Practical Attack on the Full MMB Block Cipher*

Keting Jia[1], Jiazhe Chen[2,3], Meiqin Wang[2,3], and Xiaoyun Wang[1,2,3,**]

[1] Institute for Advanced Study, Tsinghua University, Beijing 100084, China
{ktjia,xiaoyunwang}@mail.tsinghua.edu.cn

[2] Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, Jinan 250100, China
jiazhechen@mail.sdu.edu.cn, mqwang@sdu.edu.cn

[3] School of Mathematics, Shandong University, Jinan 250100, China

Abstract. Modular Multiplication based Block Cipher (MMB) is a block cipher designed by Daemen *et al.* as an alternative to the IDEA block cipher. In this paper, we give a practical sandwich attack on MMB with adaptively chosen plaintexts and ciphertexts. By constructing a 5-round sandwich distinguisher of the full 6-round MMB with probability 1, we recover the main key of MMB with text complexity 2^{40} and time complexity 2^{40} MMB encryptions. We also present a chosen plaintexts attack on the full MMB by employing the rectangle-like sandwich attack, which the complexity is $2^{66.5}$ texts, $2^{66.5}$ MMB encryptions and $2^{70.5}$ bytes of memory. In addition, we introduce an improved differential attack on MMB with 2^{96} chosen plaintexts, 2^{96} encryptions and 2^{66} bytes of memory. Especially, even if MMB is extended to 7 rounds, the improved differential attack is applicable with the same complexity as that of the full MMB.

Keywords: MMB block cipher, sandwich distinguisher, practical attack, differential attack.

1 Introduction

Modular Multiplication based Block Cipher (MMB) [7] was designed as an alternative to the IDEA block cipher [9] by Daemen, Govaerts and Vandewalle in 1993. It has 6 rounds, and both of the block size and key size are 128 bits. In [13], Wang *et al.* proposed a differential attack on the full 6-round MMB with 2^{118} chosen plaintexts, $2^{95.61}$ encryptions and 2^{66} bytes of memory. They also presented linear and square attacks on the reduced-round MMB.

Our main contribution to this paper is to introduce a fast sandwich attack on MMB. Sandwich attack was recently formalized by Dunkelman *et al.* [11], is

* Supported by 973 Project (No.2007CB807902), the National Natural Science Foundation of China (Grant No.60931160442), Tsinghua University Initiative Scientific Research Program (2009THZ01002) and China Postdoctoral Science Foundation(20110490442).

** Corresponding author.

A. Miri and S. Vaudenay (Eds.): SAC 2011, LNCS 7118, pp. 185–199, 2012.

aimed to improve the former theoretic related-key rectangle attack on the full KASUMI block cipher [3] into a fast attack. Sandwich attack is an extension of the boomerang attack, which was introduced by Wagner [14]. Similar cryptanalysis techniques with sandwich attack were also used in [4,5,14]. Usually, boomerang attack is an adaptively chosen plaintexts and ciphertexts attack. It was further developed by Kelsey *et al.* [6] into a chosen plaintexts attack called the amplified boomerang attack, which was independently introduced by Biham *et al.* with the name of the rectangle attack [2]. In [10], sandwich attack is also converted into a chosen plaintexts attack, called rectangle-like sandwich attack.

In this paper, we construct an interesting sandwich distinguisher of 5-round MMB with probability 1. Using the distinguisher, we present an adaptively chosen texts attack on MMB, which the complexity is 2^{40} texts and 2^{40} MMB encryptions. We also give a rectangle-like sandwich attack on MMB with $2^{66.5}$ chosen plaintexts, $2^{66.5}$ encryptions and $2^{70.5}$ bytes of memory.

Furthermore, we introduce a 6-round differential with probability 2^{-94}. Utilizing a 5-round differential by truncating the given 6-round differential, we show an improved differential attack on MMB with 2^{96} chosen plaintexts, 2^{96} MMB encryptions and 2^{66} bytes of memory. It is interesting that, even if MMB block cipher is increased to 7 rounds, it is still vulnerable to the differential attack with the same complexity.

The rest of this paper is organized as follows. A brief description of MMB is given in Sect. 2. We recall the sandwich attack in Sect. 3. The fast sandwich attack on MMB is introduced in Sect. 4. Section 5 describes the rectangle-like attack on MMB. And Section 6 shows the improved differential attack. Finally, we conclude the paper in Sect. 7.

2 Description of the Block Cipher MMB

MMB is a block cipher with 128-bit block and 128-bit key. It has a Substitution-Permutation Network (SPN) structure and 6-round iterations. It has two versions, called MMB 1.0 and MMB 2.0. Compared to MMB 1.0, the key schedule of MMB 2.0 is tweaked against the related-key attack [8]. In this paper, we only focus on MMB 2.0 which is simplified as MMB.

We give a brief description of MMB in the following.

Key Schedule. Let the 128-bit key of MMB be $K = (k_0, k_1, k_2, k_3)$, the subkey can be computed as:

$$k_i^j = k_{(i+j) \mod 4} \oplus (B \lll j),$$

where $B = 0x0dae$, k^j is the $(j+1)$-th round subkey, $k^j = (k_0^j, k_1^j, k_2^j, k_3^j)$, $k_i^j (i = 0, \ldots, 3)$ are 32-bit words, and $j = 0, \ldots, 6$.

MMB Encryption. MMB includes the following 6 round-transformations:

$$X_{j+1} = \rho[k^j](X_j) = \theta \circ \eta \circ \gamma \circ \sigma[k^j](X_j)$$

where X_j is the 128-bit input to the $(j+1)$-th round, and X_0 is the plaintext. The ciphertext is denoted as $C = \sigma[k^6](X_6)$.

The details of the four functions $\sigma, \gamma, \eta, \theta$ are given as follows.

1. $\sigma[k^j]$ is a bitwise XOR operation with the round subkey.

$$\sigma[k^j](a_0, a_1, a_2, a_3) = (a_0 \oplus k_0^j, a_1 \oplus k_1^j, a_2 \oplus k_2^j, a_3 \oplus k_3^j),$$

   where (a_0, a_1, a_2, a_3) is the 128-bit intermediate value, and $a_i (i = 0, 1, 2, 3)$ are 32-bit words.

