Cryptanalysis of Iterated Even-Mansour Schemes with Two Keys

Itai Dinur[1,⋆], Orr Dunkelman[2,3,⋆⋆], Nathan Keller[3,4,⋆⋆⋆], and Adi Shamir[3]

[1] Computer Science Department, Technion - Israel Institute of Technology, Haifa, Israel
[2] Département d'Informatique, École Normale Supérieure, Paris, France
[3] Computer Science Department, University of Haifa, Israel
[4] Computer Science department, The Weizmann Institute, Rehovot, Israel
[5] Department of Mathematics, Bar-Ilan University, Israel

Abstract. The iterated Even-Mansour (EM) scheme is a generalization of the original 1-round construction proposed in 1991, and can use one key, two keys, or completely independent keys. In this paper, we methodically analyze the security of all the possible iterated Even-Mansour schemes with two n-bit keys and up to four rounds, and show that none of them provides more than n-bit security. Our attacks are based on a new cryptanalytic technique called *multibridge* which splits the cipher to different parts in a novel way, such that they can be analyzed independently, exploiting its self-similarity properties. After the analysis of the parts, the key suggestions are efficiently joined using a meet-in-the-middle procedure.

As a demonstration of the multibridge technique, we devise a new attack on 4 steps of the LED-128 block cipher, reducing the time complexity of the best known attack on this scheme from 2^{96} to 2^{64}. Furthermore, we show that our technique can be used as a generic key-recovery tool, when combined with some statistical distinguishers (like those recently constructed in reflection cryptanalysis of GOST and PRINCE).

Keywords: Cryptanalysis, meet-in-the-middle attacks, iterated Even-Mansour, LED-128.

1 Introduction

Most block ciphers (such as the AES) have an iterated structure which alternately XOR's a secret key and applies some publicly known permutation (typically consisting of S-boxes and linear transformations) to the internal state. A generic way to describe such a scheme is to assume that the permutations are randomly chosen, with no weaknesses which can be exploited by the cryptanalyst.

⋆ Some of the work presented in this paper was done while the first author was a postdoctoral researcher at the Weizmann Institute, Israel.

⋆⋆ The second author was supported in part by the German-Israeli Foundation for Scientific Research and Development through grant No. 2282-2222.6/2011.

⋆⋆⋆ The third author was supported by the Alon Fellowship.

This approach has several advantages: First of all, this is a very clean construction with great theoretical appeal. In addition, we can use the randomness of the permutation in order to prove lower bounds on the complexity of all possible attacks, something we cannot hope to achieve when we instantiate the scheme with a particular choice of the permutation. Finally, any new generic attack on block ciphers with this general form can have broad practical applicability.

At Asiacrypt 1991 [10], Even and Mansour defined and analyzed the simplest example of such a block cipher, which consists of a single public permutation and two independently chosen secret keys XOR'ed before and after the permutation. We call such a scheme a 1-round 2-key Even-Mansour (EM) scheme. In their paper, Even and Mansour showed that in any attack on this scheme, $TD \geq 2^n$. This implies that any attack on the scheme has overall complexity (i.e., the maximal complexity among the time,[1] memory and data complexities) of at least $2^{n/2}$. In such a case, we say that the *security* of the scheme is $2^{n/2}$, or $n/2$ bits.[2] At Eurocrypt 2012 [9], a matching upper bound in the known plaintext attack model was proved, and thus the security of this scheme is now fully understood.

Since the security provided by a 1-round 2-key EM is much smaller than the 2^{2n} time complexity of exhaustive key search, multiple papers published in the last couple of years had studied the security of iterated EM schemes with more than one round (e.g., [2, 4, 8, 17, 20, 22]). These schemes differ not only in their number of rounds, but also in the number of keys they use and in the order in which these keys are used in the various rounds. This is somewhat analogous to the study of the security of generic Feistel structures with various numbers of rounds, which led to several fundamental results in theoretical cryptography in the last two decades (e.g., how to construct pseudo-random permutations from pseudo-random functions, and how many queries are required in order to distinguish them from truly random permutations [18, 23]).

In this paper, we study the security of iterated EM constructions using two independent keys. As the security of the 1-round variant is already determined to be $2^{n/2}$, and as it is easy to see that a 2-round variant supplies security of at most 2^n, we analyze all 3-round and 4-round variants with two keys. We show that for any possible ordering of the two keys, all the r-round variants with $r \leq 4$ provide security of at most 2^n (compared to exhaustive key search which requires 2^{2n} time). Furthermore, for all such variants[3] we obtain a complete tradeoff curve of $DT = 2^{2n}$ in the known plaintext attack model.

Since several concrete proposals for block ciphers use a relatively small number of fairly complex rounds, our theoretical analysis has immediate practical

[1] We define security in the computational model, which calculates the time complexity according to the number of operations that the attacker performs. This model is different from the information theoretical model (used, for example, in [4]), which only considers the number of queries to the internal permutations of the primitive.

[2] Note that, unlike the tradeoff attacks described in Hellman's paper [13], the overall complexity of an attack takes into account all attack stages. In particular, we do not allow any free preprocessing stage.

[3] Not including some weak variants, for which an attack of time complexity 2^n can be obtained given only 2 plaintext-ciphertext pairs (i.e., the unicity bound).

applications. For example, we can use our results in order to compare the best achievable security of schemes with various numbers of rounds and key schedules, and thus to guide the design of future schemes. More surprisingly, we can use our new generic attacks in order to improve by a large margin the running time of the best known attacks on the extensively studied lightweight block cipher LED-128, without even looking at its internal details.

LED-128 [12] is a typical example of an iterated EM scheme. It is a 64-bit block cipher that uses two unrelated 64-bit keys, which are alternately XOR'ed in consecutive rounds. Since its publication at CHES 2011, reduced variants of LED-128 have been extensively analyzed, and in particular the 4-step[4] variant (reduced from the full 12) was analyzed in 3 consecutive papers at ACISP 2012 [15], Asiacrypt 2012 [20] and FSE 2013 [22], using a variety of cryptanalytic techniques (see Table 1).

Table 1. Attacks on 4-Step LED-128

Reference	Generic†	Data††	Time	Memory	**Security**
[15]	No	2^{16} CP	2^{112}	2^{16}	2^{112}
[20]	Yes	2^{64} KP	2^{96}	2^{64}	2^{96}
[22]	Yes	$D \leq 2^{32}$ KP	$2^{128}/D$	D	2^{96}
This paper	Yes	$D \leq 2^{64}$ KP	$2^{128}/D$	D	2^{64}

† "Generic" stands for an attack independent of the actual step function.

†† The data complexity is given in chosen plaintexts (CP), or in known plaintexts (KP).

The first attack on 4-step LED-128 is described in [15]. The attack combines the splice-and-cut technique [3] with a meet-in-the-middle attack which is based on specific properties of the LED permutation. It has a time complexity of $T = 2^{112}$, and requires $D = 2^{16}$ chosen plaintext-ciphertext pairs. The second analysis of 4-step LED-128 is given in [20] and is applicable to all 4-round EM schemes with 2 alternating keys. When applied to 4-step LED-128, it has a reduced time complexity of $T = 2^{96}$ (compared to $T = 2^{112}$ of the attack of [15]), but it requires the full code-book of $D = 2^{64}$ plaintext-ciphertext pairs. The attack uses a technique related to Merkle and Hellman's attack on two-key triple-DES (2K3DES) [21], in combination with Daemen's chosen plaintext attack of EM [6]. Finally, the currently best known attack on 4-step LED-128 is a known plaintext attack given in [22]. The attack uses an extension of the SlideX attack [9] in order to obtain a flexible tradeoff curve of $TD = 2^{128}$ for any $D \leq N^{1/2}$.

