end{aligned}$$

Therefore Equation 28 holds in the quantum ideal cipher model. Then combining with the security of the ideal cipher in the quantum ideal cipher model as stated in Theorem 2:

$$\begin{aligned}\mathsf{Adv}^{\mathsf{Exp\text{-}PQ\text{-}IC}}_{\mathsf{Con}[E__]}(q_C,q_Q) &= \mathsf{Adv}^{\mathsf{SPRP\text{-}PQ\text{-}IC}}_{E}(q'_C,q_Q)+\delta(q_C)\\ &\le \frac{q_Q^2}{2^n}+\delta(q_C).\end{aligned}$$

□

The theorem also applies to constructions Con whose classical security can be reduced to the block cipher's PRP security. This yields the following bound:

$$\mathsf{Adv}^{\mathsf{Exp\text{-}PQ}}_{\mathsf{Con}[E__]}(q,t)\le\mathsf{Adv}^{\mathsf{PRP\text{-}PQ}}_{E}(q',t')+\delta(q).$$

Similarly, in QICM, we can derive:

$$\mathsf{Adv}^{\mathsf{Exp\text{-}PQ\text{-}IC}}_{\mathsf{Con}[E__]}(q_Q,q_C)\le\frac{q_Q^2}{2^n}+\delta(q_C).$$

Applications of Theorem 7 and Theorem 8. Let m and n be positive integers. Let $E : \{0,1\}^m \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher. A summary is provided in Appendix F.

CBC [EMST78].

- Construction: $\mathsf{Con}[E_k] = \mathsf{CBC}^E_k(x_1, \ldots, x_\ell) = E_k(E_k(\ldots E_k(E_k(x_1) \oplus x_2) \oplus \ldots) \oplus x_\ell)$
- Classical security [KL07]: For all probabilistic adversaries $\mathcal{A}$, it holds that:

$$\begin{aligned}\mathsf{Adv}^{\mathsf{PRF}}_{\mathsf{CBC}}(q,t) &:= \max_{\mathcal{A}} \left| \Pr_{k \leftarrow \{0,1\}^m}[\mathcal{A}^{\mathsf{CBC}[E_k]} = 1] - \Pr_f[\mathcal{A}^f = 1] \right| \\ &\leq \mathsf{Adv}^{\mathsf{PRP}}_E(q\ell, t) + \frac{q^2\ell^2}{2^n},\end{aligned}$$

  where f is chosen uniformly from the set of functions mapping $(\{0,1\}^n)^\ell$ to $\{0,1\}^n$, q is the number of queries to CBC, t is the time complexity and ℓ is the number of blocks of the longest query input.
- Post-quantum security: The post-quantum security of a construction based on another concrete block cipher, such as AES, in the PQ model is closely related to its classical security since no second oracle is available to the adversary. The equivalence holds with $\mathsf{Adv}^{\mathsf{PRF}}_E$ replaced by $\mathsf{Adv}^{\mathsf{PRP\text{-}PQ}}_E$ as stated in Theorem 7:

$$\mathsf{Adv}^{\mathsf{PRF\text{-}PQ}}_{\mathsf{CBC}}(q,t) \leq \mathsf{Adv}^{\mathsf{PRP\text{-}PQ}}_E(q\ell, t) + \frac{q^2\ell^2}{2^n}.$$

- Post-quantum security in QICM: By applying Theorem 8, we get

$$\begin{aligned}\mathsf{Adv}^{\mathsf{PRF\text{-}PQ\text{-}IC}}_{\mathsf{CBC}}(q_C, q_Q) &= \max_{\mathcal{A}} \left| \Pr_{k \leftarrow \{0,1\}^m}\left[\mathcal{A}^{\mathsf{CBC}[E_k],E} = 1\right] - \Pr_f\left[\mathcal{A}^{P,E} = 1\right] \right| \\ &\leq \frac{q_Q^2\ell^2}{2^m} + \frac{q_C^2\ell^2}{2^n}.\end{aligned}$$

Similarly as explained in [KL07], when the tag is set to be $\mathsf{CBC}_k(m)$, this is exactly CBC -MAC, and post-quantum security of CBC implies that basic CBC -MAC is post-quantum secure for messages of any fixed length. However, it is not inherently secure for variable-length messages. To address this limitation, *encrypt-last-block* offers a method to extend CBC -MAC for use with variable-length inputs. It is formally called Encrypt-last-block CBC-MAC, i.e., ECBC -MAC.

ECBC [PR00].

- Construction: $\mathsf{Con}[E_k](x) = \mathsf{ECBC}^E_{k_1,k_2}(x) = E_{k_2}(\mathsf{CBC}^E_{k_1}(x))$
- Classical security [PR00,Vau00]: For all probabilistic adversaries $\mathcal{A}$, it holds that:

$$\begin{aligned}\mathsf{Adv}^{\mathsf{PRF}}_{\mathsf{ECBC}}(q,t) &:= \max_{\mathcal{A}} \left| \Pr_{k \leftarrow \{0,1\}^m}[\mathcal{A}^{\mathsf{ECBC}[E_k]} = 1] - \Pr_f[\mathcal{A}^f = 1] \right| \\ &\leq 2\mathsf{Adv}^{\mathsf{PRP}}_E(q\ell, t) + \frac{4q^2\ell^2}{2^n}.\end{aligned}$$

  where f is chosen uniformly from the set of functions mapping $(\{0,1\}^n)^\ell$ to $\{0,1\}^n$, q is the number of queries to CBC, t is the time complexity and ℓ is the number of blocks of the longest query input.
- Post-quantum security: By applying Theorem 7, we get

$$\mathsf{Adv}^{\mathsf{PRF\text{-}PQ}}_{\mathsf{CBC}}(q,t) \leq 2\mathsf{Adv}^{\mathsf{PRP\text{-}PQ}}_E(q\ell, t) + \frac{4q^2\ell^2}{2^n}.$$

- Post-quantum security in QICM: By applying Theorem 8, we get

$$\begin{aligned}\mathsf{Adv}^{\mathsf{PRF\text{-}PQ\text{-}IC}}_{\mathsf{CBC}}(q_C, q_Q) &= \max_{\mathcal{A}} \left| \Pr_{k \leftarrow \{0,1\}^m}\left[\mathcal{A}^{\mathsf{CBC}[E_k],E} = 1\right] - \Pr_f\left[\mathcal{A}^{P,E} = 1\right] \right| \\ &\leq \frac{2q_Q^2\ell^2}{2^m} + \frac{4q_C^2\ell^2}{2^n}.\end{aligned}$$

CMAC [IK03].

– Construction: $\mathsf{Con}[E_k](x) = \mathsf{CMAC}^E_k(x) = E_{k_1}(\mathsf{CBC}^E_{k_1}(x_1\|\ldots\|x_{\ell-1}) \oplus x_\ell \oplus k_2)$
– Classical security [IK03]: For all probabilistic adversaries $\mathcal{A}$, it holds that:

$$\mathsf{Adv}^{\mathsf{Forgery}}_{\mathsf{CMAC}}(q,t) \leq \mathsf{Adv}^{\mathsf{PRP}}_E(q\ell+1, t+O(q\ell)) + \frac{5(\ell^2+1)q^2}{2^n}.$$

where q is the number of queries in the Forgery experiment, t is the time complexity and ℓ is the number of blocks of the longest query input.
– Post-quantum security: By applying Theorem 7, we get

$$\mathsf{Adv}^{\mathsf{Forgery\text{-}PQ}}_{\mathsf{CMAC}}(q,t) \leq \mathsf{Adv}^{\mathsf{PRP\text{-}PQ}}_E(q\ell+1, t+O(q\ell)) + \frac{5(\ell^2+1)q^2}{2^n}.$$

– Post-quantum security in QICM: By applying Theorem 8, we get

$$\mathsf{Adv}^{\mathsf{Forgery\text{-}PQ\text{-}IC}}_{\mathsf{CMAC}}(q_C,q_Q) \leq \frac{(q_Q\ell+1)^2}{2^m} + \frac{5(\ell^2+1)q^2}{2^n}.$$

GCM [MV04].

– Classical security [MV04,IOM12,NOMI15]: We begin by noting that the oracle in the Forgery experiment for GCM also includes a decryption oracle, denoted as GCM±. For all probabilistic adversaries $\mathcal{A}$, it holds:

$$\mathsf{Adv}^{\mathsf{PRF}}_{\mathsf{GCM}}(q,t) \leq \mathsf{Adv}^{\mathsf{PRP}}_E(q,t) + \frac{(\sigma+q+1)^2}{2^{n+1}} + \frac{\sigma+q}{2^{n-1}}$$
$$\mathsf{Adv}^{\pm\mathsf{Forgery}}_{\mathsf{GCM}}(q,t) \leq \mathsf{Adv}^{\mathsf{PRP}}_E(q,t) + \frac{(\sigma+q+q'+1)^2}{2^{n+1}} + \frac{\sigma+q+q'}{2^{n-1}} + \frac{q'(\ell+1)}{2^s}.$$

where q, q' are the number of queries made to the encryption and decryption oracles, respectively; t is the time complexity and s is the authentication tag size. Additionally ℓ is the maximum number of blocks in the input-data for any individual query, and σ is the total number of blocks of input-data across all queries.
From [Rog02], an AEAD-scheme Π is said to be "secure" if $\mathsf{Adv}^{\mathsf{PRF}}_\Pi$ and $\mathsf{Adv}^{\mathsf{Forgery}}_\Pi$ are "small" for any "reasonable" adversary $\mathcal{A}$. GCM is a widely used secure AEAD-scheme.
– Post-quantum security: By applying Theorem 7, we get

$$\mathsf{Adv}^{\mathsf{PRF\text{-}PQ}}_{\mathsf{GCM}}(q,t) \leq \mathsf{Adv}^{\mathsf{PRP\text{-}PQ}}_E(q,t) + \frac{(\sigma+q+1)^2}{2^{n+1}} + \frac{\sigma+q}{2^{n-1}}$$
$$\mathsf{Adv}^{\pm\mathsf{Forgery\text{-}PQ}}_{\mathsf{GCM}}(q,t) \leq \mathsf{Adv}^{\mathsf{PRP\text{-}PQ}}_E(q,t) + \frac{(\sigma+q+q'+1)^2}{2^{n+1}} + \frac{\sigma+q+q'}{2^{n-1}} + \frac{q'(\ell+1)}{2^s}.$$

– Post-quantum security in QICM: By applying Theorem 8, we get

$$\mathsf{Adv}^{\mathsf{PRF\text{-}PQ\text{-}IC}}_{\mathsf{GCM}}(q_C,q_Q) \leq \frac{q_Q^2\ell^2}{2^m} + \frac{(\sigma+q_C+1)^2}{2^{n+1}} + \frac{\sigma+q_C}{2^{n-1}}$$
$$\mathsf{Adv}^{\pm\mathsf{Forgery\text{-}PQ\text{-}IC}}_{\mathsf{GCM}}(q_C,q_Q) \leq \frac{q_Q^2\ell^2}{2^m} + \frac{(\sigma+q_C+q'_C+1)^2}{2^{n+1}} + \frac{\sigma+q_C+q'_C}{2^{n-1}} + \frac{q'_C(\ell+1)}{2^s}.$$

GCM-SST [CMM23,IJMM24]. When analyzing security of GCM-SST, the experiment considers Nonce-Misuse Resilience for both privacy and authenticity, denoted as nml-PRF and nml-Forgery, respectively. The nml security notions give stronger notions of security, where GCM fails to meet the requirements, but GCM-SST satisfies them.

– Classical security [IJMM24]: For all probabilistic adversaries $\mathcal{A}$, it holds that:

$$\mathsf{Adv}^{\mathsf{nml\text{-}PRF}}_{\mathsf{GCM}}(q,t) \leq \mathsf{Adv}^{\mathsf{PRP}}_E(q,t) + \frac{(\sigma+3q)^2}{2^{n+1}}$$
$$\mathsf{Adv}^{\mathsf{nml\text{-}Forgery}}_{\mathsf{GCM}}(q,t) \leq \mathsf{Adv}^{\mathsf{PRP}}_E(q,t) + \frac{(\sigma+3(q+q'))^2}{2^{n+1}} + \frac{q'\ell}{2^n} + \frac{q'}{2^s}.$$

where q, q' are the number of queries made to the encryption and decryption oracles, respectively; t is the time complexity and s is the authentication tag size. Additionally ℓ is the maximum number of blocks in the input-data for any individual query, and σ is the total number of blocks of input-data across all queries.

– Post-quantum security: By applying Theorem 7, we get

$$\mathsf{Adv}^{\mathsf{nml\text{-}PRF\text{-}PQ}}_{\mathsf{GCM}}(q,t) \le \mathsf{Adv}^{\mathsf{PRP\text{-}PQ}}_{E}(q,t) + \frac{(\sigma+3q)^2}{2^{n+1}}$$
$$\mathsf{Adv}^{\mathsf{nml\text{-}Forgery\text{-}PQ}}_{\mathsf{GCM}}(q,t) \le \mathsf{Adv}^{\mathsf{PRP\text{-}PQ}}_{E}(q,t) + \frac{(\sigma+3(q+q'))^2}{2^{n+1}} + \frac{q'\ell}{2^n} + \frac{q'}{2^s}.$$

– Post-quantum security in QICM: By applying Theorem 8, we get

$$\mathsf{Adv}^{\mathsf{nml\text{-}PRF\text{-}PQ\text{-}IC}}_{\mathsf{GCM}}(q_C,q_Q) \le \frac{q_Q^2\ell^2}{2^m} + \frac{(\sigma+3q_C)^2}{2^{n+1}}$$
$$\mathsf{Adv}^{\mathsf{nml\text{-}Forgery\text{-}PQ\text{-}IC}}_{\mathsf{GCM}}(q_C,q_Q) \le \frac{q_Q^2\ell^2}{2^m} + + \frac{(\sigma+3(q_C+q'_C))^2}{2^{n+1}} + \frac{q'_C\ell}{2^n} + \frac{q'_C}{2^s}.$$

6.4 Security of LRW and XEX2 using Theorem 7

The result from Theorem 7 extends to tweakable block cipher constructions. As a direct result, the SPRP-PQ security of LRW also follows from its classical security bound (Theorem 3).

Corollary 3. *Let LRW be as defined in Definition 7, constructed from a block cipher E and an ε-XOR universal hash function family h. Then the post-quantum security of LRW is given by:*

$$\mathit{Adv}^{\mathit{SPRP\text{-}PQ}}_{\mathit{LRW}}(q,t) \le \mathit{Adv}^{\mathit{SPRP\text{-}PQ}}_{E}(q,t) + q^2\varepsilon.$$

We analyze the SPRP-PQ security of LRW. The LRW construction is built upon such E, and consequently, the adversary $\mathcal{A}$ is granted quantum oracle access to $E(\cdot,\cdot)$.

Corollary 4. *Let LRW be as defined in Definition 7. Assuming h is XOR-universal, the post-quantum security of LRW in QICM is given by:*

$$\mathit{Adv}^{\mathit{SPRP\text{-}PQ\text{-}IC}}_{\mathit{LRW}}(q_C,q_Q) = \left| \Pr_{\substack{k\leftarrow\{0,1\}^m; k'\leftarrow\{0,1\}^\kappa \\ E\leftarrow\mathcal{E}(m,n)}} \left[\mathcal{A}^{\pm \mathit{LRW}_{k,k'}[E],|\pm E\rangle} = 1\right] - \Pr_{\substack{\widetilde{\Pi}\leftarrow\mathcal{E}(T,n); \\ E\leftarrow\mathcal{E}(m,n)}} \left[\mathcal{A}^{\pm \widetilde{\Pi},|\pm E\rangle} = 1\right] \right|$$
$$\le \frac{q_Q^2}{2^m} + \frac{q_C^2}{2^n}.$$

Similarly to the classical case, the SPRP-PQ security of XEX2 reduces to that of LRW.

Corollary 5. *Let XEX2 be as defined in Definition 8. Then the post-quantum security of XEX2 in QICM is given by:*

$$\mathit{Adv}^{\mathit{SPRP\text{-}PQ-IC}}_{\mathit{XEX2}}(q_C,q_Q) \le \frac{2q_Q^2}{2^m} + \frac{q_C^2}{2^n-1}.$$

Proof. Immediate consequence of Proposition 3, Lemma 7, and Corollary 3. □

6.5 Comparison of LRW Security Bound

Recall that the bound of LRW proved in Theorem 5 is:

$$\frac{6q_C^2}{2^n} + \frac{4\cdot\left(q_C\sqrt{q_Q} + q_Q\sqrt{q_C}\right)}{2^{(m+n)/2}}.$$

The comparison between the bounds from Corollary 4 and Theorem 5 is summarized earlier in Table 2. A detailed discussion follows below, omitting multiplicative constants. Note that in applying the general theorem, we do not need to assume that h is uniform.

– When $m \gg n$: The two bounds converge to $\frac{q_C^2}{2^n}$, and it aligns with the classical optimal bound (and classical matching attack) in Theorem 3.

– When $q_C \gg q_Q$: The bounds also align at $\frac{q_C^2}{2^n}$, and it aligns with the classical optimal bound (and classical matching attack) in Theorem 3.
– When $q_C \ll q_Q$: This scenario is more practical since online queries (q_C) are typically more scarce resources. Under these conditions, the bound in Theorem 5 simplifies to approximately $\frac{q_Q\sqrt{q_C}}{2^{(m+n)/2}}$, whereas the bound in Corollary 4 becomes $\frac{q_Q^2}{2^m}$. The bound from Theorem 5 is more favorable in this case.
Notably, this bound aligns with two quantum complete key recovery attacks: the offline-Simon attack with the trade-off $q_Q^2 q_C = 2^{(m+n)/2}$, and the Grover+Kuwakado–Morii attack with $q_Q = 2^{m/2+n/3}$ and $q_C = 2^{n/3}$.
– When $q_C \approx q_Q \approx q$: The bound in Theorem 5 simplifies to approximately $\frac{q^2}{2^n} + \frac{q^{3/2}}{2^{(m+n)/2}}$, where the second term corresponds to the offline-Simon attack described in Section C.3, assuming $m \leq 2n$. Furthermore, when $m \approx n$, both bounds reduce to $\frac{q^2}{2^n}$, aligning with the classical collision attack.

A summary is provided in Table 2. From the case analysis, the bound in Theorem 5 is typically tighter, with matching attacks. Nonetheless, the analysis in Theorem 3 and Corollary 4 provides a simpler and more general method for deriving a post-quantum security bound.

