Regular Paper

On Applicability of Differential Cryptanalysis, Linear Cryptanalysis and Mod n Cryptanalysis to an Encryption Algorithm M8 (ISO9979-20)

Toshio Tokita[†,††] and Tsutomu Matsumoto[†,†††]

This paper discusses the security of M8, which is an encryption algorithm registered in ISO9979 (No.20). M8 is a common key block cipher, of which block size is 64 bits and the number of rounds is variable, and has an encryption key and system keys, where the latter determines the structure of M8. We discuss applicability of 'differential cryptanalysis', 'linear cryptanalysis' and 'mod n cryptanalysis' to M8, respectively. As a result, we show that there exist 'differential' and 'linear' characteristics that hold with probability $p = 1$ and 'mod n' characters of which bias is remarkably high. These facts show that the strength of M8 is strongly dependent on the values of system keys.

1. Introduction

In this paper, we discuss the security of M8[3], which is an encryption algorithm registered in ISO9979 (No.20) by Hitachi, Ltd. in March, 1999. M8 is a common key block cipher, of which block size is 64 bits, and has an encryption key, of which size is 64 bits or more. The number of rounds (N) is variable and the round function is constructed from 32-bit rotation shift, 32-bit modular addition and 32-bit exclusive-or, which are specified by the system keys (algorithm determination keys (N×24 bits) and algorithm extension key (N × 96 bits)).

The encryption algorithm M8 is proposed to the international standard, ISO9979, and its specification is made open. And the structure of M8 is determined by the system keys, but the recommended system keys are not expressed clearly by the proponent of M8. Moreover, while the proponent of M8 recommends 10 or more as the number of rounds (N) from the viewpoint of security, the details of the evidence are not opened at the place of ISO and institutions. Generally, a user, who has no special knowledge of encryption algorithms, has no way to doubt the claims of the proponent. But, for the disproof of the claim of the proponent, Kaneko[8] showed that inappropriate system keys keep the outputs of round function constant, and in that case we can convert M8 to an equivalent system with smaller number of rounds. As the number of rounds, the proponent of M8 recommends 10 or more. Kaneko deduced a recurrence formula which gives the equivalent number of rounds distribution for such case. He showed that there exist weak keys which give the equivalent number of rounds less than 4 with probability 10^{-4} for 10-round M8. This means that a part of the claims of the proponent is not true in some cases depending on system keys.

Generally speaking, the researcher and developer must discuss and show the security of encryption algorithms, which specifications are opened at least, in order that we build the solid information & computer society at present and in the future.

As other approaches of cryptanalysis of M8, Sano and Matsumoto[10),11] discussed the weak keys, which are not expressed by the proponent. They showed that there exist fixed point and opposite fixed point for some system keys. Saito and Kaneko[13], and Tokita[9),12] discussed the properties of F-function of M8 from the viewpoint of the experimental approaches, respectively.

In this paper, as the another approach different from these researches, we discuss the applicability of specific cryptanalytic attacks on M8. Concretely, we note differential cryptanalysis[1], linear cryptanalysis[2], and Mod n cryptanalysis[5]. Our approaches are from the viewpoint of attackers and evaluators. We show there exist the weak system keys, on which these cryptanalytic attack techniques are applicable sufficiently or dramatically.

Of course, there exists the approach that we show the recommended system keys, on which M8 is sufficiently or dramatically strong against

[†] Graduate School of Engineering, Yokohama National University

[††] Information Technology R&D Center, Mitsubishi Electric Corporation

[†††] Graduate School of Environment and Information Sciences, Yokohama National University

these cryptanalytic attack techniques. This is a open problem. We think it is desirable that the proponent of M8 shows the recommended system keys.

Firstly, we discuss applicability of differential cryptanalysis to M8, which was proposed by Biham and Shamir in 1990 and uses the differential characteristic (differential value) between ciphertext and plaintext in cryptanalysis [1]. An encryption algorithm becomes stronger against differential cryptanalysis, when the number of rounds increases. However, we show that M8 has differential characteristics (differential values) that hold with probability $p = 1$ without dependence on the number of rounds.

Secondly, we discuss applicability of linear cryptanalysis to M8, which was proposed by Matsui in 1993 and uses the linear characteristic (mask value) with bias probability from 1/2 [2]. An encryption algorithm becomes stronger against linear cryptanalysis, when the number of rounds increases. However, we show that M8 has linear characteristics (mask values) that hold with bias probability $p = 1/2$ without dependence on the number of rounds.

