SCIS 2011 The 2011 Symposium on Cryptography and Information Security
Kokura, Japan, Jan. 25-28, 2011
The Institute of Electronics, Information and Communication Engineers

CLEFIA の差分攻撃及び線形攻撃に対する安全性評価の更新
Update of the Security Evaluation of CLEFIA Against Differential Attack and Linear Attack

三津田 敦司* 白井 太三 *
Atsushi Mitsuda Taizo Shirai

あらまし 差分攻撃法及び線形攻撃法は共通鍵ブロック暗号に対する代表的なものであり，これらの攻撃に対する十分な安全性があることを示す必要がある．128 ビットブロック暗号 CLEFIA では，複数の拡散行列を用いて差分攻撃法および線形攻撃法への耐性を高める設計技法「拡散行列切り替え法」を採用している．CLEFIA の設計者らは CLEFIA に対し，12 ラウンド以上で差分攻撃及び線形攻撃に有効に利用できるパスが存在しないことを示した．本論文では，より詳細な差分特性評価及び線形特性評価を行うことで，11 ラウンド以上で差分攻撃及び線形攻撃に有効に利用できるパスが存在しないことを示す．

キーワード 共通鍵ブロック暗号，CLEFIA, 差分特性確率，線形特性確率，安全性評価

1 はじめに

近年，共通鍵ブロック暗号は様々な分野の機器やアプリケーションに搭載されるようになり，高い安全性と高い性能を兼ね備えた暗号技術を低コストで実装するニーズはますます高まってきている．ブロック暗号に対しては多くの暗号攻撃法が知られており，特に，差分攻撃法 [2] や線形攻撃法 [6] などの汎用的な攻撃法について，その安全性を示すことがその暗号に対する信頼性を得る上で必須と考えられる．

128 ビットブロック暗号 CLEFIA[10] では，複数の拡散行列を用いて差分攻撃法および線形攻撃法への耐性を高める設計技法「拡散行列切り替え法」[7, 8, 9] を採用し，これらの攻撃法に対する安全性を示している．さらに，これ以外の既知の攻撃法についても網羅的に取り上げ，それぞれについて配慮した設計を行っている．近年，関連鍵攻撃の進展が目覚ましく，AES などのシンプルな鍵スケジュールをもつブロック暗号への適用が進んでいるが，CLEFIA では，鍵スケジュール部に対しても安全性を評価できる設計であり，関連鍵攻撃の適用を困難としている．

本論文では，CLEFIA の差分攻撃及び線形攻撃に対する安全性評価を更新したので報告する．設計者らは active S-box をカウントする手法により，CLEFIA は 12 ラウンド以上で差分攻撃及び線形攻撃に有効に利用できるパスが存在しないことを示した [10]．本論文では，設計者らの評価手法を基にした，差分特性確率及び線形特性確率の評価手法を示し，その評価手法を用いることで，CLEFIA は 11 ラウンド以上で差分攻撃及び線形攻撃に有効に利用できるパスが存在しないことを示す．

* ソニー株式会社, 〒 141-0001, 東京都品川区北品川 5-1-12 御殿山 Tec, Sony Corporation, Gotenyama Tec. 5-1-12 Kitashinagawa Shinagawa-ku, Tokyo, 141-0001.

2 諸定義

$\{0,1\}^n$: n ビット列の集合
$\oplus, \wedge, \vee$: それぞれ XOR, AND, OR の演算子
$X|Y$: ビット列または行列の連結
$0011_2, 1011_2$: 2 進数表記

3 CLEFIA

CLEFIA は 2007 年に提案された 128 ビットブロック暗号である．鍵長は 128, 192, 256 ビットから選択可能である．安全性，速度，実装コストの 3 つの基準をバランスよく実現することを考慮して設計されている．CLEFIA は鍵スケジュール部とデータ処理部に分けられており，本論文ではデータ処理部とその安全性について述べる．

3.1 データ処理部の基本構造

CLEFIA のデータ処理部では Feistel 構造を拡張した 4 系列 Type-2 一般化 Feistel 構造を採用している [11]．ブロック長が 128 ビットであることから，各系列長は 32 ビットとなる．4 系列の Type-2 構造は 1 ラウンドに 2 つ

表 1: S-box の最大差分確率及び最大線形確率

	最大差分確率	最大線形確率
S_0	$2^{-4.678}$	$2^{-4.385}$
S_1	2^{-6}	2^{-6}

の F 関数を持ち，一方の F 関数は 1 列目のデータ系列，もう一方の F 関数は 3 列目のデータ系列に適用される．

3.2 F 関数

CLEFIA の F 関数は SP 型を採用しており，ラウンド鍵の加算後，Substitution 層と Permutation 層の順に演算される．このタイプの F 関数は，Camelia[1] などの多くのブロック暗号設計に利用されている．CLEFIA は Substitution 層に 4 つの 8 ビット S-box, Permutation 層に 4×4 の拡散行列を用いている．

3.3 S-box

CLEFIA は 2 種類の 8 ビット S-box, S_0, S_1 を採用している．S_0 はランダムに選択した 4 ビット S-box に基づくものであり，S_1 は $\mathrm{GF}(2^8)$ 上の逆元関数に基づくものである．S_0, S_1 それぞれの最大差分確率と最大線形確率を表 1 に示す．

