# Simplification on Even-Mansour Scheme Attacks

HongTae Kim*

## 요 약

Block cipher is one of the prominent and important elements in cryptographic systems and study on the minimal construction is a major theme in the cryptographic research. Even and Mansour motivated by the study suggested a kind of block cipher called the Even-Mansour scheme in the early 1990s. It is a very simple cipher with one permutation and two secret keys. There have been many studies on the Even-Mansour scheme and security analysis of the scheme. We explain the Even-Mansour scheme and simplify those attacks on the Even-Mansour scheme with mathematical language. Additionally, we show that Pollard's rho attack to the discrete logarithm problem can be used to attack the Even-Mansour scheme with the same complexity of the Pollard's rho attack.

# Even-Mansour 스킴 공격방법의 간략화

김 홍 태*

## ABSTRACT

블록암호는 암호시스템 중에서 두드러지면서 중요한 부분이며, 최소의 구조를 갖는 것에 관한 연구는 암호학 연구에서 주요한 주제 중의 하나이다. 최소의 구조에 관해 관심을 갖던 Even과 Mansour는 1990년대 초반에 Even-Mansour 스킴이라고 불리는 일종의 블록암호를 제안하였다. Even-Mansour 스킴은 하나의 치환과 두 개의 비밀키를 가지는 매우 간단한 암호이다. 이러한 Even-Mansour 스킴과 그의 안전성 분석에 관한 많은 연구들이 이루어져 왔다. 우리는 Even-Mansour 스킴을 설명하고 이 스킴의 공격방법에 대해 수학적인 언어를 이용하여 단순화한다. 추가적으로, 우리는 이산로그를 공격할 때 사용하는 Pollard rho 공격과 동일한 계산량으로 Pollard rho 공격을 Even-Mansour 스킴의 공격에 적용할 수 있음을 보인다.

Key words : Block cipher, Minimal construction, Even-Mansour scheme, Security analysis,

Pollard's rho attack, Complexity

접수일(2016년 8월 22일), 수정일(1차: 2016년 10월 7일),
수정일(2차: 2016년 12월 14일),
게재확정일(2016년 12월 22일)

* 공군사관학교/기초과학과

# 1. Introduction

Block cipher is a cryptographic primitive to encrypt and decrypt messages applying Shannon's information theory [25]. DES(Data Encryption Standard) is a kind of block cipher with a Feistel-like structure and is the most well-known element. It was standardized for the United States in November 1976 [17]. DES was considered to be insecure [6, 22, 23, 3, 4] and a new block cipher called AES(Advanced Encryption Standard) was standardized for the United States in May 2002 [18]. And there have been proposed many block ciphers such as IDEA, MISTY, Camellia, KASUMI and ARIA [21, 24, 2, 26, 20].

Even and Mansour suggested a kind of much simpler block cipher called the Even-Mansour scheme in 1991 [15, 16]. It has very simple structure with a publicly known permutation and two secret keys, a prewhitening key and a postwhitening key, respectively. Daemen attacked their scheme using a CPA(Chosen Plaintext Attack) in 1991 [10]. After that, Biryukov and Wagner suggested a KPA(Known Plaintext Attack) in 2000 [7]. Dunkelman, Keller and Shamir improved the complexity of the Biryukov and Wagner's attack using a KPA in 2012 [13]. Lately, there were presented studies on the generalization of the Even-Mansour scheme and security analysis on those schemes [1, 5, 8, 9, 11, 12, 14, 19].

We analyze these attacks on the Even-Mansour scheme and reinterpret them with different approaches against the original attacks. We formalize those attacks with mathematical language and compare those attacks with each other.

The remainder of this paper is organized as follows. In Section 2, we introduce the Even-Mansour scheme. In Section 3, we simplify attacks on the Even-Mansour scheme and compare them with each other. We introduce an open problem additionally. We conclude in Section 4.

# 2. The Even-Mansour scheme

The Even-Mansour scheme $E: F_{2^n} \rightarrow F_{2^n}$ we consider is given as follows [15, 16]:

$$E(P) = F(P \oplus k_1) \oplus k_2 \qquad (1)$$

where $F_{2^n}$: finite field of order $2^n$, $k_1, k_2$: $n$-bit keys, $F$: bijection in $F_{2^n}$, $P$: $n$-bit plaintext and $\oplus$: addition in a field $F_{2^n}$ (i. e. $\oplus$ is equivalent to exclusive OR operation). We call $k_1$ a prewhitening key and $k_2$ a postwhitening key.

