The Related-Key Security of Iterated Even–Mansour Ciphers

Pooya Farshim[1(✉)] and Gordon Procter[2]

[1] Queen's University Belfast, Belfast, UK
pooya.farshim@gmail.com
[2] Royal Holloway, University of London, Egham, UK
gordon.procter.2011@live.rhul.ac.uk

Abstract. The simplicity and widespread use of blockciphers based on the iterated Even–Mansour (EM) construction has sparked recent interest in the theoretical study of their security. Previous work has established their strong pseudorandom permutation and indifferentiability properties, with some matching lower bounds presented to demonstrate tightness. In this work we initiate the study of the EM ciphers under related-key attacks which, despite extensive prior work on EM ciphers, has received little attention. We show that the simplest one-round EM cipher is strong enough to achieve non-trivial levels of RKA security even under chosen-ciphertext attacks. This class, however, does not include the practically relevant case of offsetting keys by constants. We show that two rounds suffice to reach this level under chosen-plaintext attacks and that three rounds can boost security to resist chosen-ciphertext attacks. We also formalize how indifferentiability relates to RKA security, showing strong positive results despite counterexamples presented for indifferentiability in multi-stage games.

Keywords: Even–Mansour · RKA · Ideal cipher · Indifferentiability

1 Introduction

1.1 Background

Formal analyses of cryptographic protocols often assume that cryptosystems are run on keys that are independently generated and bear no relation to each other. Implicit in this assumption is the premise that user keys are stored in protected areas that are hard to tamper with. Security under *related-key attacks* (RKAs), first identified by Biham and Knudsen [9,10,38], considers a setting where an adversary might be able to disturb user keys by injecting faults [2], and consequently run a cryptosystem on *related* keys. Resilience against RKAs has become a desirable security goal, particularly for blockciphers.

The need for RKA security is further highlighted by the fact that through (improper) design, a higher-level protocol might run a lower-level one on related keys. Prominent examples are the key derivation procedures in standardized

G. Leander (Ed.): FSE 2015, LNCS 9054, pp. 342–363, 2015.
DOI: 10.1007/978-3-662-48116-5_17

protocols such as EMV [25] and the 3GPP integrity and confidentiality algorithms [34], where efficiency considerations have led the designers to use a blockcipher under related keys. Similar considerations can arise in the construction of tweakable blockciphers [41], if a blockcipher is called on keys that are offset by xoring tweak values. An RKA-secure primitive can offer security safeguards against such protocol misuse.

Bellare and Kohno (BK) [7] initiated the theoretical treatment of security under related-key attacks and propose definitions for RKA-secure pseudorandom functions (PRFs) and pseudorandom permutations (PRPs). The BK model were subsequently extended by Albrecht et al. [1] to idealized models of computation to account for the possibility that key might be derived in ways that depend on the ideal primitive. Both works prove that the ideal cipher is RKA secure against wide sets of related-key deriving (RKD) functions. Bellare and Cash [5] present an RKA-secure pseudorandom function from standard intractability assumptions and Bellare, Cash, and Miller [6] give a comprehensive treatment of RKA security for various cryptographic primitives, leveraging the RKA resilience of PRGs to construct RKA-secure instances of various other primitives. In this work we are interested in the RKA security of blockciphers.

1.2 The Even–Mansour Ciphers

Key-alternating ciphers were introduced by Daemen and Rijmen [23] with the aim of facilitating a theoretical discussion of the design of AES. The key-alternating cipher has since become a popular paradigm for blockcipher design, with notable examples including AES [22,45], Present [14], LED [32], PRINCE [16], KLEIN [31], and Zorro [30]. Key-alternating ciphers originate in the work of Even and Mansour [26,27], who considered a single round of the construction show in Fig. 1; their motivation was to design the simplest blockcipher possible. This design is closely related to Rivest's DES-X construction, proposed as a means to protect DES against brute-force attacks [36], which itself builds on principles dating back to Shannon [49, p. 713]. In this work, we use the terms 'key-alternating cipher' and 'iterated Even–Mansour cipher' interchangeably.

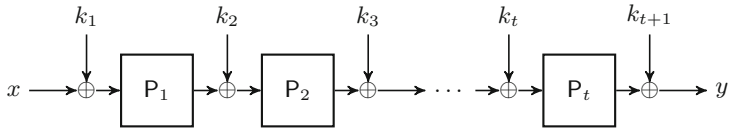

Fig. 1. The t -round iterated Even–Mansour scheme.

Provable security. Even and Mansour's original analysis [26,27] considers 'cracking' and 'forging' attacks in the random-permutation model and shows that no adversary can predict x given $\mathsf{E}(k,x)$ or $\mathsf{E}(k,x)$ given x with reasonable probability, without making q_1 queries to the permutation and q_{em} to the

encryption/decryption oracle, where $q_1 q_{em} \approx 2^n$. The indistinguishability of the Even–Mansour scheme from a random permutation is shown by Kilian and Rogaway [36,37, Theorem 3.1 with $\kappa = 0$] and Lampe, Patarin and Seurin [39, App. Bofthefullversion]. Both works show that an adversary making q_1 and q_{em} queries to the permutation oracle and the encryption/decryption oracles respectively, has a success probability of approximately $q_1 q_{em}/2^{n-1}$. Gentry and Ramzan [29] show that the permutation oracle can be instantiated by a Feistel network with a random oracle without loss of security.

At Eurocrypt 2012, Dunkelman, Keller, and Shamir [24] showed that the Even–Mansour scheme retains the same level of security using only a single key, that is $\mathsf{E}(k, x) = \mathsf{P}(x \oplus k) \oplus k$. Bogdanov et al. [15] show that the t-round Even–Mansour cipher with independent keys and permutations and at least two rounds ($t \geq 2$) provides security up to approximately $2^{2n/3}$ queries but can be broken in $t \cdot 2^{tn/(t+1)}$ queries. Following this work, several papers have moved towards proving a bound that meets this attack [39,50], with Chen and Steinberger [18] able to prove optimal bounds using Patarin's H-coefficient technique [47]. Chen et al. [17] consider two variants of the two-round Even–Mansour scheme: one with independent permutations and identical round keys, the other with identical permutations but a more complex key schedule. In both cases (under certain assumptions about the key schedule), security is maintained up to roughly $2^{2n/3}$ queries.

Maurer, Renner, and Holenstein (MRH) [43] introduce a framework which formalizes what it means for a non-monolithic object to be able to replace another in arbitrary cryptosystems. This framework, know as indifferentiability, has been used to validate the design principle behind many cryptographic constructions, and in particular that of the iterated Even–Mansour constructions. Lampe and Seurin [40] show that the 12-round Even–Mansour cipher using a single key is indifferentiable from the ideal cipher. Andreeva et al. [3] show that a modification of the single-key, 5-round Even–Mansour cipher, where the key is first processed through a random oracle, is indifferentiable from the ideal cipher.

Cryptanalysis. Daemen [21] describes a chosen-plaintext attack that recovers the key of Even–Mansour in approximately $q_1 \approx q_{em} \approx 2^{n/2}$ queries. Biryukov and Wagner [13] are able to give a known-plaintext attack against the Even–Mansour scheme with the same complexity as Daemen's chosen-plaintext attack. Dunkelman, Keller, and Shamir [24] introduce the slidex attack that uses only known plaintexts and can be carried out with any number of queries as long as $q_1 \cdot q_{em} \approx 2^n$.

Mendel et al. [44] describe how to extend Daemen's attack [21] to a related-key version, and are able to recover the keys when all round keys are independent. Bogdanov et al. [15] remark that related-key distinguishing attacks against the iterated Even–Mansour scheme with *independent* round keys "exist trivially," and describe a key-recovery attack, requiring roughly $2^{n/2}$ queries against the two-round Even–Mansour scheme with identical round keys, assuming that an adversary can xor constants into the round key.

Many key-alternating ciphers such as AES [11,12], Present [46], LED [44], and Prince [35] have been analyzed in the related-key model. One of the security claims of the LED blockcipher [32] is a high resistance to related-key attacks, which is justified by giving a lower bound on the number of active S-boxes.

1.3 Contributions

Despite extensive literature on the provable security of iterated Even–Mansour ciphers and (RKA) cryptanalysis of schemes using this design strategy, their formal related-key analysis has received little attention. In this work we initiate the provable RKA security analysis of such key-alternating ciphers. Our results build on the work of Barbosa and Farshim [4] who study the RKA of security of Feistel constructions. They show that by appropriate reuse of keys across the rounds, the 3-round Feistel construction achieves RKA security under chosen-plaintext attacks. With four rounds the authors are able to prove RKA security for chosen-ciphertext attacks. The authors also formalize a random-oracle model transform by Lucks [42] which processes the key via the random oracle before application. Our results are similar and we show that key reuse is also a viable strategy to protect against related-key attacks in key-alternating ciphers. In contrast to the Feistel constructions, key-alternating ciphers operate *intrinsically* in an idealized model of computation, and our analyses draw on techniques used in the formalization of Lucks's heuristic in [4].