3.4 拡散行列切り替え法

差分攻撃や線形攻撃への耐性を高めるために，異なる 2 つの拡散行列 M_0, M_1 を採用している．演算は $\mathrm{GF}(2^8)$ 上で行い，既約多項式は $x^8+x^4+x^3+x^2+1$ を用いる．

$$M_0 = \begin{pmatrix} 1 & 2 & 4 & 6 \\ 2 & 1 & 6 & 4 \\ 4 & 6 & 1 & 2 \\ 6 & 4 & 2 & 1 \end{pmatrix}, M_1 = \begin{pmatrix} 1 & 8 & 2 & a \\ 8 & 1 & a & 2 \\ 2 & a & 1 & 8 \\ a & 2 & 8 & 1 \end{pmatrix} \quad (1)$$

ここで，ハミング重みを以下のように定義する．

定義 1 任意の $X = (x_0|x_1|\ldots|x_{m-1}) \in (\{0,1\}^8)^m$ に対し，$\mathrm{HW}(X) = \#\{i|0 \le i \le m-1, x_i \neq 0\}$ を X のハミング重みとし，$\mathrm{HW}(X)$ を X の **HW 値**とする．

分岐数が 5 である拡散行列 M と HW 値について以下の補題が成り立つ．

補題 1 任意の $X \in \{0,1\}^{32}$ に対し，$Y = MX$ としたとき，以下の関係式を満たす．但し，$(X,Y) \neq (0,0)$ とする．

$$\mathrm{HW}(X) + \mathrm{HW}(Y) \ge 5$$

CLEFIA の 2 つの拡散行列 M_0, M_1 及び ${}^tM_0, {}^tM_1$ は分岐数が 5 であり，補題 1 を満たす．但し，${}^tM_0, {}^tM_1$ は

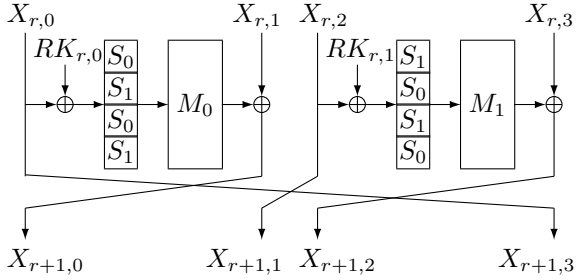

図 1: CLEFIA のラウンド関数

M_0, M_1 をビット単位の 32×32 行列としたときの転置行列とする．また，M_0, M_1 を結合した 4×8 行列 $M_0|M_1$ 及び ${}^tM_0^{-1}|{}^tM_1^{-1}$ の分岐数も 5 となるため，以下の補題が成り立つ．

補題 2 任意の $X, Y \in \{0,1\}^{32}$ に対し，$Z = M_0X \oplus M_1Y$, $Z' = {}^tM_0^{-1}X \oplus {}^tM_1^{-1}Y$ としたとき，以下の関係式を満たす．但し，$(X,Y,Z) \neq (0,0,0)$ とする．

$$\begin{cases} \mathrm{HW}(X) + \mathrm{HW}(Y) + \mathrm{HW}(Z) \ge 5 \\ \mathrm{HW}(X) + \mathrm{HW}(Y) + \mathrm{HW}(Z') \ge 5 \end{cases}$$

CLEFIA では，図 1 に示すように M_0, M_1 を F 関数内に配置している．この手法は拡散行列切り替え法 (DSM) と呼ばれる．DSM を用いた場合，近傍ラウンド中の差分消失や線形マスク消失を防ぐことができるため，active S-box の保証数が増加することが期待できる．

4 従来評価手法

4.1 差分攻撃への耐性評価

差分攻撃は Biham と Shamir によって提案された，ブロック暗号に対する汎用的な攻撃である [2, 3]．差分攻撃に対するブロック暗号の耐性を評価する方法には，以下の 2 通りがある．

1. ランダム置換との識別に利用可能な差分が存在しないことを示す
2. ランダム置換との識別に利用可能な差分特性が存在しないことを示す

多くの暗号において 1 つ目の手法により評価することは困難であることが知られている．設計者らはもう 1 つのアプローチ，即ち差分特性確率を評価する手法を採用した．これは active S-box の数を計算することで評価できることが知られており，この評価手法は AES や Camellia などでも用いられている [1, 5].

最大差分確率と最大差分特性確率の間にどれほどのギャップがあるかはこれまで明らかになっていないが，Daemen と Rijmen によって両者の関係が詳細に議論さ

れており，これによると，ある統計的な仮定のもとで，両者には統計的な関連が存在している [4]．よって，差分特性ベースのアプローチは差分攻撃に対する耐性を評価する合理的な手法の 1 つであると考えられる．

Active S-box 数評価　S-box への入力差分が非 0 であるとき，その S-box は active であるという．差分特性確率は系全体の active S-box の最大差分確率の積で抑えられる．遷移する可能性のある全ての差分パスを考慮し，active S-box 数の下界を評価することで，差分特性確率の上界を評価することができる．一般に，ブロック暗号に含まれる active S-box の数を保証する方法には 2 種類ある．1 つは証明などで示された active S-box 数の下界を用いる方法，もう 1 つは探索アルゴリズムにより，active S-box 数の下界を評価する方法である．設計者らは両方において確認を行うことで，探索ベースで求められる下界を厳密な評価として用いている．

また，CLEFIA には 2 種類の S-box S_0, S_1 があり，それぞれの最大差分確率が異なる (表 1)．設計者の観点から CLEFIA の差分攻撃に対する安全性を評価するには，全ての S-box が (差分攻撃に対して弱い=高い最大差分確率を有する) S_0 であると仮定して評価している．

Weight Base 評価　各経路毎，32 ビット全ての差分値に対して評価することは一般に困難である．そこで，設計者らは各経路の差分値のデータ表現にハミング重みを用いた．ハミング重みを用いた評価を **Weight Base 評価**とする．但し，情報量が減少しているため，XOR や F 関数における遷移の条件を考慮する必要がある．HW 値の定義より，XOR に関して以下の補題が成り立つ．

