MB+: Enhanced Multibridge Attack for Even-Mansour Schemes

Sitao Wang[1,a], Yao Zhang[1,b], Xiao Zhang[1,c],and Zhiming Zheng[1,d]

LMIB and School of Mathematics and Systems Science, Beihang University, Beijing 100191, China
[a]sitao_wang@buaa.edu.cn, [b]yaozhang@buaa.edu.cn, [c]09621@buaa.edu.cn, [d]zzheng@pku.edu.cn

Keywords: Cryptanalysis; Block Cipher; Even-Mansour Scheme; Multibridge Attack;

Abstract. Block ciphers serve as the core of the modern cryptography, with a continuing study of cryptanalysis never stopped. Recently, a specific cryptographic structure, namely Even-Mansour scheme, has been widely revisited and discussed due to its well relevance to most block ciphers. In this paper, we have proposed MB+, a novel and effective solution to key-recovery issue especially for 4 round Even-Mansour schemes. Our method is inspired by a multibridge attack that uses two round keys alternately. Specifically, based on a thorough analysis on the properties of the fixed points, we have observed the existence of invalid keys that can not be disclosed by the multibridge attack. Targeting at the reduction of invalid-key set, we obtain the MB+ method by introducing XOR-parameters in a flexible fashion. With the theoretical analysis and extensive experiments against popular block ciphers, we confirm the effectiveness of our approach systematically.

Introduction

Cryptanalysis, as well as the design of block ciphers, remains to be one of the fundamental components of the modern cryptography. Recently, a certain "round key XOR-permutation-round key XOR" structure, also formally named as *Even-Mansour* (EM) scheme [1, 2], has attracted increasingly attention in the literature. EM-based attacks can recover the secret key of a cipher algorithm with a simple assumption that the round function is a black box. Namely, launching such an attack requires no knowledge of the internal encryption module, which is very close to real adversarial scenarios. More importantly, it turns out that most block ciphers (such as Camellia [3], CLEFIA [4], SMS4 [5], etc.) can be expressed into special cases of EM schemes since the procedure of relevant algorithms inevitably evolving round key XORs. Also, it is straightforward to extend the 1-round EM cipher to a form of arbitrary rounds. As a result, looking into potential EM-based attacks becomes a necessity.

So far, one of the most effective EM-based attacks is *multibridge attack* [6], which is dedicated for the secret key recovery of 4-round EM schemes. In particular, multibridge attack can disclose the round keys for a $2n$-length secret key with a $O(2^n)$ complexity for both data and time. Essentially, multibridge attack adopts birthday paradox to balance the complexity, while a fixed-point technique is leveraged to guarantee the success of such attack.

In this paper, we introduce another look on the multibridge attack. We point out that the success of the original multibridge attack is independent from the attack times. Based on a thorough analysis on the properties of the fixed points, we have observed the existence of *invalid keys* that can not be disclosed by the multibridge attack. Targeting at the reduction of invalid-key set, we give an enhanced version of multibridge attack, namely *MB+*, that can significantly increase the effectiveness of such attack on an EM scheme. Hereby, we conclude the contribution of our paper as follows:

- We present the concept of invalid-key set. We formally prove the high correlation between failure cases and the invalid keys.
- We theoretically analyze the properties of the fixed points, showing more than 30% of the keys are invalid during the multibridge attack.
- We optimize the multibridge attack and propose MB+ to enable better attacking performance on EM schemes. Especially, MB+ used can be conduced multiple times to further increase the successful rate.

- We experimentally test the effectiveness of MB+ upon well-known ciphers such as Camellia, CLEFIA, and SMS4.

Background: Even-Mansour Cipher and Multibridge Attack

In this section we briefly introduce the standard form of Even-Mansour scheme and the multibridge attack. More complete specifications can be found in [1, 2, 6].