Scenarios	Classical	Q1 from GT	Q1 from HT
$m \gg n$	$\frac{q_C^2}{2^n}$	$\frac{q_C^2}{2^n}$	$\frac{q_C^2}{2^n}$
$q_C \gg q_Q$	$\frac{q_C^2}{2^n}$	$\frac{q_C^2}{2^n}$	$\frac{q_C^2}{2^n}$
$q_C \ll q_Q$	$\frac{q_Q}{2^m}$	$\frac{q_Q^2}{2^m}$	$\frac{q_Q\sqrt{q_C}}{2^{(m+n)/2}}$
$q_C \approx q_Q = q$	$\frac{q^2}{2^n} + \frac{q}{2^m}$	$\frac{q^2}{2^n} + \frac{q^2}{2^m}$	$\frac{q^2}{2^n} + \frac{q^{3/2}}{2^{(m+n)/2}}$

Table 2. Comparison of the classical bound (Theorem 3), the post-quantum security bounds of LRW using the General Theorem (GT, Corollary 4) and the Hybrid Technique (HT, Theorem 5). In the classical case, q_Q denotes the number of classical queries made to E, denoted for straightforward comparison.

Acknowledgments

Gorjan Alagic and Kaiyan Shi were supported in part by NSF award CNS-21547. Chen Bai acknowledges support from the Presidential Postdoctoral Fellowship at Virginia Tech. Christian Majenz acknowledges support by the Independent Research Fund Denmark via a DFF Sapere Aude grant (IM-3PQC, grant ID 10.46540/2064-00034B).

References

ABK+24. Gorjan Alagic, Chen Bai, Jonathan Katz, Christian Majenz, and Patrick Struck. Post-quantum security of tweakable Even-Mansour, and applications. In Marc Joye and Gregor Leander, editors, *EUROCRYPT 2024, Part I*, volume 14651 of *LNCS*, pages 310–338. Springer, Cham, May 2024.

ABKM22. Gorjan Alagic, Chen Bai, Jonathan Katz, and Christian Majenz. Post-quantum security of the Even-Mansour cipher. In Orr Dunkelman and Stefan Dziembowski, editors, *EUROCRYPT 2022, Part III*, volume 13277 of *LNCS*, pages 458–487. Springer, Cham, May / June 2022.

ADK+14. Martin R Albrecht, Benedikt Driessen, Elif Bilge Kavun, Gregor Leander, Christof Paar, and Tolga Yalçın. Block ciphers–focus on the linear layer (feat. pride). In *Annual Cryptology Conference*, pages 57–76. Springer, 2014.

BBBV97. Charles H Bennett, Ethan Bernstein, Gilles Brassard, and Umesh Vazirani. Strengths and weaknesses of quantum computing. *SIAM journal on Computing*, 26(5):1510–1523, 1997.

BBC+25. Jyotirmoy Basak, Ritam Bhaumik, Amit Kumar Chauhan, Ravindra Jejurikar, Ashwin Jha, Anandarup Roy, André Schrottenloher, and Suprita Talnikar. Post-quantum security of key-alternating feistel ciphers. *Cryptology ePrint Archive*, 2025.

BCG+12. Julia Borghoff, Anne Canteaut, Tim Güneysu, Elif Bilge Kavun, Miroslav Knezevic, Lars R Knudsen, Gregor Leander, Ventzislav Nikov, Christof Paar, Christian Rechberger, et al. Prince–a low-latency block cipher for pervasive computing applications. In *International conference on the theory and application of cryptology and information security*, pages 208–225. Springer, 2012.

BEM24. Chen Bai, Mehdi Esmaili, and Atul Mantri. Quantum security analysis of the key-alternating ciphers. *arXiv preprint arXiv:2412.05026*, 2024.

BHN+19. Xavier Bonnetain, Akinori Hosoyamada, María Naya-Plasencia, Yu Sasaki, and André Schrottenloher. Quantum attacks without superposition queries: The offline Simon's algorithm. In Steven D. Galbraith and Shiho Moriai, editors, *ASIACRYPT 2019, Part I*, volume 11921 of *LNCS*, pages 552–583. Springer, Cham, December 2019.

BHNP+19. Xavier Bonnetain, Akinori Hosoyamada, María Naya-Plasencia, Yu Sasaki, and André Schrottenloher. Quantum attacks without superposition queries: the offline simon's algorithm. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 552–583. Springer, 2019.

BHT97. Gilles Brassard, Peter Hoyer, and Alain Tapp. Quantum algorithm for the collision problem. *arXiv preprint quant-ph/9705002*, 1997.

BSS22. 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, Cham, May / June 2022.

CHL+25. Alexandru Cojocaru, Minki Hhan, Qipeng Liu, Takashi Yamakawa, and Aaram Yun. Quantum lifting for invertible permutations and ideal ciphers. In *Annual International Cryptology Conference*, pages 481–512. Springer, 2025.

CMM23. Matthew Campagna, Alexander Maximov, and John Preuß Mattsson. Galois counter mode with secure short tags (gcm-sst). 2023.

CNPS17. André Chailloux, María Naya-Plasencia, and André Schrottenloher. An efficient quantum collision search algorithm and implications on symmetric cryptography. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 211–240. Springer, 2017.

CSR+08. David Clunie, Rich Shroeppel, Phillip Rogaway, Vijay Bharadwaj, and Neils Ferguson. Public comments on the xts-aes mode. *Collected email comments released by NIST, available from their web page*, 2008.

DBN+01. Morris J Dworkin, Elaine Barker, James R Nechvatal, James Foti, Lawrence E Bassham, E Roback, James F Dray Jr, et al. Advanced encryption standard (aes). 2001.

Din15. Itai Dinur. Cryptanalytic time-memory-data tradeoffs for fx-constructions with applications to prince and pride. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 231–253. Springer, 2015.

Dwo01. Morris Dworkin. Recommendation for block cipher modes of operation. *NIST special publication*, 800:38B, 2001.

Dwo07. Morris J Dworkin. *Sp 800-38d. recommendation for block cipher modes of operation: Galois/counter mode (gcm) and gmac.* National Institute of Standards & Technology, 2007.

Dwo10a. Morris J Dworkin. Recommendation for block cipher modes of operation: The xts-aes mode for confidentiality on storage devices. 2010.

Dwo10b. Dworkin, Morris. Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices. Technical Report SP 800-38E, National Institute of Standards and Technology (NIST), Gaithersburg, MD, February 2010.

EMST78. William F Ehrsam, Carl HW Meyer, John L Smith, and Walter L Tuchman. Message verification and transmission error detection by block chaining, February 14 1978. US Patent 4,074,066.

GHHM21. Alex B Grilo, Kathrin Hövelmanns, Andreas Hülsing, and Christian Majenz. Tight adaptive reprogramming in the qrom. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 637–667. Springer, 2021.

GLL17. Shay Gueron, Adam Langley, and Yehuda Lindell. Aes-gcm-siv: specification and analysis. *Cryptology ePrint Archive*, 2017.

GT12. Peter Gaži and Stefano Tessaro. Efficient and optimally secure key-length extension for block ciphers via randomized cascading. In David Pointcheval and Thomas Johansson, editors, *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 63–80. Springer, Berlin, Heidelberg, April 2012.

Hos25. Akinori Hosoyamada. Post-quantum security of keyed sponge-based constructions through a modular approach. *Cryptology ePrint Archive*, 2025.

HS18. Akinori Hosoyamada and Yu Sasaki. Cryptanalysis against symmetric-key schemes with online classical queries and offline quantum computations. In *Cryptographers' Track at the RSA Conference*, pages 198–218. Springer, 2018.

HY18. 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, Cham, December 2018.

HY24. Minki Hhan and Shogo Yamada. Pseudorandom function-like states from common haar unitary. *arXiv preprint arXiv:2411.03201*, 2024.

IJMM24. Akiko Inoue, Ashwin Jha, Bart Mennink, and Kazuhiko Minematsu. Generic security of gcm-sst. *Cryptology ePrint Archive*, 2024.

IK03. Tetsu Iwata and Kaoru Kurosawa. Omac: One-key cbc mac. In *Fast Software Encryption: 10th International Workshop, FSE 2003, Lund, Sweden, February 24-26, 2003. Revised Papers 10*, pages 129–153. Springer, 2003.

IM19. Takanori Isobe and Kazuhiko Minematsu. Plaintext recovery attacks against xts beyond collisions. In *International Conference on Selected Areas in Cryptography*, pages 103–123. Springer, 2019.

IOM12. Tetsu Iwata, Keisuke Ohashi, and Kazuhiko Minematsu. Breaking and repairing gcm security proofs. In *Advances in Cryptology–CRYPTO 2012: 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings*, pages 31–49. Springer, 2012.

JN20. Ashwin Jha and Mridul Nandi. Tight security of cascaded lrw2. *Journal of Cryptology*, 33(3):1272–1317, 2020.

JST21. Joseph Jaeger, Fang Song, and Stefano Tessaro. Quantum key-length extension. In *Theory of Cryptography Conference*, pages 209–239. Springer, 2021.

KL07. Jonathan Katz and Yehuda Lindell. *Introduction to modern cryptography: principles and protocols*. Chapman and hall/CRC, 2007.

KLLN16. Marc Kaplan, Gaëtan Leurent, Anthony Leverrier, and María Naya-Plasencia. Breaking symmetric cryptosystems using quantum period finding. In Matthew Robshaw and Jonathan Katz, editors, *CRYPTO 2016, Part II*, volume 9815 of *LNCS*, pages 207–237. Springer, Berlin, Heidelberg, August 2016.

KM12. 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. IEEE, 2012.

KR96. Joe Kilian and Phillip Rogaway. How to protect DES against exhaustive key search. In Neal Koblitz, editor, *CRYPTO'96*, volume 1109 of *LNCS*, pages 252–267. Springer, Berlin, Heidelberg, August 1996.

KR01. Joe Kilian and Phillip Rogaway. How to protect DES against exhaustive key search (an analysis of DESX). *Journal of Cryptology*, 14(1):17–35, January 2001.

LM08. Moses Liskov and Kazuhiko Minematsu. Comments on xts-aes. *Comments to NIST, available from their web page*, 2008.

LRW02. Moses Liskov, Ronald L Rivest, and David Wagner. Tweakable block ciphers. In *Advances in Cryptology—CRYPTO 2002: 22nd Annual International Cryptology Conference Santa Barbara, California, USA, August 18–22, 2002 Proceedings 22*, pages 31–46. Springer, 2002.

Min06. Kazuhiko Minematsu. Improved security analysis of xex and lrw modes. In *International Workshop on Selected Areas in Cryptography*, pages 96–113. Springer, 2006.

MV04. David A McGrew and John Viega. The security and performance of the galois/counter mode of operation (full version). *Cryptology ePrint Archive*, 2004.

NOMI15. Yuichi Niwa, Keisuke Ohashi, Kazuhiko Minematsu, and Tetsu Iwata. Gcm security bounds reconsidered. In *Fast Software Encryption: 22nd International Workshop, FSE 2015, Istanbul, Turkey, March 8-11, 2015, Revised Selected Papers 22*, pages 385–407. Springer, 2015.

P1606. Ieee draft standard for authenticated encryption with length expansion for storage device. *IEEE Unapproved Draft Std P1619.1/D4, Oct 2007*, 2006.

P1619. Ieee standard for cryptographic protection of data on block-oriented storage devices. *IEEE Std 1619-2018 (Revision of IEEE Std 1619-2007)*, pages 1–41, 2019.

PR00. Erez Petrank and Charles Rackoff. Cbc mac for real-time data sources. *Journal of Cryptology*, 13:315–338, 2000.

Rog02. Phillip Rogaway. Authenticated-encryption with associated-data. In *Proceedings of the 9th ACM Conference on Computer and Communications Security*, pages 98–107, 2002.

Rog04. Phillip Rogaway. Efficient instantiations of tweakable blockciphers and refinements to modes OCB and PMAC. In Pil Joong Lee, editor, *ASIACRYPT 2004*, volume 3329 of *LNCS*, pages 16–31. Springer, Berlin, Heidelberg, December 2004.

Rog13. Phillip Rogaway. Evaluation of some blockcipher modes of operation. 2011. *Cryptography Research and Evaluation Committees (CRYPTREC) for the Government of Japan*, 2013.

Sho94. Peter W Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*, pages 124–134. Ieee, 1994.

SS19. Shingo Sato and Junji Shikata. So-cca secure pke in the quantum random oracle model or the quantum ideal cipher model. In *IMA International Conference on Cryptography and Coding*, pages 317–341. Springer, 2019.

Vau00. Serge Vaudenay. Decorrelation over infinite domains: the encrypted cbc-mac case. In *International Workshop on Selected Areas in Cryptography*, pages 189–201. Springer, 2000.

Zha19. Mark Zhandry. How to record quantum queries, and applications to quantum indifferentiability. In *Annual International Cryptology Conference*, pages 239–268. Springer, 2019.

A Proofs of the new resampling lemma

A.1 Proof of Lemma 2

Lemma 8 (Restatement of Lemma 2). *Let $\mathcal{D} = (\mathcal{D}_0, \mathcal{D}_1)$ be a quantum distinguisher in the following experiment:*

Phase 1: *Choose uniform $E \in \mathcal{E}(m,n)$ and give $\mathcal{D}$ quantum access to E and E^{-1}. Then $\mathcal{D}_0$ chooses and outputs a distribution D over $\{0,1\}^{m+2n}$.*

Phase 2: *Choose $k_0 \in \{0,1\}^m$ and $s_0, s_1 \in \{0,1\}^n$ according to D. Let $E^{(0)} = E$ and define $E^{(1)} : \{0,1\}^m \times \{0,1\}^n \to \{0,1\}^n$ by*

$$E^{(1)}_{k^*}(x) = \begin{cases} E_{k^*}(x) & \text{if } k^* \neq k_0 \\ E_{k^*} \circ \mathsf{swap}_{s_0,\,s_1}(x) & \text{if } k^* = k_0\,. \end{cases}$$

A uniform bit $b \in \{0,1\}$ is chosen, and $\mathcal{D}$ is given k_0, s_0, s_1, and quantum access to $E^{(b)}$. Then $\mathcal{D}$ outputs a guess b'.

For a probability distribution D on $\{0,1\}^{m+2n}$, we define

$$\varepsilon = \max_{(k_0^*, s_0^*, s_1^*) \in \{0,1\}^{m+2n}} D(k_0, s_0, s_1)$$

Then for any $\mathcal{D}$ making at most q queries to E in phase 1,

$$|\Pr[\mathcal{D} \text{ outputs } 1 \mid b = 1] - \Pr[\mathcal{D} \text{ outputs } 1 \mid b = 0]| \leq 4\sqrt{2^n \cdot q \cdot \varepsilon}\,.$$

Proof. The proof of this lemma generalizes Lemma 3 from [Hos25], which in turn builds on techniques from [ABKM22]. Thus, part of the proof is borrowed from these two works.

Let $F = F_{0^m} F_{0^{m-1}1}, \ldots, F_{1^m}$ be the internal register of a superposition oracle for an ideal cipher, where each $F_k = F_{k,0^n}, \ldots, F_{k,1^n}$ is a database register for a random permutation. Each F_k is initialized in the initial state $|\phi_0\rangle$ for a random permutation π, namely,

$$|\phi_0\rangle_{F_k} = (2^n!)^{-1/2} \sum_{\pi \in \mathcal{P}(n)} |\pi\rangle_{F_k}\,.$$

Moreover, define $|\Phi_0\rangle_F = |\phi_0\rangle^{\otimes 2^m}$.

Then, quantum queries to the ideal cipher can be evaluated via the unitary operators O and O^{inv}:

$$\begin{aligned} O_{KXYF}\ |k\rangle_K |x\rangle_X |y\rangle_Y |\pi\rangle_{F_k} &= |k\rangle_K |x\rangle_X |y \oplus \pi(x)\rangle_Y |\pi\rangle_{F_k} \\ O^{\mathrm{inv}}_{KXYF}\ |k\rangle_K |x\rangle_X |y\rangle_Y |\pi\rangle_{F_k} &= |k\rangle_K |x \oplus \left(\oplus_{x' : \pi(x') = y} x'\right)\rangle_X |y\rangle_Y |\pi\rangle_{F_k}\,. \end{aligned}$$

Note that O and O^{inv} act only on the register F_k, and act as the identity on all other F-registers. By analogy to the proof of [ABKM22,Hos25], define the projectors

$$(P_{k_0,s_0,s_1})_{KX} = \begin{cases} \mathbb{1} & s_0 = s_1 \\ \mathbb{1} - |k_0\rangle\langle k_0| \otimes (|s_0\rangle\langle s_0| + |s_1\rangle\langle s_1|)_X & s_0 \neq s_1 \end{cases}$$

and

$$\begin{aligned} &\left(P^{\mathrm{inv}}_{k_0,s_0,s_1}\right)_{KYF} \\ &= \begin{cases} \mathbb{1} & s_0 = s_1 \\ |k_0\rangle\langle k_0|_K \otimes \sum_{y \in \{0,1\}^n} |y\rangle\langle y|_Y \otimes (\mathbb{1} - |y\rangle\langle y|)^{\otimes 2}_{F_{k_0,s_0} F_{k_0,s_1}} & s_0 \neq s_1. \end{cases} \end{aligned}$$

Moreover, let $\bar{P}_{k_0,s_0,s_1} = \mathbb{1} - P_{k_0,s_0,s_1}$ and $\bar{P}^{\mathrm{inv}}_{k_0,s_0,s_1} = \mathbb{1} - P^{\mathrm{inv}}_{k_0,s_0,s_1}$. Define the swap operator

$$\mathsf{Swap}_{AB} |x\rangle_A |y\rangle_B = |y\rangle_A |x\rangle_B$$

.

Without loss of generality, we assume (as in [Hos25]) that $\mathcal{D}_0$ makes exactly q quantum queries and does not perform intermediate measurements. The distribution D is chosen by $\mathcal{D}_0$ as follows.

1. At the beginning, $\mathcal{D}_0$ sets a specific part of the offline register E, which we refer to as register Z, to be $|0\rangle_Z$. Register Z is untouched until $\mathcal{D}_0$ has made all its q queries.
2. After making q quantum queries, $\mathcal{D}_0$ applies a unitary to all its internal registers, including Z.
3. Then, it measures register Z to obtain the distribution D.