補題 3 任意の $A, B \in \{0,1\}^{32}$ に対し，$C = A \oplus B$ としたとき，以下の関係式を満たす．

$$\begin{cases} \mathrm{HW}(A) + \mathrm{HW}(B) \geq \mathrm{HW}(C) \\ \mathrm{HW}(B) + \mathrm{HW}(C) \geq \mathrm{HW}(A) \\ \mathrm{HW}(C) + \mathrm{HW}(A) \geq \mathrm{HW}(B) \end{cases}$$

補題 4 任意の $A, B \in \{0,1\}^{32}$ に対し，$\mathrm{HW}(A) \neq \mathrm{HW}(B)$ のとき，$\mathrm{HW}(A \oplus B) \neq 0$ を満たす．

以降では，任意の差分値 $\Delta X \in \{0,1\}^{32}$ に対する差分 HW 値を $\delta X = \mathrm{HW}(\Delta X)$ とする．ラウンド関数における差分遷移に関して以下の定理が成り立つ．

定理 1 ラウンド関数の一部における各経路の差分 HW 値 $\delta A, \delta B, \delta C$ を図 2 (左) のように置いたとき，以下の関係式を満たす．

$$\begin{cases} \delta B = \delta C & (\delta A = 0) \\ \delta A + \delta B + \delta C \geq 5 & (\delta A \neq 0) \end{cases}$$

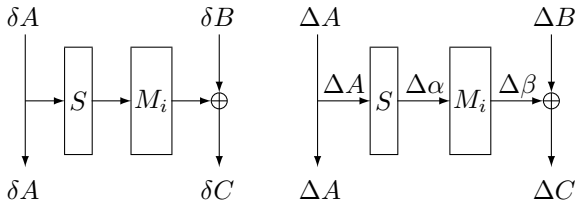

図 2: ラウンド関数の一部の差分 HW 値 (左) と差分値 (右) (但し，ラウンド鍵加算は省略，$i = 0, 1$)

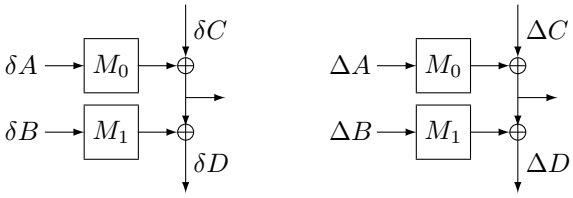

図 3: 3 ラウンド間の一部の差分 HW 値 (左) と差分値 (右) (但し，系列をひねらない表記)

証明　$\Delta A, \Delta B, \Delta C, \Delta\alpha, \Delta\beta$ を図 2 (右) のように置く．但し，$\Delta\beta = \Delta B \oplus \Delta C = M_i \Delta\alpha$ である．また，S 層の前後で HW 値は変わらないため，$\delta A = \delta\alpha$ である．

$\Delta A = \Delta\alpha = 0$ のとき，$\Delta\beta = 0$ であり，$\Delta B = \Delta C$，即ち，$\delta B = \delta C$ となる．次に，$\Delta A \neq 0$ のとき，補題 1 より，$\delta\alpha + \delta\beta \geq 5$ である．また，補題 3 より，$\delta B + \delta C \geq \delta\beta$ である．よって，$\delta A + \delta B + \delta C \geq 5$ が成り立つ．　□

また，DSM の効果により，3 ラウンド間の差分遷移に関して以下の定理が成り立つ．

定理 2 3 ラウンド間の一部における各経路の差分 HW 値 $\delta A, \delta B, \delta C, \delta D$ を図 3 (左) のように置いたとき，以下の関係式を満たす．但し，$\delta A \neq 0$ または $\delta B \neq 0$ または $\delta C \neq \delta D$ とする．

$$\delta A + \delta B + \delta C + \delta D \geq 5$$

証明　$\Delta A, \Delta B, \Delta C, \Delta D$ を図 3 (右) のように置く．このとき，$\Delta C \oplus \Delta D = M_0 \Delta A \oplus M_1 \Delta B$ となるため，補題 2, 3, 4 から，$\delta A \neq 0$ または $\delta B \neq 0$ または $\delta C \neq \delta D$ のとき，与式が成り立つ．これは M_0, M_1 が逆であっても成り立つ．　□

4.2　線形攻撃への耐性評価

線形攻撃は松井によって提案された，ブロック暗号に対する汎用的な攻撃である [6]．線形攻撃に対する耐性を評価するには，差分攻撃に対する耐性評価と同様の手法，即ち，active S-box 数と S-box の最大線形確率を用いて評価することができる．

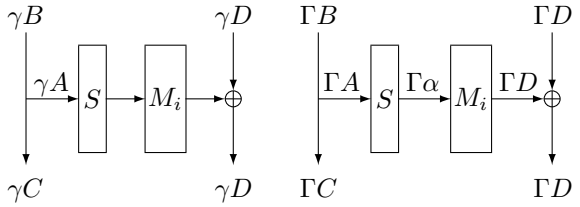

図 4: ラウンド関数の一部の線形 HW 値 (左) と線形マスク値 (右) (但し，ラウンド鍵加算は省略，$i = 0, 1$)

設計者らは，差分攻撃に対する耐性評価と同様に，各系列毎の線形マスク値を HW 値に置き換えることで Weight Base 評価を行った．

以降では，任意の線形マスク値 $\Gamma X \in \{0,1\}^{32}$ に対する線形 HW 値を $\gamma X = \mathrm{HW}(\Gamma X)$ とする．ラウンド関数における線形マスク遷移に関して以下の定理が成り立つ．

