Cryptanalysis of the full MMB block cipher

Meiqin Wang[1], Jorge Nakahara Jr[2], and Yue Sun[1]

[1] Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, Jinan 250100, China
[2] EPFL, Lausanne, Switzerland
mqwang@sdu.edu.cn, jorge.nakahara@epfl.ch, yuesun@mail.sdu.edu.cn

Abstract. The block cipher MMB was designed by Daemen, Govaerts and Vandewalle, in 1993, as an alternative to the IDEA block cipher. We exploit and describe unusual properties of the modular multiplication in $\mathbb{Z}_{2^{32}-1}$, which lead to a differential attack on the full 6-round MMB cipher (both versions 1.0 and 2.0). Further **contributions** of this paper include detailed square and linear cryptanalysis of MMB. Concerning differential cryptanalysis (DC), we can break the full MMB with 2^{118} chosen plaintexts, $2^{95.91}$ 6-round MMB encryptions and 2^{64} counters, effectively bypassing the cipher's countermeasures against DC. For the square attack, we can recover the 128-bit user key for 4-round MMB with 2^{34} chosen plaintexts, $2^{126.32}$ 4-round encryptions and 2^{64} memory blocks. Concerning linear cryptanalysis, we present a key-recovery attack on 3-round MMB requiring $2^{114.56}$ known-plaintexts and 2^{126} encryptions. Moreover, we detail a ciphertext-only attack on 2-round MMB using $2^{93.6}$ ciphertexts and $2^{93.6}$ parity computations. These attacks do not depend on weak-key or weak-subkey assumptions, and are thus independent of the key schedule algorithm.

Keywords: MMB block cipher, differential cryptanalysis, square cryptanalysis, linear cryptanalysis, modular multiplication.

1 Introduction

The block cipher MMB (Modular Multiplication Based) block cipher [4] was designed by Daemen, Govaerts and Vandewalle in 1993, and its main innovation was the use of cyclic multiplication in the ring $\mathbb{Z}_{2^n-1}$, where n is the word size of the cipher. All internal operations of MMB are on n-bit words. The designers suggested $n = 32$, leading to the ring $\mathbb{Z}_{2^{32}-1}$. MMB is an iterated cipher, composed of six rounds. MMB was proposed as an alternative to the IDEA block cipher [8]. MMB has been designed particularly to resist differential cryptanalysis [6]. This paper presents differential, square and linear cryptanalysis of the MMB cipher. Previous cryptanalysis of MMB was a related-key attack and only applied to MMB version 1.0, according to [6]. In order to resist the related-key attack, MMB version 2.0 was proposed by revising only the key schedule algorithm. As far as we know, there is no previous attack on MMB version 2.0.

However, our attacks are independent of the key schedule algorithm, so they can be applied to both versions 1.0 and 2.0.

In this paper, firstly we present differential cryptanalysis of the full 6-round MMB. Five-round differential characteristics have been identified, and we can recover the 128-bit user key with 2^{118} chosen plaintexts (CP), $2^{95.91}$ 6-round MMB encryptions and 2^{64} memory blocks. Secondly, we investigate the square attack on reduced-round MMB. We distinguished a new word type: X word, based on which we have found 2.75-round square distinguishers and applied the square attack to 4-round MMB. We can recover the 128-bit user key with 2^{34} CP, $2^{126.32}$ 4-round encryptions and 2^{64} memory blocks. Thirdly, we apply linear cryptanalysis to reduced-round MMB. We identified two linear approximations with bias $2^{-55.78}$ for 3-round MMB and recover one-bit subkey information for 3-round MMB with $2^{114.56}$ known plaintexts (KP) and equivalent parity computations; then recover 128-bit key for 3-round MMB with $2^{114.56}$ KP and 2^{126} 3-round MMB encryptions. Moreover, we can attack 2-round MMB with $2^{93.6}$ ciphertexts only (CO). From our attacks, particularly concerning differential cryptanalysis, we disprove the claims of the designers that MMB can resist DC.

The paper is organized as follows. Sec. 2 describes the MMB cipher. Sect. 3 presents the differential attack on the full MMB, and Sect. 4 details a square attack on a 4-round MMB. The linear attack on reduced-round MMB is provided in Sect. 5. Sect. 6 concludes the paper.

2 Description of the MMB Block Cipher

The MMB block cipher has a Substitution-Permutation Network (SPN) structure and operates on 128-bit text blocks, uses a 128-bit key, and iterates six rounds. One round of MMB consists of four transformations [6]:

- $\sigma[k^j]$: exclusive-or each data word with the j-th round subkey k^j. Formally,

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

  where $\oplus$ denotes bitwise exclusive-or, $a_i, k_i^j \in \mathbb{Z}_{2^{32}}$, for $0 \leq i \leq 3$. The $\sigma[k^j]$ operation is an involution, and is the only key-dependent operation in a round.
- γ: modular multiplication of each data word with fixed 32-bit constants G_i,

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

  where $a \otimes b = a * b \bmod (2^{32} - 1)$, $G_0 = 025F1CDB_x$, $G_1 = 2 \otimes G_0 = 04BE39B6_x$, $G_2 = 8 \otimes G_0 = 12F8E6D8_x$, and $G_3 = 128 \otimes G_0 = 2F8E6D81_x$ which can be efficiently computed since $(A * 2^x) \bmod (2^{32} - 1) = (A \lll x) \bmod (2^{32} - 1)$. There is a wrap-around effect in multiplication modulo $2^{32} - 1$, since $2^{32} \equiv 1 \bmod (2^{32} - 1)$, which means that the bits at the $(32 + i)$-th LSB position are shifted to the i-th LSB position. This effect is

similar to the multiplication operation modulo $2^{16}+1$ in IDEA. As cited in [6], the $\otimes$ operation can be expressed as:

$$a \otimes b = a * b \bmod (2^{32}-1) = (a * b \bmod 2^{32} + \lfloor \frac{a*b}{2^{32}} \rfloor) \bmod (2^{32}-1).$$

Notice that γ is invertible but is not an involution. Each 32-bit multiplication can be interpreted as a huge 32×32-bit S-box, since one of the operands in the multiplication is always fixed. There are two fixed points for any G_i: $0 \otimes G_i = 0$, and $(2^{32}-1) \otimes G_i = 2^{32}-1$.

- η: a data-dependent transformation operating on two out of the four input words (a_0, a_1, a_2, a_3):

$$\eta(a_0, a_1, a_2, a_3) = (a_0 \oplus (\mathrm{lsb}(a_0) * \delta), a_1, a_2, a_3 \oplus ((1 \oplus \mathrm{lsb}(a_3)) * \delta)),$$

where 'lsb' denotes the least significant bit, and $\delta = 2aaaaaaa_x$; η is an involution and a non-linear operation. η is used to resist the propagation of the differential characteristics with probability 1.

- θ: the only diffusion operation in MMB. Formally,

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

where $a_i \in \mathbb{Z}_{2^{32}}$, with $0 \le i \le 3$. θ is an involution and has branch number four (see [11]).

There are two pairs of operations that can be interchanged: (θ, $\sigma[k^j]$) and (η, $\sigma[k^j]$). In each case, the key k^j is transformed into an equivalent key $\theta(k^j)$ or $\eta(k^j)$, respectively.

The j-th (full) round transformation of MMB can be denoted:

$$\rho[k^j](X) = \theta \circ \eta \circ \gamma \circ \sigma[k^j](X) = \theta(\eta(\gamma(\sigma[k^j](X)))) \,. \tag{1}$$

The full MMB encryption of a plaintext P can be denoted:

$$\mathrm{MMB}(P) = \sigma[k^6] \circ \rho[k^5] \circ \rho[k^4] \circ \rho[k^3] \circ \rho[k^2] \circ \rho[k^1] \circ \rho[k^0](P) \,, \tag{2}$$

where $\sigma[k^6]$ is the output transformation or post-whitening operation.

In the original key schedule of MMB version 1.0, the first round subkey is simply the 128-bit user key $K = (k_0, k_1, k_2, k_3)$. Successive subkeys use K rotated by 32 bits to the left. So, for instance, (k_1, k_2, k_3, k_0), (k_2, k_3, k_0, k_1) and so forth. A redesigned key-schedule to avoid related-key attacks has led to a tweaked cipher called MMB version 2.0 [6] in which a constant value is xored to the leftmost 32-bit subkey word after each rotation.

