CLEFIAの差分攻撃及び線形攻撃耐性評価の更新

Update of the Security Evaluation of CLEFIA Against Differential Attack and Linear Attack

三津田敦司, 白井太三
ソニー株式会社

目次

- 概要
  - 目的，内容
- CLEFIA
  - 基本構造
  - 拡散行列切り替え法(DSM)
- 差分攻撃/線形攻撃に対する安全性評価
  - 従来評価結果
  - 本評価結果
  - 従来手法と新手法の評価手法の違い
- まとめ

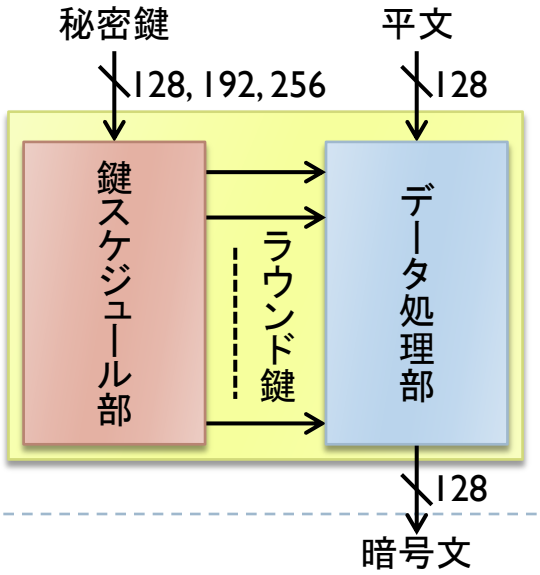
概要

- CLEFIAの差分攻撃/線形攻撃耐性は提案者らによって評価
  - ハミング重みによる差分/線形active S-box数探索
  - 特性確率評価で12ラウンドで共に安全性基準を達成
- 提案者評価における11ラウンド最大差分特性確率を与えるパスが存在しないことを発見
- CLEFIAの差分特性/線形特性の厳密な評価
  - 新たな評価手法の導出
  - 11ラウンドで安全性基準を達成

CLEFIA

- FSE2007において提案された共通鍵ブロック暗号
- 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
- ブロック長：128ビット
- 鍵長：128, 192, 256ビット
- データ処理部と鍵スケジュール部からなる

