The Related-Key Analysis of Feistel Constructions

Manuel Barbosa[1(✉)] and Pooya Farshim[2]

[1] HASLab – INESC TEC and Universidade do Minho, Braga, Portugal
mbb@di.uminho.pt
[2] Fachbereich Informatik, Technische Universität Darmstadt, Darmstadt, Germany
farshim@cased.de

Abstract. It is well known that the classical three- and four-round Feistel constructions are provably secure under chosen-plaintext and chosen-ciphertext attacks, respectively. However, irrespective of the number of rounds, no Feistel construction can resist related-key attacks where the keys can be offset by a constant. In this paper we show that, under suitable reuse of round keys, security under related-key attacks can be provably attained. Our modification is simpler and more efficient than alternatives obtained using generic transforms, namely the PRG transform of Bellare and Cash (CRYPTO 2010) and its random-oracle analogue outlined by Lucks (FSE 2004). Additionally we formalize Luck's transform and show that it does not *always* work if related keys are derived in an oracle-dependent way, and then prove it sound under appropriate restrictions.

Keywords: Feistel construction · Luby–rackoff · Related-key attack · Pseudorandom permutation · Random oracle

1 Introduction

Cryptographic algorithms deployed in the real world are subject to a multitude of threats. Many of these threats are accounted for in the theoretical security analysis carried out by cryptographers, but not all. Indeed, many documented cases [14,15,32,39] show that theoretically secure cryptographic algorithms can be vulnerable to relatively simple physical attacks, when these exploit implementation aspects that were abstracted away in the security analysis. For this reason, an enormous research effort has been undertaken in recent years to bridge the gap between physical security and theoretical security.

An important part of this effort has been dedicated to *related-key attacks* (RKA), which were first identified by Knudsen and Biham [9,27] as an important risk on implementations of block ciphers and symmetric-key cryptosystems. The idea behind these attacks is as follows. The security of cryptographic algorithms depends fundamentally on keeping secret keys hidden from attackers for extended periods of time. For this reason, secret keys are typically stored and

C. Cid and C. Rechberger (Eds.): FSE 2014, LNCS 8540, pp. 265–284, 2015.
DOI: 10.1007/978-3-662-46706-0_14

manipulated in protected memory areas and dedicated hardware components. If these mechanisms can be influenced by intrusive techniques (such as fault injection [2]) an adversary may be able to disturb the value of a secret key and observe results computed using the manipulated (likely correlated) key value.

Since the original work of Knudsen and Biham, there have been many reported cases of successful related-key cryptanalysis [8,10,28], and notably of the Advanced Encryption Standard (AES) [11,12]. These results led to the consensual view that RKA resilience should be a standard design goal for low-level cryptographic primitives such as block ciphers and hash functions. For example, in the recent SHA-3 competition, candidates were analyzed with respect to such attacks (c.f. the work of Khovratovich et al. [26]), which played an important role in the selection process.

The importance of including RKA security as a design goal for basic cryptographic components is further heightened by the fact that such low-level primitives are often *assumed* to provide RKA security when used in higher-level protocols. Prominent examples are the key derivation procedures in standard protocols such as EMV [16] and the 3GPP integrity and confidentiality algorithms [25], where efficiency considerations lead to the use of the same block cipher under closely related keys. Similar assumptions arise in constructions of *tweakable ciphers* [29], where a block cipher is called on keys which are offset by XOR-ing tweak values.

Provable RKA security. Bellare and Kohno [6] initiated the theoretical treatment of security under related-key attacks by proposing definitions for RKA-secure pseudorandom functions (PRFs) and pseudorandom permutations (PRPs), and presenting possibility and impossibility results for these primitives. The models proposed in [6] were extended by Albrecht et al. [1] to address the possibility of oracle-dependent attacks in idealized models of computation.

Various important positive results for provably RKA-secure constructions of complex cryptographic primitives were subsequently published in the literature. Bellare and Cash [4] obtained a breakthrough result by presenting a concrete construction of an RKA-secure pseudorandom function based on standard computational assumptions and in the standard model. Bellare, Cash, and Miller [5] present a comprehensive treatment of RKA security for various cryptographic primitives, focusing on the problem of leveraging the RKA resilience of one primitive to construct RKA-secure instances of another. In particular, Bellare et al. present a generic transformation in which an RKA-secure pseudorandom generator can be used to convert instances of standard primitives such as digital signatures and identity-based encryption into RKA-secure ones. Concrete constructions of RKA-secure public-key primitives were given by Wee and by Bellare et al. in [7,42].

Feistel networks. A Feistel network [17,18] is a construction that permits obtaining an efficiently computable and invertible permutation from an efficiently computable function. The network is a cascade of simple Feistel permutations, each relying on a *round function* (f, g, and h) mapping bit strings of length n to outputs of the same length. Here the input and output are shown as tuples

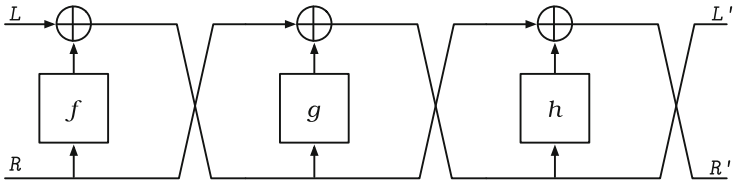

Fig. 1. A three-round Feistel network.

(L, R) and (L', R'), where each component is a string of length n. For any number of rounds, these networks provide an invertible permutation over bit strings of length $2n$. Figure 1 shows an example of a Feistel network with three rounds.

Feistel networks (and generalized variants such as those discussed by Hoang and Rogaway in [23]) have been extensively used in the construction of symmetric cryptosystems (and even asymmetric ones such as RSA-OAEP), since the notable case of the Data Encryption Standard (DES) in the 1970s [18]. In particular, a multitude of block ciphers include Feistel-like constructions in their design, including GOST, MYSTY1, Skipjack, BEAR / LION, CAST-256, RC6, and MARS [38]. For this reason, the security properties of Feistel networks received significant attention in the last decades.

Security of the Feistel construction. In their seminal paper, Luby and Rackoff [30] showed that instantiating the round functions in a Feistel construction with independently keyed secure PRFs is sufficient to obtain a secure PRP. For three rounds of cascading, this result applies when the adversary has access to results of forward computations (i.e., under chosen-plaintext attacks), and for four rounds, the result holds even if the adversary can additionally observe the results of inverse computations (i.e., under chosen-ciphertext attacks).

Following Luby and Rackoff's result, many subsequent works looked at the security of Feistel networks and generalized variants thereof. Important results were obtained with respect to the efficiency of the construction, for example by reducing the necessary key material (c.f. the work of Patarin [36]) and by weakening the security assumptions for some of the round functions as in the work of Naor and Reingold in [35]. In a different direction, the security offered by Feistel networks with increasing numbers of rounds was precisely characterized in a sequence of works by Vaudenay [41], Maurer and Pietrzak [33], Patarin [37] and Hoang and Rogaway [23]. Holenstein, Künzler, and Tessaro [24] used the Feistel construction with fourteen rounds to establish the equivalence of the random-oracle and the ideal-cipher models in a broad range of applications via the indifferentiability framework.

RKA security of Feistel networks. Despite this large body of work on the provable security of the Feistel construction and the positive results on the RKA security of advanced cryptographic primitives referred above, the RKA security of the Feistel construction has received little attention. Indeed, to the best of our knowledge, only the work of Bellare and Kohno [6] touches upon this topic, where a strong negative result is shown: the Feistel construction *irrespective of*

the number of rounds is vulnerable to related-key attacks, provided that the attacker is able to modify as little as a single bit in the key used in the last round function.[1]

Referring to Fig. 1, the attacker would proceed as follows. It would first observe the output (L'_1, R'_1) of the permutation computed on an input (L, R). Then, the adversary would modify round function h to some other function h' by manipulating its key, and observe the output (L'_2, R'_2) computed over the same input. The adversary can now determine whether it is interacting with an ideal permutation or not: If interacting with Feistel, the outputs will *always* satisfy $L'_1 = L'_2$, whereas in for an ideal (keyed) permutation the two outputs will be different with overwhelming probability. This attack is possible whenever the adversary is able to independently tweak the round function of the output stage in the network, independently of the number of rounds, and even if the round functions are instantiated with RKA-secure PRFs.