By using our new generic attack on 4-round EM with alternating keys, we can extend the tradeoff curve all the way to $D = N$. We can thus reduce the

[4] In the design of LED, the term "step" is used in order to describe what we refer to as a "round" of an iterated EM scheme.

time complexity of the best known attack on 4-step LED-128 by a large factor of 2^{32}, from the totally impractical $T = 2^{96}$ to a more practical $T = 2^{64}$. We note that when considering much smaller improvements over exhaustive search, attacks on up to 8 rounds of LED-128 have been published in [8].

In order to obtain our improved generic attacks, we had to develop a new cryptanalytic technique. The new technique stems from the dissection technique [7] and from the splice-and-cut technique [3], but has also additional features. Like the dissection technique, it divides the cipher into several parts treated independently by enumerating over an intermediate value, but unlike dissection, the parts are not consecutive but rather nested. In addition, as the splice-and-cut technique, the new attack takes advantage of "splicing" (or connecting) two ends of the cipher together. However, in the original splice-and-cut technique, the plaintexts and ciphertexts were "spliced" together, and as a result it was essentially a chosen plaintext attack. On the contrary, in our attack we bridge (or connect) together intermediate encryption values, and thus our attack does not have this constraint and can use known plaintexts. Once we connect a pair of intermediate encryption values using a bridge, we use a self-similarity property of the cipher in order to connect another pair of intermediate encryption values using another bridge. Thus, as our attack bridges between multiple parts of the cipher using multiple bridges, we call it the *multibridge* attack.

In addition to their application to iterated Even-Mansour ciphers with two keys, we notice that our techniques can also be combined with statistical distinguishers to give efficient key recovery attacks on certain block ciphers. These block ciphers have internal symmetric properties which allow us to connect (bridge) together intermediate encryption values at a relatively low cost. Such bridges are constructed in reflection cryptanalysis, a technique introduced by Kara in [16], and generalized more recently by Soleimany et al. in [27]. Thus, as an additional application of our multibridge attack, we show how to use it as a generic key-recovery tool in reflection cryptanalysis.

The self-similarity properties of the cipher that we exploit in multibridge attacks are similar to the ones exploited in the SlideX attack [9] on 1-round EM with one key, and in the later publications [8, 22]. However, in the multibridge attack the connected parts are much more complex, analyzed themselves using bridging techniques, and are joint using several meet-in-the-middle attacks.

The paper is organized as follows: in Section 2, we describe the notations and conventions used in this paper. In Section 3, we describe our new multibridge attack on the alternating key scheme, and its application to LED-128 and to reflection cryptanalysis. In Section 4, we classify all 4-round iterated EM schemes with two keys and summarize our attacks on them. We finish the analysis of 4-round iterated EM schemes in Section 5, and finally propose open problems and conclude the paper in Section 6.

2 Notations and Conventions

Notations. For a general r-round iterated EM scheme with a block size of n bits, we denote by F_i the public function of round i. We denote by K_{i-1} the round-key added at the beginning of round i (i.e., K_0 is added before round 1), while the last round-key is denoted by K_r (see Fig. 1). Given a plaintext-ciphertext pair (P, C), we denote the state after i encryption rounds by X_i (e.g., $X_0 = P$, X_1 is the state after one encryption round, etc.). In order to simplify our notation, we define $\hat{X}_i = X_i \oplus K_i$, and so $F_{i+1}(\hat{X}_i) = X_{i+1}$. In some of our attacks, we consider several parallel evaluations which are similarly denoted by $Y_{j+1} = F_{j+1}(\hat{Y}_j)$, $Z_{j+1} = F_{j+1}(\hat{Z}_j)$, etc.

Conventions. In this paper, we evaluate our attack algorithms in terms of the time complexity T, the data complexity D, and the memory complexity M, as a function of $N = 2^n$ where n is the block size. Note that this N is not necessarily the size of the key space, and exhaustive search of a 2-key EM scheme requires N^2 rather than N time. The complexities of our algorithms are generally exponential in n, and thus we can neglect multiplicative polynomial factors in n in our analysis.

We note that in all of our memory-consuming attacks, it is possible to use time-memory tradeoffs in order to reduce the amount of memory we use. However, in this paper we are mainly interested in tradeoffs between the data and time complexities of our attacks, and thus we simply assume that we have sufficient memory to execute the fastest possible version of the attack, i.e., given D known plaintext-ciphertext pairs, we always try to minimize T.

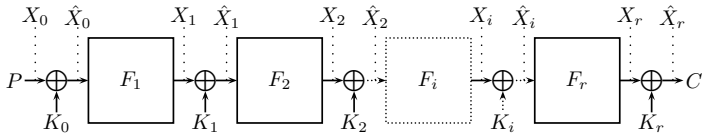

Fig. 1. Iterated Even-Mansour

3 A New attack on 4-Round Iterated Even-Mansour with Two Alternating Keys

The currently best known attack on 4-round iterated EM scheme with 2 alternating keys (see Fig. 2) was proposed in [22] as part of the analysis of 4-step

LED-128 (improving the previous attacks of [15, 20]). The attack yields a tradeoff curve of $TD = N^2$, but is limited by an expensive outer loop that guesses one of the keys and performs computations on the entire data for each such guess. Therefore, the tradeoff $TD = N^2$ is restricted by the constraint $T \geq ND$ (or $TD \geq ND^2$) and is valid only up to $D = N^{1/2}$. Consequently, the attack cannot efficiently exploit more than $D = N^{1/2}$ known plaintexts even when they are easily available. In this section, we describe a new attack, which can obtain the curve $TD = N^2$ for any amount of given data $D \leq N$. In order to provide sufficient background to our new attack, we start by describing the very simple variant of the SlideX attack (proposed in [9]) on 1-round EM with one key, and then describe the previous attack of [22] on 4-round iterated Even-Mansour with 2 alternating keys. After this background material, we describe the basic variant of our new attack on this scheme that applies in the case $D = N$, and then generalize the basic attack in order to obtain the complete curve $TD = N^2$. Finally, we apply the multibridge attack to 4-step LED-128, improving the running time of the best known attack on this well-studied scheme from 2^{96} to 2^{64}.

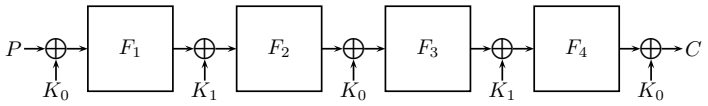

Fig. 2. 4-Round Iterated Even-Mansour with Alternating Keys

3.1 The SlideX Attack on 1-Round Even-Mansour with a Single Key

The SlideX attack [9] is an optimal known plaintext attack on 1-Round EM with one key. It is based on the observation that for each plaintext-ciphertext pair $(P, C) = (X_0, \hat{X}_1)$, $P \oplus K = \hat{X}_0$ and $C \oplus K = X_1$, and thus $P \oplus C = \hat{X}_0 \oplus X_1$ (see Fig. 3). As described in the attack below, this equality is exploited in order to match the plaintext-ciphertext pairs with independent evaluations of the public function F_1 by the attacker. Each such match yields a suggestion for the key, which we can easily test.

1. For each of the D plaintext-ciphertext pairs (P^i, C^i):
   (a) Calculate $P^i \oplus C^i$, and store it in a sorted list L, next to P^i.
2. For N/D arbitrary values $\hat{Y}_0^j$:
   (a) Compute $Y_1^j = F_1(\hat{Y}_0^j)$ and search $\hat{Y}_0^j \oplus Y_1^j$ in the list L.
   (b) For each match, obtain P^i and compute the suggestion $K = P^i \oplus \hat{Y}_0^j$.
   (c) Test the suggestion for K using a trial encryption, and if it succeeds, return it as the key.