2. The nonlinear transformation γ is a cyclic multiplication of the four 32-bit words respectively by factors G_0, G_1, G_2 and G_3.

$$\gamma(a_0, a_1, a_2, a_3) = (a_0 \otimes G_0, a_1 \otimes G_1, a_2 \otimes G_2, a_3 \otimes G_3).$$

   The cyclic multiplication $\otimes$ is defined as:

$$x \otimes y = \begin{cases} x \times y \mod 2^{32} - 1 & \text{if } x < 2^{32} - 1, \\ 2^{32} - 1 & \text{if } x = 2^{32} - 1. \end{cases}$$

   $G_i, G_i^{-1} = (G_i)^{-1} \; mod \; 2^{32} - 1, \; i = 0, 1, 2, 3$ are listed.

$$\begin{array}{ll} G_0 = 0x025f1cdb, & G_0^{-1} = 0x0dad4694, \\ G_1 = 2 \otimes G_0 = 0x04be39b6, & G_1^{-1} = 0x06d6a34a, \\ G_2 = 2^3 \otimes G_0 = 0x12f8e6d8, & G_2^{-1} = 0x81b5a8d2, \\ G_3 = 2^7 \otimes G_0 = 0x2f8e6d81, & G_3^{-1} = 0x281b5a8d. \end{array}$$

   There are two differential characteristics with probability 1 for G_i $(i = 0, 1, 2, 3)$ [7],

$$0 \xrightarrow[1]{G_i} 0, \quad \bar{0} \xrightarrow[1]{G_i} \bar{0}.$$

   The two differential characteristics result in a 2-round differential with probability 1.

3. The asymmetrical transformation η is defined as:

$$\eta(a_0, a_1, a_2, a_3) = (a_0 \oplus (lsb(a_0) \times \delta), a_1, a_2, a_3 \oplus ((1 \oplus lsb(a_3)) \times \delta)),$$

   where 'lsb' means the least significant bit and $\delta = 0x2aaaaaaa$.

4. The linear transformation θ is a diffusion operation:

$$\theta(a_0, a_1, a_2, a_3) = (a_3 \oplus a_0 \oplus a_1, a_0 \oplus a_1 \oplus a_2, a_1 \oplus a_2 \oplus a_3, a_2 \oplus a_3 \oplus a_0).$$

3 Sandwich Attack

Sandwich attack dates from boomerang attack, and was utilized to break efficiently the block cipher KASUMI in the related-key setting [10]. We give a brief description of the boomerang attack and the sandwich attack.

3.1 Boomerang Attack

The boomerang attack belongs to differential attack [1]. The purpose is to construct a quartet structure to achieve a distinguisher with more rounds by utilizing and connecting two short differential. Let E be a block cipher with block size n, that is considered as a cascade of two sub-ciphers: $E = E_1 \circ E_0$. For the sub-cipher E_0, there is a differential $\alpha \xrightarrow{E_0} \beta$ with high probability p, and for E_1, there is a differential $\gamma \xrightarrow{E_1} \zeta$ with high probability q. $E^{-1}, {E_0}^{-1}$ and ${E_1}^{-1}$ stand for the inverse of E, E_0, E_1 respectively. The boomerang distinguisher (see Fig.1) can be constructed as follows:

- Randomly choose a pair of plaintexts (P, P') such that $P' \oplus P = \alpha$.
- Ask for the encryption, and get the corresponding ciphertexts $C = E(P)$, $C' = E(P')$.
- Compute $\widetilde{C} = C \oplus \zeta$, $\widetilde{C}' = C' \oplus \zeta$.
- Ask for the decryption, and obtain $\widetilde{P} = E^{-1}(\widetilde{C})$, $\widetilde{P}' = E^{-1}(\widetilde{C}')$.
- Check whether $\widetilde{P}' \oplus \widetilde{P} = \alpha$.

For the distinguisher (see Fig. 1), $\widetilde{P}' \oplus \widetilde{P} = \alpha$ holds with probability p^2q^2. That is to say, a quarter satisfies the following conditions besides $P' \oplus P = \alpha$ and $\widetilde{P}' \oplus \widetilde{P} = \alpha$,

$$E_0(P') \oplus E_0(P) = \beta,$$
$${E_1}^{-1}(\widetilde{C}) \oplus {E_1}^{-1}(C) = E_1^{-1}(\widetilde{C}') \oplus {E_1}^{-1}(C') = \gamma.$$

It is clear that, the boomerang distinguisher is available to cryptanalyze a cipher if $pq > 2^{-n/2}$.

The rectangle (amplified boomerang) attack is a chosen plaintext attack instead of adaptive chosen plaintext and ciphertext attack by involving a birthday attack to guarantee the collision of two middle values $E_0(P)$ and $E_0(\widetilde{P}) \oplus \gamma$. A right quarter $(P, P', \widetilde{P}, \widetilde{P}')$ can be distinguished with probability $p^2q^22^{-n}$, which should satisfy the following conditions besides $P \oplus P' = \alpha$, $\widetilde{P} \oplus \widetilde{P}' = \alpha$, $C \oplus \widetilde{C} = \zeta$, $C' \oplus \widetilde{C}' = \zeta$,

$$E_0(P') \oplus E_0(P) = \beta \ , E_0(\widetilde{P}') \oplus E_0(\widetilde{P}) = \beta,$$
$$E_0(P) \oplus E_0(\widetilde{P}) = \gamma \ .$$

3.2 Sandwich Attack

The sandwich attack is obtained by pushing a middle layer in the quartet structure of the boomerang attack. So, in the sandwich attack, the block cipher should be divided into three sub-ciphers: $E = E_1 \circ E_M \circ E_0$, see Fig. 2. We denote $X = E_0(P), Y = E_M(X), C = E_1(Y)$. Let $\alpha \overset{E_0}{\to} \beta$ be a differential with probability p on the top layer, and $\gamma \overset{E_1}{\to} \zeta$ be a differential with probability q on the bottom layer, where

$$\alpha = P \oplus P' = \widetilde{P} \oplus \widetilde{P}' \ , \beta = X \oplus X' = \widetilde{X} \oplus \widetilde{X}'$$
$$\gamma = Y \oplus \widetilde{Y} = Y' \oplus \widetilde{Y}' \ , \zeta = C \oplus \widetilde{C} = C' \oplus \widetilde{C}'.$$

