Strengthening the Known-Key Security Notion for Block Ciphers

Benoît Cogliati and Yannick Seurin

University of Versailles, France
benoitcogliati@hotmail.fr

ANSSI, Paris, France
yannick.seurin@m4x.org

Abstract. We reconsider the formalization of known-key attacks against ideal primitive-based block ciphers. This was previously tackled by Andreeva, Bogdanov, and Mennink (FSE 2013), who introduced the notion of *known-key indifferentiability*. Our starting point is the observation, previously made by Cogliati and Seurin (EUROCRYPT 2015), that this notion, which considers only a single known key available to the attacker, is too weak in some settings to fully capture what one might expect from a block cipher informally deemed resistant to known-key attacks. Hence, we introduce a stronger variant of known-key indifferentiability, where the adversary is given *multiple* known keys to "play" with, the informal goal being that the block cipher construction must behave as an independent random permutation for each of these known keys. Our main result is that the 9-round iterated Even-Mansour construction (with the trivial key-schedule, i.e., the same round key xored between permutations) achieves our new "multiple" known-keys indifferentiability notion, which contrasts with the previous result of Andreeva *et al.* that one single round is sufficient when only a single known key is considered. We also show that the 3-round iterated Even-Mansour construction achieves the weaker notion of multiple known-keys *sequential* indifferentiability, which implies in particular that it is *correlation intractable* with respect to relations involving any (polynomial) number of known keys.

Keywords: block cipher, ideal cipher, known-key attacks, iterated Even-Mansour cipher, key-alternating cipher, indifferentiability, correlation intractability

1 Introduction

Background on Known-Key Attacks. Informally, a known-key attack against a block cipher E consists in the following: the adversary is given a key k from the key space of E, and must find a "non-trivial" property of the permutation E_k associated with k faster than what it would cost given only black-box access to a truly random permutation. An example of such a non-trivial property would be a plaintext/ciphertext pair (x, y) under the key k such that, say, the first half of x and the first half of y seen as bit strings are both zero (for a random permutation P over n-bit strings, it is easy to see that this requires roughly $2^{n/2}$ queries to P). Known-key attacks against block ciphers were first introduced by

Knudsen and Rijmen [18], who exhibited such attacks against a reduced-round version of AES and against certain kinds of Feistel ciphers. These attacks were extended in a number of follow-up papers, e.g. [23, 15, 24, 28, 14].

Even though the informal idea underlying known-key security might intuitively seem clear (given a key k, the permutation E_k associated with k must "look random"), how to put known-key attacks on theoretical sound grounds has remained elusive. Indeed, any attempt to rigorously formalize what is a known-attack against a fixed block cipher runs into impossibility results similar to those undermining a sound definition of what a "good" hash function should be [4]. In particular, seeing a block cipher as a family of permutations indexed by the key, the fact that the key-length is similar to the input-length of the permutations (i.e., the block-length of the block cipher) leads to the following "diagonal" problem: consider the set of pairs $(k, E_k(k))$ for k ranging over the key space (we assume that the block-length and the key-length are equal for ease of exposition); then it is hard, given oracle access to a random permutation, to find an input/output pair in this set, whereas given any key k for E it is very easy to find an input/output pair for E_k in this set.

A way to circumvent these impossibilities is to consider block cipher constructions based on some ideal primitive (for example, a Feistel cipher based on public random round functions or (iterated) Even-Mansour ciphers based on public permutations). In that case, even though the adversary is given the known key, it only has oracle access to the underlying primitive, which effectively acts as an (exponentially long) seed indexing the permutation associated with the key. A first step towards formalizing known-key attacks for ideal primitive-based block ciphers was taken by Andreeva, Bogdanov, and Mennink (ABM) [2] through what they called *known-key indifferentiability* (KK-indifferentiability for short), a variant of the standard indifferentiability notion [22]. A block cipher construction $\mathcal{C}^F$ from some underlying primitive F is said indifferentiable from an ideal cipher E if there exists an efficient simulator $\mathcal{S}$ with black box access to E such that the two pairs of oracles $(\mathcal{C}^F, F)$ and $(E, \mathcal{S}^E)$ are indistinguishable. Hence the simulator must make E "look like" $\mathcal{C}^F$ by returning answers that are coherent with the distinguisher's queries to E (without, in general, knowing these E-queries) and that are statistically close to answers of a real F oracle.

The KK-indifferentiability notion of ABM modifies the security experiment as follows: a key k is drawn at random and made available to the distinguisher and the simulator; the distinguisher is then allowed to query its left oracle (construction/ideal cipher) *only for this specific key k*. Hence the simulator's job is somehow made simpler since it has a "hint" about which queries the distinguisher can make to its left oracle. Note that in the ideal (simulated) world, the distinguisher effectively has access to a single random permutation (since an ideal cipher behaves as an independent random permutation for each key). Hence this KK-indifferentiability notion intuitively captures the requirement that for each key k, the block cipher construction $\mathcal{C}^F$ must "look like" a random permutation. In contrast, the standard indifferentiability notion is related with *chosen-key* attacks, since the distinguisher is allowed to freely choose the keys it examines.

Shortcoming of the ABM Security Notion. The starting point of this paper is an observation, previously made by Cogliati and Seurin (Appendix C of the full version of [7]) that the ABM security notion might be too restrictive in some situations because it considers *one single* known-key. This might be problematic in some cryptosystems where intuitively resistance to known-key attacks should be sufficient to provide security, but where the ABM security notion fails because the cryptosystem uses *multiple* known keys. Think for example of the permutation-based hashed functions by Rogaway and Steinberger [26, 27]: these constructions are based on a few (typically 3 to 6) public permutations, which would typically be instantiated by a block cipher used with distinct publicly known keys. A crucial requirement for the security proof of these constructions to hold (in the ideal permutation model) is that the permutations are independent. Since this is not ensured by the ABM security notion, it is not applicable here, even though one would like to say that a block cipher which is secure against known-key attacks can safely be used in the Rogaway-Steinberger constructions. (Jumping ahead, our new KK-indifferentiability notion will be sufficient to safely instantiate the block cipher in the same constructions.)

To better emphasize this gap between a single known-key notion and a multiple known-key notion, consider the case of the 1-round Even-Mansour (EM) [12, 11] construction based on a permutation P on $\{0,1\}^n$, which maps a key $k \in \{0,1\}^n$ and a plaintext $x \in \{0,1\}^n$ to the ciphertext defined as

$$\mathsf{EM}^P(k,x) = k \oplus P(k \oplus x).$$

ABM showed that when the permutation P is ideal, this construction is KK-indifferentiable from an ideal cipher in the single known-key setting. However, if the adversary is given any pair of distinct keys (k_1,k_2), it can pick any $x_1 \in \{0,1\}^n$, define $x_2 = x_1 \oplus k_1 \oplus k_2$, and compute $y_1 = \mathsf{EM}^P_{k_1}(x_1)$ and $y_2 = \mathsf{EM}^P_{k_2}(x_2)$. Then one can easily check that $x_1 \oplus x_2 = y_1 \oplus y_2$. Yet for an ideal cipher E, given two distinct keys $k_1 \neq k_2$, finding two pairs (x_1,y_1) and (x_2,y_2) such that $E_{k_1}(x_1) = y_1$, $E_{k_2}(x_2) = y_2$, and $x_1 \oplus x_2 = y_1 \oplus y_2$ can be shown to be hard: more precisely, an adversary making at most q queries to E can find such pairs with probability at most $\mathcal{O}(\frac{q^2}{2^n})$. In other words, the permutations associated with distinct keys for the 1-round EM construction do not "behave" independently.

Our Contribution. Our first contribution is definitional: in order to remedy the limitation that we just pointed out, we extend and strengthen the known-key security definition of [2], by allowing the distinguisher to be given multiple known keys. Our new notion is parameterized by an integer μ, the number of known keys that the adversary is given. For $\mu = 1$, one recovers the ABM definition. If one lets $\mu = |\mathcal{K}|$, where $\mathcal{K}$ is the key space of the block cipher, one recovers the standard indifferentiability notion. In fact, our KK-indifferentiability notion will emerge as a special case of a more general notion that we name *restricted-input*-indifferentiability, which might be of independent interest. We also formulate our KK-indifferentiability notion in a "worst-case" fashion (it must hold for *any* subset of keys of size μ), whereas the ABM notion was in the "average-case" style (the known key being randomly drawn). In addition, we define a weaker "sequential" variant [21, 7] of our new μ-KK-indifferentiability notion, called μ-KK-seq-indifferentiability, where the adversary must query its two oracles in a specific order. This notion is useful since it implies the weaker notion of correlation intractability.