  →データ処理部の安全性について述べる

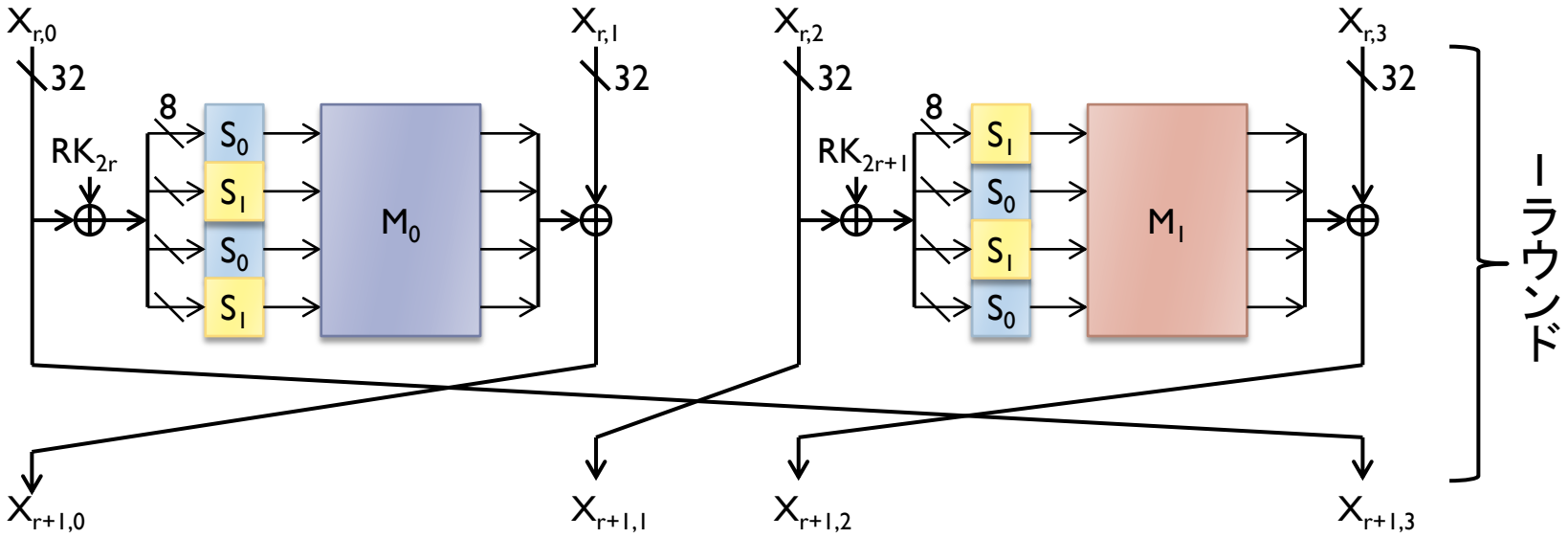


※本研究では各ラウンド鍵は
真に独立ランダムと仮定

CLEFIAのデータ処理部の基本構造

- 4系列Type-2一般化Feistel構造
- 2種類の8ビットS-box S_0, S_1
- 2種類の4×4MDS行列 M_0, M_1

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



MDS行列の入出力ハミング重み

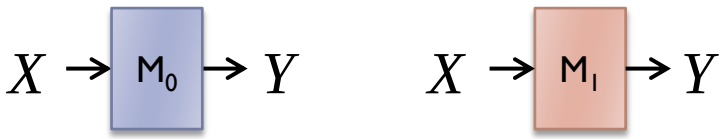
- 定義：ハミング重み δX
  - 32ビットのデータ X を8ビット毎，4つに分割したものの内，非0の個数

$$X = (x_0 \mid x_1 \mid x_2 \mid x_3) \in (\{0,1\}^8)^4$$

$$\delta X = \#\{i \mid 0 \le i \le 3, x_0 \neq 0^8\}$$

- 4×4MDS行列（分岐数5）
  - 行列の入力 X , 出力 Y に対し，次式が成り立つ

$$\begin{cases} \delta Y = 0 & (\delta X = 0) \\ \delta X + \delta Y \ge 5 & (\delta X \neq 0) \end{cases}$$



CLEFIAの特徴：拡散行列切り替え法(DSM)

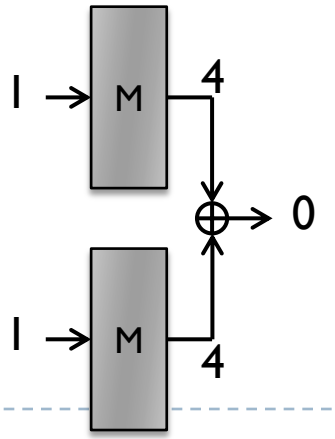
- 差分攻撃，線形攻撃に対する耐性を強化
  - 2種類のMDS行列を結合した行列の分岐数が5

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

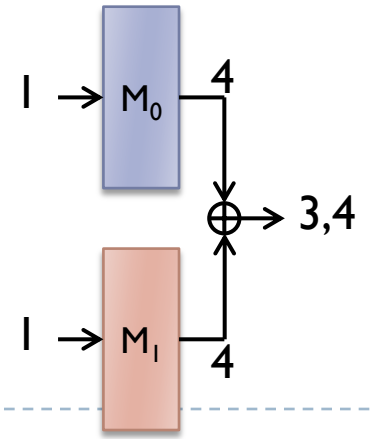
⇒近傍ラウンド中の差分/線形マスクのハミング重みを保証

- 差分ハミング重みの例

MDS行列が1種類のとき



$M_0|M_1$の分岐数が5 のとき



CLEFIAの特徴：拡散行列切り替え法(DSM)