This vulnerability is relevant for practical applications of Feistel constructions, since many important cryptanalytic results such as those presented by Biryukov et al. [11,12] can be described as utilizing related keys that are derived by XOR-ing the original key with a constant. This in particular permits an attacker to selectively modify the secret key for the output round in a Feistel network and break the security of the construction. In this work we initiate the treatment of provable RKA security of the Feistel constructions. Our main result is to prove is that specific instances of Feistel networks that reuse round keys offer *intrinsic* RKA security against practically relevant classes of RKD functions, and thus overcome the negative result by Bellare and Kohno described above. We now present our contributions in more detail.

CONTRIBUTIONS. Lucks [31] proposes a general solution to the RKA security of any cryptographic primitive in the random-oracle model: hash the secret key before applying it to the cryptosystem. The intuition is that, modeling the hash function as a random oracle, any modification to the secret key will result in a new independent key to be used in the cryptosystem, confining the RKA adversary to standard attacks. The RKA-secure PRG transform of Bellare, Cash, and Miller (BCM) [5] that we discussed above can be seen as a special standard-model analogue of this transform. Somewhat surprisingly, we show that the original random oracle transform does not *always* result in an RKA-secure construction. We amend this by first showing that, under certain restrictions on the RKD set, the random oracle is an RKA-secure PRG, and then extending the BCM result to the random-oracle model. The set of necessary restrictions is permissive enough to include offsetting keys by constants (even if those keys were hashed!) as a particular case. This solution, however, in addition to relying on strong assumptions on the hash function, gives rise to decreased efficiency with respect to the original primitive.

Moreover, the above result only applies to a transformed construction and says nothing about the RKA security of Feistel constructions (which could be

[1] Note that this does not contradict the aforementioned fourteen-round indifferentiability result as the RKA security game is multi-stage.

present in the construction of the hash function itself!). We therefore revisit the Bellare–Kohno (BK) negative result and complement it by characterizing the class of RKA-attacks that *can* be sustained by three and four rounds Feistel networks with independent round keys (i.e., the original Luby–Rackoff constructions). The class of tolerated attacks is highly restrictive and, in particular, it excludes the XOR-with-constants set. (This was to be expected, since the BK attack can be launched using these RKD functions.)

We next consider variants of Feistel constructions in which the keys to round functions in different stages of the network may be *reused*. These variants were already proposed in the literature (c.f. the work by Patarin [36]) due to the efficiency and security benefits of reducing the necessary secret key material. However, we observe that key reuse has the added effect of *limiting* the power of an RKA-adversary in targeting individual round keys. We build on this intuition to obtain our main results: we show that Feistel networks with three (respectively four) rounds can be proven CPA (respectively CCA) RKA secure by relying on an RKA-secure PRF and using specific key assignments that reuse some of the round keys.

Intuitively, our selection of key reusing assignments can be described as follows. It is well known that reusing the same keys in all rounds of the Feistel network or, more generally, any palindromic assignment of the keys, leads to totally insecure constructions. Also, the BK attack rules out key assignments where the key to the output round (in both forward and inverse computations) can be independently thwarted. These restrictions leave few plausible key assignments for intrinsic RKA security of three- and four-round Feistel networks. From these candidates we selected two specific assignments based on *two* PRF keys K_1 and K_2: we consider the key assignment (K_1, K_2, K_2) for the three-round variant, and the (K_1, K_2, K_1, K_2) key assignment for the four-round variant. We prove that the three-round variant is CPA secure and that the four-round variant is CCA secure, both in the RKA setting, assuming that the underlying PRF is RKA secure, and that the RKD set satisfies natural restrictions akin to those adopted, e.g., in [6].

Our results require no other modification to the original constructions in addition to the key assignment and therefore come with minimal modifications to deployed implementations.[2] Put differently, we are able to prove the RKA security of the three-stage (CPA) and four-stage (CCA) Luby–Rackoff constructions, whilst *reducing* the amount of key material and therefore potentially improving the efficiency of the resulting implementations.

For practical applications, the most important aspect of our results is perhaps that they cover the standard classes RKD functions considered in literature, namely those which offset the key by XOR-ing a constant. However, for the sake of generality our presentation relies on a slightly more abstract framework, where we characterize the covered classes of covered RKD functions by defining a set of sufficient restrictions that they must satisfy. This approach also enables a clearer and more modular presentation. For example, as an intermediate step,

[2] Albeit imposing a stronger security assumption on the underlying PRF.

we formalize a notion of multi-key RKA security that may be of independent interest, and relate it to the standard single-key variant.

From a foundational perspective, our result can be seen as one bringing RKA security analysis to the classical constructions of pseudorandom objects. Goldberg and Liskov [19] study this question for building RKA-secure pseudorandom generators (where the seed is interpreted as the key) from one-way functions via Goldreich–Levin [20]. However, the natural questions of transforming RKA-secure PRGs to RKA-secure PRFs via the GGM construction [21] or RKA-secure PRFs to PRPs via the Luby–Rackoff constructions [30] have not been addressed yet. Our results can been seen as giving a positive answer to the latter question.

2 Preliminaries

NOTATION. We write $x \leftarrow y$ for the action of assigning the value y to the variable x. We write $x_1, \ldots, x_n \leftarrow\!\!\$\ \mathsf{X}$ for sampling $x_1, \ldots, x_n$ from a finite set X uniformly at random. If $\mathcal{A}$ is a probabilistic algorithm we denote the action of running $\mathcal{A}$ on inputs $x_1, \ldots, x_n$ with independently chosen coins, and assigning the result to $y_1, \ldots, y_n$ by $y_1, \ldots, y_n \leftarrow\!\!\$\ \mathcal{A}(x_1, \ldots, x_n)$. For a vector $\mathbf{x} = (x_1, \ldots, x_n)$, we define $\mathbf{x}|_i = x_i$. We let $[n] := \{1, \ldots, n\}$. A function $\epsilon(\lambda)$ is negligible if $|\epsilon(\lambda)| \in \lambda^{-\omega(1)}$. PPT as usual abbreviates probabilistic polynomial-time.

KEYED FUNCTIONS AND PERMUTATIONS. Let Dom_λ, Rng_λ, and KSp_λ be three families of finite sets parametrized by a security parameter $\lambda \in \mathbb{N}$. We denote the set of all functions $\rho : \mathsf{Dom}_\lambda \longrightarrow \mathsf{Rng}_\lambda$ by $\mathrm{Func}(\mathsf{Dom}_\lambda, \mathsf{Rng}_\lambda)$. A keyed function is a set of functions in $\mathrm{Func}(\mathsf{Dom}_\lambda, \mathsf{Rng}_\lambda)$ indexed by the elements of the key space KSp_λ. We denote the set of all keyed functions by $\mathrm{Func}(\mathsf{KSp}_\lambda, \mathsf{Dom}_\lambda, \mathsf{Rng}_\lambda)$. By the ideal keyed function, we mean the family of distributions corresponding to choosing a function uniformly at random from $\mathrm{Func}(\mathsf{KSp}_\lambda, \mathsf{Dom}_\lambda, \mathsf{Rng}_\lambda)$. The random oracle is the ideal keyed function where KSp_λ for each $\lambda \in \mathbb{N}$ contains a single key. We denote the set of all permutations on Dom_λ by $\mathrm{Perm}(\mathsf{Dom}_\lambda)$. Note that each permutation uniquely defines its inverse permutation (which is also a member of this set). We define a family of keyed permutations analogously by indexing a set of permutations according to keys in some space KSp_λ. We denote the set of all such keyed permutations by $\mathrm{Perm}(\mathsf{KSp}_\lambda, \mathsf{Dom}_\lambda)$. The ideal keyed permutation (a.k.a. the ideal cipher) is defined as the family of distributions that choose a random element of $\mathrm{Perm}(\mathsf{KSp}_\lambda, \mathsf{Dom}_\lambda)$.