We start with the simplest of the key-alternating ciphers, namely the (one-round) EM cipher. We recall that for xor related-key attacks, where an adversary can offset keys by values of its choice, this construction does not provide RKA security [3,15,16,40]. Indeed, it is easy to check that $\mathsf{E}((k_1, k_2), x) = \mathsf{E}((k_1 \oplus \Delta, k_2), x \oplus \Delta)$, which only holds with negligible probability for the ideal cipher. We term this pattern of adversarial behaviour *offset switching*. One idea to thwart the above attack here would be to enforce key reuse in the construction; although the above equality no longer holds, a close variant still applies:

$$\mathsf{E}(k, x) = \mathsf{E}(k \oplus \Delta, x \oplus \Delta) \oplus \Delta \ .$$

Despite this negative result, we show that the minimal EM cipher with key-reuse enjoys a non-trivial level of RKA security (even in the chosen-ciphertext setting). For a set of allowed relate-key queries Φ, we identify a set of sufficient conditions that allow us to argue that $\mathsf{E}(\phi(k), x)$ and $\mathsf{E}(\phi'(k), x')$ for $\phi, \phi' \in \Phi$ look random and independent from an adversary's point of view. As usual, our conditions impose that the RKD functions have *unpredictable* outputs, as otherwise RKA security is trivially unachievable. (For $\phi(k) = c$, a predictable value, consider an adversary which computes $\mathsf{E}(c, 0)$ and compares it $\mathsf{E}(\phi(k), 0)$.) Our second condition looks at the generalization of the offset-switching attack above and requires it to be infeasible to find offset claws, i.e., for any pair of functions (ϕ_1, ϕ_2) and any value Δ of adversary's choice, over a random choice of k

$$\phi_1(k) \oplus \phi_2(k) \neq \Delta \ .$$

This strengthens the standard claw-freeness condition [1,4,7], which corresponds to the $\Delta = 0$ case. In our work, we also consider RKD functions that *depend* on the underlying permutations by placing queries to them. As mentioned above, this is particularly relevant for the Even–Mansour ciphers as they inherently operate in the random-permutation model. We build on previous work in the analysis of such functions [1,4] and formulate adequate restrictions on oracle queries that allow a security proof to be established. Informally, our condition requires that the queries made by ϕ's have empty intersection with the outputs of ϕ's, even with offsets.

The search for xor-RKA security leads us to consider the two-round EM constructions. The first attack discussed above, where the key is offset by a constant, still applies in this setting and once again we consider key reuse. (The two permutations are still independent.) For this cipher, the offset-switching attack no longer applies, which raises the possibility that the two-round Even–Mansour might provide xor-RKA security. We start with chosen-plaintext attacks, formulate three new conditions (analogous to those given for the basic scheme), and prove security under them. These conditions, as before, decouple the queries made to the permutation oracle and allow us to simulate the outer P_2 oracle *forgetfully* in a reduction. We then show that this new set of restrictions are *weak* enough to follow from the standard output-unpredictability and claw-freeness properties. Since xoring with constants is output unpredictable and claw-free [7], the xor-RKA security of the single-key, two-round EM construction follows. Under chosen-ciphertext attacks, however, this construction falls prey to an attack of Andreeva et al. [3] on the indifferentiability of two-round EM (adapted to the RKA setting). For CCA security, we turn to three-round constructions, where we show of the 14 possible way to reuse keys, all but one fall prey to either offset switching attacks or Andreeva et al.'s attack [3]. On the other hand, the three-round construction which uses a single key meets the desired xor-RKA security in the CCA setting.

Dunkelman, Keller, and Shamir [24] consider several variants of the Even–Mansour scheme, such as *addition* Even–Mansour where the xors are replaced with modular additions, and *involution* Even–Mansour, where random permutations are replaced with random involutions. It is reasonable to expect that our results can be modified to also apply to these schemes. Another possible variant of the Even–Mansour scheme is one where the same permutation is used across the rounds [17]; we briefly argue that our proof techniques carry over to this *permutation reuse* setting.

As mentioned above, Lampe and Seurin [40] show that the 12-round EM construction is indifferentiable from the ideal cipher when a single key is used throughout the rounds. Ristenpart, Shacham and Shrimpton [48], on the other hand, point out that indifferentiability does not necessarily guarantee composition in *multi-stage* settings and go on to note that the RKA game is multi-staged. This leaves open the question of whether indifferentiability provides any form of RKA security. We show that if RKD functions query the underlying primitive indirectly *via the construction only*, then composition holds. This level of RKA

security is fairly strong as, in our opinion, it is unclear what it menas to *syntactically* changing the RKD functions from those in the ideal setting which have access to the ideal cipher to those which (suddenly) get access to permutations. Our result, in particular, implies that Lampe and Seurin's constructions [40] and Holenstein, Künzler, and Tessaro's 14-round Feistel construction [33] are RKA secure against key offsets in the CCA setting.

Independently and concurrently to this work, Cogliati and Seurin [19,20] also study the related-key security of iterated EM ciphers. Their Theorem 2 is very similar to our Corollary 3; they analyze more general key schedules and obtain tighter bounds, while our approach deals with a wider range of RKD functions.

2 Preliminaries

Notation. We write $x \leftarrow y$ for assigning value y to variable x. We write $x \xleftarrow{\$} \mathsf{X}$ for the action of sampling x from a finite set X uniformly at random. If $\mathcal{A}$ is a probabilistic algorithm we write $y \xleftarrow{\$} \mathcal{A}(x_1, \ldots, x_n)$ for the action of running $\mathcal{A}$ on inputs $x_1, \ldots, x_n$ with randomly chosen coins, and assigning the results to y. We let $[n] := \{1, \ldots, n\}$, and we denote the bitwise complement of a bit string x by $\overline{x}$.

Blockciphers. A (block)cipher is a function $\mathsf{E}\colon \mathcal{K} \times \mathcal{M} \longrightarrow \mathcal{M}$ such that for every $k \in \mathcal{K}$ the map $\mathsf{E}(k, \cdot)$ is a permutation on $\mathcal{M}$. Such an E uniquely defines its inverse map $\mathsf{D}(k, \cdot)$ for each key k. We write $\mathsf{BC} := (\mathsf{E}, \mathsf{D})$ to denote a blockcipher, which also implicitly defines the cipher's key space $\mathcal{K}$ and message space or domain $\mathcal{M}$. We denote the set of all blockciphers with key space $\mathcal{K}$ and domain $\mathcal{M}$ by $\mathrm{Block}(\mathcal{K}, \mathcal{M})$. The ideal cipher with key space $\mathcal{K}$ and message space $\mathcal{M}$ corresponds to a model of computation where all parties have oracle access to a uniformly chosen random element of $\mathrm{Block}(\mathcal{K}, \mathcal{M})$ in both the forward and backward directions. For a blockcipher $\mathsf{BC} := (\mathsf{E}, \mathsf{D})$, notation $\mathcal{A}^{\mathsf{BC}}$ denotes oracle access to both E and D for $\mathcal{A}$.

Permutations. An ideal permutation can be viewed as a blockcipher whose key space contains a single key. In this work, we are interested in building blockciphers with large key spaces from a small number of ideal permutations $\mathsf{P}_1, \ldots, \mathsf{P}_t$ and their inverses. This is equivalent to access to a blockcipher with key space $[t]$, where $\mathsf{P}_i(x) := \mathsf{P}(i, x)$. In order to ease notation, we define a single oracle π, which provides access to all t ideal permutations in both directions. This oracle takes as input (i, x, σ), where $i \in [t]$, $x \in \mathcal{M}$, and $\sigma \in \{+, -\}$ and returns $\mathsf{P}_i(x)$ if $\sigma = +$ and $\mathsf{P}_i^{-1}(x)$ if $\sigma = -$. Slightly abusing notation, we define $\mathsf{P}_i^{\sigma}(x) := \mathsf{P}^{\sigma}(i, x) := \pi(i, x, \sigma)$, and assume $\sigma = +$ whenever it is omitted from the superscript. A blockcipher constructed from t ideal permutations π is written $\mathsf{BC}^{\pi} := (\mathsf{E}^{\pi}, \mathsf{D}^{\pi})$.

RKD functions. A related-key deriving (RKD) function maps keys to keys in some key space $\mathcal{K}$. In this paper, we view RKD functions as circuits that may contain special oracles gates π. An RKD set Φ is a set of RKD functions $\phi^{\pi} : \mathcal{K} \longrightarrow \mathcal{K}$, where π is an oracle. (The oracle will be instantiated with π as

defined above.) Throughout the paper we assume that membership in RKD sets can be efficiently decided.

RKA SECURITY. Following [1,7], we formalize the RKA security of a blockcipher $\mathsf{BC}^\pi := (\mathsf{E}^\pi, \mathsf{D}^\pi)$ in the (multiple) ideal-permutation model via the game shown in Fig. 2. The RKA game is parametrized by an RKD set Φ which specifies the RKD functions that an adversary is permitted to query during its attack. This game also includes a procedure for oracle π defined above. We define the RKCCA advantage of an adversary $\mathcal{A}$ via

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

The RKCPA game and advantage are defined similarly by considering adversaries that do not make any RKDEC queries (backwards queries to the permutations are still permitted).

$\underline{\mathsf{RKCCA}_{\mathsf{BC}^\pi,\mathcal{A},\Phi,t}}$:	$\underline{\mathrm{RKENC}(\phi^\pi, x)}$:
$b \leftarrow\!\!\$\ \{0,1\}$; $k \leftarrow\!\!\$\ \mathcal{K}$	$k' \leftarrow \phi^\pi(k)$
$(\mathsf{P}, \mathsf{P}^{-1}) \leftarrow\!\!\$\ \mathrm{Block}([t], \mathcal{M})$	If $b = 0$ Return $\mathsf{iE}(k', x)$
$(\mathsf{iE}, \mathsf{iD}) \leftarrow\!\!\$\ \mathrm{Block}(\mathcal{K}, \mathcal{M})$	Return $\mathsf{E}^\pi(k', x)$
$b' \leftarrow\!\!\$\ \mathcal{A}^{\mathrm{RKENC},\mathrm{RKDEC},\pi}$	
Return $(b' = b)$	$\underline{\mathrm{RKDEC}(\phi^\pi, x)}$:
	$k' \leftarrow \phi^\pi(k)$
$\underline{\pi(i, x, \sigma)}$:	If $b = 0$ Return $\mathsf{iD}(k', x)$
Return $\mathsf{P}^\sigma(i, x)$	Return $\mathsf{D}^\pi(k', x)$

Fig. 2. Game defining the Φ-RKCCA security of a blockcipher $\mathsf{BC}^\pi := (\mathsf{E}^\pi, \mathsf{D}^\pi)$ with access to t ideal permutations. An adversary can query the RKENC and RKDEC oracles with a $\phi^\pi \in \Phi$ only. In the RKCPA game the adversary cannot query the RKDEC oracle.