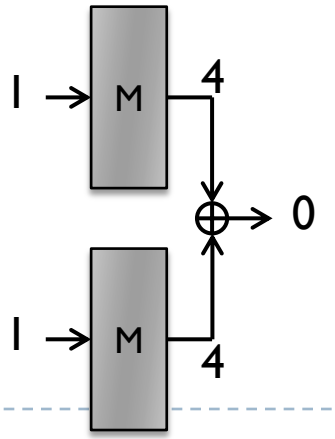
- 差分攻撃，線形攻撃に対する耐性を強化
  - 2種類のMDS行列を結合した行列の分岐数が5

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

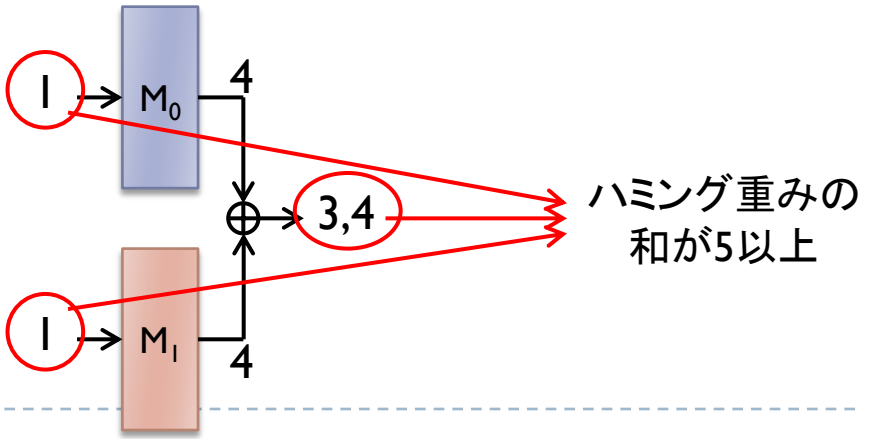
⇒近傍ラウンド中の差分/線形マスクのハミング重みを保証

- 差分ハミング重みの例

MDS行列が1種類のとき



$M_0|M_1$の分岐数が5 のとき

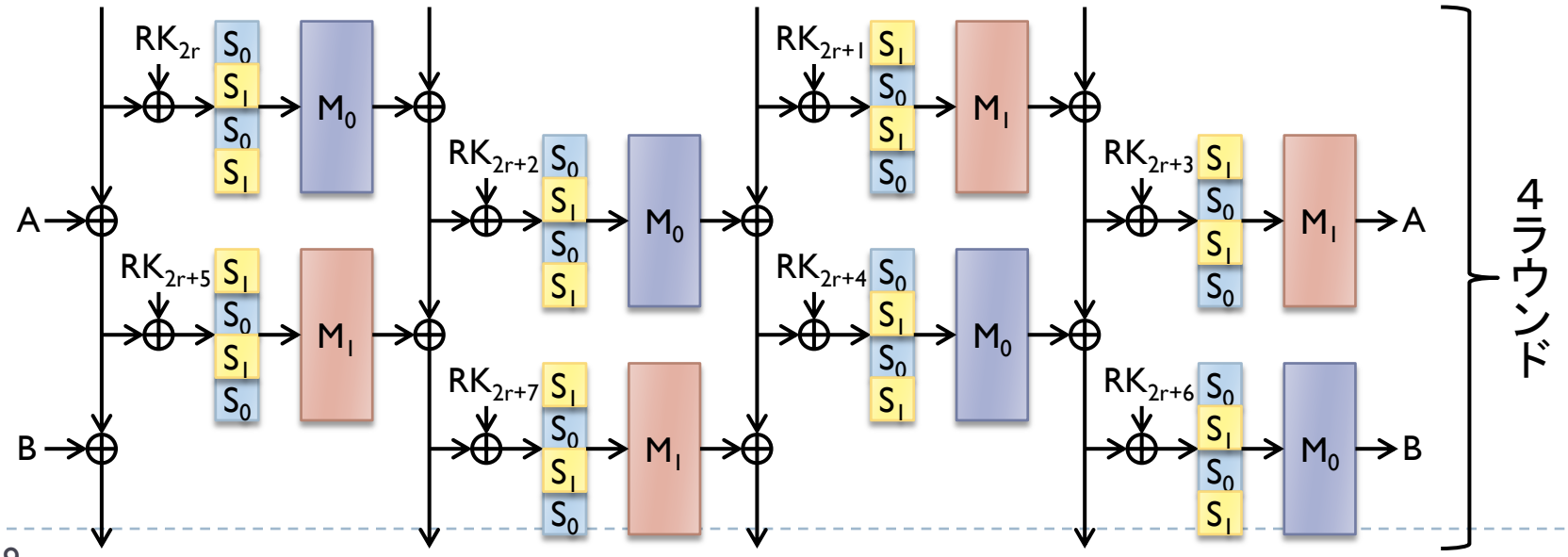


CLEFIAの特徴：拡散行列切り替え法(DSM)