We denote the projector $|D\rangle\langle D|_Z$ as P_D. Let $|\psi_0\rangle = |\psi_0'\rangle_{KXYE} |\phi_0\rangle_F$ be the initial state of $\mathcal{D}_0$. Let $|\psi\rangle$ be the quantum state right before the measurement to choose the distribution D. Then,

$$|\psi\rangle = U_q O_q \cdots U_1 O_1 |\psi_0\rangle , \tag{29}$$

holds, where each O_i (which is either O_{KXYF} or O^{inv}_{KXYF}) is the unitary operator corresponding to the ith quantum query, and U_i is a unitary operator acting on registers XYE that corresponds to some offline computation by $\mathcal{D}_0$. In addition, for arbitrary $k_0 \in \{0,1\}^m$ and $s_0, s_1 \in \{0,1\}^n$, let

$$\begin{aligned} |\psi_{\mathrm{good}}(k_0,s_0,s_1)\rangle &:= z \cdot U_q O_q P^q_{k_0,s_0,s_1} \cdots U_1 O_1 P^1_{k_0,s_0,s_1} |\psi_0\rangle \\ |\psi_{\mathrm{bad}}(k_0,s_0,s_1)\rangle &:= |\psi\rangle - |\psi_{\mathrm{good}}(k_0,s_0,s_1)\rangle , \end{aligned}$$

where

$$P^i_{k_0,s_0,s_1} := \begin{cases} (P_{k_0,s_0,s_1})_X & \text{if } O_i = O_{KXYF} \\ (P^{\mathrm{inv}}_{k_0,s_0,s_1})_{KYF} & \text{if } O_i = O^{\mathrm{inv}}_{KXYF}, \end{cases}$$

and z is a complex number such that $|z| = 1$ and $\langle \psi \mid \psi_{\mathrm{good}}(k_0,s_0,s_1)\rangle \in \mathbb{R}_{\geq 0}$. As in [ABKM22,Hos25], the vector $|\psi_{\mathrm{good}}(k_0,s_0,s_1)\rangle$ is invariant under the action of $\mathsf{Swap}_{F_{k_0,s_0},F_{k_0,s_1}}$, that is,

$$\mathsf{Swap}_{F_{k_0,s_0},F_{k_0,s_1}} |\psi_{\mathrm{good}}(k_0,s_0,s_1)\rangle = |\psi_{\mathrm{good}}(k_0,s_0,s_1)\rangle . \tag{30}$$

Moreover, let

$$\varepsilon_i(k_0,s_0,s_1) := \left\| \bar{P}^i_{k_0,s_0,s_1} U_{i-1} O_{i-1} \cdots U_1 O_1 |\psi_0\rangle \right\|_2^2 ,$$

where $\bar{P}^i_{k_0,s_0,s_1} := \mathbb{1} - P^i_{k_0,s_0,s_1}$.

Recall that, at the end of $\mathcal{D}_0$, the register Z (which is a part of register E for offline computation) is measured to choose a distribution D. The (pure) state just before the measurement is $|\psi\rangle$ of Equation 29. By the measurement, $|\psi\rangle$ changes to the mixed state

$$\sum_{D \in \mathcal{S}} P_D |\psi\rangle \langle\psi| P_D .$$

After that, k_0, s_0 and s_1 are sampled, and the state changes to

$$\rho_0 := \sum_{\substack{D \in \mathcal{S} \\ (k_0,s_0,s_1) \sim D}} D(k_0,s_0,s_1)\ P_D |\psi\rangle \langle\psi|_{KXYEF} P_D \otimes |k_0,s_0,s_1\rangle \langle k_0,s_0,s_1|_C ,$$

where C is an additional register.

If $b = 1$ and the values of the permutation are swapped on s_0 and s_1, the state further changes to

$$\rho_1 := \sum_{\substack{D \in \mathcal{S} \\ (k_0,s_0,s_1) \sim D}} D(k_0,s_0,s_1)\ \mathsf{Swap}_{F_{k_0,s_0},F_{k_0,s_1}} P_D |\psi\rangle \langle\psi| P_D \mathsf{Swap}_{F_{k_0,s_0},F_{k_0,s_1}} \otimes |k_0,s_0,s_1\rangle \langle k_0,s_0,s_1| .$$

From the standard argument for distinguishing advantages,

$$\left| \Pr[b' = 1 \mid b = 1] - \Pr[b' = 1 \mid b = 0] \right| \leq \mathsf{TD}(\rho_0, \rho_1),$$

where TD is the trace distance.

We observe that the state ρ_0 can also be produced from $|\psi\rangle$ as follows.

1. Without measuring register Z (on which the information of D is written), create the superposition of k_0, s_0 and s_1 of the form

$$\sum_{(k_0,s_0,s_1)\sim D} \sqrt{D(k_0,s_0,s_1)}\ |D\rangle_Z\,|k_0,s_0,s_1\rangle_C\,.$$

   For each D, obtaining the (pure) state

$$|\xi_0\rangle := \sum_{\substack{D\in\mathcal{S}\\(k_0,s_0,s_1)\sim D}} \sqrt{D(k_0,s_0,s_1)}\ P_D\,|\psi\rangle_{KXYEF}\otimes|k_0,s_0,s_1\rangle_C\,.$$

2. Measure registers Z and C to obtain the classical information of D, k_0, s_0, s_1.

Similarly, the state ρ_1 can be produced by measuring the registers Z and C of the pure state

$$|\xi_1\rangle := \sum_{\substack{D\in\mathcal{S}\\(k_0,s_0,s_1)\sim D}} \sqrt{D(k_0,s_0,s_1)}\ \mathsf{Swap}_{F_{k_0,s_0},F_{k_0,s_1}}P_D\,|\psi\rangle_{KXYEF}\otimes|k_0,s_0,s_1\rangle_C\,.$$

Since measurements decrease the trace distance between two states, and the trace distance between the two pure states $|\xi_0\rangle\langle\xi_0|$ and $|\xi_1\rangle\langle\xi_1|$ is upper bounded by the norm of the difference ($|\xi_0\rangle-|\xi_1\rangle$), it holds that

$$\mathsf{TD}(\rho_0,\rho_1)\ \le\ \mathsf{TD}(|\xi_0\rangle\langle\xi_0|\,,|\xi_1\rangle\langle\xi_1|)\ \le\ \|\,|\xi_0\rangle-|\xi_1\rangle\,\|_2.$$

In addition, we have

$$\begin{aligned}
\|\,|\xi_0\rangle-|\xi_1\rangle\,\|_2^2 &\overset{(i)}{=} \sum_{\substack{D\in\mathcal{S}\\(k_0,s_0,s_1)\sim D}} D(k_0,s_0,s_1)\ \Big\|P_D\big(1-\mathsf{Swap}_{F_{k_0,s_0},F_{k_0,s_1}}\big)\,|\psi\rangle\Big\|_2^2\\
&\overset{(ii)}{=} \sum_{\substack{D\in\mathcal{S}\\(k_0,s_0,s_1)\sim D}} D(k_0,s_0,s_1)\ \Big\|P_D\Big(|\psi_{\mathrm{bad}}(k_0,s_0,s_1)\rangle\\
&\qquad\qquad -\ \mathsf{Swap}_{F_{k_0,s_0},F_{k_0,s_1}}\,|\psi_{\mathrm{bad}}(k_0,s_0,s_1)\rangle\Big)\Big\|_2^2\\
&\overset{(iii)}{\le}\ 4 \sum_{\substack{D\in\mathcal{S}\\(k_0,s_0,s_1)\in\{0,1\}^{m+2n}}} D(k_0,s_0,s_1)\ \|P_D\,|\psi_{\mathrm{bad}}(k_0,s_0,s_1)\rangle\|_2^2\\
&\overset{(iv)}{\le}\ 4 \sum_{\substack{D\in\mathcal{S}\\(k_0,s_0,s_1)\in\{0,1\}^{m+2n}}} \varepsilon\ \|P_D\,|\psi_{\mathrm{bad}}(k_0,s_0,s_1)\rangle\|_2^2\\
&\overset{(v)}{=}\ 4\varepsilon\cdot 2^{m+2n}\,\mathbb{E}_{(k_0,s_0,s_1)\leftarrow\{0,1\}^{m+2n}}\left[\|\,|\psi_{\mathrm{bad}}(k_0,s_0,s_1)\rangle\,\|_2^2\right].
\end{aligned}\tag{31}$$

where we used the fact that $\left[P_D,\mathsf{Swap}_{F_{k_0,s_0},F_{k_0,s_1}}\right]=0$ [9] for (i) and (iii), Equation 30 for (ii), and the fact that $\sum_D P_D=1$ for (v).

Next, we bound $\mathbb{E}_{(k_0,s_0,s_1)\leftarrow\{0,1\}^{m+2n}}\left[\||\psi_{\mathrm{bad}}(k_0,s_0,s_1)\rangle\|_2^2\right]$. First, using the gentle measurement lemma as in [ABKM22, Section 4.2], we get

$$\||\psi_{\mathrm{bad}}(k_0,s_0,s_1)\rangle\|_2^2\ \le\ 2\sum_{i=1}^{q}\varepsilon_i(k_0,s_0,s_1).\tag{32}$$

For any normalized state $|\psi\rangle_{KXE}$, let

$$|\psi\rangle_{KXE}=\sum_{\substack{k\in\{0,1\}^m\\x\in\{0,1\}^n}}|k\rangle_K\,|x\rangle_X\otimes|\psi_{kx}\rangle_E$$

[9] P_D acts only on (a part of) register E while $\mathsf{Swap}_{F_{k_0,s_0},F_{k_0,s_1}}$ acts only on register F.

be its expansion in the computational basis on X. By the definition of ε, following [ABKM22, Section 4.2], we obtain

$$\begin{aligned}
&\mathbb{E}_{(k_0,s_0,s_1)\leftarrow\{0,1\}^{m+2n}}\left[\left\|\left(P_{k_0,s_0,s_1}\right)_{KX}|\psi\rangle_{KXE}\right\|_2^2\right]\\
&=\sum_{\substack{k\in\{0,1\}^m\\ x\in\{0,1\}^n}}\||\psi_{kx}\rangle\|_2^2\mathbb{E}_{(k_0,s_0,s_1)\leftarrow\{0,1\}^{m+2n}}\left[\left\|\left(P_{k_0,s_0,s_1}\right)_{KX}|k\rangle_K|x\rangle_X\right\|_2^2\right]\\
&=\sum_{\substack{k\in\{0,1\}^m\\ x\in\{0,1\}^n}}\||\psi_{kx}\rangle\|_2^2\Pr_{(k_0,s_0,s_1)\leftarrow\{0,1\}^{m+2n}}\left[(k,x)\in\{(k_0,s_0),(k_0,s_1)\}\right]\\
&\le 2\cdot 2^{-(n+m)}.
\end{aligned}$$

Similarly, again following [ABKM22, Section 4.2]

$$\mathop{\mathbb{E}}_{(k_0,s_0,s_1)\sim D}\left[\left\|\left(\bar{P}^{\mathrm{inv}}_{k_0,s_0,s_1}\right)_{KYF}|\psi\rangle_{KYEF}\right\|_2^2\right]\le 2\cdot 2^{-(n+m)}.$$

Then we have

$$\mathbb{E}_{(k_0,s_0,s_1)\sim D}\left[\varepsilon_i(k_0,s_0,s_1)\right]\ \le\ 2\cdot 2^{-(n+m)}. \tag{33}$$

Combining Eqs. (31) to (33), we obtain the desired bound. □

B More Details on Post-Quantum Security of FX

B.1 Proof of Proposition 1

Proposition 4 (Restatement). *For any $E\in\mathcal{E}(m,n)$, $K=(k_0,k_1,k_2)\in\{0,1\}^{m+2n}$, $j\in[1,q_C]$, transcript $T_j=\{(x_1,y_1),\ldots,(x_j,y_j)\}$ without repetition, and any $i\in\{1,\ldots,j\}$, it holds that*

$$E_{k_0}^{T_j,K}(x_i\oplus k_1)\oplus k_2=y_i.$$

Proof. We prove by strong induction on i. We start by the base case $i=j$.

$$E_{k_0}^{T_j,K}(x_j\oplus k_1)=\mathsf{swap}_{E_{k_0}^{T_{j-1},K}(x_j\oplus k_1),\,y_j\oplus k_2}\circ E_{k_0}^{T_{j-1},K}(x_j\oplus k_1)=y_j\oplus k_2.$$

Assume for all $i\in\{r,\ldots,j\}$ that $E_{k_0}^{T_j,K}(x_i\oplus k_1)\oplus k_2=y_i$. Expanding it, we obtain

$$\begin{aligned}
&E_{k_0}^{T_j,K}(x_i\oplus k_1)\\
&=\mathsf{swap}_{E_{k_0}^{T_{j-1},K}(x_j\oplus k_1),\,y_j\oplus k_2}\circ\ldots\circ\mathsf{swap}_{E_{k_0}^{T_{i-1},K}(x_i\oplus k_1),\,y_i\oplus k_2}\circ E_{k_0}^{T_{i-1},K}(x_i\oplus k_1)\\
&=F_i\circ E_{k_0}^{T_{i-1},K}(x_i\oplus k_1)=y_i\oplus k_2,
\end{aligned}$$

where we define

$$F_i=\mathsf{swap}_{E_{k_0}^{T_{j-1},K}(x_j\oplus k_1),\,y_j\oplus k_2}\circ\ldots\circ\mathsf{swap}_{E_{k_0}^{T_{i-1},K}(x_i\oplus k_1),\,y_i\oplus k_2}.$$

By rearranging, we get for all $i\in\{r,\ldots,j\}$,

$$E_{k_0}^{T_{i-1},K}(x_i\oplus k_1)=F_i^{-1}(y_i\oplus k_2).$$

We now work on case $r-1$,

$$\begin{aligned}
&E_{k_0}^{T_j,K}(x_{r-1}\oplus k_1)\\
&=\mathsf{swap}_{E_{k_0}^{T_{j-1},K}(x_j\oplus k_1),\,y_j\oplus k_2}\circ\ldots\circ\mathsf{swap}_{E_{k_0}^{T_{r-2},K}(x_{r-1}\oplus k_1),\,y_{r-1}\oplus k_2}\circ E_{k_0}^{T_{r-2},K}(x_{r-1}\oplus k_1)\\
&=\mathsf{swap}_{E_{k_0}^{T_{j-1},K}(x_j\oplus k_1),\,y_j\oplus k_2}\circ\ldots\circ\mathsf{swap}_{E_{k_0}^{T_{r-1},K}(x_r\oplus k_1),\,y_r\oplus k_2}(y_{r-1}\oplus k_2)\\
&=F_r(y_{r-1}\oplus k_2).
\end{aligned}$$

The last equality holds if the following two properties hold.

Property 1: $y_{r-1} \notin \{y_r, \ldots, y_j\}$. Since we don't allow repeated queries, then $x_{r-1} \notin \{x_r, \ldots, x_j\}$. Since R is a permutation, $R(x_{r-1}) \notin \{R(x_r), \ldots, R(x_j)\}$ which gives the desired property.

Property 2: $y_{r-1} \oplus k_2 \notin \left\{E_{k_0}^{T_{r-1},K}(x_r \oplus k_1), \ldots, E_{k_0}^{T_{j-1},K}(x_j \oplus k_1)\right\}$. We prove step by step. First by contradiction, suppose $y_{r-1} \oplus k_2 = E_{k_0}^{T_{r-1},K}(x_r \oplus k_1)$. By the inductive assumption, we get

$$\begin{aligned} y_{r-1} \oplus k_2 &= F_r^{-1}(y_r \oplus k_2) \\ F_r(y_{r-1} \oplus k_2) &= y_r \oplus k_2 \\ E_{k_0}^{T_j,K}(x_{r-1} \oplus k_1) &= E_{k_0}^{T_j,K}(x_r \oplus k_1). \end{aligned}$$

Since $E_{k_0}^{T_j,K}$ is a permutation, this contradicts the fact that $x_{r-1} \neq x_r$. Therefore we have $y_{r-1} \oplus k_2 \neq E_{k_0}^{T_{r-1},K}(x_r \oplus k_1)$. Now, we can write

$$\begin{aligned} &E_{k_0}^{T_j,K}(x_{r-1} \oplus k_1) \\ &= \mathsf{swap}_{E_{k_0}^{T_{j-1},K}(x_j \oplus k_1),\, y_j \oplus k_2} \circ \ldots \circ \mathsf{swap}_{E_{k_0}^{T_r,K}(x_{r+1} \oplus k_1),\, y_{r+1} \oplus k_2}(y_{r-1} \oplus k_2) \\ &= F_{r+1}(y_{r-1} \oplus k_2). \end{aligned}$$

By a similar prove-by-contradiction argument, using the inductive assumption on $r+1$, we obtain

$$y_{r-1} \oplus k_2 \neq E_{k_0}^{T_r,K}(x_{r+1} \oplus k_1).$$

Repeating this proof by contradiction step by step for $r+2, r+3, \ldots, j$, we eventually reach

$$y_{r-1} \oplus k_2 \neq E_{k_0}^{T_{j-1},K}(x_j \oplus k_1),$$

which establishes Property 2.

By these two properties, we can get

$$E_{k_0}^{T_j,K}(x_{r-1} \oplus k_1) = y_{r-1} \oplus k_2.$$

Then by strong induction, the proposition holds for all $i \in \{1, \ldots, j\}$. □

B.2 Handling Inverse Queries

In this section, we extend our analysis to the setting where the distinguisher may issue classical queries in the inverse direction. Conceptually, the overall hybrid structure remains unchanged, i.e., the sequence of hybrids $(\mathbf{H}_0, \ldots, \mathbf{H}_{q_C})$ is identical in both the forward and inverse query settings. This is because each hybrid depends only on the transcript $T_j = \{(x_1, y_1), \ldots, (x_j, y_j)\}$, which records the pairs of classical queries made so far. The transcript itself is invariant under the query direction: whether the adversary queried $\mathsf{FX}_K(x_i) = y_i$ or $\mathsf{FX}_K^{-1}(y_i) = x_i$, the resulting set of pairs (x_i, y_i) is the same.

Consequently, the hybrids $\mathbf{H}_j$ remain identical in both settings. The only difference arises in the definition of the intermediate hybrids, where the classical queries are handled in different directions. In particular, the query direction affects how the reprogramming is applied within each step, and thus the intermediate transitions between $\mathbf{H}_j$ and $\mathbf{H}_{j+1}$ must be redefined accordingly.