定理 3 ラウンド関数の一部における各経路の線形 HW 値 $\gamma A, \gamma B, \gamma C, \gamma D$ を図 4 (左) のように置いたとき，以下の関係式を満たす．

$$\begin{cases} \gamma A = 0 & (\gamma D = 0) \\ \gamma A + \gamma D \geq 5 & (\gamma D \neq 0) \\ \gamma A + \gamma B \geq \gamma C \\ \gamma B + \gamma C \geq \gamma A \\ \gamma C + \gamma A \geq \gamma B \end{cases}$$

証明 $\Gamma A, \Gamma B, \Gamma C, \Gamma D, \Gamma\alpha$ を図 4 (右) のように置く．但し，$\Gamma\alpha = {}^tM_i \Gamma D$ である．また，S 層の前後で HW 値は変わらないため，$\gamma A = \gamma\alpha$ である．よって，補題 1,3 より成り立つ． □

また，DSM の効果により，3 ラウンド間の線形マスク遷移に関して以下の定理が成り立つ．

定理 4 3 ラウンド間の一部における各経路の線形 HW 値 $\gamma A, \gamma B, \gamma C$ を図 5 (左) のように置いたとき，以下の関係式を満たす．但し，$(\gamma A, \gamma B, \gamma C) \neq (0, 0, 0)$ とする．

$$\gamma A + \gamma B + \gamma C \geq 5$$

証明 $\Gamma A, \Gamma B, \Gamma C$ を図 5 (右) のように置く．このとき，$\Gamma C = {}^tM_0^{-1}\Gamma A \oplus {}^tM_1^{-1}\Gamma B$ となるため，補題 2 より成り立つ．これは M_0, M_1 が逆であっても成り立つ． □

4.3 従来評価結果

設計者らは，データ表現にハミング重みを利用した Weight Base 評価を行った．定理 1,2,3,4 を用いて，遷移しうる全ての差分パス及び線形パスを考慮し，R ラウンドの CLEFIA に含まれる差分 active S-box 数及び線形 active S-box 数の下界を導出している．これを表 2 に示す．DSM(D) 及び DSM(L) はラウンド数 R における，差分 active S-box 及び差分 active S-box の最小数を示している．また，DSM の条件 (定理 2,4) を用いない場合，差分 active S-box 数の最小数と線形 active S-box 数の最小数は同じ値となり，Normal として表記している．

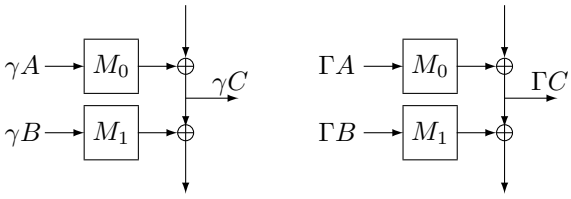

図 5: 3 ラウンド間の一部の線形 HW 値 (左) と線形マスク値 (右) (但し，系列をひねらない表記)

表 2: active S-box の保証数

R	Normal	DSM(D)	DSM(L)
1	0	0	0
2	1	1	1
3	2	2	5
4	6	6	6
5	8	8	10
6	12	12	15
7	12	14	16
8	13	18	18
9	14	20	20
10	18	22	23
11	20	24	26
12	24	28	30

この表より，12 ラウンド CLEFIA において 28 個の差分 active S-box が保証されている．S_0 の最大差分確率が $2^{-4.678}$ であることより，12 ラウンド CLEFIA の最大差分特性確率は $2^{-4.678\times 28} = 2^{-130.984}$ 以下となる．これは，攻撃者が差分攻撃に利用可能な 12 ラウンド差分特性が存在しないことを意味する．

また，12 ラウンド CLEFIA において 30 個の線形 active S-box が保証されている．S_0 の最大線形確率が $2^{-4.385}$ であることより，12 ラウンド CLEFIA の最大線形特性確率は $2^{-4.385\times 30} = 2^{-131.55}$ 以下となる．これは，攻撃者が線形攻撃に利用可能な 12 ラウンド線形特性が存在しないことを意味する．

以上より，12 ラウンド以上で差分攻撃及び線形攻撃に有効に利用できるパスが存在しないことを示した．

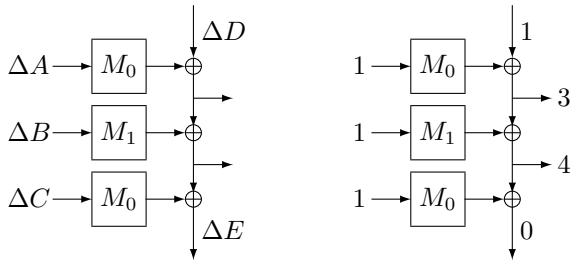

図 6: 5 ラウンド間の一部の差分値 (左) と遷移しない差分 HW 値の例 (右) (但し，系列をひねらない表記)

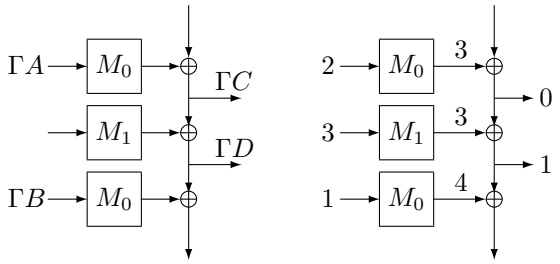

図 7: 5 ラウンド間の一部の線形マスク値 (左) と遷移しない線形 HW 値の例 (右) (但し，系列をひねらない表記)