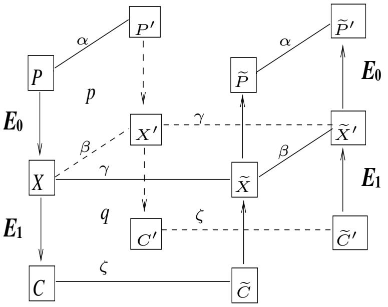

Fig. 1. Boomerange distinguisher

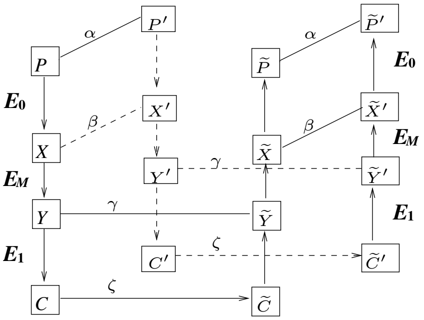

Fig. 2. Sandwich distinguisher

The middle layer is a transition differential connecting the top and bottom differentials. The probability of the transition differential is computed as follows.

$$r = Pr((\widetilde{X} \oplus \widetilde{X}' = \beta)|(Y \oplus \widetilde{Y} = \gamma) \wedge (Y' \oplus \widetilde{Y}' = \gamma) \wedge (X \oplus X' = \beta)).$$

Thus the sandwich distinguisher holds with probability p^2q^2r.

The rectangle-like sandwich attack is the combination of sandwich attack and rectangle attack, and it is a chosen plaintexts attack (see Fig. 4). The probability of the rectangle-like sandwich distinguisher is $p^2q^2r'2^{-n}$,

$$r' = Pr((Y' \oplus \widetilde{Y}' = \gamma)|(\widetilde{X} \oplus \widetilde{X}' = \beta) \wedge (X \oplus X' = \beta) \wedge (Y \oplus \widetilde{Y} = \gamma)).$$

4 Practical Sandwich Attack on the Full MMB

In this section, we first construct a sandwich distinguisher for 5-round MMB with probability 1 without related key, then give a practical key recovery attack on MMB.

4.1 5-Round Sandwich Distinguisher with Probability 1

We decompose 5-round MMB into $E = E_1 \circ E_M \circ E_0$. E_0 contains the first 2 rounds, E_M consists of the third round, and E_1 includes the last 2 rounds. See Fig. 2.

We use the following 2-round differential characteristic with probability 1 in E_0 and E_1 [13].

$$\begin{aligned}(0,\bar{0},\bar{0},0) &\xrightarrow{\sigma[k^i]} (0,\bar{0},\bar{0},0) \xrightarrow{\gamma} (0,\bar{0},\bar{0},0) \xrightarrow{\eta} (0,\bar{0},\bar{0},0) \xrightarrow{\theta} (\bar{0},0,0,\bar{0})\\ &\xrightarrow{\sigma[k^{i+1}]} (\bar{0},0,0,\bar{0}) \xrightarrow{\gamma} (\bar{0},0,0,\bar{0}) \xrightarrow{\eta} (\bar{0}\oplus\delta,0,0,\bar{0}\oplus\delta) \xrightarrow{\theta} (0,\bar{0}\oplus\delta,\bar{0}\oplus\delta,0),\end{aligned}$$

where '0' denotes a 32-bit zero difference word, and $\bar{0} = 2^{32} - 1 = 0xffffffff$. So $\alpha = \gamma = (0, \bar{0}, \bar{0}, 0)$, $\beta = \zeta = (0, \bar{0} \oplus \delta, \bar{0} \oplus \delta, 0)$, and $Pr(\alpha \xrightarrow{E_0} \beta) = 1$, $Pr(\gamma \xrightarrow{E_1} \zeta) = 1$.

The remaining is to prove that the probability of the transition differential keeps 1, i.e.,

$$Pr((\widetilde{X} \oplus \widetilde{X}' = \beta) | (Y \oplus \widetilde{Y} = \gamma) \wedge (Y' \oplus \widetilde{Y}' = \gamma) \wedge (X \oplus X' = \beta)) = 1.$$

X_i', $\widetilde{X}_i$, $\widetilde{X}_i'$ and X_i denote the i-th words of $X, X', \widetilde{X}, \widetilde{X}'$, $i = 0, 1, 2, 3$. The subkey of the third round is denoted as $\bar{k} = (\bar{k}_0, \bar{k}_1, \bar{k}_2, \bar{k}_3)$.

Since θ and η are linear, by

$$\begin{aligned} Y \oplus \widetilde{Y} &= (0, \bar{0}, \bar{0}, 0), \\ Y' \oplus \widetilde{Y}' &= (0, \bar{0}, \bar{0}, 0), \\ X \oplus X' &= (0, \bar{0} \oplus \delta, \bar{0} \oplus \delta, 0), \end{aligned} \tag{1}$$

we get

$$(\eta^{-1} \circ \theta^{-1}(Y)) \oplus (\eta^{-1} \circ \theta^{-1}(\widetilde{Y})) = (\bar{0} \oplus \delta, 0, 0, \bar{0} \oplus \delta), \tag{2}$$

$$(\eta^{-1} \circ \theta^{-1}(Y')) \oplus (\eta^{-1} \circ \theta^{-1}(\widetilde{Y}')) = (\bar{0} \oplus \delta, 0, 0, \bar{0} \oplus \delta). \tag{3}$$

From the round transformation, we know that,

$$\begin{aligned} Y &= \theta \circ \eta \circ \gamma \circ \sigma[k](X), \\ Y' &= \theta \circ \eta \circ \gamma \circ \sigma[k](X'), \\ \widetilde{Y} &= \theta \circ \eta \circ \gamma \circ \sigma[k](\widetilde{X}), \\ \widetilde{Y}' &= \theta \circ \eta \circ \gamma \circ \sigma[k](\widetilde{X}'). \end{aligned} \tag{4}$$