Finally, we discuss applicability of mod n cryptanalysis [5] to M8. Mod n cryptanalysis was proposed by Kelsey *et al.* in 1999, which uses the bias of distribution of mod n value. Kelsey *et al.* tried known-plaintext attack using mod n cryptanalysis on RC5P an M6, and showed M6 has the large bias in the difference between lower (higher) 32 bit-ciphertext and lower (higher) 32 bit-plaintext with high probability. In this paper we discuss applicability of known-plaintext attack using mod n cryptanalysis to M8, and show that M8 has system keys, which determine the structure that has large bias of distribution of difference value between lower (higher) 32 bit-ciphertext and lower (higher) 32 bit-plaintext with high probability.

As a result in this paper, we conclude that the strength of M8 against differential cryptanalysis, linear cryptanalysis and mod n cryptanalysis is strongly dependent on the values of system keys, and must be evaluated for each system key.

The contents of this paper are as follow: In Section 2, we show the notations and the outline of M8. In Section 3, we set the basic component of round function of M8 and begin by studying its statistical properties. In Section 4, we discuss the special cases (the left-rotation shift amount is equal to '0') and applicability of differential cryptanalysis, linear cryptanalysis and mod n cryptanalysis to M8, respectively. In Section 5, we conclude the discussion of this paper.

2. Preliminaries

2.1 Notations

The notations, in this paper, are as follows: (The right direction means the lower direction. The lowest bit location means the 0-th order bit location.)

P	: plaintext (64 bits)
P_L, P_R	: upper, lower plaintext (32 bits)
C	: ciphertext (64 bits)
C_L, C_R	: upper, lower ciphertext (32 bits)
$C_{L,i}$, $C_{R,i}$	: upper, lower ciphertext of the i-th round (32 bits)
$K_{L,i}$, $K_{R,i}$	: upper, lower expansion key of the i-th round (32 bits)
ΔX, $\Delta f(X)$	: exclusive-or difference of X, $f(X)$ (32 bits)
$\Delta_{j,i}$	: exclusive-or difference with '1' per j bits from i-th bit location (32 bits)
ΓX, $\Gamma f(X)$	: mask of X, $f(X)$ (32 bits)
$\Gamma_{j,i}$	: mask with '1' per j bits from i-th bit location (32 bits)
$X \oplus Y$	: bitwise XOR operation (32 bits)
$X + Y$	: modular 2^{32} addition operation (32 bits)
$X \bullet Y$	: parity bit of bitwise AND (masked value) (1 bit)

2.2 M8

We show the outline of data randomization part of M8. For more detail and the key schedule part, see Ref. 3). **Figure 1** shows the one round of the data randomization part of M8. In this paper, we define it as 'the round function of M8'. **Figure 2** shows the basic component, which is used for the study of the statistical property in Section 3.

The number of rounds of M8 is variable. The structure of Fig. 1 is iterated N times as extension Feistel type and determined by the following system keys (algorithm determination key and algorithm extension key), etc:

[algorithm determination key (N × 24 bits)]

▷ N: number of rounds

▷ [*unit* 1] . . . [*unit* 9]: kind of unit function (9 × 1 bits)

0: 2^{32} modular addition, 1: bitwise exclusive-or

▷ $S1$, $S2$, $S3$: left-rotation shift amount (3 ×

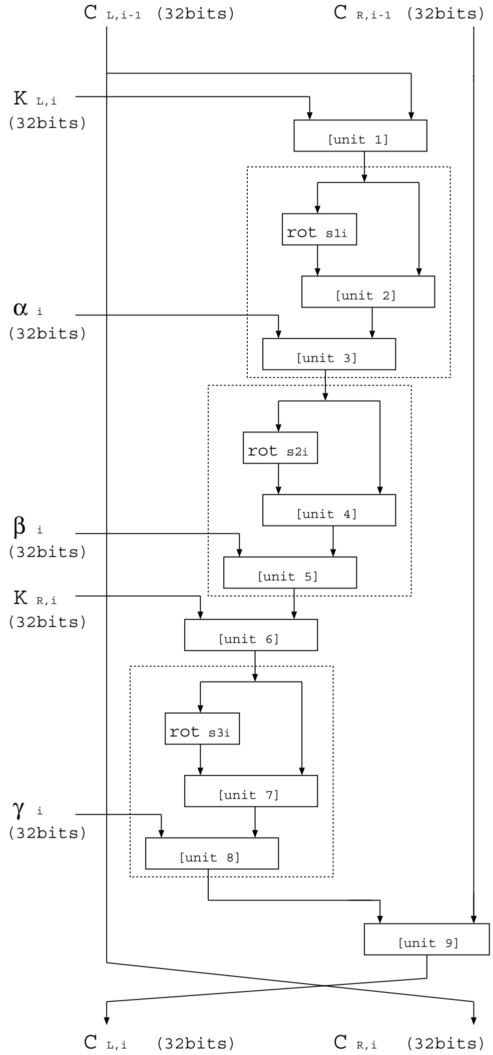

Fig. 1 The round function of M8.

