Security Analysis of Key-Alternating Feistel Ciphers*

Rodolphe Lampe** and Yannick Seurin***

February 13, 2014

Abstract. We study the security of *key-alternating Feistel* ciphers, a class of key-alternating ciphers with a Feistel structure. Alternatively, this may be viewed as the study of Feistel ciphers where the pseudorandom round functions are of the form $F_i(x \oplus k_i)$, where k_i is the (secret) round key and F_i is a *public* random function that the adversary is allowed to query in a black-box way. Interestingly, our results can be seen as a generalization of traditional results *à la* Luby-Rackoff in the sense that we can derive results for this model by simply letting the number of queries of the adversary to the public random functions F_i be zero in our general bounds. We make an extensive use of the coupling technique. In particular (and as a result of independent interest), we improve the analysis of the coupling probability for balanced Feistel schemes previously carried out by Hoang and Rogaway (CRYPTO 2010).

Keywords: block cipher, key-alternating cipher, Feistel cipher, coupling, provable security

1 Introduction

Block Ciphers. Block cipher designs roughly fall in two main classes, namely Feistel networks and substitution-permutation networks (SPNs). The primary security notion when studying a block cipher is pseudorandomness: it should be impossible except with negligible probability for any adversary with reasonable resources which has black-box access to a permutation oracle (and potentially its inverse) to distinguish whether it is interacting with the block cipher with a uniformly random key, or with a truly random permutation. Since proving upper bounds on the distinguishing advantage of a general adversary for a concrete block cipher seems out of reach of current techniques, research has focused on proving results by idealizing some components of the block cipher.

[*] © IACR 2014. This is the full version of the article submitted by the authors to the IACR and to Springer-Verlag on February 13, 2014, which appears in the proceedings of FSE 2014.

[**] University of Versailles, France. E-mail: `rodolphe.lampe@gmail.com`. This author is partially supported by the French Direction Générale de l'Armement.

[***] ANSSI, Paris, France. E-mail: `yannick.seurin@m4x.org`. This author is partially supported by the French National Agency of Research: ANR-11-INS-011.

For Feistel networks, most of the provable security work falls in what is usually named the Luby-Rackoff framework, in reference to the seminal work of Luby and Rackoff [10]. In this setting, the round functions of the Feistel scheme are idealized as being uniformly random (and secret). Such results can be directly transposed to the case where the round functions are pseudorandom via a composition theorem (but again proving any lower bound for the pseudorandomness of some concrete function family is out of reach of current techniques). Starting from the Luby-Rackoff result that the 3-round Feistel scheme is a pseudorandom permutation [10], and the proof by Patarin [16] that four rounds yield a strong pseudorandom permutation (where *strong* means that inverse queries to the permutation oracle are allowed), a long series of work established refined bounds for larger number of rounds [11, 12, 21, 17, 8, 18].

For SPN ciphers, provable security results were for a long time limited to resistance to specific attacks such as differential and linear attacks [3]. Recently though, a number of results have been obtained for the ideal *key-alternating* cipher, *a.k.a.* iterated Even-Mansour cipher. An r-round key-alternating cipher is specified by r public permutations on n bits $P_0, \ldots, P_{r-1}$, and encrypts a plaintext x as

$$y = k_r \oplus P_{r-1}(k_{r-1} \oplus P_{r-2}(\cdots P_0(k_0 \oplus x) \cdots)) \, ,$$

where $(k_0, \ldots, k_r)$ are $r+1$ keys of n bits. When $r = 1$, this construction was analyzed and its security established up to $\mathcal{O}(2^{n/2})$ queries by Even and Mansour [6] in the random permutation model for P_0, *i.e.* when the permutation P_0 is a random permutation oracle to which the adversary can make direct and inverse queries. Subsequently, a number of papers improved this seminal result to larger numbers of rounds [1, 9, 20], culminating with the proof by Chen and Steinberger [2] that the r-round ideal key-alternating cipher is secure up to $\mathcal{O}(2^{\frac{rn}{r+1}})$ adaptive, chosen plaintext and ciphertext queries (which is optimal since it matches the best known attack).

Our Contribution. In this work, we study the security of Feistel networks in a setting where the round functions are random and *public* (meaning that the adversary can make oracle queries to these functions), and an independent round key is xored before each round function. In other words, the state at round i is updated according to $(x_L, x_R) \mapsto (x_R, x_L \oplus F_i(x_R \oplus k_i))$, where x_L and x_R are respectively the left and right n-bit halves of the state, and k_i is an n-bit round key. In a sense, this can be seen as transposing the setting of recent works on the ideal key-alternating cipher (which uses the random permutation model) to Feistel ciphers (in the random function model). For this reason, we call such a design a *key-alternating Feistel cipher* (KAF cipher for short). In fact, one can easily see that two rounds of a key-alternating Feistel cipher can be rewritten as a (single-key) one-round Even-Mansour cipher, where the permutation P is a two-round (public and un-keyed) Feistel scheme (see Figure 2). When we want to insist that we consider the model where the round functions F_i are uniformly random public functions, we talk of the *ideal* KAF cipher. Hence, the setting we consider departs from the usual Luby-Rackoff framework in two ways: on one hand, we consider “complex” round functions (random function oracles), but on the other hand we consider the simplest keying procedure, namely xoring.

In this setting, the resources of the adversary are measured by the maximal number q_e of queries to the permutation oracle (and its inverse for strong pseudorandomness), and the maximal number q_f of queries to each round function. In the special case where $q_f = 0$ (*i.e.* the adversary has not access to the random round functions), one exactly recovers the more usual Luby-Rackoff setting, so that our analysis allows to directly derive results for this framework as well by letting q_f be zero.

Our analysis is based on a coupling argument, a well-known tool from the theory of Markov chains. Its use in cryptography has been pioneered by Mironov [14] for the analysis of the shuffle of the RC4 stream cipher, and later by Morris *et al.* for the analysis of maximally unbalanced Feistel schemes [15]. Later use of this technique includes [8, 9]. The work of Hoang and Rogaway [8] is particularly relevant to this paper since they analyzed (among other variants) balanced Feistel schemes, although only in the traditional Luby-Rackoff setting.

Our bounds show that an ideal KAF cipher with r rounds ensures security up to $\mathcal{O}(2^{\frac{tn}{t+1}})$ queries of the adversary, where

- $t = \lfloor \frac{r}{3} \rfloor$ for non-adaptive chosen-plaintext (NCPA) adversaries;
- $t = \lfloor \frac{r}{6} \rfloor$ for adaptive chosen-plaintext and ciphertext (CCA) adversaries.

In the Luby-Rackoff setting ($q_f = 0$), we improve on the previous work of Hoang and Rogaway [8] thanks to a more careful analysis of the coupling argument. Namely we show that the ideal LR cipher is CCA-secure up to $\mathcal{O}(2^{\frac{tn}{t+1}})$ queries, where $t = \lfloor \frac{r-1}{4} \rfloor$. The best proven security bound in the Luby-Rackoff setting remains due to Patarin [18], who showed that the 6-round Feistel cipher is secure up to $\mathcal{O}(2^n)$ queries against CCA distinguishers. However his analysis is much more complicated and does not seem to be directly transposable to the case of KAF ciphers. We feel that the simplicity of the coupling argument is an attractive feature in addition to being immediately applicable to KAF ciphers.

Other Related Work. We are only aware of two previous works in a setting similar to ours. The first is a paper by Ramzan and Reyzin [19], who showed that the 4-round Feistel construction remains (strongly) pseudorandom when the adversary is given oracle access to the two middle round functions. This setting is somehow intermediate between the Luby-Rackoff and the KAF setting. The second paper is by Gentry and Ramzan [7], who showed that the public random permutation of the Even-Mansour cipher $x \mapsto k_1 \oplus P(k_0 \oplus x)$ can be replaced by a 4-round public Feistel scheme, and the resulting construction is still a strong pseudorandom permutation. While their result shows how to construct a strong pseudorandom permutation from only four public random functions (while we need six rounds of Feistel and hence six random functions to get the same result in this paper), their analysis only yields a $\mathcal{O}(2^{n/2})$ security bound. On the contrary, our bounds improve asymptotically with the number of rounds, approaching the information-theoretic bound of $\mathcal{O}(2^n)$ queries. In fact, our results are the first ones beyond the birthday bound for KAF ciphers.

Organization. We start with some definitions and preliminaries in Section 2. In Section 3, we prove a probabilistic lemma which will be useful later to study the coupling probability for Feistel schemes. This result might be of independent interest. Finally, Section 4 contains our main results about the security of ideal KAF ciphers and Luby-Rackoff ciphers.

2 Preliminaries

2.1 General Notation

In all the following, we fix an integer $n \geq 1$. Given an integer $q \geq 1$ and a set S, we denote $(S)^{*q}$ the set of all q-tuples of pairwise distinct elements of S. We denote $[i;j]$ the set of integers k such that $i \leq k \leq j$.

The set of functions of n bits to n bits will be denoted $\mathcal{F}_n$. Let $\boldsymbol{F} = (F_0, \ldots, F_{r-1}) \in (\mathcal{F}_n)^r$ be a tuple of functions, and $u = (u_0, \ldots, u_{r-1})$ and $v = (v_0, \ldots, v_{r-1})$ where for $i = 0, \ldots, r-1$, $u_i = (u_i^1, \ldots, u_i^q) \in (\{0,1\}^n)^q$ and $v_i = (v_i^1, \ldots, v_i^q) \in (\{0,1\}^n)^q$ are q-tuples of n-bit strings. We write $F_i(u_i) = v_i$ as a shorthand to mean that $F_i(u_i^j) = v_i^j$ for all $j = 1, \ldots, q$, and $\boldsymbol{F}(u) = v$ as a shorthand to mean that $F_i(u_i) = v_i$ for all $i = 0, \ldots, r-1$.

2.2 Definitions

Given a function F from $\{0,1\}^n$ to $\{0,1\}^n$ and a n-bit key k, the one-round keyed Feistel permutation is the permutation on $\{0,1\}^{2n}$ defined as:

$$\Psi_k^F(x_L, x_R) = (x_R, x_L \oplus F(x_R \oplus k)),$$

where x_L and x_R are respectively the left and right n-bit halves of the input.

A key-alternating Feistel cipher (KAF cipher for short) with r rounds is specified by r public round functions $F_0, \ldots, F_{r-1}$ from $\{0,1\}^n$ to $\{0,1\}^n$, and will be denoted $\mathtt{KAF}^{F_0,\ldots F_{r-1}}$. It has key-space $(\{0,1\}^n)^r$ and message space $\{0,1\}^{2n}$. It maps a key $(k_0, \ldots, k_{r-1})$ and a plaintext x to the ciphertext defined as:

$$\mathtt{KAF}^{F_0,\ldots F_{r-1}}((k_0, \ldots, k_{r-1}), x) = \Psi_{k_{r-1}}^{F_{r-1}} \circ \cdots \circ \Psi_{k_0}^{F_0}(x).$$

We will denote $\mathtt{KAF}_{k_0,\ldots,k_{r-1}}^{F_0,\ldots F_{r-1}}$ the permutation on $\{0,1\}^{2n}$ mapping a plaintext x to $\mathtt{KAF}^{F_1,\ldots F_r}((k_0, \ldots, k_{r-1}), x)$. When the number of rounds is clear, we simply denote $\boldsymbol{F} = (F_0, \ldots, F_{r-1})$ and $k = (k_0, \ldots, k_{r-1})$, and $\mathtt{KAF}_k^{\boldsymbol{F}}$ the $2n$-bit permutation specified by round functions $\boldsymbol{F}$ and round keys k.