Using (2), (3) and (4), we deduce the equations

$$((X_1 \oplus \bar{k}_1) \otimes G_1) \oplus ((\widetilde{X}_1 \oplus \bar{k}_1) \otimes G_1) = 0, \tag{5}$$

$$((X_2 \oplus \bar{k}_2) \otimes G_2) \oplus ((\widetilde{X}_2 \oplus \bar{k}_2) \otimes G_2) = 0, \tag{6}$$

$$((X_1' \oplus \bar{k}_1) \otimes G_1) \oplus ((\widetilde{X}_1' \oplus \bar{k}_1) \otimes G_1) = 0, \tag{7}$$

$$((X_2' \oplus \bar{k}_2) \otimes G_2) \oplus ((\widetilde{X}_2' \oplus \bar{k}_2) \otimes G_2) = 0. \tag{8}$$

$$((X_0 \oplus \bar{k}_0) \otimes G_0) \oplus ((\widetilde{X}_0 \oplus \bar{k}_0) \otimes G_0) = \bar{0} \oplus \delta, \tag{9}$$

$$((X_3 \oplus \bar{k}_3) \otimes G_3) \oplus ((\widetilde{X}_3 \oplus \bar{k}_3) \otimes G_3) = \bar{0} \oplus \delta, \tag{10}$$

$$((X_0' \oplus \bar{k}_0) \otimes G_0) \oplus ((\widetilde{X}_0' \oplus \bar{k}_0) \otimes G_0) = \bar{0} \oplus \delta, \tag{11}$$

$$((X_3' \oplus \bar{k}_3) \otimes G_3) \oplus ((\widetilde{X}_3' \oplus \bar{k}_3) \otimes G_3) = \bar{0} \oplus \delta. \tag{12}$$

From (5), (6), (7) and (8), it is clear that,

$$X_1 = \widetilde{X}_1, \ X_2 = \widetilde{X}_2, \ X_1' = \widetilde{X}_1', \ X_2' = \widetilde{X}_2'.$$

Therefore, we deduce the conditions

$$\begin{aligned} \widetilde{X}_1 \oplus \widetilde{X}'_1 &= X_1 \oplus X'_1 = \bar{0} \oplus \delta, \\ \widetilde{X}_2 \oplus \widetilde{X}'_2 &= X_2 \oplus X'_2 = \bar{0} \oplus \delta. \end{aligned} \tag{13}$$

From (9), (10), (11) and (12), we obtain

$$((X_0 \oplus \bar{k}_0) \otimes G_0) \oplus ((\widetilde{X}_0 \oplus \bar{k}_0) \otimes G_0) = ((X'_0 \oplus \bar{k}_0) \otimes G_0) \oplus ((\widetilde{X}'_0 \oplus \bar{k}_0) \otimes G_0), \tag{14}$$

$$((X_3 \oplus \bar{k}_3) \otimes G_3) \oplus ((\widetilde{X}_3 \oplus \bar{k}_3) \otimes G_3) = ((X'_3 \oplus \bar{k}_3) \otimes G_3) \oplus ((\widetilde{X}'_3 \oplus \bar{k}_3) \otimes G_3). \tag{15}$$

Combining with (1), the following two equations hold.

$$\begin{aligned} ((\widetilde{X}_0 \oplus \bar{k}_0) \otimes G_0) &= ((\widetilde{X}'_0 \oplus \bar{k}_0) \otimes G_0), \\ ((\widetilde{X}_3 \oplus \bar{k}_3) \otimes G_3) &= ((\widetilde{X}'_3 \oplus \bar{k}_3) \otimes G_3). \end{aligned}$$

Then,

$$\begin{aligned} \widetilde{X}_0 \oplus \widetilde{X}'_0 &= 0, \\ \widetilde{X}_3 \oplus \widetilde{X}'_3 &= 0. \end{aligned} \tag{16}$$

Combining (13) and (16), we have

$$\widetilde{X} \oplus \widetilde{X}' = (0, \bar{0} \oplus \delta, \bar{0} \oplus \delta, 0) = \beta.$$

Therefore,

$$r = Pr((\widetilde{X} \oplus \widetilde{X}' = \beta) | (Y \oplus \widetilde{Y} = \gamma) \wedge (Y' \oplus \widetilde{Y}' = \gamma) \wedge (X \oplus X' = \beta)) = 1.$$

This proves that we get a 5-round sandwich distinguisher with probability 1.

4.2 The Key Recovery Attack

In this subsection, if we apply the 5-round sandwich distinguisher described in Subsect. 4.1 to rounds 2-6, we can recover 64 bits of the subkey in the first round. When we locate the distinguisher at rounds 1-5, 64 bits of the equivalent subkey in the final can be easily captured. The total key can be deduced from the recovered subkey bits by the key schedule.

Recovering 64 Bits of the First Round Subkey

Collecting Right Quartets. The sandwich distinguisher is from round 2 to round 6. In order to easily produce the sandwich distinguisher, we select the 1-st round differential as:

$$(0xfdff77ef, 0, 0, 0xdffbfeef) \xrightarrow{\sigma[k^i]} (0xfdff77ef, 0, 0, 0xdffbfeef) \xrightarrow{\gamma} \\ (\bar{0} \oplus \delta, 0, 0, \bar{0} \oplus \delta) \xrightarrow{\eta} (\bar{0}, 0, 0, \bar{0}) \xrightarrow{\theta} (0, \bar{0}, \bar{0}, 0).$$

By computer searching, both $0xfdff77ef \xrightarrow{G_0} \bar{0} \oplus \delta$ and $0xdffbfeef \xrightarrow{G_3} \bar{0} \oplus \delta$ occur with probability about 2^{-18}, so the probability of the differential is about 2^{-36}.

We collect 2^{38} plaintext pairs (P, P') and their corresponding ciphertext pairs (C, C'), where P and P' satisfy

$$P' = P \oplus (0xfdff77ef, 0, 0, 0xdffbfeef).$$

For each pair, we construct the quartet, and detect whether the quartet satisfies the differentials. The details are as follows.

- For the collected plaintext-ciphertext pair $((P, C), (P', C'))$, calculate

$$\widetilde{C} = C \oplus (0, \bar{0} \oplus \delta, \bar{0} \oplus \delta, 0),$$

$$\widetilde{C}' = C' \oplus (0, \bar{0} \oplus \delta, \bar{0} \oplus \delta, 0).$$

- Query the decryption to obtain $\widetilde{P} = E^{-1}(\widetilde{C})$, $\widetilde{P}' = E^{-1}(\widetilde{C}')$, and get the quartet $(P, P', \widetilde{P}, \widetilde{P}')$.
- For the constructed quartet $(P, P', \widetilde{P}, \widetilde{P}')$, check whether $\widetilde{P} \oplus \widetilde{P}' = (*, 0, 0, *)$ holds, where '*' stands for any non-zero 32-bit value. If $\widetilde{P} \oplus \widetilde{P}$ equals to $(*, 0, 0, *)$, output the quartet.

It is clear that, if the 1-st round differential holds, $\widetilde{P} \oplus \widetilde{P}'$ always equals to $(*, 0, 0, *)$, so among 2^{38} plaintext-ciphertext pairs $((P, C), (P', C'))$, there are about 4 quartets $(P, P', \widetilde{P}, \widetilde{P}')$ are left, and each sieved quartet is right with probability $1 - 2^{38-64} = 1 - 2^{-26}$.

