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
[2] Dept. of Computer Science, Virginia Tech
[3] Dept. of Applied Mathematics and Computer Science, Technical University of Denmark
[4] QuICS, Dept. of Computer Science, University of Maryland

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.

Keywords: post-quantum cryptography, block ciphers, theoretical foundations

1 Introduction

1.1 Background

Block ciphers. A block cipher is a keyed family of efficiently implementable permutations on $\{0,1\}^n$. It is secure if, for a uniformly random key k, the permutation π_k is indistinguishable from a random permutation to adversaries with forward and inverse access. The most well-known block cipher is the Advanced Encryption Standard (AES) [DBN+01], a core component of modern Internet security.

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 (and the block cipher case in particular), as we now 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 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

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

[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.

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

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

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 difficult. Classical techniques are based on transcripts and do not translate to this setting. While Zhandry's compressed oracle [Zha19] offers a formidable replacement of query transcripts, 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 secret key, while the block cipher is a public algorithm. Moreover, correct modeling of the construction oracle is crucial, as many commonly used ciphers are *insecure* under quantum construction queries [KLLN16] but *secure* when only classical queries are allowed [ABKM22].

In this paper, we consider attackers that have quantum access to the ideal cipher but classical-only access to constructions involving the secret key. We refer to this model as the post-quantum model. In previous literature, this model is sometimes called the Q1 model [BHNP+19,HS18,JST21,KLLN16], in contrast with the (unrealistic) Q2 model where all oracles can be queried quantumly.

We summarize our results below and provide a more technical summary later.

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 establishes security for the lightweight cipher PRINCE [BCG+12].

[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.

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 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

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

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 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. $\mathcal{D}$ continues with access to (the possibly modified) E, and eventually outputs a guess b' for b.

We show that the 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 phase-1 queries made by $\mathcal{D}$. The bound is independent of the number of phase-3 queries.

The full technical statement appears in Section 3. Using this lemma and the hybrid technique above, we prove the security of several constructions 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. The formal definition is 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*

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

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.

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

[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].

forward and inverse queries are allowed. In Section 4, we show that

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

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

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 E.

Applications to lightweight ciphers. A relatively straightforward application of lower bound for FX establishes post-quantum security of the PRINCE [BCG+12] cipher in the QICM. Concretely, the security of PRINCE is derived from that of a closely related variant of the FX construction, which we denote by $\widetilde{\mathsf{FX}}$ and define formally in Section 4.3. The post-quantum security of $\widetilde{\mathsf{FX}}$ then follows directly from the same security for FX, as in Section 4.3.

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 4.3, 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:*

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

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.

We remark that while Theorem 1 applies to FX, LRW, and XEX2 in the ideal cipher model, our hybrid-based analysis yields significantly tighter bounds.

1.4 Related Work

We review related work on post-quantum (Q1-model) security of keyed symmetric ciphers, focusing first on lower bounds and then on attacks. Since our results concern query lower bounds, we distinguish between offline computation time and queries to an "offline primitive" (e.g., a public random permutation), a distinction not always made in cryptanalytic work.

Alagic et al. [ABKM22] proved a tight lower bound for Even-Mansour using the hybrid technique, later extended to tweakable Even–Mansour [ABK+24]. These methods have since been applied to key-alternating Feistel [BBC+25], multi-round Even–Mansour [BEM24], and Ascon [Hos25].

All these ciphers admit attacks that begin with a small number of classical queries, followed by Grover search on the offline primitive to recover the key. Kuwakado and Morii showed that BHT collision finding [BHT97] yields an Even–Mansour key-recovery attack using $O(2^{n/3})$ classical and quantum queries, time, and space [KM12]. Bonnetain et al. improved this via the offline Simon algorithm, matching the query complexity while requiring only 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* $\mathsf{swap}_{a_0,\,a_1} : \mathcal{X} \to \mathcal{X}$ as

$$\mathsf{swap}_{a_0,\,a_1}(x) = \begin{cases} a_{1-b}, & \text{if } x = a_b, \\ x, & \text{otherwise.} \end{cases} \tag{13}$$

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 give a resampling lemma for ideal cipher model, generalizing [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

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

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 ($b = 1$).