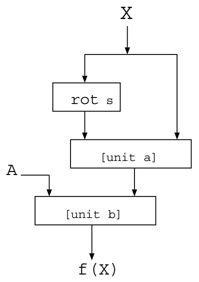

Fig. 2 The basic component of M8.

5 bits)
[algorithm extension key (N × 96 bits)]
▷ α, β, γ: input of [*unit* 3], [*unit* 5], [*unit* 8] (32 bits)

Note 1: In Fig. 1, suffix 'i' means i-th round.

Table 1 Pairs of S and ΔX such as $\Delta f(X) = 0$ with probability $p = 1$ ([*unit a*], [*unit b*]: XOR).

	S ($0 \le S \le 31$)	ΔX	$\Delta f(X)$	p
(1)	0	anything	0	1
(2)	odd numbers	*all* '1'	0	1
(3)	2, 6, 10, 14 18, 22, 26, 30	$\{\Sigma_{i=0}^{1}(k_i\Delta_{2,i})\}$ $k_i \in \{0,1\}$	0	1
(4)	4, 12, 20, 28	$\{\Sigma_{i=0}^{3}(k_i\Delta_{4,i})\}$ $k_i \in \{0,1\}$	0	1
(5)	8, 24	$\{\Sigma_{i=0}^{7}(k_i\Delta_{8,i})\}$ $k_i \in \{0,1\}$	0	1
(6)	16	$\{\Sigma_{i=0}^{15}(k_i\Delta_{16,i})\}$ $k_i \in \{0,1\}$	0	1

Note: Σ means bitwise XOR.

Note 2: Fig. 2 is equal to the part by dotted line in Fig. 1.

3. Cryptanalysis of the Basic Component of M8

To do cryptanalysis of M8, we begin by studying properties of the basic component of M8, noted in Fig. 2, which is equal to the surrounded part by dotted line in Fig. 1, against differential cryptanalysis, linear cryptanalysis and mod n cryptanalysis, respectively.

3.1 Differential Characteristics

In this section, we discuss the properties of the basic component of M8 in regard to differential cryptanalysis. We show that there exist the remarkable properties, in case the both of [*unit a*] and [*unit b*] are bitwise exclusive-or (XOR). We derive and summarize the remarkable differential characteristics in **Table 1**. S means the left-rotation shift amount.

Table 1 shows that, when input difference ΔX is the value described in Table 1 against the left-rotation shift amount S, output difference $\Delta f(X)$ becomes '0' with probability $p = 1$. Also, Table 1 shows that, when input difference value ΔX is *all* '1', output difference $\Delta f(X)$ is *all* '0' with probability $p = 1$, without dependence on the left-rotation shift amount S. These facts show that there exists the weakness of the basic component of M8, strongly dependent on the values of system keys, against differential cryptanalysis.

3.2 Linear Characteristics

In this section, we discuss the properties of the basic component of M8 in regard to linear cryptanalysis. We show that there exist the remarkable properties, in case the both of [*unit a*] and [*unit b*] are bitwise exclusive-or (XOR). We generalize Aoki-Kurokawa's discussion[4] in re-

Table 2 Pairs of S and $\Gamma f(X)$ such as $\Gamma X = 0$ with probability $p = 1$ ([*unit a*], [*unit b*]: XOR).

	S $(0 \leq S \leq 31)$	ΓX	$\Gamma f(X)$	p
(1)	0	0	anything	1
(2)	odd numbers	0	*all* '1'	1
(3)	2, 6, 10, 14 18, 22, 26, 30	0	$\{\Sigma_{i=0}^{1}(k_i\Delta_{2,i})\}$ $k_i \in \{0,1\}$	1
(4)	4, 12, 20, 28	0	$\{\Sigma_{i=0}^{3}(k_i\Delta_{4,i})\}$ $k_i \in \{0,1\}$	1
(5)	8, 24	0	$\{\Sigma_{i=0}^{7}(k_i\Delta_{8,i})\}$ $k_i \in \{0,1\}$	1
(6)	16	0	$\{\Sigma_{i=0}^{15}(k_i\Delta_{16,i})\}$ $k_i \in \{0,1\}$	1

Note: Σ means bitwise XOR.

gard to linear properties of Multi-2, derive and summarize the remarkable linear characteristics in **Table 2**. S means the left-rotation shift amount.