We now show that these inverse queries can be handled in a fully symmetric manner. Specifically, for each pair of adjacent hybrids $\mathbf{H}_j$ and $\mathbf{H}_{j+1}$, we consider the $(j+1)^{\text{st}}$ classical query as an inverse query, which is answered by the inverse oracle. To formalize this, we first introduce the notation for inverse queries. Using the fact

$$E_{k_0}^{-1} \circ \mathsf{swap}_{a,\,b} = \mathsf{swap}_{E_{k_0}^{-1}(a),\, E_{k_0}^{-1}(b)} \circ E_{k_0}^{-1},$$

we obtain

$$\begin{aligned} (E_{k_0}^{T_1,k})^{-1} &= (\mathsf{swap}_{E_{k_0}(x_1 \oplus k_1),\, y_1 \oplus k_2} \circ E_{k_0})^{-1} \\ &= E_{k_0}^{-1} \circ \mathsf{swap}_{E_{k_0}(x_1 \oplus k_1),\, y_1 \oplus k_2} \\ &= \mathsf{swap}_{x_1 \oplus k_1,\, E_{k_0}^{-1}(y_1 \oplus k_2)} \circ E_{k_0}^{-1}. \end{aligned}$$

Extending to j swaps, we get

$$\begin{aligned}(E_{k_0}^{T_j,k})^{-1}(y) &= E_{k_0}^{-1} \circ \mathsf{swap}_{E_{k_0}(x_1\oplus k_1),\, y_1\oplus k_2} \circ \cdots \circ \mathsf{swap}_{E_{k_0}^{T_{j-1},k}(x_j\oplus k_1),\, y_j\oplus k_2}(y) \\ &= (E_{k_0}^{T_{j-1},k})^{-1} \circ \mathsf{swap}_{E_{k_0}^{T_{j-1},k}(x_j\oplus k_1),\, y_j\oplus k_2}(y) \\ &= \mathsf{swap}_{x_j\oplus k_1,\,(E_{k_0}^{T_{j-1},k})^{-1}(y_j\oplus k_2)} \circ (E_{k_0}^{T_{j-1},k})^{-1}(y) \\ &= \prod_{i=j}^{1} \mathsf{swap}_{x_i\oplus k_1,\,(E_{k_0}^{T_{i-1},k})^{-1}(y_i\oplus k_2)} \circ E_{k_0}^{-1}(y).\end{aligned}$$

Moreover, define

$$(E_{k^*}^{(1)})^{-1}(y) = \begin{cases} E_{k^*}^{-1}(x) & \text{if } k^* \neq k_0 \\ \left(E_{k_0}^{-1} \circ \mathsf{swap}_{s_0,\,s_1}\right)(y) & \text{if } k^* = k_0. \end{cases}$$

Analogous to the forward case, we first define the intermediate hybrids $\mathbf{H}_j^{1,\mathrm{inv}}$ and $\mathbf{H}_j^{2,\mathrm{inv}}$ ($\mathbf{H}_3^j$ is the same in both cases). We then show that the distinguishing advantage between $\mathbf{H}_j$ and $\mathbf{H}_{j+1}$ remains the same in the inverse case. Specifically, for all $0 \leq j < q_C$, we establish the following bounds:

$$\begin{aligned} &\text{Lemma 9:} && |\Pr[\mathcal{A}(\mathbf{H}_j) = 1] - \Pr[\mathcal{A}(\mathbf{H}_j^{1,\mathrm{inv}}) = 1]| \leq 4\sqrt{\frac{q_Q}{2^m(2^n - j)}} \\ &\text{Lemma 10:} && \mathbf{H}_j^{1,\mathrm{inv}} = \mathbf{H}_j^{2,\mathrm{inv}} \\ &\text{Lemma 11:} && \mathbf{H}_j^{2,\mathrm{inv}} = \mathbf{H}_j^{3} \\ &\text{Lemma 6:} && |\Pr[\mathcal{A}(\mathbf{H}_j^{3}) = 1] - \Pr[\mathcal{A}(\mathbf{H}_{j+1}) = 1]| \leq 2 \cdot q_{Q,j+1}\sqrt{\frac{2(j+1)}{2^{m+n}}}, \end{aligned}$$

where $q_{Q,j+1}$ is the expected number of queries $\mathcal{A}$ makes to P in the $(j+1)^{\mathrm{st}}$ stage, i.e., the stage between the $(j+1)^{\mathrm{st}}$ and $(j+2)^{\mathrm{nd}}$ classical queries. By Equation 25, we obtain the same bound as in the forward case. Hence, inverse queries can be handled in a fully symmetric manner, yielding the same distinguishing advantage.

Experiment $\mathbf{H}_j^{1,\mathrm{inv}}$.

1. Run $\mathcal{A}$, answering its classical queries using R and its quantum queries using E, until $\mathcal{A}$ makes its $(j+1)^{\mathrm{st}}$ classical query y_{j+1}, which we assume for concreteness to be in the inverse direction. Let T_j be the list of the classical queries so far.
2. Define set $S = \{0,1\}^n \backslash \{y_1 \oplus k_2, \cdots, y_j \oplus k_2\}$. Choose uniform $s \in S$, and define $(E^{(1)})^{-1}$ as

$$(E_{k^*}^{(1)})^{-1}(y) = \begin{cases} E_{k^*}^{-1}(y) & \text{if } k^* \neq k_0 \\ \left(E_{k_0}^{-1} \circ \mathsf{swap}_{y_{j+1}\oplus k_2,\, s}\right)(y) & \text{if } k^* = k_0. \end{cases}$$

Then

$$(E_{k^*}^{(1)})(x) = \begin{cases} E_{k^*}(x) & \text{if } k^* \neq k_0 \\ \left(E_{k_0} \circ \mathsf{swap}_{E_{k_0}^{-1}(y_{j+1}\oplus k_2),\, E_{k_0}^{-1}(s)}\right)(x) & \text{if } k^* = k_0. \end{cases}$$

Continue running $\mathcal{A}$, answering its remaining classical queries (including the $(j+1)^{\mathrm{st}}$) using $\mathsf{FX}_K[(E^{(1)})^{T_j,K}]$, and its quantum queries using $(E^{(1)})^{T_j,K}$.

Experiment $\mathbf{H}_j^{2,\mathrm{inv}}$.

1. Run $\mathcal{A}$, answering its classical queries using R and its quantum queries using E, until $\mathcal{A}$ makes its $(j+1)^{\mathrm{st}}$ classical query y_{j+1}. Let T_j be the list of classical queries so far.

2. Define $E^{(1)}$ as in $\mathbf{H}_j^{1,\mathrm{inv}}$ and answer the $(j+1)^{\mathrm{st}}$ classical query using $\mathsf{FX}_K[(E^{(1)})^{T_j,K}]$. Denote the response as x_{j+1}, i.e.,

$$x_{j+1} = (\mathsf{FX}_K[(E^{(1)})^j])^{-1}(y_{j+1}).$$

Then the challenger constructs E^{j+1} adaptively as in Equation 22. Continue running $\mathcal{A}$, answering its remaining classical queries using $\mathsf{FX}_K[E^{T_{j+1},K}]$, and its quantum queries using $E^{T_{j+1},K}$.

Next, we prove Lemma 9, Lemma 10 and Lemma 11. The proofs are proceeded in an entirely analogous manner to those of Lemma 3, Lemma 4 and Lemma 5.

Lemma 9. *For $j = 0, \ldots, q_C$,*

$$\left|\Pr[\mathcal{A}(\mathbf{H}_j) = 1] - \Pr[\mathcal{A}(\mathbf{H}_j^{1,inv}) = 1]\right| \leq 4\sqrt{\frac{q_Q}{2^m(2^n - j)}}.$$

Proof. In this lemma, we bound the distinguishability of $\mathbf{H}_j$ and $\mathbf{H}_j^{1,\mathrm{inv}}$.

$$\begin{aligned}
\mathbf{H}_j: &\ |E\rangle, R, |E\rangle, \cdots, R, |E\rangle, \mathsf{FX}_K[\quad E^j\quad], |E^j\rangle \quad\quad, \mathsf{FX}_K\left[E^j\right], |E^j\rangle, \cdots \\
\mathbf{H}_j^{1,\mathrm{inv}}: &\ |E\rangle, R, |E\rangle, \cdots, R, |E\rangle, \mathsf{FX}_K[(E^{(1)})^j], |(E^{(1)})^j\rangle, \mathsf{FX}_K[(E^{(1)})^j], (E^{(1)})^j, \cdots.
\end{aligned}$$

Let $\mathcal{A}$ be a distinguisher between $\mathbf{H}_j$ and $\mathbf{H}_j^{1,\mathrm{inv}}$. We construct from $\mathcal{A}$ a distinguisher $\mathcal{D}$ for the resampling experiment of Lemma 2. $\mathcal{D}$ does:

Phase 1: $\mathcal{D}$ is given quantum access to an ideal cipher E. It samples a uniform $R \leftarrow \mathcal{P}_n$ and then runs $\mathcal{A}$, answering its quantum queries with E and its classical queries with R (in the appropriate directions), until $\mathcal{A}$ submits its $(j+1)^{\mathrm{st}}$ classical query y_{j+1}. At that point, $\mathcal{D}$ has a list $T_j = \{(x_1, y_1), \cdots, (x_j, y_j)\}$ of the queries/answers $\mathcal{A}$ has made to its classical oracle thus far. Next, $\mathcal{D}$ constructs a distribution D on $\{0,1\}^{m+2n}$ and it's sampling algorithm Π. To sample a tuple $(a_0, z_0, z_1) \leftarrow D$, Π does the following:
1 : Sample uniform $a_0 \in \{0,1\}^m$ and $z_0 \in \{0,1\}^n$.
2 : Construct $S = \{0,1\}^n \backslash \{z_0 \oplus y_1 \oplus y_{j+1}, \cdots, z_0 \oplus y_j \oplus y_{j+1}\} = \{0,1\}^n \backslash S^{\perp}$.
3 : Sample uniform $z_1 \in S$, and output (a_0, z_0, z_1).
Phase 2: $\mathcal{D}$ is given $(k_0, s_0, s_1) \leftarrow D$ and quantum oracle access to a cipher $E^{(b)}$. Then $\mathcal{D}$ sets $k_2 = y_{j+1} \oplus s_0$, uniform $k_1 \in \{0,1\}^n$ and $k = (k_0, k_1, k_2)$. It then continues running $\mathcal{A}$, answering its remaining classical queries (including the $(j+1)^{\mathrm{st}}$) using $\mathsf{FX}_K[(E^{(b)})^{T_j,k}]$, and its remaining quantum queries using $(E^{(b)})^{T_j,k}$. $\mathcal{D}$ outputs whatever $\mathcal{A}$ does.

Note that $s_1 \notin S^{\perp}$ where $S^{\perp} = \{y_1 \oplus k_2, \cdots y_j \oplus k_2\}$, by algorithm Π. In phase 1, distinguisher $\mathcal{D}$ perfectly simulates experiments $\mathbf{H}_j$ and $\mathbf{H}_j^{1,\mathrm{inv}}$ for $\mathcal{A}$ until the point where $\mathcal{A}$ makes its $(j+1)^{\mathrm{st}}$ classical query. If $b = 0$, $\mathcal{D}$ gets access to $E^{(0)} = E$ in phase 2. Since $\mathcal{D}$ answers all quantum queries using $(E^{(0)})^{T_j,k}$ and all classical queries using $\mathsf{FX}_K[(E^{(0)})^{T_j,k}]$, we see that $\mathcal{D}$ perfectly simulates $\mathbf{H}_j$ for $\mathcal{A}$ in that case. If, on the other hand, $b = 1$ in phase 2, then $\mathcal{D}$ gets access to $E^{(1)}$, where

$$(E_{k^*}^{(1)})^{-1}(y) = \begin{cases} E_{k^*}^{-1}(x) & \text{if } k^* \neq k_0 \\ \left(E_{k_0}^{-1} \circ \mathsf{swap}_{s_0,\, s_1}\right)(y) & \text{if } k^* = k_0. \end{cases}$$

Since $k_2 \coloneqq s_0 \oplus y_{j+1}$, it holds that

$$(E_{k^*}^{(1)})^{-1}(y) = \begin{cases} E_{k^*}^{-1}(x) & \text{if } k^* \neq k_0 \\ \left(E_{k_0}^{-1} \circ \mathsf{swap}_{k_2 \oplus y_{j+1},\, s_1}\right)(y) & \text{if } k^* = k_0. \end{cases}$$

Moreover, the fact that s_0 (and hence $s_0 \oplus y_{j+1}$), k_0 and k_1 are uniform implies that $\mathcal{D}$ perfectly simulates $\mathbf{H}_j^{1,\mathrm{inv}}$ for $\mathcal{A}$. Applying Lemma 2 thus gives

$$\left|\Pr[\mathcal{A}(\mathbf{H}_j) = 1] - \Pr[\mathcal{A}(\mathbf{H}_j^{1,\mathrm{inv}}) = 1]\right| \leq 4\sqrt{q_Q \cdot \varepsilon \cdot 2^n},$$

where ε is the same as in Lemma 3. Therefore, we have

$$\left|\Pr[\mathcal{A}(\mathbf{H}_j) = 1] - \Pr[\mathcal{A}(\mathbf{H}_j^{1,\mathrm{inv}}) = 1]\right| \leq 4\sqrt{\frac{q_Q}{2^m(2^n - j)}}\,.$$

□

Lemma 10. *For $j = 0, \ldots, q_C$,*

$$\mathbf{H}_j^{1,inv} = \mathbf{H}_j^{2,inv}\,.$$

Proof. We bound the distinguishability of $\mathbf{H}_j^{1,\mathrm{inv}}$ and $\mathbf{H}_j^{2,\mathrm{inv}}$.

$$\begin{aligned}
\mathbf{H}_j^{1,\mathrm{inv}}:&\ |E\rangle, R, |E\rangle, \cdots, R, |E\rangle, \mathsf{FX}_K[(E^{(1)})^j], |(E^{(1)})^j\rangle, \mathsf{FX}_K[(E^{(1)})^j], (E^{(1)})^j, \cdots\\
\mathbf{H}_j^{2,\mathrm{inv}}:&\ |E\rangle, R, |E\rangle, \cdots, R, |E\rangle, \mathsf{FX}_K[(E^{(1)})^j], |E^{j+1}\rangle \quad, \mathsf{FX}_K[E^{j+1}], |E^{j+1}\rangle, \cdots.
\end{aligned}$$

To prove $\mathbf{H}_j^{1,\mathrm{inv}}$ and $\mathbf{H}_j^{2,\mathrm{inv}}$ are indistinguishable, it suffices to show that the quantum oracles $(E^{(1)})^j$ and E^{j+1} are identical.

In both $\mathbf{H}_j^{1,\mathrm{inv}}$ and $\mathbf{H}_j^{2,\mathrm{inv}}$, the response to the $(j+1)^{\mathrm{st}}$ classical query is:

$$\begin{aligned}
x_{j+1} &\stackrel{\mathrm{def}}{=} (\mathsf{FX}_K[(E^{(1)})^{T_j,k}])^{-1}(y_{j+1})\\
&= ((E_{k_0}^{(1)})^{T_j,k})^{-1}(y_{j+1} \oplus k_2) \oplus k_1\\
&= \prod_{i=j}^{1} \mathsf{swap}_{x_i \oplus k_1,\, ((E_{k_0}^{(1)})^{T_{i-1},k})^{-1}(y_i \oplus k_2)} \circ (E_{k_0}^{(1)})^{-1}(y_{j+1} \oplus k_2) \oplus k_1\\
&= \prod_{i=j}^{1} \mathsf{swap}_{x_i \oplus k_1,\, (E_{k_0}^{T_{i-1},k})^{-1}(y_i \oplus k_2)} \circ (E_{k_0}^{-1} \circ \mathsf{swap}_{y_{j+1} \oplus k_2,\, s}(y_{j+1} \oplus k_2)) \oplus k_1\\
&= \prod_{i=j}^{1} \mathsf{swap}_{x_i \oplus k_1,\, (E_{k_0}^{T_{i-1},k})^{-1}(y_i \oplus k_2)} \circ E_{k_0}^{-1}(s) \oplus k_1\\
&= (E_{k_0}^{T_j,k})^{-1}(s) \oplus k_1,
\end{aligned}$$

where the fourth equality comes from Proposition 2. By rearranging $s = E_{k_0}^{T_j,k}(x_{j+1} \oplus k_1)$, it follows that for any $y \in \{0,1\}^n$,

$$\begin{aligned}
((E^{(1)})^j)^{-1}(y) &= \prod_{i=j}^{1} \mathsf{swap}_{x_i \oplus k_1,\, ((E_{k_0}^{(1)})^{j-1})^{-1}(y_i \oplus k_2)} \circ E_{k_0}^{-1} \circ \mathsf{swap}_{y_{j+1} \oplus k_2,\, s}(y)\\
&= \prod_{i=j}^{1} \mathsf{swap}_{x_i \oplus k_1,\, (E_{k_0}^{j-1})^{-1}(y_i \oplus k_2)} \circ E_{k_0}^{-1} \circ \mathsf{swap}_{y_{j+1} \oplus k_2,\, s}(y)\\
&= (E^j)^{-1} \circ \mathsf{swap}_{y_{j+1} \oplus k_2,\, E_{k_0}^j(x_{j+1} \oplus k_1)}(y)\\
&= \mathsf{swap}_{x_{j+1} \oplus k_1,\, (E^j)^{-1}(y_{j+1} \oplus k_2)} \circ (E^j)^{-1}(y)\\
&= (E^{j+1})^{-1}(y)
\end{aligned}$$

where the second equality comes from Proposition 2. This concludes the proof that $(E^{(1)})^j \equiv E^{j+1}$. Therefore, hybrids $\mathbf{H}_j^{1,\mathrm{inv}}$ and $\mathbf{H}_j^{2,\mathrm{inv}}$ are perfectly indistinguishable:

$$\mathbf{H}_j^{1,\mathrm{inv}} = \mathbf{H}_j^{2,\mathrm{inv}}\,.$$

□

Lemma 11. *For $j = 0, \ldots, q_C$, $\mathbf{H}_j^{2,inv} = \mathbf{H}_j^3$.*

Proof.

$$\mathbf{H}_j^{2,\mathrm{inv}}: \ |E\rangle, R, |E\rangle, \cdots, R, |E\rangle, \mathsf{FX}_K[(E^{(1)})^j], |E^{j+1}\rangle \quad , \mathsf{FX}_K[E^{j+1}], |E^{j+1}\rangle, \cdots$$
$$\mathbf{H}_j^{3}: \ |E\rangle, R, |E\rangle, \cdots, R, |E\rangle, \qquad R \qquad , |E^{j+1}\rangle \quad , \mathsf{FX}_K[E^{j+1}], |E^{j+1}\rangle, \cdots.$$

We observe that $\mathbf{H}_j^{2,\mathrm{inv}}$ and $\mathbf{H}_j^{3}$ differ only in the response to the $(j+1)^{\mathrm{st}}$ classical query. In $\mathbf{H}_j^{2,\mathrm{inv}}$, this query is answered using

$$x_{j+1} \ = \ (\mathsf{FX}_K[(E^{(1)})^{T_j,K}])^{-1}(y_{j+1}) \ = \ (E_{k_0}^{T_j,K})^{-1}(s) \oplus k_1,$$

as shown in Lemma 4. In contrast, in $\mathbf{H}_j^{3}$ the same query is answered with

$$x_{j+1} \ = \ R^{-1}(y_{j+1}).$$

Using Proposition 1 and following the same strategy as in Lemma 5, we conclude that the two hybrids induce identical distributions on x_{j+1}. Hence, $\mathbf{H}_j^{2,\mathrm{inv}} = \mathbf{H}_j^{3}$.

□

C Detailed Attacks on LRW and XEX2

We provide a detailed description of the attacks on standardized LRW and XEX2, as outlined in Section 5.3.