PSEUDORANDOM FUNCTION AND PERMUTATION FAMILY. A pseudorandom function family $\mathsf{PRF} := \{\mathsf{PRF}_\lambda\}_{\lambda \in \mathbb{N}}$ is a family of efficiently implementable keyed functions, i.e., functions $\mathsf{PRF}_\lambda : \mathsf{KSp}_\lambda \times \mathsf{Dom}_\lambda \longrightarrow \mathsf{Dom}_\lambda$, where PRP_λ can be computed in polynomial time in λ, together with an efficient procedure for sampling of keys and domain points which by a slight abuse of notation we denote by $\mathsf{KSp}(1^\lambda)$ and $\mathsf{Dom}(1^\lambda)$, respectively. A pseudorandom permutation family is defined analogously with the extra requirement that the inverse of each permutation in the family is also efficiently computable.

3 RKA-Secure Pseudorandom Functions and Permutations

In this section we introduce the formal framework in which we will analyze the RKA security of Feistel constructions. We begin by formalizing the notion of a family of related-key deriving (RKD) functions, which will parametrize our RKA security notions. Subsequently we introduce a generalization of the standard security model for RKA-secure pseudorandom functions and permutations to a scenario where multiple secret keys may be present in the system and influence the secret key derived by an RKD function. This is the natural setting for analyzing Feistel networks, as they use multiple instances of the same PRF.

Family of RKD sets. A family of n-ary related-key deriving (RKD) sets Φ is a family of RKD sets $\{\Phi_\lambda\}$ consisting of RKD functions ϕ (viewed as circuits) which map an n-tuple of keys in some key space KSp_λ to a new key in KSp_λ, i.e., $\phi : \mathsf{KSp}_\lambda^n \to \mathsf{KSp}_\lambda$. Throughout the paper we assume that membership in any RKD set can be efficiently decided.

Multi-key RKA security. Let $\mathsf{PRP} := \{\mathsf{PRP}_\lambda : \mathsf{KSp}_\lambda \times \mathsf{Dom}_\lambda \longrightarrow \mathsf{Dom}_\lambda\}$ be a PRP family and let $\Phi := \{\Phi_\lambda\}$ be a family of n-ary RKD sets where the implicit key space of the RKD functions in Φ_λ is KSp_λ. Let game $\mathsf{RKCCA}_{\mathsf{PRP},\mathcal{A},\Phi}(1^\lambda)$ be as shown in Fig. 2. We say that PRP is Φ-RKCCA secure if the advantage of any legitimate ppt adversary $\mathcal{A}$ defined as

$$\mathbf{Adv}^{\mathsf{rkcca}}_{\mathsf{PRP},\mathcal{A},\Phi}(\lambda) := 2 \cdot \Pr\left[\mathsf{RKCCA}_{\mathsf{PRP},\mathcal{A},\Phi}(1^\lambda)\right] - 1$$

is negligible as a function of λ. An adversary is legitimate if it queries the RKFn and RKFn^{-1} oracles with functions ϕ in Φ_λ only.[3] We say PRP is Φ-RKCPA secure if the above advantage is negligible for any legitimate ppt adversary $\mathcal{A}$ that never queries its RKFn^{-1} oracle.

In the full version [3] of this paper we prove that under the following natural (but strong) restriction on RKD sets, the single-key and multi-key RKA models are equivalent: we impose that any $\phi \in \Phi_\lambda$ is of the form $\phi : (K_1, \ldots, K_n) \mapsto \psi(K_i)$, where $i \in [n]$ and $\psi : \mathsf{KSp}_\lambda \longrightarrow \mathsf{KSp}_\lambda$ is a unary RKD function.

$\underline{\mathsf{RKCCA}_{\mathsf{PRP},\mathcal{A},\Phi}(1^\lambda)}$:	$\underline{\mathrm{RKFn}(\phi, x)}$:	$\underline{\mathrm{RKFn}^{-1}(\phi, x)}$:
$b \leftarrow\$ \{0,1\}$	$K' \leftarrow \phi(K_1, \ldots, K_n)$	$K' \leftarrow \phi(K_1, \ldots, K_n)$
$\pi \leftarrow\$ \mathrm{Perm}(\mathsf{KSp}_\lambda, \mathsf{Dom}_\lambda)$	If $b = 0$ Return $\pi(K', x)$	If $b = 0$ Return $\pi^{-1}(K', x)$
$K_1, \ldots, K_n \leftarrow\$ \mathsf{KSp}(1^\lambda)$	Return $\mathsf{PRP}(K'x)$	Return $\mathsf{PRP}^{-1}(K', x)$
$b' \leftarrow\$ \mathcal{A}^{\mathrm{RKFn}, \mathrm{RKFn}^{-1}}(1^\lambda)$		
Return $(b' = b)$		

Fig. 2. Game defining the Φ-RKCCA security of a PRP.

[3] Throughout the paper, we assume all the adversaries are, in this sense, legitimate.

REMARK. The multi-key RKA model for PRFs (under chosen-plaintext attacks) is recovered when π is sampled from $\mathrm{Func}(\mathsf{KSp}_\lambda, \mathsf{Dom}_\lambda, \mathsf{Rng}_\lambda)$ and oracle RKFN^{-1} is no longer present. When $n = 1$, we recover the single-key RKA model for PRPs and PRFs as in [6]. The standard model for PRPs/PRFs is one where the RKD sets Φ_λ contain the identity functions $id_\lambda : \mathsf{KSp}_\lambda \longrightarrow \mathsf{KSp}_\lambda; K \mapsto K$ only. The above definition is not the strongest multi-key security model that one can envision. (For instance consider a model where the adversary can choose the arity n.) However, since the applications that we will be considering in this paper have a fixed number of keys, the simpler definition above is sufficient for our purposes.

4 The Random-Oracle Transform

One way to transform a standard pseudorandom permutation to one which resists related-key attacks is to hash the PRP key before using it in the construction [31]. We call this the "Hash-then-PRP" transform. Bellare and Cash [4, Theorem 6.1] prove the soundness of this approach in the *standard* model for a restricted class of RKD functions, when the hash function is replaced by an RKA-secure pseudorandom generator. At first sight it appears that an ideal hash function (i.e., the random oracle) should be a valid instantiation of this construction. However, in the random-oracle model (ROM) the security proof should be carried out in a setting where *all* parties have access to the random oracle (which models the hash function). In this section we consider the implications of this observation, and show that the random oracle does *not* always give rise to a good instantiation of the construction. We provide a set of sufficient conditions that allows us to formally prove that the heuristic transform is sound in the ROM.

RKA-SECURE PRG IN ROM.[4] We define an *oracle* RKD function to be a circuit which contains special oracle gates, and we write an n-ary oracle RKD function as $\phi^H : \mathsf{KSp}^n \to \mathsf{KSp}$. Families of oracle RKD sets are defined in the obvious way.

Let $\mathsf{PRG}^H : \mathsf{Dom} \longrightarrow \mathsf{Rng}$ be a pseudorandom generator in the ROM. Let game $\mathsf{RKA}_{\mathsf{PRG},\mathcal{A},\Phi}$ be as shown in Fig. 3. We say that PRG is Φ-RKA secure if

$\underline{\mathrm{RKA}_{\mathsf{PRG},\mathcal{A},\Phi}(1^\lambda)}$:	$\underline{\mathrm{RKFN}(\phi)}$:
$\rho \leftarrow\$ \mathrm{Func}(\mathsf{Dom}, \mathsf{Rng})$	$K' \leftarrow \phi^H(K_1, \ldots, K_n)$
$H \leftarrow\$ \mathrm{Func}(\mathsf{Dom}', \mathsf{Rng}')$	If $b = 0$ Return $\rho(K')$
$K_1, \ldots, K_n \leftarrow\$ \mathsf{Dom}(1^\lambda)$	Return $\mathsf{PRG}^H(K')$
$b \leftarrow\$ \{0, 1\}$	
$b' \leftarrow\$ \mathcal{A}^{\mathrm{RKFN},\mathrm{RO}}(1^\lambda)$	$\underline{\mathrm{RO}(X)}$:
Return $(b' = b)$	Return $H(X)$

Fig. 3. Game defining the Φ-RKA security of a PRG. An adversary is legitimate if it queries RKFN with a $\phi \in \Phi_\lambda$ only.