Table 2 shows that, when output mask $\Gamma f(X)$ is the value described in Table 2 against the left-rotation shift amount S, input mask ΓX becomes *all* '0' with probability $p = 1$ and output masked value $\Gamma f(X) \bullet f(X)$ becomes $\Gamma f(X) \bullet A$ with probability $p = 1$. Also, when output mask $\Gamma f(X)$ is *all* '1', output masked value $\Gamma f(X) \bullet f(X)$ becomes $\Gamma f(X) \bullet A$ with probability $p = 1$, without dependence on the left-rotation shift amount S. These facts show that there exists the weakness of the basic component of M8, strongly dependent on the values of system keys, against linear cryptanalysis.

3.3 Mod n Characteristics

In this section, we discuss the properties of the basic component of M8 in regard to mod n cryptanalysis[5]. We show that there exist the remarkable properties, in case the both of [*unit a*] and [*unit b*] are 2^{32} modular addition (mod 2^{32}). For any X, $rot_S(X) \equiv 2^S X \bmod (2^{32}-1)$ is true[5]. Then,

$$X + rot_S(X) = X + rot_S(X) - 2^{32}k$$
$$\equiv (2^S+1)X - 2^{32}k \pmod{(2^{32}-1)}$$
$$(k \in \{0,1\}).$$

Because of $2^{32} - 1 = 3 \times 5 \times 17 \times 257 \times 65537$, the following equation is true,

$$2^{32} \equiv 1 \bmod n \ (n \in \{3, 5, 17, 257, 65537\}).$$

Then, for $n \in \{3, 5, 17, 257, 65537\}$ such that $2^S + 1 \equiv 0 \bmod n$,

$$X + rot_S(X) \equiv -k \bmod n \ (k \in 0, 1).$$

We derive and summarize S and n such as $2^S + 1 \equiv 0 \bmod n$ ($0 \leq S \leq 31$, $n \in \{3, 5, 17, 257, 65537\}$) in **Table 3**.

In the case of $S = 0$, $(X + rot_0(X) \equiv 2X \bmod 2^{32} \equiv 0 \bmod 2$. Then, we summarize the remarkable mod n characteristics in **Table 4**.

Table 3 S and n such as $2^S + 1 \equiv 0$.

S	n	S	n	S	n	S	n
0	-	8	257	16	65537	24	257
1	3	9	3	17	3	25	3
2	5	10	5	18	5	26	5
3	3	11	3	19	3	27	3
4	17	12	17	20	17	28	17
5	3	13	3	21	3	29	3
6	5	14	5	22	5	30	5
7	3	15	3	23	3	31	3

Table 4 $f(X) \bmod n$ ([*unit a*], [*unit* b]: mod 2^{32} ADD).

	S $(0 \leq S \leq 31)$	n	$f(X) \bmod n$	p
(1)	0	2	$A \bmod 2$	1
(2)	odd numbers	3	$A - 1 \bmod 3$ $A \bmod 3$	1/2 1/2
(3)	2, 6, 10, 14 18, 22, 26, 30	5	$A - 1 \bmod 5$ $A \bmod 5$	1/2 1/2
(4)	4, 12, 20, 28	17	$A - 1 \bmod 17$ $A \bmod 17$	1/2 1/2
(5)	8, 24	257	$A - 1 \bmod 257$ $A \bmod 257$	1/2 1/2
(6)	16	65537	$A - 1 \bmod 65537$ $A \bmod 65537$	1/2 1/2

Srictly speaking, the values of the probability 'p' in Table 4 are approximations. But the effects of the approximations to the analyses in this paper are a little and can be ignored. For simplicity and understanding of the readers, we use these approximation through this paper. These strict values of 'p' are shown in Ref. 9).

Table 4 shows that modular output value $f(X) \bmod n$ depend on only A. The fact that the categorization of the left-rotation shift amount S in Table 4 is the same to that in Tables 1 and 2, is very interest.

4. Cryptanalysis of M8

In this chapter, we discuss the security of M8. Firstly, we point out the weakness of M8 in case of the left-rotation shift amount $S = 0$. Then, we discuss applicability of differential cryptanalysis, linear cryptanalysis and mod n cryptanalysis to M8, respectively.