As we have D plaintext-ciphertext pairs (P^i, C^i) and we evaluate N/D arbitrary values $\hat{Y}_0^j$, we have $D \cdot N/D = N$ pairs of the form (i, j). Thus, according to the birthday paradox, with high probability there is a pair (i, j) such that $\hat{Y}_0^j = P^i \oplus K \triangleq \hat{X}_0^i$. This implies that $\hat{Y}_0^j \oplus Y_1^j = P^i \oplus C^i$, and thus we will get a match in Step 2.(a), suggesting the correct key K. The time complexity of Step 1 is D. The time complexity of Step 2 is N/D , since for an arbitrary value of $\hat{Y}_0^j \oplus Y_1^j$, we expect a match in Step 2.(a) with probability D/N (and thus, on average, we perform only a constant number of operations for each value of $\hat{Y}_0^j$). Consequently, the time complexity of the attack is $max(D, N/D)$, i.e., the attack gives a tradeoff curve of $TD = N$, but only for $D \leq N^{1/2}$ (i.e., it cannot efficiently exploit more than $D = N^{1/2}$ known plaintexts).

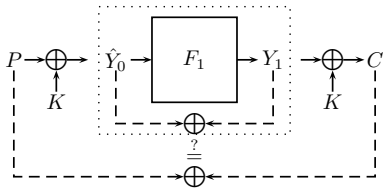

Fig. 3. The Slidex Attack on 1-Round Even-Mansour with 1 Key

3.2 The Best Previous Attack on 4-Round Iterated Even-Mansour with Two Alternating Keys [22]

The best previous attack [22] starts by guessing K_0. This guess makes it possible to eliminate the first and last XOR'ed keys and thus also the first and last permutations by partially encrypting (and decrypting) the plaintext (and ciphertext). In addition, guessing K_0 enables the attacker to combine the second and third applications of the permutations $F_3(F_2(x) \oplus K_0)$ into a single known permutation, $F'_{K_0}(x)$. This reduces the 4-round EM scheme into a single round EM scheme with a single key, which can be easily attacked by the SlideX technique (see Fig. 4). The details of this attack are described below.

1. For all values of K_0:
   (a) For each of the D plaintext-ciphertext pairs (P^i, C^i):
      i. Compute X_1^i and $\hat{X}_3^i$, and store $X_1^i \oplus \hat{X}_3^i$ in a sorted list L, next to X_1^i.
   (b) For N/D arbitrary values $\hat{Y}_1^j$:
      i. Compute Y_3^j and search $\hat{Y}_1^j \oplus Y_3^j$ in the list L.
      ii. For each match, obtain X_1^i and compute the suggestion $K_1 = X_1^i \oplus \hat{Y}_1^j$.
      iii. Test the suggestion for the full key (K_0, K_1) using a trial encryption, and if it succeeds, return it.

For the correct value of K_0, according to the birthday paradox, with high probability there is a pair (i, j) such that $\hat{Y}_1^j = \hat{X}_1^i$. This implies that $X_1^i \oplus \hat{X}_3^i = \hat{Y}_1^j \oplus Y_3^j$, and thus we get a match in Step 1.(b).i, suggesting the correct key (K_0, K_1). The time complexity of Step 1.(a) is D, and the complexity of Step 1.(b) is N/D (we do not expect more than one match in L in Step 1.(b).i for an arbitrary value of $\hat{Y}_1^j \oplus Y_3^j$). Thus, for each value of K_0 that we guess in Step 1, we perform $max(D, N/D)$ operations. Consequently, the attack gives a tradeoff curve of $TD = N^2$, but only for $D \leq N^{1/2}$, i.e., the time complexity must satisfy $T \geq N^{3/2}$. In particular, for $N = 2^{64}$, the best possible time complexity of this attack (for any available amount of data) is at least 2^{96}.

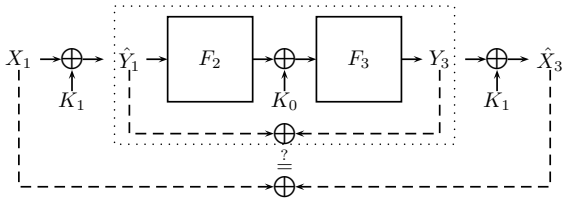

Fig. 4. The Best Previous Attack on 4-Round Iterated Even-Mansour with Two Alternating Keys

Applying a Generalized Version of the Attack to any 2-Key 4-Round Iterated Even-Mansour Scheme. Before describing our improved attack, we notice that in a general 4-round iterated EM scheme with 2 keys which can be used in any order, there is always a key that is added at most twice[5]. Thus, the attack of [22] can be easily generalized and applied with the same complexity to any 4-round iterated EM scheme with 2 keys. The generalized attack works by guessing the value of the most common key (i.e., the key that is added at least 3 times), partially encrypting (decrypting) the plaintexts (ciphertexts), and thus obtaining the inputs/outputs of a single-key EM scheme with a single permutation (which is fully known after guessing the most common key). However, as we show in the rest of this paper, when $D > N^{1/2}$, more efficient attacks exist on all 4-round 2-key EM schemes.

3.3 The Basic Version of our New Multibridge Attack on 4-Round Iterated Even-Mansour with Two Alternating Keys

The approach of the previous attack was to guess K_0, and thus "peel off" the first and last rounds on the 4-round EM scheme with 2 alternating keys. Although

[5] Schemes in which there is a key that is added only once are very weak (as we show in Section A.1).

this approach seems natural, it gives the tradeoff curve of $TD = N^2$ only for $D \leq N^{1/2}$, and thus its time complexity is at least $T \geq N^{3/2}$. We now present our new attack on this scheme which achieves the same tradeoff for any $D \leq N$, and thus enables us to reduce the time complexity to $T = N$.

Unlike the previous attack, which guessed the value of K_0, our attack guesses the value of some *internal state* for which a special self-similarity property holds. This property allows us to split the cipher into two parts which can be analyzed independently. While standard meet-in-the-middle attacks also split the cipher into two parts, in our attack the two parts of the cipher are nested (rather than concatenated), similarly to attacks based on the splice-and-cut technique [3]. However, it is interesting to note that while splice-and-cut attacks consider the first and the last rounds of the cipher as consecutive rounds (i.e., the cipher is spliced using the plaintext-ciphertext pairs), here we connect (or bridge) the cipher internally and consider as consecutive rounds its two internal ends.

We begin by describing our multibridge attack for the specific case of $D = N$ (i.e., given the full code-book), for which the attack runs in time $T = N$. In this case, we look for some plaintext-ciphertext pair (P^i, C^i) with the internal fixed-point property $X_1^i = \hat{X}_3^i$ (i.e., we connect X_1^i and $\hat{X}_3^i$ using a "bridge"). Since XOR'ing the same key twice leaves the result unchanged, this self-similarity property also implies that $\hat{X}_1^i = X_3^i$ (i.e., $\hat{X}_1^i$ and X_3^i are now connected using another bridge, which we get "for free"), and this allows us to split the cipher into 2 nested parts[6], each independently suggesting a value for the key K_0. Finally, the suggestions are merged using a meet-in-the-middle technique. Note that for a specific plaintext-ciphertext pair, this internal fixed-point property occurs with probability $1/N$, and thus given $D = N$ data, with high probability, one of the plaintext-ciphertext pairs will satisfy this property. The details of the basic multibridge attack are given below (see Fig. 5):

1. For each of the $D = N$ known plaintext-ciphertext pairs (P^i, C^i):
   (a) Calculate $P^i \oplus C^i$, and store it in a sorted list L_1, next to P^i.
2. For each of the N possible values of Y_1^j:
   (a) Compute $\hat{Y}_0^j = F_1^{-1}(Y_1^j)$.
   (b) Assume that $\hat{Y}_3^j = Y_1^j$, and compute $Y_4^j = F_4(\hat{Y}_3^j)$.
   (c) Compute $\hat{Y}_0^j \oplus Y_4^j$ and search for matches with this value in L_1.
   (d) For each match, obtain P^i, calculate a suggestion for $K_0 = P^i \oplus \hat{Y}_0^j$. Store all the suggestions in a sorted list L_2, next to Y_1^j. We expect L_2 to contain about N entries.
3. For each of the N possible values of $\hat{Z}_1^\ell$ (i.e., the intermediate encryption value obtained after applying 1 round and adding K_1):
   (a) Compute $Z_2^\ell = F_2(\hat{Z}_1^\ell)$.
   (b) Assume that $Z_3^\ell = \hat{Z}_1^\ell$, and compute $\hat{Z}_2^\ell = F_3^{-1}(Z_3^\ell)$.
   (c) Compute $K_0 = Z_2^\ell \oplus \hat{Z}_2^\ell$ and search for matches in L_2. We expect one match on average for a given value of K_0.