4 Post-Quantum Security of FX

4.1 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*

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

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

$$E_{k^*}^{T_j,K}(x) = \begin{cases} E_{k^*}(x) & \text{if } k^* \neq k_0 \\ E_{k_0}^{T_j,K}(x) & \text{if } k^* = k_0. \end{cases} \tag{21}$$

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

$$E_{k_0}^{T_j,K}(x) = \mathsf{swap}_{E_{k_0}^{T_{j-1},K}(x_j\oplus k_1),\, y_j\oplus k_2} \circ E_{k_0}^{T_{j-1},K}(x)\,. \tag{22}$$

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

$$\mathbf{H}_0, \mathbf{H}_0^1, \mathbf{H}_0^2, \mathbf{H}_0^3, \mathbf{H}_1, \mathbf{H}_1^1, \ldots, \mathbf{H}_{q_C}^3 \tag{23}$$

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

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

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

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

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

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

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

$$
\begin{aligned}
&|\Pr[\mathcal{A}(\mathbf{H}_0) = 1] - \Pr[\mathcal{A}(\mathbf{H}_{q_C}) = 1]| \\
&\le \sum_{j=0}^{q_C-1} \left(4\sqrt{\frac{q_Q}{2^m(2^n - j)}} + 2 \cdot q_{Q,j+1}\sqrt{\frac{2(j+1)}{2^{m+n}}}\right) \\
&\le \sum_{j=0}^{q_C-1} \left(4\sqrt{\frac{q_Q}{2^m(2^n - j)}} + 2 \cdot q_{Q,j+1}\sqrt{\frac{2q_C}{2^{m+n}}}\right) \\
&\le \frac{4}{\sqrt{2^m(2^n - q_C + 1)}} \cdot q_C\sqrt{q_Q} + \frac{2}{\sqrt{2^{m+n}}} q_Q\sqrt{q_C}. \qquad (24)
\end{aligned}
$$

□

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 $j = 0, \ldots, q_C$,*

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

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

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

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 $s_1 \in \{0,1\}^n \backslash S^\perp$ 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 $(E^{(1)})^{T_j,K}$, where

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

[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 $\mathcal{K}$.

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

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

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 $\mathbf{H}^1_j$ for $\mathcal{A}$. Applying Lemma 2 thus gives

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

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

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

□

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

Proof.

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

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 $r \in \{0, \ldots, j\}$*

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

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 $i \in \{1, \cdots, j\}$

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

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

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

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 21. 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 $|E^{j+1}\rangle$ 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 $F(a, k_0, x) \coloneqq E_{k_0}^a(x)$ 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 $\mathbf{H}_j^3$. It follows that $|\Pr[\mathcal{A}(\mathbf{H}_j^3) = 1] - \Pr[\mathcal{A}(\mathbf{H}_{j+1}) = 1]|$ 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 $E_{k_0^*}^{T_{j+1},K}$ and the fact that $F^{(B)}(a, k_0^*, x) = \left(E_{k_0^*}^{T_{j+1},K}\right)^a(x)$. 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

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

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 $\varepsilon \leq 2(j+1)/2^{m+n}$.

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.

4.2 Tightness

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. q_C denotes the number of online classical queries and q_Q denotes the number of offline quantum computations.

4.3 Applications

The PRINCE cipher. 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 modeled as a quantum-accessible ideal cipher.

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 (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 a tweakable permutation, where $\widetilde{\Pi}(\tau, \cdot)$ is a random permutation, and $\tau \xleftarrow{\$} \mathcal{T}$.

Remark. Definition 3 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:

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

Definition 4 (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* $x \neq y$*,*

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

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

Definition 5 (Uniformity). *A family of functions* h *is uniform if* $\forall x, y \in \{0,1\}^n$*,*

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

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

Definition 6 (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*

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

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* $\mathit{LRW}^{E,h}_{k,k'}(\tau, x)$ *as* $\mathit{LRW}_{k,k'}(\tau, x)$*, 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* $\mathit{LRW}^{E,h}$ *construction,*

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

where q *is the number of queries to* $\mathit{LRW}_{k,k'}(\cdot, \cdot)$ *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 7 (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* $j \in [0, 2^{20} - 1]$*.*

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.