4.1 Discussion in the Case of $S = 0$

We begin by studying the case that the basic component, of which the left-rotation shift amount S is equal to '0', is included in M8. Firstly, we derive the properties of round function such as [Case 1].

[Case 1]
If any one of the following conditions is true at the round function of M8, the output value of the round function becomes constant.
(1-1) $S1 = 0$ and $[unit\ 2] = 1$ (bitwise XOR)
(1-2) $S2 = 0$ and $[unit\ 4] = 1$ (bitwise XOR)
(1-3) $S3 = 0$ and $[unit\ 7] = 1$ (bitwise XOR)

We show some examples as follow:
(Ex.1) if $S3 = 0$ and $[unit\ 7] = 1$ are true, the output of the round function of M8 becomes γ, which is algorithm extension key.
(Ex.2) if $S2 = S3 = 0$, $\beta = \gamma = 0$, $[unit\ 4] = 1$ and $[unit\ 7] = 0$ are true, the output of the round function of M8 becomes $2 \times K_{R,i} \bmod 2^{32}$ ($K_{R,i}$ is expansion key).
These cases mean, once the output of exclusive-or becomes '0', the output of round function becomes constant. Secondly, we discuss the whole structure of M8.

[Case 2]
If the number of rounds N of M8 is even and [Case 1] is true, the ciphertext C_R (C_L) does not depend on plaintext P_L (P_R) but on P_R (P_L). Similarly, if the number of rounds N of M8 is odd and [Case 1] is true, the ciphertext C_R (C_L) does not depend on only plaintext P_R (P_L) but on P_L (P_R).
(Ex.1) if $S3 = 0$, $[unit\ 7] = 1$ and $\gamma = 0$ are true in every round functions of M8, the ciphertext C is equal to the plaintext P or the ciphertext C is equal to plaintext swapped by half 32 bits, for the cipher with any number of rounds N.
(Ex.2) if $S3 = 0$, $[unit\ 7] = 1$, $\gamma \neq 0$ and $[unit\ 9] = 1$ are true in every round functions of M8, the ciphertext C_R (or C_L) is equal to exclusive-or value between the plaintext P_R (or P_L) and constant, which is determined by γ in every round, for the cipher with any number of rounds N.
(Ex.3) if $S3 = 0$, $[unit\ 7] = 1$, $\gamma \neq 0$ and $[unit\ 9] = 0$ are true in every round functions of M8, the ciphertext C_R (or C_L) is equal to 2^{32} modular addition value between the plaintext P_R (or P_L) and constant, which is determined by γ in every round, for the cipher with any number of rounds N.

Generally speaking, an encryption algorithm becomes more secure, when the number of rounds increase. However, as we discussed above, M8 has no effect in security for the cipher with any number of rounds N in [Case 1] and [Case 2].

4.2 Applicability of Differential Cryptanalysis

In this section we discuss applicability of differential cryptanalysis to M8. Firstly, we derive the properties of round function such as [Case 3] and [Case 4].

[Case 3]
If [Case 1] is true at the round function of M8, the output differential value of the round function becomes '0' with probability $p = 1$ without dependence on the input differential value of the round function.

This is obvious, because the output of the basic component in [Case 1] becomes '0'.

[Case 4]
If $[unit\ 1] = [unit\ 2] = 1$ is true (bitwise XOR) at the round function of M8, the output differential value of the round function becomes '0' in case that input differential value ΔX is the value against the left-rotation shift amount $S1$ in Table 1.

This is obvious because of the results of the discussion in Section 3.1. Secondly, we derive the following property of the whole structure of M8. Cryptanalyst can propagate the difference between plaintext and ciphertext with probability $p = 1$ by controlling the differential value of plaintext in the following case.

[Case 5]
If the whole structure of M8 has the round functions, by turns, in which [Case 3] or [Case 4] is true or in which $[unit\ 9] = 1$ (bitwise XOR) is true, and the differential value of plaintext ΔP_R (or ΔP_L) is '0', then, the differential value of plaintext ΔP_L (or ΔP_R) is propagated to the differential value of ciphertext ΔC_L or ΔC_R (it depends on that the number of rounts N is either even or odd.) with probability $p = 1$.
(Ex.1) If the number of rounts N of M8 is even, $[unit\ 1] = [unit\ 2] = 1$ is true in odd rounds, $[unit\ 9] = 1$ is true in even rounds, the differential value of plaintext ΔP_L is categorized in regard to $S1$ in Table 1 in odd rounds and the differential value of plaintext $\Delta P_R = 0$ is true, then, the differential value of plaintext ΔP_L is propagated to the differential value of ciphertext ΔC_L with probability $p = 1$, such as $\Delta C_L = \Delta P_L$ and $\Delta C_R = \Delta P_R = 0$.