3 Differential Cryptanalysis of the Full MMB

Differential cryptanalysis (DC) [3] exploits the propagation of particular differences of plaintext pairs across a cipher, to certain differences of the resultant ciphertext pairs. The designers of MMB claimed that an important design criterion was resistance against DC in [4], but we break the full MMB using DC.

3.1 Differential Characteristics for MMB

The main component in the round function of MMB responsible for the confusion property (according to C. Shannon) is γ. Thus, for the cryptanalyst it is very important to minimize the number of active multiplications in order to maximize the probability of the differential characteristics. The possible distributions of active modular multiplications are listed in Table 2. In the leftmost column, the input difference is said to cause (denoted with an arrow, $\xrightarrow{1r}$) the given output difference after one round. The second column shows the number of active multiplications. The rightmost column shows the restrictions on the output difference of active multiplications, which account for η. Due to θ, the output differences from the active multiplications in one round all have to be equal. For each row in Table 2, we denote the input difference as $\Delta_{ij}, (0 \leq j \leq 3)$ and the output difference as Δ_o.

In order to identify 2-round characteristics for MMB with the highest probability, we only consider two active multiplications per round. An important property for the modular multiplication operation γ has been described in [6]

$$R_p(\bar{0} \xrightarrow{\gamma} \bar{0}) = 1,$$

where $\bar{0} = 2^{32} - 1 = ffffffff_x$. This property means that the differential characteristic $\bar{0} \xrightarrow{\gamma} \bar{0}$ holds with probability 1, leading to the following 2-round characteristic with probability 1:

$$(0, \bar{0}, \bar{0}, 0) \xrightarrow{\sigma[k^0]} (0, \bar{0}, \bar{0}, 0) \xrightarrow{\gamma} (0, \bar{0}, \bar{0}, 0) \xrightarrow{\eta} (0, \bar{0}, \bar{0}, 0) \xrightarrow{\theta} (\bar{0}, 0, 0, \bar{0})$$
$$\xrightarrow{\sigma[k^1]} (\bar{0}, 0, 0, \bar{0}) \xrightarrow{\gamma} (\bar{0}, 0, 0, \bar{0}) \xrightarrow{\eta} (\bar{0} \oplus \delta, 0, 0, \bar{0} \oplus \delta) \xrightarrow{\theta} (0, \bar{0} \oplus \delta, \bar{0} \oplus \delta, 0).$$

Then, we further extend the 2-round characteristic by two rounds above it and one round below it. For the lower round, the following differential characteristic needs to be determined:

$$(0, \bar{0} \oplus \delta, \bar{0} \oplus \delta, 0) \xrightarrow{\sigma[k^2]} (0, \bar{0} \oplus \delta, \bar{0} \oplus \delta, 0) \xrightarrow{\gamma} (0, \alpha_1, \alpha_2, 0).$$

We identified the characteristics $\bar{0} \oplus \delta \xrightarrow{G_1} fcfbdfff_x$ and $\bar{0} \oplus \delta \xrightarrow{G_2} f3ef7fff_x$, both of which have probability about 2^{-18}. With them, we construct a 3-round differential characteristic with probability 2^{-36} as follows:

$$(0, \bar{0}, \bar{0}, 0) \xrightarrow{1r} (\bar{0}, 0, 0, \bar{0}) \xrightarrow{1r} (0, \bar{0} \oplus \delta, \bar{0} \oplus \delta, 0) \xrightarrow{\sigma[k^i]} (0, \bar{0} \oplus \delta, \bar{0} \oplus \delta, 0)$$
$$\xrightarrow{\gamma} (0, fcfbdfff_x, f3ef7fff_x, 0) \xrightarrow{\eta} (0, fcfbdfff_x, f3ef7fff_x, 0)$$
$$\xrightarrow{\theta} (fcfbdfff_x, 0f14a000_x, 0f14a000_x, f3ef7fff_x).$$

For the upper round, the following differential characteristic needs to be determined:

$$(\beta_0, 0, 0, \beta_3) \xrightarrow{\sigma[k^i]} (\beta_0, 0, 0, \beta_3) \xrightarrow{\gamma} (\bar{0} \oplus \delta, 0, 0, \bar{0} \oplus \delta) \xrightarrow{\eta} (\bar{0}, 0, 0, \bar{0}) \xrightarrow{\theta}$$
$$(0, \bar{0}, \bar{0}, 0) \xrightarrow{1r} (\bar{0}, 0, 0, \bar{0}) \xrightarrow{1r} (0, \bar{0} \oplus \delta, \bar{0} \oplus \delta, 0) \xrightarrow{1r}$$
$$(fcfbdfff_x, 0f14a000_x, 0f14a000_x, f3ef7fff_x).$$

In order to further extend the above 4-round characteristic by one round above it, we only consider the cases $\beta_0 = \beta_3$. In this way, we identified the characteristics $a7cfdf7f_x \xrightarrow{G_0} \bar{0} \oplus \delta$ and $a7cfdf7f_x \xrightarrow{G_3} \bar{0} \oplus \delta$, both with probability about 2^{-21}. So, a 4-round characteristic with probability $2^{-42} \cdot 2^{-36} = 2^{-78}$ has been constructed. Then, we further extend the 4-round characteristic. The following characteristic needs to be determined,

$$\begin{aligned}(0, \xi_1, \xi_2, 0) &\xrightarrow{\sigma[k^i]} (0, \xi_1, \xi_2, 0) \xrightarrow{\gamma} (0, a7cfdf7f_x, a7cfdf7f_x, 0) \\ &\xrightarrow{\eta} (0, a7cfdf7f_x, a7cfdf7f_x, 0) \xrightarrow{\theta} (a7cfdf7f_x, 0, 0, a7cfdf7f_x) \\ &\xrightarrow{1r} (0, \bar{0}, \bar{0}, 0) \xrightarrow{1r} (\bar{0}, 0, 0, \bar{0}) \xrightarrow{1r} (0, \bar{0} \oplus \delta, \bar{0} \oplus \delta, 0) \\ &\xrightarrow{1r} (fcfbdfff_x, 0f14a000_x, 0f14a000_x, f3ef7fff_x).\end{aligned}$$

We identified the characteristics $9bd3fdf7_x \xrightarrow{G_1} a7cfdf7f_x$ and $e6f4ff7d_x \xrightarrow{G_2} a7cfdf7f_x$, both with probability about 2^{-14}. With them, we construct a 5-round characteristic with probability $2^{-28} \cdot 2^{-78} = 2^{-106}$ as follows:

$$\begin{aligned}(0, 9bd3fdf7_x, e6f4ff7d_x, 0) &\xrightarrow{1r} (a7cfdf7f_x, 0, 0, a7cfdf7f_x) \\ &\xrightarrow{1r} (0, \bar{0}, \bar{0}, 0) \xrightarrow{1r} (\bar{0}, 0, 0, \bar{0}) \xrightarrow{1r} (0, \bar{0} \oplus \delta, \bar{0} \oplus \delta, 0) \\ &\xrightarrow{1r} (fcfbdfff_x, 0f14a000_x, 0f14a000_x, f3ef7fff_x).\end{aligned} \tag{3}$$

With the 5-round characteristic in (3), we cannot attack the full 6-round MMB because the S/N is too small. In order to increase the S/N, we found another 5-round differential characteristic with probability 2^{-110} as follows:

$$\begin{aligned}(0, 9bd3fdf7_x, e6f4ff7d_x, 0) &\xrightarrow{1r} (a7cfdf7f_x, 0, 0, a7cfdf7f_x) \xrightarrow{1r} (0, \bar{0}, \bar{0}, 0) \\ &\xrightarrow{1r} (\bar{0}, 0, 0, \bar{0}) \xrightarrow{1r} (0, \bar{0} \oplus \delta, \bar{0} \oplus \delta, 0) \xrightarrow{1r} (40404040_x, 0, 0, 40404040_x),\end{aligned} \tag{4}$$

where the characteristics $\bar{0} \oplus \delta \xrightarrow{G_1} 40404040_x$ and $\bar{0} \oplus \delta \xrightarrow{G_2} 40404040_x$ have probability about 2^{-20}. Although the probability of (4) is lower than that of (3), the ratio of the counted to all pairs of ciphertext decreases prominently. Therefore we use (4) to attack the full 6-round MMB cipher.