5 改善評価手法

本節では設計者ら従来の評価手法を基にした，差分特性評価及び線形特性評価の改善評価手法を述べる．

5.1 5 ラウンド間の DSM

設計者らは DSM による条件として，補題 2 を用いて，3 ラウンド間 2 種類の MDS 行列を考慮した遷移の条件を導出した (定理 2, 4)．本節ではさらに，5 ラウンド間の 2 種類 3 つの MDS 行列を考慮した，新たな定理を示す．

定理 5 5 ラウンド間の一部における各経路の差分値 $\Delta A, \Delta B, \Delta C, \Delta D, \Delta E$ を図 6 (左) のように置いたとき，その HW 値 $\delta A, \delta B, \delta C, \delta D, \delta E$ は以下の関係式を満たす．但し，$\delta A \neq \delta C$ または $\delta B \neq 0$ または $\delta D \neq \delta E$ とする．

$$\delta A + \delta B + \delta C + \delta D + \delta E \geq 5$$

証明 $M_0(\Delta A \oplus \Delta C) \oplus M_1 \Delta B = \Delta D \oplus \Delta E$ であるため，補題 2, 4 より成り立つ．これは M_0, M_1 が逆であっても成り立つ． □

これは，定理 1, 2 からは導けない条件であり，図 6 (右) のような差分 HW 値の遷移が存在しないことを表す．

定理 6 5 ラウンド間の一部における各経路の線形マスク値 $\Gamma A, \Gamma B, \Gamma C, \Gamma D$ を図 7 (左) のように置いたとき，その HW 値 $\gamma A, \gamma B, \gamma C, \gamma D$ は以下の関係式を満たす．但し，$\gamma A \neq \gamma B$ または $\gamma C \neq \gamma D$ とする．

$$\gamma A + \gamma B + \gamma C + \gamma D \geq 5$$

証明 $\Gamma A \oplus \Gamma B = {}^t M_0(\Gamma C \oplus \Gamma D)$ であるため，補題 1, 4 より成り立つ．これは M_0, M_1 が逆であっても成り立つ． □

これは，定理 3, 4 からは導けない条件であり，図 7 (右) のような線形 HW 値の遷移が存在しないことを表す．

5.2 2 種類の S-box S_0, S_1

CLEFIA では 2 種類の S-box を利用しており，それぞれ，最大差分確率及び最大線形確率が異なる (表 1)．従来評価では上界を導出するために，2^{-128} 以下となるのに active S-box 数がそれぞれ 28 個，30 個必要であるとしていた．しかし，全ての active な S-box が S_0 でない場合，実際の特性確率はこの値よりも小さくなる．

そこで，S_0, S_1 の active 数をそれぞれ $\#\mathrm{AS}_0, \#\mathrm{AS}_1$ として，それぞれのカウントを行う．また，$\#\mathrm{AS} = \#\mathrm{AS}_0 + \#\mathrm{AS}_1$ とする．例えば，ある差分パスにおいて，$\#\mathrm{AS}_0 = 20, \#\mathrm{AS}_1 = 6$(即ち，$\#\mathrm{AS} = 26$) のとき，従来評価では差分特性確率の上界を $2^{-4.678\times 26} = 2^{-121.628}$ としていたが，本評価では $2^{-4.678\times 20 - 6\times 6} = 2^{-129.56}$ となる．このようにして，従来よりも厳密な特性確率の上界を導出することが可能である．

また，この評価方法においては最大差分特性確率及び最大線形特性確率を得るパスが，最小 active S-box 数とならない場合がある．例えば，ある差分パスにおいて，$\#\mathrm{AS}_0 = 25, \#\mathrm{AS}_1 = 2, \#\mathrm{AS} = 27$ のとき，$2^{-128.95}$ と評価され，$\#\mathrm{AS}_0 = 20, \#\mathrm{AS}_1 = 6, \#\mathrm{AS} = 26$ のときの $2^{-129.56}$ に比べ，active S-box 数が多くとも差分特性確率が大きくなる．

但し，Weight Base 評価においては S_0, S_1 を区別してカウントすることはできないため，S_0 を優先的に数えるといった方法が考えられる．例えば，F 関数への入力差分 ΔX に対し，$\delta X = 3$ のとき，$\#\mathrm{AS}_0 = 2, \#\mathrm{AS}_1 = 1$ とする．また，5.3 節の Byte Truncate 評価を用いることで，S_0, S_1 を区別してカウントできる．

5.3 Byte Truncate 評価

従来の Weight Base 評価では各系列毎のハミング重みを考慮していた．任意の差分値 ΔX, 線形マスク値 ΓX に対して，HW 値 $\delta X, \gamma X (0 \leq \delta X, \gamma X \leq 4)$ に置き換え，遷移しうる全ての HW 値について active S-box 数を計算していた．

本論文では 1 バイト毎に 0, 非 0 を考慮した評価を行

う．ここで，Byte Truncate を以下のように定義する．

定義 2 任意の $X = (x_0|x_1|\dots|x_{m-1}) \in (\{0,1\}^8)^m$ に対し，

$$\mathrm{BT}(X) = \mathrm{BT}(x_0|x_1|\dots|x_{m-1}) = \hat{x}_0|\hat{x}_1|\dots|\hat{x}_{m-1}$$

を X の Byte Truncate とし，$\mathrm{BT}(X)$ を X の **BT 値**と呼ぶ．但し，$\hat{x}_i$ は $x_i = 0$ のとき 0, $x_i \neq 0$ のとき 1 とする．即ち，$\mathrm{BT}(X) \in \{0,1\}^m$ である．