Even-Mansour scheme is a block cipher structure constructed by a random public permutation with a pre-whitening and a post-whitening, which can be denoted as

$$E(x) = k_1 \oplus F(k_0 \oplus x), \tag{1}$$

where F is a n-bits random permutation oracle and x refers to the encrypted plaintext. k_0 and k_1 are two independent n-bits keys. Considering the public permutation as the round function used in the single-round scheme, it can be easily extended to r rounds which contains r public permutations. The r-round Even-Mansour using $r+1$ independent round keys can be shown as follows:

$$E(x) = k_r \oplus F_r(k_{r-1} \oplus F_{r-1}(\cdots(k_1 \oplus F_1(k_0 \oplus x))\cdots)). \tag{2}$$

Consider the S layer and P layer as a public permutation, the SP-structure can be seen as Even-Mansour scheme. Therefore, EM scheme is also suitable for block-cipher structures such as *Feistel*.

The multibridge attack is a category of the key-recovery attacks using two round keys alternately. It is the first effective key-recovery attack for 4-round Even-Mansour schemes. Here we shows the basic procedures of a multibridge attack, the details of which are also illustrated in Fig. 1.

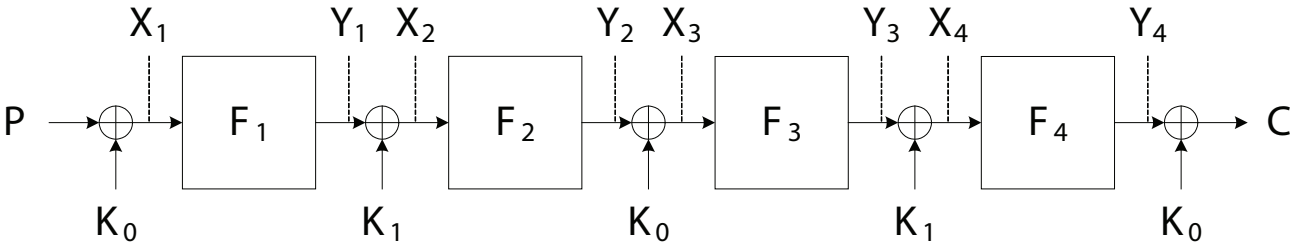

Fig. 1: A basic multibridge attack on a Even-Mansour scheme.

(1) For each plaintext P^i, calculate the ciphertext C^i and store the value $(P^i, P^i \oplus C^i)$ in list L_1.

(2) For each internal state Y_1^j, assume that $X_4^j = Y_1^j$, calculate $X_1^j = F_1^{-1}(Y_1^j)$ and $Y_4^j = F_4(X_4^j)$. Search the $X_1^j \oplus Y_4^j = P^i \oplus C^i$ in L_1. For each match, store the value $(Y_1^j, P^i \oplus X_1^j)$ in list L_2.

(3) For each internal state X_2^l, assume that $X_2^l = Y_3^l$, and calculate $Y_2^l = F_2(X_2^l)$ as well as $X_3^l = F_3^{-1}(Y_3^l)$. Then search the $Y_2^l \oplus X_3^l = P^i \oplus X_1^j$ in L_2. For each match, recover the $k_0 = Y_2^l \oplus X_3^l$ and $k_1 = Y_1^j \oplus X_2^l$.

According to Dinur *et al.* [6], given all $N = 2^n$ plaintext-ciphertext pairs, a high success probability can be guaranteed by the fixed-point properties based on birthday paradox. Since each plaintext P^i is known in the basic multibridge attack and each permutation is used for one pair of internal state, both data and time complexity is calculated as $O(2^n)$.

Improved Key Recovery Method: MB+

In this section we first analyze the fixed-point property and show that over 30 percent of the round keys are actually invalid keys in the original multibridge attack. In order to reduce the invalid-key set of multibridge attack, we present a noval MB+ attack for 4-round-2-key Even-Mansour scheme.

Analysis of fixed-point property. The basic multibridge attack assumes that the fixed point may appear with a probability of 2^{-n}. Hence, according to the birthday paradox, 2^n of plaintexts are required to upgrade the success probability close to 1. As an important property, the fixed point holds $X_4 = Y_1$ and $X_2 = Y_3$.