Data complexity is the number of queries to the $E$-oracle and queries to the $E^{-1}$-oracle. Let $D$ be the data complexity. Time complexity is the number of queries to the $F$-oracle and queries to the $F^{-1}$-oracle. Let $T$ be the time complexity. The $E$-oracle returns $E(P)$ for a given message $P \in F_{2^n}$ and the $F$-oracle returns $F(x)$ for a given input $x \in F_{2^n}$. The other oracles return each value similarly. Let $M$ be the memory and $N = 2^n$.

## 3. Simplification of attacks on the Even-Mansour scheme

There have been proposed many papers on attacks of the Even-Mansour scheme. Joan Daemen attacked the Even-Mansour scheme in the paper 'Limitations of the Even-Mansour Construction' at Asiacrypt 1991 [10]. He used a CPA. Alex Biryukov and David Wagner improved Joan Daemen's result in the paper 'Advanced Slide Attacks' at Eurocrypt 2000 [7]. They made a KPA providing fixed complexity and fixed memory according to plaintext size. Orr Dunkelman, Nathan Keller and Adi Shamir presented another KPA with flexible complexity and flexible memory according to plaintext size in the paper 'Minimalism in Cryptography: The Even-Mansour Scheme Revisited' at Eurocrypt 2012 [13]. We simplify all these attacks on the Even-Mansour scheme and apply Pollard's rho attack to this scheme.

### 3.1 Guess and determine

We can attack the Even-Mansour scheme with a trivial method. After we guess a prewhitening key $k_1$, we get the postwhitening key $k_2 = C_1 \oplus F(P_1 \oplus k_1)$ using the first key $k_1$, a pair $(P_1, C_1)$ and $F(P_1 \oplus k_1)$ where $C_1 = E(P_1)$ for some $P_1 \in F_{2^n}$. We can check the correctness of the guessing key $k_1$ and the subsequent key $k_2$ using the other pair $(P_2, C_2)$ where $E(P_2) = F(P_2 \oplus k_1) \oplus k_2$. If we guess all keys in $F_{2^n}$, we get the proper key. The method is given as Algorithm 1:

**Algorithm 1** Guess and Determine

```
1. For arbitrary $P_1, P_2 (P_1 \neq P_2) \in F_{2^n}$,
   get $C_1 = E(P_1)$ and $C_2 = E(P_2)$.
2. For $i = 1, 2, \cdots, N$, do the following:
   1) Guess $k_1 \in F_{2^n}$.
   2) Calculate $k_2 \in F_{2^n}$ such that
      $k_2 = C_1 \oplus F(P_1 \oplus k_1)$.
   3) Check guessing keys $k_1, k_2$ for
      $C_2 = F(P_2 \oplus k_1) \oplus k_2$ with $C_2 = E(P_2)$.
```

Complexity and memory are given as follows.

| **Complexity** and **Memory** |
|---|
| $D$: $O(1)$, $T$: $O(N)$, $M$: $O(1)$ |

In the above method, both $D$ and $M$ are given $O(1)$. But this is not an applicable attack because $T$ is given $O(N)$. If $n = 80$, the Even-Mansour scheme is secure against this attack.

### 3.2 Differential cryptanalysis

We can find keys $k_1, k_2$ as follows:

Define a new element $\varDelta E(P) = E(P \oplus \triangle) \oplus E(P)$ for some $P, \triangle \in F_{2^n}$. Then we get $\varDelta E(P) = F(P \oplus \triangle \oplus k_1) \oplus F(P \oplus k_1) = \varDelta F(P \oplus k_1)$ where $\varDelta F(P) = F(P \oplus \triangle) \oplus F(P)$. We can use this property to get correct keys $k_1, k_2$ after defining two sets, $S_{\varDelta E}$ and $S_{\varDelta F}$, respectively.