RKA SECURITY OF THE IDEAL CIPHER. Following [7] we define the RKA security of the ideal cipher $\mathsf{IC}' := (\mathsf{iE}', \mathsf{iD}')$ by augmenting the procedures of the above game with those for computing the ideal cipher in both directions, i.e., $(\mathsf{iE}', \mathsf{iD}')$. When working with the ideal cipher, t is often 0, but we consider RKD functions which have oracle access to the ideal procedures iE' and iD' as in [1].

EVEN–MANSOUR CIPHERS. The t-round Even–Mansour (EM) cipher $\mathsf{EM}^\pi := (\mathsf{E}^\pi, \mathsf{D}^\pi)$ with respect to t permutations $\mathsf{P}_1, \ldots, \mathsf{P}_t$ on domain $\{0,1\}^n$ has key space $\mathcal{K} = \{0,1\}^{n(t+1)}$, domain $\mathcal{M} = \{0,1\}^n$, and is defined via

$$\mathsf{E}^\pi((k_1, \ldots, k_{t+1}), x) := \mathsf{P}_t(\cdots \mathsf{P}_2(\mathsf{P}_1(x \oplus k_1) \oplus k_2) \cdots) \oplus k_{t+1} \ ,$$
$$\mathsf{D}^\pi((k_1, \ldots, k_{t+1}), x) := \mathsf{P}_1^{-1}(\cdots \mathsf{P}_{t-1}^{-1}(\mathsf{P}_t^{-1}(x \oplus k_{t+1}) \oplus k_t) \cdots) \oplus k_1 \ .$$

In this work we are interested in EM ciphers where keys are reused in various rounds. Following notation adopted in [4], we denote the EM construction

where key k_{i_j} is used before round j by $\mathsf{EM}^{\pi}[i_1, i_2, \ldots, i_{t+1}]$. We call such key schedules *simple*. Note that $\mathcal{K} = \{0,1\}^{n \cdot |\{i_1, i_2, \ldots, i_{t+1}\}|}$ in these constructions. Of particular interest to us are the $\mathsf{EM}^{\pi}[1,1]$, $\mathsf{EM}^{\pi}[1,1,1]$ and $\mathsf{EM}^{\pi}[1,1,1,1]$ constructions, where a single key is used in all rounds. We emphasize that the round permutations in all these constructions are independently chosen, unless stated otherwise.

3 Indifferentiability and RKA Security

Given the indifferentiability results for the EM and Feistel constructions discussed in the introduction, in this section we study to what extent (if any) an indifferentiable construction can provide resilience against related-key attacks. We start by recalling what it means for a blockcipher construction to be indifferentiable from the ideal cipher [43].

Indifferentiability. Let $\mathsf{BC}^{\pi} := (\mathsf{E}^{\pi}, \mathsf{D}^{\pi})$ be a blockcipher and let $\mathcal{S}^{\mathsf{IC}}$ be a simulator with oracle access to the ideal cipher having the same key and message spaces as those of BC^{π}. We define the indifferentiability advantage of a distinguished $\mathcal{D}$ with respect to $\mathcal{S}$ against BC^{π} via

$$\mathbf{Adv}^{\mathsf{indiff}}_{\mathsf{BC}^{\pi},t}(\mathcal{S},\mathcal{D}) := \Pr\left[\mathcal{D}^{\mathsf{BC}^{\pi},\pi}\right] - \Pr\left[\mathcal{D}^{\mathsf{IC},\mathcal{S}^{\mathsf{IC}}}\right] ,$$

where the first probability is taken over a random choice of π (as defined in Fig. 2), and the second probability is taken over a random choice of a blockcipher $\mathsf{IC} := (\mathsf{iE}, \mathsf{iD})$. Note that in this definition we require a *universal* simulator that does not depend on the indifferentiability distinguisher. We prove the following theorem in the full version of the paper [28].

Theorem 1. *Let Φ be an RKD set consisting of function ϕ^{OC} having access to a blockcipher oracle OC. Let π be as before, BC^{π} be a blockcipher construction, and $\mathcal{S}$ be an indifferentiability simulator. Then for any adversary $\mathcal{A}$ against the Φ-RKCCA security of BC^{π}, where the oracles in the RKD functions are instantiated with BC^{π}, there are adversaries $\mathcal{D}_1$ and $\mathcal{D}_2$ against the indifferentiability of BC^{π}, and an adversary $\mathcal{B}$ against the Φ-RKCCA of the ideal cipher, where the oracles in the RKD functions are instantiated with the ideal cipher, such that*

$$\mathbf{Adv}^{\mathsf{rkcca}}_{\mathsf{BC}^{\pi},\Phi,t}(\mathcal{A}) \leq \mathbf{Adv}^{\mathsf{indiff}}_{\mathsf{BC}^{\pi},t}(\mathcal{S},\mathcal{D}_1) + \mathbf{Adv}^{\mathsf{indiff}}_{\mathsf{BC}^{\pi},t}(\mathcal{S},\mathcal{D}_2) + \mathbf{Adv}^{\mathsf{rkcca}}_{\mathsf{IC},\Phi,t}(\mathcal{B}) .$$

Care with composition. Ristenpart, Shacham, and Shrimpton [48] show that indifferentiability does *not* always guarantee secure composition in *multi-stage* settings where multiple adversaries can only communicate in restricted ways. The authors then remark that RKA security is multi-staged. To see this, note that the RKA game can be viewed as consisting of two adversaries $\mathcal{A}_1^{\pi}$ and $\mathcal{A}_2^{\pi}$ where $\mathcal{A}_1^{\pi}$ corresponds to the standard RKA adversary $\mathcal{A}^{\pi}$ and $\mathcal{A}_2^{\pi}$ is an adversary which has access to the key k, receives an input from $\mathcal{A}_1^{\pi}$ containing the description of an RKD function ϕ^{π} and a value x, computes $\phi^{\pi}(k)$ using its access to π to get

k', and returns $\mathsf{E}^{\pi}(k', x)$ or $\mathsf{D}^{\pi}(k', x)$ to $\mathcal{A}_1^{\pi}$ as needed. With this formalization adversary $\mathcal{A}_2^{\pi}$ cannot freely communicate with $\mathcal{A}_1^{\pi}$ as it is restricted to send only encryption and decryption outputs. Our theorem above essentially states that in settings where $\mathcal{A}_2^{\pi}$ takes the restricted form $\mathcal{A}_2^{\mathsf{BC}^{\pi}}$ indifferentiability suffices. In our opinion, this restricted access to π suits the RKA security model particularly well. Indeed, when starting in the ideal setting where the RKD functions have access to the ideal cipher, one needs to address how the oracles are instantiated when moved to a construction. A natural way to do this is to simply instantiate the oracles with those of the construction as well (and in this setting, as we show, indifferentiability suffices). Giving the RKD functions direct access to π would constitute a *syntactic* change in the two RKD sets for the ideal cipher and the construction, and it is unclear one should compare RKA security in these settings.

Lampe and Seurin [40, Theorem 2] show that the 12-round $\mathsf{EM}^{\pi}[1, \cdots, 1]$ construction is indifferentiable from the ideal cipher (with a universal simulator). Bellare and Kohno [7], on the other hand, show that the ideal cipher is $\Phi^{\oplus}$-RKCCA secure, where

$$\Phi^{\oplus} := \{k \mapsto k \oplus \Delta : \Delta \in \mathcal{K}\} \ .$$

We therefore obtain as a corollary of the above theorem that the 12-round construction $\mathsf{EM}^{\pi}[1, \cdots, 1]$ is $\Phi^{\oplus}$-RKCCA secure. The same conclusion applies to the 14-round Feistel construction of Holenstein, Künzler, and Tessaro [33]. These construction, however, are suboptimal in terms rounds with respect to RKA security. Barbosa and Farshim [4] show that 4 rounds with key reuse suffices for Feistel networks. In the following sections, we study the Even–Mansour ciphers with smaller number of rounds while maintaining RKA security.

4 The RKA Security of $\mathsf{EM}^{\pi}[1, 1]$

In this section we study RKD sets Φ for which the single-key Even–Mansour construction provides Φ-RKCCA security. Our results are similar to those of Bellare and Kohno [7], Albrecht et al. [1], and Barbosa and Farshim [4] in that we identify a set of restrictions on the RKD set Φ that allow us to establish a security proof. For the one-round construction there are two simple key schedules up to relabeling: $\mathsf{EM}^{\pi}[1, 1]$ and $\mathsf{EM}^{\pi}[1, 2]$. Neither of these constructions can provide $\Phi^{\oplus}$-RKCPA security due to the offset-switching attacks discussed in the introduction. Despite this, we show that the most simple of the EM constructions, $\mathsf{EM}^{\pi}[1, 1]$, provides a non-trivial level of RKA security. The results of this section will also serve as a warm up to the end goal of achieving strong forms of RKA security, which will encompass key offsets as a special case.

4.1 Restricting RKD Sets

Bellare and Kohno [7] observe that if an adversary is able to choose a $\phi \in \Phi$ that has *predictable* outputs on a randomly chosen key, then Φ-RKCCA security

is not achievable. To see this, let ϕ be the constant zero (or any predictable) function. An adversary can simply test if it is interacting with the real or the ideal cipher by enciphering x under the zero key and comparing it to the value it receives from its RKEnc oracle on (ϕ, x). This motivates the following definition of unpredictability, adapted to the ideal-permutation model.