The 6-round MMB encryption of a plaintext P is depicted in (2). In order to decrease the time complexity, we move $\sigma[k^6]$ to the front of θ in the 6^{th} round; $\sigma[k^6]$ will be transformed to $\sigma[k^{6'}]$, where $k_0^{6'} = k_0^6 \oplus k_1^6 \oplus k_3^6$; $k_1^{6'} = k_0^6 \oplus k_1^6 \oplus k_2^6$; $k_2^{6'} = k_1^6 \oplus k_2^6 \oplus k_3^6$ and $k_3^{6'} = k_0^6 \oplus k_2^6 \oplus k_3^6$. Thus, we will recover the equivalent subkey $k^{6'}$.

3.2 Attack Algorithm

We choose 2^{54} structures of 2^{64} chosen plaintexts each. In each structure, the second and third words of the plaintext can together take 2^{64} possible values. There are 2^{63} plaintext pairs with the difference $(0, 9bd3fdf7_x, e6f4ff7d_x, 0)$ in

each structure. So, the total number of pairs in 2^{54} structures is $2^{54} \cdot 2^{63} = 2^{117}$. The differential characteristic has probability 2^{-110}, so the number of the right pairs is $2^{117} \cdot 2^{-110} = 2^7 = 128$. For each structure, there are about 2^{63} pairs of plaintexts to be considered in total.

Since the output difference of the 5^{th} round for a right pair is (40404040_x, 0, 0, 40404040_x), the difference of the ciphertext pairs should be $(\alpha \oplus \beta, \alpha, \beta, \alpha \oplus \beta)$, with $\alpha, \beta \in \mathbb{Z}_{2^{32}}$, so we can use this to discard wrong pairs. Thus, about $2^{63} \cdot 2^{-64} = 2^{-1}$ candidates for the right pairs remain from each structure.

The input difference of the 6^{th} round is $(40404040_x, 0, 0, 40404040_x)$. We found that the numbers of possible output difference values given the input difference 40404040_x for the modular multiplication G_0 or G_3 is $6738641/2^{32} = 2^{-9.32}$, so about $2^{-1} \cdot 2^{-18.64} = 2^{-19.64}$ candidates for the right pairs remain for each structure. The total number of remaining pairs in all the 2^{54} structures is $2^{54} \cdot 2^{-19.64} = 2^{34.36}$.

For each remaining ciphertext pair (C_0, C_1, C_2, C_3) and (C_0', C_1', C_2', C_3'), we guess the equivalent subkey words $k_0^{6'}$ and $k_3^{6'}$, and the total number of guessed subkey bits is 64. Then, calculate $\xi_0 = (G_0^{-1} \otimes (\eta(C_0 \oplus C_1 \oplus C_3 \oplus k_0^{6'}))) \oplus (G_0^{-1} \otimes (\eta(C_0' \oplus C_1' \oplus C_3' \oplus k_0^{6'})))$ and $\xi_3 = (G_3^{-1} \otimes (\eta(C_0 \oplus C_2 \oplus C_3 \oplus k_3^{6'}))) \oplus (G_3^{-1} \otimes (\eta(C_0' \oplus C_2' \oplus C_3' \oplus k_3^{6'})))$. If both ξ_0 and ξ_3 are equal to 40404040_x, the counter corresponding to $(k_0^{6'}, k_3^{6'})$ will be incremented by one. For G_0 and G_3 with the inputxor 40404040_x and any given outputxor, there will be at most 2^{17} pairs, so the maximum count per counted pair of the subkey words will be $2^{17} \cdot 2^{17} = 2^{34}$.

In our attack, the signal-to-noise ratio is computed as follows:

$$S/N = \frac{p \cdot 2^k}{\alpha \cdot \beta} = \frac{2^{-110} \cdot 2^{64}}{2^{-64-18.64} \cdot 2^{34}} = 2^{2.64} = 6.23.$$

The success probability is computed as follows[1]:

$$Ps = \int_{-\frac{\sqrt{\mu S/N} - \Phi^{-1}(1-2^{-a})}{\sqrt{S/N+1}}}^{\infty} \Phi(x)dx = 0.99999999,$$

where $a = 64$ is the number of subkey bits involved in the decryption and μ is the number of right pairs which can be obtained $\mu = p \cdot N = 2^{-110} \cdot 2^{117} = 128$. With probability 0.99999999 the right key can be recovered.

The attack needs 2^{118} CP and $2^{35.36} \cdot 2^{64} \cdot 2 = 2^{100.36}$ modular multiplications, which is no more than $2^{100.36}/4 = 2^{98.36}$ 1-round MMB encryptions, equivalent to $2^{98.36}/6 = 2^{95.91}$ 6-round MMB encryptions. The memory requirements are about 2^{64} 64-bit counters. The remaining 64-bit equivalent subkey $k_1^{6'}$ and $k_2^{6'}$ can be recovered by exhaustive search with about 2^{64} 6-round MMB encryptions. Finally, the 128-bit user key can be derived. In all, the data complexity is 2^{118} CP, the time complexity is $2^{95.91}$ 6-round MMB encryptions and the memory requirements are 2^{64} 64-bit blocks.

4 Square Analysis of MMB

MMB is a word-oriented cipher. More precisely, it operates on neatly partitioned 32-bit words. This wordwise behavior motivates our square analysis. Our attacks use Λ-sets of 2^{32} CP. We use the terminology of [7].

4.1 Square Distinguisher

Due to the special property for modular multiplication, we discovered a new word type: X word, which can propagate across γ. The X word is very useful for us to identify four chains of Λ-sets, each of which represents a 2.75-round square distinguisher if we consider every round transformation σ, γ, η and θ as a fraction of 0.25 of a (full) round.

- $(A, C, C, C) \xrightarrow{1r} (A, A, C, A) \xrightarrow{1r} (X, B, B, E) \xrightarrow{\sigma[k^2]} (X, B, B, E) \xrightarrow{\gamma} (X, ?, ?, E) \xrightarrow{\eta} (B, ?, ?, E)$,
- $(C, A, C, C) \xrightarrow{1r} (A, A, A, C) \xrightarrow{1r} (B, B, E, B) \xrightarrow{\sigma[k^2]} (B, B, E, B) \xrightarrow{\gamma} (?, ?, E, ?) \xrightarrow{\eta} (?, ?, E, ?)$,
- $(C, C, A, C) \xrightarrow{1r} (C, A, A, A) \xrightarrow{1r} (B, E, B, B) \xrightarrow{\sigma[k^2]} (B, E, B, B) \xrightarrow{\gamma} (?, E, ?, ?) \xrightarrow{\eta} (?, E, ?, ?)$,
- $(C, C, C, A) \xrightarrow{1r} (A, C, A, A) \xrightarrow{1r} (E, B, B, X) \xrightarrow{\sigma[k^2]} (E, B, B, X) \xrightarrow{\gamma} (E, ?, ?, X) \xrightarrow{\eta} (E, ?, ?, B)$,

where 'A' indicates an active word; 'C' denotes a passive (or constant) word; 'B' denotes a balanced word, that is, the xor sum of whose contents gives zero; 'X' denotes another special balanced word in which any value x and $\neg x$ appear the same number of times; 'E' denotes a special balanced word in which each value appears an even number of times [2]; '?' indicates that the xor sum of the 32-bit in that word is an unpredictable value. The proofs of the propagation of Λ-sets can be found in Appendix A.

4.2 Square Attack on 4-round MMB

With any of the above square distinguishers, the key-recovery attack on 4-round MMB can be applied.