C.1 Classical Distinguishing Attacks

Birthday Collision Attack As mentioned in Section 1.4, $q = O(2^{n/2})$ queries are required to distinguish LRW (Definition 7) from an ideal tweakable block cipher. The attack is outlined below, given access to a classical oracle:

1. Randomly choose $\tau \in \{0,1\}^n$.
2. Query $\widetilde{O}$ with (m, τ) for $2^{n/2}$ distinct values of m, obtaining pairs (m, c), where c is the response, and store them.
3. Randomly choose $\tau' \in \{0,1\}^n$.
4. Query $\widetilde{O}$ with (m', τ') for $2^{n/2}$ distinct values of m', obtaining pairs (m', c'), where c' is the response, and store them.
5. Find a pair (c, c') such that $m \oplus c = m' \oplus c'$.
6. Based on the construction of h, use the identified pair (c, c') (or multiple such pairs) to distinguish between an ideal tweakable cipher and LRW.

Example. Consider the LRW construction as established in [P1606], where $h_{k'}(\tau) = k' \times_* \tau$. For this construction, the attack proceeds as follows:

1. Perform steps 1–5 twice to obtain two pairs (c_1, c_1') and (c_2, c_2') corresponding to two pairs of tweaks (τ_1, τ_1') and (τ_2, τ_2').
2. Compute $k_1' = (c_1 \oplus c_1') \times_* (\tau_1 \oplus \tau_1')^{-1}$ and similarly $k_2' = (c_2 \oplus c_2') \times_* (\tau_2 \oplus \tau_2')^{-1}$.
3. If $k_1' = k_2'$, output LRW. Otherwise output ideal tweakable cipher.

Analysis of the Algorithm. If $\widetilde{O}$ is LRW, i.e. $\widetilde{O} = \mathsf{LRW}_{k,k'}$, we define $H_{k'}(m, \tau) := m \oplus h_{k'}(\tau)$. Since h is a universal hash function, for all m, τ with a uniformly selected k', $H_{k'}(m, \tau)$ is uniformly distributed. Now, recall that a birthday attack can be applied to $H_{k'}$. Specifically, with $2^{n/2}$ randomly selected inputs, there exists (with overwhelming probability) a pair (m, τ) and (m', τ') such that

$$H_{k'}(m, \tau) = H_{k'}(m', \tau') \quad \Rightarrow \quad m \oplus h_{k'}(\tau) = m' \oplus h_{k'}(\tau').$$

This implies:

$$c \oplus c' = m \oplus m' = h_{k'}(\tau) \oplus h_{k'}(\tau').$$

Substituting $h_{k'}(\tau) = k' \times_* \tau$, we get:

$$c \oplus c' = k' \times_* \tau \oplus k' \times_* \tau'.$$

Using this, we compute the hash key:

$$k' = (c \oplus c') \times_* \tau \oplus \tau')^{-1}.$$

The key k' will always be the same for all such collisions.

If $\widetilde{O}$ is an ideal tweakable cipher, then similarly, by the birthday attack, among $2^{n/2}$ randomly selected inputs, there will exist a collision where:

$$c = \widetilde{P}(m, \tau) = \widetilde{P}(m', \tau') = c'$$

i.e. a collision on the independent random permutations $f_0(\tau) = f_1(\tau')$. However, these collisions do not reveal any structure of k'; instead, the two pairs of ciphertexts and tweaks provide a random guess of k'. Thus, with overwhelming probability, $k'_1 \neq k'_2$.

In conclusion, this classical attack requires $O(2^{n/2})$ queries. This attack bound has been mentioned in several related works [LRW02].

Remark. If $\widetilde{O}$ is XEX2, i.e. $h_{k'}(\tau) = h_{k'}(i, j) = \alpha^j \otimes E_{k'}(2^i)$, we also follow step 1-5 twice for two pairs of tweaks (i, j_1, i, j'_1) and (i, j_2, i, j'_2), obtaining the corresponding ciphertext pairs (c_1, c'_1) and (c_2, c'_2). Using these, we compute $(c_1 \oplus c'_1) \times_* (\alpha^{j_1} \oplus \alpha^{j'_1})^{-1}$ and $(c_2 \oplus c'_2) \times_* (\alpha^{j_2} \oplus \alpha^{j'_2})^{-1}$ and check whether they match. It they do, this value is the candidate for $E_{k'}(2^i)$. Similar arguements work for XEX2.

Even-Mansour Attack Here, we use the fact that LRW with one tweak is an Even-Mansour to construct the distinguishing attack:

1. Randomly choose two tweaks $t, \tau' \in \{0,1\}^n$, and define two oracles

$$P(\cdot) := \widetilde{O}(\cdot, \tau), \quad R(\cdot) := \widetilde{O}(\cdot, \tau').$$

2. Define $f(x) = P(x) \oplus R(x)$. Query $f(\cdot)$ $2^{n/2}$ times and find a collision, i.e., $f(x) = f(x')$.
3. Compute $\widetilde{k} = x \oplus x'$.
4. Randomly select $x^* \in \{0,1\}^n$. Compute $R(x^* \oplus \widetilde{k}) \oplus \widetilde{k}$ and $P(x^*)$.
5. If the two results are equal, output LRW; otherwise, output ideal tweakable cipher.

Analysis of the Algorithm. If $\widetilde{O}$ is LRW, i.e. $\widetilde{O} = \mathsf{LRW}_{k,k'}$, then

$$P(x) = \widetilde{O}(x, \tau) = E_k(x \oplus h_{k'}(\tau)) \oplus h_{k'}(\tau)$$
$$R(x) = \widetilde{O}(x, \widetilde{\tau}) = E_k(x \oplus h_{k'}(\widetilde{\tau})) \oplus h_{k'}(\widetilde{\tau}).$$

We can rewrite $P(x)$ as follows:

$$\begin{aligned} P(x) &= E_k(x \oplus \underline{h_{k'}(\tau) \oplus h_{k'}(\widetilde{\tau})} \oplus h_{k'}(\widetilde{\tau})) \oplus \underline{h_{k'}(\tau) \oplus h_{k'}(\widetilde{\tau})} \oplus h_{k'}(\widetilde{\tau}) \\ &= E_k(x \oplus \widetilde{k} \oplus h_{k'}(\widetilde{\tau})) \oplus \widetilde{k} \oplus h_{k'}(\widetilde{\tau}) \\ &= R(x \oplus \widetilde{k}) \oplus \widetilde{k}, \end{aligned}$$

This shows that P is an Even-Mansour of R. Next, consider

$$\begin{aligned} f(x) &= P(x) \oplus R(x) \\ &= R(x \oplus \widetilde{k}) \oplus \widetilde{k} \oplus R(x) \\ &= R(x \oplus \widetilde{k}) \oplus \widetilde{k} \oplus R(x \oplus \widetilde{k} \oplus \widetilde{k}) \\ &= R(x \oplus \widetilde{k}) \oplus P(x \oplus \widetilde{k}) \\ &= f(x \oplus \widetilde{k}). \end{aligned}$$

This periodicity allows us to use $2^{n/2}$ queries to find a collision on $f(x) = f(x')$. The Even-Mansour key is then computed as $\widetilde{k} = x \oplus x'$. For any $x^* \in \{0,1\}^n$, the Even-Mansour relation between P and R would hold.

If $\widetilde{O}$ is an ideal tweakable cipher, then $P(x)$ and $R(x)$ are independent random permutations of input x. In this case, $f(x) = P(x) \oplus R(x)$ is the XOR of random permutations. While collisions can still be found using $2^{n/2}$ queries, the computed $\widetilde{k}$ is meaningless. For a random x^*, $P(x^*)$ and $R(x^* \oplus \widetilde{k}) \oplus \widetilde{k}$ are independently and uniformly distributed and so will not be equal for overwhelming probability.

We note that this attack works similarly for XEX2.

C.2 Classical Complete Key-Search Attack

1. Randomly select $\tau \in \{0,1\}^n$.
2. Use the classical distinguishing attack described above to recover k' (assuming an appropriate hash function construction).
3. Construct an oracle $E_k(\cdot)$ such that, for an input x, it replies
$$E_k(x) = \mathsf{LRW}_{k,k'}(x \oplus h_{k'}(\tau), \tau) \oplus h_{k'}(\tau).$$
4. Perform an exhaustive search to get key k.

Analysis of the Algorithm. If the tweakable block cipher under investigation is standardized LRW, then in step 2, k' can be computed directly. We then perform an exhaustive search to recover k. Specifically, we first query LRW using a constant number of inputs, such as $(x \oplus h_{k'}(\tau), \tau)$. Then, for each candidate k, we query $E_k(\cdot)$ with the same x values and verify whether the equation from step 3 holds. This process requires a total of $O(2^{n/2})$ online queries and $O(2^m)$ offline queries for complete key recovery.

If the tweakable block cipher under investigation is XEX2, then in step 2, using the ciphertext pair (c, c') with corresponding tweaks $(i, j), (i, j')$, we can compute $E_{k'}(2^i) = (c \oplus c') \times_* (\alpha^j \oplus \alpha^{j'})^{-1}$. Next, we query $E(\cdot, 2^i)$ 2^m times with different candidate values for k'. With high probability $(1 - \frac{1}{2^n})$, we identify the correct tweak key k'^* by verifying that $E(k'^*, 2^i) = (c \oplus c') \times_* (\alpha^j \oplus \alpha^{j'})^{-1}$. Once k' is obtained, we follow a similar process as for LRW to recover k.

Thus, the total number of queries required for complete key recovery remains $O(2^{n/2})$ online queries (plus $O(2^m)$ offline queries).

C.3 Quantum Complete Key Recovery Attack (shorter cipher key)

The best-known attack for quantum complete key search is the Offline-Simon attack [BHNP+19]. Let u be an integer such that $0 \leq u \leq n$. Define the function $F : \{0,1\}^{m+(n-u)} \times \{0,1\}^u \to \{0,1\}^n$ as follows:

$$F(i\|j, x) = E_i(x\|j) \ (i \in \{0,1\}^m, j \in \{0,1\}^{n-u}).$$

Additionally, define the function $g : \{0,1\}^u \to \{0,1\}^n$ as

$$g(x) = \mathsf{LRW}_{k,k'}(x\|0^{n-u}, \tau).$$

Note that $F(k\|h^{(2)}_{k'}(\tau), x) \oplus g(x)$ has the period $h^{(1)}_{k'}(\tau)$ since

$$F(k\|h^{(2)}_{k'}(\tau), x) \oplus g(x) = E_k(x\|h^{(2)}_{k'}(\tau)) \oplus E_k\left((x \oplus h^{(1)}_{k'}(\tau))\|h^{(2)}_{k'}(\tau)\right) \oplus h_{k'(\tau)}.$$

The procedure for recovering k and k' is as follows:

1. Randomly choose $\tau \in \{0,1\}^n$.
2. Run Alg-ExpQ1 on the defined F and g to recover k and $h^{(2)}_{k'}(\tau)$.
3. Use SimQ1 on $f_{k\|h^{(2)}_{k'}(\tau)}$ to recover $h^{(1)}_{k'}(\tau)$.
4. (Verification) Check if $E(k, k')(0^n, \tau) \oplus E_k(h_{k'}(\tau)) = h_{k'}(\tau)$. If the check fails, repeat steps 2–4.
5. Based on construction of hash function h, compute k'.

Analysis of the Algorithm. Similar to the classical case, if the tweakable block cipher under investigation is standardized LRW, k' can be easily computed from $h_{k'}(\tau)$ using $k' = h_{k'}(\tau) \times_* t^{-1}$. So $\widetilde{O}(2^{(n+m)/3})$ queries (with $m \leq 2n$) are required for a complete key search, same as the query complexity of the attack on the FX construction [BHNP+19].

If the tweakable block cipher under investigation is $\mathsf{XEX2}$, then $h_{k'}(\tau) := h_{k'}(i,j) = E_{k'}(2^i) \times \alpha^j$ is recovered from step 2 and 3. As in the classical case, we can query $E(\cdot, 2^i)$ 2^m times with different k' to identify the true key that satisfies the matching condition. Thus, $D = O(2^u)$ classical queries are made to $\mathsf{LRW}_{k,k'}(\cdot,\cdot)$ and $T = O(n^3 2^{(m+n-u)/2} + 2^{m/2}) = O(n^3 2^{(m+n-u)/2})$ offline quantum queries are performed. When $D \leq 2n$, the balance is achieved at at $T = D = \widetilde{O}(2^{(n+m)/3})$.

C.4 Quantum Complete Key Recovery Attack (longer cipher key)

Another possible quantum attack involves combining Grover's algorithm with the Kuwakado-Morii attack [KM12] by treating the Kuwakado-Morii method as a predicate and using Grover's search to find the cipher key k. Detailedly,

1. Fix a key $k \in \{0,1\}^m$.
2. Select $\tau \in \{0,1\}^n$ at random.
3. Choose x_i $(i = 1, \ldots, s)$ from $\{0,1\}^n$ at random, ensuring $x_i \neq x_j$ for $i \neq j$ and $\overline{x_i} \notin \{x_i \mid i = 1, 2, \ldots, s\}$ for any i.
4. For $i = 1, 2, \ldots, s$, compute

$$d_i = \mathsf{LRW}_{k,k'}(\tau, x_i) \oplus \mathsf{LRW}_{k,k'}(\tau, \overline{x_i})$$

   by querying $\mathsf{LRW}_{k,k'}(\cdot,\cdot)$ classically. Then define a set

$$D = \{d_i | i = 1, 2, \ldots, s\}.$$

   Assume all elements in D are distinct for simplicity.
5. Create a table S containing pairs (d_i, x_i), sorted by d_i.
6. Find z such that $L_D(z) = 1$ using the Grover algorithm with the unitary operator V_{L_D}, where $L_D : \{0,1\}^n \to \{0,1\}$ is defined as

$$L_{\mathcal{D}}(x) = \begin{cases} 0 & \text{if } E(k,x) \oplus E(k,\bar{x}) \notin D \\ 1 & \text{if } E(k,x) \oplus E(k,\bar{x}) \in D, \end{cases},$$

   and

$$V_{L_D}|x\rangle = (-1)^{L_D(x)}|x\rangle.$$

7. Compute

$$d = E(k,z) \oplus E(k,\bar{z}),$$

   then find an x from table S such that

$$d = \mathsf{LRW}_{k,k'}(\tau, x) \oplus \mathsf{LRW}_{k,k'}(\tau, \bar{x}).$$

8. Compute $h_{k'}(\tau) = x \oplus z$.
9. Select $x' \in \{0,1\}^n$ at random and obtain $\mathsf{LRW}_{k,k'}(\tau, x')$ by querying $\mathsf{LRW}_{k,k'}(\cdot,\cdot)$ classically.
10. If $E(k,x') \oplus h_{k'}(\tau) \neq \mathsf{LRW}_{k,k'}(\tau, x')$, then set $h_{k'} = \bar{x} \oplus z$.
11. Repeat step 2–10 three times to obtain three pairs: $(\tau_1, h_{k'}(\tau_1))$, $(\tau_2, h_{k'}(\tau_2))$, and $(\tau_3, h_{k'}(\tau_3))$. If $h_{k'}(\tau_1), h_{k'}(\tau_2), h_{k'}(\tau_3)$ are not uniformly distributed, output 1; otherwise, output 0.
12. Treat steps 2–11 as a predicate f, where $f(k) \in \{0,1\}$, and find k such that $f(k) = 1$ using the Grover algorithm with the unitary operator U_f.
13. (Verification) If a valid k is found, compute k' based on the construction of the hash function h and output 1 or 0 accordingly.

Analysis of the Algorithm. This combined attack employs BHT to recover the tweak term $h_{k'}(\tau)$ and Grover's algorithm to find the cipher key k. Therefore, it requires $q_Q = O(2^{m/2} \cdot 2^{n/3}) = O(2^{m/2+n/3})$ quantum queries and $q_C = O(2^{n/3})$ classical queries.

D Post-Quantum Security Proof of LRW in Theorem 5

Theorem 9 (Restatement). *Let LRW be as in Definition 7 and let $\mathcal{A}$ be an adversary making q_C classical queries to its first oracle and $q_Q \geq 1$ quantum queries to its second oracle. Assuming h is XOR-universal and uniform, it holds that in the ideal cipher model,*

$$\left| \Pr_{\substack{k\leftarrow\{0,1\}^m; k'\leftarrow\{0,1\}^\kappa \\ E\leftarrow\mathcal{E}(m,n)}} \left[\mathcal{A}^{\pm \mathsf{LRW}_{k,k'}[E__],|\pm E\rangle} = 1\right] - \Pr_{\substack{\widetilde{\Pi}\leftarrow\mathcal{E}(\mathcal{T},n); \\ E\leftarrow\mathcal{E}(m,n)}} \left[\mathcal{A}^{\pm \widetilde{\Pi},|\pm E\rangle} = 1\right] \right| \leq \frac{6q_C^2}{2^n} + \frac{4}{2^{(m+n)/2}} \left(q_C\sqrt{q_Q} + q_Q\sqrt{q_C}\right).$$

Proof. We adapt a similar hybrid technique to that used in proving the post-quantum security of FX (see Theorem 2) for the case of LRW. Similarly, we assume that all classical queries are made in the forward direction. The inverse queries can be handled in a similar manner as FX. We begin by setting down a way of modifying a given cipher based on a choice of keys and a list of classical queries to an LRW oracle. Let $E \in \mathcal{E}(m,n)$, $K = (k,k') \in \{0,1\}^{m+\kappa}$. Fix a list $\{(\tau_1,x_1,y_1),(\tau_2,x_2,y_2),\ldots,(\tau_{q_C},x_{q_C},y_{q_C})\}$. Each pair (τ_i,x_i,y_i) represents an input–output pair of a classical query. Repeated queries are not allowed. For any $j \leq q_C$, let T_j be the list containing the first j queries.

The "modified cipher" after j-many queries is denoted $E^{T_j,K}$, and is given by

$$E_{k^*}^{T_j,K}(x) = \begin{cases} E_{k^*}(x) & \text{if } k^* \neq k \\ E_k^{T_j,K}(x) & \text{if } k^* = k. \end{cases} \tag{34}$$

where $E_k^{T_j,K}$ is defined as follows. First, define $E^{T_0,k} = E$, and for all $j \in [1,q_C]$,

$$E_k^{T_j,K}(x) = \mathsf{swap}_{E_k^{T_{j-1},K}(x_j\oplus h_{k'}(\tau_j)),\, y_j\oplus h_{k'}(\tau_j)} \circ E_k^{T_{j-1},K}(x). \tag{35}$$

Roughly speaking, $E^{T_j,K}$ is the minimal modification of E that is consistent with the forward ($\rightarrow$) and inverse ($\leftarrow$) queries from the transcript T_j. For compactness, we occasionally write E^j in place of $E^{T_j,K}$ when T_j and K are clear to the context. We also set $E^0 = E$.