Inspired by the fixed-point property, hereby we prove the observation that the multibridge attack cannot recover all the round-keys. We define the round key which can not be recovered by multibridge attack as the *invalid key*. Since the 4-round Evem-Mansour scheme holds that $Y_2 = F_2(X_2)$ and $Y_3 = F_3(X_3)$, thus using the fixed-point property $X_2 = Y_3$, we have $k_0 = Y_2 \oplus X_3 = F_2(X_2) \oplus X_3 = F_2(Y_3) \oplus X_3 = F_2(F_3(X_3)) \oplus X_3$. If we set $F_2 \circ F_3(\cdot) = G(\cdot)$, then we get:

$$k_0 = G(X_3) \oplus X_3 := H(X_3). \tag{3}$$

Equation (3) shows that if there are fixed-points, k_0 can be calculated by the internal state X_3. Both F_2 and F_3 are permutations, so G is also a permutation. Yet, H can only be regarded as a function, which means the distribution of recovered k_0 depends on a function rather than a permutation.

We further assume that H is a random function, thereby the distribution of H's image k_0 will obey a Poisson distribution with an expectation λ. For a given parameter t, the probability that arbitrary image $k_0 = k$ occurs t times will be $Pr[T(k) = t] = (\lambda^t e^{-\lambda})/t!$. Since the number of plaintexts is $N = 2^n$, the expectation goes to $\lambda = N/(2^n) = 1$.

For all the choice of X_3, there exist images of $k_0 = k'$ satisfying $T(k') = 0$, which means that none of the X_3 has image k'. We call the set of such images as *invalid-key set*, and the number of invalid keys as $2^n \times Pr[T(k') = 0] = 2^n e^{-1}$. The probability shows that there are $1/e$ (> 30%) of the round keys belonging to the invalid-key set, which cannot be recovered by the multibridge attack.

Given k', and if there exists an internal state X' satisfying $k' = H(X')$, it shows that the 4-round Even-Mansour scheme with $k_0 = k'$ holds $X_2 = Y_3$ as the fixed-point property with $X_3 = X'$. Otherwise, if none of the internal state X' satisfies $k' = H(X')$ for a given k', the 4-round Even-Mansour scheme (with $k_0 = k'$) has no fixed point for each plaintext, the multibridge attack will not recover the round key k'.

The MB+ attack. The original multibridge attack can not recover the invalid keys. Since all the plaintext have been used in the multibridge attack, there is no data complexity left to improve the attack performance.

The fixed-point property used in multibridge attack is $X_2 = Y_3$, which fixed the construction of H. We propose MB+ to enable better attacking performance by introducing parameters as $X_2 = Y_3 \oplus \delta$, where δ has a size of n-bits and d equals to $|\delta|$. Each δ constructs an independent function H that enables different distributions of recovered key k_0. The number of invalid keys will be reduced by $2^n \times Pr[T(k') = 0]^d = 2^n e^{-d}$.

For example, if $d = 5$, then:

$$Pr^d[T(k') = 0] = e^{-5} < 1\%, \tag{4}$$

which means the number of invalid keys is lower than 1%. Consequently, MB+ provides a significantly better performance compared to the basic multibridge attack.

Method Evaluation

We experimentally confirm the effectiveness of MB+ in this section. We select 3 well-known block ciphers Camellia, CLEFIA, and SMS4, and test the ratio of invalid keys with a differentiating d (namely the number of δ, specified in the above section). The result is shown in Table 1.

As with our evaluation, only a slight change of d will dramatically decrease the ratio of invalid keys. For instance, when $d = 1$, the failure cases make up 36.33% of the entire cases. Nevertheless, when d rises to 5, a 99.22% successful rate is achieved by our proposal. Hence, MB+ provides an effective way of making the key recovery attack against EM schemes.

Table 1: The ratio of invalid keys with various queries in MB+ approach. Block ciphers are chosen using Camellia, CLEFIA, and SMS4.

	Camellia [3]	CLEFIA [4]	SMS4 [5]
d=1	36.33%	36.72%	33.98%
d=2	14.84%	13.67%	12.11%
d=3	4.30%	4.30%	5.86%
d=4	2.34%	1.56%	1.95%
d=5	0.78%	0.39%	0.39%

Related Work

The academic discussion of Even-Mansour scheme [1, 2] can be typically divided into two directions. One direction focuses on the security of EM schemes under certain application scenarios [7, 8]. For the other direction, people aims at constructing a distinguisher for key recovery attacks, with a varying numbers of encryption rounds and the collision pairs.