また，BT 値から HW 値への変換 $\mathrm{HW}'(\cdot)$ を以下のように定義する．

定義 3 任意の $X = (x_0|x_1|\dots|x_{m-1}) \in (\{0,1\}^8)^m$ に対し，

$$\begin{aligned}\mathrm{HW}'(\mathrm{BT}(X)) &= \mathrm{HW}'(\hat{x}_0|\hat{x}_1|\dots|\hat{x}_{m-1}) \\ &= \hat{x}_0 + \hat{x}_1 + \cdots + \hat{x}_{m-1} = \mathrm{HW}(X)\end{aligned}$$

この BT 値を用いた耐性評価を **Byte Truncate 評価**とする．任意の差分値及び線形マスク値 $\Delta X, \Gamma X \in \{0,1\}^{32}$ に対して，$\lambda X = \mathrm{BT}(\Delta X)$, $\mu X = \mathrm{BT}(\Gamma X)$ とし，$\lambda X, \mu X \in \{0,1\}^4$ に置き換えることで遷移の判定を行う．Byte Truncate 評価は Weight Base 評価に比べ，情報量の低下が少ないといえる．Weight Base 評価と同様に BT 値に対する遷移の条件を示す．BT 値，HW 値の定義より，XOR に関して以下の補題が成り立つ．

補題 5 任意の差分値 $\Delta A, \Delta B \in \{0,1\}^{32}$ 及び，線形マスク値 $\Gamma A, \Gamma B \in \{0,1\}^{32}$ は以下の関係式を満たす．

$$\begin{cases}\mathrm{HW}(\Delta A \oplus \Delta B) \leq \mathrm{HW}'(\lambda A \vee \lambda B) \leq \delta A + \delta B \\ \mathrm{HW}(\Gamma A \oplus \Gamma B) \leq \mathrm{HW}'(\mu A \vee \mu B) \leq \gamma A + \gamma B\end{cases}$$

また，$\Delta C = \Delta A \oplus \Delta B$, $\Gamma C = \Gamma A \oplus \Gamma B$ としたとき，以下の関係式を満たす．

$$\begin{cases}\lambda A \oplus \lambda B \oplus \lambda C \oplus (\lambda A \wedge \lambda B \wedge \lambda C) = 0000_2 \\ \mu A \oplus \mu B \oplus \mu C \oplus (\mu A \wedge \mu B \wedge \mu C) = 0000_2\end{cases}$$

補題 5 を利用することで，以下の定理 7,8,9,10 が成り立つ．

定理 7 ラウンド関数の一部における各経路の差分値 ΔA, $\Delta B, \Delta C$ を図 2 (右) のように置いたとき，その BT 値 $\lambda A, \lambda B, \lambda C$ は以下の関係式を満たす．

$$\begin{cases}\lambda B = \lambda C & (\lambda A = 0) \\ \mathrm{HW}'(\lambda A) + \mathrm{HW}'(\lambda B \vee \lambda C) \geq 5 & (\lambda A \neq 0)\end{cases}$$

定理 8 3 ラウンド間の一部における各経路の差分値を $\Delta A, \Delta B, \Delta C, \Delta D$ を図 3 (右) のように置いたとき，その BT 値 $\lambda A, \lambda B, \lambda C, \lambda D$ は以下の関係式を満たす．但し，$\lambda A \neq 0$ または $\lambda B \neq 0$ または $\lambda C \neq \lambda D$ とする．

$$\mathrm{HW}'(\lambda A) + \mathrm{HW}'(\lambda B) + \mathrm{HW}'(\lambda C \vee \lambda D) \geq 5$$

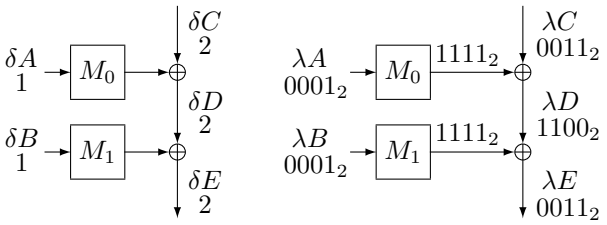

図 8: 遷移しない差分 HW 値 (左) と差分 BT 値 (右) の例

定理 9 5 ラウンド間の一部における各経路の差分値を $\Delta A, \Delta B, \Delta C, \Delta D, \Delta E$ を図 6 (左) のように置いたとき，その BT 値 $\lambda A, \lambda B, \lambda C, \lambda D, \lambda E$ は以下の関係式を満たす．但し，$\lambda A \neq \lambda C$ または $\lambda B \neq 0$ または $\lambda D \neq \lambda E$ とする．

$$\mathrm{HW}'(\lambda A \vee \lambda C) + \mathrm{HW}'(\lambda B) + \mathrm{HW}'(\lambda D \vee \lambda E) \geq 5$$

定理 10 5 ラウンド間の一部における各経路の線形マスク値を $\Gamma A, \Gamma B, \Gamma C, \Gamma D$ を図 7 (左) のように置いたとき，その BT 値 $\mu A, \mu B, \mu C, \mu D$ は以下の関係式を満たす．但し，$\mu A \neq \mu B$ または $\mu C \neq \mu D$ とする．

$$\mathrm{HW}'(\mu A \vee \mu B) + \mathrm{HW}'(\mu C \vee \mu D) \geq 5$$

証明　定理 7,8,9,10 はそれぞれ，定理 1,2,5,6 の証明において，補題 5 を加えることで導かれる．　□

定理 7,8,9,10 を用いることで，より詳細な遷移の判定を行うことが可能となる．例として，図 8 (左) のような差分 HW 値の遷移が存在しないことを示す．