Partial Key Recovery. For the right quartet $(P, P', \widetilde{P}, \widetilde{P}')$, we search the right subkey k_0^0 among 2^{32} candidates by the following equations:

$$((P_0 \oplus k_0^0) \otimes G_0) \oplus ((P_0' \oplus k_0^0) \otimes G_0) = \bar{0} \oplus \delta,$$
$$((\widetilde{P}_0 \oplus k_0^0) \otimes G_0) \oplus ((\widetilde{P}_0' \oplus k_0^0) \otimes G_0) = \bar{0} \oplus \delta.$$

Similarly, the subkey k_3^0 is derived from the equations

$$((P_3 \oplus k_3^0) \otimes G_3) \oplus ((P_3' \oplus k_3^0) \otimes G_3) = \bar{0} \oplus \delta,$$
$$((\widetilde{P}_3 \oplus k_3^0) \otimes G_3) \oplus ((\widetilde{P}_3' \oplus k_3^0) \otimes G_3) = \bar{0} \oplus \delta.$$

Because $\bar{0} \xrightarrow[1]{G_i} \bar{0}$, there are two k_0^0 can be obtained, i.e. the right subkey k_0^0 and its complement $k_0^0 \oplus \bar{0}$. It is the same for k_3^0.

Recovering 64 Bits of the Last Subkey

Collecting Right Quartets. We apply the distinguisher to rounds 1-5, and calculate 64 bits of the last subkey.

Select the final round differential

$$(0,\bar{0}\oplus\delta,\bar{0}\oplus\delta,0) \xleftarrow{\sigma^{-1}[k^5]} (0,\bar{0}\oplus\delta,\bar{0}\oplus\delta,0) \xleftarrow{\gamma^{-1}}$$
$$(0, 0xfcfbdfff, 0xf3ef7fff, 0) \xleftarrow{\eta^{-1}} (0, 0xfcfbdfff, 0xf3ef7fff, 0) \xleftarrow{\theta^{-1}}$$
$$(0xfcfbdfff, 0x0f14a000, 0x0f14a000, 0xf3ef7fff).$$

The probability of $0xfcfbdfff \xrightarrow{G_1^{-1}} \bar{0}\oplus\delta$ and $0xf3ef7fff \xrightarrow{G_2^{-1}} \bar{0}\oplus\delta$ are both 2^{-18}, so the total probability of the final round differential is 2^{-36}.

We collect 2^{38} ciphertext pairs $(C,\widetilde{C})$ and their corresponding plaintext pairs $(P,\widetilde{P})$ such that,

$$\widetilde{C} = C \oplus (0xfcfbdfff, 0x0f14a000, 0x0f14a000, 0xf3ef7fff).$$

For each pair, we build the framework of the quartet, and test whether the quartet satisfies the differential.

- For the collected plaintext-ciphertext pair $((P,C),(\widetilde{P},\widetilde{C}))$, calculate
$$P' = P \oplus (0,\bar{0},\bar{0},0),$$
$$\widetilde{P}' = P' \oplus (0,\bar{0},\bar{0},0).$$
- Ask for the ciphertexts C', $\widetilde{C}'$ of P', $\widetilde{P}'$ respectively. We obtain the quartet $(C,C',\widetilde{C},\widetilde{C}')$.
- For the collected quartet $(C,C',\widetilde{C},\widetilde{C}')$, check whether C' and $\widetilde{C}'$ satisfy the following equation.
$$C' \oplus \widetilde{C}' = (V_1, V_1\oplus V_2, V_1\oplus V_2, V_2),$$
where V_1, V_2 are non-zero 32-bit words. If the equation holds, output the quartet.

Partial Key Recovery. We firstly recover 64 bits of the equivalent key $k^{6'}$ of k^6, i.e.,

$$k_1^{6'} = k_0^6 \oplus k_1^6 \oplus k_2^6,$$
$$k_2^{6'} = k_1^6 \oplus k_2^6 \oplus k_3^6.$$

We find the right subkey $k_1^{6'}$ by searching 2^{32} candidates with the verification of the equations

$$(G_1^{-1}\otimes(C_0\oplus C_1\oplus C_2\oplus k_1^{6'}))\oplus(G_1^{-1}\otimes(C_0'\oplus C_1'\oplus C_2'\oplus k_1^{6'})) = \bar{0}\oplus\delta,$$
$$(G_1^{-1}\otimes(\widetilde{C}_0\oplus \widetilde{C}_1\oplus \widetilde{C}_2\oplus k_1^{6'}))\oplus(G_1^{-1}\otimes(\widetilde{C}_0'\oplus \widetilde{C}_1'\oplus \widetilde{C}_2'\oplus k_1^{6'})) = \bar{0}\oplus\delta.$$

In the similar way, we search the right subkey $k_2^{6'}$ among 2^{32} candidates by the following equations.

$$(G_2^{-1}\otimes(C_1\oplus C_2\oplus C_3\oplus k_2^{6'}))\oplus(G_2^{-1}\otimes(C_1'\oplus C_2'\oplus C_3'\oplus k_2^{6'})) = \bar{0}\oplus\delta,$$
$$(G_2^{-1}\otimes(\widetilde{C}_1\oplus \widetilde{C}_2\oplus \widetilde{C}_3\oplus k_2^{6'}))\oplus(G_2^{-1}\otimes(\widetilde{C}_1'\oplus \widetilde{C}_2'\oplus \widetilde{C}_3'\oplus k_2^{6'})) = \bar{0}\oplus\delta.$$

From the key schedule algorithm, we know that, k_0^0=$k_0 \oplus B$, $k_3^0 = k_3 \oplus B$, $k_1^{6'} = k_0 \oplus k_2 \oplus k_3 \oplus (B \lll 6)$, and $k_2^{6'} = k_0 \oplus k_1 \oplus k_3 \oplus (B \lll 6)$. As a result, we compute the whole 128 bits of the key. $2^4 = 16$ key can be computed, for there are 2 values for a subkey. Filter the right key by a known plaintext and corresponding ciphertexts.

Complexity. The data complexity is 2^{39} adaptive chosen plaintexts and ciphertexts. The collection of the pairs is dominant the time complexity, which is 2^{40} MMB encryptions. Once a right quarter is obtained, the right subkey can be computed. So the success rate is $(0.98)^2 = 0.96$.