Consider the square distinguisher $(A, C, C, C) \xrightarrow{1r} (A, A, C, A) \xrightarrow{1r} (X, B, B, E) \xrightarrow{\sigma[k^2]} (X, B, B, E) \xrightarrow{\gamma} (X, ?, ?, E) \xrightarrow{\eta} (B, ?, ?, E)$. A full 4-round MMB consists of

$$\sigma[k^4] \circ \theta \circ \eta \circ \gamma \circ \sigma[k^3] \circ \theta \circ \eta \circ \gamma \circ \sigma[k^2] \circ \theta \circ \eta \circ \gamma \circ \sigma[k^1] \circ \theta \circ \eta \circ \gamma \circ \sigma[k^0].$$

We aim at recovering k^4 by partial decryption. We also move $\sigma[k^4]$ across θ. We denote the modified key as $k^{4'}$. Further, we can remove θ because it is invertible and key independent.

The attack procedure is as follows:

– Step 1: Choose 2^{32} plaintexts $(x, {c_1}^0, {c_2}^0, {c_3}^0), x \in \mathbb{Z}_{2^{32}}$, ${c_1}^0, {c_2}^0$ and ${c_3}^0$ are constants.
– Step 2: Guess the 32-bit words $k_0^{4\prime}$, $k_1^{4\prime}$ and $k_3^{4\prime}$ of $k^{4\prime}$. Apply the inverse of η and γ, xor the three words to obtain a new word. If the new word is balanced, save the subkey value. On average, 2^{64} subkey values are saved.
– Step 3: for $i := 1$ to 3 do
  • Step 3.1: Choose a new group of 2^{32} plaintexts $(x, {c_1}^i, {c_2}^i, {c_3}^i), x \in \mathbb{Z}_{2^{32}}$, ${c_1}^i, {c_2}^i$ and ${c_3}^i$ are constants.
  • Step 3.2: For each saved subkey value, apply the inverse of η and γ, xor the three words to obtain the new word. If the new word is not balanced, delete the subkey value.
– Step 4: The remaining subkey value should be the right subkey with high probability.

The total number of guessed subkey bits is 96, only one Λ-set cannot identify the right subkey; on average, 2^{64} wrong guesses also satisfy the balanced property. So, we choose different constant values of the later three words in plaintexts to construct four Λ-sets. We expect any wrong subkey value to satisfy the balanced property with probability 2^{-32}, but, the right subkey value must satisfy the balanced property always.

In total, the complexity is about $(2^{96} + 2^{64} + 2^{32} + 1) \cdot 2^{32} = 2^{128}$ 1.25-round decryptions; 2^{34} CP, and memory of 2^{64} 96-bit counters. For the third word of $k^{4\prime}$, we can recover it by exhaustive search. In total, the time complexity is $2^{128} \cdot 1.25 + 6 \cdot 2^{32} = 2^{128.32}$ 1-round decryptions, or equivalently, $2^{128.32}/4 = 2^{126.32}$ full 4-round MMB encryptions. The data complexity will be 2^{34} CP. The memory complexity is 2^{64} text blocks.

5 Linear Attacks on MMB

Linear cryptanalysis typically works in a known-plaintext or ciphertext-only setting (in the latter, assuming the plaintext is ASCII text), and its origin dates back to the works of Matsui on DES [9, 10].

5.1 Linear Approximations for MMB

In MMB, the main non-linear operation that limits the effectiveness of linear approximations is the multiplication in $\mathbb{Z}_{2^{32}-1}$, namely γ. Let $M_i = (m_{i0}, m_{i1}, m_{i2}, m_{i3})$ and $M_o = (m_{o0}, m_{o1}, m_{o2}, m_{o3})$ denote the linear input mask and the linear output mask of γ, respectively. Any nonzero m_{ij} (and m_{oj}), for $0 \le j \le 3$, represents an active multiplication.

As in the differential cryptanalysis in Sect.3, the possible distributions for active multiplications in linear approximation are listed in Table 3. m_o and m_{ij}, $(0 \le j \le 3)$ represent the input mask and the output mask, respectively. Besides the γ component, η is also non-linear. To avoid the effect of η on linear approximations, it is necessary to guarantee that the output mask m_o for the active G_i satisfies $m_o \cdot \delta = 0$, where $\cdot$ is the dot product.

We recall the rotational invariant property [5] of multiplication modulo $2^{32}-1$,

$$a \otimes (x << k) = (a \otimes x) << k.$$

The linear approximation for one multiplication can be used to obtain the linear approximation for the other three multiplications. The bias ϵ for $m_{i1} \xrightarrow{G_1} m_o$ and the bias ϵ' for $m_{i1} \lll 2 \xrightarrow{G_2} m_o$ will be equal. In particular, with the rotational property, for $m_i = \bar{0}$ and $m_o = \bar{0}$, the biases for the linear approximation of multiplication for all G_i are equal (to $2^{-12.0897}$). But, the mask $\bar{0}$ is not appropriate concerning η. The corresponding bias for a one-round linear approximation is zero because $\bar{0} \cdot \delta = 1$.

In order to construct multi-round linear approximations, the output masks for different active multiplications must be equal. From the experiments of different masks for G_i, we conjecture that the linear approximations for modular multiplication with maximum bias have the following forms:

$$\begin{aligned} &mmmmmmmm_x \xrightarrow{G_i} nnnnnnnn_x, \\ &m_0m_1m_0m_1m_0m_1m_0m_1{}_x \xrightarrow{G_i} n_0n_1n_0n_1n_0n_1n_0n_1{}_x, \\ &m_0m_1m_2m_3m_4m_5m_6m_7{}_x \xrightarrow{G_i} m_0m_1m_2m_3m_4m_5m_6m_7{}_x, \end{aligned} \tag{5}$$

where $m, n, m_i, n_i \in \mathbb{Z}_{2^4}$, $0 \le i \le 7$. The probability for the above linear relations with the maximum bias decreases gradually. We have only searched the first two linear approximations in (5). The last linear relation needs too large a test space, so we have not searched it.

Linear Approximations for Modulo Multiplication:

The best linear approximations we identified have bias $2^{-8.8}$ for each G_i, and some of them are

$$\begin{aligned} &3c3c3c3c_x \xrightarrow{G_0} 0f0f0f0f_x,\ 3c3c3c3c_x \xrightarrow{G_1} 1e1e1e1e_x, \\ &3c3c3c3c_x \xrightarrow{G_2} 78787878_x,\ 3c3c3c3c_x \xrightarrow{G_3} 87878787_x. \end{aligned}$$

Based on the above linear approximations for G_i, one-round linear approximations with only one active multiplication can be obtained with bias $2^{-8.8}$.

Two-Round Linear Approximations:

Two-round linear approximations can be obtained with only two active modular multiplications in each round. For active G_0 and G_2, for instance

$$(m_{i0}, 0, m_{i2}, 0) \xrightarrow{1r} (m_2, 0, m_2, 0) \xrightarrow{1r} (m_3, 0, m_3, 0), \tag{6}$$

where m_{i0}, m_{i2}, m_2 and m_3 are independent 32-bit masks, and 1r means 1-round linear approximation. The following local approximations are required:

$m_{i0} \xrightarrow{G_0} m_2$, $m_{i2} \xrightarrow{G_2} m_2$ and $m_2 \xrightarrow{G_j} m_3$ for $j \in \{0, 2\}$ with nonzero bias. The maximum bias we identified was $2^{-36.82}$ for 2-round linear approximation:

$$\begin{aligned}&(1b1b1b1b_x, 0, 63636363_x, 0) \xrightarrow{1r} (6c6c6c6c_x, 0, 6c6c6c6c_x, 0)\\ &\xrightarrow{1r} (72727272_x, 0, 72727272_x, 0),\end{aligned} \tag{7}$$

where the linear approximations for G_0 and G_2 are

$$\begin{aligned}&1b1b1b1b_x \xrightarrow{G_0} 6c6c6c6c_x, \epsilon = 2^{-9.40};\ \ 63636363_x \xrightarrow{G_2} 6c6c6c6c_x, \epsilon = 2^{-9.40};\\ &6c6c6c6c_x \xrightarrow{G_0} 72727272_x, \epsilon = 2^{-9.78};\ 6c6c6c6c_x \xrightarrow{G_2} 72727272_x, \epsilon = 2^{-11.24}.\end{aligned}$$

In addition, we identified 2-round linear approximation for active G_1 and G_3 as follows:

$$(0, m_{i1}, 0, m_{i3}) \xrightarrow{1r} (0, m_2, 0, m_2) \xrightarrow{1r} (0, m_3, 0, m_3). \tag{8}$$