[4] We remark that this game can also be seen as extension of correlated-input secure hashing [22] to the random-oracle model.

the advantage of any PPT adversary $\mathcal{A}$ as defined below is negligible in λ.

$$\mathbf{Adv}^{\mathsf{rka}}_{\mathsf{PRG},\Phi,\mathcal{A}}(\lambda) := 2 \cdot \Pr\left[\mathsf{RKA}_{\mathsf{PRF},\mathcal{A},\Phi}(1^\lambda)\right] - 1 \ .$$

The question that we wish to answer is under which conditions does the random oracle itself (i.e., when $\mathsf{PRG}^H(X) := H(X)$) constitute an RKA-secure PRG. The attack we now show and the ensuing discussion demonstrate that this is only the case if we exclude certain forms of *oracle-dependent* related-key attacks.

The attack. Consider a unary RKD set containing the identity function and an oracle-dependent RKD function ϕ^H [1]: $\Phi := \{id : K \mapsto K,\ \phi^H : K \mapsto H(K)\}$. Here, H denotes the random oracle. Now consider an adversary that first requests a PRG value of the seed by querying id to the RKFn oracle. It receives as response a value y which is either $H(K)$, when $b = 1$, or $\rho(K)$ when $b = 0$, where ρ is an independent random oracle. The adversary now queries y to RO to get a new value z which is either $H(H(K))$ or $H(\rho(K))$. Finally, the adversary queries ϕ^H to RKFn to get a value z' which is either $H(H(K))$ or $\rho(H(K))$. Now, when $b = 1$, then $z = z'$ with probability 1. When $b = 0$ the values z and z' would only match if $H(\rho(K)) = \rho(H(K))$. The probability of this event is negligible, so the adversary wins with overwhelming probability by returning $(z = z')$.

We now define a sufficient set of restrictions on oracle RKD sets that allow us to prove a ROM analogue of the result by Bellare and Cash [4]. Intuitively the restrictions are strong enough to rule out attacks that follow the above pattern.

Output unpredictability. A family of oracle RKD sets Φ is output unpredictable (UP) if the following definition of advantage is negligible in λ for any PPT adversary $\mathcal{A}$ outputting a list of RKD functions and a list of keys.

$$\mathbf{Adv}^{\mathsf{up}}_{\mathcal{A},\Phi}(\lambda) := \Pr\left[\exists\ (\phi, \mathbf{K}^*) \in \mathsf{L}_1 \times \mathsf{L}_2 \ \text{ s.t. } \ \phi^H(\mathbf{K}) = \mathbf{K}^* : H \leftarrow\!\!\$\ \mathsf{Func}(\mathsf{KSp}, \mathsf{KSp}); \mathbf{K} \leftarrow\!\!\$\ \mathsf{KSp}^n; (\mathsf{L}_1, \mathsf{L}_2) \leftarrow\!\!\$\ \mathcal{A}^H(1^\lambda)\right]$$

Claw-freeness. A family of oracle RKD sets Φ is claw-free (CF) if the following definition of advantage is negligible in λ for any PPT adversary $\mathcal{A}$ outputting a list of RKD functions.

$$\mathbf{Adv}^{\mathsf{cf}}_{\mathcal{A},\Phi}(\lambda) := \Pr\left[\exists\ \phi_1^H, \phi_2^H \in \mathsf{L} \ \text{ s.t. } \ \phi_1^H(\mathbf{K}) = \phi_2^H(\mathbf{K}) \wedge \phi_1^H \neq \phi_2^H : H \leftarrow\!\!\$\ \mathsf{Func}(\mathsf{KSp}, \mathsf{KSp}); \mathbf{K} \leftarrow\!\!\$\ \mathsf{KSp}^n; \mathsf{L} \leftarrow\!\!\$\ \mathcal{A}^H(1^\lambda)\right]$$

Query independence. A family of oracle RKD sets Φ is query independent (QI) if the following definition of advantage is negligible in λ for any PPT adversary $\mathcal{A}$ outputting a list of RKD functions.

$$\mathbf{Adv}^{\mathsf{qi}}_{\mathcal{A},\Phi}(\lambda) := \Pr\left[\exists \phi_1^H, \phi_2^H \in \mathsf{L} \ \text{ s.t. } \ \phi_1^H(\mathbf{K}) \in \mathsf{Qry}[\phi_2^H(\mathbf{K})] : H \leftarrow\!\!\$\ \mathsf{Func}(\mathsf{KSp}, \mathsf{KSp}); \mathbf{K} \leftarrow\!\!\$\ \mathsf{KSp}^n; \mathsf{L} \leftarrow\!\!\$\ \mathcal{A}^H(1^\lambda)\right]$$

Here, $\mathsf{Qry}[\phi_2^H(\mathbf{K})]$ denotes the set of queries placed to H by ϕ_2^H when run on a vector of keys $\mathbf{K}$. Note that RKD functions ϕ_1^H and ϕ_2^H need not be distinct.

We recover the standard (non-oracle) definition of output unpredictability and claw-freeness [6], when the RKD functions do not make any oracle queries: the random oracle can be simulated using lazy sampling. Query independence is trivially satisfied for such non-oracle RKD functions.

We now prove that the random oracle is an RKA-secure pseudorandom generator under the above restrictions on the oracle RKD set, and then build on this result to establish security of the Hash-then-PRP transform in the random oracle model. Looking ahead, this result allows us to take a Luby–Rackoff PRP and generically transform it to obtain an RKA-secure PRP. In subsequent sections we will explore less intrusive, more efficient alternatives that take advantage of the inner structure of the Feistel construction.

Theorem 1 (RKA Security of the Random Oracle). *Let Φ be a family of oracle RKD sets. For any Φ-RKCCA adversary $\mathcal{A}$ against the pseudorandom generator $\mathsf{PRG}^H(K) := H(K)$, there are adversaries $\mathcal{A}_1$, $\mathcal{A}_2$, and $\mathcal{A}_3$ such that*

$$\mathbf{Adv}^{\mathsf{rkcpa}}_{\mathsf{PRG},\mathcal{A},\Phi}(\lambda) \leq \mathbf{Adv}^{\mathsf{up}}_{\mathcal{A}_1,\Phi}(\lambda) + 2 \cdot \mathbf{Adv}^{\mathsf{cf}}_{\mathcal{A}_2,\Phi}(\lambda) + \mathbf{Adv}^{\mathsf{qi}}_{\mathcal{A}_3,\Phi}(\lambda) \ ,$$

Proof (Sketch). We give only the intuition; the details of the proof can be found in the full version. Assume, without loss of generality, that the adversary never places repeat queries to its RKFn and RO oracles. Let Game_0 denote the RKA game where H is used in the RKFn oracle (i.e., the challenge bit is 1).

We modify Game_0 to Game_1 by implementing the H oracle in the RKFn oracle in a forgetful way (i.e., we won't keep track of repetitions), but leaving it unchanged for the explicit queries made through RO and the indirect queries placed by the oracle RKD functions. Note that in this game the adversary receives independently and uniformly distributed strings from either of its oracles.

Games Game_0 and Game_1 are identical unless one of the following events takes place: (1) A repeat H query is placed as a result of an explicit RO query and an output of an oracle RKD function queried to RKFn: this leads to a violation of the output unpredictability. (2) There is a repeat query to H as a result of two distinct RKFn queries: this leads to a claw-freeness break. (3) There is a repeat H query as a result of a query to RKFn and an indirect query placed by an oracle RKD function to H: this breaks the query-independence property.

We now modify Game_1 to Game_2 by changing the forgetful oracle and implementing it using an independently chosen (non-forgetful) random oracle. The games are identical unless there is a claw among the RKD functions queried to RKFn, which by the above analysis happens with negligible probability. Finally note that Game_2 is identical to the RKA game conditioned on $b = 0$.[5] □

In the full version we state and prove the analogue of the RKA-secure PRG transform of Bellare, Cash, and Miller [5], which in combination with Theorem 1 establishes security of the Hash-then-PRP transform in the random oracle model.

[5] This transition my be avoided by observing that Game_0 and Game_2 are also identical until the same bad events which separate Game_0 and Game_1.