4.3 Experimental Results

We performed an experiment on the number of right quartets. We implement the quartet framework in Sect. 4.2, check the right quartets, and we repeated the procedure for 1320 times. The number of right quartet are given in Tab. 1, and we can see from Fig. 3 that the experimental data approximates well to the theoretic data.

Table 1. The Number of Right Quartets

#Right Quartets	0	1	2	3	4	5	6	7	8	9	10	11	12
Experiment	23	106	202	252	273	185	137	86	30	17	5	4	0
Theory	24.1	96.7	193.4	257.8	257.8	206.3	137.5	78.5	39.2	17.4	6.9	2.5	0.8

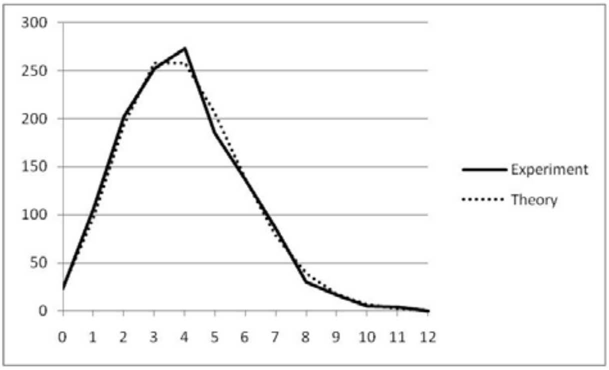

Fig. 3. The Number of Right Quartets in Our Experiment and the Theory

Our experiment was carried out on a IBM X3950 M2 server, with 64 Intel Xeon E7330 2.4GHz cores inside. The operation system is Red Hat 4.1.2-46, Linux 2.6.18. The compiler is gcc 4.1.2, and we use the standard optimization flags, one thread in each core. It takes about 1 hour to identify a right quartet, and recovery the main key of MMB.

5 Rectangle-Like Sandwich Attack on MMB

The sandwich attack is an adaptive chosen plaintexts and ciphertexts attack. So we have to query the decryptions of the adapted ciphertexts. This section is to fulfill the rectangle-like sandwich attack, which can result in a chosen-plaintext attack.

5.1 5-Round Rectangle-Like Sandwich Distinguisher

Firstly, we give a 5-round rectangle-like sandwich distinguisher which can be detected with the birthday attack complexity. We transform the above 5-round sandwich distinguisher into a rectangle-like sandwich distinguisher directly.

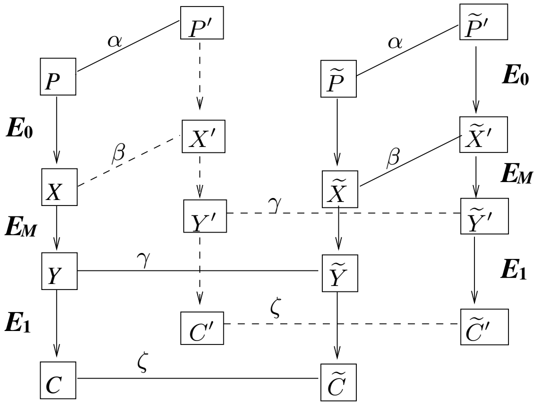

Fig. 4. Rectangle-like sandwich distinguisher

We decompose 5-round MMB into $E = E_1 \circ E_M \circ E_0$ the same as Subsect. 4.1. Let $\alpha = \gamma = (0, \bar{0}, \bar{0}, 0)$, $\beta = \zeta = (0, \bar{0} \oplus \delta, \bar{0} \oplus \delta, 0)$. In the rectangle-like sandwich distinguisher (see Fig. 4), we choose $P \oplus P' = \alpha$, $\widetilde{P} \oplus \widetilde{P}' = \alpha$. Query the corresponding ciphertexts of the 5-round MMB (C, C', $\widetilde{C}$, $\widetilde{C}'$). If the equations $C \oplus \widetilde{C} = \zeta$ and $C' \oplus \widetilde{C}' = \zeta$ hold, the quartet is right.

Since the probability of the 2-round differential is 1, similar with Subsect. 4.1, we know that

$$Pr((Y' \oplus \widetilde{Y}' = \gamma)|(Y \oplus \widetilde{Y} = \gamma) \wedge (\widetilde{X} \oplus \widetilde{X}' = \beta) \wedge (X \oplus X' = \beta)) = 1,$$
$$Pr((Y \oplus \widetilde{Y} = \gamma)|(Y' \oplus \widetilde{Y}' = \gamma) \wedge (\widetilde{X} \oplus \widetilde{X}' = \beta) \wedge (X \oplus X' = \beta)) = 1.$$

It is easy to know that, $C \oplus \widetilde{C} = \zeta$ holds if and only if $C' \oplus \widetilde{C}' = \zeta$ holds.

Using the birthday searching algorithm, we get a pair $(C, \widetilde{C})$ corresponding to the collision $C = \widetilde{C} \oplus \zeta$ by searching two sets with 2^{64} chosen pairs (P, P') and $(\widetilde{P}, \widetilde{P}')$ respectively. $(C, \widetilde{C})$ and the corresponding $(C', \widetilde{C}')$ consists of a right quartet. So, the 5-round rectangle-like sandwich distinguisher can be distinguished with 2^{64} chosen plaintexts and 2^{64} table lookups.

5.2 The Key Recovery Attack

We set the 5-round rectangle-like sandwich distinguisher from round 1 to round 5. If a right quartet occurs, the ciphertext differences should satisfy the following two equations:

$$C \oplus \widetilde{C} = (V_1, V_1 \oplus V_2, V_1 \oplus V_2, V_2) \tag{17}$$

$$C' \oplus \widetilde{C}' = (W_1, W_1 \oplus W_2, W_1 \oplus W_2, W_2) \tag{18}$$

where V_1 and W_1 are output diffrences of G_1 corresponding to input difference $(\bar{0} \oplus \delta)$, V_2 and W_2 are output differences of G_2 corresponding to input difference $(\bar{0} \oplus \delta)$.

