The Key-Dependent Message Security of Key-Alternating Feistel Ciphers

Pooya Farshim[1], Louiza Khati[2], Yannick Seurin[2], and Damien Vergnaud[3]

[1] University of York, Department of Computer Science, York, United Kingdom
[2] ANSSI, Paris, France
[3] Sorbonne Université, LIP6, Paris, France and Institut Universitaire de France

Abstract. Key-Alternating Feistel (KAF) ciphers are a popular variant of Feistel ciphers whereby the round functions are defined as $x \mapsto \mathsf{F}(k_i \oplus x)$, where k_i are the round keys and F is a public random function. Most Feistel ciphers, such as DES, indeed have such a structure. However, the security of this construction has only been studied in the classical CPA/CCA models. We provide the first security analysis of KAF ciphers in the key-dependent message (KDM) attack model, where plaintexts can be related to the private key. This model is motivated by cryptographic schemes used within application scenarios such as full-disk encryption or anonymous credential systems.

We show that the four-round KAF cipher, with a single function F reused across the rounds, provides KDM security for a non-trivial set of KDM functions. To do so, we develop a generic proof methodology, based on the H-coefficient technique, that can ease the analysis of other block ciphers in such strong models of security.

1 Introduction

The notion of key-dependent message (KDM) security for block ciphers was introduced by Black, Rogaway, and Shrimpton [5]. It guarantees strong confidentiality of communicated ciphertexts, i.e., the infeasibility of learning anything about plaintexts from the ciphertexts, even if an adversary has access to encryptions of messages that may depend on the secret key. This model captures practical settings where possibly adversarial correlations between the secret key and encrypted data exist, as is for example the case in anonymous credential and disk encryption systems; see [2, 5, 13, 18] and references therein.

Typically, block ciphers are based on well-known iterative structures such as substitution-permutation or Feistel networks. The Feistel network, introduced in the seminal Luby–Rackoff paper [20], is a construction that builds an $(n_1 + n_2)$-bit pseudorandom permutation family from a smaller random function family that takes n_1-bit inputs and gives n_2-bit outputs. The general network is a repetition of a simple network (the one-round Feistel network as shown in Figure 1) based on pseudorandom functions, which can be the same or different for different rounds. Starting from the Luby–Rackoff result that the 3-round Feistel scheme is a pseudorandom permutation [20], Patarin [24] proved that four rounds

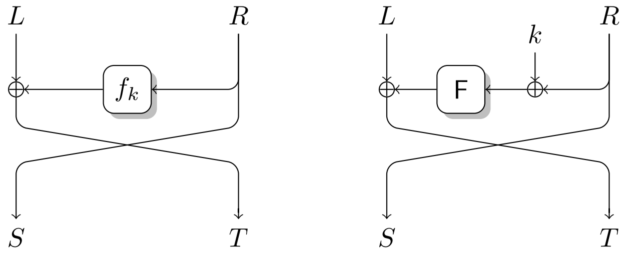

Fig. 1. Round functions of the Feistel network (left) and the KAF network (right).

is indistinguishable from a strong pseudorandom permutation, where chosen-ciphertext attacks (CCAs) are considered. Other analyses gave better bounds for r rounds with $r \geq 4$; see for example [22, 26, 23]. Dai and Steinberger [10] proved that the 8-round Feistel network is indifferentiable from a random permutation, and Barbosa and Farshim gave an analysis in the related-key attack model [3].

Some Feistel networks are *balanced* in that the input is split into two equal-length values L and R and use an n-bit to n-bit round function. For instance, DES and Simon [4] are balanced. Other designs, notably BEAR, LION [1], MISTY [21] and RC6 [17], are unbalanced [16]. Usually, the round functions of a practical block cipher are instantiated with a single public random function and a round key as shown in Figure 1. This design is known as the key-alternating Feistel (KAF) cipher [19] and is of interest due to its practical use cases. For instance, DES is a 16-round balanced KAF where all round functions are identical and where each round key is derived from a master key.

More formally, a KAF cipher is a Feistel network where the i-th round function F_i is instantiated by $\mathsf{F}_i(k_i, x) = f_i(k_i \oplus x)$ where the round functions f_i are public. The KAF construction is said to be idealized when the public functions f_i are modelled as random functions. Lampe and Seurin [19] analyzed the indistinguishability of this construction and proved a security bound up to $2^{\frac{rn}{r+1}}$ for $6r$ rounds using the coupling technique. In these settings the adversary has to distinguish two systems $(\mathsf{KAF}, f_1, \ldots, f_r)$ and $(\mathsf{P}, f_1, \ldots, f_r)$ where f_i are the public random functions and P is a random permutation. They also observed that two rounds of a KAF can be seen as a singly keyed Even–Mansour cipher. Guo and Lin [14] proved that the 21-round KAF* construction, a variant of KAF whereby the key k_i is xored *after* the application of the functions f_i, is indifferentiable from a random permutation. A recent work [15] analyzes the KAF construction with respect to short keys and in a multi-user setting. In the following, we consider only balanced KAFs.

Key-dependent message (KDM) security. As mentioned above, the KDM model gives the adversary the possibility of asking for encryptions of functions ϕ of the encryption key k (without knowing this key). An encryption scheme is said to be KDM secure with respect to some set Φ of functions ϕ mapping keys to messages, if it is secure against an adversary that can obtain encryption of $\phi(k)$ for any function $\phi \in \Phi$. KDM security for symmetric encryption was defined by

Black, Rogaway and Shrimpton [5] and subsequently analyses for both symmetric and asymmetric constructions were done in this model; see, e.g., [5, 13, 6, 7, 2].

The KDM security of the ideal cipher and the Even–Mansour construction [11] were recently analyzed by Farshim, Khati, and Vergnaud [13]. They showed that the ideal cipher is KDM secure with respect to a set Φ of *claw-free* functions, i.e., a set where distinct functions have distinct outputs with high probability when run on a random input. The Even–Mansour (EM) is an iterated block cipher based on public n-bit permutation. Farshim et al. proved that the 1-round EM construction already achieves KDM security under chosen-ciphertext attacks if the set of functions available to the attacker is both claw-free and *offset-free*. The latter property requires that functions do not offset the key by a constant. On the other hand, the 2-round EM construction achieves KDM security if the set of functions available to the attacker is only claw-free (as long as two different permutations are used). To achieve these results, Farshim et al. introduced a so-called *"splitting and forgetting"* technique which is general enough to be applied to other symmetric constructions and/or other security models. Unfortunately, the analysis of KAF with $r \geq 4$ rounds and a unique round function makes this technique difficult to use.

Contributions. In this paper, we provide the first analysis of the KAF in the key-dependent message attack model. To do so, we develop a generic proof strategy, based on the H-coefficient technique of Patarin [24, 25, 28, 9], to analyze the KDM security of block ciphers. We show how to adapt the H-coefficient technique to take KDM queries into account. We show that the 4-round KAF, where the internal functions are reused, is KDM secure for KDM sets Φ that are claw-free, offset-free, and *offset-xor free*. The latter property requires that functions do not offset the xor of two round keys by a constant. Although our security proofs are somewhat intricate, they still simplify the *"splitting and forgetting"* technique of [13].

In order to allow a convenient application of the H-coefficient technique when proving the KDM security of a block cipher, we introduce an intermediate world (in addition to the classical ideal world and real world), that we call the perfect world (pw) which dispenses with the key. We believe this technique (whose game-based analogues appear in [13]) might be of independent interest and can potentially be applied in other settings. In particular, using our techniques we give an arguably simpler proof of the KDM-security of the 1-round EM construction (which was analyzed in [13]) with respect to claw-free and offset-free functions (see Appendix A).

Moreover, we show in Section 5 that if the adversary is only constrained to claw-free functions, it can indeed break the KDM indistinguishability game. We also give sliding KDM attacks on the basic KAF configuration with a single internal public function and either a single or two intervening keys, that *recovers* the key(s) and is adaptable for *any* number of rounds.

2 Preliminaries

Notation. Given an integer $n \geq 1$, the set of all functions from $\{0,1\}^n$ to $\{0,1\}^n$ is denoted $\mathsf{Func}(n)$. We let $\mathbb{N} \coloneqq \{0, 1, \dots\}$ denote the set of non-negative integers, and $\{0,1\}^*$ denote the set of all finite-length bit strings. For two bit strings X and Y, $X|Y$ (or simply XY when no confusion is possible) denotes their concatenation and (X, Y) denotes a uniquely decodable encoding of X and Y. By $x \twoheadleftarrow S$ we mean sampling x uniformly from a finite set S. The cardinality of the set S, i.e., the number of elements in the set S, is denoted $|S|$. We let $L \leftarrow []$ denote initializing a list to empty and $L : X$ denote appending element X to list L. A table T is a list of pairs (x, y), and we write $T(x) \leftarrow y$ to mean that the pair (x, y) is appended to the table. We let $\mathsf{Dom}(T)$ denote the set of values x such that $(x, y) \in T$ for some y and $\mathsf{Rng}(T)$ denote the set of values y such that $(x, y) \in T$ for some x. Given a function F, we let $\mathsf{F}^i(x) \coloneqq \mathsf{F} \circ \cdots \circ \mathsf{F}(x)$ denote the i-th iterate of F. For integers $1 \leq b \leq a$, we will write $(a)_b \coloneqq a(a-1)\cdots(a-b+1)$ and $(a)_0 \coloneqq 1$ by convention. Note that the probability that a random permutation P on $\{0,1\}^n$ satisfies q equations $P(x_i) = y_i$ for distinct x_i's and distinct y_i's is exactly $1/(2^n)_q$.

Block ciphers. Given two non-empty subsets $\mathcal{K}$ and $\mathcal{M}$ of $\{0,1\}^*$, called the key space and the message space respectively, we let $\mathsf{Block}(\mathcal{K}, \mathcal{M})$ denote the set of all functions $\mathsf{E} : \mathcal{K} \times \mathcal{M} \to \mathcal{M}$ such that for each $k \in \mathcal{K}$ the map $\mathsf{E}(k, \cdot)$ is (1) a permutation on $\mathcal{M}$ and (2) length preserving in the sense that for all $p \in \mathcal{M}$ we have that $|\mathsf{E}(k, p)| = |p|$. Such an E uniquely defines its inverse $\mathsf{D} : \mathcal{K} \times \mathcal{M} \to \mathcal{M}$. A block cipher for key space $\mathcal{K}$ and message space $\mathcal{M}$ is a triple of efficient algorithms $\mathrm{BC} \coloneqq (\mathsf{K}, \mathsf{E}, \mathsf{D})$ such that $\mathsf{E} \in \mathsf{Block}(\mathcal{K}, \mathcal{M})$ and its inverse is D. In more detail, K is the randomized key-generation algorithm which returns a key $\mathbf{k} \in \mathcal{K}$. Typically $\mathcal{K} = \{0,1\}^k$ for some $k \in \mathbb{N}$ called the key length, and K endows it with the uniform distribution. Algorithm E is the deterministic enciphering algorithm with signature $\mathsf{E} : \mathcal{K} \times \mathcal{M} \to \mathcal{M}$. Typically $\mathcal{M} = \{0,1\}^n$ for some $n \in \mathbb{N}$ called the block length. (3) D is the deterministic deciphering algorithm with signature $\mathsf{D} : \mathcal{K} \times \mathcal{M} \to \mathcal{M}$. A block cipher is correct in the sense that for all $k \in \mathcal{K}$ and all $p \in \mathcal{M}$ we have that $\mathsf{D}(k, \mathsf{E}(k, p)) = p$. A permutation on $\mathcal{M}$ is simply a block cipher with key space $\mathcal{K} = \{\varepsilon\}$. We denote a permutation with P and its inverse with P^-. A permutation can be trivially obtained from a block cipher (by fixing the key). For a block cipher $\mathrm{BC} \coloneqq (\mathsf{K}, \mathsf{E}, \mathsf{D})$, notation $\mathcal{A}^{\mathrm{BC}}$ denotes oracle access to both E and D for $\mathcal{A}$. We abbreviate $\mathsf{Block}(\{0,1\}^k, \{0,1\}^n)$ by $\mathsf{Block}(k, n)$ and $\mathsf{Block}(\{\varepsilon\}, \{0,1\}^n)$ by $\mathsf{Perm}(n)$.

Key-alternating Feistel (KAF) ciphers. For a given public function $\mathsf{F} \in \mathsf{Func}(n)$ and a key $k \in \{0,1\}^n$, the one-round KAF is the permutation $\mathsf{P} \in \mathsf{Func}(2n)$ defined via

$$\mathsf{P}_k^{\mathsf{F}}(LR) \coloneqq R|\mathsf{F}(k \oplus R) \oplus L \ .$$

The values L and R are respectively the left and right n-bit halves of the input. The left and right n-bit halves of the output are usually denoted S and T

respectively. Given r public functions $\mathsf{F}_1, \mathsf{F}_2, \ldots, \mathsf{F}_r$ and r keys $k_1, k_2, \ldots, k_r$, the r-round KAF is defined as

$$\mathsf{KAF}^{\mathsf{F}_1,\mathsf{F}_2,\ldots,\mathsf{F}_r}_{k_1,k_2,\ldots,k_r}(LR) \coloneqq \mathsf{P}^{\mathsf{F}_r}_{k_r} \circ \cdots \circ \mathsf{P}^{\mathsf{F}_1}_{k_1}(LR) \ .$$

In the following, we write keys $k_1, k_2, \ldots, k_r$ as a key vector $\mathbf{k} = (k_1, k_2, \ldots, k_r)$. When a single public function F is used we write r-round KAF as $\mathsf{KAF}^{\mathsf{F}}_{\mathbf{k}}$.