Our second contribution is about constructions: we show that KK-indifferentiability is a meaningful notion by proving that the iterated Even-Mansour (IEM) construction with nine rounds is μ-KK-indifferentiable from an ideal cipher for any $\mu = \texttt{poly}(n)$ (where n is a security parameter indexing the construction), which contrasts with the fact that one round is sufficient when considering one single known-key, and also with the best number of rounds known to be sufficient to achieve full indifferentiability from an ideal cipher, namely twelve [20]. We also show that three rounds are necessary and sufficient to achieve the weaker μ-KK-seq-indifferentiability notion, which again contrast with the fact that four rounds are necessary and sufficient to achieve (full) seq-indifferentiability from an ideal cipher [7]. See Table 1 for a summary of known results on the IEM construction.

More Related Work. A number of papers have studied the indifferentiability of variants of the IEM construction. In particular, Andreeva *et al.* [1] have studied the case where the key-schedule is modeled as a random oracle, and Guo and Lin have studied the case of Even-Mansour ciphers with two interleaved keys [16] and of key-alternating Feistel ciphers [17].

Organization. We start with some general definitions in Section 2. Then we define precisely our strengthened KK-indifferentiability notion (as well as the more general notion of *restricted-input*-indifferentiability, of which KK-indifferentiability is a special case) in Section 3. In Section 4, we give a known-key attack (using two known keys) against the 2-round IEM construction. Finally, we prove that the 3-round, resp. 9-round, IEM construction achieves μ-KK-seq-indifferentiability, resp. μ-KK-indifferentiability, in Sections 5 and 6.

2 Preliminaries

General Notation. In all the following, we fix an integer $n \geq 1$ and denote $N = 2^n$. Given a non-empty set $\mathcal{M}$, the set of all permutations of $\mathcal{M}$ will be denoted $\mathsf{Perm}(\mathcal{M})$. We simply denote $\mathsf{Perm}(n)$ the set of all permutations over $\{0,1\}^n$. A block cipher with key space $\mathcal{K}$ and message space $\mathcal{M}$ is a mapping $E : \mathcal{K} \times \mathcal{M} \to \mathcal{M}$ such that for any key $k \in \mathcal{K}$, $x \mapsto E(k, x)$ is a permutation. We interchangeably use the notations $E(k, x)$ and $E_k(x)$. We denote $\mathsf{BC}(\mathcal{K}, \mathcal{M})$ the set of all block ciphers with key space $\mathcal{K}$ and message space $\mathcal{M}$, and $\mathsf{BC}(n, n)$ the set of block ciphers with key space and message space $\{0,1\}^n$. For integers $1 \leq s \leq t$, we will write $(t)_s = t(t-1)\cdots(t-s+1)$ and $(t)_0 = 1$ by convention.

Table 1. Summary of provable security results for the iterated Even-Mansour cipher with independent inner permutations and the trivial key-schedule. The first two notions are secret-key notions, the other ones are indifferentiability-based.

Sec. notion	# rounds	Sec. bound	Sim. complexity (query / time)	Ref.
Single-key (pseudorandomness)	1	$q^2/2^n$	—	[12, 11]
	2	$q^{3/2}/2^n$	—	[5]
XOR Related-Key	3	$q^2/2^n$	—	[7, 13]
1-KK-indiff.	1	0	q / q	[2]
μ-KK-Seq-indiff., $\mu > 1$	3	$\mu^2 q^2/2^n$	μq / μq	this paper
Full Seq-indiff.	4	$q^4/2^n$	q^2 / q^2	[7]
μ-KK-indiff., $\mu > 1$	9	$\mu^6 q^6/2^n$	$\mu^2 q$ / $\mu^2 q$	this paper
Full indiff.	12	$q^{12}/2^n$	q^4 / q^6	[20]

Ideal Primitives. An *ideal primitive* F is a triplet $(\mathsf{F.Dom}, \mathsf{F.Rng}, \mathsf{F.Inst})$: the domain $\mathsf{F.Dom}$ and the range $\mathsf{F.Rng}$ are two non-empty sets, and the instance space $\mathsf{F.Inst}$ is a set of functions $F : \mathsf{F.Dom} \to \mathsf{F.Rng}$.

The two main ideal primitives we will be interested in are ideal permutations and ideal ciphers. Given a non-empty set $\mathcal{M}$, the ideal permutation P over $\mathcal{M}$ is defined as follows. Let $\mathsf{P.Dom} = \{+, -\} \times \mathcal{M}$ and $\mathsf{P.Rng} = \mathcal{M}$, and define

$$\mathsf{P.Inst} \overset{\text{def}}{=} \left\{P : \exists \pi \in \mathsf{Perm}(\mathcal{M}), P(+, x) = \pi(x) \text{ and } P(-, y) = \pi^{-1}(y)\right\}.$$

Clearly, there is a one-to-one correspondence between $\mathsf{P.Inst}$ and $\mathsf{Perm}(\mathcal{M})$.

Similarly, given two non-empty sets $\mathcal{K}$ and $\mathcal{M}$, the ideal cipher with key space $\mathcal{K}$ and message space $\mathcal{M}$ is defined as follows. Let $\mathsf{E.Dom} = \{+, -\} \times \mathcal{K} \times \mathcal{M}$, $\mathsf{E.Rng} = \mathcal{M}$, and define

$$\mathsf{E.Inst} \overset{\text{def}}{=} \left\{E : \exists \eta \in \mathsf{BC}(\mathcal{K}, \mathcal{M}), E(+, k, x) = \eta_k(x) \text{ and } E(-, k, y) = \eta_k^{-1}(y)\right\}.$$

Again, there is a one-to-one correspondence between $\mathsf{E.Inst}$ and $\mathsf{BC}(\mathcal{K}, \mathcal{M})$.

The Iterated Even-Mansour Cipher. Fix integers $n, r \geq 1$. Let $\mathbf{f} = (f_0, \ldots, f_r)$ be a $(r+1)$-tuple of permutations of $\{0,1\}^n$. The r-round iterated Even-Mansour construction $\mathsf{EM}[n, r, \mathbf{f}]$ specifies, from any r-tuple $\mathbf{P} = (P_1, \ldots, P_r)$ of permutations of $\{0,1\}^n$, a block cipher with n-bit keys and n-bit messages, simply denoted $\mathsf{EM}^{\mathbf{P}}$ in all the following (parameters $[n, r, \mathbf{f}]$ will always be clear from the context), which maps a plaintext $x \in \{0,1\}^n$ and a key $k \in \{0,1\}^n$ to the ciphertext defined by (see Fig. 1):

$$\mathsf{EM}^{\mathbf{P}}(k, x) = f_r(k) \oplus P_r(f_{r-1}(k) \oplus P_{r-1}(\cdots P_2(f_1(k) \oplus P_1(f_0(k) \oplus x))\cdots)).$$

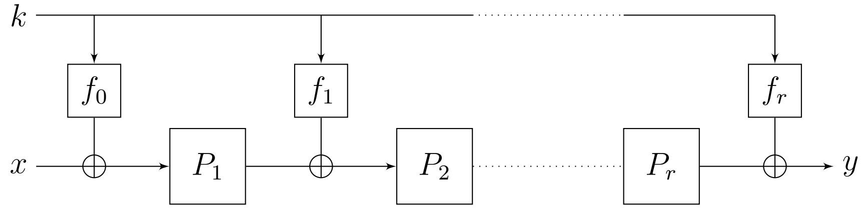

Fig. 1. The r-round iterated Even-Mansour cipher.

We say that the key-schedule is *trivial* when all f_i's are the identity.