Output unpredictability (OUP). The advantage of an adversary $\mathcal{A}$ against the *output unpredictability* of an RKD set Φ with access to t ideal permutations is defined via

$$\mathbf{Adv}^{\mathsf{oup}}_{\Phi,t}(\mathcal{A}) := \Pr\left[\exists\,(\phi^\pi, c) \in \mathsf{List} : \phi^\pi(k) = c; \mathsf{List} \leftarrow\!\!\$\ \mathcal{A}^\pi\right] .$$

Here List contains pairs of the form (ϕ^π, c) for $\phi^\pi \in \Phi$ and $c \in \mathcal{K}$, and π is the oracle containing t ideal permutations. The probability is taken over a random choice of $k \leftarrow\!\!\$\ \mathcal{K}$, the t random permutations implicit in π, and the coins of the adversary. Note that via a simple guessing argument, this definition can be shown to be equivalent to one where the adversary is required to output a single pair, with a loss of $1/|\mathsf{List}|$ in the reduction.

A second condition that Bellare and Kohno [7] introduce is *claw-freeness*. Roughly speaking, a set Φ has claws if there are two distinct $\phi_1, \phi_2 \in \Phi$ such that $\phi_1(k) = \phi_2(k)$. Although this condition is not in general necessary—given an arbitrary claw there isn't necessarily an attack—it turns out that existence of claws prevent natural approaches to proofs of security. We lift claw-freeness to the ideal-permutation model below.

Claw-freeness (CF). The advantage of an adversary $\mathcal{A}$ against the *claw-freeness* of an RKD set Φ with access to t ideal permutations is defined via

$$\mathbf{Adv}^{\mathsf{cf}}_{\Phi,t}(\mathcal{A}) := \Pr\left[\exists\,(\phi_1^\pi, \phi_2^\pi) \in \mathsf{List} : \phi_1^\pi(k) = \phi_2^\pi(k) \wedge \phi_1^\pi \neq \phi_2^\pi : \mathsf{List} \leftarrow\!\!\$\ \mathcal{A}^\pi\right] .$$

Here List contains pairs of RKD functions, π is as before, and the probability space is defined similarly to that for output unpredictability. Once again this definition is equivalent to one where List is restricted to be of size one.

Claw-freeness is not a strong enough condition for the one-round EM construction to be RKA secure. Indeed, consider an adversary that queries its encryption oracle with two pairs (ϕ_1, x_1) and (ϕ_2, x_2), possibly with $x_1 \neq x_2$, such that

$$x_1 \oplus \phi_1(k) = x_2 \oplus \phi_2(k) .$$

Then the permutation underlying the construction will be queried at the same point and the resulting ciphertexts will differ by $\phi_1(k) \oplus \phi_2(k) = x_1 \oplus x_2$, a predictable value. This observation motivates a strengthening of the claw-freeness property.

Xor claw-freeness (XCF). The advantage of an adversary $\mathcal{A}$ against the *xor claw-freeness* of an RKD set Φ with access to t ideal permutations is defined via

$$\mathbf{Adv}^{\mathsf{xcf}}_{\Phi,t}(\mathcal{A}) := \Pr\left[\exists\,(\phi_1^\pi, \phi_2^\pi, c) \in \mathsf{List} : \phi_1^\pi(k) \oplus \phi_2^\pi(k) = c \wedge \phi_1^\pi \neq \phi_2^\pi : \mathsf{List} \leftarrow\!\!\$ \mathcal{A}^\pi\right] .$$

The variables and probability space are defined similarly to those for claw-freeness.

Xor claw-freeness implies claw-freeness as the latter is a special case with $c = 0$. That claw-freeness is weaker than xor claw-freeness can be seen by considering the set $\Phi^{\oplus}$ corresponding to xoring with constants. This set can be easily shown to be output unpredictable and claw-free [7], but is not xor claw-free as

$$\phi_{\Delta_1}(k) \oplus \phi_{\Delta_2}(k) = \Delta_1 \oplus \Delta_2 \quad \text{where} \quad \phi_{\Delta}(k) := k \oplus \Delta \ .$$

We also observe that xor claw-freeness of Φ implies that there is at most one $\phi \in \Phi$ which is predictable as any *two* predictable RKD functions can be used to break xor claw-freeness.

Let us now consider oracle access in the RKD functions. Following the attacks identified in [1,4], we consider the oracle-dependent RKD set

$$\Phi := \left\{ id : k \mapsto k,\ \phi^{\mathsf{P}} : k \mapsto \mathsf{P}(k) \right\} \ .$$

Consider the following Φ-RKCPA adversary against $\mathsf{EM}^{\pi}[1,1]$. Query $(id, 0)$ and get $y = \mathsf{P}(k) \oplus k$. Query (ϕ^{P}, y) and get z. Return $(z = 0)$. When interacting with $\mathsf{EM}^{\pi}[1,1]$ we have that

$$z = \mathsf{E}^{\mathsf{P}}(\mathsf{P}(k), \mathsf{P}(k) \oplus k) = \mathsf{P}(\mathsf{P}(k) \oplus k \oplus \mathsf{P}(k)) \oplus \mathsf{P}(k) = \mathsf{P}(k) \oplus \mathsf{P}(k) = 0 \ .$$

On the other hand, this identity is true with probability at most $1/(2^n - 1)$ with respect to the ideal cipher. This attack stems from the fact that when answering an RKEnc query, π is evaluated at a point already queried by an RKD function. Our final restriction below formalizes what it means for the oracle queries of the RKD function to be disjoint from those of the adversary, including those made implicitly through the encryption or decryption procedures, even up to xoring constants.

Xor query independence (XQI). The advantage of an adversary $\mathcal{A}$ against the *xor query independence* of an RKD set Φ with access to t ideal permutations is defined via

$$\mathbf{Adv}^{\mathsf{xqi}}_{\Phi,t}(\mathcal{A}) := \Pr\left[\exists (i, \sigma, \phi_1^{\pi}, \phi_2^{\pi}, c) \in \mathsf{List} : (i, \phi_1^{\pi}(k) \oplus c, \sigma) \in \overline{\mathsf{Qry}}[\phi_2^{\pi}(k)]; \mathsf{List} \leftarrow\!\!\$\, \mathcal{A}^{\pi}\right]$$

where

$$\mathsf{Qry}[\phi^{\pi}(k)] := \{(i, x, \sigma) : (i, x, \sigma) \text{ queried to } \pi \text{ by } \phi^{\pi}(k)\} \ ,$$
$$\overline{\mathsf{Qry}}[k^{\pi}(k)] := \mathsf{Qry}[\phi^{\pi}(k)] \cup \{(i, \pi(i, x, \sigma), -\sigma) : (i, x, \sigma) \in \mathsf{Qry}[\phi^{\pi}(k)]\} \ .$$

Note that for the EM cipher, restricting the above definition to $i = 1$ suffices. We also define *query independence* [1] as above but demand that $c = 0$.

Examples. The OUP, XCF, and XQI conditions introduced above do not lead to vacuous RKD sets. As an example of an RKD set which is independent of the permutations consider

$$\Phi^{\mathsf{xu}} := \{k \mapsto H(k, x) : x \in \mathcal{K}'\} \ ,$$

where H is an xor-universal hash function from $\mathcal{K}$ to $\mathcal{K}$ with key space $\mathcal{K}'$. As a simple instantiation, let $\mathcal{K}' = \{0,1\}^k \setminus 0^k$ and for $k \in \mathcal{K}'$ define $H(k,x) := k \cdot x$, where $\{0,1\}^k$ is interpreted as $\mathrm{GF}(2^k)$ with respect to a fixed irreducible polynomial, and multiplication is defined over $\mathrm{GF}(2^k)$.

As an example of an oracle-dependent RKD set, one can take

$$\Phi := \{k \mapsto \mathsf{P}(k \oplus \Delta) : \Delta \in \mathcal{K}\} \ .$$

4.2 Sufficiency of the Conditions

We now show that if an RKD set Φ meets the output unpredictability, xor claw-freeness and xor query independence properties defined above, then $\mathsf{EM}^\pi[1,1]$ provides Φ-RKCCA security. Throughput the paper we denote the number of queries to various oracles in an attack as follows:

q_i: the number of direct, distinct queries to π with index i made by the adversary $\mathcal{A}$.
q_{em}: the number of distinct queries to the RKEnc and (if present) RKDec oracles by $\mathcal{A}$.
q_i^ϕ: the number of distinct queries to π with index i made by the RKD function ϕ^π.

We call an RKA adversary repeat-free if it does not query its RKEnc or RKDec oracle on a pair (ϕ, x) twice. We call an RKA adversary redundancy-free if it does not query RKEnc on (ϕ, x) to get y and then RKDec on (ϕ, y) to get x, or vice versa. Without loss of generality, we assume that all adversaries in this paper are repeat-free and redundancy-free.

Theorem 2 (Φ-RKCCA ***security of*** EM^π [1,1]). Let Φ be an RKD set. Then for any adversary $\mathcal{A}$ against the Φ-RKCCA security of $\mathsf{EM}^\pi[1,1]$ with parameters as defined above, there are adversaries $\mathcal{B}_1$, $\mathcal{B}_2$, $\mathcal{B}_3$ and $\mathcal{B}_4$ such that

$$\begin{aligned}\mathbf{Adv}^{\mathsf{rkcca}}_{\mathsf{EM}^\pi[1,1],\Phi,1}(\mathcal{A}) \leq & \mathbf{Adv}^{\mathsf{oup}}_{\Phi,1}(\mathcal{B}_1) + \mathbf{Adv}^{\mathsf{xqi}}_{\Phi,1}(\mathcal{B}_2) + \mathbf{Adv}^{\mathsf{xcf}}_{\Phi,1}(\mathcal{B}_3) + \mathbf{Adv}^{\mathsf{cf}}_{\Phi}(\mathcal{B}_4) \\ & + \frac{q_{em}(q_1 + \sum_\phi q_1^\phi)}{2^n - (q_1 + \sum_\phi q_1^\phi)} + \frac{2q_{em}^2}{2^n} \ ,\end{aligned}$$

where $\mathcal{B}_1$, $\mathcal{B}_2$, $\mathcal{B}_3$ and $\mathcal{B}_4$ output lists of sizes $2q_1q_{em}$, $2q_{em}^2$, q_{em}^2, and q_{em}^2 respectively and they all make q_1 queries to π.