We identified the maximum bias $2^{-36.95}$ for 2-round linear approximation as follows:

$$\begin{aligned}&(0, 99999999_x, 0, 66666666_x) \xrightarrow{1r} (0_x, 33333333_x, 0, 33333333_x)\\ &\xrightarrow{1r} (0, 66666666_x, 0, 66666666_x),\end{aligned} \tag{9}$$

where the linear approximations for G_1 and G_3 are

$$\begin{aligned}&99999999_x \xrightarrow{G_1} 33333333_x, \epsilon = 2^{-9.56};\quad 66666666_x \xrightarrow{G_3} 33333333_x, \epsilon = 2^{-9.56};\\ &33333333_x \xrightarrow{G_1} 66666666_x, \epsilon = 2^{-9.56};\quad 33333333_x \xrightarrow{G_3} 66666666_x, \epsilon = 2^{-11.27}.\end{aligned}$$

Three-Round Linear Approximations:

We found the 3-round linear approximation for active G_0 and G_2 as follows:

$$\begin{aligned}&(d8d8d8d8_x, 0, 1b1b1b1b_x, 0) \xrightarrow{1r} (63636363_x, 0, 63636363_x, 0)\\ &\xrightarrow{1r} (36363636_x, 0_x, 36363636_x, 0_x) \xrightarrow{1r} (63636363_x, 0, 63636363_x, 0),\end{aligned}$$

where the linear approximations for G_0 and G_2 are

$$\begin{aligned}&d8d8d8d8_x \xrightarrow{G_0} 63636363_x, \epsilon = 2^{-9.40};\quad 1b1b1b1b_x \xrightarrow{G_2} 63636363_x, \epsilon = 2^{-9.40};\\ &63636363_x \xrightarrow{G_0} 36363636_x, \epsilon = 2^{-13.76};\quad 63636363_x \xrightarrow{G_2} 36363636_x, \epsilon = 2^{-10.56};\\ &36363636_x \xrightarrow{G_0} 63636363_x, \epsilon = 2^{-13.76};\quad 36363636_x \xrightarrow{G_2} 63636363_x, \epsilon = 2^{-10.56}.\end{aligned}$$

The bias for the 3-round linear approximation is $2^{-9.40 \cdot 2 - 13.76 \cdot 2 - 10.56 \cdot 2 + 5} = 2^{-62.44}$. Moreover, if G_1 and G_3 are active, we identified two linear approximations for 3-round MMB with the maximum bias $2^{-55.78}$ as follows:

$$\begin{aligned}&(0_x, 99999999_x, 0_x, 66666666_x) \xrightarrow{1r} (0_x, 33333333_x, 0_x, 33333333_x)\\ &\xrightarrow{1r} (0_x, 66666666_x, 0_x, 66666666_x) \xrightarrow{1r} (0_x, 33333333_x, 0_x, 33333333_x),\end{aligned} \tag{10}$$

$$\begin{aligned}&(0, 33333333_x, 0, cccccccc_x) \xrightarrow{1r} (0, 66666666_x, 0, 66666666_x)\\ &\xrightarrow{1r} (0, 33333333_x, 0, 33333333_x) \xrightarrow{1r} (0, 66666666_x, 0, 66666666_x),\end{aligned} \tag{11}$$

where the linear approximations for G_1 and G_3 are

$$\begin{array}{ll} 99999999_x \xrightarrow{G_1} 33333333_x, \epsilon = 2^{-9.56}; & 66666666_x \xrightarrow{G_3} 33333333_x, \epsilon = 2^{-9.56};\\ 33333333_x \xrightarrow{G_1} 66666666_x, \epsilon = 2^{-9.56}; & 33333333_x \xrightarrow{G_3} 66666666_x, \epsilon = 2^{-11.27};\\ 66666666_x \xrightarrow{G_1} 33333333_x, \epsilon = 2^{-11.27}; & cccccccc_x \xrightarrow{G_3} 66666666_x, \epsilon = 2^{-9.56}. \end{array}$$

The bias for the two 3-round linear approximations is $2^{-9.56\cdot 2-9.56\cdot 2-11.27\cdot 2+5} = 2^{-55.78}$.

In Appendix B, we list a linear approximation for four rounds, but whose bias is too low for an effective attack.

5.2 Linear Attack on Reduced-Round MMB

Known Plaintext Linear Attack:

With the 3-round linear approximation in (10), a linear relation involving some plaintext bits, ciphertext bits and subkey bits can be derived. Using Algorithm 1 in [9], we can deduce the XOR value for the subkey bits involved in the linear relation. So, we can recover one bit of key information from 3-round MMB using $8 \cdot (2^{-55.78})^{-2} = 2^{114.56}$ KP and equivalent parity computations. Further, we can use the 3-round linear approximation in (11) to recover another one bit of key information from 3-round MMB. In all, two bits of key information can be recovered. For this step, the time complexity is $2^{115.56}$ parity computations. The remaining 126-bit subkey can be obtained by exhaustive search with about 2^{126} 3-round encryptions. In all, we can recover 128-bit key for 3-round MMB with $2^{114.56}$ known plaintexts and 2^{126} 3-round encryptions.

Ciphertext-Only Linear Attack:

If the plaintexts are ASCII, then particular bitmasks involving only the most significant bit of each plaintext byte may allow a ciphertext-only (CO) linear attack on MMB. This is a more attractive attack setting than the conventional known-plaintext (KP) setting, since an opponent only needs ciphertext blocks. For MMB, we have identified 2-round linear relations with bitmasks that involve only the most significant bits of bytes in plaintext blocks. The linear relation with active G_0 and G_2 is identified as follows:

$$\begin{aligned}&(80808080_x, 0, 80808080_x, 0) \xrightarrow{1r} (65656565_x, 0, 65656565_x, 0)\\ &\xrightarrow{1r} (1e1e1e1e_x, 0, 1e1e1e1e_x, 0),\end{aligned} \tag{12}$$

where the linear approximations for G_0 and G_2 are $80808080_x \xrightarrow{G_0} 65656565_x$, with $\epsilon = 2^{-15.74}$; $80808080_x \xrightarrow{G_2} 65656565_x$, with $\epsilon = 2^{-8.85}$; $65656565_x \xrightarrow{G_0}$

$1e1e1e1e_x$, with $\epsilon = 2^{-15.57}$; $65656565_x \xrightarrow{G_2} 1e1e1e1e_x$, with $\epsilon = 2^{-11.54}$. The bias for relation (12) is $2^{-15.74-8.85-15.57-11.54+3} = 2^{-48.70}$. The linear relation with active G_1 and G_3 is identified as follows:

$$\begin{aligned}&(0_x, 80808080_x, 0_x, 80808080_x) \xrightarrow{1r} (0_x, 59595959_x, 0_x, 59595959_x)\\ &\xrightarrow{1r} (0_x, 74747474_x, 0_x, 74747474_x),\end{aligned} \tag{13}$$

where the linear approximations for G_1 and G_3 are $80808080_x \xrightarrow{G_1} 59595959_x$, with $\epsilon = 2^{-8.85}$; $80808080_x \xrightarrow{G_3} 59595959_x$, with $\epsilon = 2^{-16.83}$; $59595959_x \xrightarrow{G_1} 74747474_x$, with $\epsilon = 2^{-11.85}$; $59595959_x \xrightarrow{G_3} 74747474_x$, with $\epsilon = 2^{-10.77}$. The bias for relation (13) is $2^{-8.85-16.83-11.85-10.77+3} = 2^{-45.30}$. This bias only leads to a distinguishing attack on 2-round MMB, with $8 \cdot (2^{-45.30)})^{-2} = 2^{93.60}$ CO, and equivalent number of parity computations.

6 Conclusions

This paper described the first detailed differential, square and linear attacks on versions 1.0 and 2.0 of the MMB block cipher, a design by Daemen, Govaerts and Vandewalle, dated from 1993, as an alternative to the IDEA block cipher. For differential cryptanalysis, the characteristic $\bar{0} \xrightarrow{\gamma} \bar{0}$ with probability 1 is the key point towards successful attack of the full MMB cipher. For square attack, the identical property of $\bar{0} \xrightarrow{\gamma} \bar{0}$ leads us to identify a new word type, the X word, which is relevant to identify 2.75-round square distinguishers. Without it, only 2-round square distinguishers can be found. For linear cryptanalysis, although the designers did not claim resistance of the MMB cipher against linear cryptanalysis, it is interesting that we were able to find better differential attacks than linear attacks.