While the pseudorandomness of the IEM cipher was mostly studied with *independent* round keys [3, 19, 6] (with the notable exception of [5]), it is well known that independent round keys cannot, in general, provide any security in the setting where the adversary has some control over the master key (related-, known-, or chosen-key attacks) [20]. Hence, in this paper, we focus on the case where the round keys are derived from an n-bit master key (actually, all our results deal with the case of the trivial key-schedule).

3 Restricted-Input Indifferentiability and Variants

We introduce the notion of restricted-input indifferentiability (*RI-indifferentiability*), and explain how known-key indifferentiability is a special case of it. Let E and F be two ideal primitives.[1] A *construction* implementing E from F is a deterministic algorithm $\mathcal{C}$ with oracle access to an instance F of F, which we denote $\mathcal{C}^F$, such that for any $F \in \mathsf{F.Inst}$, $\mathcal{C}^F \in \mathsf{E.Inst}$. A *simulator* for F is a randomized algorithm with oracle access to an instance E of E, which we denote $\mathcal{S}^E$, such that for any $E \in \mathsf{E.Inst}$, $\mathcal{S}^E : \mathsf{F.Dom} \to \mathsf{F.Rng}$. A distinguisher $\mathcal{D}$ is a deterministic[2] algorithm with oracle access to two oracles, the first one with signature $\mathsf{E.Dom} \to \mathsf{E.Rng}$, the second one with signature $\mathsf{F.Dom} \to \mathsf{F.Rng}$, and which returns a bit b, which we denote $\mathcal{D}(\mathcal{O}_1, \mathcal{O}_2) = b$. We will call $\mathcal{O}_1$ the *left* oracle and $\mathcal{O}_2$ the *right* oracle. Following [21], we define the *total oracle query cost* of $\mathcal{D}$ as the maximum, over $F \in \mathsf{F.Inst}$, of the total number of queries received by F (from $\mathcal{D}$ or $\mathcal{C}$) when $\mathcal{D}$ interacts with $(\mathcal{C}^F, F)$. The indifferentiability advantage of $\mathcal{D}$ against $(\mathcal{C}, \mathcal{S})$ is defined by

$$\begin{aligned}\mathbf{Adv}^{\mathrm{indiff}}_{\mathcal{C},\mathcal{S}}(\mathcal{D}) = \Big| &\Pr\left[E \leftarrow_{\$} \mathsf{E.Inst} : \mathcal{D}(E, \mathcal{S}^E) = 1\right] \\ &- \Pr\left[F \leftarrow_{\$} \mathsf{F.Inst} : \mathcal{D}(\mathcal{C}^F, F) = 1\right]\Big|. \end{aligned} \quad (1)$$

(Note that the first probability is also taken over the randomness of $\mathcal{S}$).

[1] This might be any ideal primitives, in particular E might not be an ideal cipher.

[2] Since we will consider computationally unbounded distinguishers, this is without loss of generality.

For any subset of X of $\mathsf{E}.\mathsf{Dom}$, $\mathcal{D}$ is said X-restricted if it only makes queries to its left oracle (E or $\mathcal{C}^F$) from the set X.

Definition 1 (Restricted-Input Indifferentiability). *Let* E *and* F *be two ideal primitives and* $\mathcal{C}$ *be a construction implementing* E *from* F. *Let* $q, \sigma, t \in \mathbb{N}$ *and* $\varepsilon \in \mathbb{R}^+$. *Let* $\mathcal{X}$ *be a family of subsets of* $\mathsf{E}.\mathsf{Dom}$. *Construction* $\mathcal{C}$ *is said* $(\mathcal{X}, q, \sigma, t, \varepsilon)$*-RI-indifferentiable from* E *if for any* $X \in \mathcal{X}$*, there exists a simulator* $\mathcal{S}$ *such that for any* X*-restricted distinguisher* $\mathcal{D}$ *of total oracle query cost at most* q*,* $\mathcal{S}$ *makes at most* σ *oracle queries, runs in time at most* t*, and*

$$\mathbf{Adv}^{\text{indiff}}_{\mathcal{C},\mathcal{S}}(\mathcal{D}) \leq \varepsilon.$$

Informally, we simply say that $\mathcal{C}$ is $\mathcal{X}$-RI-indifferentiable from E if it is $(\mathcal{X}, q, \sigma, t, \varepsilon)$-RI-indifferentiable for "reasonable" values of σ, t, and ε expressed as functions of q (in particular, when $\mathcal{C}$ is indexed by some security parameter $n \in \mathbb{N}$, if $\sigma, t \in \texttt{poly}(n)$ and $\varepsilon \in \texttt{negl}(n)$ for any $q \in \texttt{poly}(n)$).

As is standard in works on indifferentiability, this definition is information-theoretic, i.e., the distinguisher is allowed to be computationally unbounded (this is sometimes called *statistical indifferentiability*), and demands the existence of a *universal* simulator which does not depend on the distinguisher (this is sometimes called *strong* indifferentiability; when the simulator is allowed to depend on the distinguisher, this is called *weak* indifferentiability).

Note also the following points:

- by letting $\mathcal{X} = \{\mathsf{E}.\mathsf{Dom}\}$ in the definition above, one recovers the standard definition of indifferentiability [22];
- when $\mathcal{X} = \{X\}$ is reduced to a single subset of $\mathsf{E}.\mathsf{Dom}$, the definition is equivalent to the standard definition of indifferentiability of the restriction of $\mathcal{C}^F$ to X from the restriction of E to X; hence this definition is only "new" when considering at least two distinct subsets X and X' such that $X \nsubseteq X'$ and $X' \nsubseteq X$ (since a X-restricted distinguisher is also a X'-restricted distinguisher when $X \subseteq X'$), and can be equivalently rephrased as the indifferentiability of the family of restrictions of $\mathcal{C}$ to sets in $\mathcal{X}$, with a uniform upper bound on the simulator's complexity and the distinguisher's advantage;
- the simulator is allowed to depend on the specific set $X \in \mathcal{X}$ considered;
- the upper bound on the advantage of the distinguisher must hold for any $X \in \mathcal{X}$ (not, say, on average on the random draw of X from $\mathcal{X}$).

The RI version of indifferentiability can be combined with other flavors of indifferentiability, in particular with public indifferentiability [10, 29] and sequential indifferentiability [21, 7]. Let us elaborate for the case of sequential indifferentiability. A distinguisher is called *sequential* if after its first query to its left ($\mathsf{E}/\mathcal{C}^F$) oracle, it does not make any query to its right ($\mathcal{S}^E/F$) oracle any more. In other words, it works in two phases: first it only queries its right oracle, and then only its left oracle. Then we can define *RI-seq-indifferentiability* exactly as in Definition 1, except that we quantify over X-restricted *sequential* distinguishers only. (Hence this is a weaker definition since for each subset $X \in \mathcal{X}$, the simulator has to be effective only against a smaller class of distinguishers, namely sequential ones.)

Composition Theorem. The meaningfulness of the indifferentiability notion comes from the following composition theorem [22]: if a cryptosystem is proven secure when implemented with ideal primitive E, then it remains provably secure when E is replaced with $\mathcal{C}$ based on ideal primitive F, assuming $\mathcal{C}$ is indifferentiable from E. (For this theorem to hold, the security of the cryptosystem must be defined with respect to a class of adversaries which "supports" the simulator used to prove that $\mathcal{C}$ is indifferentiable from E [25, 9].) This theorem straightforwardly translates to $\mathcal{X}$-RI-indifferentiability as follows: if a cryptosystem is proven secure when implemented with ideal primitive E and *if for any adversary $\mathcal{A}$, there is $X \in \mathcal{X}$ such that the challenger of the security game only queries E on inputs $x \in X$ when interacting with $\mathcal{A}$*, then it remains provably secure when E is replaced with $\mathcal{C}$ based on ideal primitive F, assuming $\mathcal{C}$ is $\mathcal{X}$-RI-indifferentiable from E. The short proof is as follows: denote Γ the challenger for the security game, which has access to an instance of E, and fix an adversary $\mathcal{A}$ against the cryptosystem implemented with $\mathcal{C}^F$ (hence $\mathcal{A}$ has oracle access to the instance F of the ideal primitive F); see the combination of Γ and $\mathcal{A}$ as a single X-restricted distinguisher $\mathcal{D}$; by the $\mathcal{X}$-RI-indifferentiability assumption, there is a simulator $\mathcal{S}$ such that $(\mathcal{C}^F, F)$ cannot be distinguished from $(E, \mathcal{S}^E)$; then the combination of $\mathcal{A}$ and $\mathcal{S}$ constitutes an attacker against the cryptosystem implemented with E, and the winning probability of $\mathcal{A}'$ is small by the assumption that the cryptosystem is secure when implemented with E; hence the winning probability of $\mathcal{A}$ is small as well.