We give the intuition behind the proof here and leave the details to the full version [28]. The adversary $\mathcal{A}$ in the Φ-RKCCA game is run with respect to the oracles

$$\mathsf{P}(x), \quad \mathsf{P}^{-1}(x), \quad \mathsf{P}(x \oplus \phi^\pi(k)) \oplus \phi^\pi(k), \quad \mathsf{P}^{-1}(x \oplus \phi^\pi(k)) \oplus \phi^\pi(k) \ .$$

Our goal is to make a transition to an environment with the oracles

$$\mathsf{P}(x), \quad \mathsf{P}^{-1}(x), \quad \mathsf{iE}(\phi^\pi(k), x), \quad \mathsf{iD}(\phi^\pi(k), x) \ ,$$

where $(\mathsf{iE}, \mathsf{iD})$ denotes the ideal cipher. To this end, we consider two intermediate environments where the last two oracles corresponding to RKEnc and RKDec are handled via a *forgetful* oracle \$ that returns uniform strings on each invocation, irrespectively of its inputs. Applying this change to the first environment above gives

$$\mathsf{P}(x), \quad \mathsf{P}^{-1}(x), \quad \$(x \oplus \phi^\pi(k)) \oplus \phi^\pi(k), \quad \$(x \oplus \phi^\pi(k)) \oplus \phi^\pi(k) \ ,$$

while the second gives

$$\mathsf{P}(x), \quad \mathsf{P}^{-1}(x), \quad \$(\phi^\pi(k), x), \quad \$(\phi^\pi(k), x) \ ,$$

both of which are identical to the environment $(\mathsf{P}(x), \mathsf{P}^{-1}(x), \$(), \$())$. We will now argue that the above changes alter $\mathcal{A}$'s winning probabilities negligibly, down to the conditions on Φ that we introduced in the previous section.

Let us first look at the change where we replace $\mathsf{iE}(\phi^\pi(k), x)$ and $\mathsf{iD}(\phi^\pi(k), x)$ with $\$(\phi^\pi(k), x)$. We introduce another game and replace the random keyed permutations iE and iD by random keyed *functions* iF and iC:

$$\mathsf{P}(x), \quad \mathsf{P}^{-1}(x), \quad \mathsf{iF}(\phi^\pi(k), x), \quad \mathsf{iC}(\phi^\pi(k), x) \ .$$

Via (a keyed extension of) the random permutation/random function (RP/RF) switching lemma [8], the environments containing $(\mathsf{iF}, \mathsf{iC})$ and $(\mathsf{iE}, \mathsf{iD})$ can be shown to be indistinguishable up to the birthday bound $q_{em}^2/2^n$. The environments containing $\mathsf{iF}(\phi^\pi(k), x)$ and $\mathsf{iC}(\phi^\pi(k), x)$ and two copies of $\$(\phi^\pi(k), x)$ and can be shown to be identical down to the CF property. Indeed, an inconsistency could arise whenever $(\phi_1^\pi, x_1) \neq (\phi_2^\pi, x_2)$ but $(\phi_1^\pi(k), x_1) = (\phi_2^\pi(k), x_2)$. This means $x_1 = x_2$ and hence we must have that $\phi_1^\pi \neq \phi_2^\pi$. But $\phi_1^\pi(k) = \phi_2^\pi(k)$ and this leads to a break of the claw-freeness.

Let us now look at the changes made when we replace $\mathsf{P}^\pm(x \oplus \phi^\pi(k)) \oplus \phi^\pi(k)$ with $\$(x \oplus \phi^\pi(k)) \oplus \phi^\pi(k)$. We need to consider the points where a forgetful simulation of P or P^{-1} via \$ in the last two oracles leads to inconsistencies. Let us define the following six lists.

$$\mathsf{List}_\mathsf{P}^+ := [(a, \mathsf{P}(a)) : \mathcal{A} \text{ queries } a \text{ to } \mathsf{P}], \mathsf{List}_\mathsf{P}^- := [(\mathsf{P}^{-1}(b), b) : \mathcal{A} \text{ queries } b \text{ to } \mathsf{P}^{-1}] \ ,$$

$$\mathsf{List}_\phi^+ := [(a, \mathsf{P}(a)) : \phi^\pi(k) \text{ queries } \mathsf{P}(a)], \mathsf{List}_\phi^- := [(\mathsf{P}^{-1}(b), b) : \phi^\pi(k) \text{ queries } \mathsf{P}^{-1}(b)]$$

$$\mathsf{List}_\$^+ := [(x \oplus \phi^\pi(k), \$(x \oplus \phi^\pi(k))) : \mathcal{A} \text{ queries } (\phi^\pi, x) \text{ to RKEnc}] \ ,$$

$$\mathsf{List}_\$^- := [(\$(\phi^\pi(k) \oplus y), \phi^\pi(k) \oplus y) : \mathcal{A} \text{ queries } (\phi^\pi, y) \text{ to RKDec}] \ .$$

Let $\mathsf{List}_\star$ be the union of the above lists over all ϕ queried to RKEnc or RKDec. This list encodes the trace of the attack, as in the forgetful environment no queries to P or P^{-1} are made while handling RKEnc and RKDec queries. This trace is consistent with one coming from a permutation unless $\mathsf{List}_\star$ does not respect the permutivity properties, i.e., there are two entries $(a, b), (a', b') \in \mathsf{List}_\star$ such that it is not the case that $(a = a' \iff b = b')$. Note that one of these pairs must be in $\mathsf{List}_\$:= \mathsf{List}_\$^+ \cup \mathsf{List}_\$^-$ as the other oracles are faithfully implemented.

There is an inconsistency on $\mathsf{List}_\star$ if and only if there is an inconsistency among two lists (one of which is either $\mathsf{List}^+_\$$ or $\mathsf{List}^-_\$$). There are 20 possibilities to consider, including the order that queries are made. We consider first query of a pair being on $\mathsf{List}^+_\$$; the other cases are dealt with symmetrically.

$\mathsf{List}^+_\$$ and $\mathsf{List}^+_\mathsf{P}$: (1) The first component of a pair on $\mathsf{List}^+_\$$—we call this a first entry on $\mathsf{List}^+_\$$—matches a first entry a on $\mathsf{List}^+_\mathsf{P}$. This means that for some query (ϕ^π, x) to RKEnc we have that $a = \phi^\pi(k) \oplus x$. This leads to a break of output unpredictability. (2) The second entry on these lists match. More explicitly, we are looking at the probability that $\mathsf{P}(a) = R$, for R the output of \$ on a forward query. Here we can assume that R is known and this addresses the adaptivity of choice of a. But even in this case the probability of this event is small as P is a random permutation.

$\mathsf{List}^+_\$$ and $\mathsf{List}^-_\mathsf{P}$: (1) A second entry on $\mathsf{List}^+_\$$ matches a second entry b' on $\mathsf{List}^-_\mathsf{P}$. This means that for some query (ϕ^π, x) to RKEnc with output y we have that $b' = \phi^\pi(k) \oplus y$. This leads to a break of output unpredictability. (2) The first entries match on these lists. The argument is similar to case (2) above, but now is for P^{-1}.

$\mathsf{List}^+_\$$ and List^+_ϕ: (1) A first entry on $\mathsf{List}^+_\$$ matches a first entry List^+_ϕ. This means that for some query (ϕ^π_1, x) to RKEnc we have that $a = \phi^\pi_1(k) \oplus x$ for a query a of some other ϕ^π_2. This leads to a break of xor query independence. (2) The second entries match on these lists. The argument is as in case (2) of first pair of lists.

$\mathsf{List}^+_\$$ and List^-_ϕ: (1) A second entry on $\mathsf{List}^+_\$$ matches a second entry b' on List^-_ϕ. This means that for some query (ϕ^π_1, x) to RKEnc with output y we have that $b' = \phi^\pi_1(k) \oplus y$ for a query b' of some other ϕ^π_2. This leads to a break of xor query independence. (2) The first entries match on these lists. The argument is as in case (2) of the second pair of lists.

$\mathsf{List}^+_\$$ and $\mathsf{List}^+_\$$: Two first entries on $\mathsf{List}^+_\$$ match. This means that for two queries (ϕ^π_1, x_1) and (ϕ^π_2, x_2) to RKEnc we have that $\phi^\pi_1(k) \oplus x_1 = \phi^\pi_2(k) \oplus x_2$. Repeat-freeness ensures that $\phi_1 \neq \phi_2$ as otherwise $x_1 = x_2$ as well. This leads to a break of xor claw-freeness. (2) The second entries match on these lists. Since the oracle returns independent random values, this probability can be bounded by the birthday bound.

$\mathsf{List}^+_\$$ and $\mathsf{List}^-_\$$: A second entry on $\mathsf{List}^+_\$$ matches a second entry on $\mathsf{List}^-_\$$. This means that for a queries (ϕ^π_1, x_1) to RKEnc with outputs y_1 and (ϕ^π_2, x_2) to RKDec, we have that $\phi^\pi_1(k) \oplus y_1 = \phi^\pi_2(k) \oplus x_2$. Redundancy-freeness ensures that $\phi_1 \neq \phi_2$ as otherwise x_2 would be an encryption of x_1. This leads to a break of xor claw-freeness. (2) The first entries match on these lists. The probability of this event can be also bounded by the birthday bound.

Hence inconsistencies among any two pairs of lists happen with small probability, and this shows that $\mathsf{List}_\star$ is also inconsistent with small probability.

5 The Φ-RKCPA Security of $\mathsf{EM}^{\pi}[1,1,1]$

The theorem established in the previous section does not encompass $\Phi^{\oplus}$-RKA security as this set is not xor claw-free. In this section, we investigate whether an extra round of iteration can extend RKA security to the $\Phi^{\oplus}$ set. For the two-round EM constructions, up to relabelling, there are 5 simple key schedules: $[1,1,1]$, $[1,1,2]$, $[1,2,1]$, $[1,2,2]$, and $[1,2,3]$. It is easy to see that offset-switching attacks can be used to attack the $\Phi^{\oplus}$-RKCPA security of all but the first of these. In the following subsections we study the RKA security of the only remaining construction, $\mathsf{EM}^{\pi}[1,1,1]$.