5 The Feistel Construction

In this section we recall the formal definitions related to the Feistel constructions and introduce the notion of key assignment. We also establish a general result that permits shifting the analysis of Feistel networks with any number of rounds where the round functions are instantiated with an RKA-secure PRF to a more convenient setting where the round functions are instantiated with the ideal keyed function.

Feistel networks. The one-round Feistel construction and its inverse with respect to a function f is defined as

$$\mathbf{F}[f](L,R) := (R, L \oplus f(R)) \quad \text{and} \quad \mathbf{F^{-1}}[f](L,R) := (R \oplus f(L), L) \ .$$

The n-round Feistel construction with respect to functions $f_1, \ldots, f_n$ is defined recursively via the following equations (see Fig. 1 for a pictorial representation).

$$\begin{aligned} \mathbf{F}[f_1, \ldots, f_n](L,R) &:= \mathbf{F}[f_2, \ldots, f_n](\mathbf{F}[f_1](L,R)) \ , \\ \mathbf{F^{-1}}[f_1, \ldots, f_n](L,R) &:= \mathbf{F^{-1}}[f_1, \ldots, f_{n-1}](\mathbf{F^{-1}}[f_n](L,R)) \end{aligned}$$

Typically, functions $f_i(\cdot)$ are implemented using a PRF under independently generated keys $K_1, \ldots, K_n$. In our analysis we will also consider the conceptual setting in which these functions are instantiated by an ideal keyed function ρ, again under independently generated keys $K_1, \ldots, K_n$. In this case we denote the constructions by $\mathbf{F}^{\mathsf{PRF}}[K_1, \ldots, K_n]$ and $\mathbf{F}^{\rho}[K_1, \ldots, K_n]$, respectively.

Key assignment. A key assignment is a family of circuits $\kappa_\lambda : \overline{\mathsf{KSp}}_\lambda \longrightarrow \mathsf{KSp}^n$, where $\overline{\mathsf{KSp}}$ is an arbitrary key space. Given $\kappa := \{\kappa_\lambda\}$ and $K \in \overline{\mathsf{KSp}}_\lambda$, we consider the associated n-round Feistel construction $\mathbf{F}^{\mathsf{PRF}}[\kappa(K)]$. When the key $K \in \overline{\mathsf{KSp}}_\lambda$ is randomly generated, we denote the construct by $\mathbf{F}^{\mathsf{PRF}}[\kappa]$. For example, the Hash-then-PRP transform of the previous section can be viewed as $\mathbf{F}^{\mathsf{PRF}}[H]$. We are, however, interested in simple key assignments of the form $\kappa : (K_1, \ldots, K_m) \mapsto (K_{i_1}, \ldots, K_{i_n})$, where $i_1, \ldots, i_n$ are fixed indices in $[m]$. We will therefore compactly write the Feistel construction associated to the simple key assignment above by $\mathbf{F}^{\mathsf{PRF}}[i_1, \ldots, i_n]$. For example, when $\kappa(K_1, K_2) := (K_1, K_2, K_2)$, the associated Feistel construction is written as $\mathbf{F}^{\mathsf{PRF}}[1, 2, 2]$.

When the round functions in a 3-round Feistel construction are instantiated with a PRF under independent keys, we obtain the classic CPA-secure Luby–Rackoff pseudorandom permutation. When 4 rounds are used, we obtain its CCA-secure counterpart. As stated in the introduction, Bellare and Kohno [6] observed that if an adversary can arbitrarily tamper with the key used in the last round of any Feistel network, then a successful related-key attack is possible (even if the underlying PRF is RKA secure).

As discussed in the previous section, by applying the Hash-then-PRP transform to the Luby–Rackoff construction, we can obtain a PRP which resists related-key attacks. The underlying PRG can be instantiated in the standard model via an RKA-secure PRF (e.g., that used in the Luby–Rackoff construction) as suggested in [4] or, outside the standard model, using random oracles.

Both transformations, however, come with two major drawbacks. The first drawback is the performance penalty. The standard-model approach incurs a total of six PRF computations in the 3-round network: 3 calls to generate the keys and another 3 to compute the PRP.[6] (The total number of calls is eight for the CCA case.) Note that the amortized complexity of the construction cannot be brought down back to 3 by storing the generated keys, as related-key attacks can be applied to these keys. In the ROM transform (on top of strong assumptions) the penalty will be smaller if the hash function is more efficient than the PRF. However, this leads to a second drawback: the transform is software/hardware intrusive, as extra circuitry for the implementation key-derivation procedure need to be added.

For these reasons, in the remainder of the paper, we will consider more efficient alternatives to obtaining RKA-secure PRPs by exploring directly the structure of Feistel constructions via simple key assignments. Before doing so, we prove a general theorem that allows us to move from the security analysis of a Feistel construction with respect to an RKA-secure PRF to a setting in which the round functions are instantiated by the ideal keyed function. Our result holds for any number of rounds and any key assignment.

Theorem 2 (Computational RKA Transition). *Let Φ be a family of RKD sets containing functions of the form $\mathsf{KSp}^m \longrightarrow \mathsf{KSp}^m$ and let $\kappa : \mathsf{KSp}^m \longrightarrow \mathsf{KSp}^n$ be a key assignment. Define $\Psi := \cup_i (\kappa \circ \Phi)_i$, where $(\kappa \circ \Phi)_i$ is the RKD set obtained by composing function in Φ by κ on the right and then projecting to i-th component for $1 \leq i \leq n$. Let ρ denote the ideal keyed function, and let* PRF *denote be a pseudorandom function. Then for any* PPT *adversary $\mathcal{A}$ against the* Φ-RKCCA *security of $\mathbf{F}^{\mathsf{PRF}}[\kappa]$, there is an adversary $\mathcal{B}$ against the* Ψ-RKCPA *security of* PRF *such that*

$$\mathbf{Adv}^{\mathsf{rkcca}}_{\mathbf{F}^{\mathsf{PRF}}[\kappa],\mathcal{A},\Phi}(\lambda) \leq \mathbf{Adv}^{\mathsf{rkcca}}_{\mathbf{F}^{\rho}[\kappa],\mathcal{A},\Phi}(\lambda) + \mathbf{Adv}^{\mathsf{rkcpa}}_{\mathsf{PRF},\mathcal{B},\Psi}(\lambda).$$

An analogous result holds for Φ-RKCPA *adversaries.*

Proof (Sketch). We start with the Φ-RKCCA game for $\mathbf{F}^{\mathsf{PRF}}[\kappa]$ and replace all n rounds function in the Feistel construction with an ideal keyed function. Any change in an adversary $\mathcal{A}$'s advantage in the two games can be used to break the (multi-key) Ψ-RKCCA security of PRF via an adversary $\mathcal{B}$. Algorithm $\mathcal{B}$ runs $\mathcal{A}$ and answers its forward queries to the Feistel construction as follows. On input (ϕ, x) where $\phi \in \Phi$, algorithm $\mathcal{B}$ sets $\psi_1 := (\kappa \circ \phi)|_1$ and calls the RKFn oracle on (ψ_1, x) to get x_1. It then sets $\psi_2 := (\kappa \circ \phi)|_2$, queries RKFn on (ψ_2, x_1) to get x_2. Algorithm $\mathcal{B}$ continues in this way for all n rounds and returns the final output. Backward queries can be also handled similarly using RKFn in the reverse direction. Clearly, according to the challenge bit b used in the Ψ-RKCPA game, $\mathcal{B}$ simulates the Φ-RKCCA game with the same challenge bit b for algorithm $\mathcal{A}$. □

[6] The overall tightness of security obtained via [4, Theorem 6.1] is also worse than what we obtain here, although it is possible that it can be improved via a direct analysis.

6 CPA Security: The 3-Round Constructions

As we discussed in the Introduction, no palindromic assignment of keys in a three-round Feistel construction can result in a CPA-secure PRP, since the construction in the forward direction can be used to compute inverses, and a trivial distinguishing attack emerges. Moreover, if the key used in the third round is independent of those used in first and second rounds, then the BK attack applies. Under these restriction, for simple key assignments and up to relabeling of the indices, we are left with only one 3-round construction which can potentially achieve CPA security under related-key attacks: $\mathbf{F}^{\mathsf{PRF}}[1,2,2]$.