As already noted in [4], a KAF cipher with an even number of rounds can be seen as a special case of a (permutation-based) key-alternating cipher, also known as an iterated Even-Mansour cipher. Indeed, two rounds of a KAF cipher can be rewritten as (see Figure 2):

$$\Psi_{k_{i+1}}^{F_{i+1}} \circ \Psi_{k_i}^{F_i}(x) = (k_{i+1} \| k_i) \oplus \Psi_0^{F_{i+1}} \circ \Psi_0^{F_i}((k_{i+1} \| k_i) \oplus x) \,.$$

Here $\Psi_0^{F_{i+1}} \circ \Psi_0^{F_i}$ is the un-keyed two-round Feistel permutation with round functions F_i and F_{i+1}. Hence this permutation is public since the two round functions F_i and F_{i+1} are public oracles. Recall that the (single-key) Even-Mansour cipher on $2n$ bits is defined from a public permutation P on $2n$ bits as $E(k, x) = k \oplus P(k \oplus x)$, where k is the $2n$-bit key and x the $2n$-bit plaintext [6, 5]. Hence, a $2r'$-round KAF cipher with round functions $(F_0, \ldots, F_{2r'-1})$ and round keys $(k_0, \ldots, k_{2r'-1})$ can be seen as an r'-round key-alternating cipher, where the i-th permutation, $i = 0, \ldots, r'-1$, is the (un-keyed) two-round Feistel scheme with round functions F_{2i} and F_{2i+1}, and the sequence of $2n$-bit keys is $(\tilde{k}_0, \tilde{k}_0 \oplus \tilde{k}_1, \ldots, \tilde{k}_{r'-2} \oplus \tilde{k}_{r'-1}, \tilde{k}_{r'-1})$ with $\tilde{k}_i = k_{2i+1} \| k_{2i}$. (This is more accurately described as the cascade of r' single-key one-round Even-Mansour ciphers.)

As already mentioned in introduction, the iterated Even-Mansour cipher has been subject to extensive security analysis recently (these works often consider the case where all keys are independent, but virtually all the results, in particular [2, 9], apply to the cascade of single-key one-round Even-Mansour schemes). However, these results cannot be transposed to the case of KAF ciphers since they are a special sub-case of the general construction, and hence a dedicated analysis is required. In particular, note that even though the single-key one-round Even-Mansour cipher with a $2n$-bit permutation is provably secure up to $\mathcal{O}(2^n)$ queries against CCA distinguishers, the two-round ideal KAF cipher is easily distinguishable from a random permutation with only two chosen plaintext queries (namely: query the encryption oracle on (x_L, x_R) and (x'_L, x_R), and check whether the respective ciphertexts (y_L, y_R) and (y'_L, y'_R) satisfy $y_L \oplus y'_L = x_L \oplus x'_L$).

2.3 Security Notions

In order to study the pseudorandomness of KAF ciphers, we will consider distinguishers $\mathcal{D}$ interacting with r function oracles $\boldsymbol{F} = (F_0, \ldots, F_{r-1})$ from n bits to n bits and a $2n$-bit permutation oracle (and potentially its inverse) which is either the KAF cipher $\mathtt{KAF}_k^{\boldsymbol{F}}$ specified by $\boldsymbol{F}$ with a uniformly random key $k = (k_0, \ldots, k_{r-1})$, or a perfectly random permutation P (independent from $\boldsymbol{F}$). A (q_e, q_f)-distinguisher is a distinguisher that makes at most q_e queries to the permutation oracle and at most q_f queries to each round function $F_0, \ldots, F_{r-1}$. We will consider only computationally unbounded distinguishers. As usual we restrict ourself *wlog* to deterministic distinguishers that never make redundant queries and always make the maximal number of allowed queries to each oracle.

As in [9], we will define two types of distinguishers, depending on the way it can make its queries to the oracles, namely non-adaptive chosen-plaintext (NCPA) distinguishers, and (adaptive) chosen-plaintext and ciphertext (CCA) distinguishers. We stress that the distinction adaptive/non-adaptive only refers

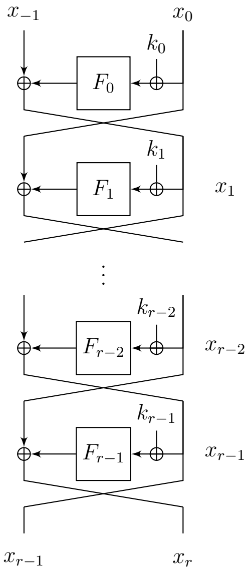

Fig. 1. Notations used for a r-round KAF cipher.

to the queries to the permutation oracle. We now give the precise definitions of these two classes of distinguishers.

Definition 1. *A (q_e, q_f)-NCPA distinguisher runs in two phases:*

1. *in a first phase, it makes exactly q_f queries to each round function F_i. These queries can be adaptive.*
2. *in a second phase, it chooses a tuple of q_e non-adaptive forward queries $x = (x^1, \ldots, x^{q_e})$ to the permutation oracle, and receives the corresponding answers. By non-adaptive queries, we mean that all queries must be chosen before receiving any answer from the permutation oracle, however these queries may depend on the answers received in the previous phase from the round function oracles F_i.*

A (q_e, q_f)-CCA distinguisher is the most general one: it makes adaptively q_f queries to each round function F_i and q_e forward or backward queries to the permutation oracle, in any order (in particular it may interleave queries to the permutation oracle and to the round function oracles).

In all the following, the probability of an event E when $\mathcal{D}$ interacts with $(\boldsymbol{F}, P)$ where P is a random permutation independent from the uniformly random round functions $\boldsymbol{F}$ will simply be denoted $\Pr^*[E]$, whereas the probability of an event E when $\mathcal{D}$ interacts with $(\boldsymbol{F}, \mathtt{KAF}_k^{\boldsymbol{F}})$, where the key $k = (k_0, \ldots, k_{r-1})$ is uniformly random, will simply be denoted $\Pr[E]$. With these notations, the advantage of a distinguisher $\mathcal{D}$ is defined as $|\Pr[\mathcal{D}(1^n) = 1] - \Pr^*[\mathcal{D}(1^n) = 1]|$

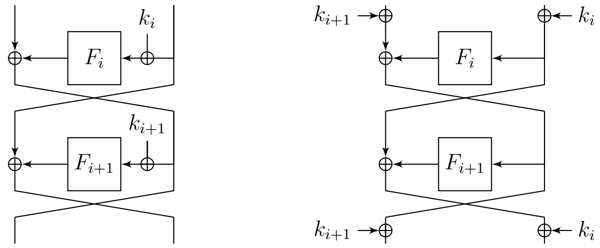

Fig. 2. An alternative view of two rounds of a KAF cipher.

(we omit the oracles in this notation since they can be deduced from the notation $\Pr[\cdot]$ or $\Pr^*[\cdot]$). The maximum advantage of a (q_e, q_f)-ATK-distinguisher against the ideal r-round KAF cipher with n-bit round functions (where ATK is NCPA or CCA) will be denoted $\mathbf{Adv}^{\text{atk}}_{\mathtt{KAF}[n,r]}(q_e, q_f)$.

When $q_f = 0$, *i.e.* in the setting where the distinguisher is not allowed to query the round functions, it is not hard to see that the round keys $k_0, \ldots, k_{r-1}$ do not add any security, so that they can all be taken equal to zero. Hence we are brought back to the usual security framework *à la* Luby-Rackoff, where the round functions are uniformly random and play the role of the secret key (in other words, the key space in this setting is $(\mathcal{F}_n)^r$, where $\mathcal{F}_n$ is the set of all functions from n bits to n bits). In that case, our definitions of an NCPA and a CCA distinguisher correspond to the usual definitions of pseudorandomness of a blockcipher in the standard model (*i.e.* when no additional oracles are involved). In order to emphasize that this setting is qualitatively different, we will denote $\mathbf{Adv}^{\text{atk}}_{\mathtt{LR}[n,r]}(q_e)$ the advantage of a $(q_e, q_f = 0)$-ATK-distinguisher against the ideal r-round Luby-Rackoff cipher.

To sum up, we consider in a single framework two flavors of Feistel ciphers: Luby-Rackoff ciphers, where the round functions are random and secret, and key-alternating Feistel ciphers, where round functions are of the type $F_i(x \oplus k_i)$, where k_i is a secret round key and F_i a public random function oracle.

2.4 Statistical Distance and Coupling

Given a finite event space Ω and two probability distributions μ and ν defined on Ω, the *statistical distance* (or total variation distance) between μ and ν, denoted $\|\mu - \nu\|$ is defined as:

$$\|\mu - \nu\| = \frac{1}{2} \sum_{x \in \Omega} |\mu(x) - \nu(x)| \,.$$

A *coupling* of μ and ν is a distribution λ on $\Omega \times \Omega$ such that for all $x \in \Omega$, $\sum_{y \in \Omega} \lambda(x, y) = \mu(x)$ and for all $y \in \Omega$, $\sum_{x \in \Omega} \lambda(x, y) = \nu(y)$. In other words, λ is a joint distribution whose marginal distributions are resp. μ and ν. The fundamental result of the coupling technique is the following one. See *e.g.* [9] for a proof.

Lemma 1 (Coupling Lemma). *Let μ and ν be probability distributions on a finite event space Ω, let λ be a coupling of μ and ν, and let $(X, Y) \sim \lambda$ (*i.e.* (X, Y) is a random variable sampled according to distribution λ). Then $\|\mu - \nu\| \leq \Pr[X \neq Y]$.*

3 A Useful Probabilistic Lemma

Readers may skip this section at first reading and come back after Lemma 11. In all the following, we interchangeably use the notation $A_i A_j$ to denote the intersection $A_i \cap A_j$ of two events, and more generally $A_{i_1} A_{i_2} \cdots A_{i_k}$ to denote $A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}$.

In this section, we consider the following problem: for $r \geq 2$, let $A_1, \ldots, A_r$ be events defined over the same probability space Ω, satisfying the following "negative dependence" condition:

Definition 2. *Let $p \in]0, 1[$. A sequence of events $A_1, \ldots, A_r$ is said to be p-negatively dependent if for any $i \in [1; r]$ and any subset $S \subseteq [1; i-1]$, one has:*

$$\Pr\left[A_i \middle| \bigcap_{j \in S} A_j \right] \leq p \,,$$

with the convention that an empty intersection is the certain event Ω (hence, in particular $\Pr[A_i] \leq p$ for $i \in [1; r]$).

We denote C_r the event $C_r = \cap_{i=1}^{r-1} (A_i \cup A_{i+1})$, or in a more eloquent form:

$$C_r = (A_1 \cup A_2)(A_2 \cup A_3) \cdots (A_{r-2} \cup A_{r-1})(A_{r-1} \cup A_r) \,.$$

Our goal is to find an upper bound on the probability $\Pr[C_r]$ of this event. Note that C_r is an event in conjunctive normal form, which is not directly amenable to deriving an adequate upper bound. However, once written in disjunctive normal form, one can easily upper bound its probability using the following simple fact:

Lemma 2. *Let $A_1, \ldots, A_r$ be p-negatively dependent events. Then for any $k \in [1; r]$ and any distinct integers $i_1, \ldots, i_k$ in $[1; r]$ one has:*

$$\Pr[A_{i_1} \cdots A_{i_k}] \leq p^k \,.$$

Proof. By induction on k. □

In the following, for a sequence $\alpha \in \{0, 1\}^{r-1}$, we denote α_i the i-th bit of α. By developing straightforwardly event C_r, one obtains the following expression.