We need two sets about $\varDelta E(P)$ and $\varDelta F(P)$, respectively. Define a set $S_{\Delta E}=\{\Delta E(P_i)|P_i\in F_{2^n}, i=1,2,\cdots,2^d\}$ and a set $S_{\Delta F}=\{\Delta F(P_i)|P_i\in F_{2^n}, i=1,2,\cdots,2^{n-d}\}$, respectively. Then we can find $P_i(\in F_{2^n})$ in the set $S_{\Delta E}$ and $P_j(\in F_{2^n})$ in the set $S_{\Delta F}$ such that $\Delta E(P_i)=\Delta F(P_j)$. In this case, we get the key $k_1=P_i\oplus P_j$ with a high probability. The concrete method is given as Algorithm 2:

**Algorithm 2** Differential cryptanalysis

```
1. For arbitrary $P\in F_{2^n}$, get $C=E(P)$.
2. For $i=1,2,\cdots,2^d$, get $\Delta E(P_i)$ and store
   $(P_i, \Delta E(P_i))$ in Tab 1 after sorting $\Delta E(P_i)$.
3. For $i=1,2,\cdots,2^{n-d}$, get $\Delta F(P_i)$ and
   compare it with the Tab 1.
4. For each collision with $\Delta E(P_i)=\Delta F(P_j)$,
   check the guess $k_1=P_i\oplus P_j$ and
   $k_2=\Delta E(P_i)\oplus\Delta F(P_j)$ for
   $C=F(P\oplus k_1)\oplus k_2$ with $C=E(P)$.
```

Using the above method, we can attack the Even-Mansour scheme with the following complexity and memory.

**Complexity** and **Memory**

$D$: $O(2^d)$, $T$: $O(2^{n-d})$, $M$: $O(min\{2^d,2^{n-d}\})$

### 3.3 Advanced slide attack

We can find keys $k_1,k_2$ as follows:

We know that $E(P_1)\oplus F(P_2\oplus\triangle)=E(P_2)\oplus F(P_1\oplus\triangle)$ where $P_1\oplus P_2=k_1\oplus\triangle$ for some $P_1,P_2,\triangle\in F_{2^n}$. Define $x=P_1, y=P_2\oplus\triangle$. Then we get $E(x)\oplus F(y)=E(y\oplus\triangle)\oplus F(x\oplus\triangle)$. Let $c=x\oplus y\oplus\triangle$. Then we get $E(x)\oplus F(y)=E(x\oplus c)\oplus F(y\oplus c)$. We can use this property to get correct keys $k_1,k_2$.

Define $G(x,y)=E(x)\oplus F(y)$. From the above fact, $G(x,y)=G(x\oplus c,y\oplus c)$. Define $S_{G(x,y)}=\{G(x\oplus i,y\oplus i)|x,y\in F_{2^n},i=0,1,\cdots,\sqrt{N}\}$. Then we can find $(x_i,y_i),(x_j,y_j)$ such that $G(x_i,y_i)=G(x_j,y_j)$ where $(x_i,y_i)=(x\oplus i,y\oplus i)$. In this case, we get the key $k_1=x_i\oplus y_i$ with a high probability from $k_1=x_i\oplus x_j\oplus\triangle=c\oplus\triangle=x_i\oplus y_i$. We can attack the Even-Mansour scheme with the following complexity and memory.

**Complexity** and **Memory**

$D$: $O(\sqrt{N})$, $T$: $O(\sqrt{N})$, $M$: $O(\sqrt{N})$

In fact, this method doesn't give a trade-off between $D$ and $T$ owing to the function $G(x,y)$.

### 3.4 Slidex attack

The slidex attack is an improved method of the advanced slide attack. We can find key using the original slidex attack as Algorithm 3 [13]:

**Algorithm 3** Advanced slide attack

```
1. For $i=1,2,\cdots,2^d$, get $\Delta E(P_i)$.
2. For $l=1,2,\cdots,2^{n-d}$, choose $\Delta_l$ and
   do the following:
    1) Get $F(P_i\oplus\triangle_l)_{i=1,2,\cdots,2^d}$.
    2) Store $(P_{i,}E(P_i)\oplus F(P_i\oplus\triangle_l))$ after
       sorting $E(P_i)\oplus F(P_i\oplus\triangle_l)$.
3. Search for a collision such that
   $E(P_i)\oplus F(P_i\oplus\triangle_l)=E(P_j)\oplus F(P_j\oplus\triangle_l)$
   and check the guess $k_1=P_i\oplus P_j\oplus\triangle_l$,
   $k_2=E(P_i)\oplus F(P_j\oplus\triangle_l)$ for
   $C_1=F(P_1\oplus k_1)\oplus k_2$ with $C_1=E(P_1)$.
```

Then we can attack the Even-Mansour scheme with the following complexity and memory.