- 差分攻撃，線形攻撃に対する耐性を強化
  - 2種類のMDS行列を結合した行列の分岐数が5となる様に設計

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

⇒近傍ラウンド中の差分/線形マスクのハミング重みを保証



差分攻撃/線形攻撃に対する安全性評価

- ブロック暗号に対する汎用的かつ強力な攻撃
- 差分攻撃に対する安全性評価
  - 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
  - S-boxの最大差分確率と差分active S-box数を用いて評価
    - 差分特性確率≦(S-boxの最大差分確率)$^{\text{最小差分active S-box数}}$
  - 差分特性確率が2^{-128}以下であるとき安全
- 線形攻撃に対する安全性評価
  - 線形active S-box数を用いて同様に評価
    - 線形特性確率≦(S-boxの最大線形確率)$^{\text{最小線形active S-box数}}$
- active S-box数の計算手法
  - 証明ベース
  - 計算機実験

⇒従来評価及び本評価では計算機実験を用いている

従来評価結果

- active S-boxの下界を導出
  - 全てのactive S-boxがS_0であるとし，特性確率の上界を求める

	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}

- 最大差分特性確率 : maxDCP
  - 12ラウンド中に28個以上のactive S-box

$$\max DCP \le (2^{-4.678})^{28} = 2^{-130.984} < 2^{-128}$$

- 最大線形特性確率 : maxLCP
  - 12ラウンド中に30個以上のactive S-box

$$\max LCP \le (2^{-4.385})^{30} = 2^{-131.550} < 2^{-128}$$

12ラウンドで安全性基準を達成

active S-boxの保証数

ラウンド数	差分	線形
1	0	0
2	1	1
3	2	5
4	6	6
5	8	10
6	12	15
7	14	16
8	18	18
9	20	20
10	22	23
11	24	26
12	28	30

従来評価結果

- active S-boxの下界を導出
  - 全てのactive S-boxがS_0であるとし，特性確率の上界を求める

	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}

- 最大差分特性確率 : maxDCP
  - 12ラウンド中に28個以上のactive S-box

$$\max DCP \le (2^{-4.678})^{28} = 2^{-130.984} < 2^{-128}$$

- 最大線形特性確率 : maxLCP
  - 12ラウンド中に30個以上のactive S-box

$$\max LCP \le (2^{-4.385})^{30} = 2^{-131.550} < 2^{-128}$$

12ラウンドで安全性基準を達成

active S-boxの保証数

ラウンド数	差分	線形
1	0	0
2	1	1
3	2	5
4	6	6
5	8	10
6	12	15
7	14	16
8	18	18
9	20	20
10	22	23
11	24	26
12	28	30

24個となるパス遷移に矛盾があったため，より詳細な評価を行った

本評価結果

- 厳密な評価を行うことで，よりタイトな特性確率の上界を導出

$-\log_2$(最大差分特性確率)

ラウンド数	従来手法	新手法
1	0	0
2	4.678	4.678
3	9.356	10.678
4	28.068	32.034
5	37.424	41.390
6	56.136	62.746
7	65.492	73.424
8	84.204	101.492
9	93.560	110.136
10	102.916	119.492
11	112.272	134.848
12	130.984	151.526

※予稿集にミス

$-\log_2$(最大線形特性確率)

ラウンド数	従来手法	新手法
1	0	0
2	4.385	4.385
3	21.925	21.925
4	26.310	29.540
5	43.850	47.080
6	65.775	70.620
7	70.160	82.620
8	78.930	98.545
9	87.700	113.775
10	100.855	121.390
11	114.010	134.085
12	131.550	144.470