We now define the bad event $\mathsf{Bad}_j = \mathsf{Bad}_{j,1} \vee \mathsf{Bad}_{j,2}$, where:

- $\mathsf{Bad}_{j,1}$: A collision occurs in the set $\{x_1 \oplus h_{k'}(\tau_1),\ldots,x_j \oplus h_{k'}(\tau_j)\}$.
- $\mathsf{Bad}_{j,2}$: A collision occurs in the set $\{y_1 \oplus h_{k'}(\tau_1),\ldots,y_j \oplus h_{k'}(\tau_j)\}$.

The probability of the bad event occurring depends on the distributions of E_k, k and T_j. Given the XOR-universality of h and that k' is sampled uniformly at random (after T_j is fixed), the bad event occurs with probability $\Pr[\mathsf{Bad}_j] \leq \frac{j^2}{2^n}$. Conditioned on this event, we derive statements analogous to those in Proposition 1 in the proof of FX.

Proposition 5. *For any $E \in \mathcal{E}(m,n)$, $K = (k,k') \in \{0,1\}^{m+\kappa}$, $j \in \{1,\ldots,q_C\}$, transcript $T_j = \{(x_1,y_1),\ldots,(x_j,y_j)\}$ without repetition, and any $i \in \{1,\ldots,j\}$, if $\neg\mathsf{Bad}_j$,*

$$E_k^{T_j,K}(x_i \oplus h_{k'}(\tau_i)) \oplus h_{k'}(\tau_i) = y_i.$$

Proof. We prove by strong induction on i. We start by the base case $i = j$.

$$E_k^{T_j,K}(x_j \oplus h_{k'}(\tau_j)) = \mathsf{swap}_{E_k^{T_{j-1},K}(x_j\oplus h_{k'}(\tau_j)),\, y_j\oplus h_{k'}(\tau_j)} \circ E_k^{T_{j-1},K}(x_j \oplus h_{k'}(\tau_j)) = y_j \oplus h_{k'}(\tau_j).$$

Assume for all $i \in \{r,\ldots,j\}$ that $E_k^{T_j,K}(x_i \oplus h_{k'}(\tau_i)) \oplus h_{k'}(\tau_i) = y_i$. Expanding it, we obtain

$$\begin{aligned} &E_k^{T_j,K}(x_i \oplus h_{k'}(\tau_i)) \\ &= \mathsf{swap}_{E_k^{T_j,K}(x_j\oplus h_{k'}(\tau_j)),\, y_j\oplus h_{k'}(\tau_j)} \circ \ldots \circ \mathsf{swap}_{E_k^{T_{i-1},K}(x_i\oplus h_{k'}(\tau_i)),\, y_i\oplus h_{k'}(\tau_i)} \circ E_k^{T_{i-1},K}(x_i \oplus h_{k'}(\tau_i)) \\ &= F_i \circ E_k^{T_{i-1},K}(x_i \oplus h_{k'}(\tau_i)) = y_i \oplus h_{k'}(\tau_i), \end{aligned}$$

where we define

$$F_i = \mathsf{swap}_{E_k^{T_j,K}(x_j \oplus h_{k'}(\tau_j)),\, y_j \oplus h_{k'}(\tau_j)} \circ \ldots \circ \mathsf{swap}_{E_k^{T_{i-1},K}(x_i \oplus h_{k'}(\tau_i)),\, y_i \oplus h_{k'}(\tau_i)}.$$

By rearranging, we get for all $i \in \{r, \ldots, j\}$,

$$E_k^{T_{i-1},K}(x_i \oplus h_{k'}(\tau_i)) = F_i^{-1}(y_i \oplus h_{k'}(\tau_i)).$$

We now work on case $r-1$,

$$\begin{aligned}
&E_k^{T_j,K}(x_{r-1} \oplus h_{k'}(\tau_{r-1})) \\
&= \mathsf{swap}_{E_k^{T_{j-1},K}(x_j \oplus h_{k'}(\tau_j)),\, y_j \oplus h_{k'}(\tau_j)} \circ \ldots \circ \mathsf{swap}_{E_k^{T_{r-2},K}(x_{r-1} \oplus h_{k'}(\tau_{r-1})),\, y_{r-1} \oplus h_{k'}(\tau_{r-1})} \\
&\qquad \circ E_k^{T_{r-2},K}(x_{r-1} \oplus h_{k'}(\tau_{r-1})) \\
&= \mathsf{swap}_{E_k^{T_{j-1},K}(x_j \oplus h_{k'}(\tau_j)),\, y_j \oplus h_{k'}(\tau_j)} \circ \ldots \circ \mathsf{swap}_{E_k^{T_{r-1},K}(x_r \oplus h_{k'}(\tau_r)),\, y_r \oplus h_{k'}(\tau_r)}(y_{r-1} \oplus h_{k'}(\tau_{r-1})) \\
&= F_r(y_{r-1} \oplus h_{k'}(\tau_{r-1})).
\end{aligned}$$

We now argue the following two properties:

Property 1: $y_{r-1} \oplus h_{k'}(\tau_{r-1}) \notin \{y_r \oplus h_{k'}(\tau_r), \ldots, y_j \oplus h_{k'}(\tau_j)\}$**.** This follows from the assumption $\neg\mathsf{Bad}_{j,2}$.

Property 2: $y_{r-1} \oplus h_{k'}(\tau_{r-1}) \notin \{E_k^{T_{r-1},K}(x_r \oplus h_{k'}(\tau_r)), \ldots, E_k^{T_{j-1},K}(x_j \oplus h_{k'}(\tau_j))\}$. We prove step by step. First by contradiction, suppose $y_{r-1} \oplus h_{k'}(\tau_{r-1}) = E_k^{T_{r-1},K}(x_r \oplus h_{k'}(\tau_r))$. Then by the inductive assumption, we get

$$\begin{aligned}
y_{r-1} \oplus h_{k'}(\tau_{r-1}) &= F_r^{-1}(y_r \oplus h_{k'}(\tau_r)) \\
F_r(y_{r-1} \oplus h_{k'}(\tau_{r-1})) &= y_r \oplus h_{k'}(\tau_r) \\
E_k^{T_j,K}(x_{r-1} \oplus h_{k'}(\tau_{r-1})) &= E_k^{T_j,K}(x_r \oplus h_{k'}(\tau_r)).
\end{aligned}$$

Since $E_{k_0}^{T_j,K}$ is a permutation, this contradicts the assumption $(\neg\mathsf{Bad}_{j,1})$ that $x_{r-1} \oplus h_{k'}(\tau_{r-1}) \neq x_r \oplus h_{k'}(\tau_r)$. Therefore we have $y_{r-1} \oplus h_{k'}(\tau_{r-1}) \neq E_k^{T_{r-1},K}(x_r \oplus h_{k'}(\tau_r))$. Now, we can write

$$\begin{aligned}
&E_k^{T_j,K}(x_{r-1} \oplus h_{k'}(\tau_{r-1})) \\
&= \mathsf{swap}_{E_k^{T_{j-1},K}(x_j \oplus h_{k'}(\tau_j)),\, y_j \oplus h_{k'}(\tau_j)} \circ \ldots \circ \mathsf{swap}_{E_k^{T_r,K}(x_{r+1} \oplus h_{k'}(\tau_{r+1})),\, y_{r+1} \oplus h_{k'}(\tau_{r+1})}(y_{r-1} \oplus h_{k'}(\tau_{r-1})) \\
&= F_{r+1}(y_{r-1} \oplus h_{k'}(\tau_{r-1})).
\end{aligned}$$

By a similar prove-by-contradiction argument, using the inductive assumption on $r+1$, we obtain

$$y_{r-1} \oplus h_{k'}(\tau_{r-1}) \neq E_k^{T_r,K}(x_{r+1} \oplus h_{k'}(\tau_{r+1})).$$

Repeating this proof by contradiction step by step for $r+2, r+3, \ldots, j$, we eventually reach

$$y_{r-1} \oplus h_{k'}(\tau_{r-1}) \neq E_k^{T_{j-1},K}(x_j \oplus h_{k'}(\tau_j)),$$

which establishes Property 2.

By these two properties, we can get

$$E_k^{T_j,K}(x_{r-1} \oplus h_{k'}(\tau_{r-1})) = y_{r-1} \oplus h_{k'}(\tau_{r-1}).$$

Then by strong induction, the proposition holds for all $i \in \{1, \ldots, j\}$. □

We now define a sequence

$$\mathbf{H}_0, \mathbf{H}_0^1, \mathbf{H}_0^2, \mathbf{H}_0^3, \mathbf{H}_1, \mathbf{H}_1^1, \ldots, \mathbf{H}_{q_C}^3 \tag{36}$$

of hybrid experiments. Each experiment begins with sampling uniform $\widetilde{\Pi} \in \mathcal{E}(\mathcal{T}, n)$ and $E \in \mathcal{E}(m, n)$, and a uniform key pair $K = (k, k') \in \{0,1\}^{m+\kappa}$. The remaining steps of each hybrid are as follows.

Experiment $\mathbf{H}_j$.

1. Run $\mathcal{A}$, answering its classical queries using $\widetilde{\Pi}$ and its quantum queries using E, stopping immediately *before* its $(j+1)^{\text{st}}$ classical query. Let $T_j = \{(\tau_1, x_1, y_1), \ldots, (\tau_j, x_j, y_j)\}$ be the list of classical queries so far.
2. For the remainder of the execution of $\mathcal{A}$, answer its classical queries by $\mathsf{LRW}_K[E^{T_j,K}]$ and its quantum queries by $E^{T_j,k}$.

Experiment $\mathbf{H}_j^1$.

1. Run $\mathcal{A}$, answering its classical queries using $\widetilde{\Pi}$ and its quantum queries using E, until $\mathcal{A}$ makes its $(j+1)^{\text{st}}$ classical query (τ_{j+1}, x_{j+1}).
2. Choose uniform $s \in \{0,1\}^n$, and define $E^{(1)}$ as

$$E^{(1)}_{k^*}(x) = \begin{cases} E_{k^*}(x) & \text{if } k^* \neq k \\ \left(E_k \circ \mathsf{swap}_{x_{j+1} \oplus h_{k'}(\tau_{j+1}),\, s}\right)(x) & \text{if } k^* = k. \end{cases}$$

   Continue running $\mathcal{A}$, answering its remaining classical queries (including the $(j+1)^{\text{st}}$) using $\mathsf{LRW}_K[(E^{(1)})^{T_j,K}]$, and its quantum queries using $(E^{(1)})^{T_j,K}$.

Experiment $\mathbf{H}_j^2$.

1. Run $\mathcal{A}$, answering its classical queries using $\widetilde{\Pi}$ and its quantum queries using E, until $\mathcal{A}$ makes its $(j+1)^{\text{st}}$ classical query (τ_{j+1}, x_{j+1}).
2. Define $E^{(1)}$ as in $\mathbf{H}_j^1$ and answer the $(j+1)^{\text{st}}$ using $\mathsf{LRW}_K[(E^{(1)})^{T_j,K}]$. Denote the response as y_{j+1}, i.e.,

$$y_{j+1} = \mathsf{LRW}_K[(E^{(1)})^j](\tau_{j+1}, x_{j+1}).$$

   Continue running $\mathcal{A}$, answering its remaining classical queries using $\mathsf{LRW}_K[E^{T_{j+1},K}]$, and its quantum queries using $E^{T_{j+1},K}$.

Experiment $\mathbf{H}_j^3$.

1. Run $\mathcal{A}$, answering its classical queries using $\widetilde{\Pi}$ and its quantum queries using E, stopping immediately *after* its $(j+1)^{\text{st}}$ classical query. Let $T_{j+1} = \{(\tau_1, x_1, y_1), \ldots, (\tau_{j+1}, x_{j+1}, y_{j+1})\}$ be the classical queries so far.
2. For the remainder of the execution of $\mathcal{A}$, answer its classical queries using $\mathsf{LRW}_K\left[E^{T_{j+1},K}\right]$ and its quantum queries using $E^{T_{j+1},K}$, i.e. $|E^{j+1}\rangle$.

We can compactly represent $\left\{\mathbf{H}_j, \mathbf{H}_j^1, \mathbf{H}_j^2, \mathbf{H}_j^3, \mathbf{H}_{j+1}\right\}$ as the experiment in which $\mathcal{A}$'s queries are answered using the following oracle sequences. We also define $(E^{(1)})^j$ to denote $(E_k^{(1)})^{T_j,K}$.

$$\begin{aligned}
\mathbf{H}_j &: |E\rangle, \widetilde{\Pi}, |E\rangle, \cdots, \widetilde{\Pi}, |E\rangle, \mathsf{LRW}_K[\ \ E^j\ \ ], |E^j\rangle, \mathsf{LRW}_K\left[E^j\right], |E^j\rangle, \cdots \\
\mathbf{H}_j^1 &: |E\rangle, \widetilde{\Pi}, |E\rangle, \cdots, \widetilde{\Pi}, |E\rangle, \mathsf{LRW}_K[(E^{(1)})^j], |(E^{(1)})^j\rangle, \mathsf{LRW}_K[(E^{(1)})^j], (E^{(1)})^j, \cdots \\
\mathbf{H}_j^2 &: |E\rangle, \widetilde{\Pi}, |E\rangle, \cdots, \widetilde{\Pi}, |E\rangle, \mathsf{LRW}_K[(E^{(1)})^j], |E^{j+1}\rangle, \mathsf{LRW}_K[E^{j+1}], |E^{j+1}\rangle, \cdots \\
\mathbf{H}_j^3 &: |E\rangle, \widetilde{\Pi}, |E\rangle, \cdots, \widetilde{\Pi}, |E\rangle, \widetilde{\Pi}, |E^{j+1}\rangle, \mathsf{LRW}_K[E^{j+1}], |E^{j+1}\rangle, \cdots \\
\mathbf{H}_{j+1} &: \underbrace{|E\rangle, \widetilde{\Pi}, |E\rangle, \cdots, \widetilde{\Pi}, |E\rangle}_{j \text{ classical queries}}, \underbrace{\widetilde{\Pi}, |E\rangle}_{(j+1)^{\text{st}} \text{ classical query}}, \underbrace{\mathsf{LRW}_K[E^{j+1}], |E^{j+1}\rangle, \cdots}_{q_C - j - 1 \text{ classical queries}}.
\end{aligned}$$

Then we establish the following bounds on the distinguishability of $\mathbf{H}_j$ and $\mathbf{H}_{j+1}$, step by step, for $0 \leq j < q_C$:

Lemma 12: $|\Pr[\mathcal{A}(\mathbf{H}_j) = 1 \wedge \neg\mathsf{Bad}_j] - \Pr[\mathcal{A}(\mathbf{H}_j^1) = 1 \wedge \neg\mathsf{Bad}_j]| \leq 4\sqrt{\frac{q_Q}{2^{m+n}}}$

Lemma 13: $|\Pr[\mathcal{A}(\mathbf{H}_j^1) = 1 \wedge \neg\mathsf{Bad}_j] - \Pr[\mathcal{A}(\mathbf{H}_j^2) = 1 \wedge \neg\mathsf{Bad}_j]| \leq \frac{2j}{2^n}$

Lemma 14: $|\Pr[\mathcal{A}(\mathbf{H}_j^2) = 1 \wedge \neg\mathsf{Bad}_j] - \Pr[\mathcal{A}(\mathbf{H}_j^3) = 1 \wedge \neg\mathsf{Bad}_j]| \leq \frac{2j}{2^n}$

Lemma 15: $|\Pr[\mathcal{A}(\mathbf{H}_j^3) = 1 \wedge \neg\mathsf{Bad}_j] - \Pr[\mathcal{A}(\mathbf{H}_{j+1}) = 1 \wedge \neg\mathsf{Bad}_{j+1}]| \leq 2 \cdot q_{Q,j+1}\sqrt{\frac{2(j+1)}{2^{m+n}}}$,

where the last equation, $q_{Q,j+1}$ is the expected number of queries $\mathcal{A}$ makes to P in the $(j+1)^{\text{st}}$ stage.

Using the above, we have

$$\begin{aligned}
&|\Pr[\mathcal{A}(\mathbf{H}_0)=1]-\Pr[\mathcal{A}(\mathbf{H}_{q_C})=1]| \\
&=|\Pr[\mathcal{A}(\mathbf{H}_0)=1]-\Pr[\mathcal{A}(\mathbf{H}_{q_C})=1\wedge\neg\mathsf{Bad}_{q_C}]-\Pr[\mathcal{A}(\mathbf{H}_{q_C})=1\wedge\mathsf{Bad}_{q_C}]| \\
&\le|\Pr[\mathcal{A}(\mathbf{H}_0)=1]-\Pr[\mathcal{A}(\mathbf{H}_{q_C})=1\wedge\neg\mathsf{Bad}_{q_C}]|+|\Pr[\mathsf{Bad}_{q_C}]| \\
&\le\sum_{j=0}^{q_C-1}|\Pr[\mathcal{A}(\mathbf{H}_j)=1\wedge\neg\mathsf{Bad}_j]-\Pr[\mathcal{A}(\mathbf{H}_{j+1})=1\wedge\neg\mathsf{Bad}_{j+1}]|+|\Pr[\mathsf{Bad}_{q_C}]| \\
&\le\sum_{j=0}^{q_C-1}\left(4\sqrt{\frac{q_Q}{2^{m+n}}}+\frac{4j}{2^n}+2\cdot q_{Q,j+1}\sqrt{\frac{2(j+1)}{2^{m+n}}}\right)+\frac{2q_C^2}{2^n} \\
&\le\frac{6q_C^2}{2^n}+\sum_{j=0}^{q_C-1}\left(4\sqrt{\frac{q_Q}{2^{m+n}}}+2\sqrt{2}\cdot q_{Q,j+1}\sqrt{\frac{q_C}{2^{m+n}}}\right) \\
&\le\frac{6q_C^2}{2^n}+\frac{4}{\sqrt{2^{m+n}}}\cdot\left(q_C\sqrt{q_Q}+q_Q\sqrt{q_C}\right),
\end{aligned}$$

which concludes the proof. □

We now prove Lemma 12, Lemma 13, Lemma 14 and Lemma 15.