In order to be available to search the right quartet by fulfilling the birthday attack, we convert (17) and (18) into the following equivalent four equations.

$$(C_0 \oplus C_1 \oplus C_3) \oplus (\widetilde{C}_0 \oplus \widetilde{C}_1 \oplus \widetilde{C}_3) = 0,$$
$$(C_0 \oplus C_2 \oplus C_3) \oplus (\widetilde{C}_0 \oplus \widetilde{C}_2 \oplus \widetilde{C}_3) = 0,$$
$$(C'_0 \oplus C'_1 \oplus C'_3) \oplus (\widetilde{C}'_0 \oplus \widetilde{C}'_1 \oplus \widetilde{C}'_3) = 0,$$
$$(C'_0 \oplus C'_2 \oplus C'_3) \oplus (\widetilde{C}'_0 \oplus \widetilde{C}'_2 \oplus \widetilde{C}'_3) = 0.$$

We choose $2^{65.5}$ plaintext pairs (P, P') at random with the difference $(0, \bar{0}, \bar{0}, 0)$. Encrypt the corresponding ciphertext pairs (C, C'). Compute $2^{65.5}$ 128-bit values which consist of set A.

$$A = \{Z |\ Z = (C_0 \oplus C_1 \oplus C_3, C_0 \oplus C_2 \oplus C_3, C'_0 \oplus C'_1 \oplus C'_3, C'_0 \oplus C'_2 \oplus C'_3)\}.$$

Search all the collisions of set A by birthday attack. The expected number of collisions is 8. This is because, for each 2^{64} pairs of A, there is a right quartet according to Subsect. 5.1. So, there are about 4 collisions in A which implies 4 right quartets. According to birthday attack, there are another $2^{65.5} \cdot 2^{65.5} \cdot 2^{-1} \cdot 2^{-128} = 4$ collisions $(Z, \widetilde{Z})$ occur. So, we have totally 8 corresponding quartets $(C, C', \widetilde{C}, \widetilde{C}')$, and there are 4 right quartets.

For each sieved quartet, we get the equivalent key $k_1^{6'}$ and $k_2^{6'}$ respectively as in Subsect. 4.2 with 2^{30} MMB encryptions. Then we find the rest 64-bit keys by exhaustively searching. The data complexity of the attack is $2 \cdot 2^{65.5} = 2^{66.5}$ chosen plaintexts, the memory complexity is $2^{65.5}$ 128-bit block pairs, i.e., $2^{70.5}$ bytes.

6 The Improved Differential Cryptanalysis of MMB

A 6-round differential with high probability is given in this section, which can be used to 7-round extended MMB. The differential path is given as,

$$(0, \bar{0}, \bar{0}, 0) \xrightarrow[1]{\rho[k^0]} (\bar{0}, 0, 0, \bar{0}) \xrightarrow[1]{\rho[k^1]} (0, \bar{0} \oplus \delta, \bar{0} \oplus \delta, 0) \xrightarrow[p_1]{\rho[k^2]} (\tau, 0, 0, \tau) \xrightarrow[p_2]{\rho[k^3]} (0, \bar{0}, \bar{0}, 0) \xrightarrow{\rho[k^4]}$$
$$(\bar{0}, 0, 0, \bar{0}) \xrightarrow[1]{\rho[k^5]} (0, \bar{0} \oplus \delta, \bar{0} \oplus \delta, 0),$$

where τ satisfies the following two differtials.

$$\bar{0} \oplus \delta \xrightarrow{G_1} \tau \xrightarrow{G_0} \bar{0}, \tag{19}$$

$$\bar{0} \oplus \delta \xrightarrow{G_2} \tau \xrightarrow{G_3} \bar{0}. \tag{20}$$

By search all the τ, the 5-round differential holds with probability $p_1 . p_2 = 2^{-94}$. Because there are 16862718720 pairs make the differential characteristics (19) and (20) hold together, the probability is $16862718720/(2^{128}) \doteq 2^{-94}$.

6.1 Improved Differential Attack on the Full MMB

We use the last five rounds of the differential path to attack the full round MMB. The 5-round differential is as follows.

$$(\bar{0}, 0, 0, \bar{0}) \xrightarrow[1]{\rho[k^0]} (0, \bar{0} \oplus \delta, \bar{0} \oplus \delta, 0) \xrightarrow[p_1]{\rho[k^1]} (\tau, 0, 0, \tau) \xrightarrow[p_2]{\rho[k^2]} (0, \bar{0}, \bar{0}, 0) \xrightarrow[1]{\rho[k^3]}$$
$$(\bar{0}, 0, 0, \bar{0}) \xrightarrow[1]{\rho[k^4]} (0, \bar{0} \oplus \delta, \bar{0} \oplus \delta, 0),$$

We mount the 5-round differential path to rounds 1-5 of the 6 rounds. In the rest of the section, we give the attack algorithm.

The Key Recovery Attack. We choose 2^{96} pairs of plaintext with difference $(\bar{0}, 0, 0, \bar{0})$, then there are 4 right pairs. The output difference of the 5-th round for a right pair is $(0, \bar{0} \oplus \delta, \bar{0} \oplus \delta, 0)$, so the difference of the ciphertext should be $(V_1, V_1 \oplus V_2, V_1 \oplus V_2, V_2)$, where V_1, V_2 are non-zero 32-bit words. We use this to sieve the ciphertext pairs, and there will be $2^{96} \cdot 2^{-64} = 2^{32}$ pairs left. Furthermore, the input difference of the 6-th round is $(0, \bar{0} \oplus \delta, \bar{0} \oplus \delta, 0)$, the number of possible output difference values given the input difference $\bar{0} \oplus \delta$ for G_1 or G_2 is about $2^{28.56}$. So there are $2^{32} \cdot 2^{(28.56-32)\times 2} = 2^{25.12}$ pairs satisfying the output difference.

For each of $2^{25.12}$ pairs, we recover the key as Subsect. 4.2. Calculate the 32-bit words $k_1^{6'}$, $k_2^{6'}$ respectively, and increase the counter corresponding to $(k_1^{6'}, k_2^{6'})$ by 1. For G_1 and G_2, the number of pairs with input difference $\bar{0} \oplus \delta$ and any given output difference is at most $2^{14.28}$, so the maximum count per counted pair of the wrong subkey words will be $2^{14.28} \cdot 2^{14.28} = 2^{28.56}$. The signal-to-noise ratio is :

$$S/N = \frac{p \cdot 2^k}{\alpha \cdot \beta} = \frac{2^{-94} \times 2^{64}}{2^{-64-6.88} \times 2^{28.56}} = 2^{10.32}.$$

According to [12], the success probability is

$$Ps = \int_{-\frac{\sqrt{\mu S/N} - \Phi^{-1}(1-2^{-a})}{\sqrt{S/N+1}}}^{\infty} \Phi(x)dx = 0.9686,$$

where $a = 64$ is the number of subkey bits guessed, μ is the number of right pairs and $\mu = 4$.