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.

5.2 Post-Quantum Security of LRW using the Hybrid Technique

Theorem 5. *Let LRW be as in Definition 6 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 the proof for FX (Theorem 2). [9] 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 j^{th} 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]. □

[9] For the complete proof, please refer to the arXiv version of our paper: https://arxiv.org/abs/2510.08725

5.3 Attacks and Tightness

We summarize the best-known attacks on standardized LRW and XEX2:
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 require only $O(2^{n/2})$ online queries, matching the $q_C^2 \cdot 2^{-n}$ term in the security bound.
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 $q_C = O(2^{n/3})$. This matches the offline-Simon's attack trade-off, $q_Q^2 q_C = O(2^{(m+n)/2})$. Alternatively, we can apply Grover's algorithm alone to recover the cipher key and tweak, resulting in $q_Q = O(2^{(m+n)/2})$. The choice of attack depends on whether we prioritize minimizing quantum or classical queries. 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 8 (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 9 (SPRP(-PQ) Security). *Let $E : \{0,1\}^m \times \{0,1\}^n \to \{0,1\}^n$ be an efficient keyed permutation. (PQ) strong pseudorandom permutation security of E is measured by 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 $\mathcal{A}$.

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 the adversary can make to its oracles.

Definition 10. *Let E be the ideal cipher in the quantum ideal cipher model. Let $\mathcal{A}$ be a quantum adversary. The advantage of $\mathcal{A}$ in attacking E is measured by:*

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

For simplicity of presentation, we 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 11. *(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*

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

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*

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

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 $\mathsf{Q2}$ model, in which the adversary can query both of its oracles quantumly.

6.3 Security of Block Cipher Modes

Construction Con. A polynomial-time algorithm, that uses a (black-box) permutation as input to produce a specific construction.
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 success of the adversary $\mathcal{A}$ is quantified by the probability that it achieves a favorable outcome in Exp. The security of the scheme Con is determined by evaluating the maximum advantage achievable by any adversary $\mathcal{A}$. This is expressed as:

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

General Theorem. 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. 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.*

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.

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:*

$$\mathsf{Adv}^{\mathsf{Exp\text{-}PQ\text{-}IC}}_{\mathsf{Con}[E_\_]}(q_C,q_Q) \leq \mathsf{Adv}^{\mathsf{SPRP\text{-}PQ\text{-}IC}}_{E}(q'_C,q_Q) + \delta(q_C) = \frac{q_Q^2}{2^m} + \delta(q_C)$$

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.*

We omit a detailed discussions of Con and Exp here. A comprehensive treatment of their definitions and properties, together with proofs and applications of Theorem 7 and Theorem 8 on multiple block cipher modes, including CBC, ECBC, CMAC, GCM and GCM-SST, are provided in the arXiv version.

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 6, 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:*

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

We analyze the SPRP-PQ security of LRW. Since LRW is built on E, the adversary $\mathcal{A}$ is granted quantum oracle access to $E(\cdot,\cdot)$.

Corollary 4. *Let LRW be as defined in Definition 6. Assuming h is XOR-universal, the post-quantum security of LRW in QICM is given by:*

$$\mathsf{Adv}^{\mathsf{SPRP\text{-}PQ\text{-}IC}}_{\mathsf{LRW}}(q_C, q_Q) \leq \frac{q_Q^2}{2^m} + \frac{q_C^2}{2^n}.$$

Similarly to the classical case, the SPRP-PQ security of XEX2 reduces to that of LRW. Below, we state only a corollary for the security of XEX2 in the QICM, as the plain model case can be obtained in the same way.

Corollary 5. *Let XEX2 be as defined in Definition 7. Then the post-quantum security of XEX2 in QICM is given by:*

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

Proof. Immediate consequence of Theorem 4 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 in Table 2. From the case analysis, the bound in Theorem 5 is typically tighter, with matching attacks. Nonetheless, Theorem 3 and Corollary 4 give a simpler and more general way to derive post-quantum security bounds.

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.

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.

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.

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.

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.

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.

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.

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.

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