**Complexity** and **Memory**

$D$: $O(2^d)$, $T$: $O(2^{n-d})$, $M$: $O(min\{2^d,2^{n-d}\})$

### 3.5 Pollard's rho attack

Pollard's rho attack is a probabilistic method. We can find keys $k_1,k_2$ as follows:

Choose arbitrary elements $x_0,y_0\in F_{2^n}$ and let $c=x_0\oplus y_0$. Define $G(x,y)=E(x)\oplus F(y)$. Define an element $(x_{i+1},y_{i+1})=(G(x_i,y_i),G(x_i,y_i)\oplus c)$ for an integer $i\geq 0$. Then we can find a pair $(z_i,z_{2i+1})$ for $z_i=G(x_i,y_i)$ with a high probability in the following pairs:

$\{(z_0,z_1),(z_1,z_3),\cdots,(z_{\sqrt{N}},z_{2\sqrt{N}+1})\}$

We can attack the Even-Mansour scheme with the following complexity and memory.

**Complexity** and **Memory**

$D$: $O(\sqrt{N})$, $T$: $O(\sqrt{N})$, $M$: $O(1)$

### 3.6 Comparison and open problem

Table 1 gives the result on attacks of the Even-Mansour scheme. According to Table 1, we can attack the Even-Mansour scheme with flexible number of known plaintexts using the Slidex attack. Pollard's rho attack is a randomized attack with a negligible amount of storage. To make any attack on the Even-Mansour scheme feasible, $D$ must be sufficiently small size. Therefore we can ask the following question:

Is there any attack with $D\ll O(\sqrt{N})$ satisfying $DT=O(N)$, $M=O(1)$ (except "Guess and Determine")?

<Table 1> Comparison of attacks on the Even-Mansour scheme

| Attack | $D$ | $T$ | $M$ | Attack model |
|---|---|---|---|---|
| Guess & Determine | $O(1)$ | $O(N)$ | $O(1)$ | KPA |
| Differential | $O(2^d)$ | $O(2^{n-d})$ | $O(min\{2^{\mathrm{d}},2^{n-d}\})$ | CPA |
| Slide | $O(\sqrt{N})$ | $O(\sqrt{N})$ | $O(\sqrt{N})$ | KPA |
| Slidex | $O(2^d)$ | $O(2^{n-d})$ | $O(min\{2^{\mathrm{d}},2^{n-d}\})$ | KPA |
| Pollard | $O(\sqrt{N})$ | $O(\sqrt{N})$ | $O(1)$ | adaptive CPA |

## 4. Conclusion

There have been presented studies on the Even-Mansour scheme and generalization of the Even-Mansour scheme. We introduced the Even-Mansour scheme and simplified attacks on the scheme. We can get the essential principle of attack on the Even-Mansour scheme after simplifying attacks with mathematical language. Additionally, we applied Pollard's rho attack to the scheme. We were able to attack the Even-Mansour scheme with the same complexity of Pollard's rho attack on the discrete logarithm problem. It would be interesting to find a method with feasible implementation of the Even-Mansour scheme and to find an attack with $D \ll O(\sqrt{N})$ for $DT = O(N)$, $M = O(1)$.

## References

[1] E. Andreeva, A. Bogdanov, Y. Dodis, B. Mennink and J. P. Steinberger, "On the Indifferentiability of Key-Alternating Ciphers", Advances in Cryptology – CRYPTO 2013, LNCS Vol. 8042, pp. 531-550, 2013.

[2] K. Aoki, T. Ichikawa, M. Kanda, M. Matsui, S. Moriai, J. Nakajima and T. Tokita, "Specification of Camellia – a 128-bit Block Cipher", http://info.isl.ntt.co.jp/camellia/, 2000.

[3] E. Biham and A. Biryukov, "An Improvement of Davies' Attack on DES", Journal of Cryptology, Vol. 10, No. 3, pp. 195-206, 1997.

[4] E. Biham, O. Dunkelman and N. Keller, "Enhancing Differential-Linear Cryptanalysis", Advances in Cryptology-ASIACRYPT 2002, LNCS Vol. 2501, pp. 254-266, 2002.

[5] E. Biham and A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystems", Advances in Cryptology – CRYPTO 1990, LNCS Vol. 537, pp. 2-21, 1990.

[6] A. Biryukov and D. Wagner, "Advanced Slide Attacks", Advances in Cryptology – EUROCRYPT 2000, LNCS Vol. 1807, pp. 589-606, 2000.