- 11ラウンドで共に特性確率が2^{-128}以下となる

⇒ 11ラウンドでも安全性基準を達成

従来手法と新手法

- 共通点
  - 計算機を用いたパス探索による最大差分/線形特性確率の導出
- 変更点
  1. パス遷移の依存ラウンド数

     3ラウンド ⇒ 5ラウンド
  2. 各系列のデータ表現

     ハミング重み ⇒ byte truncate
  3. 2種類のS-boxの区別

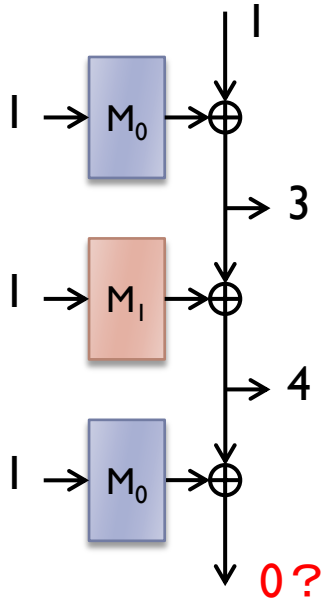
     S_0の最大差分/線形確率を利用 ⇒ S_0,S_1それぞれの最大差分/線形確率を利用
  4. パス遷移条件

     拡散行列切り替え法による入出力重みを考慮

     ⇒ 拡散行列の値に着目した代数的条件を考慮

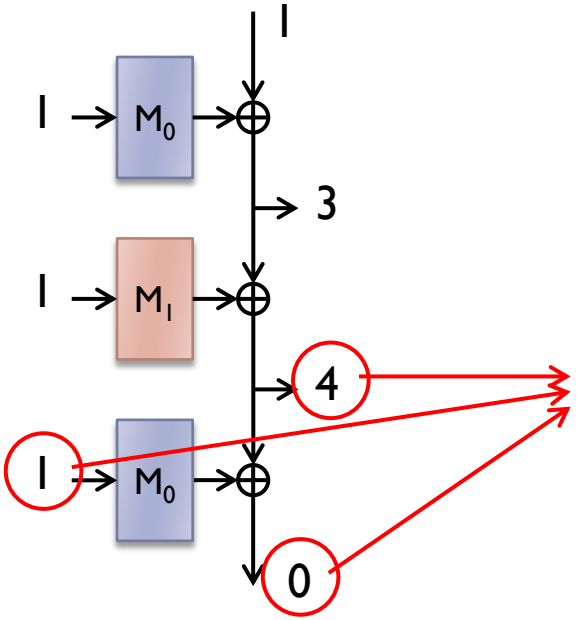
1. パス遷移の依存ラウンド数

- 新手法では5ラウンド間のパスを考慮
  - 従来手法では3ラウンド間のパスを考慮
- 例として以下の差分ハミング重み遷移を考える



1. パス遷移の依存ラウンド数

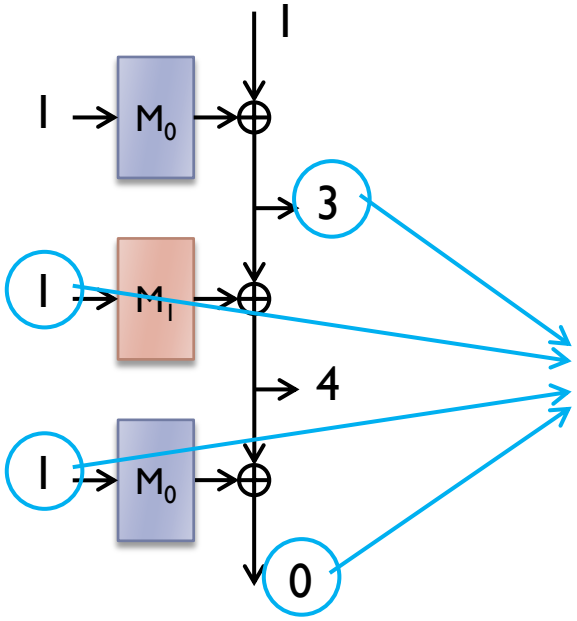
- 新手法では5ラウンド間のパスを考慮
  - 従来手法では3ラウンド間のパスを考慮
- 例として以下の差分ハミング重み遷移を考える