Lemma 3.

$$\bigcap_{i=1}^{r-1}(A_i \cup A_{i+1}) = \bigcup_{\alpha\in\{0,1\}^{r-1}} \bigcap_{i=1}^{r-1} A_{i+\alpha_i} \,.$$

Proof. By induction on r. □

For any sequence $\alpha \in \{0,1\}^{r-1}$, we will denote $B_{r,\alpha} = \cap_{i=1}^{r-1} A_{i+\alpha_i}$, so that $C_r = \cup_{\alpha\in\{0,1\}^{r-1}} B_{r,\alpha}$. Depending on α, $B_{r,\alpha}$ may be the intersection of strictly less than $r-1$ events (*e.g.* as soon as $\alpha_i = 1$ and $\alpha_{i+1} = 0$ for some i). Moreover, for two distinct sequences α and α', it may happen that $B_{r,\alpha} \subset B_{r,\alpha'}$. Consider for example the simple case $r = 3$. Then $B_{3,00} = A_1 \cap A_2$ and $B_{3,10} = A_2 \cap A_2 = A_2$, so that $B_{3,00} \subset B_{3,10}$ (see Table 1 for the developed and "reduced" disjunctive form of C_r for r up to 8). This motivates the following definition of *irreducible* sequences, which informally characterize the "minimal" set of events $B_{r,\alpha}$ covering C_r.

Definition 3. *We define the set of* irreducible *sequences as the following regular language (λ denotes the empty string):*

$$\mathcal{I} = \{\lambda, 0\}\{10, 100\}^*\{\lambda, 1\} \,.$$

In other words, irreducible sequences are obtained by concatenating possibly a single 0, then the two patterns 10 and 100 arbitrarily, and finally possibly a single 1. Sequences in $\{0,1\}^* \setminus \mathcal{I}$ are called reducible. *We denote $\mathcal{I}_r$ the set of irreducible sequences of length r.*

It is easy to see that irreducible sequences are exactly sequences α such that 0α does not contain three consecutive zeros or two consecutive ones, but we will not need this characterization here.

The usefulness of irreducible sequences comes from the following lemma.

Lemma 4. $\Pr[C_r] \leq \sum_{\alpha\in\mathcal{I}_{r-1}} \Pr[B_{r,\alpha}]$.

Proof. We show by induction on r that $C_r \subseteq \cup_{\alpha\in\mathcal{I}_{r-1}} B_{r,\alpha}$, from which the lemma follows by the union bound. We first show it directly for $r = 2, 3, 4$. This trivially holds for $r = 2$ since $C_2 = A_1 \cup A_2 = B_{2,0} \cup B_{2,1}$ and the two sequences 0 and 1 are irreducible. For $r = 3$, we have:

$$C_3 = (A_1 \cup A_2)(A_2 \cup A_3) \subseteq A_1A_3 \cup A_2 = B_{3,01} \cup B_{3,10} \,,$$

from which the result follows since 01 and 10 are irreducible while 00 and 11 are reducible. For $r = 4$, we have

$$\begin{aligned} C_4 = (A_1 \cup A_2)(A_2 \cup A_3)(A_3 \cup A_4) &\subseteq A_1A_3 \cup A_2A_3 \cup A_2A_4 \\ &\subseteq B_{4,010} \cup B_{4,100} \cup B_{4,101} \,, \end{aligned}$$

from which the result follows since 010, 100, and 101 are the only irreducible sequences of length 3.

Let us now show the result for $r \geq 5$, assuming that the result holds for $r-1$. We have:

$$\begin{aligned} C_r = C_{r-1} \cap (A_{r-1} \cup A_r) &\subseteq \big(\cup_{\alpha \in \mathcal{I}_{r-2}} B_{r-1,\alpha}\big) \cap (A_{r-1} \cup A_r) \\ &\subseteq \big(\cup_{\alpha \in \mathcal{I}_{r-2}} B_{r,\alpha 0}\big) \cup \big(\cup_{\alpha \in \mathcal{I}_{r-2}} B_{r,\alpha 1}\big) \end{aligned}$$

Hence, it suffices to show that for any irreducible $\alpha \in \mathcal{I}_{r-2}$ such that $\alpha 0$, resp. $\alpha 1$, is reducible, there is an irreducible $\bar{\alpha} \in \mathcal{I}_{r-1}$ such that $B_{r,\alpha 0} \subseteq B_{r,\bar{\alpha}}$, resp. $B_{r,\alpha 1} \subseteq B_{r,\bar{\alpha}}$. We distinguish three cases depending on the form of $\alpha \in \mathcal{I}_{r-2}$. Note that since we assume $r-2 \geq 3$, α contains at least a pattern 10 or 100, so that either $\alpha = \alpha' 10$, or $\alpha = \alpha' 100$, or $\alpha = \alpha' 1$, with $\alpha' \in \{\lambda, 0\}\{10, 100\}^*$ in each case.

- Case 1: $\alpha = \alpha' 10$; in that case, we see that both $\alpha 0 = \alpha' 100$ and $\alpha 1 = \alpha' 101$ are irreducible, so there is nothing to prove.
- Case 2: $\alpha = \alpha' 100$; in that case, $\alpha 1 = \alpha' 1001$ is irreducible, so there is nothing to prove for $\alpha 1$. On the other hand, $\alpha 0 = \alpha' 1000$ is reducible. Let $\bar{\alpha} = \alpha' 1010$. Note that $\bar{\alpha}$ is irreducible. Moreover:

$$\begin{aligned} B_{r,\alpha 0} &= B_{r,\alpha' 1000} = B_{r-4,\alpha'} \cap A_{r-3} A_{r-2} A_{r-1} \\ B_{r,\bar{\alpha}} &= B_{r,\alpha' 1010} = B_{r-4,\alpha'} \cap A_{r-3} A_{r-1} \,, \end{aligned}$$

  so that $B_{r,\alpha 0} \subseteq B_{r,\bar{\alpha}}$.
- Case 3: $\alpha = \alpha' 1$; in that case, $\alpha 0 = \alpha' 10$ is irreducible, so there is nothing to prove for $\alpha 0$. On the other hand, $\alpha 1 = \alpha' 11$ is reducible. Let $\bar{\alpha} = \alpha' 10$. Note that $\bar{\alpha}$ is irreducible. Moreover:

$$\begin{aligned} B_{r,\alpha 1} &= B_{r,\alpha' 11} = B_{r-2,\alpha'} \cap A_{r-1} A_r \\ B_{r,\bar{\alpha}} &= B_{r,\alpha' 10} = B_{r-2,\alpha'} \cap A_{r-1} \,, \end{aligned}$$

  so that $B_{r,\alpha 1} \subseteq B_{r,\bar{\alpha}}$.

Hence $C_r \subseteq \cup_{\alpha \in \mathcal{I}_{r-1}} B_{r,\alpha}$, which concludes the proof. □

We now give an upper bound for the probability of events $B_{r,\alpha}$ for irreducible sequences α. For this, we introduce the following definition.

Definition 4. *The weight of a sequence $\alpha \in \{0,1\}^*$, denoted $\mathbf{w}(\alpha)$, is the number of patterns* 10 *it contains (*i.e. *the number of integers i such that $\alpha_i = 1$ and $\alpha_{i+1} = 0$).*

Lemma 5. *Let $\alpha \in \{0,1\}^{r-1}$ be an irreducible sequence. Then:*

$$\Pr[B_{r,\alpha}] \leq p^{r-1-\mathbf{w}(\alpha)} \,.$$

Proof. Let $k = \mathbf{w}(\alpha)$. By definition, there are exactly k distinct integers $i_1 < \ldots < i_k$ such that for each $i \in \{i_1, \ldots, i_k\}$ we have $\alpha_i = 1$ and $\alpha_{i+1} = 0$, which implies $A_{i+\alpha_i} A_{i+1+\alpha_{i+1}} = A_{i+1} = A_{i+\alpha_i}$. Hence we see that:

$$B_{r,\alpha} \subseteq \bigcap_{\substack{i=1 \\ i \neq i_1+1,\ldots,i_k+1}}^{r-1} A_{i+\alpha_i} \,,$$

which implies the result by Lemma 2 since the event on the right hand side is the intersection of exactly $r-1-k$ distinct events A_j. □

It remains to count the number of irreducible sequences of a given weight.

Lemma 6. *The number of irreducible sequences of length r and weight k is $\binom{k+2}{r-2k}$. Moreover the minimal and maximal weights of an irreducible sequence are respectively $k_{\min} = \lceil \frac{r-2}{3} \rceil$ and $k_{\max} = \lfloor \frac{r}{2} \rfloor$.*

Proof. Let a and b denote respectively the number of patterns 10 and 100 in an irreducible sequence. Clearly the weight k of the sequence satisfies $k = a + b$. Moreover, depending on whether the sequence starts with a single 0 and ends with a single 1, we have the following relation between a and b and the length r of the sequence:

- for sequences of the form $\lambda\{10, 100\}^*\lambda$, one has $2a + 3b = r$
- for sequences of the form $0\{10, 100\}^*\lambda$ or $\lambda\{10, 100\}^*1$, one has $2a+3b = r-1$
- for sequences of the form $0\{10, 100\}^*1$, one has $2a + 3b = r - 2$

Denoting $r' = r$, $r-1$ or $r-2$ depending on the case, we always have $2a+3b = r'$, which combined with $a + b = k$ yields $b = r' - 2k$. For each case the number of possible sequences is $\binom{a+b}{b} = \binom{k}{r'-2k}$. Hence the total number of irreducible sequences of length r and weight k is:

$$\binom{k}{r-2k} + 2\binom{k}{r-1-2k} + \binom{k}{r-2-2k} = \binom{k+2}{r-2k}.$$

The minimal and maximal weights of an irreducible sequence directly follows from the condition $0 \le r - 2k \le k + 2$ for $\binom{k+2}{r-2k}$ to be non-zero. This concludes the proof. □

We are now ready to state and prove the main result of this section, namely the following upper bound for $\Pr[C_r]$.

Lemma 7. *Let $A_1, \ldots, A_r$ be p-negatively dependent events. Then:*

$$\Pr\left[\bigcap_{i=1}^{r-1} (A_i \cup A_{i+1})\right] \le \sum_{k=\lfloor \frac{r}{2} \rfloor}^{\lfloor \frac{2r}{3} \rfloor} \binom{r+1-k}{2r-3k} p^k .$$

Proof. Combining Lemmas 4, 5, and 6 (note that we apply this last lemma to sequences of length $r-1$), we have:

$$\Pr[C_r] \le \sum_{k=\lceil \frac{r-3}{3} \rceil}^{\lfloor \frac{r-1}{2} \rfloor} \binom{k+2}{r-1-2k} p^{r-1-k} .$$

which after the change of variable $r - 1 - k \leftarrow k'$ yields the desired bound. □

We checked Lemma 7 by directly expanding and reducing the conjunctive normal form of C_r for small values of r (see Table 1 for the upper bound obtained for values of r up to 8).