H-coefficient. The H-coefficient technique [28] was introduced by Patarin and is widely used to prove the security of block cipher constructions such as the Even–Mansour cipher [8] or Feistel schemes [27]. Consider a deterministic adversary $\mathcal{A}$ that takes no input, interacts with a set of oracles w (informally called a *world* or a game), and returns a bit b. We write this interaction as $\mathcal{A}^{\mathsf{w}} \Rightarrow b$. Given two worlds w_0 and w_1, offering the same interfaces, the advantage of $\mathcal{A}$ in distinguishing w_0 and w_1 is defined as

$$\mathbf{Adv}_{\mathsf{w}_0,\mathsf{w}_1}(\mathcal{A}) \coloneqq |\Pr[\mathcal{A}^{\mathsf{w}_0} \Rightarrow 1] - \Pr[\mathcal{A}^{\mathsf{w}_1} \Rightarrow 1]| \ .$$

A transcript τ consists of the list of all query/answer pairs respectively made by the adversary and returned by the oracles. Let $X_{\mathcal{A},\mathsf{w}}$ be the random variable distributed as the transcript resulting from the interaction of $\mathcal{A}$ with world w. A transcript τ is said to be *attainable for $\mathcal{A}$ and* w if this transcript can be the result of the interaction of $\mathcal{A}$ with world w, i.e., when $\Pr[X_{\mathcal{A},\mathsf{w}} = \tau] > 0$.

Lemma 2.1 (H-coefficient). *Let w_0 and w_1 be two worlds and $\mathcal{A}$ be a distinguisher. Let $\mathcal{T}$ be the set of attainable transcripts for $\mathcal{A}$ in w_0, and let $\mathcal{T}_{\text{good}}$ and $\mathcal{T}_{\text{bad}}$ be a partition of $\mathcal{T}$ such that $\mathcal{T} = \mathcal{T}_{\text{good}} \cup \mathcal{T}_{\text{bad}}$. Then if for some ε_{bad}*

$$\Pr[X_{\mathcal{A},\mathsf{w}_0} \in \mathcal{T}_{\text{bad}}] \leq \varepsilon_{\text{bad}} \ ,$$

and for some $\varepsilon_{\text{good}}$ we have that for all $\tau \in \mathcal{T}_{\text{good}}$

$$\frac{\Pr[X_{\mathcal{A},\mathsf{w}_1} = \tau]}{\Pr[X_{\mathcal{A},\mathsf{w}_0} = \tau]} \geq 1 - \varepsilon_{\text{good}} \ ,$$

then $\mathbf{Adv}_{\mathsf{w}_0,\mathsf{w}_1}(\mathcal{A}) \leq \varepsilon_{\text{good}} + \varepsilon_{\text{bad}}$.

For a given transcript $\mathcal{Q}_{\mathsf{F}}$ and a function F, we say that F extends $\mathcal{Q}_{\mathsf{F}}$ and write $\mathsf{F} \vdash \mathcal{Q}_{\mathsf{F}}$ if $v = \mathsf{F}(u)$ for all $(u, v) \in \mathcal{Q}_{\mathsf{F}}$.

3 KDM Security and a Generic Lemma

3.1 Definitions

KDM functions. A key-dependent-message (KDM) function for key space $\mathcal{K}$ and message space $\mathcal{M}$ is a function $\phi : \mathcal{K} \to \mathcal{M}$ computed by a deterministic and stateless circuit. A KDM set Φ is a set of KDM functions ϕ on the same key and message spaces. We let $\Phi_{\mathcal{M}}$ denote the set of all constant KDM functions, i.e., KDM functions ϕ such that for some $x \in \mathcal{M}$ and $\forall\ k \in \mathcal{K}, \phi : k \mapsto x$. We denote such functions by $\phi : k \mapsto x$ and assume that the constant value x can be read-off from (the description of) ϕ. We also assume membership in KDM sets can be efficiently decided. In what follows, even though we work in an idealized model of computation where all parties have access to some oracle O, we do not consider KDM functions computed by circuits with O-oracle gates. We start by defining the following three properties for KDM sets.

Definition 3.1 (Claw-freeness). *Let Φ be a KDM set for key space $\mathcal{K}$ and message space $\mathcal{M}$. The claw-freeness of Φ is defined as*

$$\mathbf{cf}(\Phi) := \max_{\phi_1 \neq \phi_2 \in \Phi} \Pr[k \twoheadleftarrow \mathcal{K} : \phi_1(k) = \phi_2(k)] \ .$$

Definition 3.2 (Offset-freeness). *Fix integers $n, \ell > 0$. Let Φ be a KDM set for key space $\mathcal{K} = (\{0,1\}^n)^\ell$ and message space $\mathcal{M} = \{0,1\}^n$. The offset-freeness of Φ is defined as*

$$\mathbf{of}(\Phi) := \max_{\substack{i \in \{1,\ldots,\ell\} \\ \phi \in \Phi,\, x \in \{0,1\}^n}} \Pr[(k_1, \ldots, k_\ell) \twoheadleftarrow \mathcal{K} : \phi(k_1, \ldots, k_\ell) = k_i \oplus x] \ .$$

Definition 3.3 (Offset-xor-freeness). *Fix integers $n, \ell > 0$. Let Φ be a KDM set for key space $\mathcal{K} = (\{0,1\}^n)^\ell$ and message space $\mathcal{M} = \{0,1\}^n$. The offset-xor-freeness of Φ is defined as*

$$\mathbf{oxf}(\Phi) := \max_{\substack{i \neq j \in \{1,\ldots,\ell\} \\ \phi \in \Phi,\, x \in \{0,1\}^n}} \Pr[(k_1, \ldots, k_\ell) \twoheadleftarrow \mathcal{K} : \phi(k_1, \ldots, k_\ell) = k_i \oplus k_j \oplus x] \ .$$

Example KDM set. One may ask whether or not there are any KDM sets that satisfy the above three conditions. Suppose $\mathcal{K} = \{0,1\}^k$. Let Φ_d be the sets of all functions mapping $(k_1, \ldots, k_\ell)$ to $P(k_1, \ldots, k_\ell)$ where P is a multivariate polynomial over GF(2^k) of total degree at most d, with $\oplus$ being field addition and multiplication defined modulo a fixed irreducible polynomial. We consider a subset of Φ_d consisting of all P such that $P(k_1, \ldots, k_\ell) \oplus k_i$ and $P(k_1, \ldots, k_\ell) \oplus k_i \oplus k_j$ are non-constant for any distinct i and j. Then a direct application of the (multi-variate) Schwartz-Zippel lemma [29] shows that this KDM set satisfies the above three properties, with all advantages upper bounded by $d/2^k$, where d is the total degree of P. Note that this term is negligible for total degree up to $d = 2^{k-\omega(\log k)}$.

KDM security. Consider a block cipher $\mathrm{BC}^{\mathsf{O}} := (\mathsf{K}, \mathsf{E}^{\mathsf{O}}, \mathsf{D}^{\mathsf{O}})$ with key space $\mathcal{K}$ and message space $\mathcal{M}$ based on some ideal primitive O sampled from some oracle space OSp. We formalize security under key-dependent message and chosen-ciphertext attacks (KDM-CCA) as a distinguishing game between two worlds that we call the *real* and *ideal* worlds. Given a KDM set Φ, the adversary $\mathcal{A}$ has access to a KDM encryption oracle KDEnc which takes as input a function $\phi \in \Phi$ and returns a ciphertext $y \in \mathcal{M}$, a decryption oracle Dec which takes as input a ciphertext $y \in \mathcal{M}$ and returns a plaintext $x \in \mathcal{M}$, and the oracle O. We do not allow the adversary to ask for decryption of key-dependent ciphertexts as we are not aware of any use cases where such an oracle is available. In the real world, a key k is drawn uniformly at random from $\mathcal{K}$ and $\textsc{KDEnc}(\phi)$ returns $\mathsf{E}^{\mathsf{O}}(k, \phi(k))$ while $\textsc{Dec}(y)$ returns $\mathsf{D}^{\mathsf{O}}(k, y)$. The ideal world is similar to the real world except that $\mathsf{E}(k, \cdot)$ and $\mathsf{D}(k, \cdot)$ are replaced by a random permutation P and its inverse. To exclude trivial attacks, we do not allow decryption of ciphertexts that were obtained from the encryption oracle and such queries are answered by $\perp$ in both worlds. (Otherwise the key can be recovered by decrypting the encryption of $\phi(k)$ if ϕ is easily invertible.) The real and ideal world are formally defined in Figure 2 (ignore the additional world pw for now). The KDM-CCA advantage of an adversary $\mathcal{A}$ against BC with respect to Φ is defined as

$$\mathbf{Adv}^{\text{kdm-cca}}_{\mathrm{BC}^{\mathsf{O}}}(\mathcal{A}, \Phi) \coloneqq \mathbf{Adv}_{\mathsf{iw},\mathsf{rw}}(\mathcal{A}) \ .$$

Without loss of generality we assume throughout the paper that the adversary does not place repeat queries to its oracles. This is indeed without loss of generality since all oracles are deterministic and repeat queries can be handled by keeping track of queries made so far.

3.2 A generic lemma

In order to allow a convenient application of the H-coefficient technique when proving the KDM security of a block cipher BC^{O}, we introduce an intermediate world, called the perfect world (pw), defined in Figure 2. Note that this world does not involve any key. The encryption and decryption oracles lazily sample two independent random permutations stored respectively in tables T_{enc} and T_{dec}, except that consistency is ensured for constant functions $\phi \in \mathit{\Phi}_{\mathcal{M}}$: when a decryption query $\textsc{Dec}(y)$ is made with $y \notin \mathsf{Dom}(\mathsf{T}_{\text{dec}})$, a plaintext x is sampled from $\mathcal{M} \setminus \mathsf{Rng}(\mathsf{T}_{\text{dec}})$ and the world assigns $\mathsf{T}_{\text{dec}}(y) \coloneqq x$ and $\mathsf{T}_{\text{enc}}(\phi) \coloneqq y$, where ϕ is the constant function $k \mapsto x$.

The following lemma upper-bounds the distinguishing advantage between the ideal and the perfect worlds. It does not depend on the block cipher at hand (neither the ideal nor the perfect world depends on it) nor on the oracle O (since neither in the ideal nor in the perfect world the encryption and decryption oracles depend on it). For specific block ciphers, this allows us to focus on the distinguishing advantage between the perfect and the real worlds, since by the triangular inequality

$$\mathbf{Adv}_{\mathsf{iw},\mathsf{rw}}(\mathcal{A}) \le \mathbf{Adv}_{\mathsf{iw},\mathsf{pw}}(\mathcal{A}) + \mathbf{Adv}_{\mathsf{pw},\mathsf{rw}}(\mathcal{A}) \ . \tag{1}$$

Lemma 3.1. *Let Φ be a KDM set for key space $\mathcal{K}$ and message space $\mathcal{M}$. Let $\mathcal{A}$ be an adversary making at most q queries to* $\textsc{KDEnc}$ *or* $\textsc{Dec}$. *Then*

$$\mathbf{Adv}_{\mathsf{iw},\mathsf{pw}}(\mathcal{A}) \le q^2 \cdot \mathbf{cf}(\Phi) + \frac{q^2}{|\mathcal{M}| - q} \ .$$

Proof. We apply the H-coefficient technique with $\mathsf{w}_0 \coloneqq \mathsf{pw}$ and $\mathsf{w}_1 \coloneqq \mathsf{iw}$. Fix a, without loss of generality, deterministic distinguisher $\mathcal{A}$ making at most q encryption or decryption queries. We assume, without loss of generality, that

```
Game rw    // real
$\mathsf{O} \twoheadleftarrow \mathsf{OSp}$
$k \twoheadleftarrow \mathsf{K}$
$L \leftarrow []$

Proc. KDEnc($\phi$)
if $\phi \notin \Phi$ return $\perp$
$x \leftarrow \phi(k)$
$L \leftarrow L : \{\mathsf{E}^{\mathsf{O}}(k, x)\}$
return $\mathsf{E}^{\mathsf{O}}(k, x)$

Proc. Dec($y$)
if $y \in L$ return $\perp$
else return $\mathsf{D}^{\mathsf{O}}(k, y)$

Proc. $\mathsf{O}(x)$
return $\mathsf{O}(x)$
```

```
Game pw    // perfect
$\mathsf{O} \twoheadleftarrow \mathsf{OSp}$
$\mathsf{T}_{\mathrm{enc}} \leftarrow []; \mathsf{T}_{\mathrm{dec}} \leftarrow []$

Proc. KDEnc($\phi$)
if $\phi \notin \Phi$ return $\perp$
if $\phi \notin \mathsf{Dom}(\mathsf{T}_{\mathrm{enc}})$ then
    $\mathsf{T}_{\mathrm{enc}}(\phi) \twoheadleftarrow \mathcal{M} \setminus \mathsf{Rng}(\mathsf{T}_{\mathrm{enc}})$
return $\mathsf{T}_{\mathrm{enc}}(\phi)$

Proc. Dec($y$)
if $y \in \mathsf{Rng}(\mathsf{T}_{\mathrm{enc}})$ return $\perp$
if $y \notin \mathsf{Dom}(\mathsf{T}_{\mathrm{dec}})$ then
    $x \twoheadleftarrow \mathcal{M} \setminus \mathsf{Rng}(\mathsf{T}_{\mathrm{dec}})$
    $\mathsf{T}_{\mathrm{dec}}(y) \leftarrow x$
    $\mathsf{T}_{\mathrm{enc}}(\phi\colon k \mapsto x) \leftarrow y$
return $\mathsf{T}_{\mathrm{dec}}(y)$

Proc. $\mathsf{O}(x)$
return $\mathsf{O}(x)$
```

```
Game iw    // ideal
$\mathsf{O} \twoheadleftarrow \mathsf{OSp}$
$k \twoheadleftarrow \mathsf{K}; L \leftarrow []$
$\mathsf{P} \twoheadleftarrow \mathsf{Perm}(\mathcal{M})$

Proc. KDEnc($\phi$)
if $\phi \notin \Phi$ return $\perp$
$x \leftarrow \phi(k)$
$L \leftarrow L : \{\mathsf{P}(x)\}$
return $\mathsf{P}(x)$

Proc. Dec($y$)
if $y \in L$ return $\perp$
else return $\mathsf{P}^{-1}(y)$

Proc. $\mathsf{O}(x)$
return $\mathsf{O}(x)$
```

Fig. 2. The real world rw (left) and the ideal world iw (right) defining KDM-CCA security. The intermediate perfect world pw (middle) is used in Lemma 3.1. Here K denotes a key-generation algorithm.