[6] In fact, as described in the detailed attack, the first part of the cipher is in itself also composed of 2 parts.

(d) For each match, obtain Y_1^j, calculate a suggestion for $K_1 = Y_1^j \oplus \hat{Z}_1^\ell$.
(e) Test the suggestion for the full key (K_0, K_1) using a trial encryption, and if it succeeds, return it.

The success of the attack is based on the observation above, namely, given $D = N$ plaintext-ciphertext pairs (P^i, C^i), then with high probability, there exists an i such that $X_1^i = \hat{X}_3^i$. Since we iterate over all possible values of Y_1^j in Step 2 of the attack, then for $Y_1^j = X_1^i$, we calculate $\hat{Y}_0^j \oplus Y_4^j = \hat{X}_0^i \oplus X_4^i = P^i \oplus C^i$ in step 2.(c). Thus, we get a match with the correct value of K_0 is Step 2.(d), and we store it next to $Y_1^j = X_1^i$ in the list L_2. Similarly, since we iterate over all possible values of $\hat{Z}_1^\ell$, then for $\hat{Z}_1^\ell = \hat{X}_1^i$, we have $Z_3^\ell = \hat{Z}_1^\ell = \hat{X}_1^i = X_3^i$. Hence, we calculate the correct value of K_0 in Step 3.(c), obtain the match with L_2 such that $Y_1^j = X_1^i$, and obtain the correct $K_1 = Y_1^j \oplus \hat{Z}_1^\ell = X_1^i \oplus \hat{X}_1^i$. As a result, we encounter the correct suggestion for the full key in Step 3.(e) and return it.

The attack is composed of a sequential execution of 3 mains steps, each has a time complexity of N: in Step 1, we perform a simple XOR operation for each of the $D = N$ plaintext-ciphertext pairs, and allocate the list L_1, which is of size N. In Step 2, we iterate over N possible values of Y_1^j, and for each such value we expect a single match in L_1 in Step 2.(c), implying that the complexity of Step 2 is N. Finally, since the expected size of L_2 is N, for each suggestion of K_0 we expect a single match in Step 3.(c), and thus the time complexity of Step 3 is N, as claimed. In total, the analysis shows that the time complexity of the full attack is N, and its memory complexity is N as well.

3.4 Our Generalized Multibridge Attack on 4-Round Iterated Even-Mansour with Two Alternating Keys

Given $D < N$ data, we do not expect to have a plaintext-ciphertext pair that satisfies the internal fixed-point property. In order to generalize the attack for any $D \leq N$, we first notice that the internal fixed-point property $X_1^i = \hat{X}_3^i$ can be replaced by the more general "bridging" property $X_1^i = \hat{X}_3^i \oplus \Delta$, for any fixed known value of[7] Δ (the previously described fixed-point property is the special case of $\Delta = 0$). Thus, in Step 2.(b) we calculate $\hat{Y}_3^j = Y_1^j \oplus \Delta$, and similarly in Step 3.(b) we calculate $Z_3^\ell = \hat{Z}_1^\ell \oplus \Delta$.

When we fix one value of Δ, we expect to have a pair (P^i, C^i) such that $X_1^i = \hat{X}_3^i \oplus \Delta$ with probability of about D/N. Thus, in order to recover the key with high probability, we randomly choose N/D different values of Δ, indexed by Δ^s, and run a variant of the fixed-point multibridge attack independently for each value. This is a similar approach to the one used in [9] in order to extend the SlideX attack on 1-round 2-key EM to all $D \leq N^{1/2}$. The details of the generalized multibridge attack are given below:

1. For each of the D plaintext-ciphertext pairs (P^i, C^i):

[7] Thus, we do not exploit the actual fixed-point in a strong way (such as in [1]), but merely some fixed linear relation between X_1^i and $\hat{X}_3^i$.

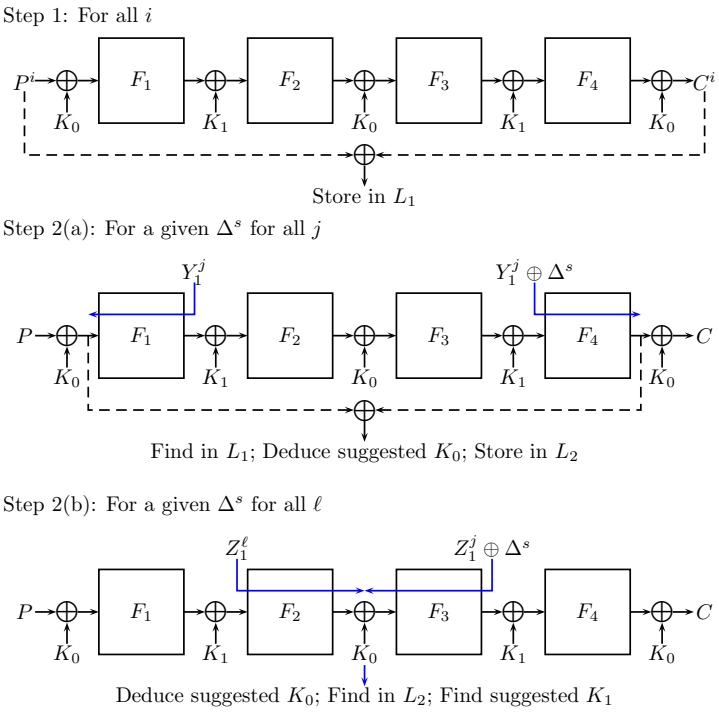

Fig. 5. The Multibridge Attack

(a) Calculate $P^i \oplus C^i$, and store it in a sorted list L_1, next to P^i.

2. For N/D arbitrary values of Δ^s:
   (a) Apply a variant of the basic multibridge attack using Δ^s.

As we execute a variant of the fixed-point attack N/D times, the expected time complexity of the attack is N^2/D. The size of the list L_1 is D, implying that the size of L_2 (the second list allocated in the multibridge attack) is D as well, and thus the memory complexity of the attack is D.

We conclude by noting that this attack can also be applied directly to the attack of Merkle and Hellman against 2K3DES [13]. The resulting attack is essentially the known plaintext variant of van Oorschot and Wiener [28] to Merkle and Hellman's attack, i.e., an attack on 2K3DES with D known plaintexts and running time of N^2/D.

3.5 Application to 4-Step LED-128

LED is a 64-bit lightweight iterated EM block cipher, proposed at CHES 2011 [12]. The cipher has two main variants: a one-key version called LED-64, and a two-key version called LED-128. We concentrate on the 128-bit variant, which has

12 steps, in which the two keys are alternately used. The best previously known attack on 4-step LED-128 was described in [22] (and also described in Section 3.2 for a general 4-step EM cipher with alternating keys), and gives a tradeoff of $TD = 2^{128}$, but only for $D \leq 2^{32}$. We can directly apply our improved attack, described in Section 3.4, to 4-step LED-128, we obtain the tradeoff of $TD = 2^{128}$ for any $D \leq 2^{64}$. Thus, we improve the time complexity of the best known attack on this scheme from 2^{96} to 2^{64}.