Known-Key Indifferentiability. We now explain how to formalize resistance to known-key attacks using RI-indifferentiability. Fix non-empty sets $\mathcal{K}$ and $\mathcal{M}$, and let E be the ideal cipher with key space $\mathcal{K}$ and message space $\mathcal{M}$. Recall that $\mathsf{E.Dom} = \{+,-\} \times \mathcal{K} \times \mathcal{M}$. For any integer $1 \leq \mu \leq |\mathcal{K}|$, let $\mathcal{X}_\mu$ be the family of subsets of $\mathsf{E.Dom}$ consisting of queries whose key is in $\mathcal{K}'$, for $\mathcal{K}'$ ranging over all subsets of $\mathcal{K}$ of size μ; more formally,

$$\mathcal{X}_\mu = \{\{(+,k,x) : k \in \mathcal{K}'\} \cup \{(-,k,y) : k \in \mathcal{K}'\} : \mathcal{K}' \subseteq \mathcal{K}, |\mathcal{K}'| = \mu\}.$$

Note that $\mathcal{X}_{|\mathcal{K}|} = \{\mathsf{E.Dom}\}$.

Definition 2 (μ-Known-Key Indifferentiability). *Let $\mathcal{C}$ be a construction of a block cipher with key space $\mathcal{K}$ and message space $\mathcal{M}$ from an ideal primitive F. Let $\mu, q, \sigma, t \in \mathbb{N}$ and $\varepsilon \in \mathbb{R}^+$. Construction $\mathcal{C}$ is said to be $(\mu, q, \sigma, t, \varepsilon)$-KK-indifferentiable from an ideal cipher if and only if it is $(\mathcal{X}_\mu, q, \sigma, t, \varepsilon)$-RI-indifferentiable from an ideal cipher, with $\mathcal{X}_\mu$ defined as above.*

Unfolding the definition, this is equivalent to the following: for any subset $\mathcal{K}' \subseteq \mathcal{K}$ of size μ, there exists a simulator $\mathcal{S}$ such that for any distinguisher $\mathcal{D}$ whose queries to its first (construction/ideal cipher) oracle use only keys $k \in \mathcal{K}'$ and of total oracle query cost at most q, $\mathcal{S}$ makes at most σ oracle queries, runs in time at most t, and

$$\mathbf{Adv}^{\mathrm{indiff}}_{\mathcal{C},\mathcal{S}}(\mathcal{D}) \leq \varepsilon.$$

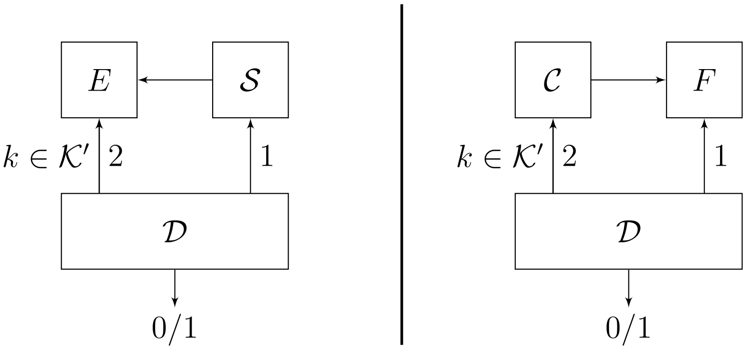

Fig. 2. Various flavors of the indifferentiability notion. For full indifferentiability, the queries of the distinguisher are completely unrestricted. For μ-known-key indifferentiability, queries to the left oracle (ideal cipher/construction) can only be made for keys $k \in \mathcal{K}'$ for some subset $\mathcal{K}'$ of size μ of the key space $\mathcal{K}$ (the simulator being allowed to depend on $\mathcal{K}'$). For sequential indifferentiability, the numbers next to query arrows indicate in which order the distinguisher accesses both oracles. After its first query to the left oracle, the distinguisher cannot query the right oracle any more. Combining the two constraints results in the KK-seq-indifferentiability notion.

The KK-indifferentiability notion of Andreeva *et al.* [2] corresponds to the definition above for $\mu = 1$. In fact, this is slightly more subtle. Their variant is rather an "average" version of this definition over the random draw of the known key, resulting from the following changes: the security experiment starts by drawing a random key k which is given as input to both the distinguisher and the simulator, and the two probabilities involved in the definition (1) of the advantage of the distinguisher are also taken over the random draw of the challenge key $k \leftarrow_\$ \mathcal{K}$. It is not hard to see that our "worst-case" variant of the definition is stronger (i.e., implies) the average-case version (the average-case simulator simply has a copy of each worst-case simulator $\mathcal{S}_{\mathcal{K}'}$ for each possible subset $\mathcal{K}' \subseteq \mathcal{K}$ of size μ, and on input the challenge subset of keys runs the corresponding worst-case simulator).

The standard indifferentiability notion [22] is recovered by letting $\mu = |\mathcal{K}|$ in the definition above. The composition theorem specializes to the case of μ-KK-indifferentiability as follows: if a cryptosystem is proven secure when implemented with an ideal cipher E with key space $\mathcal{K}$ and if for any adversary $\mathcal{A}$, there is a subset of keys $\mathcal{K}'$ of size μ such that the challenger of the security game only queries E with keys $k \in \mathcal{K}'$ when interacting with $\mathcal{A}$, then it remains provably secure when E is replaced with $\mathcal{C}$ based on ideal primitive F, assuming $\mathcal{C}$ is μ-KK-indifferentiable from an ideal cipher.

Known-Key Correlation Intractability. As for the general notion of RI-indifferentiability, KK-indifferentiability can be combined with the notion of sequential indifferentiability. Hence, if we restrict Definition 2 by quantifying only over sequential distinguishers, we obtain the notion of KK-seq-indifferentiability (see also Fig. 2). This notion is interesting because it implies the (arguably more natural) notion of known-key *correlation intractability*, as we explain now.

For this, we first recall the concept of evasive relation and correlation intractability [4, 21, 7]. Let E be an ideal primitive. For an integer $m \geq 1$, an m-ary *relation* $\mathcal{R}$ (for E) is simply a subset $\mathcal{R} \subset (\mathsf{E.Dom})^m \times (\mathsf{E.Rng})^m$. Informally, a relation is *evasive* with respect to E if it is hard, on average, for an adversary with oracle access to a random instance E of E to find a tuple of inputs $(\alpha_1, \ldots, \alpha_m)$ such that $((\alpha_1, \ldots, \alpha_m), (E(\alpha_1), \ldots, E(\alpha_m)))$ satisfies this relation. The definition below is very general and applies to any ideal primitive.

Definition 3 (Evasive Relation). *Let E be an ideal primitive. An m-ary relation $\mathcal{R}$ for E is said (q, ε)-*evasive *if for any adversary $\mathcal{A}$ with oracle access to an instance E of E, making at most q oracle queries, one has*

$$\Pr\Big[E \leftarrow_{\$} \mathsf{E.Inst}, (\alpha_1, \ldots, \alpha_m) \leftarrow \mathcal{A}^E : \\ ((\alpha_1, \ldots, \alpha_m), (E(\alpha_1), \ldots, E(\alpha_m))) \in \mathcal{R}\Big] \leq \varepsilon,$$

where the probability is taken over the random draw of E and the random coins of $\mathcal{A}$.

Recall that the domain and the range of an ideal cipher E with key space $\mathcal{K}$ and message space $\mathcal{M}$ are $\mathsf{E.Dom} = \{+, -\} \times \mathcal{K} \times \mathcal{M}$ and $\mathsf{E.Rng} = \mathcal{M}$ so that, if we particularize the definition above for an ideal cipher, each α_i is a triplet in $\mathsf{E.Dom}$, and $E(\alpha_i) \in \mathcal{M}$.