5.1 Weakening the Conditions

We start by following a similar proof strategy to that given for $\mathsf{EM}^{\pi}[1,1]$ and identify a set of restrictions which are strong enough to enable a security proof, yet weak enough to encompass the $\Phi^{\oplus}$ set. Starting from the CPA environment

$$\pi(i,x,\sigma), \quad \mathsf{P}_2(\mathsf{P}_1(x \oplus \phi^{\pi}(k)) \oplus \phi^{\pi}(k)) \oplus \phi^{\pi}(k) \ ,$$

we simulate the P_2 oracle forgetfully and move to a setting with oracles

$$\pi(i,x,\sigma), \quad \$(\mathsf{P}_1(x \oplus \phi^{\pi}(k)) \oplus \phi^{\pi}(k)) \oplus \phi^{\pi}(k) \qquad \equiv \qquad \pi(i,x,\sigma), \quad \$() \ .$$

This game can be also be reached from the ideal game $\pi(i,x,\sigma), \mathsf{iE}(\phi^{\pi}(k),x)$ via an application of the RP/RF switching lemma [8] and the claw-freeness property as in the analysis of $\mathsf{EM}^{\pi}[1,1]$.

We now analyze the probability that the second environment simulates the first one in an inconsistent way. We look at inconsistencies which arise due to oracles being queried on the same inputs. The first place such an inconsistency might arise is when $\mathcal{A}$ makes an explicit π query $(2,a,+)$ that matches a query made to \$, i.e., $\mathsf{P}_1(x \oplus \phi^{\pi}(k)) \oplus \phi^{\pi}(k) = a$ for some (ϕ^{π}, x). Our first condition below addresses this event; we give a slight strengthening of the condition as we will be using it later on.

First-order output unpredictability. Let $t \geq 1$. The advantage of an adversary $\mathcal{A}$ against the *first-order output unpredictability* of an RKD set Φ with access to t ideal permutations is defined via

$$\mathbf{Adv}^{\mathsf{oup1}}_{\Phi,t}(\mathcal{A}) := \Pr[\exists (i,\sigma,\phi^{\pi},x,c) \in \mathsf{List} \text{ s.t. } \mathsf{P}_i^{\sigma}(\phi^{\pi}(k) \oplus x) \oplus \phi^{\pi}(k) = c : \mathsf{List} \leftarrow\!\!\$\ \mathcal{A}^{\pi}] \ .$$

Oracle π, the probability space, and List are defined analogously to the previous definitions. Note that in the RKCPA setting we do not need to consider inconsistencies resulting from inputs to P_1^{-1} or P_2^{-1} arising through RKDec queries, and only need to consider $(i,\sigma) = (1,+)$ above.

Inconsistencies arising as a result of two RKEnc queries (this oracle places queries to \$) lead to the following modification of claw-freeness.

First-order claw-freeness. Let $t \geq 1$. The advantage of an adversary $\mathcal{A}$ against the *first-order claw-freeness* of an RKD set Φ with access to t ideal permutations is defined via

$$\mathbf{Adv}^{\mathsf{cf1}}_{\Phi,t}(\mathcal{A}) := \Pr[\exists\,(i,\sigma,\phi_1^\pi,x_1,\phi_2^\pi,x_2) \in \mathsf{List} \text{ s.t.} \\ \mathsf{P}_i^\sigma(\phi_1^\pi(k)\oplus x_1)\oplus\phi_1^\pi(k) = \mathsf{P}_i^\sigma(\phi_2^\pi(k)\oplus x_2)\oplus\phi_2^\pi(k) \wedge \phi_1^\pi \neq \phi_2^\pi : \mathsf{List} \leftarrow\!\!\$\, \mathcal{A}^\pi]\ .$$

We now look at inconsistencies in the simulation due to a mismatch in an RKD query to π and a query to \$ made via the RKEnc oracle. Since only the second function is forgetfully simulated, we require independence of queries for P_2 only. Once again, in the RKCPA setting, restricting the definition to $(i,\sigma) = (1,+)$ suffices.

First-order query independence. Let $t \geq 2$. The advantage of an adversary $\mathcal{A}$ against the *first-order query independence* of an RKD set Φ with access to t ideal permutations is defined via

$$\mathbf{Adv}^{\mathsf{qi1}}_{\Phi,t}(\mathcal{A}) := \Pr[\exists(i,\sigma,\phi_1^\pi,x_1,\phi_2^\pi) \in \mathsf{List} : (2,\mathsf{P}_i^\sigma(\phi_1^\pi(k)\oplus x_1)\oplus\phi_1^\pi(k),\pm) \in \\ \in \overline{\mathsf{Qry}}[\phi_2^\pi(k)]; \mathsf{List} \leftarrow\!\!\$\, \mathcal{A}^\pi]\ ,$$

where, as before,

$$\mathsf{Qry}[\phi^\pi(k)] := \{(i,x,\sigma) : (i,x,\sigma) \text{ queried to } \pi \text{ by } \phi^\pi(k)\}\ , \\ \overline{\mathsf{Qry}}[k^\pi(k)] := \mathsf{Qry}[\phi^\pi(k)] \cup \{(i,\pi(i,x,\sigma),-\sigma) : (i,x,\sigma) \in \mathsf{Qry}[\phi^\pi(k)]\}\ .$$

The new set of conditions identified above allow us to carry out a similar proof strategy to that of Theorem 2 and establish the following result. (See the full version [28] for the details of the proof.)

Theorem 3 (Φ-RKCPA ***security of*** $\mathsf{EM}^\pi[1,1,1]$). *Let Φ be an RKD set. Then for any adversary $\mathcal{A}$ against the Φ-RKCPA security of $\mathsf{EM}^\pi[1,1,1]$ with parameters as defined before there are $\mathcal{B}_{1a}$ against $\mathsf{OUP1}$, $\mathcal{B}_{1b}$ against OUP, $\mathcal{B}_{2a}$ against $\mathsf{QI1}$, $\mathcal{B}_{2b}$ against XQI, $\mathcal{B}_3$ against $\mathsf{CF1}$, and $\mathcal{B}_4$ against CF such that*

$$\mathbf{Adv}^{\mathsf{rkcpa}}_{\mathsf{EM}^\pi[1,1,1],\Phi,2}(\mathcal{A}) \leq \mathbf{Adv}^{\mathsf{oup1}}_{\Phi,2}(\mathcal{B}_{1a}) + \mathbf{Adv}^{\mathsf{oup}}_{\Phi,2}(\mathcal{B}_{1b}) + \mathbf{Adv}^{\mathsf{qi1}}_{\Phi,2}(\mathcal{B}_{2a}) + \mathbf{Adv}^{\mathsf{xqi}}_{\Phi,2}(\mathcal{B}_{2b}) \\ + 2\mathbf{Adv}^{\mathsf{cf1}}_{\Phi,2}(\mathcal{B}_3) + \mathbf{Adv}^{\mathsf{cf}}_{\Phi,2}(\mathcal{B}_4) + \frac{q_{em}(q_2+\sum_\phi q_2^\phi)}{2^n-(q_2+\sum_\phi q_2^\phi)} + \frac{2q_{em}^2}{2^n}\ ,$$

where $\mathcal{B}_{1a}$ and $\mathcal{B}_{1b}$ output lists of length $q_2 q_{em}$, $\mathcal{B}_{2a}$ and $\mathcal{B}_{2b}$ lists of length q_{em}^2, $\mathcal{B}_3$ a list of length q_{em}^2, and $\mathcal{B}_4$ a list of length at most q_{em}^2.

5.2 $\Phi^\oplus$-RKCPA Security

We show that the restrictions identified above are weak enough so that the offset RKD set $\Phi^\oplus$ can be shown to satisfy them. We start by showing that for oracle-independent sets, Φ is output unpredictable and claw-free if and only if it is first-order output unpredictable and first-order claw-free.

Proposition 1 ($\mathsf{OUP} \wedge \mathsf{CF} \iff \mathsf{OUP1} \wedge \mathsf{CF1}$). *Let Φ be an oracle-independent RKD set and let $t \geq 1$. Then for any adversary $\mathcal{A}$ against the* OUP *(resp.* CF*) game outputting a list of size ℓ and placing q_i permutation queries with index i, there is an adversary $\mathcal{B}_1$ (resp. $\mathcal{B}_2$) outputting a list of size ℓ (resp. ℓ) and placing $q_i + \delta_{1i}\ell$ (resp. q_i) permutation queries with index i such that*

$$\mathbf{Adv}^{\mathsf{oup}}_{\Phi,t}(\mathcal{A}) \leq \mathbf{Adv}^{\mathsf{oup1}}_{\Phi,t}(\mathcal{B}_1) \quad \textit{and} \quad \mathbf{Adv}^{\mathsf{cf}}_{\Phi,t}(\mathcal{A}) \leq \mathbf{Adv}^{\mathsf{cf1}}_{\Phi,t}(\mathcal{B}_2) \ .$$

Moreover, for any adversary $\mathcal{A}$ against OUP1 *with parameters as before, there is an adversary $\mathcal{B}_1$ against* OUP *outputting a list of size $\ell \cdot q_\pi := \ell \cdot \sum_i q_i$, where it places q_i permutation queries with index i such that*

$$\mathbf{Adv}^{\mathsf{oup1}}_{\Phi,t}(\mathcal{A}) \leq \mathbf{Adv}^{\mathsf{oup}}_{\Phi,t}(\mathcal{B}_1) + \frac{\ell(q_\pi + 1)}{2^n - \ell} \ .$$

Finally, for any adversary $\mathcal{A}$ against CF1 *with parameters as before, there are adversaries $\mathcal{B}_1$ and $\mathcal{B}_2$, where $\mathcal{B}_1$ is as in the previous case, and $\mathcal{B}_2$ outputs a list of size ℓ and makes q_i permutation queries with index i such that*

$$\mathbf{Adv}^{\mathsf{cf1}}_{\Phi,t}(\mathcal{A}) \leq \mathbf{Adv}^{\mathsf{oup}}_{\Phi,t}(\mathcal{B}_1) + 2 \cdot \mathbf{Adv}^{\mathsf{cf}}_{\Phi,t}(\mathcal{B}_2) + \frac{\ell}{2^n - \ell} + \frac{\ell}{2^n - 2\ell} \ .$$

Bellare and Kohno [7] show that the RKD set $\Phi^{\oplus}$ is output unpredictable with advantage $\ell/2^n$ for any adversary outputting a list of size ℓ, and claw-free with advantage 0. The above proposition allow us to conclude that this set is also first-order output unpredictable and first-order claw-free.