We note that recently, up to 8 steps of the 2-key alternating EM scheme have been attacked faster than exhaustive search (see [8]). However, all the known attacks on more than 4 steps are marginal in the sense that they improve the time complexity of exhaustive search only by a logarithmic factor in N, and thus our new attack on the 4-step version of LED-128 is currently the best non-marginal attack on this scheme.

3.6 Application to Reflection Cryptanalysis

Reflection cryptanalysis was introduced by Kara in [16] as a self-similarity attack on GOST and related block ciphers, and generalized to a statistical attack on a broader class of ciphers (called "PRINCE-like" ciphers) by Soleimany et al. in [27]. A PRINCE-like cipher is designed to have a specific symmetry property around its middle round, called α-reflection.[8] The definition and analysis of PRINCE-like ciphers in [27], was inspired by the block cipher PRINCE [5], that used the α-reflection property in order to realize decryption on top of encryption with a negligible cost.

In reflection cryptanalysis of PRINCE-like ciphers, we consider the encryption process of a single plaintext, and study the difference between its internal encryption values, which are symmetric with respect to the middle round of the cipher. The goal is to iteratively construct a *reflection distinguisher*, which is a strong non-random property, likely to be present in several rounds of PRINCE-like ciphers (as shown in [27]). In particular, a reflection distinguisher on r rounds of the cipher (denoted by E_K), gives a specific value of Δ for which $\Pr(X \oplus E_K(X) = \Delta) > 2^{-n}$ (where the probability is taken over the input X).

In this section, we present a variant of the multibridge attack as a generic key-recovery method for reflection cryptanalysis. This attack can be considered as the reflection cryptanalysis counterpart of the key-recovery attack of Daemen [6] for differential cryptanalysis of ciphers based on the Even-Mansour construction. The attack assumes that we have a reflection distinguisher with probability $p > 2^{-n}$ on r rounds of the cipher, and recovers the secret key for a total of $r + 2$ rounds, by adding one round at the beginning and one round at the end (i.e., the reflection distinguisher covers rounds $2, 3, \ldots, r + 1$). For the sake of simplicity, we first assume that the cipher is a single-key iterated Even-Mansour scheme, where the secret key is denoted by K. We now describe the attack, assuming that we obtain D plaintext-ciphertext pairs, such that $D > p^{-1}$.

[8] If we denote by E_K the encryption of r rounds in the middle of the cipher under the key K, then the α-reflection property (for a fixed value of α) states that for any input X, $E_K(X) = E^{-1}_{K \oplus \alpha}(X)$.

1. For $2^n/(p \cdot D)$ arbitrary values of $\hat{Y}_0^j$:
   (a) Compute $Y_1^j = F_1(\hat{Y}_0^j)$.
   (b) Assume that $\hat{Y}_{r+1}^j = Y_1^j \oplus \Delta$ (where the value of Δ is given by the reflection distinguisher), and compute $Y_{r+2}^j = F_{r+2}(\hat{Y}_{r+1}^j)$.
   (c) Store $\hat{Y}_0^j \oplus Y_{r+2}^j$ in a sorted list L, next to $\hat{Y}_0^j$.
2. For each of the D plaintext-ciphertext pairs (P^i, C^i):
   (a) Compute $P^i \oplus C^i$, and search the list L for matches.
   (b) For each match obtain $\hat{Y}_0^j$, and calculate a suggestion for $K = P^i \oplus \hat{Y}_0^j$.
   (c) Test the suggestion for the key K using a trial encryption, and if it succeeds, return it.

We have $D > p^{-1}$ plaintext-ciphertext pairs, out of which $p \cdot D > 1$ are expected to satisfy the reflection characteristic. As we evaluate $2^n/(p \cdot D)$ values of $\hat{Y}_0^j$ in Step 1 of the attack, according to the birthday paradox, we expect at least one match between $\hat{Y}_0^j$ and $P^i \oplus K$ such that (P^i, C^i) satisfies the reflection property. Once we obtain such a match (i.e., $\hat{Y}_0^j = P^i \oplus K$), we recover the correct key in Step 2.(c).

As we expect less than one match in L in Step 2.(a) for an arbitrary (P^i, C^i), the time complexity of the attack is $max(D, 2^n/(p \cdot D))$. The time complexity is minimized to $2^{n/2} \cdot p^{-1/2}$ by choosing $D = 2^{n/2} \cdot p^{-1/2}$ (note that it is not reasonable to exploit more than $2^{n/2} \cdot p^{-1/2}$ data). The memory complexity of the attack is $2^n/(p \cdot D)$, but can be easily reduced to D, by exchanging the order of steps 1 and 2 of the attack.

In order to apply the attack to more complex key schedules, the attacker can exploit the internal properties of the reflection distinguisher to recover more key material (perhaps using more data, or function evaluations in Step 1 of the attack). However, this extension is highly dependent on the internal properties of the cipher, and is thus out of the scope of this paper.

4 Classification and Summary of our Attacks on all 4-Round 2-Key Iterated Even-Mansour Schemes

In the rest of the paper, we analyze all the remaining iterated EM schemes with 4 rounds and 2 keys, and show that the best attack on each one of them has a time complexity of N. We begin by noting that each such construction can be described by a sequence of 5 keys, which specifies the order in which the keys K_0 and K_1 are added (over $GF(2)$) to the internal state. For example, we denote the 4-round EM scheme with alternating keys (of Fig. 2) by $[K_0, K_1, K_0, K_1, K_0]$. Clearly, each such scheme has an equivalent representation which is obtained by renaming the keys K_0 and K_1 (e.g., $[K_0, K_0, K_1, K_1, K_0]$ is equivalent to $[K_1, K_1, K_0, K_0, K_1]$). In addition, since our attacks assume that the public permutations F_i (and F_i^{-1}) are chosen at random (i.e., we do not exploit any special properties of the public permutations), from a cryptanalytic point of view, the roles of encryption and decryption can be exchanged.

Namely, if we reverse the order in which the keys are added, we get an equivalent scheme. For example, the scheme $[K_0, K_0, K_1, K_1, K_0]$ is equivalent to $[K_0, K_1, K_1, K_0, K_0]$, since any attack on $[K_0, K_0, K_1, K_1, K_0]$ can also be applied to $[K_0, K_1, K_1, K_0, K_0]$ (by reversing the roles of encryption and decryption), and vice-versa. Altogether, the scheme $[K_0, K_0, K_1, K_1, K_0]$ belongs to an equivalence class (EC) with 4 members, containing the 3 additional schemes $[K_1, K_1, K_0, K_0, K_1]$, $[K_0, K_1, K_1, K_0, K_0]$ and $[K_1, K_0, K_0, K_1, K_1]$. Since any attack on a member of an EC is applicable to its other members, we only need to describe an attack on a representative of the EC.

Table 2 lists the equivalence classes of all the 4-round 2-key iterated EM schemes, next to the complexities of our best attacks. For the sake of simplification, we will refer to each EC as a single scheme, using its ID as described in Table 2. For example, our attack on the schemes of the first EC is simply refereed to an attack on the "EC1 scheme", whose representative is $[K_0, K_1, K_1, K_1, K_1]$.

The attack on EC7, which is 4-round EM with alternating keys, was already described in Section 3.4. In the next section we present the most complex multibridge attacks on the classes EC8 and EC9. Finally, the simpler attacks on EC1–EC6 are presented for sake of completeness in Appendix A.