If we now consider a construction $\mathcal{C}$ implementing E from some other ideal primitive F, a natural thing to ask is that any relation which is evasive with respect to E remains hard to find for $\mathcal{C}^F$, on average over the random draw of F, for any adversary with oracle access to F. This is formalized by the following definition.

Definition 4 (Correlation Intractability). *Let E and F be two ideal primitives, and let $\mathcal{C}$ be a construction implementing E from F. Let $\mathcal{R}$ be an m-ary relation for E. Then $\mathcal{C}$ is said to be (q, ε)-*correlation intractable *with respect to $\mathcal{R}$ if for any adversary $\mathcal{A}$ with oracle access to an instance of F, making at most q oracle queries, one has*

$$\Pr\Big[F \leftarrow_{\$} \mathsf{F.Inst}, (\alpha_1, \ldots, \alpha_m) \leftarrow \mathcal{A}^F : \\ ((\alpha_1, \ldots, \alpha_m), (\mathcal{C}^F(\alpha_1), \ldots, \mathcal{C}^F(\alpha_m))) \in \mathcal{R}\Big] \leq \varepsilon,$$

where the probability is taken over the random draw of F and the random coins of $\mathcal{A}$.

A theorem by Mandal *et al.* [21] (see also [7, Theorem 4]) establishes that seq-indifferentiability allows, for any relation $\mathcal{R}$, to "reduce" the correlation intractability of $\mathcal{C}$ with respect to $\mathcal{R}$ to the evasiveness of $\mathcal{R}$ (with respect to

E). More precisely, if $\mathcal{C}$ is seq-indifferentiable from E and if a relation $\mathcal{R}$ is (q,ε)-evasive with respect to E, then $\mathcal{C}$ is (q',ε')-correlation intractable with respect to $\mathcal{R}$, and the "degradation" of security parameters (q',ε') compared with (q,ε) depends on the seq-indifferentiability parameters. In other words, if $\mathcal{C}$ is seq-indifferentiable from E, then any relation which is hard to find for E remains hard to find for $\mathcal{C}^F$ (on average over the random draw of F).

This result can be straightforwardly declined for the case of KK-seq-indifferentiability (and more generally RI-seq-indifferentiability): if $\mathcal{C}$ is $\mathcal{X}$-RI-seq-indifferentiable from E for some family $\mathcal{X}$ of subsets of $\mathsf{E.Dom}$, then a similar result holds, but only for relations $\mathcal{R}$ such that all inputs involved in $\mathcal{R}$ belong to some subset $X \in \mathcal{X}$; similarly, if $\mathcal{C}$ is μ-KK-seq-indifferentiable from an ideal cipher E with key space $\mathcal{K}$, then the result holds for relations $\mathcal{R}$ such that all inputs involved in $\mathcal{R}$ use the same μ keys.

Concretely we have the following theorem. The proof is similar to the proof of [7, Theorem 4] and therefore deferred to the full version of the paper [8]. First we give two preliminary definitions. Let E be an ideal primitive, and X be a subset of $\mathsf{E.Dom}$; then an m-ary relation $\mathcal{R}$ for E is said X-restricted if

$$\forall((\alpha_1,\ldots,\alpha_m),(\beta_1,\ldots,\beta_m)) \in \mathcal{R},\ \forall i=1,\ldots,m,\ \alpha_i \in X.$$

Similarly, let E be an ideal cipher with key space $\mathcal{K}$, and $\mu \geq 1$; then an m-ary relation $\mathcal{R}$ for E is said μ-restricted if there exists a subset $\mathcal{K}'$ of $\mathcal{K}$ of size μ such that

$$\forall((\delta_i,k_i,z_i),\ldots,(\delta_m,k_m,z_m)),(z'_1,\ldots,z'_m)) \in \mathcal{R},\ \forall i=1,\ldots,m,\ k_i \in \mathcal{K}'.$$

Theorem 1. *Let E and F be two ideal primitives, and let $\mathcal{C}$ be a construction implementing E from F such that $\mathcal{C}$ makes at most c queries to its oracle on any input. Let $\mathcal{X}$ be a family of subsets of $\mathsf{E.Dom}$. Assume that $\mathcal{C}$ is $(\mathcal{X},q+cm,\sigma,t,\varepsilon)$-RI-seq-indifferentiable from E. Then for any m-ary relation $\mathcal{R}$ which is X-restricted for some $X \in \mathcal{X}$, if $\mathcal{R}$ is $(\sigma+m,\varepsilon_{\mathcal{R}})$-evasive with respect to E, then $\mathcal{C}$ is $(q,\varepsilon+\varepsilon_{\mathcal{R}})$-correlation intractable with respect to $\mathcal{R}$.*

In particular, let E be an ideal cipher with key space $\mathcal{K}$, and assume that $\mathcal{C}$ is $(\mu,q+cm,\sigma,t,\varepsilon)$-KK-seq-indifferentiable from E. Then for any μ-restricted m-ary relation $\mathcal{R}$, if $\mathcal{R}$ is $(\sigma+m,\varepsilon_{\mathcal{R}})$-evasive with respect to E, then $\mathcal{C}$ is $(q,\varepsilon+\varepsilon_{\mathcal{R}})$-correlation intractable with respect to $\mathcal{R}$.

Remark 1. We need to dispel some confusion that might be created by the following observation (this will also help illustrate all definitions above with a concrete example): Lampe and Seurin [20] have exhibited an attacker against the 3-round IEM construction which, given oracle access to the inner permutations, finds four tuples (k_i,x_i,y_i), $i=1,\ldots,4$, satisfying the following evasive relation:

$$\begin{cases} k_1 \oplus k_2 \oplus k_3 \oplus k_4 = 0 \\ x_1 \oplus x_2 \oplus x_3 \oplus x_4 = 0 \\ y_1 \oplus y_2 \oplus y_3 \oplus y_4 = 0. \end{cases}$$

Since we will later prove that the 3-round IEM construction is μ-KK-seq-indifferentiable from an ideal cipher for any polynomial μ, this might seem contradictory with Theorem 1. The catch is that two of the four keys involved in the relation and obtained at the end of the attack are not controlled by the adversary and in fact range over the entire key space when the inner permutations range over $\mathsf{Perm}(n)$. Hence, the evasive relation actually involves keys from the entire key space (not just a small subset of it).

4 KK-Attack on the Two-Round IEM Construction

We explained in Section 1 that the 1-round EM construction is not resistant to μ-known-key attacks for $\mu \geq 2$. We show here that this extends to the 2-round IEM construction (with independent inner permutations and the trivial key-schedule), more formally, that this construction is not μ-KK-seq-indifferentiable from an ideal cipher for $\mu \geq 2$. Our attack shares some similarities with the related-key attack against the same construction of [7]. Formally, we prove the following theorem.

Theorem 2. *The 2-round IEM construction* $\mathsf{EM}[n, 2, \mathbf{f}]$ *with independent inner permutations and the trivial key schedule*[3] $\mathbf{f}$ *is not* 2*-KK-seq-indifferentiable from an ideal cipher. More precisely, for any pair of distinct keys* (k_1, k_2)*, there is an adversary which distinguishes the construction from an ideal cipher with advantage close to 1 by making only queries to its left (construction/ideal cipher) oracle involving these two keys. The adversary makes no queries to its right (inner permutations/simulator) oracle.*

Proof. We denote generically (E, F) the oracles to which the adversary has access and (k_1, k_2) two distinct keys the attacker is allowed to use. Consider the following distinguisher (see Fig. 3 for a diagram of the attack):

(1) choose an arbitrary value $x_1 \in \{0, 1\}^n$, and query $y_1 := E(+, k_1, x_1)$;
(2) compute $x_2 := x_1 \oplus k_2 \oplus k_1$, and query $y_2 := E(+, k_2, x_2)$;
(3) compute $y_3 := y_1 \oplus k_1 \oplus k_2$, and query $x_3 := E(-, k_2, y_3)$;
(4) compute $y_4 := y_2 \oplus k_2 \oplus k_1$, and query $x_4 := E(-, k_1, y_4)$;
(5) check whether $x_4 = x_3 \oplus k_1 \oplus k_2$.