Table 1. Disjunctive normal form of event C_r and upper bound on $\Pr[C_r]$ for r up to 8.

r	C_r (developed and reduced)	$\Pr[C_r]$ upper bound
2	$A_1 \cup A_2$	$2p$
3	$A_1A_3 \cup A_2$	$p + p^2$
4	$A_1A_3 \cup A_2A_3 \cup A_2A_4$	$3p^2$
5	$A_1A_3A_4 \cup A_1A_3A_5 \cup A_2A_3A_5 \cup A_2A_4$	$p^2 + 3p^3$
6	$A_1A_3A_4A_6 \cup A_1A_3A_5 \cup A_2A_3A_5 \cup A_2A_4A_5 \cup A_2A_4A_6$	$4p^3 + p^4$
7	$A_1A_3A_4A_6 \cup A_1A_3A_5A_6 \cup A_1A_3A_5A_7 \cup A_2A_3A_5A_6 \cup$ $A_2A_3A_5A_7 \cup A_2A_4A_5A_7 \cup A_2A_4A_6$	$p^3 + 6p^4$
8	$A_1A_3A_4A_6A_7 \cup A_1A_3A_4A_6A_8 \cup A_1A_3A_5A_6A_8 \cup$ $A_1A_3A_5A_7 \cup A_2A_3A_5A_6A_8 \cup A_2A_3A_5A_7 \cup$ $A_2A_4A_5A_7 \cup A_2A_4A_6A_7 \cup A_2A_4A_6A_8$	$5p^4 + 4p^5$

4 Application to the Security of Key-Alternating Feistel Ciphers

4.1 Coupling For Non-Adaptive Distinguishers

We will first bound the advantage against the r-round ideal KAF cipher $\mathtt{KAF}[n, r]$ of any NCPA distinguisher making at most q_e queries to the cipher and q_f queries to each round function. For this we will upper bound the statistical distance between the outputs of the KAF cipher, conditioned on partial information about round functions obtained through the oracle queries to $F_0, \ldots, F_{r-1}$, and the uniform distribution on $(\{0,1\}^{2n})^{*q_e}$.

For any tuples $u = (u_0, \ldots, u_{r-1})$ and $v = (v_0, \ldots, v_{r-1})$ with $u_i, v_i \in (\{0,1\}^n)^{q_f}$, and $x \in (\{0,1\}^{2n})^{*q_e}$, we denote $\mu_{x,u,v}$ the distribution of the q_e-tuple $y = \mathtt{KAF}_k^{\boldsymbol{F}}(x)$ when the key $k = (k_0, \ldots, k_{r-1})$ is uniformly random, and the round functions $\boldsymbol{F} = (F_0, \ldots, F_{r-1})$ are uniformly random among functions satisfying $\boldsymbol{F}(u) = v$. In the Luby-Rackoff setting ($q_f = 0$), we sometimes simply denote this distribution μ_x. We also denote μ^* the uniform distribution over $(\{0,1\}^{2n})^{*q_e}$. Then we have the following lemma. Its proof is standard and very similar to the proof of [9, Lemma 4], and therefore omitted.

Lemma 8. *Let q_e, q_f be positive integers. Assume that there exists α such that for any tuples $u = (u_0, \ldots, u_{r-1})$, $v = (v_0, \ldots, v_{r-1})$ with $u_i, v_i \in (\{0,1\}^n)^{q_f}$, and $x \in (\{0,1\}^{2n})^{*q_e}$, we have $\|\mu_{x,u,v} - \mu^*\| \leq \alpha$. Then $\mathbf{Adv}^{\mathrm{ncpa}}_{\mathtt{KAF}[n,r]}(q_e, q_f) \leq \alpha$.*

In the remainder of this section, we will establish an upper bound α on $\|\mu_{x,u,v} - \mu^*\|$ by using a coupling argument similar to the one of Hoang and Rogaway [8] (and an improved analysis of this coupling in the Luby-Rackoff setting). In all the following, we fix tuples $u = (u_0, \ldots, u_{r-1})$, $v = (v_0, \ldots, v_{r-1})$ with $u_i = (u_i^1, \ldots, u_i^{q_f}) \in (\{0,1\}^n)^{q_f}$ and $v_i = (v_i^1, \ldots, v_i^{q_f}) \in (\{0,1\}^n)^{q_f}$, and $x = (x^1, \ldots, x^{q_e}) \in (\{0,1\}^{2n})^{*q_e}$.

For $0 \leq \ell \leq q_e - 1$, we denote ν_ℓ the distribution of the $(\ell+1)$ outputs of the KAF cipher when it receives inputs $(x^1, \ldots, x^\ell, x^{\ell+1})$, and ν_ℓ^* the distribution of the $(\ell+1)$ outputs of the KAF cipher when it receives inputs $(x^1, \ldots, x^\ell, z^{\ell+1})$, where $z^{\ell+1}$ is uniformly distributed over $\{0,1\}^{2n} \setminus \{x^1, \ldots, x^\ell\}$ (in both cases the key $k = (k_0, \ldots, k_{r-1})$ is uniformly random, and the round functions $\boldsymbol{F} = (F_0, \ldots, F_{r-1})$ are uniformly random among functions satisfying $\boldsymbol{F}(u) = v$). Then we have the following lemma, whose proof is similar to the one of [15, Lemma 2] (this lemma is not specific to our setting, and applies to any block cipher).

Lemma 9. $\|\mu_{x,u,v} - \mu^*\| \leq \sum_{\ell=0}^{q_e-1} \|\nu_\ell - \nu_\ell^*\|$.

Proof. Deferred to Appendix A. □

We now turn to upper bounding $\|\nu_\ell - \nu_\ell^*\|$ for $0 \leq \ell \leq q_e - 1$. Our goal is to describe a coupling of ν_ℓ and ν_ℓ^*, *i.e.* a joint distribution on pairs of $(\ell+1)$-tuples of $2n$-bit strings, whose marginal distributions are ν_ℓ and ν_ℓ^*. For this, we consider two KAF ciphers in parallel. The first one, $\mathtt{KAF}_k^{\boldsymbol{F}}$, takes as inputs $(x^1, \ldots, x^\ell, x^{\ell+1})$, while the second one, $\mathtt{KAF}_{k'}^{\boldsymbol{F}'}$, where $\boldsymbol{F}' = (F_0', \ldots, F_{r-1}')$, takes as inputs $(x^1, \ldots, x^\ell, z^{\ell+1})$, where $z_{\ell+1}$ is any value in $\{0,1\}^{2n} \setminus \{x^1, \ldots, x^\ell\}$ (we upper bound the statistical distance between the outputs of the two systems for any $z_{\ell+1}$, from which it follows that the same upper bound holds when $z^{\ell+1}$ is uniformly random in $\{0,1\}^{2n} \setminus \{x^1, \ldots, x^\ell\}$). We assume that k is uniformly random and $\boldsymbol{F}$ is uniformly random among function tuples satisfying $\boldsymbol{F}(u) = v$, and we will define k' and $\boldsymbol{F}'$ so that they also satisfy these properties. This will ensure that the marginal distribution of the outputs of the first KAF cipher is ν_ℓ, and the marginal distribution of the outputs of the second KAF cipher is ν_ℓ^*.

The coupling. We now explain how the coupling of the two KAF ciphers is defined. First, the round keys in the second KAF cipher are the same as in the first one, namely $k' = k$. For $1 \leq j \leq \ell + 1$, let x_{-1}^j and x_0^j denote respectively the left and right n-bit halves of x^j and for $1 \leq i \leq r$ let x_i^j be recursively defined as $x_i^j = x_{i-2}^j \oplus F_{i-1}(x_{i-1}^j \oplus k_{i-1})$ (see Figure 1). For any $1 \leq j \leq \ell$ and any $0 \leq i \leq r-1$, we simply set $F_i'(x_i^j \oplus k_i) = F_i(x_i^j \oplus k_i)$ (note that this is consistent with the condition $\boldsymbol{F}'(u) = v$ in case some value $x_i^j \oplus k_i$ belongs to $u_i = (u_i^1, \ldots, u_i^{q_f})$, the set of queries of the distinguisher to the i-th round function). Since the ℓ first queries to the second KAF cipher are the same as the queries made to the first KAF cipher, this ensures that the ℓ first outputs of both ciphers are equal. It remains to explain how the $(\ell+1)$-th queries are coupled. Let $z_{-1}^{\ell+1}$ and $z_0^{\ell+1}$ be respectively the left and right n-bit halves of $z^{\ell+1}$. We will define recursively for $1 \leq i \leq r$ the round values $z_i^{\ell+1} = z_{i-2}^{\ell+1} \oplus F_{i-1}'(z_{i-1}^{\ell+1} \oplus k_{i-1})$. For this, we define two bad events which may happen at round $0 \leq i \leq r-1$ in each KAF cipher. We say that $\mathtt{XColl}_i$ happens if $x_i^{\ell+1} \oplus k_i$ is equal to $x_i^j \oplus k_i$ for some $1 \leq j \leq \ell$ (*i.e.* the input value to the i-th round function when enciphering $x^{\ell+1}$ collides with the input value to the i-th round function when enciphering some previous query x^j). We say that $\mathtt{FColl}_i$ happens if $x_i^{\ell+1} \oplus k_i \in u_i$ (*i.e.*

the input value to the i-th round function when enciphering $x^{\ell+1}$ is equal to one of the oracle queries made to F_i by the distinguisher). We simply denote $\texttt{Coll}_i = \texttt{XColl}_i \cup \texttt{FColl}_i$. Similarly, we say that $\texttt{XColl}'_i$ happens if $z_i^{\ell+1} \oplus k_i$ is equal to $x_i^j \oplus k_i$ for some $1 \leq j \leq \ell$, that $\texttt{FColl}'_i$ happens if $z_i^{\ell+1} \oplus k_i \in u_i$, and we denote $\texttt{Coll}'_i = \texttt{XColl}'_i \cup \texttt{FColl}'_i$. Then, for $i = 0, \ldots, r-1$, we define $F'_i(z_i^{\ell+1} \oplus k_i)$ as follows:

(1) if $\texttt{Coll}'_i$ happens, then $F'_i(z_i^{\ell+1} \oplus k_i)$ is already defined (either because $z_i^{\ell+1} \oplus k_i = x_i^j \oplus k_i$ for some $j \leq \ell$, or by the constraint $\boldsymbol{F}'(u) = v$);
(2) if $\texttt{Coll}'_i$ does not happen but $\texttt{Coll}_i$ happens, $F'_i(z_i^{\ell+1} \oplus k_i)$ is chosen uniformly at random;
(3) if neither $\texttt{Coll}_i$ nor $\texttt{Coll}'_i$ happens, then we define $F'_i(z_i^{\ell+1} \oplus k_i)$ so that $z_{i+1}^{\ell+1} = x_{i+1}^{\ell+1}$, namely:

$$F'_i(z_i^{\ell+1} \oplus k_i) = z_{i-1}^{\ell+1} \oplus x_{i-1}^{\ell+1} \oplus F_i(x_i^{\ell+1} \oplus k_i)\,.$$

One can check that the round functions $\boldsymbol{F}'$ in the second KAF cipher are uniformly random among functions tuples satisfying $\boldsymbol{F}'(u) = v$. This is clear when $F'_i(z_i^{\ell+1} \oplus k_i)$ is defined according to rule (1) or (2). When $F'_i(z_i^{\ell+1} \oplus k_i)$ is defined according to rule (3), then $F_i(x_i^{\ell+1} \oplus k_i)$ is uniformly random since $\texttt{Coll}_i$ does not happen, so that $F'_i(z_i^{\ell+1} \oplus k_i)$ is uniformly random as well. This implies that the outputs of the second KAF cipher are distributed according to ν_ℓ^* as wanted.

We say that the coupling is successful if all the outputs of both KAF ciphers are equal. Since the ℓ first outputs are aways equal by definition of the coupling, this is simply equivalent to having $z_{r-1}^{\ell+1} = x_{r-1}^{\ell+1}$ and $z_r^{\ell+1} = x_r^{\ell+1}$.