Table 2. Classification and Attacks on Iterated Even-Mansour Schemes with Four Rounds and Two Keys

EC ID	EC Representative	Section	Data	Time	Memory
EC1	$[K_0, K_1, K_1, K_1, K_1]$	A.1	$O(1)$	N	$O(1)$
EC2	$[K_0, K_1, K_0, K_0, K_0]$	A.1	$O(1)$	N	$O(1)$
EC3	$[K_0, K_0, K_1, K_0, K_0]$	A.1	$O(1)$	N	$O(1)$
EC4	$[K_0, K_0, K_1, K_1, K_1]$	A.2	$O(1)$	N	N
EC5	$[K_0, K_1, K_1, K_0, K_0]$	A.2	$O(1)$	N	N
EC6	$[K_0, K_1, K_1, K_1, K_0]$	A.3	$D \leq N$	N^2/D	D
EC7	$[K_0, K_1, K_0, K_1, K_0]$	3.4	$D \leq N$	N^2/D	D
EC8	$[K_0, K_1, K_0, K_1, K_1]$	5.1	$D \leq N$	N^2/D	D
EC9	$[K_0, K_1, K_0, K_0, K_1]$	5.2	$D \leq N^{1/2}$	N^2/D	D
			$N^{1/2} < D \leq N$	N^2/D	N

Each EC (equivalence class) is described using an ID and a representative scheme.

Classification and Attacks on all 3-Round 2-Key Iterated Even-Mansour Schemes. We did not find any cryptanalytic techniques which are specifically applicable to 3-round 2-key EM schemes. However, for the sake of completeness, we also classify all 3-round 2-key iterated EM schemes and specify which variant of our 4-round attacks can be used to break it (with the same complexities).

1. $[K_0, K_1, K_1, K_1]$ and $[K_0, K_1, K_0, K_0]$ can be broken with a variant of the attack on EC1.

2. $[K_0, K_1, K_1, K_0]$ can be broken with a variant of the attack on EC4.
3. $[K_0, K_1, K_0, K_1]$ can be broken with a variant of the attack on EC7.

5 Multibridge Attacks on EC8 and EC9

In this section we consider the schemes EC8 and EC9, and show that they can be attacked with complexity $DT = N^2$, for all $D \leq N$. The attacks on these schemes use the same general multibridge technique as our previous attack on EC7 in Section 3, namely, we use a generalized version of the internal fixed-point property in order to internally bridge different parts of the cipher. Finally, the suggestions for the key obtained from the two parts are merged using a meet-in-the-middle technique.

5.1 A Multibridge Attack on EC8

In order to attack the scheme $[K_0, K_1, K_0, K_1, K_1]$, we look for a plaintext-ciphertext pair (P^i, C^i) such that $\hat{X}_2^i = P^i \oplus \Delta^s$ (for arbitrary values of Δ^s). The details of the multibridge attack on EC8 are given below:

1. For N/D arbitrary values of Δ^s:
   (a) For each of the D plaintext-ciphertext pairs (P^i, C^i):
      i. Assume that $\hat{X}_2^i = P^i \oplus \Delta^s$ and compute $X_3^i = F_3(\hat{X}_2^i)$.
      ii. Compute $X_3^i \oplus C^i$ and store it in a sorted list L_1, next to C^i.
   (b) For each of the N possible values of $\hat{Y}_3^j$:
      i. Compute $Y_4^j = F_4(\hat{Y}_3^j)$.
      ii. Compute $\hat{Y}_3^j \oplus Y_4^j$, and search for matches in L_1.
      iii. For each match, obtain C^i, compute a suggestion for $K_1 = C^i \oplus Y_4^j$, and store the suggestion in a sorted list L_2, next to P^i.
   (c) For each of the N possible values of $\hat{Z}_0^\ell$:
      i. Compute $Z_1^\ell = F_1(\hat{Z}_0^\ell)$.
      ii. Assume that $Z_2^\ell = \hat{Z}_0^\ell \oplus \Delta^s$, and compute $\hat{Z}_1^\ell = F_2^{-1}(Z_2^\ell)$.
      iii. Compute a suggestion for $K_1 = Z_1^\ell \oplus \hat{Z}_1^\ell$ and search for it in the list L_2.
      iv. For each match, obtain P^i, compute a suggestion for $K_0 = P^i \oplus \hat{Z}_0^\ell$.
      v. Test the full key (K_0, K_1) using a trial encryption, and if it succeeds, return it.

The analysis of the attack is very similar to the analysis of our general multibridge attack in Section 3.4, and thus given $D \leq N$ known plaintext-ciphertext pairs, its time complexity is N^2/D and its memory complexity is D.

5.2 A Multibridge Attack on EC9

In order to attack the scheme $[K_0, K_1, K_0, K_0, K_1]$, we look for a plaintext-ciphertext pair (P^i, C^i) such that $X_1^i = C^i \oplus \Delta^s$ (for arbitrary values of Δ^s). The details of the multibridge attack on EC9 are given below:

1. For N/D arbitrary values of Δ^s:
   (a) For each of the D plaintext-ciphertext pairs (P^i, C^i):
      i. Assume that $X_1^i = C^i \oplus \Delta^s$ and compute $\hat{X}_0^i = F_1^{-1}(X_1^i)$.
      ii. Compute a suggestion for $K_0 = \hat{X}_0^i \oplus P^i$ and store it in a sorted list L_1, next to X_1^i.
   (b) For each of the N possible values of $\hat{Y}_1^j$:
      i. Compute $Y_2^j = F_2(\hat{Y}_1^j)$.
      ii. Assume that $Y_4^j = \hat{Y}_1^j \oplus \Delta^s$ and compute $\hat{Y}_3^j = F_4^{-1}(Y_4^j)$.
      iii. Compute $Y_2^j \oplus \hat{Y}_3^j$ and store this value on a sorted list L_2, next to $\hat{Y}_1^j$ and Y_2^j.
   (c) For each of the N possible values of $\hat{Z}_2^\ell$:
      i. Compute $Z_3^\ell = F_3(\hat{Z}_2^\ell)$.
      ii. Compute $\hat{Z}_2^\ell \oplus Z_3^\ell$ and search for it in the list L_2.
      iii. For each match, obtain Y_2^j (and $\hat{Y}_1^j$), compute a suggestion for $K_0 = Y_2^j \oplus \hat{Z}_2^\ell$, and search it in the sorted list L_1.
      iv. For each match, obtain X_1^i and compute a suggestion for $K_1 = X_1^i \oplus \hat{Y}_1^j$.
      v. Test the full key (K_0, K_1) using a trial encryption, and if it succeeds, return it.

Similarly to the multibridge attacks on EC7 and EC8, the time complexity of the attack is N^2/D for any $D \leq N$, as the time complexity of each of the Steps 1.(a), 1.(b) and 1.(c) is N. However, unlike the previous attacks which had a reduced memory complexity of D, the list L_2 contains N elements, and thus the memory complexity of this attack is N. As a result, when $D \leq N^{1/2}$, the most efficient attack on this scheme is the generalized version of the attack presented in Section 3.2, which has the same running time but requires less memory.

We note that in cases where $D > N^{1/2}$, but the available memory M satisfies $D \leq M < N$, it is possible obtain a tradeoff between the memory and time complexities of the attack. Although in this paper we mainly consider tradeoffs between data and time, an interesting open question is whether it is possible to reduce the memory complexity of the attack for $D > N^{1/2}$ without increasing its time complexity.

6 Conclusions and Open Problems

In this paper, we studied the security of iterated Even-Mansour schemes with two keys. We showed that all such schemes with at most 4 rounds provide security of at most 2^n (compared to the 2^{2n} complexity of exhaustive key search). Our

theoretical results allowed us to reduce the complexity of the best known attack on 4-step LED-128 from 2^{96} to 2^{64}, and to develop a generic key-recovery tool for reflection cryptanalysis. In order to obtain these results, we developed the novel multibridge technique which combines the advantages of the dissection [7] and the splice-and-cut [3] techniques.