When the distinguisher is interacting with an ideal cipher E, two cases can occur. Either $y_4 = y_1$, or $y_4 \neq y_1$. In the first case, this means that $y_1 \oplus y_2 = k_1 \oplus k_2$, which happens with probability 2^{-n} since x_1 and x_2 are the first queries to the uniformly random and independent permutations E_{k_1} and E_{k_2}. If $y_4 \neq y_1$, then y_4 is the second query to the uniformly random permutation E_{k_1}, thus x_4 is uniformly random and this equality happens with probability at most $1/(2^n - 1)$. Moreover one has $y_2 \neq y_1 \oplus k_1 \oplus k_2$ which happens with probability $1 - 2^{-n}$ since x_2 is the first query to E_{k_2}. Since E is a uniformly randomly drawn blockcipher, E_{k_1} and E_{k_2} are independent permutations and this case happens with probability at most 2^{-n}. Overall, when E is an ideal cipher, this relation is satisfied with a probability at most 2^{n-1}.

[3] In fact, the attack applies whenever the key-schedule is linear.

Now we show that when the distinguisher is interacting with the two round Even-Mansour construction, it always returns 1, independently of k, and the inner permutations, which we denote P_1 and P_2. Noting that, by definition, $x_2 = x_1 \oplus k_2 \oplus k_1$, we denote u_1 the common value

$$u_1 \overset{\text{def}}{=} x_1 \oplus k_1 = x_2 \oplus k_2,$$

and we denote $v_1 = P_1(u_1)$. We also denote

$$\begin{aligned} u_2 &= v_1 \oplus k_1 && (2) \\ v_2 &= P_2(u_2) \\ u_2' &= v_1 \oplus k_2 && (3) \\ v_2' &= P_2(u_2'). \end{aligned}$$

Hence, one has

$$\begin{aligned} y_1 &= v_2 \oplus k_1 && (4) \\ y_2 &= v_2' \oplus k_2. && (5) \end{aligned}$$

Since $y_3 = y_1 \oplus k_1 \oplus k_2$, we can see, using (4), that

$$y_3 \oplus k_2 = y_1 \oplus k_1 = v_2.$$

Define

$$\begin{aligned} v_1' &= u_2 \oplus k_2 && (6) \\ u_1' &= P_1^{-1}(v_1'). \end{aligned}$$

This implies that

$$x_3 = u_1' \oplus k_2. \tag{7}$$

Since $y_4 = y_2 \oplus k_2 \oplus k_1$, we see by (5) that

$$y_4 \oplus k_1 = y_2 \oplus k_2 = v_2'.$$

Moreover, we have

$$\begin{aligned} u_2' \oplus k_1 &= u_2' \oplus k_2 \oplus k_1 \oplus k_2 \\ &= v_1 \oplus k_1 \oplus k_2 && \text{by (3)} \\ &= u_2 \oplus k_2 && \text{by (2)} \\ &= v_1' && \text{by (6).} \end{aligned}$$

This finally implies by (7) that

$$x_4 \oplus k_1 = u_1' = x_3 \oplus k_2,$$

which concludes the proof. □

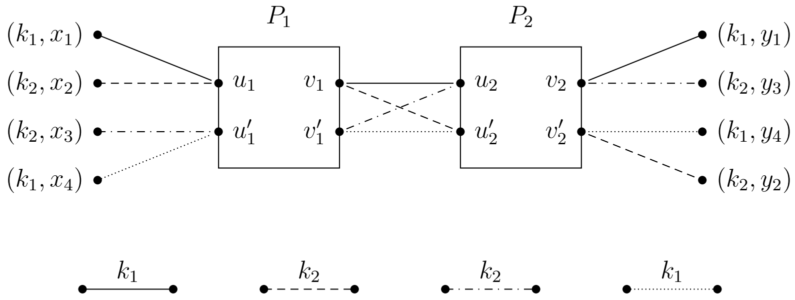

Fig. 3. A 2-known-key attack on the iterated Even-Mansour cipher with two rounds and the trivial key-schedule.

5 KK-Seq-Indifferentiability for Three Rounds

We have just given a 2-known-keys attack against the 2-round IEM cipher. This implies that the 2-round IEM construction cannot be μ-KK-seq-indifferentiable from an ideal cipher as soon as $\mu \geq 2$. (Remember on the other hand that the 1-round EM construction is 1-KK-indifferentiable from an ideal cipher [2].) Hence, at least three rounds are necessary (and, as we will see now, sufficient) to achieve μ-KK-seq-indifferentiability from an ideal cipher for $\mu \geq 2$.

Concretely, the main result of this section regarding the KK-seq-indifferentiability of the 3-round IEM cipher is as follows.

Theorem 3. *Let $N = 2^n$. For any integers μ and q such that $\mu q \leq N/4$, the 3-round IEM construction $\mathsf{EM}[n, 3, \mathbf{f}]$ with independent permutations and the trivial key-schedule $\mathbf{f}$ is $(\mu, q, \sigma, t, \varepsilon)$-KK-seq-indifferentiable from an ideal cipher with n-bit blocks and n-bit keys, with*

$$\sigma = \mu q, \quad t = \mathcal{O}(\mu q), \quad \textit{and} \quad \varepsilon = \frac{57\mu^2 q^2}{N}.$$

As a corollary, we obtain from Theorem 1 that for any m-ary relation $\mathcal{R}$ which is μ-restricted and $(\mu q, \varepsilon)$-evasive w.r.t. an ideal cipher (and assuming q is large compared with $c = 3$ and m), the 3-round IEM cipher is $\left(q, \varepsilon + \mathcal{O}\left(\mu^2 q^2 / 2^n\right)\right)$-correlation intractable with respect to $\mathcal{R}$.

It is also known [21] that for stateless ideal primitives (i.e., primitives whose answers do not depend on the order of the queries it receives), seq-indifferentiability implies public indifferentiability [29, 10], a variant of indifferentiability where the simulator gets to know all queries of the distinguisher to the ideal primitive E. Since an ideal cipher is stateless, Theorem 3 implies that the 3-round IEM construction is also KK-publicly indifferentiable from an ideal cipher.

Proof Idea. The proof of Theorem 3 is very similar to the proof of (full, not KK) seq-indifferentiability for the 4-round IEM construction of [7]. The main difference

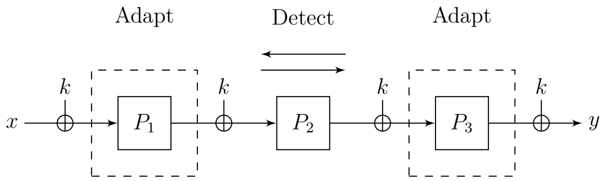

Fig. 4. Detection and adaptations zones used by the simulator for proving KK-seq-indifferentiability of the 3-round iterated Even-Mansour construction from an ideal cipher.

in the simulation strategy is the following: in the full seq-indifferentiability setting, the simulator has no hint about which key(s) the adversary is using to try to distinguish the real world from the ideal (simulated) world. Hence, it uses a 2-round "detection" zone in the middle made of permutations P_2 and P_3, which allows, given a query to P_2 (say, $P_2(u_2) = v_2$) and a query to P_3 (say, $P_3(u_3) = v_3$), to deduce the key associated to this "chain" of queries (namely, $k = v_2 \oplus u_3$). Permutations P_1 and P_4 are then used to "adapt" these detected chains and make them match the ideal cipher E. In the KK-setting, the simulator knows the set $\mathcal{K}'$ of keys that the distinguisher is allowed to use in its ideal cipher queries. Hence, the detection zone can be reduced to one single round (the middle one, i.e. P_2 for the 3-round IEM): each time the distinguisher makes a query to P_2, the simulator completes the μ chains corresponding to this query and *each key* $k \in \mathcal{K}'$, again using extremal round P_1 and P_3 to adapt the chains (see Fig. 4).