Lemma 12. *For $j=0,\dots,q_C$,*

$$\left|\Pr[\mathcal{A}(\mathbf{H}_j)=1\wedge \mathit{Bad}_j]-\Pr[\mathcal{A}(\mathbf{H}_j^1)=1\wedge \mathit{Bad}_j]\right|\le 4\sqrt{\frac{q_Q}{2^{n+m}}}.$$

Proof. In this lemma, we bound the distinguishability of $\mathbf{H}_j$ and $\mathbf{H}_j^1$.

$$\begin{aligned}
\mathbf{H}_j:&\ |E\rangle,\widetilde{\Pi},|E\rangle,\cdots,\widetilde{\Pi},|E\rangle,\mathsf{LRW}_K[\quad E^j\quad],|E^j\rangle\qquad,\mathsf{LRW}_K\left[E^j\right],|E^j\rangle,\cdots\\
\mathbf{H}_j^1:&\ |E\rangle,\widetilde{\Pi},|E\rangle,\cdots,\widetilde{\Pi},|E\rangle,\mathsf{LRW}_K[(E^{(1)})^j],|(E^{(1)})^j\rangle\ ,\mathsf{LRW}_K[(E^{(1)})^j],(E^{(1)})^j,\cdots.
\end{aligned}$$

Let $\mathcal{A}$ be a distinguisher between $\mathbf{H}_j$ and $\mathbf{H}_j^1$. We construct from $\mathcal{A}$ a distinguisher $\mathcal{D}$ for the resampling experiment of Lemma 2. Fixing D to be uniform distribution over $\{0,1\}^{m+2n}$ (so $\varepsilon=2^{-(m+2n)}$ in Lemma 2), $\mathcal{D}$ does:

Phase 1: $\mathcal{D}$ is given quantum access to an ideal cipher E. It samples a uniform $\widetilde{\Pi}\leftarrow\mathcal{E}(\mathcal{T},n)$ and then runs $\mathcal{A}$, answering its quantum queries with E and its classical queries with $\widetilde{\Pi}$ (in the appropriate directions), until $\mathcal{A}$ submits its $(j+1)^{\text{st}}$ classical query (τ_{j+1},x_{j+1}). At that point, $\mathcal{D}$ has a list $T_j=\{(\tau_1,x_1,y_1),\dots,(\tau_j,x_j,y_j)\}$ of the queries/answers $\mathcal{A}$ has made to its classical oracle thus far. If Bad_j, then set flag to 1; otherwise, set flag to 0.

Phase 2: $\mathcal{D}$ is given $(k,s_0,s_1)\leftarrow D$ and quantum oracle access to a cipher $E^{(b)}$. Then $\mathcal{D}$ selects the k' conditioned on $h_{k'}(\tau_{j+1})=x_{j+1}\oplus s_0$ (at least one such k' must exist since $\kappa\ge n$), and sets $K=(k,k')$. It then continues running $\mathcal{A}$, answering its remaining classical queries (including the $(j+1)^{\text{st}}$) using $\mathsf{LRW}_K[(E^{(b)})^{T_j,K}]$, and its remaining quantum queries using $(E^{(b)})^{T_j,K}$. If $\mathsf{flag}=1$, $\mathcal{D}$ outputs 0; otherwise, $\mathcal{D}$ outputs whatever $\mathcal{A}$ does.

Note that in phase 1, distinguisher $\mathcal{D}$ perfectly simulates experiments $\mathbf{H}_j$ and $\mathbf{H}_j^1$ for $\mathcal{A}$ until the point where $\mathcal{A}$ makes its $(j+1)^{\text{st}}$ classical query. In phase 2, we now argue that k' is uniformly

distributed. For any $k^* \in \{0,1\}^\kappa$,

$$\begin{aligned}
\Pr_{k':h_{k'}(\tau_{j+1})=x_{j+1}\oplus s_0}[k'=k^*] &= \Pr_{k'\in\{0,1\}^\kappa}[k'=k^*|h_{k'}(\tau_{j+1})=x_{j+1}\oplus s_0] \\
&= \frac{\Pr_{k'\in\{0,1\}^\kappa}[h_{k'}(\tau_{j+1})=x_{j+1}\oplus s_0|k'=k^*]\cdot\Pr_{k'\in\{0,1\}^\kappa}[k'=k^*]}{\Pr_{k'\in\{0,1\}^\kappa}[h_{k'}(\tau_{j+1})=x_{j+1}\oplus s_0]} \\
&= \frac{\Pr_{k'\in\{0,1\}^\kappa}[h_{k'}(\tau_{j+1})=x_{j+1}\oplus s_0|k'=k^*]\cdot\Pr_{k'\in\{0,1\}^\kappa}[k'=k^*]}{\sum_{\widetilde{k}\in\{0,1\}^\kappa}\Pr_{k'\in\{0,1\}^\kappa}[h_{k'}(\tau_{j+1})=x_{j+1}\oplus s_0|k'=\widetilde{k}]\Pr_{\widetilde{k}}[k'=\widetilde{k}]} \\
&= \frac{\Pr_{k'\in\{0,1\}^\kappa}[h_{k'}(\tau_{j+1})=x_{j+1}\oplus s_0|k'=k^*]}{\sum_{\widetilde{k}\in\{0,1\}^\kappa}\Pr_{k'\in\{0,1\}^\kappa}[h_{k'}(\tau_{j+1})=x_{j+1}\oplus s_0|k'=\widetilde{k}]} \\
&= \frac{\Pr[h_{k^*}(\tau_{j+1})=x_{j+1}\oplus s_0]}{\sum_{\widetilde{k}\in\{0,1\}^\kappa}\Pr[h_{\widetilde{k}}(\tau_{j+1})=x_{j+1}\oplus s_0]} \\
&= \frac{1/2^\kappa}{\sum_{\widetilde{k}}1/2^\kappa} \\
&= \frac{1}{2^\kappa}
\end{aligned}$$

where the third equality follows from $\Pr_{k'}[k'=k^*]=\Pr_{k'}[k'=\widetilde{k}]=\frac{1}{2^\kappa}$. The second last equality holds because s_0 is drawn uniformly at random and h is uniform.

If $b=0$ and $\mathsf{flag}=0$, $\mathcal{D}$ gets access to $E^{(0)}=E$ in phase 2. Since $\mathcal{D}$ answers all quantum queries using $\left(E^{(0)}\right)^{T_j,K}$ and all classical queries using $\mathsf{LRW}_K\left[\left(E^{(0)}\right)^{T_j,K}\right]$, we see that $\mathcal{D}$ perfectly simulates $\mathbf{H}_j$ for $\mathcal{A}$ in that case. If, on the other hand, $b=1$ and $\mathsf{flag}=0$ in phase 2, then $\mathcal{D}$ gets access to $E^{(1)}$, where

$$E^{(1)}_{k^*}(x)=\begin{cases}E_{k^*}(x) & \text{if } k^*\neq k\\ E_k\circ\mathsf{swap}_{s_0,\,s_1}(x) & \text{if } k^*=k.\end{cases}$$

Since $h_{k'}(\tau_{j+1}):=s_0\oplus x_{j+1}$, it holds that

$$E^{(1)}_{k^*}(x)=\begin{cases}E_{k^*}(x) & \text{if } k^*\neq k\\ E_k\circ\mathsf{swap}_{x_{j+1}\oplus h_{k'}(\tau_{j+1}),\,s_1}(x) & \text{if } k^*=k.\end{cases}$$

Moreover, the uniformity property of h and the fact that s_0 (and then $s_0\oplus x_{j+1}$) is uniform imply that the joint distribution of k' and $s_0\oplus x_{j+1}$ is equal to the joint distribution of $\widetilde{k}$ and $h_{\widetilde{k}}(\tau_{j+1})$ for a uniform $\widetilde{k}$. Thus, in this case $\mathcal{D}$ perfectly simulates $\mathbf{H}^1_j$ for $\mathcal{A}$. Applying Lemma 2 thus gives

$$\begin{aligned}
&|\Pr[\mathcal{A}(\mathbf{H}_j)=1\wedge\neg\mathsf{Bad}_j]-\Pr[\mathcal{A}(\mathbf{H}^1_j)=1\wedge\neg\mathsf{Bad}_j]| \\
&=|\Pr[\mathcal{D}=1\wedge\mathsf{flag}=0|b=0]-\Pr[\mathcal{D}=1\wedge\mathsf{flag}=0|b=1]| \\
&\leq|\Pr[\mathcal{D}=1|b=0]-\Pr[\mathcal{D}=1|b=1]| \\
&\leq 4\sqrt{2^n\cdot q_Q\cdot\varepsilon} \\
&\leq 4\sqrt{\frac{q_Q}{2^{m+n}}},
\end{aligned}$$

where the first inequality holds due to the independence of $\mathcal{D}$'s output from $\mathcal{A}$'s output when $\mathsf{flag}=1$, and $\Pr[\mathsf{flag}=1]$ being the same for $b=0$ and $b=1$. □

Lemma 13. *For $j=0,\ldots,q_C$,*

$$\left|\Pr[\mathcal{A}(\mathbf{H}^1_j)=1\wedge\neg\mathsf{Bad}_j]-\Pr[\mathcal{A}(\mathbf{H}^2_j)=1\wedge\neg\mathsf{Bad}_j]\right|\leq\frac{2j}{2^n}\,.$$

Proof. Next, we bound the distinguishability of $\mathbf{H}^1_j$ and $\mathbf{H}^2_j$.

$$\begin{aligned}
\mathbf{H}^1_j:&\ |E\rangle\,,\widetilde{\Pi},|E\rangle\,,\cdots,\widetilde{\Pi},|E\rangle\,,\mathsf{LRW}_K[(E^{(1)})^j],|(E^{(1)})^j\rangle\ ,\mathsf{LRW}_K[(E^{(1)})^j],(E^{(1)})^j,\cdots\\
\mathbf{H}^2_j:&\ |E\rangle\,,\widetilde{\Pi},|E\rangle\,,\cdots,\widetilde{\Pi},|E\rangle\,,\mathsf{LRW}_K[(E^{(1)})^j],|E^{j+1}\rangle\quad\ ,\mathsf{LRW}_K[E^{j+1}],|E^{j+1}\rangle\,,\cdots\,.
\end{aligned}$$

We first prove the following proposition.

Proposition 6. *For all $i \in \{1,\dots,j\}$ and all $r \in \{0,\dots,j\}$*

$$(E_k^{(1)})^{T_r,K}(x_i \oplus h_{k'}(\tau_i)) \;=\; E_k^{T_r,K}(x_i \oplus h_{k'}(\tau_i)),$$

when $s \notin \{x_1 \oplus h_{k'}(\tau_1), \cdots x_j \oplus h_{k'}(\tau_j)\}$ and $x_{j+1} \oplus h_{k'}(\tau_{j+1}) \notin \{x_1 \oplus h_{k'}(\tau_1), \cdots x_j \oplus h_{k'}(\tau_j)\}$.

Proof. We will do a proof by induction on r. We start with the base case $r = 0$. By the constraint on s and $x_{j+1} \oplus h_{k'}(\tau_{j+1})$, we have that for all $i \in \{1, \cdots, j\}$

$$\begin{aligned}(E_k^{(1)})^{T_0,K}(x_i \oplus h_{k'}(\tau_i)) &:= E_k^{(1)}(x_i \oplus h_{k'}(\tau_i)) \\ &= E_k \circ \mathsf{swap}_{x_{j+1}\oplus h_{k'}(\tau_{j+1}),\, s}(x_i \oplus h_{k'}(\tau_i)) \\ &= E_k(x_i \oplus h_{k'}(\tau_{j+1})).\end{aligned}$$

Assume for some $r - 1 \geq 0$ that

$$(E_k^{(1)})^{T_{r-1},K}(x_i \oplus h_{k'}(\tau_i)) = E_k^{T_{r-1},K}(x_i \oplus h_{k'}(\tau_i)).$$

Then by the definition,

$$\begin{aligned}(E_k^{(1)})^{T_r,K}(x_i \oplus h_{k'}(\tau_i)) &= \mathsf{swap}_{(E_k^{(1)})^{T_{r-1},K}(x_r\oplus h_{k'}(\tau_r)),\, y_r\oplus h_{k'}(\tau_r)} \circ (E_k^{(1)})^{T_{r-1},K}(x_i \oplus h_{k'}(\tau_i)) \\ &= \mathsf{swap}_{E_k^{T_{r-1},K}(x_r\oplus h_{k'}(\tau_r)),\, y_r\oplus h_{k'}(\tau_r)} \circ E_k^{T_{r-1},K}(x_i \oplus h_{k'}(\tau_i)) \\ &= E_k^{T_r,K}(x_i \oplus h_{k'}(\tau_i)).\end{aligned}$$

By induction, the proposition holds for all $r \in \{0,\dots,j\}$. □

In particular, for all $i \in \{1,\dots,j\}$,

$$(E_k^{(1)})^{T_{i-1},K}(x_i \oplus h_{k'}(\tau_i)) = E_{k_0}^{T_{i-1},K}(x_i \oplus h_{k'}(\tau_i)).$$

To analyze the distinguishability between $\mathbf{H}_j^1$ and $\mathbf{H}_j^2$, it suffices to examine the distinguishability between the quantum oracles $(E^{(1)})^j$ and E^{j+1}. We begin under the constraint that

- $s \notin \{x_1 \oplus h_{k'}(\tau_1), \dots, x_j \oplus h_{k'}(\tau_j)\}$
- $x_{j+1} \oplus h_{k'}(\tau_{j+1}) \notin \{x_1 \oplus h_{k'}(\tau_1), \dots, x_j \oplus h_{k'}(\tau_j)\}$.

In this case, the response to the $(j+1)^{\text{st}}$ classical query is identical in both $\mathbf{H}_j^1$ and $\mathbf{H}_j^2$:

$$\begin{aligned}y_{j+1} &\stackrel{\text{def}}{=} \mathsf{LRW}_K[(E^{(1)})^{T_j,K}](\tau_{j+1}, x_{j+1}) \\ &= (E_k^{(1)})^{T_j,K}(x_{j+1} \oplus h_{k'}(\tau_{j+1})) \oplus h_{k'}(\tau_{j+1}) \\ &= \mathsf{swap}_{(E_k^{(1)})^{T_{j-1},K}(x_j\oplus h_{k'}(\tau_j)),\, y_j\oplus h_{k'}(\tau_j)} \circ (E_k^{(1)})^{T_{j-1},K}(x_{j+1} \oplus h_{k'}(\tau_{j+1})) \oplus h_{k'}(\tau_{j+1}) \\ &= \left(\prod_{i=j}^{1} \mathsf{swap}_{(E_k^{(1)})^{T_{i-1},K}(x_i\oplus h_{k'}(\tau_i)),\, y_i\oplus h_{k'}(\tau_i)}\right) \circ E_k^{(1)}(x_{j+1} \oplus h_{k'}(\tau_{j+1})) \oplus h_{k'}(\tau_{j+1}) \\ &= \left(\prod_{i=j}^{1} \mathsf{swap}_{(E_k)^{T_{i-1},K}(x_i\oplus h_{k'}(\tau_i)),\, y_i\oplus h_{k'}(\tau_i)}\right) \circ E_k(s) \oplus h_{k'}(\tau_{j+1}) \\ &= E_k^{T_j,K}(s) \oplus h_{k'}(\tau_{j+1}).\end{aligned}$$

By rearranging $s = \left(E_{k_0}^{T_j,K}\right)^{-1}(y_{j+1} \oplus h_{k'}(\tau_{j+1}))$. It follows that for any $x \in \{0,1\}^n$,

$$\begin{aligned}&(E^{(1)})^j(x) \\ &= \mathsf{swap}_{(E_k^{(1)})^{j-1}(x_j\oplus h_{k'}(\tau_j)),\, y_j\oplus h_{k'}(\tau_j)} \circ \cdots \circ \mathsf{swap}_{E_k^{(1)}(x_1\oplus h_{k'}(\tau_1)),\, y_1\oplus h_{k'}(\tau_1)} \\ &\qquad \circ E_k \circ \mathsf{swap}_{x_{j+1}\oplus h_{k'}(\tau_{j+1}),\, s}(x) \\ &= \mathsf{swap}_{E_k^{j-1}(x_j\oplus h_{k'}(\tau_j)),\, y_j\oplus h_{k'}(\tau_j)} \circ \cdots \circ \mathsf{swap}_{E_k(x_1\oplus h_{k'}(\tau_1)),\, y_1\oplus h_{k'}(\tau_1)} \circ E_k \circ \mathsf{swap}_{x_{j+1}\oplus h_{k'}(\tau_{j+1}),\, s}(x) \\ &= E^j \circ \mathsf{swap}_{x_{j+1}\oplus h_{k'}(\tau_{j+1}),\, (E^j)^{-1}(y_{j+1}\oplus h_{k'}(\tau_{j+1}))}(x) \\ &= \mathsf{swap}_{E^j(x_{j+1}\oplus h_{k'}(\tau_{j+1})),\, y_{j+1}\oplus h_{k'}(\tau_{j+1})} \circ E^j(x) \\ &= E^{j+1}(x),\end{aligned}$$

where the second equality comes from Proposition 6. Under these constraints, we have $(E^{(1)})^j \equiv E^{j+1}$, making the hybrids $\mathbf{H}_j^1$ and $\mathbf{H}_j^2$ perfectly indistinguishable. We then introduce the constraints Bad_j, which is independent of the new constraints on s and $x_{j+1} \oplus h_{k'}(\tau_{j+1})$ and has the same probability in two hybrids. Thus, these constraints do not affect the perfect indistinguishability. To bound the distinguishability of the hybrids with $\neg\mathsf{Bad}_j$, we analyze the probability of these new constraints occurring:

$$\begin{aligned}
&\left|\Pr[\mathcal{A}(\mathbf{H}_j^1) = 1 \wedge \neg\mathsf{Bad}_j] - \Pr[\mathcal{A}(\mathbf{H}_j^2) = 1 \wedge \neg\mathsf{Bad}_j]\right| \\
&\leq \left|\Pr[\mathcal{A}(\mathbf{H}_j^1) = 1] - \Pr[\mathcal{A}(\mathbf{H}_j^2) = 1]\right| \\
&\leq \Pr[s \in S] + \Pr[x_{j+1} \oplus h_{k'}(\tau_{j+1}) \in S] \\
&= \frac{2j}{2^n},
\end{aligned}$$

where $S = \{x_1 \oplus h_{k'}(\tau_1), \ldots, x_j \oplus h_{k'}(\tau_j)\}$. Since s is uniformly distributed over $\{0,1\}^n$, the probability of the first term is $\frac{j}{2^n}$. For the second term,

$$x_{j+1} \oplus h_{k'}(\tau_{j+1}) \in S \;\;\Rightarrow\;\; \bigcup_{i=1}^{j} \left\{ h_{k'}(\tau_{j+1}) \oplus h_{k'}(\tau_i) = x_{j+1} \oplus x_i \right\},$$

and by the XOR-universality of h, this occurs with probability $\frac{j}{2^n}$. □

Lemma 14. *For $j = 0, \ldots, q_C$,*

$$\left|\Pr[\mathcal{A}(\mathbf{H}_j^2) = 1 \wedge \mathit{Bad}_j] - \Pr[\mathcal{A}(\mathbf{H}_j^3) = 1 \wedge \mathit{Bad}_j]\right| \leq \frac{2j}{2^n}\,.$$