The main proof of this section is an information-theoretic argument showing that $\mathbf{F}^{\rho}[1,2,2]$ is Φ-RKCPA secure for Φ's which are claw-free and switch-free. Combined with Theorem 2 in the previous section, this implies that $\mathbf{F}^{\mathsf{PRF}}[1,2,2]$ offers *intrinsic* RKA-resilience, in the sense that it permits leveraging the RKA-security properties of its underlying PRF.

For the security proof in this and the next sections we need to rely on an additional restriction on RKD sets.

Switch-freeness. A family of RKD sets Φ with arity $n > 2$ is called switch-free (SF) if the advantage of any PPT adversary $\mathcal{A}$ as defined below is negligible as a function of λ.

$$\mathbf{Adv}^{\mathsf{sf}}_{\mathcal{A},\Phi}(\lambda) := \Pr\left[(\exists \phi_1, \phi_2 \in \mathsf{L})(\exists i \neq j \in [n])\ \ \phi_1(\mathbf{K})|_i = \phi_2(\mathbf{K})|_j : \mathbf{K} \leftarrow\!\!\$\ \mathsf{KSp}^n; \mathsf{L} \leftarrow\!\!\$\ \mathcal{A}(1^\lambda)\right]$$

We note that the switch-free and claw-free properties are in general incomparable. Consider, for example, the set consisting of *id* and a function which agrees with *id* on all but one point. This set is switch-free but not claw-free. Conversely, consider the set consisting of *id* and the map $(K_1, K_2) \mapsto (K_2, K_1)$. This set is claw-free but not switch-free.

Theorem 3 ($\mathbf{F}^{\rho}[1,2,2]$ Security). *Let Φ be a family of RKD sets. The $\mathbf{F}^{\rho}[1,2,2]$ construction is Φ-RKCPA secure in the ideal keyed function model if Φ is claw-fee and switch-free. More precisely, for every Φ-RKCPA adversary $\mathcal{A}$ placing at most $Q(\lambda)$ queries to* RKFn*, there exist adversaries $\mathcal{B}_1$ and $\mathcal{B}_2$ such that*

$$\mathbf{Adv}^{\mathsf{rkcpa}}_{\mathbf{F}^{\rho}[1,2,2],\mathcal{A},\Phi}(\lambda) \leq \mathbf{Adv}^{\mathsf{rf/rp}}_{\mathcal{A},\Phi}(\lambda) + 2\mathbf{Adv}^{\mathsf{sf}}_{\mathcal{B}_1,\Phi}(\lambda) + 4\mathbf{Adv}^{\mathsf{cf}}_{\mathcal{B}_2,\Phi}(\lambda) + \frac{2^5 Q(\lambda)^2}{|\mathsf{Dom}_\lambda|}\,.$$

Proof (Intuition). We give a high-level description of the proof and refer the reader to the full version for the full details. We assume, without loss of generality, that the adversary is non-repeating in the sense that it not place redundant repeat queries to its oracle. We start with the Φ-RKCPA game, and consider an modified game where the round functions are implemented as follows. The first round is implemented using a consistent ideal keyed function (as in the original construction). The second and third round functions, however, will be forgetful and return independent random values on each invocation irrespective of the input values.

Note that the outputs of the network computed according to this game are random, and, by an appropriate strengthening of the classical PRP/PRF switching lemma (given in the full version), they are also indistinguishable from an ideal keyed permutation. Furthermore, in this game the values of the outputs of the first round function remain hidden as they are masked by random values generated in the third round.

Now the game above differs from the original CPA game due to inconsistencies occurring in computing round function values both across and within the same round, when the adversary is able to cause collisions in round function inputs in the original CPA game that are ignored in the game above. There are five such pairs of inconsistencies possible (we keep track of queries to the first round, so inconsistencies wont happen here). If there is a collision in inputs, which include the keys, to the first and second or first and third rounds, then the keys collide and this event leads to a violation of switch-freeness. Now suppose the inconsistency is due to a collision between the inputs to the third round function. Since the outputs of the second round function are randomly chosen at each invocation, this event happens with probability roughly $Q(\lambda)^2/|\mathsf{Dom}_\lambda|$ by the birthday bound. Collisions between the inputs to the second and third rounds also happen with negligible probably as the outputs of the first round remain hidden from the adversary. Finally, we are left with collisions in the inputs to the second round function. Note that this means that the keys input to this function are identical. Now if the keys or right halves of the inputs used in the first round in the two colliding queries were different, then the outputs of the first round function would be random and independent, and a collision would happen with a negligible probability (as first-round outputs are hidden). If the keys and right halves were identical, a collision can only take place if the left halves are also identical. However, due to the non-repeating condition, in this case we must have that the queried RKD functions are distinct, and consequently a claw in the RKD set is discovered. □

We emphasize that we do not claim the switch-free and claw-free restrictions are *necessary* for non-existence of attacks. On the other hand, these restrictions are akin to those adopted in previous works on RKA security, and do not overly constrain the practical applicability of our results. For example, the n-ary RKD sets for XOR-ing with constants defined by

$$\Phi_m^{\oplus} := \{\phi_{C_1,\ldots,C_m} : (K_1,\ldots,K_m) \mapsto (K_1 \oplus C_1,\ldots,K_m \oplus C_m) \ : \\ (C_1,\ldots,C_m) \in \mathsf{KSp}^m\}$$

can be easily shown to satisfy these restrictions. Unpredictability follows from the fact that each map in the set induces a permutation over the keys (and hence output distribution is uniform). For claw-freeness suppose we are given two distinct RKD functions. Suppose they differ in their i-th component, i.e., $C_i \neq C_i'$. Then, since the keys K_i and K_j are chosen independently and uniformly at random, the probability that the i-th output keys match, i.e., that $K_i \oplus C_i = K_j \oplus C_i'$, is negligible. Switch-freeness follows from a similar argument.

Note finally that the restrictions needed for the reduction to the RKA security of the underlying PRF are easily shown to be satisfied by the above set, as the key assignment is simple. We obtain the following corollary.

Corollary 1. $\mathbf{F}^{\mathsf{PRF}}[1,2,2]$ *is a* $\Phi_2^{\oplus}$-RKCPA-*secure pseudorandom permutation, if* PRF *is a* $\Phi_1^{\oplus}$-RKCPA-*secure PRF.*

In the full version we characterize the RKA security of the original three-round Luby–Rackoff construction, where three independent round keys are used.

7 CCA Security: The 4-Round Constructions

It is well known that the $\mathbf{F}^{\rho}[1,2,3]$ construction is CCA insecure. For example, the attacker can proceed as follows: 1) Choose arbitrary L, R, L', query $\mathrm{RKF}_N(L,R)$ to obtain C_1 and query $\mathrm{RKF}_N(L',R)$ to obtain C_2; 2) Query $\mathrm{RKF}_N^{-1}(C_2 \oplus (0, L \oplus L'))$ to obtain C_3; 3) Check if $(C_1 \oplus C_2 \oplus \mathsf{Swap}(C_3))$ is same as R. The same attack applies to all Feistel networks with three rounds, independently of the key assignment, and so there is no hope that such constructions can achieve any form of CCA security.

In this section we investigate the CCA security of 4-round constructions under related-key attacks. Due to the generic related-key attacks that we listed in the previous section (insecurity of palindromic key assignment and tampering with the last key), and the fact the in the CCA model the construction can be accessed in both the forward and backward directions, the only candidates than can potentially satisfy RKCCA security are: $\mathbf{F}^{\rho}[1,1,2,1]$, its inverse $\mathbf{F}^{\rho}[1,2,1,1]$, $\mathbf{F}^{\rho}[1,1,2,2]$, $\mathbf{F}^{\rho}[1,2,1,2]$, and $\mathbf{F}^{\rho}[1,2,3,1]$. In this work, we look at $\mathbf{F}^{\rho}[1,2,1,2]$.

The proof of RKCCA security for the $\mathbf{F}[1,2,1,2]$ construction, as in the RKCPA case, has two components: a computational part allowing transition from PRFs to ideal keyed functions, and an information-theoretic argument that establishes security when the construction is instantiated with an ideal keyed function. The first part of the proof follows from Theorem 2. We now prove the second part.