Generally speaking, an encryption algorithm becomes more secure, when the number of rounds increase. However, as we discussed above, M8 has no effect in the view point of security for the cipher with any number of rounts

N in [Case 5] against differential cryptanalysis.

4.3 Applicability of Linear Cryptanalysis

In this section we discuss applicability of linear cryptanalysis to M8. Firstly, we derive the properties of round function such as [Case 6] and [Case 7].

[Case 6]

If [Case 1] is true at the round function of M8, the masked value of the round function becomes '0' or '1' with probability $p = 1$ without dependence on the output mask of the round function.

This is obvious, because the output of the basic component in [Case 1] becomes '0' and final output of round function becomes constant.

[Case 7]

If $[\textit{unit } 7] = [\textit{unit } 8] = 1$ is true (bitwise XOR) at the round function of M8, the input mask of the round function becomes '0' in case that output mask $\Gamma f(X)$ is the value against the left-rotation shift amount $S3$ in Table 2.

This is obvious because of the results of the discussion in Section 3.2. Secondly, we derive the following property of the whole structure of M8 from the properties of round functions. Cryptanalyst can propagate the mask between plaintext and ciphertext with probability $p = 1$ by controlling the mask of plaintext in the following case.

[Case 8]

If the whole structure of M8 has the round function, every other round, in which [Case 6] or [Case 7] is true and in which $[\textit{unit } 9] = 1$ (bitwise XOR) is true, and the mask of plaintext ΓP_R (or ΓP_L) is '0', then, the mask of plaintext ΓP_L (or ΓP_R) is propagated to the mask of ciphertext ΓC_L or ΓC_R (it depends on the number of rounds N is either even or odd.) with probability $p = 1$.

(Ex.1) If the number of rounds N of M8 is even, $[\textit{unit}\, 7] = [\textit{unit}\, 8] = 1$ is true in odd rounds, $[\textit{unit}\, 9] = 1$ is true in odd rounds, the mask of plaintext ΓP_R is categorized in regard to $S3$ in Table 2 in odd rounds and the mask of plaintext $\Gamma P_L = 0$ are true, then, the mask of plaintext ΓP_R is propagated to the mask of ciphertext ΓC_R with probability $p = 1$, such as $\Gamma C_R = \Gamma P_R$ *and* $\Gamma C_L = \Gamma P_L = 0$.

Generally speaking, an encryption algorithm becomes more secure, when the number of rounds increase. However, as we discussed above, M8 has no effect in the view of security for the cipher with any number of rounds N in [Case 8] against linear cryptanalysis.

4.4 Applicability of Mod n Cryptanalysis

In this section we discuss applicability of mod n cryptanalysis to M8. Firstly, we derive the following properties of round function such as [Case 9].

[Case 9]

If any one of following conditions is true at the round function of M8, the 2^{32} modular output value of the round function has statistical strong bias as follow:

(9-1) $[\textit{unit } 7] = [\textit{unit } 8] = 0$

(9-2) $[\textit{unit } 4] = [\textit{unit } 5] = [\textit{unit } 6]$
$= [\textit{unit } 7] = [\textit{unit } 8] = 0$

(9-3) $[\textit{unit } 2] = [\textit{unit } 3] = [\textit{unit } 4] = [\textit{unit } 5]$
$= [\textit{unit}\, 6] = [\textit{unit}\, 7] = [\textit{unit}\, 8] = 0$

Case (9-1): There exists strong bias of 'mod n' output value of round function with strong dependence on γ. From the discussion in the Section 3.3, the bias of mod n output value of round function is the same in Table 4 (as A $= \gamma$).

(Ex.1) Table 4 shows the distribution of mod n output value categorized by $S3$ and n in case of (9-1) (as A $= \gamma$).

Case (9-2): There exists strong bias of 'mod n' output value of round function with strong dependence on $S2$, β, K_R, $S3$ *and* γ. For example, if $S2$ and $S3$ are categorized in the same S in Table 4, we can derive the distribution of mod n output value (using the results of Table 4), which is dependent on β, K_R, γ.

Case (9-3): There exists strong bias of 'mod n' output value of round function with strong dependence on $S1$, α, $S2$, β, K_R, $S3$ *and* γ. For example, if $S1$, $S2$ and $S3$ are categorized in the same S in Table 4, we can derive the distribution of mod n output value (using the result of Table 4), which is dependent on α, β, K_R, γ.