We only give an informal description of the simulator here and defer the formal description in pseudocode and the full proof of Theorem 3 to the full version of the paper [8]. The simulator is given the subset $\mathcal{K}'$ of keys that the distinguisher is bound to use. It offers an interface $\mathsf{Query}(i, \delta, w)$ to the distinguisher for querying the internal permutations, where $i \in \{1, 2, 3\}$ names the permutation, $\delta \in \{+, -\}$ indicates whether this a direct or inverse query, and $w \in \{0,1\}^n$ is the actual value queried. For each $i = 1, \ldots, 3$, the simulator internally maintains a table Π_i reflecting which values have been already internally set for each simulated permutation. Each table maps entries $(\delta, w) \in \{+,-\} \times \{0,1\}^n$ to values $w' \in \{0,1\}^n$, initially undefined for all entries. We denote Π_i^+, resp. Π_i^-, the (time-dependent) sets of strings $w \in \{0,1\}^n$ such that $\Pi_i(+, w)$, resp. $\Pi_i(-, w)$, is defined. When the simulator receives a query (i, δ, w), it checks in table Π_i whether the corresponding answer $\Pi_i(\delta, w)$ is already defined. When this is the case, it returns the answer to the distinguisher and waits for the next query. Otherwise, it randomly draws an answer $w' \in \{0,1\}^n$ and defines $\Pi_i(\delta, w) := w'$ as well as the answer to the opposite query $\Pi_i(\overline{\delta}, w') := w$. The randomness used by the simulator is made explicit through a tuple of random permutations $\mathbf{P} = (P_1, P_2, P_3)$ with $P_i := \{+,-\} \times \{0,1\}^n \to \{0,1\}^n$, and for any $u, v \in \{0,1\}^n$, $P_i(+, u) = v \Leftrightarrow P_i(-, v) = u$. We assume that the tuple (P_1, P_2, P_3) is drawn uniformly at random at the beginning of the experiment, but we note that $\mathcal{S}$

could equivalently lazily sample these permutations throughout its execution. Then w' is simply defined by the simulator as $w' := P_i(\delta, w)$.[4]

Before returning w' to the distinguisher, the simulator takes additional steps to ensure that the whole IEM construction matches the ideal cipher E by running a *chain completion* mechanism. Namely, if the distinguisher called $\mathsf{Query}(i, \delta, w)$ with $i = 2$, the simulator completes the "chains" for each known key $k \in \mathcal{K}'$ by executing a procedure $\mathsf{CompleteChain}(u_2, v_2, k, \ell)$, where ℓ indicates where the chain will be "adapted" and (u_2, v_2) is the pair of values that was just added to Π_2. For example, assume that the distinguisher called $\mathsf{Query}(2, +, u_2)$ and that the answer randomly chosen by the simulator was v_2. Then for each $k \in \mathcal{K}'$, the simulator computes the corresponding value $u_3 = v_2 \oplus k$, and evaluates the IEM construction backward, letting $v_1 := u_2 \oplus k$, $u_1 := \Pi_1(-, v_1)$ (setting this value at random in case it was not in Π_1), $x := u_1 \oplus k$, $y := E(+, k, x)$ (hence making a query to E to "wrap around"), and $v_3 := y \oplus k$, until the corresponding input/output values (u_3, v_3) for the third permutation are defined. It then "adapts" (rather than setting randomly) table Π_3 by calling procedure $\mathsf{ForceVal}(u_3, v_3, 3)$ which sets $\Pi_3(+, u_3) := v_3$ and $\Pi_3(-, v_3) := u_3$ in order to ensure consistency of the simulated IEM construction with E. (A crucial point of the proof will be to show that this does not cause an overwrite, i.e., that these two values are undefined before the adaptation occurs.) In case the query was to $\mathsf{Query}(2, -, \cdot)$, the behavior of the simulator is symmetric, namely adaptation of the chain takes place in table Π_1.

6 KK-indifferentiability for Nine Rounds

In this section, we show that nine rounds of the IEM construction are sufficient to achieve μ-KK-indifferentiability from an ideal cipher. Note that this is less than what is currently known to be sufficient to achieve full indifferentiability from an ideal cipher, namely twelve rounds, as shown by Lampe and Seurin [20]. We conjecture that four rounds are actually sufficient.

We use the same technique as in Section 5 for going from four rounds for seq-indifferentiability to three rounds for KK-seq-indifferentiability: we start from the 12-round simulator of [20], and shorten the detection zones using the fact that the simulator knows the subset of keys used by the distinguisher.

We only give an informal description of the simulator and sketch how to modify the indifferentiability proof of [20], so that the result should rather be considered as a (substantiated) conjecture. (Given that nine is unlikely to be the minimal number of rounds needed to achieve μ-KK-indifferentiability, and that we already known that twelve rounds are sufficient to achieve full indifferentiability and hence μ-KK-indifferentiability, the benefit of writing down the full proof is rather low.) The high-level principle of how the simulator works is similar to

[4] Note that for $i = 1$ and $i = 3$, this is not equivalent to letting $w' \leftarrow_{\$} \{0,1\}^n \setminus \Pi_i^{\bar{\delta}}$ since the simulator sometimes "adapts" the value of these tables, so that the tables Π_i and the permutations P_i will differ (with overwhelming probability) on adapted entries.

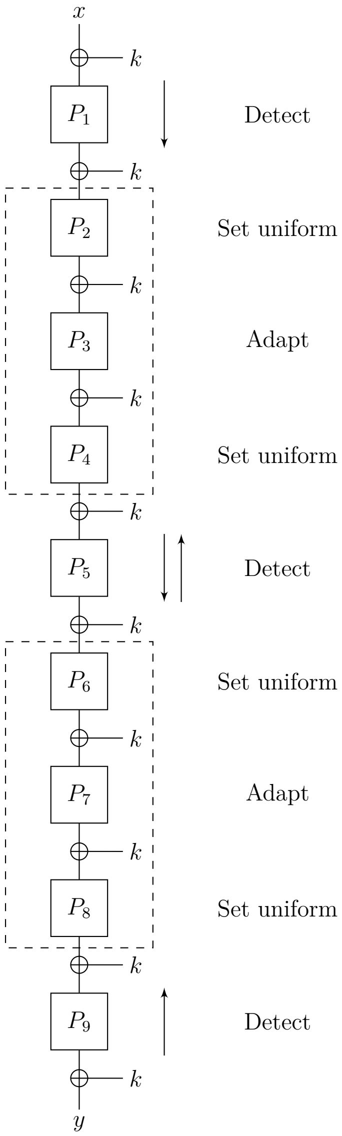

Fig. 5. Detection and adaptation zones used by the simulator for proving KK-indifferentiability of the 9-round iterated Even-Mansour construction from an ideal cipher.

Section 5 except that there are now additional detection zones besides the middle one preventing the distinguisher from creating "wrap around" chains (remember that the distinguisher is not bound to be sequential here, so it can make an ideal cipher query $y := E(+, k, x)$ and evaluate the IEM construction from both extremities by making permutation queries until the simulator is trapped into a contradiction). Moreover, since the simulator can now recurse (i.e., completing a chain can create new chains to be completed), it uses a queue of chains detected and to be completed as in [20].

As before, the simulator reacts on any query to P_5, and completes the chains for any key $k \in \mathcal{K}'$ by adapting at P_7 if this is a direct query and adapting at P_3 if this is an inverse query. Moreover, the simulator also reacts on direct queries to P_1 or inverse queries to P_9. Let us consider the case of a query $P_1(+, u_1)$. Then for each key $k \in \mathcal{K}'$, the simulator computes $x := u_1 \oplus k$, queries $y := E(+, k, x)$, lets $v_9 := y \oplus k$, and checks if $v_9 \in \mathit{\Pi}_9^-$. If this is the case, then the chain (u_1, k) is enqueued to be completed and adapted at P_3. For an inverse query to P_9, adaptation takes place at P_7. As in [20], the four "buffer" rounds P_2, P_4, P_6 and P_8 surrounding adaptation rounds ensure that no collision can occur when adapting distinct chains.

The analysis of this simulator then follows the same lines as in [20]. Its complexity can be upper bounded as follows: first, one applies the standard argument that the number of wrap-around chains that will be detected is upper bounded (with very high probability) by the number of ideal cipher queries of the distinguisher, hence by q. This implies that the size of table $\mathit{\Pi}_5$ is always at most $2q$ (since it increases only because of a distinguisher's query or when completing a wrap-around chain). It follows that the number of middle chains completed is at most $2\mu q$, and the size of all tables $\mathit{\Pi}_i$ for $i \neq 5$ is at most $q + q + 2\mu q = 2(\mu + 1)q$. Also, the number of calls made by the simulator to the ideal cipher can be upper bounded by $2\mu q$ (number of middle chains that are completed), plus $4\mu(\mu + 1)q$ (number of wrap-around chains that are checked), hence it is $O(\mu^2 q)$ (the running time is similar).