In 1991, Daemen [9] presented the first EM-based attack using the differential characteristics of permutation. Later, Biryukov and Wagner [10] proposed a slide attack which was further improved in 2005 [11]. Such slide attacks leverage the internal self-similarity of the encryption algorithms, and provide a new approach for the key recovery attack on EM schemes [2]. In 2012, Dinur [6] performed a sophisticated slide attack on the EM scheme. Then, Dinur and Nikolić [12, 13] improved the method with higher attacking rounds, achieving lower key recovery complexity. Note that the above approaches are able to disclose correct keys, yet invalid keys will also appear with a certain probability. Such issue is considered systematically in this paper.

Conclusion

In this paper, we present MB+, an enhanced multibridge attack on Even-Mansour schemes. We first present the concept of invalid-key set in multibridge attacks and in depth prove the high correlation between failure cases and the invalid keys. After analyzing the properties of the fixed points, we show that the basic multibridge has an inherent probability over 30% that leads to the disclosed keys to be invalid. In comparison, MB+ achieves significantly effective performance. Our result is further verified through a comprehensive evaluation based on well-known block ciphers.

References

[1] S. Even and Y. Mansour, A Construction of a Cipher from a Single Pseudorandom Permutation. Journal of Cryptology 10.3 (1997): 151-161.

[2] O. Dunkelman, N. Keller, and A. Shamir, Minimalism in Cryptography: The Even-Mansour Scheme Revisited. Advances in Cryptology–EUROCRYPT 2012. Springer Berlin Heidelberg, 2012. 336-354.

[3] M. Matsui, S. Moriai, and J. Nakajima, A Description of the Camellia Encryption Algorithm. RFC 3713, 2004.

[4] T. Shirai, K. Shibutani, T. Akishita, S. Moriai, and T. Iwata, The 128-Bit Blockcipher CLEFIA. In Fast Software Encryption. Springer Berlin Heidelberg, 2007. 181-195.

[5] F. Liu, W. Ji, L. Hu, J. Ding, S. Lv, A. Pyshkin, and R.P. Weinmann, Analysis of the SMS4 block cipher. In Information Security and Privacy. Springer Berlin Heidelberg, 2007. 158-170.

[6] I. Dinur, O. Dunkelman, N. Keller, and A. Shamir, Cryptanalysis of Iterated Even-Mansour Schemes with Two Keys. Advances in Cryptology–ASIACRYPT 2014. Springer Berlin Heidelberg, 2014. 439-457.

[7] S. Chen., R. Lampe, J. Lee, Y. Seurin, and J. Steinberger, Minimizing the Two-Round Even-Mansour Cipher. In Advances in Cryptology–CRYPTO 2014. Springer Berlin Heidelberg, 2014. 39-56.

[8] C. Shan, and J. Steinberger, Tight Security Bounds for Key-Alternating Ciphers. Advances in Cryptology–EUROCRYPT 2014. Springer Berlin Heidelberg, 2014. 327-350.

[9] J. Daemen, Limitations of the Even-Mansour Construction. Advances in Cryptology—ASIACRYPT'91. Springer Berlin Heidelberg, 1993. 495-498.

[10] A. Biryukov, and D. Wagner, Slide Attacks. In Fast Software Encryption. Springer Berlin Heidelberg, 1999. 245-259.

[11] A. Biryukov, and D. Wagner, Advanced Slide Attacks, Advances in Cryptology—EUROCRYPT 2000. Springer Berlin Heidelberg, 2000. 589-606.

[12] I. Dinur, O. Dunkelman, N. Keller, and A. Shamir, Key Recovery Attacks on 3-round Even-Mansour, 8-step LED-128, and Full AES2. Advances in Cryptology-ASIACRYPT 2013. Springer Berlin Heidelberg, 2013. 337-356.

[13] I. Nikolić, W. Lei, and W. Shuang, Cryptanalysis of Round-Reduced LED. In Fast Software Encryption. Springer Berlin Heidelberg, 2014. 112-129.