A summary of our attacks is in Table 1. We have presented both distinguishing-from-random and key-recovery attacks on the full and reduced-round MMB cipher. Our attacks apply equally well to MMB version 2.0 [6], which only differs from the original MMB in the key schedule algorithm, designed to avoid related-key attacks.

An unusual property of the θ and γ layers of MMB under a square attack is described in Appendix C. This attack demonstrates the importance of the η layer in MMB, in order to resist square attacks.

Acknowledgements

It is a pleasure to acknowledge Xiaoyun Wang for various discussions on this paper. We would like to thank Yinglong Wang and Jinshan Pan in Shandong Computer Science Center for their providing the cluster computers to finish our experiments. We would also like to thank the anonymous reviewers for their very important comments.

This research is supported by 973 Program of China (Grant No. 2007CB807902) and National Outstanding Young Scientist fund of China (Grant No. 60525201).

Table 1. Summary of attacks on MMB.

#Rounds	Time	Data	Memory	Type
2	$2^{93.6}$ PC	$2^{93.6}$ CO	—	LC, DR
3	$2^{114.56}$ PC	$2^{114.56}$ KP	—	LC, DR
3	2^{126} EN	$2^{114.56}$ KP	—	LC, KR
4	$2^{126.32}$ EN	2^{34} CP	2^{64}	SC, KR
6	$2^{95.91}$ EN	2^{118} CP	2^{64}	DC, KR

PC: number of parity computations; EN: number of encryptions;
LC, DR: Linear Distinguishing Attack;
LC, KR: Key-recovery Attack with Linear Cryptanalysis;
DC, KR: Key-recovery Attack with Differential Cryptanalysis;
SC, KR: Key-recovery Attack with Square Cryptanalysis.

References

1. A.A. Selcuk, A. Bicak, On Probability of Success in Linear and Differential Cryptanalysis, SCN 2002, Springer, LNCS 2576, 2003, 174–185.
2. A. Biryukov, A. Shamir, Structural Cryptanalysis of SASAS, Adv. in Cryptology, Eurocrypt 2001, Springer, LNCS 2045, 2001, 394–405.
3. E. Biham, A. Shamir, Differential Cryptanalysis of DES-like Cryptosystems, Journal of Cryptology, vol.4, no.1, Springer, 1991, 3–72.
4. J. Daemen, R. Govaerts, J. Vandewalle, Block Ciphers Based on Modular Multiplication, Proceedings of 3rd Symposium on State and Progress of Research in Cryptography, W. Wolfowicz, (ed.), Fondazione Ugo Bordoni, 1993, 80–89.
5. J. Daemen, L. Van Linden, R. Govaerts and J. Vandewalle, Propagation Properties of Multiplication Modulo $2^n - 1$, Proceedings of the 13th Symposium on Information Theory in the Benelux, Werkgemeenschap voor informatie- en Communicatietheorie, Enschede, The Netherlands, 1992, 111–118.
6. J. Daemen, Cipher and Hash Function Design – Strategies based on Linear and Differential Cryptanalysis, PhD Thesis, Dept. Elektrotechniek, Katholieke Universiteit Leuven, Belgium, Mar. 1995.
7. J. Daemen, L.R. Knudsen, V. Rijmen, The Block Cipher Square, 4th Fast Software Encryption Workshop (FSE), E. Biham, Ed., Springer, LNCS 1267, 1997, 149–165.
8. X. Lai, On the Design and Security of Block Ciphers, ETH Series in Information Processing, J.L. Massey (ed.), Vol. 1, 1995, Hartung-Gorre Verlag, Konstanz.
9. M. Matsui, Linear Cryptanalysis Method for DES Cipher, Adv. in Cryptology, Eurocrypt'93, T. Helleseth (ed.), Springer, LNCS 765, 1994, 386–397.
10. M. Matsui, The First Experimental Cryptanalysis of the Data Encryption Standard, Adv. in Cryptology, Crypto'94, Y.G. Desmedt (ed.), Springer, LNCS 839, 1994, 1–11.
11. V. Rijmen, J. Daemen, B. Preneel, A. Bosselaers, E. De Win, The Cipher SHARK, 3rd International Workshop on Fast Software Encryption (FSE), D. Gollmann (ed.), Springer, LNCS 1039, 1996, 99–111.

Appendix

Table 2. One-round differential characteristics for MMB: $\Delta_{ij}(0 \le j \le 3)$, and Δ_o are nonzero 32-bit xor difference values.

input difference $\xrightarrow{1r}$ output difference	# active multiplications	restriction on Δ_o
$(\Delta_{i0}, 0, 0, 0) \xrightarrow{1r} (\Delta_o, \Delta_o, 0, \Delta_o)$	1	lsb(Δ_o)=0
$(0, \Delta_{i1}, 0, 0) \xrightarrow{1r} (\Delta_o, \Delta_o, \Delta_o, 0)$	1	—
$(0, 0, \Delta_{i2}, 0) \xrightarrow{1r} (0, \Delta_o, \Delta_o, \Delta_o)$	1	—
$(0, 0, 0, \Delta_{i3}) \xrightarrow{1r} (\Delta_o, 0, \Delta_o, \Delta_o)$	1	lsb(Δ_o)=0
$(\Delta_{i0}, \Delta_{i1}, 0, 0) \xrightarrow{1r} (0, 0, \Delta_o, \Delta_o)$	2	lsb(Δ_o)=0
$(\Delta_{i0}, 0, \Delta_{i2}, 0) \xrightarrow{1r} (\Delta_o, 0, \Delta_o, 0)$	2	lsb(Δ_o)=0
$(\Delta_{i0}, 0, 0, \Delta_{i3}) \xrightarrow{1r} (0, \Delta_o, \Delta_o, 0)$	2	lsb(Δ_o)=0
$(0, \Delta_{i1}, \Delta_{i2}, 0) \xrightarrow{1r} (\Delta_o, 0, 0, \Delta_o)$	2	—
$(0, \Delta_{i1}, 0, \Delta_{i3}) \xrightarrow{1r} (0, \Delta_o, 0, \Delta_o)$	2	lsb(Δ_o)=0
$(0, 0, \Delta_{i2}, \Delta_{i3}) \xrightarrow{1r} (\Delta_o, \Delta_o, 0, 0)$	2	lsb(Δ_o)=0
$(\Delta_{i0}, \Delta_{i1}, \Delta_{i2}, 0) \xrightarrow{1r} (0, \Delta_o, 0, 0)$	3	lsb(Δ_o)=0
$(\Delta_{i0}, \Delta_{i1}, 0, \Delta_{i3}) \xrightarrow{1r} (\Delta_o, 0, 0, 0)$	3	lsb(Δ_o)=0
$(\Delta_{i0}, 0, \Delta_{i2}, \Delta_{i3}) \xrightarrow{1r} (0, 0, 0, \Delta_o)$	3	lsb(Δ_o)=0
$(0, \Delta_{i1}, \Delta_{i2}, \Delta_{i3}) \xrightarrow{1r} (0, 0, \Delta_o, 0)$	3	lsb(Δ_o)=0
$(\Delta_{i0}, \Delta_{i1}, \Delta_{i2}, \Delta_{i3}) \xrightarrow{1r} (\Delta_o, \Delta_o, \Delta_o, \Delta_o)$	4	lsb(Δ_o)=0

Table 3. One-round linear relations for MMB: $m_{ij}(0 \le j \le 3)$, and m_o are nonzero 32-bit masks.