- the adversary never repeats a query;
- the adversary never queries the constant function $\phi : k \mapsto x$ to KDEnc if it has received x as answer to some query Dec(y) before (since in both worlds such a query would be answered by y); and
- the adversary never queries y to Dec if it has received y as answer to some query KDEnc(ϕ) before (since in both worlds such a query would be answered by $\perp$).

We will refer to this as the *no-pointless-query* assumption.

We record the queries of the adversary to oracles KDEnc or Dec in a list $\mathcal{Q}_{\mathrm{BC}}$: it contains all tuples $(+, \phi, y)$ such that $\mathcal{A}$ queried KDEnc(ϕ) and received answer y, and all tuples $(-, x, y)$ such that $\mathcal{A}$ queried Dec(y) and received answer x. The queries of the adversary to oracle O are recorded in a list $\mathcal{Q}_{\mathsf{O}}$. After the adversary has finished querying the oracles, we reveal the key k in case the adversary interacts with the ideal world, while in the perfect world we reveal a uniformly random key independent of the oracle answers. Hence, a transcript is a triple $(\mathcal{Q}_{\mathrm{BC}}, \mathcal{Q}_{\mathsf{O}}, k)$.

Let $\mathcal{T}$ be the set of attainable transcripts for $\mathcal{A}$ and pw. An attainable transcript $\tau = (\mathcal{Q}_{\mathrm{BC}}, \mathcal{Q}_{\mathsf{O}}, k)$ is said to be *bad* iff any of the following holds.

(C-1) there exist $(+, \phi, y) \neq (+, \phi', y') \in \mathcal{Q}_{\mathrm{BC}}$ such that
  (a) $\phi(k) = \phi'(k)$ or
  (b) $y = y'$;

(C-2) there exist $(+, \phi, y), (-, x, y') \in \mathcal{Q}_{\mathrm{BC}}$ such that
  (a) $\phi(k) = x$ or
  (b) $y = y'$;

(C-3) there exist $(-x, y) \neq (-, x', y') \in \mathcal{Q}_{\mathrm{BC}}$ such that
  (a) $x = x'$ or
  (b) $y = y'$.

Let $\mathcal{T}_{\mathrm{bad}}$ denote the set of bad transcripts and let $\mathcal{T}_{\mathrm{good}} \coloneqq \mathcal{T} \setminus \mathcal{T}_{\mathrm{bad}}$. We first upper bound the probability of getting a bad transcript in the perfect world.

Claim. $\Pr[X_{\mathcal{A},\mathsf{pw}} \in \mathcal{T}_{\mathrm{bad}}] \leq q^2 \cdot \mathbf{cf}(\Phi) + q^2/(|\mathcal{M}| - q)$.

Proof. We consider the probability of each condition in turn. Recall that in the perfect world, the key k is drawn at random independently of the oracle answers.

(C-1) Fix two queries $(+, \phi, y) \neq (+, \phi', y') \in \mathcal{Q}_{\mathrm{BC}}$.
  (a) By Definition 3.1, $\phi(k) = \phi'(k)$ with probability at most $\mathbf{cf}(\Phi)$ over the choice of a random key k.
  (b) By the no-pointless-queries assumption, $\phi \neq \phi'$ and hence necessarily $y \neq y'$.

  Summing over all possible pairs, (C-1) happens with probability at most $q^2/2 \cdot \mathbf{cf}(\Phi)$.

(C-2) Fix two queries $(+, \phi, y), (-, x, y') \in \mathcal{Q}_{\mathrm{BC}}$.
  (a) If query $(+, \phi, y)$ came first, then x is uniformly random in a set of size at least $|\mathcal{M}| - q$ and independent of $\phi(k)$. Hence $\phi(k) = x$ with probability at most $1/(|\mathcal{M}| - q)$. If query $(-, x, y')$ came first, then by the no-pointless-query assumption, $\phi \neq (k \mapsto x)$, so that $\phi(k) = x$ with probability at most $\mathbf{cf}(\Phi)$ (otherwise it would constitute a claw with the constant function). All in all, $\phi(k) = x$ with probability at most $1/(|\mathcal{M}| - q) + \mathbf{cf}(\Phi)$.
  (b) If query $(+, \phi, y)$ came first, then by the no-pointless-query assumption $y' \neq y$. If query $(-, x, y')$ came first, then y is uniformly random in a set of size at least $|\mathcal{M}| - q$ and independent of y'. Hence $y = y'$ with probability at most $1/(|\mathcal{M}| - q)$.

  Summing over all possible pairs of queries, (C-2) happens with probability at most $q^2/2 \cdot (2/(|\mathcal{M}| - q) + \mathbf{cf}(\Phi))$.

(C-3) Fix two queries $(-, x, y) \neq (-, x', y') \in \mathcal{Q}_{\mathrm{BC}}$. Then, by the no-pointless-queries assumption, $y \neq y'$ and hence $x \neq x'$, so that condition (C-3) cannot hold.

The result follows by applying the union bound.

Claim. Fix a good transcript $\tau = (\mathcal{Q}_{\mathrm{BC}}, \mathcal{Q}_{\mathsf{O}}, k)$. Then

$$\frac{\Pr[X_{\mathcal{A},\mathsf{iw}} = \tau]}{\Pr[X_{\mathcal{A},\mathsf{pw}} = \tau]} \geq 1 \ .$$

Proof. Let q_{enc}, resp. q_{dec}, denote the number of queries to KDEnc, resp. Dec, in $\mathcal{Q}_{\mathrm{BC}}$ (with $q_{\mathrm{enc}} + q_{\mathrm{dec}} = q$). In the perfect world, queries to KDEnc and Dec are answered by lazily sampling two independent injections $\mathsf{I}_{\mathrm{enc}} \colon [q_{\mathrm{enc}}] \to \mathcal{M}$ and $\mathsf{I}_{\mathrm{dec}} \colon [q_{\mathrm{dec}}] \to \mathcal{M}$. This follows from the no-pointless-queries assumption which implies that for any query KDEnc(ϕ) we have $\phi \notin \mathsf{Dom}(\mathsf{T}_{\mathrm{enc}})$ and for any query Dec(y) we have $y \notin \mathsf{Dom}(\mathsf{T}_{\mathrm{dec}})$. Hence, letting $\mathcal{Q}_{\mathrm{enc}}$ and $\mathcal{Q}_{\mathrm{dec}}$ respectively denote the set of encryption and decryption queries in $\mathcal{Q}_{\mathrm{BC}}$ and K the key-generation algorithm we have

$$\begin{aligned}\Pr[X_{\mathcal{A},\mathsf{pw}} = \tau] &= \Pr_{k' \twoheadleftarrow \mathsf{K}}[k' = k] \cdot \Pr_{\mathsf{O} \twoheadleftarrow \mathsf{OSp}}[\mathsf{O} \vdash \mathcal{Q}_{\mathsf{O}}] \cdot \Pr_{\mathsf{I}_{\mathrm{enc}}}[\mathsf{I}_{\mathrm{enc}} \vdash \mathcal{Q}_{\mathrm{enc}}] \cdot \Pr_{\mathsf{I}_{\mathrm{dec}}}[\mathsf{I}_{\mathrm{dec}} \vdash \mathcal{Q}_{\mathrm{dec}}] \\ &= \Pr_{k' \twoheadleftarrow \mathsf{K}}[k' = k] \cdot \Pr_{\mathsf{O} \twoheadleftarrow \mathsf{OSp}}[\mathsf{O} \vdash \mathcal{Q}_{\mathsf{O}}] \cdot \frac{1}{(|\mathcal{M}|)_{q_{\mathrm{enc}}} \cdot (|\mathcal{M}|)_{q_{\mathrm{dec}}}} \ .\end{aligned}$$

We now compute the probability of obtaining a good transcript τ in the ideal world. Consider the modified transcript $\mathcal{Q}'_{\mathrm{BC}}$ containing pairs $(x, y) \in \mathcal{M}^2$ constructed from $\mathcal{Q}_{\mathrm{BC}}$ as follows. For each triplet $(+, \phi, y) \in \mathcal{Q}_{\mathrm{BC}}$, append $(\phi(k), y)$ to $\mathcal{Q}'_{\mathrm{BC}}$ and for each $(-, x, y) \in \mathcal{Q}_{\mathrm{BC}}$, append (x, y) to $\mathcal{Q}'_{\mathrm{BC}}$. Then, for any $(x, y) \neq (x', y') \in \mathcal{Q}'_{\mathrm{BC}}$, we have $x \neq x'$ (as otherwise condition (C-1a), (C-2a), or (C-3a) would be met) and $y \neq y'$ (as otherwise condition (C-1b), (C-2b), or (C-3b) would be met). Hence,

$$\begin{aligned}\Pr[X_{\mathcal{A},\mathsf{iw}} = \tau] &= \Pr_{k' \twoheadleftarrow \mathsf{K}}[k' = k] \cdot \Pr_{\mathsf{O} \twoheadleftarrow \mathsf{OSp}}[\mathsf{O} \vdash \mathcal{Q}_{\mathsf{O}}] \cdot \Pr_{\mathsf{P} \twoheadleftarrow \mathsf{Perm}(\mathcal{M})}[\mathsf{P} \vdash \mathcal{Q}'_{\mathrm{BC}}] \\ &= \Pr_{k' \twoheadleftarrow \mathsf{K}}[k' = k] \cdot \Pr_{\mathsf{O} \twoheadleftarrow \mathsf{OSp}}[\mathsf{O} \vdash \mathcal{Q}_{\mathsf{O}}] \cdot \frac{1}{(|\mathcal{M}|)_{q}} \ .\end{aligned}$$

Thus,

$$\frac{\Pr[X_{\mathcal{A},\mathsf{iw}} = \tau]}{\Pr[X_{\mathcal{A},\mathsf{pw}} = \tau]} = \frac{(|\mathcal{M}|)_{q_{\mathrm{enc}}} \cdot (|\mathcal{M}|)_{q_{\mathrm{dec}}}}{(|\mathcal{M}|)_{q}} \geq 1 \ ,$$

where the inequality follows from $q_{\mathrm{enc}} + q_{\mathrm{dec}} = q$.

Lemma 3.1 follows by combining the above two claims with Lemma 2.1.

4 Four-Round KAF

In this section we study the 4-round KAF cipher with a single round function $\mathsf{F} \colon \{0,1\}^n \to \{0,1\}^n$ and key $\mathbf{k} = (k_1, k_2, k_3, k_4) \in (\{0,1\}^n)^4$ where k_1 and

k_4 are uniformly random. Our results do not rely on any assumptions on the distributions of k_2 and k_3 (which could be, for example, both set to 0). Given a KDM function ϕ with range $\{0,1\}^{2n}$, we let ϕ_L and ϕ_R to respectively denote the functions that return the n leftmost and the n rightmost bits of ϕ. Given a KDM set Φ for message space $\mathcal{M} = \{0,1\}^{2n}$, we define $\Phi_L \coloneqq \{\phi_L : \phi \in \Phi\}$ and $\Phi_R \coloneqq \{\phi_R : \phi \in \Phi\}$.

The theorem below states that the 4-round KAF with the same round function and uniformly random round keys k_1 and k_4 is KDM-CCA secure if the set Φ of key-dependent functions has negligible claw-freeness (cf. Definition 3.1) and Φ_R has negligible offset-freeness and offset-xor-freeness (cf. Definition 3.2 and Definition 3.3).

Theorem 4.1. *Let $\mathsf{KAF}^{\mathsf{F}}_{\mathbf{k}}$ be the 4-round key-alternating Feistel cipher based on a single round function $\mathsf{F}\colon \{0,1\}^n \to \{0,1\}^n$ where the key $\mathbf{k} = (k_1, k_2, k_3, k_4)$ is such that k_1 and k_4 are uniformly random and independent. Let $\mathcal{A}$ be an adversary making at most $q \leq 2^n$ queries to* KDEnc *or* Dec *and at most q_{f} queries to F, which is modeled as a random oracle. Then,*

$$\mathbf{Adv}^{\text{kdm-cca}}_{\mathsf{KAF}^{\mathsf{F}}_{\mathbf{k}}}(\mathcal{A}, \Phi) \leq q^2 \cdot \big(2 \cdot \mathbf{cf}(\Phi) + 3/2 \cdot \mathbf{oxf}(\Phi_R) + 22/2^n\big) + q q_{\mathrm{f}} \cdot \big(\mathbf{of}(\Phi_R) + 7/2^n\big) \ .$$

Proof. Fix an adversary $\mathcal{A}$ attempting to distinguish the real and ideal worlds defined in Figure 2, where $\mathsf{OSp} \coloneqq \mathsf{Func}(n)$ and $\mathrm{BC} = \mathsf{KAF}^{\mathsf{F}}$. Assume that $\mathcal{A}$ makes at most $q \leq 2^n$ queries to KDEnc or Dec and q_{f} queries to F. By Equation 1 and Lemma 3.1, we have

$$\begin{aligned}\mathbf{Adv}^{\text{kdm-cca}}_{\mathsf{KAF}^{\mathsf{F}}_{\mathbf{k}}}(\mathcal{A}, \Phi) &\leq q^2 \cdot \mathbf{cf}(\Phi) + q^2/(|\mathcal{M}| - q) + \mathbf{Adv}_{\mathsf{pw},\mathsf{rw}}(\mathcal{A}) \\ &\leq q^2 \cdot \mathbf{cf}(\Phi) + q^2/2^n + \mathbf{Adv}_{\mathsf{pw},\mathsf{rw}}(\mathcal{A}) \ ,\end{aligned}$$

where we used that $|\mathcal{M}| = 2^{2n}$ and $1/(2^{2n} - q) \leq 1/2^n$. Hence, it remains to upper bound $\mathbf{Adv}_{\mathsf{pw},\mathsf{rw}}(\mathcal{A})$. We prove below that

$$\mathbf{Adv}_{\mathsf{pw},\mathsf{rw}}(\mathcal{A}) \leq q^2 \cdot \big(\mathbf{cf}(\Phi) + 3/2 \cdot \mathbf{oxf}(\Phi_R) + 21/2^n\big) + q q_{\mathrm{f}} \cdot \big(\mathbf{of}(\Phi_R) + 7/2^n\big) \ , \tag{2}$$

from which the result follows.