Corollary 1. *Let $t \geq 1$ and suppose $\Phi^{\oplus}$ is defined with respect to a key space of size 2^n. Then for any $\mathcal{A}$ outputting a list of at most $\ell \leq 2^n/4$ and making at most q_1 queries to its P_1 oracle,*

$$\mathbf{Adv}^{\mathsf{oup1}}_{\Phi^{\oplus},t}(\mathcal{A}) \leq \frac{\ell \cdot (q_1 + 1)}{2^{n-1}} \quad \textit{and} \quad \mathbf{Adv}^{\mathsf{cf1}}_{\Phi^{\oplus},t}(\mathcal{A}) \leq \frac{\ell \cdot (q_1 + 2)}{2^{n-1}} \ .$$

This corollary together with Theorem 3 allow us to establish that $\mathsf{EM}^{\pi}[1,1,1]$ is $\Phi^{\oplus}$-RKCPA secure.

Corollary 2. *For any adversary $\mathcal{A}$ against the $\Phi^{\oplus}$-*RKCPA *security of $\mathsf{EM}^{\pi}[1,1,1]$ that makes at most q_π queries to its π oracle (of which q_i are to $\pi(i,\cdot,\cdot)$) and at most q_{em} queries to its* RKEnc *oracle, with $q_2 q_{em}$, $q_{em}^2 \leq 2^n/4$, we have*

$$\mathbf{Adv}^{\mathsf{rkcpa}}_{\mathsf{EM}^{\pi}[1,1,1],\Phi^{\oplus},2}(\mathcal{A}) \leq \frac{q_{em}(q_2 + q_{em})(2q_1 + 5)}{2^n} + \frac{q_2 q_{em}}{2^n - q_2} \ .$$

We remark that via a direct analysis (but at the expense of modularity) the cubic bound above can be tightened to a quadratic one.

Remark. The above results raises the question if the security proof can be extended to the CCA setting. Adapting an attack due to Andreeva et al. [3] on the indifferentiability of the two-round EM construction to the RKA setting, it can be seen that $\mathsf{EM}^{\pi}[1,1,1]$ is $\Phi^{\oplus}$-RKCCA insecure. Details are given in the full version [28]. This attack also applies if $\mathsf{P}_2 = \mathsf{P}_1$.

6 The Φ-RKCCA Security of $\mathsf{EM}^{\pi}[1,1,1,1]$

Building on the results of the previous sections, we set out to find a key schedule for the iterated Even–Mansour construction that provides $\Phi^{\oplus}$-RKCCA security. Our previous results show that at least three rounds are necessary. We start by showing that of the fourteen possible simple key schedules for three-round EM, all but one fall prey to $\Phi^{\oplus}$-RKCCA attacks. We then show that the remaining $\mathsf{EM}^{\pi}[1,1,1,1]$ construction does indeed provide $\Phi^{\oplus}$-RKCCA security.

Up to relabeling, then there are 14 possible key schedules for the three-round Even–Mansour schemes. Of these, 9 are susceptible to offset-switching attacks. These are key schedules where a key appears only in the first or the last round and nowhere else, e.g., $[1,2,2,2]$, $[1,2,2,3]$, or $[1,2,2,1]$. This rules out 9 key schedules. Another 4 can be attacked using Andreeva et al.'s attack [3]. These are the $[1,1,2,1]$, $[1,2,1,1]$, $[1,1,2,2]$, and $[1,2,1,2]$ schedules. Details are given in the full version of the paper [28].

These attacks give a generic 4-query related-key distinguisher for reduced-round LED [32] (8 out of 32 rounds for LED-64 and 16 out of 48 for LED-128). Our results lend support to the designers' claim that LED provides good related-key attack security in spite of the simple key schedule, even though they do not apply directly to LED as the round functions are neither random permutations nor independent.

We now show that $\mathsf{EM}^{\pi}[1,1,1,1]$ achieves Φ-RKCCA security for sets Φ which include, amongst others, the $\Phi^{\oplus}$ set. As before, we motivate a number of restrictions on Φ by considering a simulation strategy and analyzing the inconsistencies that could arise. The adversary in the Φ-RKCCA game with respect to the construction has access to π and the oracles

$$\mathsf{P}_3(\mathsf{P}_2(\mathsf{P}_1(x \oplus \phi^{\pi}(k)) \oplus \phi^{\pi}(k)) \oplus \phi^{\pi}(k)) \oplus \phi^{\pi}(k) \ ,$$

$$\mathsf{P}_1^{-1}(\mathsf{P}_2^{-1}(\mathsf{P}_3^{-1}(x \oplus \phi^{\pi}(k)) \oplus \phi^{\pi}(k)) \oplus \phi^{\pi}(k)) \oplus \phi^{\pi}(k) \ .$$

Once again we aim to simulate the above two oracles by returning uniformly random values. There are at least two way to perform this:

(a) Simulate the outer permutations in RKEnc and RKDec forgetfully. That is, the P_3 oracle in RKEnc and the P_1^{-1} oracle in RKDec are forgetfully implemented.
(b) Simulate the middle oracles P_2 and P_2^{-1} forgetfully. This will ensure that the inputs to $\mathsf{P}_1^{\pm}$ and $\mathsf{P}_3^{\pm}$ are randomized, and hence their outputs will be also random.

The first approach, although in some sense the more natural one, does not work. This is due to the fact that P_1 (resp. P_3) also appear as the first-round permutation in RKEnc (resp. RKDec). An adversary which performs an offset switch can trigger collisions in these oracles without being detected. We therefore adapt the second simulation strategy and for forgetful oracle \$ consider

$$\mathsf{P}_3(\$(\mathsf{P}_1(x \oplus \phi^{\pi}(k)) \oplus \phi^{\pi}(k)) \oplus \phi^{\pi}(k)) \oplus \phi^{\pi}(k) \ ,$$

$$\mathsf{P}_1^{-1}(\$(\mathsf{P}_3^{-1}(x \oplus \phi^{\pi}(k)) \oplus \phi^{\pi}(k)) \oplus \phi^{\pi}(k)) \oplus \phi^{\pi}(k) \ .$$

We now consider inconsistencies, starting with a query collision between π (from a query of $\mathcal{A}$) and \$ arising from either the forward or backwards direction. Here we rely on first-order output unpredictability, but note that $(i, \sigma) = (1, +)$ and $(i, \sigma) = (3, -)$ will be critically relied on. Collisions arising between an RKD query to π and a \$ query in either direction can be ruled out down to first-order query independence; once again $(i, \sigma) \in \{(1, +), (3, -)\}$ will be used. Finally, the probability that a collision occurs as a result of two queries to \$ (due to forward or backward queries) can be bounded by the first-order claw freeness property. As before, inconsistencies also arise due to collisions between the outputs of oracle queries; the probability of this occurring can be bounded information theoretically. Note that here we also rely on independence of queries to the second permutation, but both cases $(i, \sigma) \in \{(1, +), (3, -)\}$ in the definition will be used. We formally prove the following theorem in [28].

Theorem 4 (Φ-RKCCA **Security of** $\mathsf{EM}^{\pi}[1,1,1,1]$). *Let Φ be an RKD set. Then for any adversary $\mathcal{A}$ against the* Φ-RKCPA *security of* $\mathsf{EM}^{\pi}[1,1,1,1]$ *with parameters as before, we have adversaries $\mathcal{B}_1$, $\mathcal{B}_2$, $\mathcal{B}_3$, and $\mathcal{B}_4$ such that*

$$\begin{aligned}\mathbf{Adv}^{\mathsf{rkcca}}_{\mathsf{EM}^{\pi}[1,1,1,1],\Phi,3}(\mathcal{A}) \leq & \mathbf{Adv}^{\mathsf{oup1}}_{\Phi,3}(\mathcal{B}_1) + \mathbf{Adv}^{\mathsf{xqi1}}_{\Phi,3}(\mathcal{B}_2) + 2\mathbf{Adv}^{\mathsf{cf1}}_{\Phi,3}(\mathcal{B}_3) \\ & + \mathbf{Adv}^{\mathsf{cf}}_{\Phi,3}(\mathcal{B}_4) + \frac{2q_{em}^2}{2^n} + \frac{2q_{em}(q_2 + \sum_{\phi} q_2^{\phi})}{2^n - (q_2 + \sum_{\phi} q_2^{\phi})} \ ,\end{aligned}$$

where $\mathcal{B}_1$ outputs a list of length $2q_2q_{em}$, $\mathcal{B}_2$ a list of length $2q_{em}^2$, $\mathcal{B}_3$ a list of length q_{em}^2, and $\mathcal{B}_4$ a list of length at most q_{em}^2.