This is obvious because of the results of the discussion in the Section 3.3. Secondly, we derive the following property of the whole structure of M8 from the properties of round functions. Cryptanalyst can propagate the large bias of the distribution between plaintext and ciphertext by controlling modulus 'n' in the following case.

[Case 10]

If the whole structure of M8 has the round functions, every other round, in which [Case 9] is true and in which $[\textit{unit } 9] = 0$ (mod 2^{32} ADD) is true, then, the 'mod n' value of difference between ciphertext C_L (or C_R) and plaintext

P_L (or P_R) has distribution, which has large bias from random distribution. In this case, the least common multiple value among S3s, which the round functions in [Case 9] have, should be selected as modulus 'n'.

The distribution depends on the round function structure, which hold [Case 9]. For typical example, we show the details in the case (9-1) such that $S3$s are categorized to the same S.

(Ex.1) Case (9-1): We derive and summarize the distribution of $C_{R,i}$ - $C_{L,i-1}$ (mod n) (n is in regard to $S3$ in Table 4) in **Table 5**.

(Ex.2) Case (9-1): We summarize the bias of distribution of $P_L - C_L$ (mod n) (or $P_L - C_R$ (mod n)) in **Fig. 3**, in case that the number of rounds N is even (or odd) and that $S3$s are categorized to the same n in Table 5 (Note: we call M8 of this case 'mod n class' in Fig. 3).

Table 5 The distribution of $C_{R,i-1} - C_{L,i}$ (mod n) ([*unit* 7], [*unit* 8], [*unit* 9]: mod 2^{32} ADD).

	$S3$ ($0 \le S3 \le 31$)	n	$C_{R,i-1} - C_{L,i}$ mod n	p
(1)	0	2	$\gamma - 1$ mod 2 γ mod 2	1/2 1/2
(2)	odd numbers	3	$\gamma - 2$ mod 3 $\gamma - 1$ mod 3 γ mod 3	1/4 1/2 1/4
(3)	2, 6, 10, 14 18, 22, 26, 30	5	$\gamma - 2$ mod 5 $\gamma - 1$ mod 5 γ mod 5	1/4 1/2 1/4
(4)	4, 12, 20, 28	17	$\gamma - 2$ mod 17 $\gamma - 1$ mod 17 γ mod 17	1/4 1/2 1/4
(5)	8, 24	257	$\gamma - 2$ mod 257 $\gamma - 1$ mod 257 γ mod 257	1/4 1/2 1/4
(6)	16	65537	$\gamma - 2$ mod 65537 $\gamma - 1$ mod 65537 γ mod 65537	1/4 1/2 1/4

In mod n cryptanalysis, $\chi^2 test$ is used to distinguish a target distribution with the distribution of random function [5]. In this paper, we use the l_2 norm [5] as the measure of bias in Fig. 3. Then the samples of a pair of plaintext and ciphertext necessary to distinguish those blocks from a random sequence of blocks, are proportional to an inverse number of the bias [5].

We discuss the distinction between M8 and random function. We can estimate the number of a pair of known-paintexts necessary to distinguish from random function is equal to $C/bias$ (C is constant.) when the bias is expected as $C(k+1) - 1$ with $k - 1$ degree of freedom [5]. Therefore, in case of 'mod 3 class' (degree of freedom is 2) the constant C is estimated at $C \cong 2.4$, and in case of 'mod 5 class' (degree of freedom is 4) the constant C is estimated at $C \cong 1.8$, so that can distinguish from random function with probability p more than 0.99 [6]. Note that the upper limit on the number of known-plaintext is 2^{64}, since the block size of M8 is 64 bits. From the discussion above and the result in Fig. 3, M8 must have more than 33 rounds in case of 'mod 3 class', more than 108 rounds in case of 'mod 5 class', so that the probability p with which we succeed in distinguishing from the random function becomes less