1ラウンド間：MDS行列による遷移判定
1+4+0≧5

1. パス遷移の依存ラウンド数

- 新手法では5ラウンド間のパスを考慮
  - 従来手法では3ラウンド間のパスを考慮
- 例として以下の差分ハミング重み遷移を考える



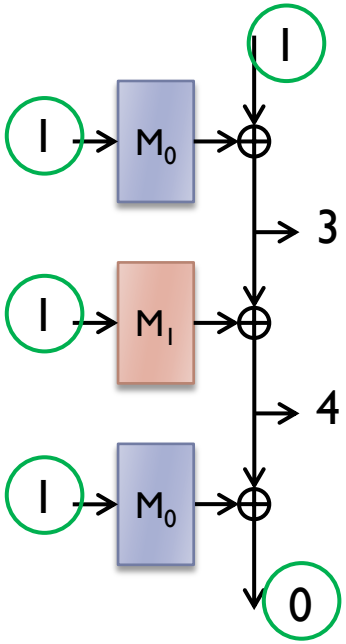
3ラウンド間：DSMによる遷移判定

1+1+3+0≧5

⇒3ラウンド間の関係では矛盾がなく，
従来手法では正しい遷移としていた

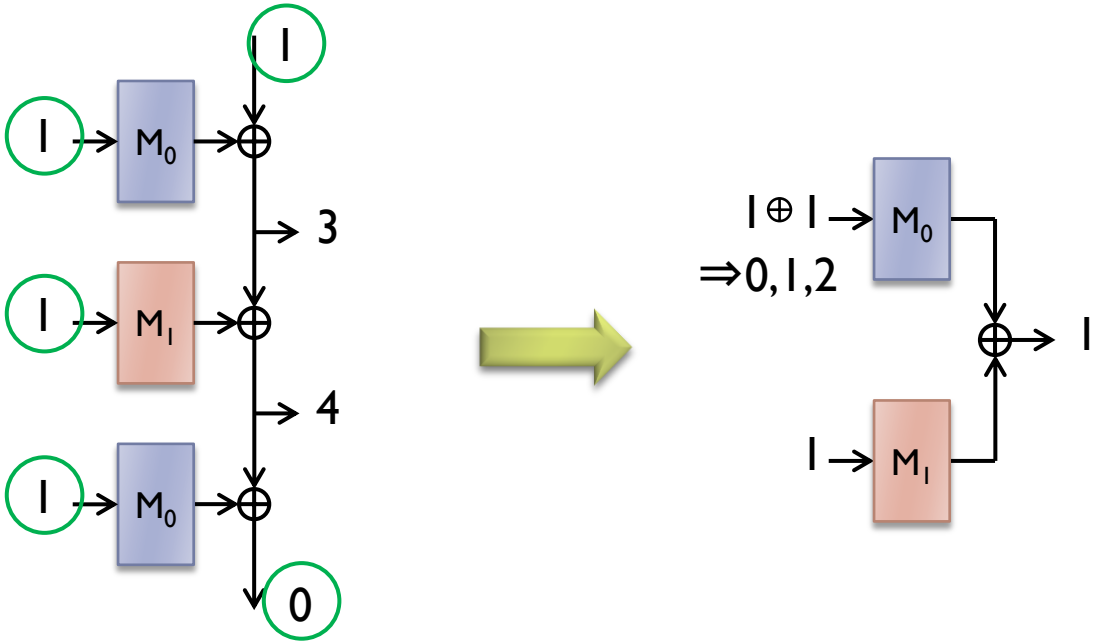
1. パス遷移の依存ラウンド数

- 新手法では5ラウンド間のパスを考慮
  - 従来手法では3ラウンド間のパスを考慮