The remainder of this section is devoted to the proof of Equation 2. Without loss of generality, we make the same no-pointless-query assumption that we made in the proof of Lemma 3.1. Our proof will use the H-coefficient technique. A transcript τ is a tuple $(\mathcal{Q}_{\mathrm{BC}}, \mathcal{Q}_{\mathsf{F}}, \mathbf{k})$, where $\mathcal{Q}_{\mathrm{BC}}$ is the list of all forward queries $(+, \phi, ST)$, with $\phi \in \Phi$ the query to KDEnc and ST the corresponding answer, together with all backward queries $(-, L'R', S'T')$ with $L'R, S'T' \in (\{0,1\}^n)^2$ and $L'R'$ the answer of Dec when called on $S'T'$. List $\mathcal{Q}_{\mathsf{F}}$ contains queries $(u, v) \in (\{0,1\}^n)^2$ to the public function F, where v is the answer of the oracle F when called on input u. The key $\mathbf{k}$ is only revealed to the adversary after it has finished its queries, and is drawn independently of the oracle answers in the perfect world using the key-generation algorithm K (whose first and fourth components are uniform but not necessarily its second or third components).

We first define bad transcripts and upper bound the probability of obtaining such a transcript in the perfect world. Informally, a transcript is said to be bad if an unexpected collision occurs in the set of all inputs to the *first* or the *fourth* round functions. Note that the adversary can let some inputs collide with probability 1, for example by querying $\textsc{Dec}(ST)$ and $\textsc{Dec}(ST')$; bad transcripts only capture collisions that happen "by chance." We formalize this next.

Definition 4.1. *A transcript $\tau = (\mathcal{Q}_{\mathrm{BC}}, \mathcal{Q}_{\mathsf{F}}, \mathbf{k})$ with $\mathbf{k} = (k_1, k_2, k_3, k_4)$ in the perfect world is said to be* bad *iff any of the following holds.*

(C-1) there exist $(+, \phi, ST) \in \mathcal{Q}_{\mathrm{BC}}$ and $(u, v) \in \mathcal{Q}_{\mathsf{F}}$ such that
(a) $\phi_R(\mathbf{k}) \oplus k_1 = u$ or
(b) $S \oplus k_4 = u$;

(C-2) there exist $(-, LR, ST) \in \mathcal{Q}_{\mathrm{BC}}$ and $(u, v) \in \mathcal{Q}_{\mathsf{F}}$ such that
(a) $R \oplus k_1 = u$ or
(b) $S \oplus k_4 = u$;

(C-3) there exist $(+, \phi, ST) \neq (+, \phi', S'T') \in \mathcal{Q}_{\mathrm{BC}}$ such that
(a) $\phi(\mathbf{k}) = \phi'(\mathbf{k})$ or
(b) $S = S'$;

(C-4) there exist $(+, \phi, ST), (+, \phi', S'T') \in \mathcal{Q}_{\mathrm{BC}}$ (not necessarily distinct) such that $\phi_R(\mathbf{k}) \oplus k_1 = S' \oplus k_4$;

(C-5) there exist $(-, LR, ST) \neq (-, L'R', S'T') \in \mathcal{Q}_{\mathrm{BC}}$ such that $R = R'$;

(C-6) there exist $(-, LR, ST), (-, L'R', S'T') \in \mathcal{Q}_{\mathrm{BC}}$ (not necessarily distinct) such that $R \oplus k_1 = S' \oplus k_4$;

(C-7) there exist $(+, \phi, ST), (-, L'R', S'T') \in \mathcal{Q}_{\mathrm{BC}}$ such that
(a) $\phi(\mathbf{k}) = L'R'$ or
(b) $ST = S'T'$ or
(c) $\phi_R(\mathbf{k}) \oplus k_1 = S' \oplus k_4$ or
(d) $S \oplus k_4 = R' \oplus k_1$.

Let $\mathcal{T}_{\mathrm{bad}}$ denote the set of bad transcripts and let $\mathcal{T}_{\mathrm{good}} \coloneqq \mathcal{T} \setminus \mathcal{T}_{\mathrm{bad}}$.

Lemma 4.1. *Let $\mathcal{A}$ be a distinguisher making at most $q \leq 2^n$ queries to* $\textsc{KDEnc}$ *or* $\textsc{Dec}$ *and q_{f} queries to F. With $\mathcal{T}_{\mathrm{bad}}$ defined as above,*

$$\Pr[X_{\mathcal{A},\mathsf{pw}} \in \mathcal{T}_{\mathrm{bad}}] \leq q^2 \cdot (\mathbf{cf}(\Phi) + 3/2 \cdot \mathbf{oxf}(\Phi_R) + 6/2^n) + q q_{\mathrm{f}} \cdot (\mathbf{of}(\Phi_R) + 3/2^n) \ .$$

Proof. We compute the probability of each condition in turn. Recall that in pw, the key $\mathbf{k} = (k_1, k_2, k_3, k_4)$ is drawn at random and independently of all oracle answers at the end.

(C-1) Fix an encryption query $(+, \phi, ST) \in \mathcal{Q}_{\mathrm{BC}}$ and a query to the public function $(u, v) \in \mathcal{Q}_{\mathsf{F}}$.
(a) By Definition 3.2, $\phi_R(\mathbf{k}) = k_1 \oplus u$ with probability at most $\mathbf{of}(\Phi_R)$;
(b) Since k_4 is uniformly random and independent of the query transcript, $k_4 = S \oplus u$ with probability at most $1/2^n$.

Summing over all possible pairs, condition (C-1) happens with probability at most $qq_{\mathrm{f}}(\mathbf{of}(\Phi_R)+1/2^n)$.

(C-2) Fix a decryption query $(-, LR, ST) \in \mathcal{Q}_{\mathrm{BC}}$ and a query to F $(u,v) \in \mathcal{Q}_{\mathsf{F}}$.
  (a) Since k_1 is uniformly random and independent of the query transcript, $R \oplus u = k_1$ with probability at most $1/2^n$.
  (b) Since k_4 is uniformly random and independent of the query transcript, $S \oplus u = k_4$ with probability at most $1/2^n$.
  Summing over all possible pairs, condition (C-2) happens with probability at most $2qq_{\mathrm{f}}/2^n$.

(C-3) Fix two queries $(+, \phi, ST) \neq (+, \phi', S'T') \in \mathcal{Q}_{\mathrm{BC}}$. Since the adversary never repeats queries, we have $\phi \neq \phi'$.
  (a) By Definition 3.1, $\phi(\mathbf{k}) = \phi'(\mathbf{k})$ with probability at most $\mathbf{cf}(\Phi)$ over the choice of a random $\mathbf{k}$.
  (b) Since $\phi \neq \phi'$, the output $S'T'$ is sampled uniformly at random in a set of size at least $2^{2n}-q$ and independently of ST. Thus $S = S'$ with probability at most $2^n/(2^{2n}-q) \leq 1/(2^n-1) \leq 2/2^n$.
  Summing over all possible distinct pairs, condition (C-3) happens with probability at most $q^2/2 \cdot (\mathbf{cf}(\Phi)+4/2^n)$.

(C-4) Fix two queries $(+, \phi, ST), (+, \phi', S'T') \in \mathcal{Q}_{\mathrm{BC}}$. By Definition 3.3, $\phi_R(\mathbf{k}) = S' \oplus k_1 \oplus k_4$ with probability at most $\mathbf{oxf}(\Phi_R)$ over the choice of $\mathbf{k}$. Summing over all possible pairs, condition (C-4) happens with probability at most $q^2 \cdot \mathbf{oxf}(\Phi_R)$.

(C-5) Fix two decryption queries $(-, LR, ST) \neq (-, L'R', S'T') \in \mathcal{Q}_{\mathrm{BC}}$. The value $L'R'$ is sampled uniformly at random in a set of size at least $2^{2n}-q$ and independently of LR. Thus, $R = R'$ with probability at most $2^n/(2^{2n}-q) \leq 1/(2^n-1) \leq 2/2^n$. Summing over all possible distinct pairs, condition (C-5) happens with probability at most $q^2/2^n$.

(C-6) Fix two decryption queries $(-, LR, ST), (-, L'R', S'T') \in \mathcal{Q}_{\mathrm{BC}}$. As k_1 and k_4 are randomly sampled, $R \oplus S' = k_1 \oplus k_4$ with probability at most $1/2^n$. Summing over all possible distinct pairs, condition (C-6) happens with probability at most $q^2/2^n$.

(C-7) Fix an encryption query $(+, \phi, ST) \in \mathcal{Q}_{\mathrm{BC}}$ and a decryption query $(-, L'R', S'T') \in \mathcal{Q}_{\mathrm{BC}}$.
  (a) By Definition 3.1, $\phi(\mathbf{k}) = L'R'$ with probability at most $\mathbf{cf}(\Phi)$.
  (b) We distinguish two cases. If the encryption query occurs before the decryption query, then necessarily $ST \neq S'T'$ due to the no-pointless-query assumption (the adversary cannot ask DEC to decrypt a value that was received as an answer to the KDENC oracle). If the decryption query occurs before the encryption query, then ST is uniformly random in a set of size at least $2^{2n}-q$ and independent of $S'T'$. Hence, the condition occurs with probability at most $1/(2^{2n}-q) \leq 1/2^n$.
  (c) By Definition 3.3, $\phi_R(\mathbf{k}) = S' \oplus k_1 \oplus k_4$ with probability at most $\mathbf{oxf}(\Phi_R)$ over the choice of $\mathbf{k}$.

(d) Since k_1 and k_4 are drawn uniformly at random and independently of the query transcript, the probability that $k_1 \oplus k_4 = S \oplus R'$ is at most $1/2^n$.

Summing over all possible distinct pairs, condition (C-7) happens with probability at most $q^2/2 \cdot (\mathbf{cf}(\Phi) + \mathbf{oxf}(\Phi_R) + 4/2^n)$.

The result follows by applying the union bound over conditions (C-1) to (C-7).

We now lower bound $\Pr[X_{\mathcal{A},\mathsf{rw}} = \tau]/\Pr[X_{\mathcal{A},\mathsf{pw}} = \tau]$ for a good transcript τ. To this end, we introduce the following definition of a *bad function* F with respect to a good τ. Informally, this definition states that there is a collision among the set of all inputs to the second or third-round functions (conditions (C′-3), (C′-5), and (C′-7)) or among these and direct, first-round, or second-round queries (conditions (C′-1) and (C′-2)).

Definition 4.2. *Fix a good transcript $\tau = (\mathcal{Q}_{\mathrm{BC}}, \mathcal{Q}_{\mathsf{F}}, \mathbf{k})$. Let*

$$\mathsf{Dom}(\mathsf{F}) \coloneqq \{u \in \{0,1\}^n : \exists (u,v) \in \mathcal{Q}_{\mathsf{F}}\}, \quad \textit{and}$$

$$\mathsf{Dom}'(\mathsf{F}) \coloneqq \left\{ u \in \{0,1\}^n : \begin{array}{l} \exists(+,\phi,ST) \in \mathcal{Q}_{\mathrm{BC}}, u = \phi_R(\mathbf{k}) \oplus k_1 \vee \\ \exists(+,\phi,ST) \in \mathcal{Q}_{\mathrm{BC}}, u = S \oplus k_4 \vee \\ \exists(-,LR,ST) \in \mathcal{Q}_{\mathrm{BC}}, u = R \oplus k_1 \vee \\ \exists(-,LR,ST) \in \mathcal{Q}_{\mathrm{BC}}, u = S \oplus k_4 \end{array} \right\}.$$

A function F is said to be bad with respect to τ, *denoted $\mathsf{Bad}(\mathsf{F},\tau)$, iff any of the following holds.*

(C′-1) there exists $(+,\phi,ST) \in \mathcal{Q}_{\mathrm{BC}}$ such that
(a) $\phi_L(\mathbf{k}) \oplus \mathsf{F}(\phi_R(\mathbf{k}) \oplus k_1) \oplus k_2 \in \mathsf{Dom}(\mathsf{F}) \cup \mathsf{Dom}'(\mathsf{F})$ or
(b) $T \oplus \mathsf{F}(S \oplus k_4) \oplus k_3 \in \mathsf{Dom}(\mathsf{F}) \cup \mathsf{Dom}'(\mathsf{F})$;

(C′-2) there exists $(-,LR,ST) \in \mathcal{Q}_{\mathrm{BC}}$ such that
(a) $L \oplus \mathsf{F}(R \oplus k_1) \oplus k_2 \in \mathsf{Dom}(\mathsf{F}) \cup \mathsf{Dom}'(\mathsf{F})$ or
(b) $T \oplus \mathsf{F}(S \oplus k_4) \oplus k_3 \in \mathsf{Dom}(\mathsf{F}) \cup \mathsf{Dom}'(\mathsf{F})$;

(C′-3) there exist $(+,\phi,ST) \neq (+,\phi',S'T') \in \mathcal{Q}_{\mathrm{BC}}$ such that
(a) $\phi_L(\mathbf{k}) \oplus \mathsf{F}(\phi_R(\mathbf{k}) \oplus k_1) = \phi'_L(\mathbf{k}) \oplus \mathsf{F}(\phi'_R(\mathbf{k}) \oplus k_1)$ or
(b) $T \oplus \mathsf{F}(S \oplus k_4) = T' \oplus \mathsf{F}(S' \oplus k_4)$;

(C′-4) there exist $(+,\phi,ST),(+,\phi',S'T') \in \mathcal{Q}_{\mathrm{BC}}$ (not necessarily distinct) such that $\phi_L(\mathbf{k}) \oplus \mathsf{F}(\phi_R(\mathbf{k}) \oplus k_1) \oplus k_2 = T' \oplus \mathsf{F}(S' \oplus k_4) \oplus k_3$;

(C′-5) there exist $(-,LR,ST) \neq (-,L'R',S'T') \in \mathcal{Q}_{\mathrm{BC}}$ such that
(a) $L \oplus \mathsf{F}(R \oplus k_1) = L' \oplus \mathsf{F}(R' \oplus k_1)$ or
(b) $T \oplus \mathsf{F}(S \oplus k_4) = T' \oplus \mathsf{F}(S' \oplus k_4)$;

(C′-6) there exist $(-,LR,ST),(-,L'R',S'T') \in \mathcal{Q}_{\mathrm{BC}}$ (not necessarily distinct) such that $L \oplus \mathsf{F}(R \oplus k_1) \oplus k_2 = T' \oplus \mathsf{F}(S' \oplus k_4) \oplus k_3$;

(C′-7) there exist $(+,\phi,ST),(-,L'R',S'T') \in \mathcal{Q}_{\mathrm{BC}}$ such that
(a) $\phi_L(\mathbf{k}) \oplus \mathsf{F}(\phi_R(\mathbf{k}) \oplus k_1) = L' \oplus \mathsf{F}(R' \oplus k_1)$ or
(b) $T \oplus \mathsf{F}(S \oplus k_4) = T' \oplus \mathsf{F}(S' \oplus k_4)$ or

(c) $\phi_L(\mathbf{k}) \oplus \mathsf{F}(\phi_R(\mathbf{k}) \oplus k_1) \oplus k_2 = T' \oplus \mathsf{F}(S' \oplus k_4) \oplus k_3$ *or*
(d) $T \oplus \mathsf{F}(S \oplus k_4) \oplus k_3 = L' \oplus \mathsf{F}(R' \oplus k_1) \oplus k_2$.