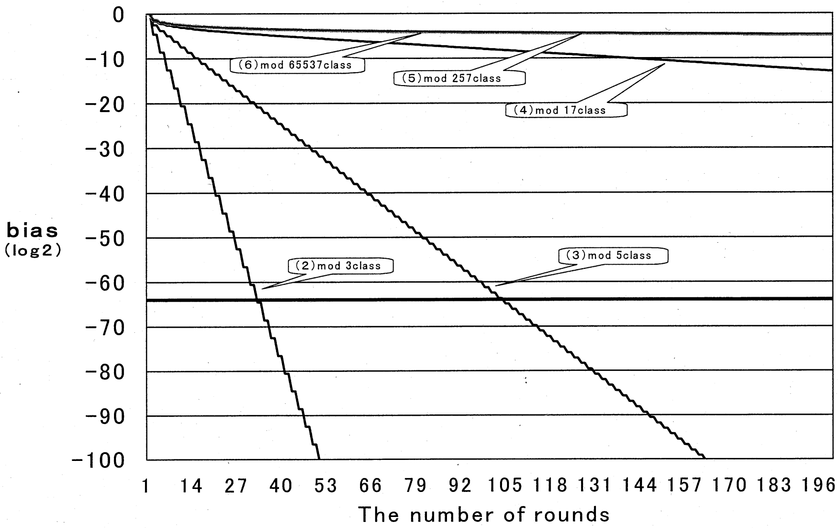

Fig. 3 The bias of 'mod n class' (in case (9-1)).

than 0.01.

5. Conclusions

In this paper, we discuss the security of M8 against differential cryptanalysis, linear cryptanalysis and mod n cryptanalysis, respectively. As a result, we show that there exist differential and linear characteristics that hold with probability $p = 1$ and modulus n characteristics of which the bias of distribution is remarkably high. These mean there exists strong possibility that M8 has remarkable statistic properties and is breakable by differential cryptanalysis, linear cryptanalysis and mod n cryptanalysis, respectively. These facts show that the strength of M8 is strongly dependent on the values of system keys, and must be evaluated for each system key. We think that it is more desirable for the proponent of M8 to show recommended system keys.

References

1) Biham, E. and Shamir, A.: *Differential Cryptanalysis of the Data Encryption Standard*, Springer-Verlag (1993).
2) Matsui, M.: Linear Cryptanalysis Method for DES cipher. *Advances in Cryptology—Eurocrypt '93*, Lecture Notes in Computer Science, Vol.765, Springer-Verlag (1993).
3) M8: ALGORITHM REGISTER ENTRY iso standard 9979 m8 (20), (inquiry) IPA, crypt@ipa.go.jp
4) Aoki, K. and Kurokawa, K.: A Study on Linear Cryptanalysis of Multi 2, SCIS95-A4.1 (1995).
5) Kelsey, J., Schneier, B. and Wagner, D.: Mod n Cryptanalysis, with Applications Against RCP5P and M6, *Fast Software Encryption, 6th International Workshop, FSE '99*, Lecture Notes in Computer Science, Vol.1636, Springer-Verlag (1999).
6) Hoel, P.: *Introduction to Mathematical Statistics*, 4th edition, Bai-fu-kan (1978).
7) Tokita, T.: Cryptanalysis of M8—A registered encryption algorithm in ISO9979 (No.20), *IEICE*, *ISEC99-24* (Sep. 1999).
8) Kaneko, T.: On the Weak Keys in M8 Encryption System, *IEICE*, *ISEC99-25* (1999).
9) Tokita, T.: Cryptanalysis of M8(2)—A registered encryption algorithm in ISO9979 (No.20), *IEICE*, *ISEC99-41* (Sep. 1999).
10) Sano, F. and Matsumoto, T.: On the Weakness in M8 Encryption Algorithm, *ISEC99-42* (1999).
11) Sano, F. and Matsumoto, T.: On the System Parameters in M8 Algorithm, *SCIS2000*, A-07 (2000).
12) Tokita, T.: Cryptanalysis of M8(3)—A registered encryption algorithm in ISO9979 (No.20), *SCIS2000*, A-08 (2000).
13) Saito, T. and Kaneko, T.: On the Output Property of F-function of M8, *SCIS2000*, A-48 (2000).

(Received December 1, 2000)
(Accepted June 19, 2001)

Toshio Tokita was born in 1964, received M.E. degree from Yokohama National University in 1989, and since then, he has joined Mitsubishi Electric Corporation. He is also a student in Ph.D. couse of Yokohama National University. He is a member of IACR, IEICE and IPSJ.

Tsutomu Matsumoto was born in Maebashi, Japan, on October 20, 1958. He received the Dr. Eng. degree from the University of Tokyo in 1986, and since then, his base has been in Yokohama National University where he is enjoying research and teaching in the field of cryptography and information security as a Professor in Graduate School of Environment and Information Sciences. He is a member of Cryptography Research and Evaluation Committee of Japan. He served as the general chair of ASIACRYPT 2000. He is an associated editor of Journal of Computer Security and was on the board of International Association for Cryptologic Research and the Japan Society of Security Management. He received Achievement Award from the IEICE in 1996.