Theorem 4 ($\mathbf{F}[1,2,1,2]$ Security). *Let* Φ *be a family of RKD sets. Suppose* Φ *is claw-fee and switch-free. Then the* $\mathbf{F}^{\rho}[1,2,1,2]$ *construction is* Φ-RKCPA *secure in the ideal keyed function model. More precisely, for every* Φ-RKCCA *adversary* $\mathcal{A}$ *placing at most* $Q(\lambda)$ *queries to* RKF_N *or* RKF_N^{-1}*, there are* $\mathcal{B}_1$ *and* $\mathcal{B}_2$ *such that*

$$\mathbf{Adv}^{\mathsf{rkcca}}_{\mathbf{F}^{\rho}[1,2,1,2],\mathcal{A},\Phi}(\lambda) \leq \mathbf{Adv}^{\mathsf{rf/rp}}_{\mathcal{A},\Phi}(\lambda) + 2\mathbf{Adv}^{\mathsf{sf}}_{\mathcal{B}_1,\Phi}(\lambda) + 8\mathbf{Adv}^{\mathsf{cf}}_{\mathcal{B}_2,\Phi}(\lambda) + \frac{2^8 Q(\lambda)^2}{|\mathsf{Dom}_\lambda|}.$$

Proof (Intuition). We give a high-level description of the proof and refer the reader to the full version for the full details. The proof follows the same structure as Theorem 3, but it is slightly more complex due to the possibility of collisions occurring in the inputs of the round functions when they are used in the RKF$_N$

and RKF_N^{-1} oracles. We assume, without loss of generality, that the adversary is non-repeating in the sense that it does not place repeat queries to either of its oracles, does not decipher an enciphered value, and does not enciphered a deciphered value.

We start with the Φ-RKCCA game where the round functions faithfully implement an ideal keyed function. We then consider a game where all round functions are implemented in a *forgetful* way except that (1) the input round function in RKF_N is consistent and also keeps track of the entries contributed from RKF_N^{-1}'s output round; and (2) the input round function in RKF_N^{-1} is consistent and also keeps track of the entries contributed from RKF_N's output round. In this game the output values of the construction are random and hence indistinguishable from those from an ideal keyed permutation by the PRP/PRF switching lemma. Furthermore, the outputs of the input round functions in the RKF_N and RKF_N^{-1} oracles remain hidden as they are masked by the forgetful action of the remaining round functions.

As in the CPA setting, we need to keep track of collisions in the inputs to various pairs of round functions with lead to inconsistencies, as follows. (1) First forward and fourth backward rounds are consistent with previous queries due to their implementation. (2) Collisions between even and odd numbered round functions in both directions happen with negligible probability due to switch-freeness. (3) Inputs to the third and fourth forward rounds collide with negligible probability with the previous inputs of all other round functions due to the randomness of their respective inputs. A similar argument applies to the first and second backward rounds. (4) Collisions between first forward and third forward/backward rounds happen with negligible probability as the outputs of the fourth backward round are random and remain hidden from the adversary. A similar argument applies to the fourth/second rounds in the backward direction. (5) Collisions between second forward and fourth forward/backward rounds happen with negligible probability as outputs of the first forward round are random and remain hidden. A similar argument applies to the second round in the backward direction. (6) Finally, collisions between the second forward round and itself or second backward can be bounded using the fact that outputs of the first forward round are random remain hidden, combined with claw-freeness, similarly to the CPA case. A similar argument applies to the third backward round. □

As in the CPA setting, the family $\Phi_4^{\oplus}$ satisfies all the prerequisites required for the reduction to the RKA security of the underlying PRF and we obtain the following corollary.

Corollary 2. $\mathbf{F}^{\mathsf{PRF}}[1,2,1,2]$ *is a* $\Phi_2^{\oplus}$-RKCCA-*secure PRP, if the underlying* PRF *is a* $\Phi_1^{\oplus}$-RKCCA-*secure PRF.*

In the full version we give a positive result for the RKA security of the original 4-round Luby–Rackoff construction.

8 Directions for Further Research

This works takes a first step in the construction of RKA-secure symmetric cryptosystems based on Feistel networks, and leaves open a number of directions for future research. From a conceptual point of view, the RKA-security of many-round Feistel networks (including beyond-birthday-type concrete security) are important open questions. From a practical point of view, the RKA security of alternative constructions of PRPs such as generalized Feistel networks [23] and key-alternating ciphers [13], along with their potential (dis)advantages over Feistel networks are another interesting direction for future work.

We conclude the paper with a conjecture about the RKA security of Feistel networks with respect to arbitrary numbers of rounds and key assignments, which generalizes the CCA characterization studied in [34], and generalizes our result in Sect. 7 to the other plausible key assignments.

Conjecture. Let $n > 3$ be an integer, $\kappa : \mathsf{KSp}^m \longrightarrow \mathsf{KSp}^n$ be a simple key assignment, and Φ be a family of RKD sets consisting of functions $\phi : \mathsf{KSp}^m \longrightarrow \mathsf{KSp}^m$. Suppose that the following requirements are satisfied.

1. $\kappa \circ \Phi$ is output unpredictable and claw-free.
2. (κ, Φ) is palindrome-fee: for any $\phi, \phi' \in \Phi$ the probability over a random $(K_1, \ldots, K_m)$ that $\kappa \circ \phi'(K_1, \ldots, K_m) = \sigma \circ \kappa \circ \phi(K_1, \ldots, K_m)$ is negligible, where $\sigma(K_1, \ldots, K_m) := (K_m, \ldots, K_1)$.
3. (κ, Φ) is first-key repeating: for any distinct $\phi, \phi' \in \Phi$ the probability over a random $(K_1, \ldots, K_m)$ that $[\kappa \circ \phi(K_1, \ldots, K_m)]_1 \neq [\kappa \circ \phi'(K_1, \ldots, K_m)]_1$ and $[\kappa \circ \phi(K_1, \ldots, K_m)]_i = [\kappa \circ \phi'(K_1, \ldots, K_m)]_i$ for all $1 < i \leq n$ is small.
4. (κ, Φ) is last-key repeating: for any distinct $\phi, \phi' \in \Phi$ the probability over a random $(K_1, \ldots, K_m)$ that $[\kappa \circ \phi(K_1, \ldots, K_m)]_n \neq [\kappa \circ \phi'(K_1, \ldots, K_m)]_n$ and $[\kappa \circ \phi(K_1, \ldots, K_m)]_i = [\kappa \circ \phi'(K_1, \ldots, K_m)]_i$ for all $1 \leq i < n$ is small.

Then the $\mathbf{F}^{\rho}[\kappa]$ construction is Φ-RKCCA secure in the ideal keyed function model and hence, combined with Theorem 2, the $\mathbf{F}^{\mathsf{PRF}}[\kappa]$ construction is Φ-RKCCA secure for a Ψ-RKCPA-secure PRF, for Ψ as in the statement of Theorem 2.

We note that among the above restrictions claw-freeness is the only requirement which is not known to be necessary. Hence we obtain an "almost" characterization. Note, however, that the RKA security of a deterministic cryptosystems seems difficult to be established without assuming claw-freeness (nevertheless, cf. [5] for a weaker ICR notion). The conjecture strengthens and extends some of the results presented in the previous sections.

Acknowledgements. Manuel Barbosa was supported by Project Best Case, co-financed by the North Portugal Regional Operational Programme (ON.2 – O Novo Norte), under the National Strategic Reference Framework (NSRF), through the European Regional Development Fund (ERDF). Pooya Farshim was supported by grant Fi 940/4-1 of the German Research Foundation (DFG).