Lemma 4.2. *Fix a good transcript* $\tau = (\mathcal{Q}_{\mathrm{BC}}, \mathcal{Q}_{\mathsf{F}}, \mathbf{k})$. *Then*

$$\Pr_{\mathsf{F} \twoheadleftarrow \mathsf{Func}(n)}[\mathsf{Bad}(\mathsf{F}, \tau) \mid \mathsf{F} \vdash \mathcal{Q}_{\mathsf{F}}] \leq 4 \cdot q q_{\mathrm{f}}/2^n + 14 \cdot q^2/2^n \ .$$

Proof. First, note that $|\mathsf{Dom}(\mathsf{F})| = q_{\mathrm{f}}$ and $|\mathsf{Dom}'(\mathsf{F})| \leq 2q$. We now consider each condition in turn.[4]

(C′-1) Fix an encryption query $(+, \phi, ST) \in \mathcal{Q}_{\mathrm{BC}}$.
(a) By ¬(C-1a), $\phi_R(\mathbf{k}) \oplus k_1$ is a fresh input for the function F and hence $\mathsf{F}(\phi_R(\mathbf{k}) \oplus k_1)$ is uniformly random. Thus, $\phi_L(\mathbf{k}) \oplus \mathsf{F}(\phi_R(\mathbf{k}) \oplus k_1) \oplus k_2 \in \mathsf{Dom}(\mathsf{F}) \cup \mathsf{Dom}'(\mathsf{F})$ with probability at most $(q_{\mathrm{f}} + 2q)/2^n$.
(b) By ¬(C-1b), $S \oplus k_4$ is a fresh input for the function F and hence $\mathsf{F}(S \oplus k_4)$ is uniformly random. Thus, $T \oplus \mathsf{F}(S \oplus k_4) \oplus k_3 \in \mathsf{Dom}(\mathsf{F}) \cup \mathsf{Dom}'(\mathsf{F})$ with probability at most $(q_{\mathrm{f}} + 2q)/2^n$.
Summing over all encryption queries, condition (C′-1) happens with probability at most $2q(q_{\mathrm{f}} + 2q)/2^n$.

(C′-2) Fix a decryption query $(-, LR, ST) \in \mathcal{Q}_{\mathrm{BC}}$.
(a) By ¬(C-2a), $R \oplus k_1$ is a fresh input for the function F and hence $\mathsf{F}(R \oplus k_1)$ is uniformly random. Thus, $L \oplus \mathsf{F}(R \oplus k_1) \oplus k_2 \in \mathsf{Dom}(\mathsf{F}) \cup \mathsf{Dom}'(\mathsf{F})$ with probability at most $(q_{\mathrm{f}} + 2q)/2^n$.
(b) By ¬(C-2b), $S \oplus k_4$ is a fresh value for the function F and hence $T \oplus \mathsf{F}(S \oplus k_4) \oplus k_3 \in \mathsf{Dom}(\mathsf{F}) \cup \mathsf{Dom}'(\mathsf{F})$ with probability at most $(q_{\mathrm{f}} + 2q)/2^n$.
Summing over all decryption queries, condition (C′-2) happens with probability at most $2q(q_{\mathrm{f}} + 2q)/2^n$.

(C′-3) Fix $(+, \phi, ST) \neq (+, \phi', S'T') \in \mathcal{Q}_{\mathrm{BC}}$.
(a) By ¬(C-1a), we have $\phi_R(\mathbf{k}) \oplus k_1 \notin \mathsf{Dom}(\mathsf{F})$ and $\phi'_R(\mathbf{k}) \oplus k_1 \notin \mathsf{Dom}(\mathsf{F})$. Moreover, by ¬(C-3a), we have that $\phi(\mathbf{k}) \neq \phi'(\mathbf{k})$. We distinguish two cases. If $\phi_R(\mathbf{k}) \neq \phi'_R(\mathbf{k})$, then $\mathsf{F}(\phi_R(\mathbf{k}) \oplus k_1)$ and $\mathsf{F}(\phi'_R(\mathbf{k}) \oplus k_1)$ are uniformly random and independent, so that $\phi_L(\mathbf{k}) \oplus \mathsf{F}(\phi_R(\mathbf{k}) \oplus k_1) = \phi'_L(\mathbf{k}) \oplus \mathsf{F}(\phi'_R(\mathbf{k}) \oplus k_1)$ with probability $1/2^n$. If $\phi_R(\mathbf{k}) = \phi'_R(\mathbf{k})$, then necessarily $\phi_L(\mathbf{k}) \neq \phi'_L(\mathbf{k})$, so that the condition cannot hold. Hence, this condition holds with probability at most $1/2^n$.
(b) By ¬(C-1b), $S \oplus k_4 \notin \mathsf{Dom}(\mathsf{F})$ and $S' \oplus k_4 \notin \mathsf{Dom}(\mathsf{F})$; moreover, by ¬(C-3b), $S \neq S'$, so that $\mathsf{F}(S \oplus k_4)$ and $\mathsf{F}(S' \oplus k_4)$ are uniformly random and independent; hence, $T \oplus \mathsf{F}(S \oplus k_4) = T' \oplus \mathsf{F}(S' \oplus k_4)$ with probability at most $1/2^n$.
Summing over all possible pairs of distinct encryption queries, condition (C′-3) happens with probability at most $q^2/2^n$.

[4] In what follows, we will argue using the fact that the transcript is good by referring to which specific condition defining a bad transcript would hold, saying e.g., "By ¬(C-*ix*), . . . ".

(C′-4) Fix two (possibly equal) encryption queries $(+, \phi, ST), (+, \phi', S'T') \in \mathcal{Q}_{\mathrm{BC}}$. By ¬(C-1a), $\phi_R(\mathbf{k}) \oplus k_1 \notin \mathsf{Dom}(\mathsf{F})$ and by ¬(C-1b), $S' \oplus k_4 \notin \mathsf{Dom}(\mathsf{F})$; moreover, by ¬(C-4), we have $\phi_R(\mathbf{k}) \oplus k_1 \neq S' \oplus k_4$, so that $\mathsf{F}(\phi_R(\mathbf{k}) \oplus k_1)$ and $\mathsf{F}(S' \oplus k_4)$ are uniformly random and independent; hence, $\phi_L(\mathbf{k}) \oplus \mathsf{F}(\phi_R(\mathbf{k}) \oplus k_1) \oplus k_2 = T' \oplus \mathsf{F}(S' \oplus k_4) \oplus k_3$ with probability at most $1/2^n$. Summing over all possible pairs, condition (C′-4) happens with probability at most $q^2/2^n$.

(C′-5) Fix two decryption queries $(-, LR, ST) \neq (-, L'R', S'T') \in \mathcal{Q}_{\mathrm{BC}}$.

(a) By ¬(C-2a), $R \oplus k_1 \notin \mathsf{Dom}(\mathsf{F})$ and $R' \oplus k_1 \notin \mathsf{Dom}(\mathsf{F})$; moreover, by ¬(C-5), $R \neq R'$ so that $\mathsf{F}(R \oplus k_1)$ and $\mathsf{F}(R' \oplus k_1)$ are uniformly random and independent. Hence, $L \oplus \mathsf{F}(R \oplus k_1) = L' \oplus \mathsf{F}(R' \oplus k_1)$ with probability at most $1/2^n$.

(b) By ¬(C-2b), $S \oplus k_4 \notin \mathsf{Dom}(\mathsf{F})$ and $S' \oplus k_4 \notin \mathsf{Dom}(\mathsf{F})$. We distinguish two cases. If $S \neq S'$ then $\mathsf{F}(S \oplus k_4)$ and $\mathsf{F}(S' \oplus k_4)$ are uniformly random and independent and hence $T \oplus \mathsf{F}(S \oplus k_4) = T' \oplus \mathsf{F}(S' \oplus k_4)$ with probability at most $1/2^n$. If $S = S'$ then necessarily $T \neq T'$ since the adversary does not repeat queries and hence the condition cannot hold. In all cases, the conditions hold with probability at most $1/2^n$.

By summing over all possible pairs of distinct decryption queries, condition (C′-5) happens with probability at most $q^2/2^n$.

(C′-6) Fix two (possibly equal) decryption queries $(-, LR, ST), (-, L'R', S'T') \in \mathcal{Q}_{\mathrm{BC}}$. By ¬(C-2a), $R \oplus k_1 \notin \mathsf{Dom}(\mathsf{F})$ and by ¬(C-2b), $S' \oplus k_4 \notin \mathsf{Dom}(\mathsf{F})$; moreover, by ¬(C-6), $R \oplus k_1 \neq S' \oplus k_4$ so that $\mathsf{F}(R \oplus k_1)$ and $\mathsf{F}(S' \oplus k_4)$ are uniformly random and independent; hence, $L \oplus \mathsf{F}(R \oplus k_1) \oplus k_2 = T' \oplus \mathsf{F}(S' \oplus k_4) \oplus k_3$ with probability at most $1/2^n$. Summing over all possible pairs, condition (C′-6) happens with probability at most $q^2/2^n$.

(C′-7) Fix an encryption query $(+, \phi, ST) \in \mathcal{Q}_{\mathrm{BC}}$ and a decryption query $(-, L'R', S'T') \in \mathcal{Q}_{\mathrm{BC}}$. By respectively ¬(C-1a), ¬(C-1b), ¬(C-2a), and ¬(C-2b), $\phi_R(\mathbf{k}) \oplus k_1$, $S \oplus k_4$, $R' \oplus k_1$, and $S' \oplus k_4$ are all fresh input values to F.

(a) By ¬(C-7a), $\phi(\mathbf{k}) \neq L'R'$. We distinguish two cases. If $\phi_R(\mathbf{k}) \neq R'$, then $\mathsf{F}(\phi_R(\mathbf{k}) \oplus k_1)$ and $\mathsf{F}(R' \oplus k_1)$ are uniformly random and independent and thus $\phi_L(\mathbf{k}) \oplus \mathsf{F}(\phi_R(\mathbf{k}) \oplus k_1) = L' \oplus \mathsf{F}(R' \oplus k_1)$ with probability at most $1/2^n$. If $\phi_R(\mathbf{k}) = R'$, then necessarily $\phi_L(\mathbf{k}) \neq L'$ and hence the condition cannot hold. In all cases, the condition holds with probability at most $1/2^n$.

(b) By ¬(C-7b), $ST \neq S'T'$. If $S \neq S'$, then $\mathsf{F}(S \oplus k_4)$ and $\mathsf{F}(S' \oplus k_4)$ are uniformly random and independent and hence $T \oplus \mathsf{F}(S \oplus k_4) = T' \oplus \mathsf{F}(S' \oplus k_4)$ with probability at most $1/2^n$. If $S = S'$, then necessarily $T \neq T'$ and the condition cannot hold. In all cases, the condition holds with probability at most $1/2^n$.

(c) By ¬(C-7c), $\phi_R(\mathbf{k}) \oplus k_1 \neq S' \oplus k_4$ so that $\mathsf{F}(\phi_R(\mathbf{k}) \oplus k_1)$ and $\mathsf{F}(S' \oplus k_4)$ are uniformly random and independent and thus $\phi_L(\mathbf{k}) \oplus \mathsf{F}(\phi_R(\mathbf{k}) \oplus k_1) \oplus k_2 = T' \oplus \mathsf{F}(S' \oplus k_4) \oplus k_3$ with probability at most $1/2^n$.

(d) By $\neg$(C-7d), $S \oplus k_4 \neq R' \oplus k_1$ so that $\mathsf{F}(S \oplus k_4)$ and $\mathsf{F}(R' \oplus k_1)$ are uniformly random and independent and thus $T \oplus \mathsf{F}(S \oplus k_4) \oplus k_3 = L' \oplus \mathsf{F}(R' \oplus k_1) \oplus k_2$ with probability at most $1/2^n$.

By summing over all possible pairs, condition (C′-7) happens with probability at most $2q^2/2^n$.

The result follows by applying the union bound over all conditions.