The data complexity of the attack is 2^{96} chosen plaintexts, which is dominant the time complexity. We need $2 \cdot 2^{14.28} \cdot 2^{25.12} = 2^{40.40}$ XOR operations and $2^{14.28} \cdot$

Table 2. Summary of the Attacks on MMB

#Rounds	Type	Time	Data	Memory	Source
3	LC	2^{126} EN	$2^{114.56}$ KP	-	[13]
4	SQ	$2^{126.32}$ EN	2^{34} CP	2^{66}	[13]
6	DC	2^{118} EN	2^{118} CP	2^{66}	[13]
6	SW	2^{40}EN	2^{39} ACP	2^{18}	this paper
6	SR	$2^{66.5}$ EN	$2^{66.5}$ CP	$2^{70.5}$	this paper
6	DC	2^{96} EN	2^{96} CP	2^{66}	this paper
7	DC	2^{96} EN	2^{96} CP	2^{66}	this paper

LC: Linear Cryptanalysis; DC: Differential Cryptanalysis.
SQ: Square Attack; SW: Sandwich Attack; SR: Rectangle-like Sandwich Attack.
EN: MMB Encryption.
KP: Known Plaintexts; CP: Chosen Plaintexts; ACP: adaptive chosen Texts.

$2^{14.28} \cdot 2^{25.12} = 2^{53.68}$ counts, equivalent to 2^{43} MMB encryptions to recovery the 64-bit subkey. The memory complexity is 2^{64} 64-bit counters, equivalent to 2^{66} bytes. There are 4 values for 64 bits of the key, and the rest 64 bits can be recovered by exhaustive search.

6.2 Differential Attack of MMB$^+$

If we call the 7-round version of MMB as MMB$^+$, we show that MMB$^+$ can also be broken with the same complexity of the 6-round differential attack. Note that in the above subsection, we only use 5 rounds out of the 6-round differential path, and the probability of the 5-round path is the same as the 6-round path. So if we use the 6-round differential path, we can also attack MMB$^+$ by the same manner described in the above subsection. It means that even if MMB has 7 rounds it is still vulnerable to the differential attack.

7 Conclusion

In this paper, we construct a 5-round sandwich distinguisher for MMB with high probability 1. With the distinguisher, we recover the 128-bit key of MMB with 2^{39} adaptive chosen plaintexts and ciphertexts, 2^{40} MMB encryptions. On this bases, we present a rectangle-like sandwich attack to MMB, with $2^{66.5}$ chosen plaintexts, $2^{66.5}$ MMB encryptions and $2^{70.5}$ bytes memory. Besides, we improve the differential attack on MMB in [13]. The data complexity is 2^{96} chosen plaintexts, the time complexity is 2^{96} MMB encryptions and the memory complexity is 2^{66} bytes. We summarize the results on MMB in Table 2.

Acknowledgements. We would like to thank anonymous reviewers for their very helpful comments on the paper. We also hope to thank Yuliang Zheng for the discussion on the cryptanalysis of 7-round MMB during his stay in Tsinghua University.

References

1. Biham, E., Shamir, A.: Differential Cryptanalysis of The Data Encryption Standard. Springer, London (1993)
2. Biham, E., Dunkelman, O., Keller, N.: The Rectangle Attack - Rectangling the Serpent. In: Pfitzmann, B. (ed.) EUROCRYPT 2001. LNCS, vol. 2045, pp. 340–357. Springer, Heidelberg (2001)
3. Biham, E., Dunkelman, O., Keller, N.: A Related-Key Rectangle Attack on the Full KASUMI. In: Roy, B. (ed.) ASIACRYPT 2005. LNCS, vol. 3788, pp. 443–461. Springer, Heidelberg (2005)
4. Biryukov, A., De Cannière, C., Dellkrantz, G.: Cryptanalysis of SAFER++. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 195–211. Springer, Heidelberg (2003)
5. Biryukov, A., Khovratovich, D.: Related-Key Cryptanalysis of the Full AES-192 and AES-256. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 1–18. Springer, Heidelberg (2009)
6. Kelsey, J., Kohno, T., Schneier, B.: Amplified Boomerang Attacks Against Reduced-Round MARS and Serpent. In: Schneier, B. (ed.) FSE 2000. LNCS, vol. 1978, pp. 75–93. Springer, Heidelberg (2001)
7. Daemen, J., Govaerts, R., Vandewalle, J.: Block Ciphers Based on Modular Multiplication. In: Wolfowicz, W. (ed.) Proceedings of 3rd Symposium on State and Progress of Research in Cryptography, Fondazione Ugo Bordoni, pp. 80–89 (1993)
8. Daemen, J.: Cipher and Hash Function Design Strategies based on Linear and Differential Cryptanalysis. PhD Thesis, Dept. Elektrotechniek, Katholieke Universiteit Leuven, Belgium (1995)
9. Lai, X., Massey, J.: A Proposal for a New Block Encryption Standard. In: Damgård, I.B. (ed.) EUROCRYPT 1990. LNCS, vol. 473, pp. 389–404. Springer, Heidelberg (1991)
10. Dunkelman, O., Keller, N., Shamir, A.: A Practical-Time Attack on the A5/3 Cryptosystem Used in Third Generation GSM Telephony, `http://eprint.iacr.org/2010/013`
11. Dunkelman, O., Keller, N., Shamir, A.: A Practical-Time Related-Key Attack on the KASUMI Cryptosystem Used in GSM and 3G Telephony. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 393–410. Springer, Heidelberg (2010)
12. Selçuk, A.A., Biçak, A.: On Probability of Success in Linear and Differential Cryptanalysis. In: Cimato, S., Galdi, C., Persiano, G. (eds.) SCN 2002. LNCS, vol. 2576, pp. 174–185. Springer, Heidelberg (2003)
13. Wang, M., Nakahara Jr., J., Sun, Y.: Cryptanalysis of the Full MMB Block Cipher. In: Jacobson Jr., M.J., Rijmen, V., Safavi-Naini, R. (eds.) SAC 2009. LNCS, vol. 5867, pp. 231–248. Springer, Heidelberg (2009)
14. Wagner, D.: The Boomerang Attack. In: Knudsen, L.R. (ed.) FSE 1999. LNCS, vol. 1636, pp. 156–170. Springer, Heidelberg (1999)