input mask $\xrightarrow{1r}$ output mask	#active multiplications	restriction on m_o
$(m_{i0}, 0, 0, 0) \xrightarrow{1r} (m_o, m_o, 0, m_o)$	1	$m_o \cdot \delta = 0$
$(0, m_i, 0, 0) \xrightarrow{1r} (m_o, m_o, m_o, 0)$	1	—
$(0, 0, m_i, 0) \xrightarrow{1r} (0, m_o, m_o, m_o)$	1	—
$(0, 0, 0, m_i) \xrightarrow{1r} (m_o, 0, m_o, m_o)$	1	$m_o \cdot \delta = 0$
$(m_{i0}, m_{i1}, 0, 0) \xrightarrow{1r} (0, 0, m_o, m_o)$	2	$m_o \cdot \delta = 0$
$(m_{i0}, 0, m_{i2}, 0) \xrightarrow{1r} (m_o, 0, m_o, 0)$	2	$m_o \cdot \delta = 0$
$(m_{i0}, 0, 0, m_{i3}) \xrightarrow{1r} (0, m_o, m_o, 0)$	2	$m_o \cdot \delta = 0$
$(0, m_{i1}, m_{i2}, 0) \xrightarrow{1r} (m_o, 0, 0, m_o)$	2	—
$(0, m_{i1}, 0, m_{i3}) \xrightarrow{1r} (0, m_o, 0, m_o)$	2	$m_o \cdot \delta = 0$
$(0, 0, m_{i2}, m_{i3}) \xrightarrow{1r} (m_o, m_o, 0, 0)$	2	$m_o \cdot \delta = 0$
$(m_{i0}, m_{i1}, m_{i2}, 0) \xrightarrow{1r} (0, m_o, 0, 0)$	3	$m_o \cdot \delta = 0$
$(m_{i0}, m_{i1}, 0, m_{i3}) \xrightarrow{1r} (m_o, 0, 0, 0)$	3	$m_o \cdot \delta = 0$
$(m_{i0}, 0, m_{i2}, m_{i3}) \xrightarrow{1r} (0, 0, 0, m_o)$	3	$m_o \cdot \delta = 0$
$(0, m_{i1}, m_{i2}, m_{i3}) \xrightarrow{1r} (0, 0, m_o, 0)$	3	$m_o \cdot \delta = 0$
$(m_{i0}, m_{i1}, m_{i2}, m_{i3}) \xrightarrow{1r} (m_o, m_o, m_o, m_o)$	4	$m_o \cdot \delta = 0$

A Proofs of Square Distinguishers

A.1.Proof of the First Distinguisher:

For the first distinguisher, we denote each word after η in the first round as $S(v)$; S is the status for the word, such as A, B, E and X, and v represents the variable; the first distinguisher can be written as

$$
\begin{aligned}
&(A,C,C,C) \overset{\sigma[k^0]}{\rightarrow} (A,C,C,C) \overset{\gamma}{\rightarrow} (A,C,C,C) \overset{\eta}{\rightarrow} (A(x),C(c_1),C(c_2),C(c_3))\\
&\overset{\theta}{\rightarrow} (A(x\oplus c_1\oplus c_3),A(x\oplus c_1\oplus c_2),C(c_1\oplus c_2\oplus c_3),A(x\oplus c_2\oplus c_3))\\
&\overset{\sigma[k^1]}{\rightarrow} (A(x\oplus c_1\oplus c_3\oplus k_0^1),A(x\oplus c_1\oplus c_2\oplus k_1^1),C(c_1\oplus c_2\oplus c_3\oplus k_2^1),\\
&A(x\oplus c_2\oplus c_3\oplus k_3^1))\\
&\overset{\gamma}{\rightarrow} (A(G_0\otimes(x\oplus c_1\oplus c_3\oplus k_0^1)),A(G_1\otimes(x\oplus c_1\oplus c_2\oplus k_1^1)),\\
&C(G_2\otimes(c_1\oplus c_2\oplus c_3\oplus k_2^1)),A(G_3\otimes(x\oplus c_2\oplus c_3\oplus k_3^1)))\\
&\overset{\eta}{\rightarrow} (A(\eta(G_0\otimes(x\oplus c_1\oplus c_3\oplus k_0^1))),A(G_1\otimes(x\oplus c_1\oplus c_2\oplus k_1^1)),\\
&C(G_2\otimes(c_1\oplus c_2\oplus c_3\oplus k_2^1)),A(\eta(G_3\otimes(x\oplus c_2\oplus c_3\oplus k_3^1))))\\
&\overset{\theta}{\rightarrow} (X(y_0),B(y_1),B(y_2),E(y_3))\\
&\overset{\sigma[k^2]}{\rightarrow} (X(y_0\oplus k_0^2),B(y_1\oplus k_1^2),B(y_2\oplus k_2^2),E(y_3\oplus k_3^2))\\
&\overset{\gamma}{\rightarrow} (X(z_0),?(z_1),?(z_2),E(z_3))\\
&\overset{\eta}{\rightarrow} (B(u_0),?(u_1),?(u_2),E(u_3)).
\end{aligned}
$$

In the above transitions, the first output word of η in the first round is an A word and the other three output words are constants, so we denote them as the variables x, c_1, c_2 and c_3, respectively. In addition, η only affects the output of the first and the last words. We denote the four status variables after the operation of θ in the second round as $y_i(0 \le i \le 3)$, the four words after γ in the third round as $z_i(0 \le i \le 3)$, and the four words after η in the third round as $u_i(0 \le i \le 3)$. The square distinguisher can be proved in three steps.

1. Prove that y_0 is X, y_3 is E and both y_1 and y_2 are B words.
2. Prove that z_0 is an X word and z_3 is an E word.
3. Prove that u_0 is a B word and u_3 is an E word.

Step 1: Prove that y_0 is X, y_3 is E and both y_1 and y_2 are B words:

We extend y_i as follows:

$$
\begin{aligned}
y_0 = \eta(G_0\otimes(x\oplus c_1\oplus c_3\oplus k_0^1))\oplus(G_1\otimes(x\oplus c_1\oplus c_2\oplus k_1^1))\oplus\\
\eta(G_3\otimes(x\oplus c_2\oplus c_3\oplus k_3^1)),
\end{aligned}
\tag{14}
$$

$$
\begin{aligned}
y_1 = \eta(G_0\otimes(x\oplus c_1\oplus c_3\oplus k_0^1))\oplus(G_1\otimes(x\oplus c_1\oplus c_2\oplus k_1^1))\oplus\\
(G_2\otimes(c_1\oplus c_2\oplus c_3\oplus k_2^1)),
\end{aligned}
\tag{15}
$$

$$
\begin{aligned}
y_2 = (G_1\otimes(x\oplus c_1\oplus c_2\oplus k_1^1))\oplus(G_2\otimes(c_1\oplus c_2\oplus c_3\oplus k_2^1))\oplus\\
\eta(G_3\otimes(x\oplus c_2\oplus c_3\oplus k_3^1)),
\end{aligned}
\tag{16}
$$

$$y_3 = \eta(G_0 \otimes (x \oplus c_1 \oplus c_3 \oplus k_0^1)) \oplus (G_2 \otimes (c_1 \oplus c_2 \oplus c_3 \oplus k_2^1)) \oplus \eta(G_3 \otimes (x \oplus c_2 \oplus c_3 \oplus k_3^1)). \quad (17)$$

In (14)–(17), x is a variable of an A word, so the input x and $\neg x$ must appear once each. Then, we have

$$\begin{aligned} &y_0(x) \oplus y_0(\neg x) = \eta(G_0 \otimes (x \oplus c_1 \oplus c_3 \oplus k_0^1)) \oplus \eta(G_0 \otimes (\neg x \oplus c_1 \oplus c_3 \oplus k_0^1)) \\ &\oplus (G_1 \otimes (x \oplus c_1 \oplus c_2 \oplus k_1^1)) \oplus (G_1 \otimes (\neg x \oplus c_1 \oplus c_2 \oplus k_1^1)) \\ &\oplus \eta(G_3 \otimes (x \oplus c_2 \oplus c_3 \oplus k_3^1)) \oplus \eta(G_3 \otimes (\neg x \oplus c_2 \oplus c_3 \oplus k_3^1)). \end{aligned}$$