Lemma 4.3. *Fix a good transcript* $\tau = (\mathcal{Q}_{\mathrm{BC}}, \mathcal{Q}_{\mathsf{F}}, \mathbf{k})$*. Then*

$$\Pr_{\mathsf{F} \twoheadleftarrow \mathsf{Func}(n)}[\mathsf{KAF}^{\mathsf{F}}_{\mathbf{k}} \vdash \mathcal{Q}_{\mathrm{BC}} \mid \mathsf{F} \vdash \mathcal{Q}_{\mathsf{F}} \wedge \neg \mathsf{Bad}(\mathsf{F}, \tau)] = \frac{1}{(2^n)^{2q}} \ .$$

Proof. Let q_{enc} and q_{dec} respectively denote the number of queries to KDEnc and Dec in $\mathcal{Q}_{\mathrm{BC}}$ (with $q_{\mathrm{enc}} + q_{\mathrm{dec}} = q$). Using an arbitrary ordering, let

$$\mathcal{Q}_{\mathrm{BC}} = \big[(+, \phi_1, S_1 T_1), \ldots, (+, \phi_{q_{\mathrm{enc}}}, S_{q_{\mathrm{enc}}} T_{q_{\mathrm{enc}}}),\\ (-, L_{q_{\mathrm{enc}}+1} R_{q_{\mathrm{enc}}+1}, S_{q_{\mathrm{enc}}+1} T_{q_{\mathrm{enc}}+1}), \ldots, (-, L_q R_q, S_q T_q)\big] \ .$$

For a given function F, let w_i and z_i be the i-th input to F in the second and third rounds respectively, i.e.,

$$\begin{aligned} w_i &= \phi_{i,L}(\mathbf{k}) \oplus \mathsf{F}(\phi_{i,R}(\mathbf{k}) \oplus k_1) \oplus k_2 && \text{for } 1 \le i \le q_{\mathrm{enc}} \\ &= L_i \oplus \mathsf{F}(R_i \oplus k_1) \oplus k_2 && \text{for } q_{\mathrm{enc}} + 1 \le i \le q \\ z_i &= T_i \oplus \mathsf{F}(S_i \oplus k_4) \oplus k_3 && \text{for } 1 \le i \le q \ . \end{aligned}$$

Then event $\mathsf{KAF}^{\mathsf{F}}_{\mathbf{k}} \vdash \mathcal{Q}_{\mathrm{BC}}$ is equivalent to

$$\begin{cases} \mathsf{F}(w_i) = \phi_{i,R}(\mathbf{k}) \oplus T_i \oplus \mathsf{F}(S_i \oplus k_4) \\ \mathsf{F}(z_i) = S_i \oplus \phi_{i,L}(\mathbf{k}) \oplus \mathsf{F}(\phi_{i,R}(\mathbf{k}) \oplus k_1) \end{cases} \quad \text{for } 1 \le i \le q_{\mathrm{enc}} \tag{3}$$

$$\begin{cases} \mathsf{F}(w_i) = R_i \oplus T_i \oplus \mathsf{F}(S_i \oplus k_4) \\ \mathsf{F}(z_i) = S_i \oplus L_i \oplus \mathsf{F}(R_i \oplus k_1) \end{cases} \quad \text{for } q_{\mathrm{enc}} + 1 \le i \le q \ . \tag{4}$$

Conditioned on event $\neg\mathsf{Bad}(\mathsf{F}, \tau)$, we have that $w_1, \ldots, w_q, z_1, \ldots, z_q$ are $2q$ distinct values as otherwise one of the conditions (C′-3)–(C′-7) would be fulfilled. Moreover, all these $2q$ values are distinct from values in $\mathsf{Dom}(\mathsf{F}) \cup \mathsf{Dom}'(\mathsf{F})$, as otherwise condition (C′-1) or (C′-2) would be fulfilled. This implies that, even conditioned on $\mathsf{F} \vdash \mathcal{Q}_{\mathsf{F}}$, the $2q$ random values $\mathsf{F}(w_1), \ldots, \mathsf{F}(w_q), \mathsf{F}(z_1), \ldots, \mathsf{F}(z_q)$ are uniform and independent of $\mathsf{F}(\phi_{i,R}(\mathbf{k}) \oplus k_1)$ for $1 \le i \le q_{\mathrm{enc}}$, $\mathsf{F}(R_i \oplus k_1)$ for $q_{\mathrm{enc}} + 1 \le i \le q$, and $\mathsf{F}(S_i \oplus k_4)$ for $1 \le i \le q$. Hence, Equations (3) and (4) hold with probability $(1/2^n)^{2q}$.

Lemma 4.4. *Fix a good transcript* $\tau = (\mathcal{Q}_{\mathrm{BC}}, \mathcal{Q}_{\mathsf{F}}, \mathbf{k})$*. Then,*

$$\frac{\Pr[X_{\mathcal{A},\mathsf{rw}} = \tau]}{\Pr[X_{\mathcal{A},\mathsf{pw}} = \tau]} \ge 1 - 4 \cdot q q_{\mathrm{f}}/2^n - 15 \cdot q^2/2^n \ .$$

Proof. Let $\tau = (\mathcal{Q}_{\mathrm{BC}}, \mathcal{Q}_{\mathsf{F}}, \mathbf{k})$ with $\mathbf{k} = (k_1, k_2, k_3, k_4)$ be a good transcript, and let q_{enc}, resp. q_{dec}, denote the number of queries to KDEnc, resp. Dec, in $\mathcal{Q}_{\mathrm{BC}}$, with $q_{\mathrm{enc}} + q_{\mathrm{dec}} = q$.

Exactly as in the proof of Lemma 3.1, one can show that

$$\Pr[X_{\mathcal{A},\mathsf{pw}} = \tau] = \Pr_{\mathbf{k}' \twoheadleftarrow \mathsf{K}}[\mathbf{k}' = \mathbf{k}] \cdot \frac{1}{(2^n)^{q_{\mathrm{f}}}} \cdot \frac{1}{(2^{2n})_{q_{\mathrm{enc}}}} \cdot \frac{1}{(2^{2n})_{q_{\mathrm{dec}}}} \ . \tag{5}$$

where K is the key-generation algorithm.

We now lower bound the probability that $X_{\mathcal{A},\mathsf{rw}} = \tau$.

$$\begin{align}
&\Pr[X_{\mathcal{A},\mathsf{rw}} = \tau] \tag{6}\\
&= \Pr_{\mathbf{k}' \twoheadleftarrow \mathsf{K}}[\mathbf{k}' = \mathbf{k}] \cdot \Pr_{\mathsf{F} \twoheadleftarrow \mathsf{Func}(n)}[\mathsf{KAF}^{\mathsf{F}}_{\mathbf{k}} \vdash \mathcal{Q}_{\mathrm{BC}} \ \wedge \ \mathsf{F} \vdash \mathcal{Q}_{\mathsf{F}}] \notag\\
&= \Pr_{\mathbf{k}' \twoheadleftarrow \mathsf{K}}[\mathbf{k}' = \mathbf{k}] \cdot \Pr_{\mathsf{F} \twoheadleftarrow \mathsf{Func}(n)}[\mathsf{F} \vdash \mathcal{Q}_{\mathsf{F}}] \cdot \Pr_{\mathsf{F} \twoheadleftarrow \mathsf{Func}(n)}[\mathsf{KAF}^{\mathsf{F}}_{\mathbf{k}} \vdash \mathcal{Q}_{\mathrm{BC}} \,|\, \mathsf{F} \vdash \mathcal{Q}_{\mathsf{F}}] \notag\\
&= \Pr_{\mathbf{k}' \twoheadleftarrow \mathsf{K}}[\mathbf{k}' = \mathbf{k}] \cdot \frac{1}{(2^n)^{q_{\mathrm{f}}}} \cdot \Pr_{\mathsf{F} \twoheadleftarrow \mathsf{Func}(n)}[\mathsf{KAF}^{\mathsf{F}}_{\mathbf{k}} \vdash \mathcal{Q}_{\mathrm{BC}} \,|\, \mathsf{F} \vdash \mathcal{Q}_{\mathsf{F}}] \notag\\
&= \Pr_{\mathbf{k}' \twoheadleftarrow \mathsf{K}}[\mathbf{k}' = \mathbf{k}] \cdot \frac{1}{(2^n)^{q_{\mathrm{f}}}} \cdot \Pr_{\mathsf{F} \twoheadleftarrow \mathsf{Func}(n)}[\mathsf{KAF}^{\mathsf{F}}_{\mathbf{k}} \vdash \mathcal{Q}_{\mathrm{BC}} \,|\, \mathsf{F} \vdash \mathcal{Q}_{\mathsf{F}} \ \wedge \ \neg\mathsf{Bad}(\mathsf{F}, \tau)] \notag\\
&\qquad\qquad \cdot (1 - \Pr_{\mathsf{F} \twoheadleftarrow \mathsf{Func}(n)}[\mathsf{Bad}(\mathsf{F}, \tau) \,|\, \mathsf{F} \vdash \mathcal{Q}_{\mathsf{F}}]) \ . \tag{7}
\end{align}$$

Combining Equation 7 and Equation 5 we get

$$\begin{aligned}
\frac{\Pr[X_{\mathcal{A},\mathsf{rw}} = \tau]}{\Pr[X_{\mathcal{A},\mathsf{pw}} = \tau]} &= (2^{2n})_{q_{\mathrm{enc}}} \cdot (2^{2n})_{q_{\mathrm{dec}}} \cdot \Pr[\mathsf{KAF}^{\mathsf{F}}_{\mathbf{k}} \vdash \mathcal{Q}_{\mathrm{BC}} \,|\, \mathsf{F} \vdash \mathcal{Q}_{\mathsf{F}} \ \wedge \ \neg\mathsf{Bad}(\mathsf{F}, \tau)] \\
&\qquad \cdot (1 - \Pr[\mathsf{Bad}(\mathsf{F}, \tau) \,|\, \mathsf{F} \vdash \mathcal{Q}_{\mathsf{F}}]) \ ,
\end{aligned}$$

where all probabilities are over $\mathsf{F} \twoheadleftarrow \mathsf{Func}(n)$. Using Lemma 4.3 and Lemma 4.2, we obtain

$$\begin{align}
\frac{\Pr[X_{\mathcal{A},\mathsf{rw}} = \tau]}{\Pr[X_{\mathcal{A},\mathsf{pw}} = \tau]} &\geq \frac{(2^{2n})_{q_{\mathrm{enc}}} \cdot (2^{2n})_{q_{\mathrm{dec}}}}{(2^n)^{2q}} \cdot \left(1 - \frac{4qq_{\mathrm{f}}}{2^n} - \frac{14q^2}{2^n}\right) \tag{8}\\
&= \left(1 - \frac{4qq_{\mathrm{f}}}{2^n} - \frac{14q^2}{2^n}\right) \cdot \prod_{i=0}^{q_{\mathrm{enc}}-1} \left(1 - \frac{i}{2^{2n}}\right) \cdot \prod_{i=0}^{q_{\mathrm{dec}}-1} \left(1 - \frac{i}{2^{2n}}\right) \tag{9}\\
&\geq \left(1 - \frac{4qq_{\mathrm{f}}}{2^n} - \frac{14q^2}{2^n}\right) \cdot \left(1 - \frac{q_{\mathrm{enc}}^2}{2 \cdot 2^{2n}}\right) \cdot \left(1 - \frac{q_{\mathrm{dec}}^2}{2 \cdot 2^{2n}}\right) \tag{10}\\
&\geq 1 - \frac{4qq_{\mathrm{f}}}{2^n} - \frac{15q^2}{2^n} \ . \tag{11}
\end{align}$$

Combining Lemma 2.1 with Lemma 4.1 and Lemma 4.4, we finally obtain Equation 2, which concludes the proof of Theorem 4.1.

5 Attacks

5.1 Necessity of offset-freeness

We start by showing that the condition that Φ_R is offset-free is necessary for the KDM-CPA security of 4-round KAF (with the same round function F and independent keys $\mathbf{k} = (k_1, k_2, k_3, k_4)$).[5] This attack takes advantage of a collision at the inputs to the third-round F within two encryption queries:

- Adversary $\mathcal{A}$ chooses two distinct values x and x' and obtains $\mathsf{F}(x)$, $\mathsf{F}(x')$, $\mathsf{F}^2(x)$ and $\mathsf{F}^2(x')$ and builds the values
$$\varDelta_L \coloneqq \mathsf{F}^2(x) \oplus x, \varDelta_R \coloneqq \mathsf{F}(x), \varDelta'_L \coloneqq \mathsf{F}^2(x') \oplus x', \varDelta'_R \coloneqq \mathsf{F}(x') \ .$$
- $\mathcal{A}$ then calls the KDEnc oracle twice on inputs $\phi = (\phi_L, \phi_R)$ and $\phi' = (\phi'_L, \phi'_R)$ where
$$\phi_L(\mathbf{k}) \coloneqq k_2 \oplus \varDelta_L \quad \text{and} \quad \phi_R(\mathbf{k}) \coloneqq k_1 \oplus \varDelta_R \ ,$$
$$\phi'_L(\mathbf{k}) \coloneqq k_2 \oplus \varDelta'_L \quad \text{and} \quad \phi'_R(\mathbf{k}) \coloneqq k_1 \oplus \varDelta'_R \ .$$
The adversary receives ST and $S'T'$ as the respective answers. Note that any set Φ_R containing both ϕ_R and ϕ'_R is not offset-free.
- $\mathcal{A}$ returns 1 iff $S \oplus S' = x \oplus x'$.

The adversary returns 1 with probability 1 in the real world whereas it returns 1 with probability $1/2^n$ in the ideal world. To see the former, note that the input $k_2 \oplus \mathsf{F}^2(x) \oplus x | k_1 \oplus \mathsf{F}(x)$ is processed though the first three rounds as follows:

$$\begin{gathered} k_2 \oplus \mathsf{F}^2(x) \oplus x | k_1 \oplus \mathsf{F}(x) \\ \downarrow \\ k_1 \oplus \mathsf{F}(x) | x \oplus k_2 \\ \downarrow \\ x \oplus k_2 | k_1 \\ \downarrow \\ k_1 | x \oplus k_2 \oplus \mathsf{F}(k_1 \oplus k_3). \end{gathered}$$

Thus the left half of the output is $x \oplus k_2 \oplus \mathsf{F}(k_1 \oplus k_3)$. Hence the xor of the left halves of two encryptions with constants x and x' is $x \oplus x'$. Note that this attack triggers a collision in the third round function.

[5] Note that for a set Φ, if Φ_R is offset-free then so is Φ, but not necessary the other way round.

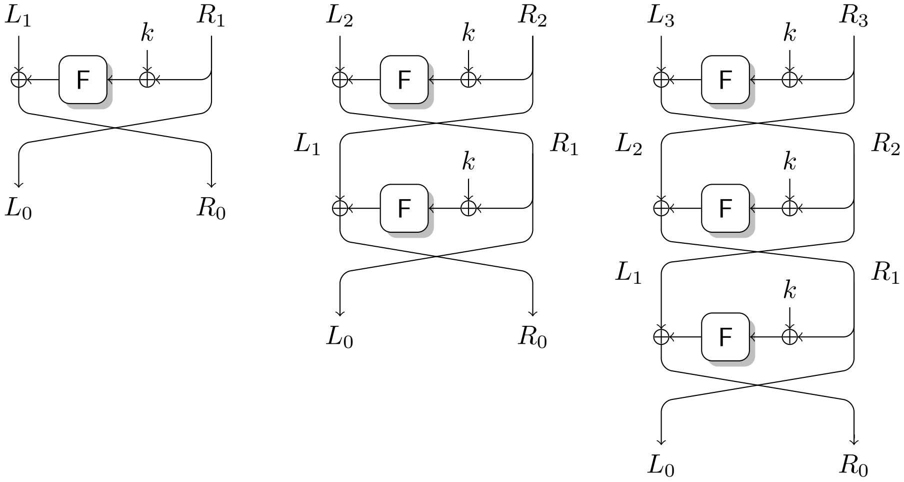

Fig. 3. Backwards construction of inputs leading to a particular output.