We conclude this paper with a list of several open problems and research directions which arise naturally from the results of our paper.

1. **Finding better attacks on 3-round EM with two keys.** Using our techniques, we could not find attacks on 3-round EM with alternating keys which are better than the attacks on 4-round EM with alternating keys. If such attacks indeed do not exist, then there is no security gain in adding a round to the 3-round EM scheme. Such a situation is somewhat unusual, and hence, one may anticipate that better attacks exist on 3-round EM with alternating keys. We note that this is a similar scenario to cascade encryption, where the complexity of the best attack on 3-encryption is the same as the complexity of the best attack on 4-encryption [7]. However, in cascade encryption, the complexities are equal only for the specific attacks that minimize the time complexity, while in our case, the complexities are the same for all attacks on the tradeoff curve.
2. **Finding the minimal number r for which r-round EM with two keys provides $2n$-bit security.** This is an interesting research direction whose equivalent has been extensively studied in the domain of Feistel constructions (see [19, 24, 25]). In the case of EM with two keys, we are not aware of any attacks on the 5-round alternating key scheme which improve over exhaustive search by a significant factor. On the other hand, when considering relatively small (polynomial in n) improvements over exhaustive search, up to 8 rounds can be broken (see [8]), but no attacks at all are known for $r \geq 9$ rounds. Clearly, this fundamental question can be generalized to more keys, namely, what is the minimal number of rounds for which mn-bit security can be achieved for n-bit iterated EM constructions with m independent keys?
3. **Other attack models.** In this paper, we concentrated on attacks in the most conservative model in which the adversary has access only to known plaintexts, and the complexity of the attack takes into consideration all operations (including a potential preprocessing stage). It would be interesting to see whether the complexities of the attacks can be reduced in other models, where chosen or even adaptively chosen plaintext queries are allowed, and perhaps precomputation is not counted in the overall complexity of the attack. We note that in a recent work of Joux and Fouque [11], such improved attacks were found for the 1-round EM construction with two keys, suggesting that similar results may be possible for iterated EM with two keys as well.
4. **Considering memory complexity.** As in all previous papers on iterated EM, we concentrated in this paper on tradeoffs between data and time complexities, assuming that we always have enough memory to apply the most efficient attack. It would be interesting to consider more general tradeoffs

between data, memory and time complexities, and in particular, minimize the memory complexity for which the (presumably) optimal curve $DT = 2^{2n}$ can be obtained. We note that a similar question with respect to 1-round EM was asked in [9] and partially answered in [11].

5. **More complex key schedules.** As stated in the introduction, iterated EM schemes can be considered with a wide variety of key schedules, generating an endless field of research. However, even when restricted to schemes with two keys as we do in this paper, one may consider more complex key schedules in which combinations of the keys $K0$ and $K1$ can be used as round keys. It seems that the attacks presented in this paper cannot target such key schedules, and for example, we could not find an attack of complexity 2^n on 4-round EM with the keys $[K0, K1, K0, K1, K0 \oplus K1]$. Hence, it will be interesting to find new techniques that will be able to handle such key schedules, or to show lower bounds on the security of the respective iterated EM schemes.

References

1. Wim Aerts, Eli Biham, Dieter De Moitie, Elke De Mulder, Orr Dunkelman, Sebastiaan Indesteege, Nathan Keller, Bart Preneel, Guy A. E. Vandenbosch, and Ingrid Verbauwhede. A Practical Attack on KeeLoq. *J. Cryptology*, 25(1):136–157, 2012.
2. Elena Andreeva, Andrey Bogdanov, Yevgeniy Dodis, Bart Mennink, and John P. Steinberger. On the Indifferentiability of Key-Alternating Ciphers. In Ran Canetti and Juan A. Garay, editors, *CRYPTO (1)*, volume 8042 of *Lecture Notes in Computer Science*, pages 531–550. Springer, 2013.
3. Kazumaro Aoki and Yu Sasaki. Preimage Attacks on One-Block MD4, 63-Step MD5 and More. In Roberto Maria Avanzi, Liam Keliher, and Francesco Sica, editors, *Selected Areas in Cryptography*, volume 5381 of *Lecture Notes in Computer Science*, pages 103–119. Springer, 2008.
4. Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, François-Xavier Standaert, John P. Steinberger, and Elmar Tischhauser. Key-Alternating Ciphers in a Provable Setting: Encryption Using a Small Number of Public Permutations - (Extended Abstract). In Pointcheval and Johansson [26], pages 45–62.
5. Julia Borghoff, Anne Canteaut, Tim Güneysu, Elif Bilge Kavun, Miroslav Knezevic, Lars R. Knudsen, Gregor Leander, Ventzislav Nikov, Christof Paar, Christian Rechberger, Peter Rombouts, Søren S. Thomsen, and Tolga Yalçin. PRINCE - A Low-Latency Block Cipher for Pervasive Computing Applications - Extended Abstract. In Wang and Sako [30], pages 208–225.
6. Joan Daemen. Limitations of the Even-Mansour Construction. In Imai et al. [14], pages 495–498.
7. Itai Dinur, Orr Dunkelman, Nathan Keller, and Adi Shamir. Efficient Dissection of Composite Problems, with Applications to Cryptanalysis, Knapsacks, and Combinatorial Search Problems. In Reihaneh Safavi-Naini and Ran Canetti, editors, *CRYPTO*, volume 7417 of *Lecture Notes in Computer Science*, pages 719–740. Springer, 2012.
8. Itai Dinur, Orr Dunkelman, Nathan Keller, and Adi Shamir. Key Recovery Attacks on 3-round Even-Mansour, 8-step LED-128, and Full AES^2. In Kazue Sako and Palash Sarkar, editors, *ASIACRYPT (1)*, volume 8269 of *Lecture Notes in Computer Science*, pages 337–356. Springer, 2013.