Proof. We bound the distinguishability of $\mathbf{H}_j^2$ and $\mathbf{H}_j^3$.

$$\begin{aligned}
\mathbf{H}_j^2 :&\;\; |E\rangle, \widetilde{\Pi}, |E\rangle, \cdots, \widetilde{\Pi}, |E\rangle, \mathsf{LRW}_K[(E^{(1)})^j], |E^{j+1}\rangle, \mathsf{LRW}_K[E^{j+1}], |E^{j+1}\rangle, \cdots \\
\mathbf{H}_j^3 :&\;\; |E\rangle, \widetilde{\Pi}, |E\rangle, \cdots, \widetilde{\Pi}, |E\rangle, \qquad \widetilde{\Pi} \qquad, |E^{j+1}\rangle, \mathsf{LRW}_K[E^{j+1}], |E^{j+1}\rangle, \cdots.
\end{aligned}$$

We observe that $\mathbf{H}_j^2$ and $\mathbf{H}_j^3$ differ only in the response to the $(j+1)^{\text{st}}$ classical query. In $\mathbf{H}_j^2$, as specified in Lemma 13, under the constraint

- $s \notin \{x_1 \oplus h_{k'}(\tau_1), \ldots, x_j \oplus h_{k'}(\tau_j)\}$,
- $x_{j+1} \oplus h_{k'}(\tau_{j+1}) \notin \{x_1 \oplus h_{k'}(\tau_1), \ldots, x_j \oplus h_{k'}(\tau_j)\}$,

the $(j+1)$-st query is answered as

$$y_{j+1} = \mathsf{LRW}_K\left[(E^{(1)})^{T_j,K}\right](\tau_{j+1}, x_{j+1}) \;=\; E_k^{T_j,K}(s) \oplus h_{k'}(\tau_{j+1}).$$

as shown in Lemma 13. We then introduce the event $\neg\mathsf{Bad}_j$. Recall Proposition 5, under $\neg\mathsf{Bad}_j$, we have

$$y_i \;=\; E_k^{T_j,K}(x_i \oplus h_{k'}(\tau_i)) \oplus h_{k'}(\tau_i), \quad \forall i \in [1, j],$$

and since $s \in \{0,1\}^n \setminus \{x_1 \oplus h_{k'}(\tau_1), \ldots, x_j \oplus h_{k'}(\tau_j)\}$, it follows that in $\mathbf{H}_j^2$,

$$y_{j+1} = E_k^{T_j,K}(s) \oplus h_{k'}(\tau_{j+1}) \in \{0,1\}^n \setminus \{y_1 \oplus h_{k'}(\tau_1) \oplus h_{k'}(\tau_{j+1}), \ldots, y_j \oplus h_{k'}(\tau_j) \oplus h_{k'}(\tau_{j+1})\}.$$

Moreover, because $E_k^{T_j,K}$ is a permutation, the mapping

$$x_i \oplus h_{k'}(\tau_i) \;\mapsto\; y_i = E_k^{T_j,K}(x_i \oplus h_{k'}(\tau_i)) \oplus h_{k'}(\tau_i)$$

is injective. Since s is chosen uniformly from $\{0,1\}^n \setminus \{x_1 \oplus h_{k'}(\tau_1), \ldots, x_j \oplus h_{k'}(\tau_j)\}$, $E_k^{T_j,K}(s)$ is uniformly distributed over

$$\{0,1\}^n \setminus \{E_k^{T_j,K}(x_1 \oplus h_{k'}(\tau_1)), \ldots, E_k^{T_j,K}(x_j \oplus h_{k'}(\tau_j))\} = \{0,1\}^n \setminus \{y_1 \oplus h_{k'}(\tau_1), \ldots, y_j \oplus h_{k'}(\tau_j)\}.$$

It follows that the output y_{j+1} is uniformly distributed over $\{0,1\}^n \setminus \{y_1 \oplus h_{k'}(\tau_1) \oplus h_{k'}(\tau_{j+1}), \ldots, y_j \oplus h_{k'}(\tau_j) \oplus h_{k'}(\tau_{j+1})\}$ in $\mathbf{H}_j^2$.

In contrast, in $\mathbf{H}_j^3$ the same query is answered with

$$y_{j+1} \;=\; \widetilde{\Pi}(\tau_{j+1}, x_{j+1}).$$

Next, we conduct a case-by-case analysis to demonstrate that y_{j+1} has the same distribution conditioned on all previous queries is identical in both $\mathbf{H}_j^2$ and $\mathbf{H}_j^3$.

- **Case** $\tau_{j+1} \notin \{\tau_1, \ldots, \tau_j\}$. In $\mathbf{H}_j^2$, since h is XOR-universal, for all $i \in [1, j]$, the value $h_{k'}(\tau_i) \oplus h_{k'}(\tau_{j+1})$ is uniformly distributed over $\{0,1\}^n$. Consequently, y_{j+1} is uniformly distributed over $\{0,1\}^n$. In $\mathbf{H}_j^3$, as τ_{j+1} is new, $\widetilde{\Pi}_{\tau_{j+1}}$ represents a fresh permutation, and thus $y_{j+1} = \widetilde{\Pi}_{\tau_{j+1}}(x_{j+1})$ is uniformly distributed over $\{0,1\}^n$.
- **Case** $\tau_{j+1} \in \{\tau_1, \ldots, \tau_j\}$. Assume $\tau_{j+1} = \tau_a$ for some $a \in [1, j]$. In $\mathbf{H}_j^2$, we have $y_{j+1} \neq y_a \oplus h_{k'}(\tau_a) \oplus h_{k'}(\tau_a) = y_a$. For the remaining elements, since h is XOR-universal, they are uniformly distributed over $\{0,1\}^n$. Thus, y_{j+1} is uniformly distributed over $\{0,1\}^n \setminus \{y_a\}$. In $\mathbf{H}_j^3$, note that repeated queries are not permitted, so $x_{j+1} \neq x_a$. Therefore, $y_{j+1} = \widetilde{\Pi}_a(x_{j+1}) \neq \widetilde{\Pi}_a(x_a) = y_a$. Consequently, y_{j+1} is also uniformly distributed over $\{0,1\}^n \setminus \{y_a\}$. We note that τ_{j+1} may equal multiple elements in $\{\tau_1, \ldots, \tau_j\}$, but the argument still holds.

Moreover, in both $\mathbf{H}_j^2$ and $\mathbf{H}_j^3$, the construction of E^{j+1} follows exactly the same procedure, i.e., from the first $j+1$ classical input–output pairs and E as specified in Equation 35. Consequently, the two hybrids yield identical distributions under constraints described before.

Therefore, the probability with which $\mathcal{A}$ can distinguish $\mathbf{H}_j^2$ and $\mathbf{H}_j^3$ is

$$\begin{aligned}
&|\Pr[\mathcal{A}(\mathbf{H}_j^2) = 1 \wedge \neg \mathsf{Bad}_j] - \Pr[\mathcal{A}(\mathbf{H}_j^3) = 1 \wedge \neg \mathsf{Bad}_j]| \\
&\leq |\Pr[\mathcal{A}(\mathbf{H}_j^2) = 1 | \neg \mathsf{Bad}_j] - \Pr[\mathcal{A}(\mathbf{H}_j^3) = 1 | \neg \mathsf{Bad}_j]| \\
&\leq \Pr[s \in S] + \Pr[x_{j+1} \oplus h_{k'}(\tau_{j+1}) \in S] \\
&= \frac{2j}{2^n},
\end{aligned}$$

where $S = \{x_1 \oplus h_{k'}(\tau_1), \ldots, x_j \oplus h_{k'}(\tau_j)\}$. □

Lemma 15. *For $j = 0, \ldots, q_C - 1$,*

$$\Pr[\mathcal{A}(\mathbf{H}_j^3) = 1 \wedge \mathit{Bad}_j] - \Pr[\mathcal{A}(\mathbf{H}_{j+1}) = 1 \wedge \mathit{Bad}_{j+1}]| \leq 2 \cdot q_{Q,j+1} \sqrt{\frac{2(j+1)}{2^{m+n}}},$$

where $q_{Q,j+1}$ is the expected number of queries $\mathcal{A}$ makes to P in the $(j+1)^{st}$ stage in the ideal world (i.e., in $\mathbf{H}_{q_C}$).

Proof. Let $\mathcal{A}$ be a distinguisher between $\mathbf{H}_j^3$ and $\mathbf{H}_{j+1}$. We construct from $\mathcal{A}$ a distinguisher $\mathcal{D}$ for the experiment from Lemma 1:

Phase 1: $\mathcal{D}$ samples uniform $\widetilde{\Pi} \in \mathcal{E}(\mathcal{T}, n)$ and $E \in \mathcal{E}(m, n)$. It then runs $\mathcal{A}$, answering its quantum queries using E and its classical queries using $\widetilde{\Pi}$, until after it responds to $\mathcal{A}$'s $(j+1)^{\text{st}}$ classical query. If Bad_{j+1}, set $\mathsf{flag} = 1$; otherwise, set $\mathsf{flag} = 0$. Let $T_{j+1} = \{(\tau_1, x_1, y_1), \ldots, (\tau_{j+1}, x_{j+1}, y_{j+1})\}$ be the list of input/output pairs $\mathcal{A}$ received from its classical oracle thus far. $\mathcal{D}$ defines $F(a, K^*, x) := E_{k^*}^a(x)$ for $a \in \{1, -1\}$. It also define the following randomized algorithm $\mathcal{B}$: sample $K \leftarrow \{0,1\}^m \times \{0,1\}^\kappa$ and then compute the blinded set B to be the input/output pairs that are reprogrammed so that $F^{(B)}(a, K^*, x) = \left(E_{k^*}^{T_{j+1}, K}\right)^a(x)$ for all a, K^*, x, i.e.,

$$B = \left\{((a, K^*, x), \left(E_{k^*}^{T_{j+1}, K}\right)^a(x))\right\}.$$

Phase 2: $\mathcal{B}$ is run to generate B and $\mathcal{D}$ is given quantum access to an oracle F_b. $\mathcal{D}$ resumes running $\mathcal{A}$, answering its quantum queries using F_b. Phase 2 ends when $\mathcal{A}$ makes its next (i.e., $((j+2)^{\text{nd}}$) classical query.

Phase 3: $\mathcal{D}$ is given the randomness used by $\mathcal{B}$ to generate K. It resumes running $\mathcal{A}$, answering its classical queries using $\mathsf{LRW}_K\left[E^{T_{j+1},K}\right]$ and its quantum queries using $E^{T_{j+1},K}$. Finally, if $\mathsf{flag}=1$, $\mathcal{D}$ outputs 0; otherwise, it outputs whatever $\mathcal{A}$ outputs.

It is immediate that if $b=0$ and $\mathsf{flag}=0$ (i.e., $\mathcal{D}$'s oracle in phase 2 is $F_0=F$), then $\mathcal{A}$'s output is identically distributed to its output in $\mathbf{H}_{j+1}$, whereas if $b=1$ (i.e., $\mathcal{D}$'s oracle in phase 2 is $F_1=F^{(B)}$) and and $\mathsf{flag}=0$, then $\mathcal{A}$'s output is identically distributed to its output in $\mathbf{H}^3_j$. It follows that $|\Pr[\mathcal{A}(\mathbf{H}^3_j)=1]-\Pr[\mathcal{A}(\mathbf{H}_{j+1})=1]|$ is equal to the distinguishing advantage of $\mathcal{D}$ in the reprogramming experiment of Lemma 1. To bound this quantity, we bound the parameter ε and the expected number of queries made by $\mathcal{D}$ in phase 2 (when $F=F_0$.)

The value of ε can be bounded using the definition of $E^{T_{j+1},K}$ and the fact that $F^{(B)}(a,K^*,x)=\left(E^{T_{j+1},K}_{k^*}\right)^a(x)$. Fixing E and T_{j+1}, the probability that any particular input (a,K^*,x) is reprogrammed is at most the probability (over K) that it is in the set

$$\left\{\begin{array}{l}(1,k,x_i\oplus h_{k'}(\tau_i)),\left(1,k,E_k^{-1}\left(y_i\oplus h_{k'}(\tau_i)\right)\right),\\(-1,k,E_k\left(x_i\oplus h_{k'}(\tau_i)\right)),(-1,k,y_i\oplus h_{k'}(\tau_i))\end{array}\right\}_{i=1}^{j+1}.$$

Since $h_{k'}(\tau_i)$ is uniform, taking a union bound gives $\varepsilon\le 2(j+1)/2^{m+n}$.

The expected number of queries made by $\mathcal{D}$ in phase 2 when $F=F_0$ is equal to the expected number of queries made by $\mathcal{A}$ in its $(j+1)^{\text{st}}$ stage in $\mathbf{H}_{j+1}$. Since $\mathbf{H}_{j+1}$ and $\mathbf{H}_{q_C}$ are identical until after the $(j+1)^{\text{st}}$ is complete, this is precisely $q_{Q,j+1}$.

Applying Lemma 1 thus gives

$$\begin{aligned}&|\Pr[\mathcal{A}(\mathbf{H}^3_j)=1\wedge\neg\mathsf{Bad}_j]-\Pr[\mathcal{A}(\mathbf{H}_{j+1})=1\wedge\neg\mathsf{Bad}_{j+1}]|\\&=|\Pr[\mathcal{A}(\mathbf{H}^3_j)=1\wedge\neg\mathsf{Bad}_{j+1}]-\Pr[\mathcal{A}(\mathbf{H}_{j+1})=1\wedge\neg\mathsf{Bad}_{j+1}]|\\&=|\Pr[\mathcal{D}=1\wedge\mathsf{flag}=0|b=0]-\Pr[\mathcal{D}=1\wedge\mathsf{flag}=0|b=1]|\\&\le|\Pr[\mathcal{D}=1|b=0]-\Pr[\mathcal{D}=1|b=1]|\\&\le 2\cdot q_{Q,j+1}\sqrt{\frac{2(j+1)}{2^{m+n}}},\end{aligned}$$

where the first equality arises because the $(j+1)^{\text{st}}$ query is answered identically by $\widetilde{\Pi}$ in both worlds. The first inequality holds due to the independence of $\mathcal{D}$'s output from $\mathcal{A}$'s output when $\mathsf{flag}=1$, and $\Pr[\mathsf{flag}=1]$ being the same for $b=0$ and $b=1$. □

E Quantum Oracle Constructions in the Proof of Theorem 6

We describe how to implement the functions E' and E'^{-1} using a quantum oracle f, given the full descriptions of $P(\cdot)$ and $E(\cdot,\cdot)$. The definitions are:

$$E'(k,\tau)=\begin{cases}P(\tau) & \text{if } f(k)=1,\\ E(k,\tau) & \text{if } f(k)\neq 1,\end{cases}\qquad E'^{-1}(k,\tau)=\begin{cases}P^{-1}(\tau) & \text{if } f(k)=1,\\ E^{-1}(k,\tau) & \text{if } f(k)\neq 1.\end{cases}$$

Using quantum oracle access to $\mathcal{O}_f$, we can construct $\mathcal{O}_{E'}$ and $\mathcal{O}_{E'^{-1}}$. Below is the construction of $\mathcal{O}_{E'}$:

$$\begin{aligned}&|k\rangle|\tau\rangle|y\rangle\\&\xrightarrow{\text{add aux registers}}|k\rangle_1|\tau\rangle_2|y\rangle_3|0\rangle_4|0\rangle_5|0\rangle_6|0\rangle_7\\&\xrightarrow{\mathcal{O}_{E,1,2,7}\mathcal{O}_{P,1,6}X_5\mathcal{O}_{f,1,5}\mathcal{O}_{f,1,4}}|k\rangle|\tau\rangle|y\rangle|f(k)\rangle|\overline{f(k)}\rangle|P(x)\rangle|E(k,\tau)\rangle\\&\xrightarrow{\text{CCNOT}_{6,4,3}}|k\rangle|\tau\rangle|y\oplus(P(\tau)\cdot f(k))\rangle|f(k)\rangle|\overline{f(k)}\rangle|P(x)\rangle|E(k,\tau)\rangle\\&\xrightarrow{\text{CCNOT}_{7,5,3}}|k\rangle|\tau\rangle|y\oplus(P(\tau)\cdot f(k))\oplus(E(k,\tau)\cdot\overline{f(k)})\rangle|f(k)\rangle|\overline{f(k)}\rangle|P(x)\rangle|E(k,\tau)\rangle\\&\xrightarrow{\mathcal{O}_{E,1,2,7}\mathcal{O}_{P,1,6}X_5\mathcal{O}_{f,1,5}\mathcal{O}_{f,1,4}}|k\rangle|\tau\rangle|y\oplus(P(\tau)\cdot f(k))\oplus(E(k,\tau)\cdot\overline{f(k)})\rangle|0\rangle|0\rangle|0\rangle|0\rangle\\&\xrightarrow{\text{drop aux}}|k\rangle|\tau\rangle|y\oplus(P(\tau)\cdot f(k))\oplus(E(k,\tau)\cdot\overline{f(k)})\rangle\end{aligned}$$

The construction of $\mathcal{O}_{E'^{-1}}$ follows the same process, substituting P^{-1} and E^{-1} in place of P and E, respectively:

$$|k\rangle|\tau\rangle|y\rangle \longrightarrow |y \oplus (P^{-1}(\tau)\cdot f(k)) \oplus (E^{-1}(k,\tau)\cdot \overline{f(k)})\rangle\,.$$

F Post-Quantum Lower Bounds for Modes

A summary of applications of the general theorem for block cipher mode post-quantum security is given in Table 3.

Block Cipher Modes	Post-Quantum Security Bound
CBC	$\frac{q_Q^2\ell^2}{2^m} + \frac{q_C^2\ell^2}{2^n}$
ECBC	$\frac{2q_Q^2\ell^2}{2^m} + \frac{4q_C^2\ell^2}{2^n}$
CMAC	$\frac{(q_Q\ell+1)^2}{2^m} + \frac{5(\ell^2+1)q^2}{2^n}$
GCM	$\frac{q_Q^2\ell^2}{2^m} + \frac{(\sigma+q_C+q'_C+1)^2}{2^{n+1}} + \frac{\sigma+q_C+q'_C}{2^{n-1}} + \frac{q'_C(\ell+1)}{2^s}$
GCM-SST	$\frac{q_Q^2\ell^2}{2^m} + \frac{(\sigma+3(q_C+q'_C))^2}{2^{n+1}} + \frac{q'_C\ell}{2^n} + \frac{q'_C}{2^s}$
LRW	$\frac{q_Q^2}{2^m} + \frac{q_C^2}{2^n}$
XEX2	$\frac{q_Q^2}{2^m} + \frac{3q_C^2}{2^n}$

Table 3. Post-quantum security bound of block cipher modes in the QICM. ℓ is the block length for every query. Detailed explanations of the corresponding parameters can be found in Section 6.3.