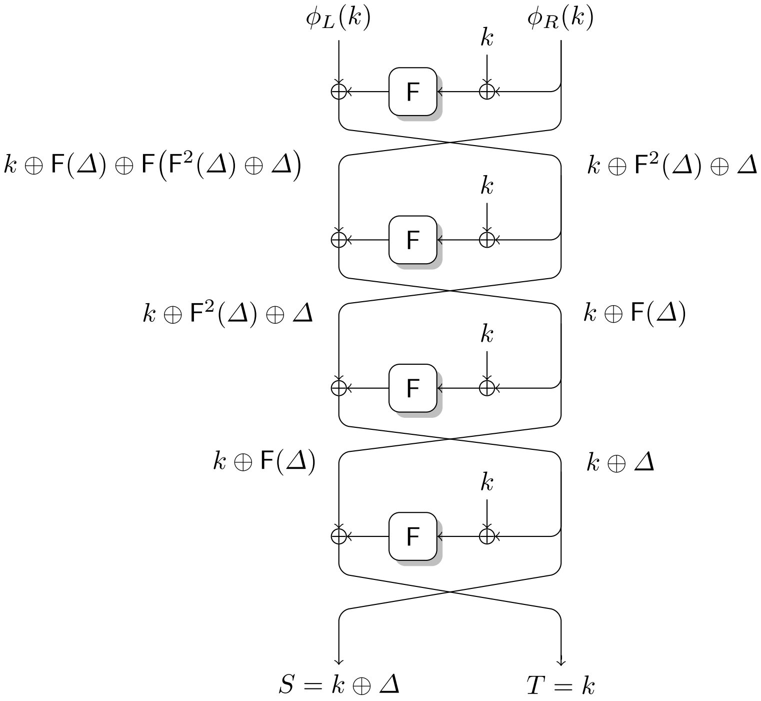
$\phi_L(k)$
k
$\phi_R(k)$
F
$k \oplus \mathsf{F}(\varDelta) \oplus \mathsf{F}\big(\mathsf{F}^2(\varDelta) \oplus \varDelta\big)$
k
$k \oplus \mathsf{F}^2(\varDelta) \oplus \varDelta$
F
$k \oplus \mathsf{F}^2(\varDelta) \oplus \varDelta$
k
$k \oplus \mathsf{F}(\varDelta)$
F
$k \oplus \mathsf{F}(\varDelta)$
k
$k \oplus \varDelta$
F
$S = k \oplus \varDelta$
$T = k$

Fig. 4. Sliding attack on 4-round KAF with reuse of keys and round functions.

5.2 Sliding attacks

We now analyze the most simple KAF configuration whereby all round functions and keys are identical. This construction is already known to be insecure in the CPA model for any number of rounds: using two encryption queries we have $\mathsf{KAF}(LR) = ST$ and $\mathsf{KAF}(TS) = LR$, which is unlikely for the ideal cipher. In the KDM model, however, we are able to give a stronger *key-recovery* attack using a single query. The adversary chooses an arbitrary value $\varDelta \in \{0,1\}^n$ and calls KDEnc on function ϕ, where

$$\begin{aligned}\phi_R(k) &:= k \oplus \mathsf{F}(\varDelta) \oplus \mathsf{F}\big(\mathsf{F}^2(\varDelta) \oplus \varDelta\big)\\ \phi_L(k) &:= k \oplus \mathsf{F}^2(\varDelta) \oplus \varDelta \oplus \mathsf{F}\big(\mathsf{F}(\varDelta) \oplus \mathsf{F}(\mathsf{F}^2(\varDelta) \oplus \varDelta)\big)\ .\end{aligned}$$

It receives a value ST as the answer and returns T as its guess for the k. This attack is depicted in Figure 4.

This attack can be generalized for any number of rounds. Instead of giving a direct expression for any number of rounds r (which we believe would be somewhat hard to read) we give a recursive definition based on Figure 4. The idea is that we arrange an input $L_r|R_r$ to the r-round KAF so that its output $S|T$ is $L_0|R_0 = k \oplus \varDelta|k$. To this end, following the decryption circuit (see Figure 3), for $i > 0$ we define

$$L_{i+1} \mid R_{i+1} := \mathsf{F}(L_i \oplus k) \oplus R_i \mid L_i\ .$$

Observe that $L_r|R_r$ corresponds to the decryption of $L_0|R_0$ and hence an encryption of $L_r|R_r$ will result in $L_0|R_0$. We also let $L_0^* \mid R_0^* := \varDelta \mid 0^n$ and similarly define

$$L_{i+1}^* \mid R_{i+1}^* := \mathsf{F}(L_i^*) \oplus R_i^* \mid L_i^*\ .$$

We claim that for any $i \geq 0$,

$$L_i \mid R_i = L_i^* \oplus k \mid R_i^* \oplus k\ .$$

Now since $L_{i+1}^* \mid R_{i+1}^*$ is independent of k, we can define two maps $\phi_L(k) := L_r^* \oplus k$ and $\phi_R(k) := R_r^* \oplus k$ that offset the key by constants. Next we query KDEnc on (ϕ_L, ϕ_R), which corresponds to encrypting $L_r|R_r$, the result of which will be $L_0|R_0$, and from which the key k can be read off.

We now prove the claim inductively. The claim trivially holds for $i = 0$. Suppose now that the claim holds for i. We show that it holds for $i+1$:

$$\begin{aligned}L_{i+1} \mid R_{i+1} &= \mathsf{F}(L_i \oplus k) \oplus R_i \mid L_i\\ &= \mathsf{F}(L_i^* \oplus k \oplus k) \oplus R_i^* \oplus k \mid L_i^* \oplus k\\ &= \mathsf{F}(L_i^*) \oplus R_i^* \oplus k \mid L_i^* \oplus k\\ &= L_{i+1}^* \oplus k \mid R_{i+1}^* \oplus k\ .\end{aligned}$$

In the above, the first equality is by the definition of $L_{i+1} \mid R_{i+1}$, the second by the induction hypothesis, and the last by the definition of $L_{i+1}^* \mid R_{i+1}^*$.

The attack generalizes further to r-round KAF where two keys k_1 and k_0 are alternatively used in odd and even-numbered rounds. We define $L_0 :=$

$k_{r \bmod 2} \oplus \varDelta, R_0 \coloneqq k_{r+1 \bmod 2}, L_0^* \coloneqq \varDelta$, and $R_0^* \coloneqq 0^n$. Following the decryption circuit we set

$$\begin{aligned} L_{i+1} \mid R_{i+1} &\coloneqq \mathsf{F}(L_i \oplus k_{i+r \bmod 2}) \oplus R_i \mid L_i, \quad \text{and} \\ L_{i+1}^* \mid R_{i+1}^* &\coloneqq \mathsf{F}(L_i^*) \oplus R_i^* \mid L_i^* \ . \end{aligned}$$

Note, once again, that $L_{i+1}^* \mid R_{i+1}^*$ is independent of the key and the sequence can be computed via access to F. We prove inductively that

$$L_i \mid R_i = L_i^* \oplus k_{i+r \bmod 2} \mid R_i^* \oplus k_{i+r+1 \bmod 2} \ .$$

This is trivial when $i = 0$. Furthermore,

$$\begin{aligned} L_{i+1} \mid R_{i+1} &= \mathsf{F}(L_i \oplus k_{i+r \bmod 2}) \oplus R_i \mid L_i \\ &= \mathsf{F}(L_i^* \oplus k_{i+r \bmod 2} \oplus k_{i+r \bmod 2}) \oplus R_i^* \oplus k_{i+r+1 \bmod 2} \mid L_i^* \oplus k_{i+r \bmod 2} \\ &= \mathsf{F}(L_i^*) \oplus R_i^* \oplus k_{i+r+1 \bmod 2} \mid L_i^* \oplus k_{i+r \bmod 2} \\ &= L_{i+1}^* \oplus k_{(i+1)+r \bmod 2} \mid R_{i+1}^* \oplus k_{(i+1)+r+1 \bmod 2} \ . \end{aligned}$$

Hence keys k_1 and k_0 can be extracted by querying $\text{KDE}\textsc{nc}(\phi_L, \phi_R)$, where $\phi_L(k) \coloneqq L_r^* \oplus k_0$ and $\phi_R(k) \coloneqq R_r^* \oplus k_1$ as the response will be $L_0 | R_0 = k_{r \bmod 2} \oplus \varDelta | k_{r+1 \bmod 2}$.

6 Discussion

We developed a generic proof strategy, based on the H-coefficient technique to analyze the KDM security of block ciphers. In Appendix A, we show that our technique can be applied in other settings and we revisit the KDM security of the basic Even–Mansour cipher with only a single round [13, Section 6.1]. We obtain another (arguably simpler) proof of the KDM security of the 1-round EM construction if the set of functions available to the attacker is claw-free and offset-free.

We studied the KDM-CCA security of the 4-round KAF cipher with a single round function if the set of key-dependent functions has negligible claw-freeness, offset-freeness and offset-xor-freeness. An important open problem is to find the minimal k such that the k-round KAF cipher with a single round function achieves KDM-CCA security assuming only that the set of key-dependent functions has (only) negligible claw-freeness. Our attack shows that necessarily $k \geq 5$. Our proof strategy does go through directly for $k \in \{5, 6, 7\}$ since an adversary can cause a collision in inputs to the first and third round function if it can use offsets as key-dependent functions. We do not claim that k-round KAF for $k \in \{5, 6, 7\}$ are KDM-CCA-insecure for some class of claw-free key-dependent functions but only that our technique cannot disprove it. It seems doable to prove the security of 8-round KAF in this setting using our technique but the proof would be much harder along lines we have considered.

References

[1] Ross J. Anderson and Eli Biham. Two practical and provably secure block ciphers: BEARS and LION. In Dieter Gollmann, editor, *FSE'96*, volume 1039 of *LNCS*, pages 113–120. Springer, Heidelberg, February 1996.

[2] Benny Applebaum. Key-dependent message security: Generic amplification and completeness. In Kenneth G. Paterson, editor, *EUROCRYPT 2011*, volume 6632 of *LNCS*, pages 527–546. Springer, Heidelberg, May 2011.

[3] Manuel Barbosa and Pooya Farshim. The related-key analysis of Feistel constructions. In Carlos Cid and Christian Rechberger, editors, *FSE 2014*, volume 8540 of *LNCS*, pages 265–284. Springer, Heidelberg, March 2015.

[4] Ray Beaulieu, Douglas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks, and Louis Wingers. The SIMON and SPECK families of lightweight block ciphers. Cryptology ePrint Archive, Report 2013/404, 2013. http://eprint.iacr.org/2013/404.

[5] John Black, Phillip Rogaway, and Thomas Shrimpton. Encryption-scheme security in the presence of key-dependent messages. In Kaisa Nyberg and Howard M. Heys, editors, *SAC 2002*, volume 2595 of *LNCS*, pages 62–75. Springer, Heidelberg, August 2003.

[6] Dan Boneh, Shai Halevi, Michael Hamburg, and Rafail Ostrovsky. Circular-secure encryption from decision Diffie-Hellman. In David Wagner, editor, *CRYPTO 2008*, volume 5157 of *LNCS*, pages 108–125. Springer, Heidelberg, August 2008.

[7] Jan Camenisch, Nishanth Chandran, and Victor Shoup. A public key encryption scheme secure against key dependent chosen plaintext and adaptive chosen ciphertext attacks. In Antoine Joux, editor, *EUROCRYPT 2009*, volume 5479 of *LNCS*, pages 351–368. Springer, Heidelberg, April 2009.

[8] Shan Chen, Rodolphe Lampe, Jooyoung Lee, Yannick Seurin, and John P. Steinberger. Minimizing the two-round Even-Mansour cipher. In Juan A. Garay and Rosario Gennaro, editors, *CRYPTO 2014, Part I*, volume 8616 of *LNCS*, pages 39–56. Springer, Heidelberg, August 2014.

[9] Shan Chen and John P. Steinberger. Tight security bounds for key-alternating ciphers. In Phong Q. Nguyen and Elisabeth Oswald, editors, *EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 327–350. Springer, Heidelberg, May 2014.

[10] Yuanxi Dai and John P. Steinberger. Indifferentiability of 8-round Feistel networks. In Matthew Robshaw and Jonathan Katz, editors, *CRYPTO 2016, Part I*, volume 9814 of *LNCS*, pages 95–120. Springer, Heidelberg, August 2016.

[11] Shimon Even and Yishay Mansour. A construction of a cipher from a single pseudorandom permutation. In Hideki Imai, Ronald L. Rivest, and Tsutomu Matsumoto, editors, *ASIACRYPT'91*, volume 739 of *LNCS*, pages 210–224. Springer, Heidelberg, November 1993.

[12] Pooya Farshim, Louiza Khati, Yannick Seurin, and Damien Vergnaud. The key-dependent message security of key-alternating Feistel ciphers, 2021. IACR Cryptol. ePrint Arch.

[13] Pooya Farshim, Louiza Khati, and Damien Vergnaud. Security of Even–Mansour ciphers under key-dependent messages. *IACR Trans. Symm. Cryptol.*, 2017(2):84–104, 2017.

[14] Chun Guo and Dongdai Lin. On the indifferentiability of key-alternating Feistel ciphers with no key derivation. In Yevgeniy Dodis and Jesper Buus Nielsen, editors, *TCC 2015, Part I*, volume 9014 of *LNCS*, pages 110–133. Springer, Heidelberg, March 2015.