$\delta C = 2$ より，$\lambda C = 0011_2$ とおく．このとき，$\delta A = 1, \delta D = 2$ 及び定理 7 より，$\lambda D = 1100_2$ となる．同様に，$\delta B = 1, \delta E = 2$ より，$\lambda E = 0011_2$ となる．また，DSM の条件 (補題 2) より，

$$\mathrm{HW}(\Delta A) + \mathrm{HW}(\Delta B) + \mathrm{HW}(\Delta C \oplus \Delta E) \geq 5$$

を満たす必要がある．しかし，$\mathrm{HW}(\Delta A) = \mathrm{HW}(\Delta B) = 1$, $\lambda C = \lambda E = 0011_2$ 及び定理 8 より，

$$\begin{aligned}&\mathrm{HW}(\Delta A) + \mathrm{HW}(\Delta B) + \mathrm{HW}(\Delta C \oplus \Delta E) \\ &\leq 2 + \mathrm{HW}'(\lambda C \vee \lambda E) = 2 + \mathrm{HW}'(0011_2) = 4\end{aligned}$$

であるため，不適である．他の λC の値に対しても同様である．よって，図 8 (左) のような差分 HW 値の遷移は起こらない．

Byte Truncate 評価では値の XOR に関する条件式において，Weight Base 評価に比べ情報量の低下が少ないため，ハミング重みだけでなく，非 0 のバイト位置を考慮した条件を利用可能となる．また，Byte Truncate 評価では各 S-box 毎に active かどうかを判別できるため，$\#\mathrm{AS}_0, \#\mathrm{AS}_1$ をそれぞれカウント可能である．

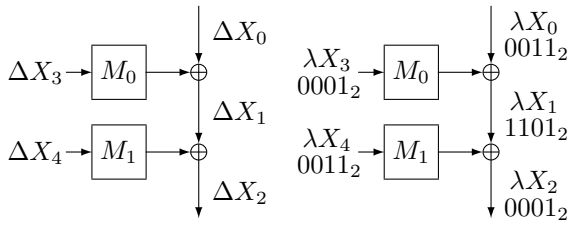

図 9: 3 ラウンド間の一部の差分値 (左) と遷移しない差分 BT 値の例 (右)

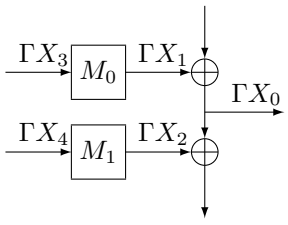

図 10: 3 ラウンド間の一部の線形マスク値

5.4 代数条件の導入

ここまでは，MDS 行列の入出力重みや，HW 値，BT 値の XOR の性質を利用することで，遷移の条件を導出してきた．本節では CLEFIA で用いられる 2 種類の MDS 行列の要素の値 (式 1) に着目した代数的な条件を導出する．

ここで，3 ラウンド間の一部の差分値 $\Delta X_0, \Delta X_1, \Delta X_2, \Delta X_3, \Delta X_4$ を図 9 (左) のように置くと，次式が成り立つ．

$$\begin{pmatrix} I & I & Z & M_0 & Z \\ Z & I & I & Z & M_1 \end{pmatrix} \times \begin{pmatrix} \Delta X_0 \\ \Delta X_1 \\ \Delta X_2 \\ \Delta X_3 \\ \Delta X_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \quad (2)$$

但し，I を単位行列，Z をゼロ行列とする．

ここで，$\Delta X_i = (x_{i,0}|x_{i,1}|x_{i,2}|x_{i,3})$ とし，式 2 を 8 ビット毎に分割した方程式を考える．例として，図 9 (右) のような差分 BT 値について以下に述べる．

各 λX_i の値より，式 2 を整理すると次式が得られる．但し，$x_{0,2}, x_{0,3}, x_{1,0}, x_{1,1}, x_{1,3}, x_{2,3}, x_{3,3}, x_{4,2}, x_{4,3} \in \{0,1\}^8$ は全て非 0 である．

$$\begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 6 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 4 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 2 & a \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & a & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 8 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 8 & 1 \end{pmatrix} \times \begin{pmatrix} x_{0,2} \\ x_{0,3} \\ x_{1,0} \\ x_{1,1} \\ x_{1,3} \\ x_{2,3} \\ x_{3,3} \\ x_{4,2} \\ x_{4,3} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

各行列の要素は GF(2^8) 上の要素である．この式を解くと，$x_{0,2}, x_{0,3}, x_{1,0}, x_{1,1}, x_{1,3}, x_{2,3}, x_{3,3}, x_{4,2}, x_{4,3}$ が全て非 0 となる解は存在しないことが分かる．即ち，図 9 (右) のような差分 BT 値の遷移が起こらないことを表す．

このように，任意の λX_i について，同様に行列を解くことで，その差分 BT 値の遷移が起こるかどうかを判定することが可能である．但し，この行列の要素の値を用いた遷移の判定は，これまでの条件とは違い，M_0, M_1 を入れ替えると判定結果が異なる場合がある．

線形マスク値についても同様に行列を利用した線形マスク遷移の判定が可能である．3 ラウンド間の一部の線形マスク値 $\Gamma X_0, \Gamma X_1, \Gamma X_2, \Gamma X_3, \Gamma X_4$ を図 10 のように置くと，次式が成り立つ．

$$\begin{pmatrix} I & I & I & Z & Z \\ Z & {}^tM_0 & Z & I & Z \\ Z & Z & {}^tM_1 & Z & I \end{pmatrix} \times \begin{pmatrix} \Gamma X_0 \\ \Gamma X_1 \\ \Gamma X_2 \\ \Gamma X_3 \\ \Gamma X_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \quad (3)$$