9. Orr Dunkelman, Nathan Keller, and Adi Shamir. Minimalism in Cryptography: The Even-Mansour Scheme Revisited. In Pointcheval and Johansson [26], pages 336–354.
10. Shimon Even and Yishay Mansour. A construction of a cioher from a single pseudorandom permutation. In Imai et al. [14], pages 210–224.
11. Pierre-Alain Fouque, Antoine Joux, and Chrysanthi Mavromati. Multi-user collisions: Applications to discrete logs, even-mansour and prince. Cryptology ePrint Archive, Report 2013/761, 2013. `http://eprint.iacr.org/`.
12. Jian Guo, Thomas Peyrin, Axel Poschmann, and Matthew J. B. Robshaw. The LED Block Cipher. In Bart Preneel and Tsuyoshi Takagi, editors, *CHES*, volume 6917 of *Lecture Notes in Computer Science*, pages 326–341. Springer, 2011.
13. Martin E. Hellman. A Cryptanalytic Time-Memory Trade-Off. *IEEE Transactions on Information Theory*, 26(4):401–406, 1980.
14. Hideki Imai, Ronald L. Rivest, and Tsutomu Matsumoto, editors. *Advances in Cryptology - ASIACRYPT '91, International Conference on the Theory and Applications of Cryptology, Fujiyoshida, Japan, November 11-14, 1991, Proceedings*, volume 739 of *Lecture Notes in Computer Science*. Springer, 1993.
15. Takanori Isobe and Kyoji Shibutani. Security Analysis of the Lightweight Block Ciphers XTEA, LED and Piccolo. In Willy Susilo, Yi Mu, and Jennifer Seberry, editors, *ACISP*, volume 7372 of *Lecture Notes in Computer Science*, pages 71–86. Springer, 2012.
16. Orhun Kara. Reflection Cryptanalysis of Some Ciphers. In Dipanwita Roy Chowdhury, Vincent Rijmen, and Abhijit Das, editors, *INDOCRYPT*, volume 5365 of *Lecture Notes in Computer Science*, pages 294–307. Springer, 2008.
17. Rodolphe Lampe, Jacques Patarin, and Yannick Seurin. An Asymptotically Tight Security Analysis of the Iterated Even-Mansour Cipher. In Wang and Sako [30], pages 278–295.
18. Michael Luby and Charles Rackoff. How to Construct Pseudorandom Permutations from Pseudorandom Functions. *SIAM J. Comput.*, 17(2):373–386, 1988.
19. Avradip Mandal, Jacques Patarin, and Yannick Seurin. On the Public Indifferentiability and Correlation Intractability of the 6-Round Feistel Construction. In Ronald Cramer, editor, *TCC*, volume 7194 of *Lecture Notes in Computer Science*, pages 285–302. Springer, 2012.
20. Florian Mendel, Vincent Rijmen, Deniz Toz, and Kerem Varici. Differential Analysis of the LED Block Cipher. In Wang and Sako [30], pages 190–207.
21. Ralph C. Merkle and Martin E. Hellman. On the Security of Multiple Encryption. *Commun. ACM*, 24(7):465–467, 1981.
22. Ivica Nikolić, Lei Wang, and Shuang Wu. Cryptanalysis of Round-Reduced LED. In *FSE*, 2013. To appear in Lecture Notes in Computer Science.
23. Jacques Patarin. Improved security bounds for pseudorandom permutations. In Richard Graveman, Philippe A. Janson, Clifford Neumann, and Li Gong, editors, *ACM Conference on Computer and Communications Security*, pages 142–150. ACM, 1997.
24. Jacques Patarin. Luby-Rackoff: 7 Rounds Are Enough for $2^{n(1\text{-epsilon})}$Security. In Dan Boneh, editor, *CRYPTO*, volume 2729 of *Lecture Notes in Computer Science*, pages 513–529. Springer, 2003.
25. Jacques Patarin. Security of Random Feistel Schemes with 5 or More Rounds. In Matthew K. Franklin, editor, *CRYPTO*, volume 3152 of *Lecture Notes in Computer Science*, pages 106–122. Springer, 2004.

26. David Pointcheval and Thomas Johansson, editors. *Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings*, volume 7237 of *Lecture Notes in Computer Science*. Springer, 2012.
27. Hadi Soleimany, Céline Blondeau, Xiaoli Yu, Wenling Wu, Kaisa Nyberg, Huiling Zhang, Lei Zhang, and Yanfeng Wang. Reflection Cryptanalysis of PRINCE-Like Ciphers. *Journal of Cryptology*, pages 1–27, 2013.
28. Paul C. van Oorschot and Michael J. Wiener. A Known Plaintext Attack on Two-Key Triple Encryption. In Ivan Damgård, editor, *EUROCRYPT*, volume 473 of *Lecture Notes in Computer Science*, pages 318–325. Springer, 1990.
29. Paul C. van Oorschot and Michael J. Wiener. Parallel Collision Search with Cryptanalytic Applications. *J. Cryptology*, 12(1):1–28, 1999.
30. Xiaoyun Wang and Kazue Sako, editors. *Advances in Cryptology - ASIACRYPT 2012 - 18th International Conference on the Theory and Application of Cryptology and Information Security, Beijing, China, December 2-6, 2012. Proceedings*, volume 7658 of *Lecture Notes in Computer Science*. Springer, 2012.

A Simple Attacks on 4-Round Iterated Even-Mansour Schemes with Two Keys

In this section, we describe attacks on the EM schemes EC1–EC6 (as defined in Table 2), which can be broken using very simple techniques.

A.1 Attacks on EC1, EC2 and EC3

The first 3 schemes, which add the key K_0 (or K_1) only once, are very simple to analyze. We describe below an attack on the representative of EC1 ($[K_0, K_1, K_1, K_1, K_1]$), using 2 plaintext-ciphertext pairs (which is the unicity bound). The attacks on EC2 and EC3 are similar.

1. For all K_1 values:
   (a) Using C^1 and K_1, calculate $\hat{X}_0^1$, and compute the suggestion $K_0 = P^1 \oplus \hat{X}_0^1$.
   (b) Test the full key (K_0, K_1) using (P^2, C^2), and if the test succeeds, return (K_0, K_1).

The time complexity of the attack is N, while it requires a constant amount of memory (as summarized in Table 2).

A.2 Attacks on EC4 and EC5

We analyze the schemes EC4 and EC5, which add the key K_0 (or K_1) only in two consecutive rounds. Our attack on the representative of EC4 ($[K_0, K_0, K_1, K_1, K_1]$) is described below, using 2 plaintext-ciphertext pairs (i.e., the unicity bound).

1. For all values of $\hat{Y}_0^j$:
   (a) Calculate $Y_1^j = F_1(\hat{Y}_0^j)$, and store $\hat{Y}_0^j \oplus Y_1^j$ in a sorted list L, next to $\hat{Y}_0^j$.

2. For each value of K_1:
   (a) Using C^1 and K_1, compute $\hat{X}_1^1$, and search the list L for the value $P^1 \oplus \hat{X}_1^1$.
   (b) For each match, obtain $\hat{Y}_0^j$, and compute the suggestion $K_0 = P^1 \oplus \hat{Y}_0^j$.
   (c) Test the full key (K_0, K_1) using (P_2, C_2), and if the test succeeds, return (K_0, K_1).

For the correct value of K_1, we will get a match in Step 2.(a) such that $\hat{Y}_0^j = \hat{X}_0^1$, thus obtaining the correct key in Step 2.(c). Since the list L contains N entries, the memory complexity of the attack is N. As we expect one match for each value of K_1 in Step 2.(a), the time complexity of the attack is N.

We note that if the available memory is smaller than N, it is possible to obtain a time-memory tradeoff by changing the structure of the attack, and using the parallel collision search algorithm [29] by finding collisions between two functions: one function maps K_0 to $P^1 \oplus \hat{X}_1^1$, and the second function maps $\hat{Y}_0^j$ to $\hat{Y}_0^j \oplus Y_1^j$. However, as noted in Section 2, this is out of the scope of this paper.

The attack on EC5 ($[K_0, K_1, K_1, K_0, K_0]$) is very similar, as in Step 1 we iterate over all values of $\hat{Y}_1^j$ (instead of $\hat{Y}_0^j$) and in Step 2 we iterate over all values of K_0 (instead of K_1), and modify the rest of the attack accordingly.

A.3 An Attack on EC6

The last simple scheme we analyze is EC6 ($[K_0, K_1, K_1, K_1, K_0]$), which adds the key K_0 only at the beginning and at the end of the encryption process. The attack (described below) guesses K_1, and for each guess applies the SlideX attack on the resultant 1-round EM scheme.

1. For each of the D plaintext-ciphertext pair (P^i, C^i):
   (a) Calculate $P^i \oplus C^i$, and store it in a sorted list L, next to P^i.
2. For each value of K_1:
   (a) For N/D arbitrary values $\hat{Y}_0^j$:
      i. Compute Y_4^j and search $\hat{Y}_0^j \oplus Y_4^j$ in the list L.
      ii. For each match, obtain P^i and compute the suggestion $K_0 = P^i \oplus \hat{Y}_0^j$.
      iii. Test full key (K_0, K_1) using a trial encryption, and if it succeeds, return it as the key.

Given D plaintext-ciphertext pairs, the expected time complexity of the attack is N^2/D, and its memory complexity is D. Note that since Step 1 is executed only once (it does not depend on K_1), then the time complexity of the attack is N^2/D for any $D \leq N$.