Finally, proving a rigorous upper bound on the distinguishing advantage is a cumbersome task that remains to be done. A rough estimation following the lines of [20] would be that bad events that would make the simulator to overwrite a value when adapting chains (which is what dominates the security bound) happen with probability at most $(\max |\mathit{\Pi}_i|)^6/2^n$, hence $O(\mu^6 q^6)$.

References

[1] E. Andreeva, A. Bogdanov, Y. Dodis, B. Mennink, and J. P. Steinberger. On the Indifferentiability of Key-Alternating Ciphers. In *Advances in Cryptology - CRYPTO 2013 (Proceedings, Part I)*, volume 8042 of *LNCS*, pages 531–550. Springer, 2013. Full version available at http://eprint.iacr.org/2013/061.

[2] E. Andreeva, A. Bogdanov, and B. Mennink. Towards Understanding the Known-Key Security of Block Ciphers. In *Fast Software Encryption - FSE 2013*, volume 8424 of *LNCS*, pages 348–366. Springer, 2013.

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

[4] R. Canetti, O. Goldreich, and S. Halevi. The Random Oracle Methodology, Revisited (Preliminary Version). In *Symposium on Theory of Computing - STOC '98*, pages 209–218. ACM, 1998. Full version available at http://arxiv.org/abs/cs.CR/0010019.

[5] S. Chen, R. Lampe, J. Lee, Y. Seurin, and J. P. Steinberger. Minimizing the Two-Round Even-Mansour Cipher. In *Advances in Cryptology - CRYPTO 2014 (Proceedings, Part I)*, volume 8616 of *LNCS*, pages 39–56. Springer, 2014. Full version available at http://eprint.iacr.org/2014/443.

[6] S. Chen and J. Steinberger. Tight Security Bounds for Key-Alternating Ciphers. In *Advances in Cryptology - EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 327–350. Springer, 2014. Full version available at http://eprint.iacr.org/2013/222.

[7] B. Cogliati and Y. Seurin. On the Provable Security of the Iterated Even-Mansour Cipher against Related-Key and Chosen-Key Attacks. In *Advances in Cryptology - EUROCRYPT 2015 (Proceedings, Part I)*, volume 9056 of *LNCS*, pages 584–613. Springer, 2015. Full version available at http://eprint.iacr.org/2015/069.

[8] B. Cogliati and Y. Seurin. Strengthening the Known-Key Security Notion for Block Ciphers. Full version of this paper. Available at http://eprint.iacr.org/2016/394.

[9] G. Demay, P. Gazi, M. Hirt, and U. Maurer. Resource-Restricted Indifferentiability. In *Advances in Cryptology - EUROCRYPT 2013*, volume 7881 of *LNCS*, pages 664–683. Springer, 2013. Full version available at http://eprint.iacr.org/2012/613.

[10] Y. Dodis, T. Ristenpart, and T. Shrimpton. Salvaging Merkle-Damgård for Practical Applications. In *Advances in Cryptology - EUROCRYPT 2009*, volume 5479 of *LNCS*, pages 371–388. Springer, 2009.

[11] O. Dunkelman, N. Keller, and A. Shamir. Minimalism in Cryptography: The Even-Mansour Scheme Revisited. In *Advances in Cryptology - EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 336–354. Springer, 2012.

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

[13] P. Farshim and G. Procter. The Related-Key Security of Iterated Even-Mansour Ciphers. In *Fast Software Encryption - FSE 2015*, volume 9054 of *LNCS*, pages 342–363. Springer, 2015. Full version available at http://eprint.iacr.org/2014/953.

[14] H. Gilbert. A Simplified Representation of AES. In *Advances in Cryptology - ASIACRYPT 2014 (Proceedings, Part I)*, volume 8873 of *LNCS*, pages 200–222. Springer, 2014.

[15] H. Gilbert and T. Peyrin. Super-Sbox Cryptanalysis: Improved Attacks for AES-Like Permutations. In *Fast Software Encryption - FSE 2010*, volume 6147 of *LNCS*, pages 365–383. Springer, 2010.

[16] C. Guo and D. Lin. A Synthetic Indifferentiability Analysis of Interleaved Double-Key Even-Mansour Ciphers. In *Advances in Cryptology - ASIACRYPT 2015 (Proceedings, Part II)*, volume 9453 of *LNCS*, pages 389–410. Springer, 2015.

[17] C. Guo and D. Lin. On the Indifferentiability of Key-Alternating Feistel Ciphers with No Key Derivation. In *Theory of Cryptography - TCC 2015 (Proceedings, Part I)*, volume 9014 of *LNCS*, pages 110–133. Springer, 2015.

[18] L. R. Knudsen and V. Rijmen. Known-Key Distinguishers for Some Block Ciphers. In *Advances in Cryptology - ASIACRYPT 2007*, volume 4833 of *LNCS*, pages 315–324. Springer, 2007.

[19] R. Lampe, J. Patarin, and Y. Seurin. An Asymptotically Tight Security Analysis of the Iterated Even-Mansour Cipher. In *Advances in Cryptology - ASIACRYPT 2012*, volume 7658 of *LNCS*, pages 278–295. Springer, 2012.

[20] R. Lampe and Y. Seurin. How to Construct an Ideal Cipher from a Small Set of Public Permutations. In *Advances in Cryptology - ASIACRYPT 2013 (Proceedings, Part I)*, volume 8269 of *LNCS*, pages 444–463. Springer, 2013. Full version available at http://eprint.iacr.org/2013/255.

[21] A. Mandal, J. Patarin, and Y. Seurin. On the Public Indifferentiability and Correlation Intractability of the 6-Round Feistel Construction. In *Theory of Cryptography Conference - TCC 2012*, volume 7194 of *LNCS*, pages 285–302. Springer, 2012. Full version available at http://eprint.iacr.org/2011/496.

[22] U. M. Maurer, R. Renner, and C. Holenstein. Indifferentiability, Impossibility Results on Reductions, and Applications to the Random Oracle Methodology. In *Theory of Cryptography Conference- TCC 2004*, volume 2951 of *LNCS*, pages 21–39. Springer, 2004.

[23] M. Minier, R. C.-W. Phan, and B. Pousse. Distinguishers for Ciphers and Known Key Attack against Rijndael with Large Blocks. In *Progress in Cryptology - AFRICACRYPT 2009*, volume 5580 of *LNCS*, pages 60–76. Springer, 2009.

[24] I. Nikolic, J. Pieprzyk, P. Sokolowski, and R. Steinfeld. Known and Chosen Key Differential Distinguishers for Block Ciphers. In *Information Security and Cryptology - ICISC 2010*, volume 6829 of *LNCS*, pages 29–48. Springer, 2010.

[25] T. Ristenpart, H. Shacham, and T. Shrimpton. Careful with Composition: Limitations of the Indifferentiability Framework. In *Advances in Cryptology - EUROCRYPT 2011*, volume 6632 of *LNCS*, pages 487–506. Springer, 2011.

[26] P. Rogaway and J. P. Steinberger. Constructing Cryptographic Hash Functions from Fixed-Key Blockciphers. In *Advances in Cryptology - CRYPTO 2008*, volume 5157 of *LNCS*, pages 433–450. Springer, 2008.

[27] P. Rogaway and J. P. Steinberger. Security/Efficiency Tradeoffs for Permutation-Based Hashing. In *Advances in Cryptology - EUROCRYPT 2008*, volume 4965 of *LNCS*, pages 220–236. Springer, 2008.

[28] Y. Sasaki and K. Yasuda. Known-Key Distinguishers on 11-Round Feistel and Collision Attacks on Its Hashing Modes. In *Fast Software Encryption - FSE 2011*, volume 6733 of *LNCS*, pages 397–415. Springer, 2011.

[29] K. Yoneyama, S. Miyagawa, and K. Ohta. Leaky Random Oracle. *IEICE Transactions*, 92-A(8):1795–1807, 2009.