Due to

$$\begin{aligned} &G_i \otimes (\neg x \oplus c) = G_i \otimes (\bar{0} \oplus x \oplus c) = G_i \otimes (\bar{0} \oplus (x \oplus c)) \\ &= G_i \otimes (\bar{0} - (x \oplus c)) = (G_i \otimes \bar{0}) - G_i \otimes (x \oplus c) \\ &= \bar{0} - G_i \otimes (x \oplus c) = \bar{0} \oplus G_i \otimes (x \oplus c) = \neg(G_i \otimes (x \oplus c)) \end{aligned} \quad (18)$$

and

$$\eta(w) \oplus \eta(\neg w) = \delta \oplus \bar{0} = d5555555_x, \quad (19)$$

we obtain

$$\begin{aligned} &y_0(x) \oplus y_0(\neg x) = \eta(G_0 \otimes (x \oplus c_1 \oplus c_3 \oplus k_0^1)) \oplus \eta(\neg(G_0 \otimes (x \oplus c_1 \oplus c_3 \oplus k_0^1))) \\ &\oplus (G_1 \otimes (x \oplus c_1 \oplus c_2 \oplus k_1^1)) \oplus \neg(G_1 \otimes (x \oplus c_1 \oplus c_2 \oplus k_1^1)) \\ &\oplus \eta(G_3 \otimes (x \oplus c_2 \oplus c_3 \oplus k_3^1)) \oplus \eta(\neg(G_3 \otimes (x \oplus c_2 \oplus c_3 \oplus k_3^1))) \\ &= d5555555_x \oplus \bar{0} \oplus d5555555_x = \bar{0}. \end{aligned}$$

We derive $y_0(x) = \neg y_0(\neg x)$. As a variable of an A word, both x and $\neg x$ must appear once each. So, $y_0(x)$ and $y_0(\neg x) = \neg y_0(x)$ must appear just as often. There are 2^{31} pairs of $(x, \neg x)$, so there are 2^{31} pairs of $(y_0, \neg y_0)$, which means that the xor sum of 2^{32} y_0 is zero (equal to 2^{31} times of the xor sum of $\bar{0}$). Therefore, y_0 is an X word.

$$\begin{aligned} &y_3(x) \oplus y_3(\neg x) = \eta(G_0 \otimes (x \oplus c_1 \oplus c_3 \oplus k_0^1)) \oplus \eta(G_0 \otimes (\neg x \oplus c_1 \oplus c_3 \oplus k_0^1)) \\ &\oplus (G_2 \otimes (c_1 \oplus c_2 \oplus c_3 \oplus k_2^1)) \oplus (G_2 \otimes (c_1 \oplus c_2 \oplus c_3 \oplus k_2^1)) \\ &\oplus \eta(G_3 \otimes (x \oplus c_2 \oplus c_3 \oplus k_3^1)) \oplus \eta(G_3 \otimes (\neg x \oplus c_2 \oplus c_3 \oplus k_3^1)) \\ &= d5555555_x \oplus d5555555_x = 0 \end{aligned}$$

We obtain $y_3(x) = y_3(\neg x)$, i.e. any value of y_3 will appear an even number of times, so y_3 is an E word.

$$\begin{aligned} &y_1(x) \oplus y_1(\neg x) = \eta(G_0 \otimes (x \oplus c_1 \oplus c_3 \oplus k_0^1))) \oplus \eta(G_0 \otimes (\neg x \oplus c_1 \oplus c_3 \oplus k_0^1))) \\ &\oplus (G_1 \otimes (x \oplus c_1 \oplus c_2 \oplus k_1^1)) \oplus (G_1 \otimes (\neg x \oplus c_1 \oplus c_2 \oplus k_1^1)) \\ &\oplus (G_2 \otimes (c_1 \oplus c_2 \oplus c_3 \oplus k_2^1)) \oplus (G_2 \otimes (c_1 \oplus c_2 \oplus c_3 \oplus k_2^1)) \\ &= d5555555_x \oplus \bar{0} = \delta \end{aligned}$$

We cannot assure that y_1 and $\neg y_1$ appear at the same time, so y_1 is not an X word. But, 2^{31} pairs of $(x, \neg x)$ result in the xor sum of 2^{32} y_1 is zero (equal to 2^{31} times of the xor sum of δ). So, y_1 is a B word. In this way, we can prove y_2 is also a B word.

Step 2: Prove that z_0 is an X word and z_3 is an E word:

We extend y_i as the following equations,

$$z_0 = G_0 \otimes (y_0 \oplus k_0^2),\ z_1 = G_1 \otimes (y_1 \oplus k_1^2),$$
$$z_2 = G_2 \otimes (y_2 \oplus k_2^2),\ z_3 = G_3 \otimes (y_3 \oplus k_3^2).$$

We have proved y_0 is an X word which means that y_0 and $\neg y_0$ must appear at the same time. From (18), $G_0 \otimes (y_0 \oplus k_0^2) = \neg G_0 \otimes (\neg y_0 \oplus k_0^2)$, we can obtain $z_0(y_0) = \neg z_0(\neg y_0)$, which means any value of z_0 and $\neg z_0$ will appear at the same time. So z_0 is also an X word.

In addition, y_3 is an E word which means that any value of y_3 will appear an even number of times and results any value of z_3 will appear an even number of times too. Thus, z_3 should be an E word, too. Because y_1 and y_2 are B words, and B words cannot usually cross γ, so the status for z_1 and z_2 cannot be decided.

Step 3: Prove that u_0 is a B word and u_3 is an E word:

We extend u_i as the following $u_0 = \eta(z_0)$, $u_1 = \eta(z_1) = z_1$, $u_2 = \eta(z_2) = z_2$, $u_3 = \eta(z_3)$. Recall that z_0 is an X word, which means that any value of z_0 and $\neg z_0$ will appear at the same time. From (19), $u_0(z_0) \oplus u_0(\neg z_0) = d5555555_x$. There are 2^{31} pairs of $(u_0(z_0), u_0(\neg z_0))$. So, the xor sum of 2^{32} u_0 is zero (equal to 2^{31} times of the xor sum for $d5555555_x$). Therefore, u_0 is a B word but not an X word. Since z_3 is an E word, it follows that any value of $u_3(z_3)$ will appear even times. So, u_3 is an E word. After θ in the third round, the balanced property will be destroyed in all four words.

A.2.Proof of the other three Distinguishers:

The proof of the other three distinguishers is similar to the above proof for the first distinguisher.

B Four-Round Linear Approximation

We have identified a 4-round linear relation with bias $2^{3\cdot(-9.56-11.27)-9.56\cdot 2+7} = 2^{-74.61}$ which is given as follows:

$$(0_x, 99999999_x, 0_x, 66666666_x) \xrightarrow{1r} (0_x, 33333333_x, 0_x, 33333333_x)$$
$$\xrightarrow{1r} (0_x, 66666666_x, 0_x, 66666666_x) \xrightarrow{1r} (0_x, 33333333_x, 0_x, 33333333_x)$$
$$\xrightarrow{1r} (0_x, 66666666_x, 0_x, 66666666_x).$$

C A note on the $\theta \circ \gamma \circ \sigma$ layer

Consider a modified MMB cipher whose round structure does not include η (call it MMB$-\eta$, read "MMB minus η"), that is, a full round consists of only $\theta \circ \gamma \circ \sigma$.

We have verified very peculiar Λ-set propagations in MMB$-\eta$, such as (A, C, C, C) $\stackrel{1r}{\rightarrow}$ (A, A, C, A) $\stackrel{1r}{\rightarrow}$ (X, E, E, E) $\stackrel{1r}{\rightarrow}$ (X, X, E, X) $\stackrel{1r}{\rightarrow}$ (X, E, E, E). After the fourth round, the patterns (X, X, E, X) and (X, E, E, E) alternate, that is, balanced Λ-sets propagate **indefinitely (for an arbitrary number of rounds)**. This unusual behavior can be explained similarly to that of other patterns in Sect. 4. We concluded that

- this property does not depend on the round subkeys, or on the user key or even on the key schedule;
- this property is independent of the particular permutation used in the initial A word, or the constants used in the C words;
- it highlights the importance of the η layer (a data-dependent, nonlinear operation) in the security of the original MMB against square attacks, since its presence destroys the propagation of balanced Λ-sets after 2.75 rounds;
- the above distinguish-from-random attack applies to an arbitary number of rounds of MMB-η and costs only 2^{32} CP, an equivalent number of encryptions and negligible memory.