References

1. Albrecht, M.R., Farshim, P., Paterson, K.G., Watson, G.J.: On cipher-dependent related-key attacks in the ideal-cipher model. In: Joux, A. (ed.) FSE 2011. LNCS, vol. 6733, pp. 128–145. Springer, Heidelberg (2011)
2. Anderson, R., Kuhn, M.: Low cost attacks on tamper resistant devices. In: Christianson, B., Lomas, M., Crispo, B., Roe, M. (eds.) Security Protocols 1997. LNCS, vol. 1361, pp. 125–136. Springer, Heidelberg (1998)
3. Barbosa, M., Farshim, P.: The Related-key analysis of feistel constructions. In: Cryptology ePrint Archive, Report 2014/093 (2014)
4. Bellare, M., Cash, D.: Pseudorandom functions and permutations provably secure against related-key attacks. In: Cryptology ePrint Archive, Report 2010/397 (2013)
5. Bellare, M., Cash, D., Miller, R.: Cryptography secure against related-key attacks and tampering. In: Lee, D.H., Wang, X. (eds.) ASIACRYPT 2011. LNCS, vol. 7073, pp. 486–503. Springer, Heidelberg (2011)
6. Bellare, M., Kohno, T.: A theoretical treatment of related-key attacks: RKA-PRPs, RKA-PRFs, and applications. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, vol. 2656, pp. 491–506. Springer, Heidelberg (2003)
7. Bellare, M., Paterson, K.G., Thomson, S.: RKA security beyond the linear barrier: IBE, encryption and signatures. In: Wang, X., Sako, K. (eds.) ASIACRYPT 2012. LNCS, vol. 7658, pp. 331–348. Springer, Heidelberg (2012)
8. Biham, E.: How to decrypt or even substitute DES-encrypted messages in 228 steps. Inf. Process. Lett. **84**(3), 117–124 (2002)
9. Biham, E.: New types of cryptoanalytic attacks using related keys. J. Cryptol. **7**(4), 229–246 (1994)
10. Biham, E., Dunkelman, O., Keller, N.: Related-key boomerang and rectangle attacks. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 507–525. Springer, Heidelberg (2005)
11. Biryukov, A., Khovratovich, D.: Related-key cryptanalysis of the full AES-192 and AES-256. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 1–18. Springer, Heidelberg (2009)
12. Biryukov, A., Khovratovich, D., Nikolić, I.: Distinguisher and related-key attack on the full AES-256. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 231–249. Springer, Heidelberg (2009)
13. Bogdanov, A., Knudsen, L.R., Leander, G., Standaert, F.-X., Steinberger, J., Tischhauser, E.: Key-alternating ciphers in a provable setting: encryption using a small number of public permutations. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 45–62. Springer, Heidelberg (2012)
14. Brier, E., Clavier, C., Olivier, F.: Correlation power analysis with a leakage model. In: Joye, M., Quisquater, J.-J. (eds.) CHES 2004. LNCS, vol. 3156, pp. 16–29. Springer, Heidelberg (2004)
15. Chari, S., Rao, J.R., Rohatgi, P.: Template attacks. In: Kaliski Jr., B.S., Koç, Ç.K., Paar, C. (eds.) Cryptographic Hardware and Embedded Systems - CHES 2002. LNCS, vol. 2523, pp. 13–28. Springer, Heidelberg (2002)
16. EMV integrated circuit card specifications for payment systems. Book 2 Security and Key Management, Version 4.2, June 2008
17. Feistel, H.: Cryptography and computer privacy. Sci. Am. **228**, 15–23 (1973)
18. Feistel, H., Notz, W.A., Lynn Smithm, J.: Some cryptographic techniques for machine-to-machine data communications. Proc. of the IEEE **63**(11), 1545–1554 (1975)

19. Goldenberg, D., Liskov, M.: On related-secret pseudorandomness. In: Micciancio, D. (ed.) TCC 2010. LNCS, vol. 5978, pp. 255–272. Springer, Heidelberg (2010)
20. Goldreich, O., Levin, L.: A hard-core predicate for all one-way functions. In: Vitter, J.S. (ed.) STOC, pp. 25–32. ACM (1989)
21. Goldreich, O., Goldwasser, S., Micali, S.: How to construct random functions. J. ACM **33**(4), 792–807 (1986)
22. Goyal, V., O'Neill, A., Rao, V.: Correlated-input secure hash functions. In: Ishai, Y. (ed.) TCC 2011. LNCS, vol. 6597, pp. 182–200. Springer, Heidelberg (2011)
23. Hoang, V.T., Rogaway, P.: On generalized feistel networks. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 613–630. Springer, Heidelberg (2010)
24. Holenstein, T., Künzler, R., Tessaro, S.: The equivalence of the random oracle model and the ideal cipher model, revisited. In Fortnow, L., Vadhan, S.P. (eds.) STOC 2011, pp. 89–98. ACM (2011)
25. Iwata, T., Kohno, T.: New security proofs for the 3gpp confidentiality and integrity algorithms. In: Roy, B., Meier, W. (eds.) FSE 2004. LNCS, vol. 3017, pp. 427–445. Springer, Heidelberg (2004)
26. Khovratovich, D., Nikolić, I., Rechberger, C.: Rotational rebound attacks on reduced skein. In: Abe, M. (ed.) ASIACRYPT 2010. LNCS, vol. 6477, pp. 1–19. Springer, Heidelberg (2010)
27. Knudsen, L.R.: Cryptanalysis of LOKI91. In: Seberry, J., Zheng, Y. (eds.) Advances in Cryptology – AUSCRYPT '92. LNCS, vol. 718, pp. 196–208. Springer, Heidelberg (1993)
28. Knudsen, L.R., Kohno, T.: Analysis of RMAC. In: Johansson, T. (ed.) FSE 2003. LNCS, vol. 2887, pp. 182–191. Springer, Heidelberg (2003)
29. Liskov, M., Rivest, R.L., Wagner, D.: Tweakable block ciphers. In: Yung, M. (ed.) CRYPTO 2002. LNCS, vol. 2442, p. 31. Springer, Heidelberg (2002)
30. Luby, M., Rackoff, C.: How to construct pseudo-random permutations from pseudo-random functions. SIAM J. Comput. **17**(2), 373–386 (1988)
31. Lucks, S.: Ciphers secure against related-key attacks. In: Roy, B., Meier, W. (eds.) FSE 2004. LNCS, vol. 3017, pp. 359–370. Springer, Heidelberg (2004)
32. Kocher, P.C., Jaffe, J., Jun, B.: Differential power analysis. In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol. 1666, p. 388. Springer, Heidelberg (1999)
33. Maurer, U., Pietrzak, K.: The security of many-round luby-rackoff pseudo-random permutations. In: Biham, Eli (ed.) EUROCRYPT 2003. LNCS, vol. 2656, pp. 544–561. Springer, Heidelberg (2003)
34. Nandi, M.: The characterization of luby-rackoff and its optimum single-key variants. In: Gong, G., Gupta, K.C. (eds.) INDOCRYPT 2010. LNCS, vol. 6498, pp. 82–97. Springer, Heidelberg (2010)
35. Naor, M., Reingold, O.: On the construction of pseudorandom permutations: Luby-Rackoff revisited. J. Cryptol. **12**(1), 29–66 (1999)
36. Patarin, J.: How to construct pseudorandom permutations and super pseudorandom permutations from one single pseudorandom functions. In: Rueppel, R.A. (ed.) Advances in Cryptology – EUROCRYPT 1992. LNCS, vol. 658, pp. 256–266. Springer, Heidelberg (1992)
37. Patarin, J.: Security of random feistel schemes with 5 or more rounds. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 106–122. Springer, Heidelberg (2004)
38. Piret, G.: Block Ciphers: Security Proofs, Cryptanalysis, Design, and Fault Attacks. Ph.D. Thesis, Université Catholique de Louvain (2005)
39. Sarkar, S., Maitra, S.: Side channel attack to actual cryptanalysis: breaking crt-rsa with low weight decryption exponents. In: Prouff, E., Schaumont, P. (eds.) CHES 2012. LNCS, vol. 7428, pp. 476–493. Springer, Heidelberg (2012)

40. Shoup, V.: Sequences of games: a tool for taming complexity in security proofs. In: Cryptology ePrint Archive, Report 2004/332 (2004)
41. Vaudenay, S.: Feistel ciphers with L_2-decorrelation. In: Tavares, S., Meijer, H. (eds.) SAC 1998. LNCS, vol. 1556, p. 1. Springer, Heidelberg (1999)
42. Wee, H.: Public key encryption against related key attacks. In: Fischlin, M., Buchmann, J., Manulis, M. (eds.) PKC 2012. LNCS, vol. 7293, pp. 262–279. Springer, Heidelberg (2012)