The following lemma simply states the key idea of a coupling argument: if the states just after round i when enciphering $x^{\ell+1}$ in the first cipher and $z^{\ell+1}$ in the second cipher, namely $(x_i^{\ell+1}, x_{i+1}^{\ell+1})$ and $(z_i^{\ell+1}, z_{i+1}^{\ell+1})$, are equal, then they remain equal after any subsequent round so that the coupling is successful.

Lemma 10. *If there exists $i \leq r-1$ such that $z_i^{\ell+1} = x_i^{\ell+1}$ and $z_{i+1}^{\ell+1} = x_{i+1}^{\ell+1}$, then the coupling is successful.*

Proof. We proceed by reverse induction. If $i = r-1$, there is nothing to prove. Fix $i < r-1$, and assume that the property is satisfied for $i+1$. Then, if $z_i^{\ell+1} = x_i^{\ell+1}$ and $z_{i+1}^{\ell+1} = x_{i+1}^{\ell+1}$, we simply have to prove that $z_{i+2}^{\ell+1} = x_{i+2}^{\ell+1}$ and the coupling will be successful by the induction hypothesis.

Assume first that $\texttt{Coll}'_{i+1}$ happens, namely $z_{i+1}^{\ell+1} \oplus k_{i+1}$ is equal to $x_{i+1}^j \oplus k_{i+1}$ for some $1 \leq j \leq \ell$ or to $u_{i+1}^{j'}$ for some $1 \leq j' \leq q_f$. In both cases we see that $F'_{i+1}(z_{i+1}^{\ell+1} \oplus k_{i+1}) = F_{i+1}(x_{i+1}^{\ell+1} \oplus k_{i+1})$, so that

$$z_{i+2}^{\ell+1} = z_i^{\ell+1} \oplus F'_{i+1}(z_{i+1}^{\ell+1} \oplus k_{i+1}) = x_i^{\ell+1} \oplus F_{i+1}(x_{i+1}^{\ell+1} \oplus k_{i+1}) = x_{i+2}^{\ell+1}\,.$$

When $\texttt{Coll}'_{i+1}$ does not happen, then $\texttt{Coll}_{i+1}$ does not happen either since we assume $x_{i+1}^{\ell+1} = z_{i+1}^{\ell+1}$, so that by definition of the coupling $F'_{i+1}(z_{i+1}^{l+1} \oplus k_{i+1})$ is chosen such that $z_{i+2}^{\ell+1} = x_{i+2}^{\ell+1}$. □

The following lemma states that if neither $\texttt{Coll}_i$ nor $\texttt{Coll}'_i$ happen for two consecutive rounds, then the coupling is successful. Note that in general we cannot use round 0 to try to couple since we cannot prevent the distinguisher from choosing $x^{\ell+1}$ such that $x_0^{\ell+1} = x_0^j$ for some $j \leq \ell$, in which case $\texttt{Coll}_0$ happens with probability 1.

Lemma 11. *For $i \in [1; r-1]$, define $A_i = \texttt{Coll}_i \cup \texttt{Coll}'_i$. Let $\texttt{Fail}$ be the event that the coupling does not succeed. Then:*

$$\Pr[\texttt{Fail}] \leq \Pr\left[\bigcap_{i=1}^{r-2} (A_i \cup A_{i+1})\right].$$

Proof. Fix $i \in [1; r-2]$. We will show that $\neg(A_i \cup A_{i+1}) \implies \neg\texttt{Fail}$. Indeed, if none of the events $\texttt{Coll}_i$, $\texttt{Coll}'_i$, $\texttt{Coll}_{i+1}$, and $\texttt{Coll}'_{i+1}$ happens, then by definition of the coupling $F'_i(z_i^{\ell+1} \oplus k_i)$ and $F'_{i+1}(z_{i+1}^{\ell+1} \oplus k_{i+1})$ are chosen such that one has $z_{i+1}^{\ell+1} = x_{i+1}^{\ell+1}$ and $z_{i+2}^{\ell+1} = x_{i+2}^{\ell+1}$. By Lemma 10, this implies that the coupling is successful. We just proved that $\neg\texttt{Fail} \supset \cup_{i=1}^{r-2} \neg(A_i \cup A_{i+1})$, which yields the result by negation. □

Hence, the probability that the coupling fails is exactly the probability of event C_{r-1} that we studied in Section 3. At this point, the analysis differs for the KAF and the Luby-Rackoff settings. Indeed, in the LR setting, we can show that events A_i are p-negatively dependent, whereas this does not hold in the KAF setting.

4.2 The KAF Setting

In the KAF setting, we cannot show that events A_i are p-negatively dependent. However, they satisfy some weaker form of negative dependence.

Lemma 12. *For any $i \in [1; r-1]$ and any subset $S \subseteq [1; i-2]$, one has:*

$$\Pr[A_i | \cap_{s \in S} A_s] \leq \frac{2(\ell + 2q_f)}{2^n}.$$

Proof. We need to prove that for any $i \in [1; r-1]$ and any subset $S \subseteq [1; i-2]$, one has:

$$\Pr\left[\texttt{Coll}_i \cup \texttt{Coll}'_i \middle| \cap_{s \in S} A_s\right] \leq \frac{2(\ell + 2q_f)}{2^n}.$$

We upper bound the conditional probability of $\texttt{Coll}_i$, the reasoning for $\texttt{Coll}'_i$ being similar. Recall that $\texttt{XColl}_i$ is the event that $x_i^{\ell+1} \oplus k_i$ is equal to $x_i^j \oplus k_i$ for some $j \in [1; \ell]$, and $\texttt{FColl}_i$ is the event that $x_i^{\ell+1} \oplus k_i$ is equal to $u_i^{j'}$ for some $j' \in [1; q_f]$, and that $\texttt{Coll}_i = \texttt{XColl}_i \cup \texttt{FColl}_i$.

We first consider the probability of $\texttt{FColl}_i$. Since k_i is uniformly random and independent from $\cap_{s \in S} A_s$, this probability is at most $q_f/2^n$.

We now consider the probability of $\mathtt{XColl}_i$, *i.e.* that $x_i^{\ell+1} \oplus k_i = x_i^j \oplus k_i$ for some $j \in [1;\ell]$. Note that this is equivalent to

$$x_{i-2}^{\ell+1} \oplus F_{i-1}(x_{i-1}^{\ell+1} \oplus k_{i-1}) = x_{i-2}^{j} \oplus F_{i-1}(x_{i-1}^{j} \oplus k_{i-1})\,. \tag{1}$$

Here, we face the problem that conditioned on $\mathtt{FColl}_{i-1}$, $F_{i-1}(x_{i-1}^{\ell+1} \oplus k_{i-1})$ is not random because of the constraint $\boldsymbol{F}(u) = v$. Hence, denoting $B = \cap_{s \in S} A_s$, we write:

$$\begin{aligned}\Pr\left[\mathtt{XColl}_i | B\right] = \Pr\left[\mathtt{XColl}_i | B \cap \mathtt{FColl}_{i-1}\right] \Pr\left[\mathtt{FColl}_{i-1} | B\right] \\ + \Pr\left[\mathtt{XColl}_i | B \cap \overline{\mathtt{FColl}_{i-1}}\right] \Pr\left[\overline{\mathtt{FColl}_{i-1}} | B\right] \\ \leq \Pr\left[\mathtt{FColl}_{i-1} | B\right] + \Pr\left[\mathtt{XColl}_i | B \cap \overline{\mathtt{FColl}_{i-1}}\right]\,.\end{aligned}$$

Since k_{i-1} is random and independent from $B = \cap_{s \in S} A_s$ (recall that $S \subseteq [1; i-2]$), we have $\Pr\left[\mathtt{FColl}_{i-1} | B\right] \leq q_f / 2^n$. To upper bound the second probability, note that if $x_{i-1}^{\ell+1} = x_{i-1}^{j}$, then necessarily $x_i^{\ell+1} \neq x_i^j$ since otherwise this would contradict the hypothesis that queries $x^{\ell+1}$ and x^j are distinct. If $x_{i-1}^{\ell+1} \neq x_{i-1}^{j}$, then conditioned on $\overline{\mathtt{FColl}_{i-1}}$, $F_{i-1}(x_{i-1}^{\ell+1} \oplus k_{i-1})$ is uniformly random and equation (1) is satisfied with probability at most 2^{-n} for each j, so that summing over $j \in [1;\ell]$ we obtain $\Pr\left[\mathtt{XColl}_i | B \cap \overline{\mathtt{FColl}_{i-1}}\right] \leq \ell / 2^n$. Hence we have that $\Pr[\mathtt{Coll}_i] \leq (\ell + 2q_f)/2^n$. The reasoning and the bound are the same for the probability that $\mathtt{Coll}'_i$ happens, hence the result. □

Lemma 13. *Let q_e, q_f be positive integers. Then for any tuples $x \in (\{0,1\}^{2n})^{*q_e}$ and $u = (u_0, \ldots, u_{r-1})$, $v = (v_0, \ldots, v_{r-1})$ with $u_i, v_i \in (\{0,1\}^n)^{q_f}$, one has:*

$$\|\mu_{x,u,v} - \mu^*\| \leq \frac{4^t}{t+1} \frac{(q_e + 2q_f)^{t+1}}{2^{tn}} \quad \textit{with} \quad t = \left\lfloor \frac{r}{3} \right\rfloor\,.$$

Proof. Using successively the Coupling Lemma (Lemma 1), Lemma 11, and Lemma 12, one has:

$$\begin{aligned}\|\nu_\ell - \nu_\ell^*\| \leq \Pr\left[\mathtt{Fail}\right] \leq \Pr\left[\bigcap_{i=1}^{r-2} (A_i \cup A_{i+1})\right] \\ \leq \Pr\left[(A_1 \cup A_2)(A_4 \cup A_5) \cdots (A_{3 \cdot \lfloor \frac{r}{3} \rfloor - 2} \cup A_{3 \cdot \lfloor \frac{r}{3} \rfloor - 1})\right] \\ \leq \left(\frac{4(\ell + 2q_f)}{2^n}\right)^t \quad \text{with} \quad t = \left\lfloor \frac{r}{3} \right\rfloor\,.\end{aligned}$$

Hence, by Lemma 9, we have for any tuples x, u, v:

$$\begin{aligned}\|\mu_{x,u,v} - \mu^*\| \leq \sum_{\ell=0}^{q_e - 1} \|\nu_\ell - \nu_\ell^*\| \leq \frac{4^t}{2^{tn}} \sum_{\ell=0}^{q_e-1} (\ell + 2q_f)^t \\ \leq \frac{4^t}{2^{tn}} \int_{\ell=0}^{q_e} (\ell + 2q_f)^t \, d\ell \leq \frac{4^t}{t+1} \frac{(q_e + 2q_f)^{t+1}}{2^{tn}}\,,\end{aligned}$$

which concludes the proof. □

Finally, combining Lemmas 8 and 13, we obtain the following bound for the NCPA-security of the ideal KAF cipher.

Theorem 1. *Let q_e, q_f be positive integers. Then:*

$$\mathbf{Adv}^{\mathrm{ncpa}}_{\mathtt{KAF}[n,r]}(q_e, q_f) \leq \frac{4^t}{t+1} \frac{(q_e + 2q_f)^{t+1}}{2^{tn}} \quad \text{with} \quad t = \left\lfloor \frac{r}{3} \right\rfloor .$$

Hence, the ideal KAF cipher with r rounds ensures NCPA-security up to $\mathcal{O}(2^{\frac{tn}{t+1}})$ queries of the adversary for $t = \lfloor \frac{r}{3} \rfloor$.