[7] A. Bogdanov, L. R. Knudsen, G. Leander, F. Standaert, J. Steinberger and E. Tischhauser, "Key-Alternating Ciphers in a Provable Setting: Encryption Using a Small Number of Public Permutations", Advances in Cryptology – EUROCRYPT 2012, LNCS Vol. 7237, pp. 45-62, 2012.

[8] S. Chen, R. Lampe, J. Lee, Y. Seurin and J. P. Steinberger, "Minimizing the two-round Even-Mansour cipher", Advances in Cryptology – CRYPTO 2014, LNCS Vol. 8616, pp. 39-56, 2014.

[9] S. Chen and J. P. Steinberger, "Tight Security Bounds for Key-Alternating Ciphers", Advances in Cryptology – EUROCRYPT 2014, LNCS Vol. 8441, pp. 327-350, 2014.

[10] J. Daemen, "Limitations of the Even-Mansour Construction", Advances in Cryptology – ASIACRYPT 1991, LNCS Vol. 739, pp. 495-498, 1993.

[11] Y. Dai, J. Lee, B. Mennink and J. P. Steinberger, "The Security of Multiple Encryption in the Ideal Cipher Model", Advances in Cryptology – CRYPTO 2014, LNCS Vol. 8616, pp. 20-38, 2014.

[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, LNCS Vol. 8269, pp. 337-356, 2013.

[13] I. Dinur, O. Dunkelman, N. Keller and A. Shamir, "Cryptanalysis of Iterated Even-Mansour Schemes with Two Keys", Advances in Cryptology – ASIACRYPT 2014, LNCS Vol. 8873, pp. 439-457, 2014.

[14] O. Dunkelman, N. Keller and A. Shamir, "Minimalism in Cryptography: The Even-Mansour Scheme Revisited", Advances in Cryptology – EUROCRYPT 2012, LNCS Vol. 7237, pp. 336-354, 2012.

[15] S. Even and Y. Mansour, "A Construction of a Cipher from a Single Pseudorandom Permutation",

Advances in Cryptology - ASIACRYPT 1991, LNCS Vol. 739, pp. 210-224, 1993.

[16] S. Even and Y. Mansour, "A Construction of a Cipher from a Single Pseudorandom Permutation", Journal of Cryptology, Vol. 10, No. 3, pp. 151-162, 1997.

[17] FIPS PUB 46: Data Encryption Standard (DES). National Institute of Standards and Technology, 1977.

[18] FIPS PUB 197: Advanced Encryption Standard (AES). National Institute of Standards and Technology, 2001.

[19] P. Gazi and S. Tessaro, "Efficient and Optimally Secure Key-Length Extension for Block Ciphers via Randomized Cascading", Advances in Cryptology - EUROCRYPT 2012, LNCS Vol. 7237, pp. 63-80, 2012.

[20] D. Kwon, J. Kim, S. Park, S. H. Sung, Y. Sohn, J. H. Song, Y. Yeom, E. J. Yoon, S. Lee, J. Lee, S. Chee, D. Han and J. Hong, "New Block Cipher: ARIA", ICISC 2003, LNCS Vol. 2971, pp. 432-445, 2003.

[21] X. Lai and J. L. Massey, "A Proposal for a New Block Encryption Standard", Advances in Cryptology - EUROCRYPT 1990, LNCS Vol. 473, pp. 389-404, 1991.

[22] M. Matsui, "Linear Cryptanalysis Method for DES Cipher", Advances in Cryptology - EUROCRYPT 1993, LNCS Vol. 765, pp. 386-397, 1993.

[23] M. Matsui, "The First Experimental Cryptanalysis of the Data Encryption Standard", Advances in Cryptology - CRYPTO 1994, LNCS Vol. 839, pp. 1-11, 1994.

[24] M. Matsui, "Block encryption algorithm MISTY", proceedings of Fast Software Encryption 1997, LNCS Vol. 1267, pp. 64-74, 1997.

[25] C. E. Shannon, "Communication theory of secrecy systems", Bell System Technical Journal, Vol. 28, pp. 656-715, 1949.

[26] 3rd Generation Partnership Project, Technical Specification Group Services and System Aspects, 3G Security, Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 2: KASUMI Specification, V3.1.1, 2001.

## [著者紹介]

김 홍 태 (HongTae Kim)
2003년 2월 서울대 수리과학부 학사
2006년 2월 서울대 수리과학부 석사
2013년 2월 서울대 수리과학부 박사
2013년 2월 ~ 현재 공군사관학교
기초과학과 수학교수
email : yeskafa@naver.com