[15] Chun Guo and Lei Wang. Revisiting key-alternating Feistel ciphers for shorter keys and multi-user security. In Thomas Peyrin and Steven Galbraith, editors, *ASIACRYPT 2018, Part I*, volume 11272 of *LNCS*, pages 213–243. Springer, Heidelberg, December 2018.

[16] Viet Tung Hoang and Phillip Rogaway. On generalized Feistel networks. In Tal Rabin, editor, *CRYPTO 2010*, volume 6223 of *LNCS*, pages 613–630. Springer, Heidelberg, August 2010.

[17] Tetsu Iwata and Kaoru Kurosawa. On the pseudorandomness of the AES finalists - RC6 and Serpent. In Bruce Schneier, editor, *FSE 2000*, volume 1978 of *LNCS*, pages 231–243. Springer, Heidelberg, April 2001.

[18] Louiza Khati, Nicky Mouha, and Damien Vergnaud. Full disk encryption: Bridging theory and practice. In Helena Handschuh, editor, *CT-RSA 2017*, volume 10159 of *LNCS*, pages 241–257. Springer, Heidelberg, February 2017.

[19] Rodolphe Lampe and Yannick Seurin. Security analysis of key-alternating Feistel ciphers. In Carlos Cid and Christian Rechberger, editors, *FSE 2014*, volume 8540 of *LNCS*, pages 243–264. Springer, Heidelberg, March 2015.

[20] Michael Luby and Charles Rackoff. How to construct pseudo-random permutations from pseudo-random functions (abstract). In Hugh C. Williams, editor, *CRYPTO'85*, volume 218 of *LNCS*, page 447. Springer, Heidelberg, August 1986.

[21] Mitsuru Matsui. New block encryption algorithm MISTY. In Eli Biham, editor, *FSE'97*, volume 1267 of *LNCS*, pages 54–68. Springer, Heidelberg, January 1997.

[22] Ueli M. Maurer. A simplified and generalized treatment of Luby-Rackoff pseudorandom permutation generator. In Rainer A. Rueppel, editor, *EUROCRYPT'92*, volume 658 of *LNCS*, pages 239–255. Springer, Heidelberg, May 1993.

[23] Ueli M. Maurer and Krzysztof Pietrzak. The security of many-round Luby-Rackoff pseudo-random permutations. In Eli Biham, editor, *EUROCRYPT 2003*, volume 2656 of *LNCS*, pages 544–561. Springer, Heidelberg, May 2003.

[24] Jacques Patarin. Pseudorandom permutations based on the D.E.S. scheme. In *ESORICS'90*, LNCS, pages 185–187. AFCET, October 1990.

[25] Jacques Patarin. New results on pseudorandom permutation generators based on the DES scheme. In Joan Feigenbaum, editor, *CRYPTO'91*, volume 576 of *LNCS*, pages 301–312. Springer, Heidelberg, August 1992.

[26] Jacques Patarin. About Feistel schemes with six (or more) rounds. In Serge Vaudenay, editor, *FSE'98*, volume 1372 of *LNCS*, pages 103–121. Springer, Heidelberg, March 1998.

[27] Jacques Patarin. Security of random Feistel schemes with 5 or more rounds. In Matthew Franklin, editor, *CRYPTO 2004*, volume 3152 of *LNCS*, pages 106–122. Springer, Heidelberg, August 2004.

[28] Jacques Patarin. The "coefficients H" technique (invited talk). In Roberto Maria Avanzi, Liam Keliher, and Francesco Sica, editors, *SAC 2008*, volume 5381 of *LNCS*, pages 328–345. Springer, Heidelberg, August 2009.

[29] Jacob T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *Journal of the ACM (JACM)*, 27(4):701–717, 1980.

A KDM Security of Even–Mansour via H-Coefficient

Following [13], the r-round Even–Mansour (EM) cipher in a model of computation with access to r permutations $\mathsf{P}_1^{\pm}, \ldots, \mathsf{P}_r^{\pm}$ with domain $\mathcal{M} = \{0,1\}^n$ is a block cipher with key space $\mathcal{K} = \{0,1\}^{(r+1)n}$ and enciphering and deciphering algorithms

$$\mathsf{E}^{\mathsf{P}_1,\ldots,\mathsf{P}_r}((k_1,\ldots,k_{r+1}),p) \coloneqq \mathsf{P}_r(\cdots \mathsf{P}_2(\mathsf{P}_1(p \oplus k_1) \oplus k_2)\cdots) \oplus k_{r+1} \ ,$$
$$\mathsf{D}^{\mathsf{P}_1^-,\ldots,\mathsf{P}_r^-}((k_1,\ldots,k_{r+1}),p) \coloneqq \mathsf{P}_1^-(\cdots \mathsf{P}_{r-1}^-(\mathsf{P}_r^-(p \oplus k_{r+1}) \oplus k_r)\cdots) \oplus k_1 \ .$$

We revisit the KDM security of the basic Even–Mansour cipher with only a single round [13, Section 6.1]. We obtain another (arguably simpler) proof of the KDM security of the 1-round EM construction if the set of functions available to the attacker is claw-free and offset-free. The same restrictions are made in [13, Section 6.1].

Theorem A.1. *Let Φ be a KDM set that is claw-free and offset-free. Then $\mathsf{EM}^{\mathsf{P}}_{k_1,k_2}$ is Φ-KDM-secure. More precisely,*

$$\mathbf{Adv}^{\text{kdm-cca}}_{\mathsf{EM}^{\mathsf{P}}_{k_1,k_2}}(\mathcal{A},\Phi) \le 2q^2 \cdot \mathbf{cf}(\Phi) + qq_{\mathrm{p}} \cdot \mathbf{of}(\Phi) + 3/2 \cdot q^2/(2^n-1) + 3qq_{\mathrm{p}} \cdot 1/2^n \ ,$$

where q is the number of queries of $\mathcal{A}$ to either KDEnc *or* Dec *and q_{p} is the number of its queries to $\mathsf{P}^{\pm}$ in either direction.*

Proof. By Equation 1 and Lemma 3.1, we have

$$\mathbf{Adv}^{\text{kdm-cca}}_{\mathsf{EM}^{\mathsf{P}}_{k_1,k_2}}(\mathcal{A},\Phi) \le q^2 \cdot \mathbf{cf}(\Phi) + \frac{q^2}{2^n - q} + \mathbf{Adv}_{\mathsf{pw},\mathsf{rw}}(\mathcal{A}) \ .$$

Applying the H-coefficient technique to the perfect and real worlds as well as Lemma A.1 and Lemma A.2 below gives

$$\mathbf{Adv}_{\mathsf{pw},\mathsf{rw}}(\mathcal{A}) \le q^2 \cdot \mathbf{cf}(\Phi) + qq_{\mathrm{p}} \cdot \mathbf{of}(\Phi) + q^2/2 \cdot 1/(2^n - q) + 3qq_{\mathrm{p}}/2^n \ .$$

Combining the above two inequalities gives the result.

Real vs. Perfect. In the following, we give the analysis that bounds the advantage of any adversary distinguishing the perfect world pw and the real world rw. We define the bad transcripts for 1-round Even–Mansour as transcripts that contain queries where non-trivial/unexpected collisions exist.

Definition A.1. *A transcript $\tau = (\mathcal{Q}_{\mathsf{EM}}, q_{\mathrm{p}}, \mathbf{k})$ with $\mathbf{k} = (k_1,k_2)$ is said to be bad iff any of the following conditions holds.*

(C-1) there exist $(+,\phi,y) \ne (+,\phi',y') \in \mathcal{Q}_{\mathsf{EM}}$ such that
  (a) $\phi(\mathbf{k}) = \phi'(\mathbf{k})$ or
  (b) $y = y'$;
(C-2) there exist $(+,\phi,y) \ne (-,x',y') \in \mathcal{Q}_{\mathsf{EM}}$ such that
  (a) $\phi(\mathbf{k}) = x'$ or
  (b) $y = y'$;
(C-3) there exist $(+,\phi,y) \in \mathcal{Q}_{\mathsf{EM}}$ and $(u,v) \in \mathcal{Q}_{\mathsf{P}}$ such that
  (a) $\phi(\mathbf{k}) \oplus k_1 = u$ or

(b) $y \oplus k_2 = v$;

(C-4) *there exist* $(-, x, y) \in \mathcal{Q}_{\mathsf{EM}}$ *and* $(u, v) \in \mathcal{Q}_{\mathsf{P}}$ *such that*

(a) $x \oplus k_1 = u$ *or*

(b) $y \oplus k_2 = v$.

Lemma A.1. *Let* $\mathsf{OSp} := \mathsf{Perm}(n)$ *and* $\mathrm{BC} := \mathsf{EM}^{\mathsf{P}}_{k_1,k_2}$. *Let* $\mathcal{A}$ *be a distinguisher making at most* $q \leq 2^n$ *queries to* KDEnc *or* Dec *and* q_{p} *queries to* $\mathsf{P}^{\pm}$ *in either direction. Then with* $\mathcal{T}_{\mathrm{bad}}$ *as defined above,*

$$\Pr[X_{\mathcal{A},\mathsf{pw}} \in \mathcal{T}_{\mathrm{bad}}] \leq q^2 \cdot \mathbf{cf}(\Phi) + q^2/2 \cdot 1/(2^n - q) + qq_{\mathrm{p}} \cdot \mathbf{of}(\Phi) + 3qq_{\mathrm{p}}/2^n \ .$$

Proof. We analyze the probability of each condition in Definition A.1 in the perfect world pw where the keys k_1 and k_2 are sampled at random independently of the oracle answers.[6]

(C-1) For two encryption queries in $\mathcal{Q}_{\mathsf{EM}}$, by Definition 3.1, the probability of condition (C-1a) is at most $\mathbf{cf}(\Phi)$. The probability of condition (C-1b) is zero by the no-pointless-query assumption. Summing over all the possible distinct pairs, condition (C-1) happens with probability at most $q^2/2 \cdot \mathbf{cf}(\Phi)$.

(C-2) Fix an encryption query $(+, \phi, y) \in \mathcal{Q}_{\mathsf{EM}}$ and a decryption query $(-, x', y') \in \mathcal{Q}_{\mathsf{EM}}$.

(a) Here the function ϕ is different from the constant function $\mathbf{k} \mapsto x'$ as otherwise there is a repeat/pointless query $(+, \phi, y) = (-, x', y') \in \mathcal{Q}_{\mathsf{EM}}$. As the key vector $\mathbf{k}$ is sampled uniformly at random after all encryption/decryption query, the probability that $\phi(\mathbf{k}) = x'$ is, by Definition 3.1, at most $\mathbf{cf}(\Phi)$.

(b) The decryption query has to come before the encryption query in the transcript as otherwise the encryption query would be a pointless one. Thus the value y is sampled in a set of size at least $2^n - q$ independently of the value y'. Hence the probability that $\phi(\mathbf{k}) = x'$ is at most $1/(2^n - q)$.

Summing over all the possible distinct pairs, condition (C-2) happens with probability at most $q^2/2 \cdot 1/(2^n - q) + q^2/2 \cdot \mathbf{cf}(\Phi)$.

(C-3) Fix a query to the encryption oracle $(+, \phi, y) \in \mathcal{Q}_{\mathsf{EM}}$ and a query to the public permutation $(u, v) \in \mathcal{Q}_{\mathsf{P}}$.

(a) By Definition 3.2, $\phi(\mathbf{k}) \oplus k_1 = u$ with probability at most $\mathbf{of}(\Phi)$.

(b) As k_2 is sampled uniformly at random and independently of all queries, the collision $y \oplus k_2 = v$ happens with probability at most $1/2^n$.

Summing over all the possible pairs, condition (C-3) happens with probability at most $qq_{\mathrm{p}} \cdot \mathbf{of}(\Phi) + qq_{\mathrm{p}}/2^n$.

(C-4) Fix a decryption query $(-, x, y) \in \mathcal{Q}_{\mathsf{EM}}$ and a public permutation query $(u, v) \in \mathcal{Q}_{\mathsf{P}}$. The keys k_1 and k_2 are drawn uniformly and independently at random at the end. Thus collisions due to (C-4a) and (C-4b) each happen with probability at most $1/2^n$. Summing over all possible pairs, condition (C-4) happens with probability at most $2qq_{\mathrm{p}}/2^n$.

[6] We note that the analysis also holds when k_1 and k_2 are set to a common random value.

The result follows by applying the union bound.

Lemma A.2. *Let τ be a good transcript. Then*

$$\frac{\Pr[X_{\mathcal{A},\mathsf{rw}} = \tau]}{\Pr[X_{\mathcal{A},\mathsf{pw}} = \tau]} \geq 1 \ .$$

Proof. Let $\tau = (\mathcal{Q}_{\mathsf{EM}}, \mathcal{Q}_{\mathsf{P}}, \mathbf{k})$ with $\mathbf{k} = (k_1, k_2)$ be a good transcript, and let q_{enc} and q_{dec} respectively denote the number of queries to KDEnc and Dec, with $q_{\mathrm{enc}} + q_{\mathrm{dec}} = q$. Recall that one has

$$\Pr_{\mathsf{P} \twoheadleftarrow \mathsf{Perm}(n)}[X_{\mathcal{A},\mathsf{pw}} = \tau] = \frac{1}{|\mathcal{K}|} \cdot \frac{1}{(2^n)_{q_{\mathrm{enc}}}} \cdot \frac{1}{(2^n)_{q_{\mathrm{dec}}}} \cdot \frac{1}{(2^n)_{q_{\mathrm{p}}}} \ , \tag{12}$$

where $\mathcal{K} \coloneqq (\{0,1\}^n)^2$ denotes the key space of 1-round Even–Mansour.

In the real world, one obtains the transcript $(\mathcal{Q}_{\mathsf{EM}}, \mathcal{Q}_{\mathsf{P}}, \mathbf{k})$ *iff* P satisfies $q + q_{\mathrm{p}}$ distinct and "compatible" equations. Thus

$$\Pr_{\mathsf{P} \twoheadleftarrow \mathsf{Perm}(n)}[X_{\mathcal{A},\mathsf{rw}} = \tau] = \frac{1}{|\mathcal{K}|} \cdot \frac{1}{(2^n)_{q+q_{\mathrm{p}}}} \ . \tag{13}$$

Combining Equation 12 and Equation 13 we obtain Lemma A.2.