Corollary 1 together with Theorem 4 allow us to establish that the three-round single-key Even–Manour construction with independent round permutations is $\Phi^{\oplus}$-RKCCA secure:

Corollary 3. *For any adversary $\mathcal{A}$ against the* $\Phi^{\oplus}$-RKCCA *security of* $\mathsf{EM}^{\pi}[1,1,1,1]$ *with parameters defined as before. Then*

$$\mathbf{Adv}^{\mathsf{rkcca}}_{\mathsf{EM}^{\pi}[1,1,1,1],\Phi^{\oplus},3}(\mathcal{A}) \leq \frac{2q_{em}(q_2 + q_{em})(2q_1 + 2q_3 + 9)}{2^n} + \frac{2q_{em}q_2}{2^n - q_2} \ .$$

Once again, via a direct analysis (but at the expense of modularity) the cubic bound above can be tightened to a quadratic one.

Acknowledgments. The authors would like to thank Martijn Stam for discussions on the relation between indifferentiability and RKA security.

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.J., Kuhn, M.G.: 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. Andreeva, E., Bogdanov, A., Dodis, Y., Mennink, B., Steinberger, J.P.: On the indifferentiability of key-alternating ciphers. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013, Part I. LNCS, vol. 8042, pp. 531–550. Springer, Heidelberg (2013)
4. Barbosa, M., Farshim, P.: The related-key analysis of feistel constructions. In: Cid, C., Rechberger, C. (eds.) FSE 2014. LNCS, vol. 8540, pp. 265–284. Springer, Heidelberg (2015)
5. Bellare, M., Cash, D.: Pseudorandom functions and permutations provably secure against related-key attacks. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 666–684. Springer, Heidelberg (2010)
6. 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)
7. 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)
8. Bellare, M., Rogaway, P.: The security of triple encryption and a framework for code-based game-playing proofs. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 409–426. Springer, Heidelberg (2006)
9. Biham, E.: New types of cryptanalytic attacks using related keys. J. Cryptology **7**(4), 229–246 (1994)
10. Biham, E.: New types of cryptanalytic attacks using related keys. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 398–409. Springer, Heidelberg (1994)
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. Biryukov, A., Wagner, D.: Advanced slide attacks. In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, pp. 589–606. Springer, Heidelberg (2000)
14. Bogdanov, A.A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M., Seurin, Y., Vikkelsoe, C.: PRESENT: an ultra-lightweight block cipher. In: Paillier, P., Verbauwhede, I. (eds.) CHES 2007. LNCS, vol. 4727, pp. 450–466. Springer, Heidelberg (2007)
15. 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)
16. Borghoff, J., et al.: PRINCE – A low-latency block cipher for pervasive computing applications. In: Wang, X., Sako, K. (eds.) ASIACRYPT 2012. LNCS, vol. 7658, pp. 208–225. Springer, Heidelberg (2012)
17. Chen, S., Lampe, R., Lee, J., Seurin, Y., Steinberger, J.: Minimizing the two-round even-mansour cipher. In: Garay, J.A., Gennaro, R. (eds.) CRYPTO 2014, Part I. LNCS, vol. 8616, pp. 39–56. Springer, Heidelberg (2014)
18. Chen, S., Steinberger, J.: Tight security bounds for key-alternating ciphers. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 327–350. Springer, Heidelberg (2014)

19. Cogliati, B., Seurin, Y.: On the provable security of the iterated even-mansour cipher against related-key and chosen-key attacks. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015. LNCS, vol. 9056, pp. 584–613. Springer, Heidelberg (2015)
20. Cogliati, B., Seurin, Y.: On the provable security of the iterated Even-Mansour cipher against related-key and chosen-key attacks. Cryptology ePrint Archive, Report 2015/069 (2015). http://eprint.iacr.org/2015/069
21. Daemen, J.: Limitations of the Even-Mansour construction (rump session). In: Imai, H., Rivest, R.L., Matsumoto, T. (eds.) ASIACRYPT 1991. LNCS, vol. 739, pp. 495–498. Springer, Heidelberg (1993)
22. Daemen, J., Rijmen, V.: The block cipher Rijndael. In: Quisquater, J.-J., Schneier, B. (eds.) CARDIS 1998. LNCS, vol. 1820, pp. 277–284. Springer, Berlin Heidelberg (2000)
23. Daemen, J., Rijmen, V.: The wide trail design strategy. In: Honary, B. (ed.) Cryptography and Coding 2001. LNCS, vol. 2260, pp. 222–238. Springer, Heidelberg (2001)
24. Dunkelman, O., Keller, N., Shamir, A.: Minimalism in cryptography: the even-mansour scheme revisited. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 336–354. Springer, Heidelberg (2012)
25. EMVCo. EMV Integrated Circuit Card Specifications for Payment Systems, Book 2, Security and Key Management, June 2008. Version 4.2
26. Even, S., Mansour, Y.: A construction of a cipher from a single pseudorandom permutation. In: Imai, H., Rivest, R.L., Matsumoto, T. (eds.) ASIACRYPT 1991. LNCS, vol. 739, pp. 210–224. Springer, Heidelberg (1993)
27. Even, S., Mansour, Y.: A construction of a cipher from a single pseudorandom permutation. J. Cryptology **10**(3), 151–162 (1997)
28. Farshim, P., Procter, G.: The related-key security of iterated even-mansour ciphers. Cryptology ePrint Archive, Report 2014/953 (2014). http://eprint.iacr.org/2014/953
29. Gentry, C., Ramzan, Z.: Eliminating random permutation oracles in the even-mansour cipher. In: Lee, P.J. (ed.) ASIACRYPT 2004. LNCS, vol. 3329, pp. 32–47. Springer, Heidelberg (2004)
30. Gérard, B., Grosso, V., Naya-Plasencia, M., Standaert, F.-X.: Block ciphers that are easier to mask: how far can we go? In: Bertoni, G., Coron, J.-S. (eds.) CHES 2013. LNCS, vol. 8086, pp. 383–399. Springer, Heidelberg (2013)
31. Gong, Z., Nikova, S., Law, Y.W.: KLEIN: a new family of lightweight block ciphers. In: Juels, A., Paar, C. (eds.) RFIDSec 2011. LNCS, vol. 7055, pp. 1–18. Springer, Heidelberg (2012)
32. Guo, J., Peyrin, T., Poschmann, A., Robshaw, M.: The LED block cipher. In: Preneel, B., Takagi, T. (eds.) CHES 2011. LNCS, vol. 6917, pp. 326–341. Springer, Heidelberg (2011)
33. 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.) 43rd ACM STOC, pp. 89–98. ACM Press, June 2011
34. 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)
35. Jean, J., Nikolić, I., Peyrin, T., Wang, L., Wu, S.: Security analysis of PRINCE. In: Moriai, S. (ed.) FSE 2013. LNCS, vol. 8424, pp. 92–111. Springer, Heidelberg (2014)

36. Kilian, J., Rogaway, P.: How to protect DES against exhaustive key search. In: Koblitz, N. (ed.) CRYPTO 1996. LNCS, vol. 1109, pp. 252–267. Springer, Heidelberg (1996)
37. Kilian, J., Rogaway, P.: How to protect DES against exhaustive key search (an analysis of DESX). J. Cryptology **14**(1), 17–35 (2001)
38. Knudsen, L.R.: Cryptanalysis of LOKI 91. In: Seberry, J., Zheng, Y. (eds.) AUSCRYPT 1992. LNCS, vol. 718, pp. 196–208. Springer, Heidelberg (1993)
39. Lampe, R., Patarin, J., Seurin, Y.: An asymptotically tight security analysis of the iterated even-mansour cipher. In: Wang, X., Sako, K. (eds.) ASIACRYPT 2012. LNCS, vol. 7658, pp. 278–295. Springer, Heidelberg (2012)
40. Lampe, R., Seurin, Y.: How to construct an ideal cipher from a small set of public permutations. In: Sako, K., Sarkar, P. (eds.) ASIACRYPT 2013, Part I. LNCS, vol. 8269, pp. 444–463. Springer, Heidelberg (2013)
41. Liskov, M., Rivest, R.L., Wagner, D.: Tweakable block ciphers. In: Yung, M. (ed.) CRYPTO 2002. LNCS, vol. 2442, pp. 31–46. Springer, Heidelberg (2002)
42. 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)
43. Maurer, U.M., Renner, R.S., Holenstein, C.: Indifferentiability, impossibility results on reductions, and applications to the random oracle methodology. In: Naor, M. (ed.) TCC 2004. LNCS, vol. 2951, pp. 21–39. Springer, Heidelberg (2004)
44. Mendel, F., Rijmen, V., Toz, D., Varıcı, K.: Differential analysis of the LED block cipher. In: Wang, X., Sako, K. (eds.) ASIACRYPT 2012. LNCS, vol. 7658, pp. 190–207. Springer, Heidelberg (2012)
45. National Institute of Standards and Technology. FIPS Publication 197, Announcing the Advanced Encryption Standard (AES) (2001)
46. Özen, O., Varıcı, K., Tezcan, C., Kocair, Ç.: Lightweight block ciphers revisited: cryptanalysis of reduced round PRESENT and HIGHT. In: Boyd, C., González Nieto, J. (eds.) ACISP 2009. LNCS, vol. 5594, pp. 90–107. Springer, Heidelberg (2009)
47. Patarin, J.: The "Coefficients H" technique. In: Avanzi, R.M., Keliher, L., Sica, F. (eds.) SAC 2008. LNCS, vol. 5381, pp. 328–345. Springer, Heidelberg (2009)
48. Ristenpart, T., Shacham, H., Shrimpton, T.: Careful with composition: limitations of the indifferentiability framework. In: Paterson, K.G. (ed.) EUROCRYPT 2011. LNCS, vol. 6632, pp. 487–506. Springer, Heidelberg (2011)
49. Shannon, C.E.: Communication theory of secrecy systems. Bell Syst. Tech. J. **128**(4), 656–715 (1949)
50. Steinberger, J.: Improved security bounds for key-alternating ciphers via hellinger distance. Cryptology ePrint Archive, Report 2012/481 (2012). http://eprint.iacr.org/2012/481