4.3 The Luby-Rackoff Setting

In the Luby-Rackoff setting, events A_i can be shown to be p-negatively dependent. This will allow to use the results of Section 3 to upper bound the probability that the coupling fails.

Lemma 14. *In the Luby-Rackoff setting ($q_f = 0$), events $A_1, \ldots, A_{r-1}$ are p-negatively dependent for $p = \frac{2\ell}{2^n}$.*

Proof. We need to prove that for any $i \in [1; r-1]$ and any subset $S \subseteq [1; i-1]$, one has:

$$\Pr\left[\mathtt{Coll}_i \cup \mathtt{Coll}'_i \middle| \cap_{s \in S} A_s\right] \leq \frac{2\ell}{2^n} .$$

In the Luby-Rackoff setting, $q_f = 0$ so that events $\mathtt{FColl}_i$ and $\mathtt{FColl}'_i$ cannot happen. Hence, we simply have to consider events $\mathtt{XColl}_i$ and $\mathtt{XColl}'_i$. Event $\mathtt{XColl}_i$ happens if $x_i^{\ell+1} \oplus k_i = x_i^j \oplus k_i$ for some $j \in [1; \ell]$. Note that this is equivalent to

$$x_{i-2}^{\ell+1} \oplus F_{i-1}(x_{i-1}^{\ell+1} \oplus k_{i-1}) = x_{i-2}^j \oplus F_{i-1}(x_{i-1}^j \oplus k_{i-1}) .$$

If $x_{i-1}^{\ell+1} \neq x_{i-1}^j$, then this happens with probability at most 2^{-n} since in the LR setting F_{i-1} is uniformly random and independent of $\cap_{s \in S} A_s$. If $x_{i-1}^{\ell+1} = x_{i-1}^j$, then necessarily $x_i^{\ell+1} \neq x_i^j$ since otherwise this would contradict the hypothesis that queries $x^{\ell+1}$ and x^j are distinct.[1] Summing over $j \in [1; \ell]$, the probability of $\mathtt{XColl}_i$ is at most $\ell/2^n$. The reasoning is similar for the probability that $\mathtt{XColl}'_i$ happens, hence the result. □

This allows to use Lemma 7 to upper bound the probability that the coupling fails.

Lemma 15. *Let q_e be a positive integer. Then for any tuple $x \in (\{0,1\}^{2n})^{*q_e}$, one has:*

$$\|\mu_x - \mu^*\| \leq \sum_{t=\lfloor \frac{r-1}{2} \rfloor}^{\lfloor \frac{2r-2}{3} \rfloor} \frac{2^t}{t+1} \binom{r-t}{2r-2-3t} \frac{q_e^{t+1}}{2^{tn}} .$$

[1] Note that whether $x_{i-1}^{\ell+1}$ and x_{i-1}^j are distinct or not depends on $\cap_{s \in S} A_s$, so that the event $x_i^{\ell+1} = x_i^j$ is not independent from $\cap_{s \in S} A_s$.

Proof. Using successively the Coupling Lemma (Lemma 1), Lemma 11, and Lemma 7 combined with Lemma 14, one has (note that we apply Lemma 7 with $r-1$ rather than r):

$$\|\nu_\ell - \nu_\ell^*\| \leq \Pr\left[\mathtt{Fail}\right] \leq \Pr\left[\bigcap_{i=1}^{r-2}(A_i \cup A_{i+1})\right] \leq \sum_{t=\lfloor\frac{r-1}{2}\rfloor}^{\lfloor\frac{2r-2}{3}\rfloor} \binom{r-t}{2r-2-3t} \left(\frac{2\ell}{2^n}\right)^t .$$

Hence, by Lemma 9, we have for any tuple $x \in (\{0,1\}^{2n})^{*q_e}$:

$$\begin{aligned}\|\mu_x - \mu^*\| \leq \sum_{\ell=0}^{q_e-1} \|\nu_\ell - \nu_\ell^*\| &\leq \sum_{t=\lfloor\frac{r-1}{2}\rfloor}^{\lfloor\frac{2r-2}{3}\rfloor} \binom{r-t}{2r-2-3t} \sum_{\ell=0}^{q_e-1} \left(\frac{2\ell}{2^n}\right)^t \\ &\leq \sum_{t=\lfloor\frac{r-1}{2}\rfloor}^{\lfloor\frac{2r-2}{3}\rfloor} \binom{r-t}{2r-2-3t} \left(\frac{2}{2^n}\right)^t \int_{\ell=0}^{q_e} \ell^t d\ell \\ &\leq \sum_{t=\lfloor\frac{r-1}{2}\rfloor}^{\lfloor\frac{2r-2}{3}\rfloor} \frac{2^t}{t+1} \binom{r-t}{2r-2-3t} \frac{q_e^{t+1}}{2^{tn}} ,\end{aligned}$$

which concludes the proof. □

Finally, combining Lemmas 8 and 15, we obtain the following bound for the NCPA-security of the ideal LR cipher.

Theorem 2. *Let q_e be a positive integer. Then:*

$$\mathbf{Adv}^{\mathrm{ncpa}}_{\mathtt{LR}[n,r]}(q_e) \leq \sum_{t=\lfloor\frac{r-1}{2}\rfloor}^{\lfloor\frac{2r-2}{3}\rfloor} \frac{2^t}{t+1} \binom{r-t}{2r-2-3t} \frac{q_e^{t+1}}{2^{tn}} .$$

The bound in this theorem is dominated by the term corresponding to $t = \lfloor (r-1)/2 \rfloor$. In particular, when $r = 2r'+1$, the coefficient of this leading term is simply $2^{r'}$, so that the dominating term is simply $2^{r'} q_e^{r'+1}/2^{r'n}$. (Incidentally, this is exactly the bound that was proved in [9] for the r'-round Even-Mansour cipher with n-bit permutations.) In other words, against NCPA-distinguishers, the ideal LR cipher is secure up to $\mathcal{O}(2^{\frac{tn}{t+1}})$ queries of the adversary with $t = \lfloor (r-1)/2 \rfloor$.

Comparison with the Hoang-Rogaway (HR) bound. In [8], Hoang and Rogaway proved the following bound for the security of the ideal Luby-Rackoff cipher $\mathtt{LR}[n,r]$:

$$\mathbf{Adv}^{\mathrm{ncpa}}_{\mathtt{LR}[n,r]}(q_e) \leq \frac{4^t}{t+1} \frac{q_e^{t+1}}{2^{tn}} \quad \text{with} \quad t = \left\lfloor \frac{r}{3} \right\rfloor .$$

In a nutshell, their analysis of the coupling probability proceeds as follows: they show that the probability not to couple over three rounds is at most $4\ell/2^n$, and

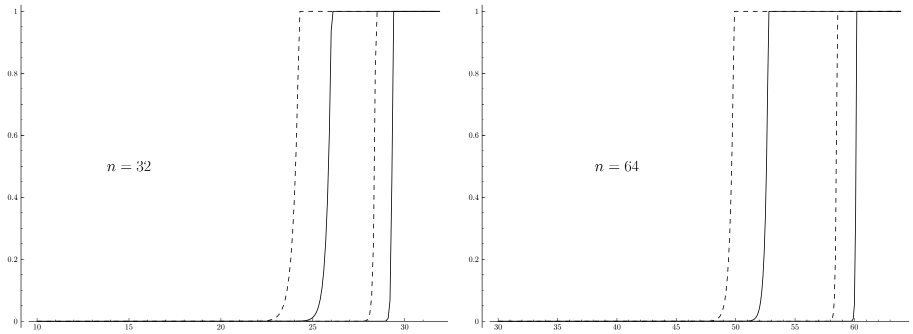

Fig. 3. Proven CCA-security for the ideal Luby-Rackoff cipher $\mathtt{LR}[n, r]$ as a function of $\log_2(q_e)$, the log of the number of adversary's queries (left: $n = 32$, right: $n = 64$). The dashed lines depict the Hoang-Rogaway bound [8], while the solid lines depict the bound proven in this paper. On each graph, the two leftmost curves are for $r = 24$ while the two rightmost curves are for $r = 96$.

then iterate the process for the next three rounds, etc. In effect, they prove an additional security margin only every three rounds. Our analysis of the coupling probability is tighter: we roughly get the same bonus every two rounds, hence substantially ameliorating the security bound. For example, for three rounds, both the HR bound and our bound show that the advantage is upper bounded by $2q_e^2/2^n$ (which is exactly the original Luby-Rackoff bound). While for five rounds the HR bound does not improve, ours already shows that the advantage is upper bounded by $4q_e^3/2^{2n}$, while the HR bound yields a $\mathcal{O}(q_e^3/2^{2n})$-security bound only for six rounds. See also Figure 4.4 for a concrete comparison of the two bounds once leveraged to CCA-security.

4.4 Adaptive Distinguishers

In order to prove security against CCA distinguishers, we use the classical strategy (which was already used in all previous works using a coupling argument [15, 8, 9]) of composing two NCPA-secure ciphers. This is justified by the following lemma.

Lemma 16 ([13]). *If G and H are two blockciphers with the same message space, then for any q:*

$$\mathbf{Adv}^{\mathrm{cca}}_{H^{-1}\circ G}(q) \leq \mathbf{Adv}^{\mathrm{ncpa}}_{G}(q) + \mathbf{Adv}^{\mathrm{ncpa}}_{H}(q)\,,$$

where in $H^{-1} \circ G$ the two block ciphers are independently keyed.

Unfortunately, this result was only proved in the standard model (*i.e.* when the block ciphers do not depend on additional oracles), which allows us to use it only in the Luby-Rackoff setting.

Theorem 3. *Let q_e be a positive integer. Then:*

$$\mathbf{Adv}^{\mathrm{cca}}_{\mathtt{LR}[n,2r'-1]}(q_e) \leq \sum_{t=\lfloor\frac{r'-1}{2}\rfloor}^{\lfloor\frac{2r'-2}{3}\rfloor} \frac{2^{t+1}}{t+1}\binom{r'-t}{2r'-2-3t}\frac{q_e^{t+1}}{2^{tn}}\,.$$

Proof. Let $\mathtt{Rev}$ be the operation defined as $\mathtt{Rev}(x_L, x_R) = (x_R, x_L)$. Then, as already noticed in [12], a $(2r'-1)$-round Feistel scheme with round functions $F_0, \ldots, F_{2r'-2}$ can be written as $\mathtt{Rev}\circ H^{-1}\circ G$, where G and H are r'-round Feistel schemes. This can be seen by writing the middle round function $F_{r'-1}$ as the xor of two independent round functions $F'_{r'-1} \oplus F''_{r'-1}$ (clearly, this does not change the distribution of the outputs of the system): then G is the Feistel scheme with round functions $F_0, \ldots, F_{r'-2}, F'_{r'-1}$, while H is the Feistel scheme with round functions $F_{2r'-2}, \ldots, F_{r'}, F''_{r'-1}$. The result then follows from Lemma 16 and Theorem 2 (clearly composing with $\mathtt{Rev}$ does not change the advantage). □

For a $2r'$-round Luby-Rackoff cipher, we get the same bound as for $2r'-1$ rounds. Again, the bound in this theorem is dominated by the term corresponding to $t = \lfloor (r'-1)/2\rfloor$. Hence, this shows that an r-round Luby-Rackoff cipher ensures CCA-security up to $\mathcal{O}(2^{\frac{tn}{t+1}})$ queries, where $t = \left\lfloor \frac{\lfloor (r+1)/2\rfloor - 1}{2}\right\rfloor = \lfloor\frac{r-1}{4}\rfloor$.