同様に任意の μX_i について，行列を解くことで，その線形 BT 値の遷移が起こるかどうかの判定を行う．

さらに，差分値及び線形マスク値に対し，3 ラウンド以上であっても同様の方程式が立てられる．本評価では 5 ラウンド間の関係式による判定を行っている．

5.5 改善評価手法のまとめ

DSM の条件に依存するラウンドを 3 ラウンドから 5 ラウンドへと変更して評価することで，遷移の判定をより詳細に行うことが可能となった．また，差分確率，線形確率の異なる 2 種類の S-box を区別することで，より厳密な特性確率を導出することが可能となった．

次に，データ表現においてハミング重みの代わりにバイト毎の 0, 非 0 を扱う，Byte Truncate 評価を行った．計算量は増加するが，情報量の低下が少なく，遷移の詳細な条件が導出でき，2 種類の S-box を区別することが可能となる．また，MDS 行列の入出力重みによる条件でなく，MDS 行列の要素の値からなる条件を考慮することで，遷移の判定をさらに詳細に行うことが可能となった．

5.6 改善された評価結果

Byte Truncate 評価及び代数条件は従来評価手法と比べ，計算量が膨大なものとなる．Weight Base 評価と Byte Truncate 評価及び代数条件を併用することにより，計算量の削減を図った．

これらの改善評価手法を適用した計算機実験による，R ラウンド CLEFIA における最大差分特性確率及び最

表 3: 最大差分特性確率及び最大線形特性確率の評価結果

	最大差分特性確率		最大線形特性確率	
R	従来評価	本評価	従来評価	本評価
1	0	0	0	0
2	4.678	4.678	4.385	4.385
3	9.356	9.356	21.925	21.925
4	28.068	32.034	26.310	29.540
5	37.424	41.390	43.850	47.080
6	56.136	62.746	65.775	70.620
7	65.492	73.424	70.160	82.620
8	84.204	101.492	78.930	98.545
9	93.560	110.136	87.700	113.775
10	102.916	119.492	100.855	121.390
11	112.272	134.848	114.010	134.085
12	130.984	151.526	131.550	144.470

※ 但し，それぞれの確率に対し，$-\log_2$ を取った．また，網掛けは 128 以上を表す．

大線形特性確率の評価結果を表 3 に示す．従来評価では特性確率が 2^{-128} 以下となるのは差分，線形共に 12 ラウンドが最低限必要としていたが，本評価手法を適用することで 11 ラウンドでも 2^{-128} 以下となることが分かった．これは，攻撃者が差分攻撃及び線形攻撃に利用可能な 11 ラウンド差分特性及び線形特性が存在しないことを意味する．

6 まとめ

本論文では，CLEFIA に対し，設計者らの評価手法を基にした，差分特性確率及び線形特性確率の改善評価手法を示した．また，その評価手法を用いることで，差分攻撃及び線形攻撃に対する安全性評価を更新し，CLEFIA は 11 ラウンド以上で差分攻撃及び線形攻撃に利用可能なパスが存在しないことを示した．

参考文献

[1] K. Aoki, T. Ichikawa, M. Kanda, M. Matsui, S. Moriai, J. Nakajima, and T. Tokita, “Camellia: A 128-bit block cipher suitable for multiple platforms,” in Proceedings of Selected Areas in Cryptography - SAC’00 (D. R. Stinson and S. E. Tavares, eds.), no. 2012 in LNCS, pp. 41–54, Springer-Verlag, 2001.

[2] E. Biham and A. Shamir, “Differential cryptanalysis of DES-like cryptosystems,” Journal of Cryptology, vol. 4, pp. 3–72, 1991.

[3] E. Biham and A. Shamir, “Differential Cryptanalysis of the Data Encryption Standard,” Springer-Verlag, 1993.

[4] J. Daemen and V. Rijmen, “Statistics of Correlation and Differentials in Block Ciphers,” in IACR ePrint archive 2005/212, 2005.

[5] J. Daemen and V. Rijmen, “The Design of Rijndael: AES — The Advanced Encryption Standard (Information Security and Cryptography),” Springer, 2002.

[6] M. Matsui, “Linear cryptanalysis of the data encryption standard,” in Proceedings of Eurocrypt’93 (T. Helleseth, ed.), no. 765 in LNCS, pp. 386–397, Springer-Verlag, 1994.

[7] T. Shirai and B. Preneel, “On Feistel ciphers using optimal diffusion mappings across multiple rounds,” in Proceedings of ASIACRYPT’04 (P. J. Lee, ed.), no. 3329 in LNCS, pp. 1–15, Springer-Verlag, 2004.

[8] T. Shirai and K. Shibutani, “Improving immunity of Feistel ciphers against differential cryptanalysis by using multiple MDS matrices,” in Proceedings of Fast Software Encryption - FSE’04 (B. Roy and W. Meier, eds.), no. 3017 in LNCS, pp. 260–278, Springer-Verlag, 2004.

[9] T. Shirai and K. Shibutani, “On Feistel structures using a diffusion switching mechanism,” in Proceedings of Fast Software Encryption —FSE’06 (M. Robshaw, ed.), no. 4047 in LNCS, pp. 41–56, Springer-Verlag, 2006.

[10] T. Shirai, K. Shibutani, T. Akishita, S. Moriai, and T. Iwata, “The 128-bit blockcipher CLEFIA,” in Proceedings of Fast Software Encryption - FSE’07 (A. Biryukov, ed.), no. 4593 in LNCS, pp. 181–195, Springer-Verlag, 2007.

[11] Y. Zheng, T. Matsumoto, and H. Imai, “On the Construction of Block Ciphers Provably Secure and Not Relying on Any Unproved Hypotheses,” in Proceedings of CRYPTO 89 (G. Brassard, ed.), no. 435 in LNCS, pp. 461–480, Springer-Verlag, 1989.