For KAF ciphers, since we cannot apply Lemma 16 directly because the cipher depends on additional oracles, we will appeal to the same strategy as in [9], which relies on the following lemma, a refinement to Lemma 8.

Lemma 17. *Let $G^{\boldsymbol{F}}$ and $H^{\boldsymbol{F}'}$ be two block ciphers with the same message space, where $G^{\boldsymbol{F}}$ and $H^{\boldsymbol{F}'}$ depend respectively on oracles $\boldsymbol{F} = (F_0, \ldots, F_{r-1})$ and $\boldsymbol{F}' = (F'_0, \ldots, F'_{r'-1})$ (this might be arbitrary oracles, not necessarily random functions). Assume that there exists α_G such that for any tuple $x \in (\mathtt{MsgSp}(G))^{*q_e}$ and any tuples $u = (u_0, \ldots, u_{r-1})$ and $v = (v_0, \ldots, v_{r-1})$ where $u_i \in (\mathtt{Dom}(F_i))^{q_f}$ and $v_i \in (\mathtt{Rng}(F_i))^{q_f}$, one has $\|\mu^G_{x,u,v} - \mu^*\| \leq \alpha_G$, and that there exists α_H such that for any tuple $x' \in (\mathtt{MsgSp}(H))^{*q_e}$ and any tuples $u' = (u'_0, \ldots, u'_{r-1})$ and $v' = (v'_0, \ldots, v'_{r-1})$ where $u'_i \in (\mathtt{Dom}(F'_i))^{q_f}$ and $v'_i \in (\mathtt{Rng}(F'_i))^{q_f}$, one has $\|\mu^H_{x',u',v'} - \mu^*\| \leq \alpha_H$.*

(Here, $\mathtt{MsgSp}(E)$ is the message space of block cipher E, $\mathtt{Dom}(F)$ and $\mathtt{Rng}(F)$ are respectively the domain and the range of the oracle F, and the distributions are defined as in Section 4.1, namely $\mu^G_{x,u,v}$ is the distribution of the outputs of $G^{\boldsymbol{F}}$ when receiving inputs x, conditioned on $\boldsymbol{F}(u) = v$, and $\mu^H_{x',u',v'}$ is the distribution of the outputs of $H^{\boldsymbol{F}'}$ when receiving inputs x', conditioned on $\boldsymbol{F}'(u') = v'$.)

Then:

$$\mathbf{Adv}^{\mathrm{cca}}_{(H^{\boldsymbol{F}'})^{-1}\circ G^{\boldsymbol{F}}}(q_e, q_f) \leq 2(\sqrt{\alpha_G} + \sqrt{\alpha_H})\,.$$

Proof. Deferred to Appendix B. □

Theorem 4. *Let q_e, q_f be positive integers. Then:*

$$\mathbf{Adv}^{\mathrm{cca}}_{\mathtt{KAF}[n,2r']}(q_e, q_f) \leq 4\left(\frac{4^t}{t+1}\frac{(q_e+2q_f)^{t+1}}{2^{tn}}\right)^{1/2} \quad \text{with} \quad t = \left\lfloor\frac{r'}{3}\right\rfloor\,.$$

Proof. Since in this context the distinguisher has oracle access to the round functions, we cannot use the same trick as in the proof of Theorem 3 of writing the middle round function of a $(2r'-1)$-round Feistel scheme as the xor of two independent functions. Hence, we consider a $2r'$-round KAF cipher. First, we note that all the results of Section 4.1 apply *mutatis mutandis* to the inverse of a KAF cipher, *i.e.* when the state at round i is updated according $(x_L, x_R) \mapsto (x_R \oplus F_i(x_L \oplus k_i), x_L)$. Hence, we can see this $2r'$-round KAF cipher as the cascade of an r'-round KAF cipher and the inverse of the inverse of an independent r'-round KAF cipher. The result then follows directly by combining Lemmas 17 and 13. □

For a $(2r'+1)$-round KAF cipher, we get the same bound as for a $2r'$-round KAF cipher. Hence, a r-round KAF cipher ensures CCA-security up to $\mathcal{O}(2^{\frac{tn}{t+1}})$ queries in total, where $t = \left\lfloor \frac{\lfloor r/2 \rfloor}{3} \right\rfloor = \left\lfloor \frac{r}{6} \right\rfloor$.

References

[1] A. Bogdanov, L. R. Knudsen, G. Leander, F.-X. Standaert, J. P. Steinberger, and E. Tischhauser. Key-Alternating Ciphers in a Provable Setting: Encryption Using a Small Number of Public Permutations - (Extended Abstract). In D. Pointcheval and T. Johansson, editors, *Advances in Cryptology - EUROCRYPT 2012*, volume 7237 of *Lecture Notes in Computer Science*, pages 45–62. Springer, 2012.

[2] S. Chen and J. Steinberger. Tight Security Bounds for Key-Alternating Ciphers. In *EUROCRYPT 2014*, 2014. To appear. Full version available at http://eprint.iacr.org/2013/222.

[3] J. Daemen and V. Rijmen. *The Design of Rijndael: AES - The Advanced Encryption Standard*. Springer, 2002.

[4] J. Daemen and V. Rijmen. Probability distributions of correlation and differentials in block ciphers. *J. Mathematical Cryptology*, 1(3):221–242, 2007.

[5] O. Dunkelman, N. Keller, and A. Shamir. Minimalism in Cryptography: The Even-Mansour Scheme Revisited. In D. Pointcheval and T. Johansson, editors, *Advances in Cryptology - EUROCRYPT 2012*, volume 7237 of *Lecture Notes in Computer Science*, pages 336–354. Springer, 2012.

[6] S. Even and Y. Mansour. A Construction of a Cipher from a Single Pseudorandom Permutation. *Journal of Cryptology*, 10(3):151–162, 1997.

[7] C. Gentry and Z. Ramzan. Eliminating Random Permutation Oracles in the Even-Mansour Cipher. In P. J. Lee, editor, *Advances in Cryptology - ASIACRYPT 2004*, volume 3329 of *Lecture Notes in Computer Science*, pages 32–47. Springer, 2004.

[8] V. T. Hoang and P. Rogaway. On Generalized Feistel Networks. In T. Rabin, editor, *Advances in Cryptology - CRYPTO 2010*, volume 6223 of *Lecture Notes in Computer Science*, pages 613–630. Springer, 2010.

[9] R. Lampe, J. Patarin, and Y. Seurin. An Asymptotically Tight Security Analysis of the Iterated Even-Mansour Cipher. In X. Wang and K. Sako, editors, *Advances in Cryptology - ASIACRYPT 2012*, volume 7658 of *Lecture Notes in Computer Science*, pages 278–295. Springer, 2012.

[10] M. Luby and C. Rackoff. How to Construct Pseudorandom Permutations from Pseudorandom Functions. *SIAM Journal on Computing*, 17(2):373–386, 1988.

[11] U. M. Maurer. A Simplified and Generalized Treatment of Luby-Rackoff Pseudorandom Permutation Generator. In R. A. Rueppel, editor, *Advances in Cryptology - EUROCRYPT '92*, volume 658 of *Lecture Notes in Computer Science*, pages 239–255. Springer, 1992.

[12] U. M. Maurer and K. Pietrzak. The Security of Many-Round Luby-Rackoff Pseudo-Random Permutations. In E. Biham, editor, *Advances in Cryptology - EUROCRYPT 2003*, volume 2656 of *Lecture Notes in Computer Science*, pages 544–561. Springer, 2003.

[13] U. M. Maurer, K. Pietrzak, and R. Renner. Indistinguishability Amplification. In A. Menezes, editor, *Advances in Cryptology - CRYPTO 2007*, volume 4622 of *Lecture Notes in Computer Science*, pages 130–149. Springer, 2007.

[14] I. Mironov. (Not So) Random Shuffles of RC4. In M. Yung, editor, *Advances in Cryptology - CRYPTO 2002*, volume 2442 of *Lecture Notes in Computer Science*, pages 304–319. Springer, 2002.

[15] B. Morris, P. Rogaway, and T. Stegers. How to Encipher Messages on a Small Domain. In S. Halevi, editor, *Advances in Cryptology - CRYPTO 2009*, volume 5677 of *Lecture Notes in Computer Science*, pages 286–302. Springer, 2009.

[16] J. Patarin. Pseudorandom Permutations Based on the DES Scheme. In G. D. Cohen and P. Charpin, editors, *EUROCODE '90*, volume 514 of *Lecture Notes in Computer Science*, pages 193–204. Springer, 1990.

[17] J. Patarin. Security of Random Feistel Schemes with 5 or More Rounds. In M. K. Franklin, editor, *Advances in Cryptology - CRYPTO 2004*, volume 3152 of *Lecture Notes in Computer Science*, pages 106–122. Springer, 2004.

[18] J. Patarin. Security of balanced and unbalanced Feistel Schemes with Linear Non Equalities. 2010. Available at http://eprint.iacr.org/2010/293.

[19] Z. Ramzan and L. Reyzin. On the Round Security of Symmetric-Key Cryptographic Primitives. In M. Bellare, editor, *Advances in Cryptology - CRYPTO 2000*, volume 1880 of *Lecture Notes in Computer Science*, pages 376–393. Springer, 2000.

[20] J. Steinberger. Improved Security Bounds for Key-Alternating Ciphers via Hellinger Distance. IACR Cryptology ePrint Archive, Report 2012/481, 2012. Available at http://eprint.iacr.org/2012/481.

[21] S. Vaudenay. Decorrelation: A Theory for Block Cipher Security. *Journal of Cryptology*, 16(4):249–286, 2003.

A Proof of Lemma 9

We recall that for any distributions μ and ν on the same set Ω, there always exists a coupling λ_{op}, called an *optimal* coupling, achieving:

$$\|\mu - \nu\| = \Pr_{(X,Y)\sim\lambda_{\mathrm{op}}}[X \neq Y] \,.$$

Lemma.

$$\|\mu_{x,u,v} - \mu^*\| \leq \sum_{\ell=0}^{q_e-1} \|\nu_\ell - \nu_\ell^*\| \,.$$

Proof. For any distribution ν on q_e-tuples of distinct elements of $\{0,1\}^{2n}$, and any $(y^1,\ldots,y^\ell) \in (\{0,1\}^{2n})^{*\ell}$ with $\ell \geq 0$, we denote

$$\nu(y^{\ell+1}|y^1,\ldots,y^\ell) = \Pr[Y^{\ell+1} = y^{\ell+1}|Y^1 = y^1,\ldots,Y^\ell = y^\ell]\,,$$

where $(Y^1,\ldots,Y^{q_e}) \sim \nu$. For $\ell = 0$ we simply denote $\nu(\cdot|\Omega)$ the (unconditional) distribution of the fist coordinate Y^1 (Ω denotes the certain event).

We define a coupling (Y,Z), where $Y = (Y^1,\ldots,Y^{q_e}) \sim \mu_{x,u,v}$ and $Z = (Z^1,\ldots,Z^{q_e}) \sim \mu^*$, as follows. First, we draw (Y_1,Z_1) according to the optimal coupling of $\mu_{x,u,v}(\cdot|\Omega)$ and $\mu^*(\cdot|\Omega)$. Then, for $\ell = 1.\ldots,q_e-1$, we proceed as follows: if $(Y^1,\ldots,Y^\ell) = (Z^1,\ldots,Z^\ell) = (y^1,\ldots,y^\ell)$, we draw $(Y^{\ell+1},Z^{\ell+1})$ according to the optimal coupling of $\mu_{x,u,v}(\cdot|y^1,\ldots,y^\ell)$ and $\mu^*(\cdot|y^1,\ldots,y^\ell)$. Otherwise, if $(Y^1,\ldots,Y^\ell) \neq (Z^1,\ldots,Z^\ell)$, we couple $(Y^{\ell+1},Z^{\ell+1})$ arbitrarily.

Then by the Coupling Lemma:

$$\begin{aligned}
\|\mu_{x,u,v} - \mu^*\| &\leq \Pr[Y \neq Z] \\
&\leq \sum_{\ell=0}^{q_e-1} \Pr[(Y^1,\ldots,Y^\ell) = (Z^1,\ldots,Z^\ell) \wedge Y^{\ell+1} \neq Z^{\ell+1}] \\
&\leq \sum_{\ell=1}^{q_e-1} \mathbb{E}_{Y\sim\mu_{x,u,v}}\left[\|\mu_{x,u,v}(\cdot|Y^1,\ldots,Y^\ell) - \mu^*(\cdot|Y^1,\ldots,Y^\ell)\|\right]\,,
\end{aligned}$$

where

$$\begin{aligned}
&\mathbb{E}_{Y\sim\mu_{x,u,v}}\left[\|\mu_{x,u,v}(\cdot|Y^1,\ldots,Y^\ell) - \mu^*(\cdot|Y^1,\ldots,Y^\ell)\|\right] = \\
&\qquad \sum_{(y^1,\ldots,y^\ell)} \Pr_{Y\sim\mu_{x,u,v}}[(Y^1,\ldots,Y^\ell) = (y^1,\ldots,y^\ell)]\times \\
&\qquad\qquad \|\mu_{x,u,v}(\cdot|y^1,\ldots,y^\ell) - \mu^*(\cdot|y^1,\ldots,y^\ell)\|\,.
\end{aligned}$$

The third inequality above follows from the fact that when $(Y^1,\ldots,Y^\ell) = (Z^1,\ldots,Z^\ell) = (y^1,\ldots,y^\ell)$, $(Y^{\ell+1},Z^{\ell+1})$ is chosen according to the optimal coupling of $\mu_{x,u,v}(\cdot|y^1,\ldots,y^\ell)$ and $\mu^*(\cdot|y^1,\ldots,y^\ell)$.

We also have:

$$\begin{aligned}
\|\nu_\ell - \nu_\ell^*\| &= \frac{1}{2}\sum_{(y^1,\ldots,y^{\ell+1})} |\nu_\ell(y^1,\ldots,y^{\ell+1}) - \nu_\ell^*(y^1,\ldots,y^{\ell+1})| \\
&= \frac{1}{2}\sum_{(y^1,\ldots,y^{\ell+1})} \nu_{\ell-1}(y^1,\ldots,y^\ell)\times \\
&\qquad\qquad \left|\mu_{x,u,v}(y^{\ell+1}|y^1,\ldots,y^\ell) - \mu^*(y^{\ell+1}|y^1,\ldots,y^\ell)\right| \\
&= \sum_{(y^1,\ldots,y^\ell)} \nu_{\ell-1}(y^1,\ldots,y^\ell)\|\mu_{x,u,v}(\cdot|y^1,\ldots,y^\ell) - \mu^*(\cdot|y^1,\ldots,y^\ell)\| \\
&= \mathbb{E}_{Y\sim\mu_{x,u,v}}\left[\|\mu_{x,u,v}(\cdot|Y^1,\ldots,Y^\ell) - \mu^*(\cdot|Y^1,\ldots,Y^\ell)\|\right]\,,
\end{aligned}$$

which concludes the proof. □

B Proof of Lemma 17

In order to prove Lemma 17, we need the following two lemmas. The proof of the first one is very similar to the proof of [9, Lemma 6] and therefore omitted. The second one is exactly [9, Lemma 2].

Lemma 18. *Let q_e, q_f be positive integers. Let $E^{\boldsymbol{F}}$ be a block cipher depending on oracles $\boldsymbol{F} = (F_0, \dots F_{r-1})$. Assume that there exists β such that for any tuples $x, y \in (\texttt{MsgSp}(E))^{*q_e}$, and any tuples $u = (u_0, \dots, u_{r-1})$ and $v = (v_0, \dots, v_{r-1})$ with $u_i \in (\texttt{Dom}(F_i))^{q_f}$ and $v_i \in (\texttt{Rng}(F_i))^{q_f}$, one has*

$$\Pr[\boldsymbol{F}(u) = v \wedge E_k^{\boldsymbol{F}}(x) = y] \geq (1-\beta)\Pr{}^*[\boldsymbol{F}(u) = v \wedge P(x) = y]\,,$$

where the probability on the left hand side is taken over the randomness of $\boldsymbol{F}$ and a uniformly random key k, and

$$\Pr{}^*[\boldsymbol{F}(u) = v \wedge P(x) = y] = \frac{\Pr[\boldsymbol{F}(u) = v]}{M(M-1)\cdots(M-q_e+1)}$$

is the probability when P is a uniformly random permutation independent of $\boldsymbol{F}$. (M denotes $|\texttt{MsgSp}(E)|$.) Then:

$$\mathbf{Adv}_E^{\mathrm{cca}}(q_e, q_f) \leq \beta\,.$$

Lemma 19. *Let Ω be some finite event space and ν be the uniform probability distribution on Ω. Let μ be a probability distribution on Ω such that $\|\mu - \nu\| \leq \varepsilon$. Then there is a set $S \subset \Omega$ such that:*

- $|S| \geq (1-\sqrt{\varepsilon})|\Omega|$
- $\forall x \in S,\ \mu(x) \geq (1-\sqrt{\varepsilon})\nu(x)$

Proof. Define $S = \{x \in \Omega : \mu(x) \geq (1-\sqrt{\varepsilon})\nu(x)\}$. We will show that $|S| \geq (1-\sqrt{\varepsilon})|\Omega|$. Assume for contradiction that $|S| < (1-\sqrt{\varepsilon})|\Omega|$, or equivalently $|\bar{S}| > \sqrt{\varepsilon}|\Omega|$, *i.e.* $\nu(\bar{S}) > \sqrt{\varepsilon}$. By definition, for any $x \in \bar{S}$, $\nu(x) - \mu(x) > \sqrt{\varepsilon}\nu(x)$. Consequently,

$$\nu(\bar{S}) - \mu(\bar{S}) > \sqrt{\varepsilon}\nu(\bar{S}) > (\sqrt{\varepsilon})^2 = \varepsilon\,,$$

a contradiction with $\|\mu - \nu\| \leq \varepsilon$. □

We are now ready to prove Lemma 17. Again, the proof is very similar to the one of [9, Lemma 7].

Proof (of Lemma 17). We recall the notation. Let $G^{\boldsymbol{F}}$ and $H^{\boldsymbol{F}'}$ be two block ciphers with the same message space, where $G^{\boldsymbol{F}}$ and $H^{\boldsymbol{F}'}$ depend respectively on oracles $\boldsymbol{F} = (F_0, \dots, F_{r-1})$ and $\boldsymbol{F}' = (F'_0, \dots, F'_{r'-1})$. We assume that there exists α_G such that for any tuple $x \in (\texttt{MsgSp}(G))^{*q_e}$ and any tuples $u = (u_0, \dots, u_{r-1})$ and $v = (v_0, \dots, v_{r-1})$ where $u_i \in (\texttt{Dom}(F_i))^{q_f}$ and $v_i \in (\texttt{Rng}(F_i))^{q_f}$, one has $\|\mu^G_{x,u,v} - \mu^*\| \leq \alpha_G$, and that there exists α_H such that for any tuple $y \in (\texttt{MsgSp}(H))^{*q_e}$ and any tuples $u' = (u'_0, \dots, u'_{r-1})$ and $v' =$

$(v_0', \dots, v_{r-1}')$ where $u_i' \in (\mathtt{Dom}(F_i'))^{q_f}$ and $v_i' \in (\mathtt{Rng}(F_i'))^{q_f}$, one has $\|\mu^H_{y,u',v'} - \mu^*\| \le \alpha_H$. We also denote $M = |\mathtt{MsgSp}(G)| = |\mathtt{MsgSp}(H)|$.

We now apply Lemma 19 to both G and H. This implies that there exists a subset $S_x \subseteq (\mathtt{MsgSp}(G))^{*q_e}$ of size at least

$$(1 - \sqrt{\alpha_G})M(M-1)\cdots(M-q_e+1)$$

such that for all $z \in S_x$, one has:

$$\mu^G_{x,u,v}(z) \ge (1 - \sqrt{\alpha_G})\frac{1}{M(M-1)\cdots(M-q_e+1)}\,.$$

Similarly, there exists a subset $S_y \subseteq (\mathtt{MsgSp}(H))^{*q_e}$ of size at least

$$(1 - \sqrt{\alpha_H})M(M-1)\cdots(M-q_e+1)$$

such that for all $z \in S_y$, one has:

$$\mu^H_{y,u',v'}(z) \ge (1 - \sqrt{\alpha_H})\frac{1}{M(M-1)\cdots(M-q_e+1)}\,.$$

We can now lower bound the probability that $(H^{\boldsymbol{F}'})^{-1} \circ G^{\boldsymbol{F}}(x) = y$ by summing over all intermediate values $z \in S_x \cap S_y$ the probability that $G^{\boldsymbol{F}}(x) = z$ and $H^{\boldsymbol{F}'}(y) = z$. More precisely:

$$\begin{aligned}
&\Pr[\boldsymbol{F}(u) = v \wedge \boldsymbol{F}'(u') = v' \wedge (H^{\boldsymbol{F}'})^{-1} \circ G^{\boldsymbol{F}}(x) = y] \\
&\qquad \ge \Pr[\boldsymbol{F}(u) = v \wedge \boldsymbol{F}'(u') = v'] \sum_{z \in S_x \cap S_y} \mu^G_{x,u,v}(z)\mu^H_{y,u',v'}(z) \\
&\qquad \ge \Pr[\boldsymbol{F}(u) = v \wedge \boldsymbol{F}'(u') = v'] \frac{|S_x \cap S_y|(1-\sqrt{\alpha_G})(1-\sqrt{\alpha_H})}{(M(M-1)\cdots(M-q_e+1))^2}\,.
\end{aligned}$$

Finally, noting that $|S_x \cap S_y| \ge (1 - \sqrt{\alpha_G} - \sqrt{\alpha_H})M(M-1)\cdots(M-q_e+1)$, and using

$$(1 - \sqrt{\alpha_G} - \sqrt{\alpha_H})(1-\sqrt{\alpha_G})(1-\sqrt{\alpha_H}) \ge 1 - 2(\sqrt{\alpha_G} + \sqrt{\alpha_H})\,,$$

we obtain:

$$\begin{aligned}
&\Pr[\boldsymbol{F}(u) = v \wedge \boldsymbol{F}'(u') = v' \wedge (H^{\boldsymbol{F}'})^{-1} \circ G^{\boldsymbol{F}}(x) = y] \ge \\
&\qquad\qquad (1-\beta)\frac{Pr[\boldsymbol{F}(u) = v \wedge \boldsymbol{F}'(u') = v']}{M(M-1)\cdots(M-q_e+1)}
\end{aligned}$$

where $\beta = 2(\sqrt{\alpha_G} + \sqrt{\alpha_H})$, which with Lemma 18 concludes the proof. □