- 例として以下の差分ハミング重み遷移を考える



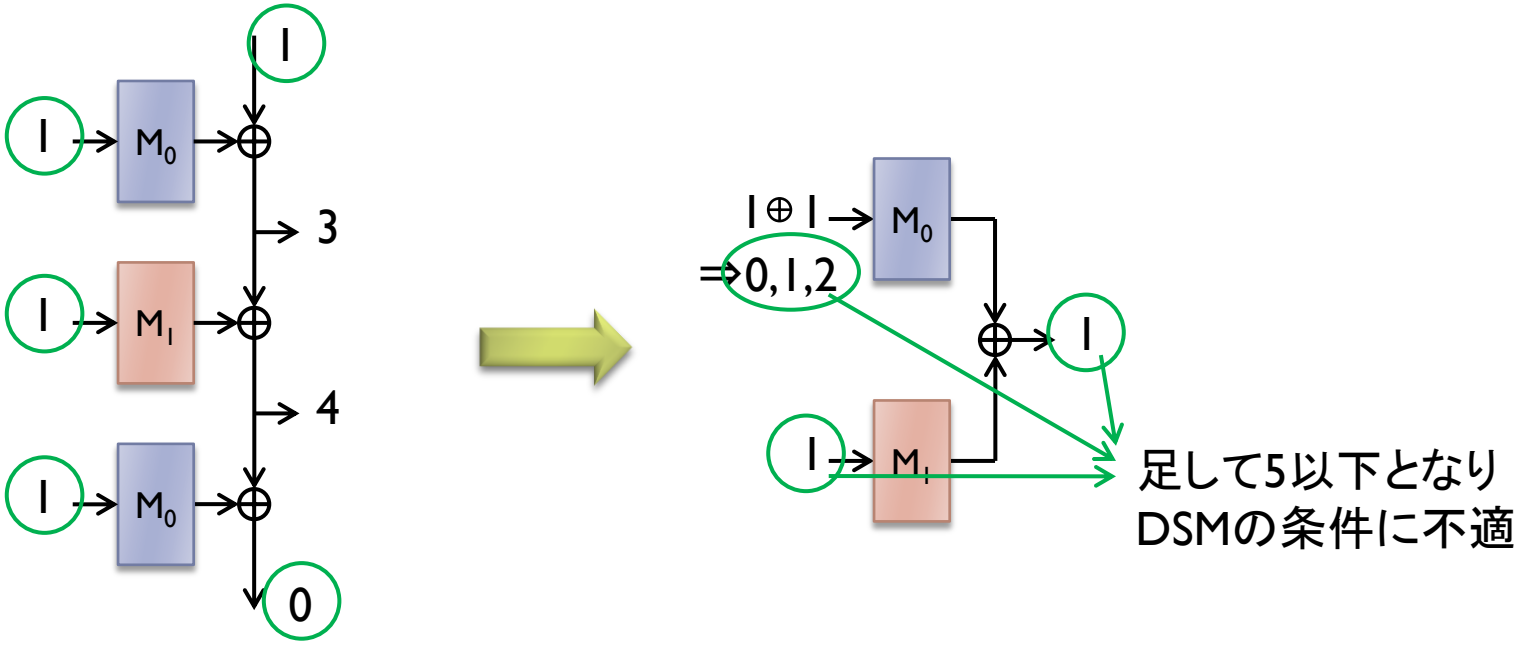
1. パス遷移の依存ラウンド数

- 新手法では5ラウンド間のパスを考慮
  - 従来手法では3ラウンド間のパスを考慮
- 例として以下の差分ハミング重み遷移を考える



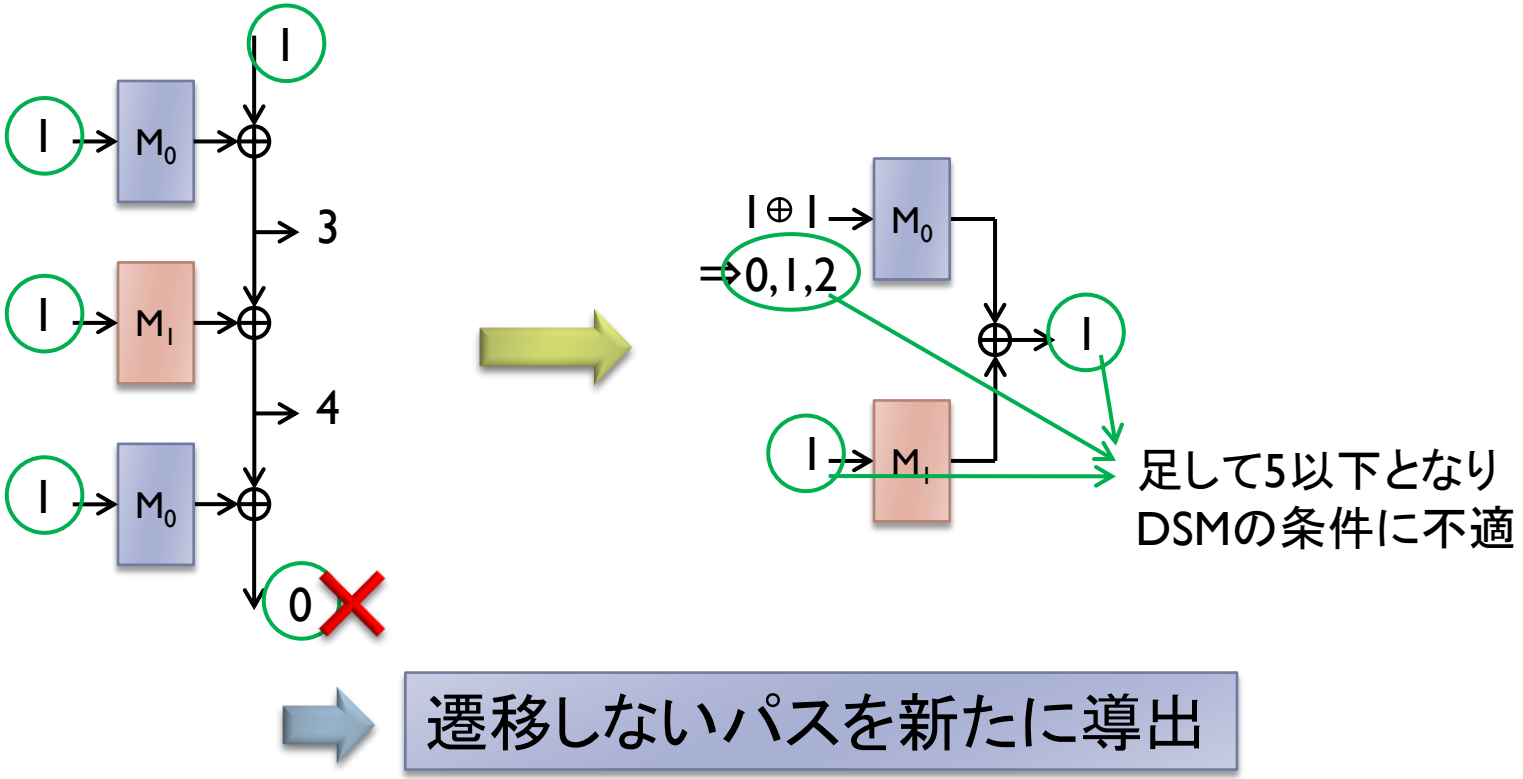
1. パス遷移の依存ラウンド数

- 新手法では5ラウンド間のパスを考慮
  - 従来手法では3ラウンド間のパスを考慮
- 例として以下の差分ハミング重み遷移を考える



1. パス遷移の依存ラウンド数

- 新手法では5ラウンド間のパスを考慮
  - 従来手法では3ラウンド間のパスを考慮
- 例として以下の差分ハミング重み遷移を考える



2. 各系列のデータ表現

- 各系列32ビット毎のデータ全てを評価することは困難　$\rightarrow 2^{32}$
- バイト毎の0,非0を考慮したデータに置き換え

$$X = (x_0 \mid x_1 \mid x_2 \mid x_3) \in (\{0,1\}^8)^4$$

- ハミング重み（従来手法）
  - 系列毎に，byte単位の非0の個数で置き換え　$\rightarrow 0 \sim 4$

$$\delta X = \#\{i \mid 0 \le i \le 3, x_0 \ne 0^8\}$$

- Byte truncate（新手法）
  - 系列毎に，byte単位で0, 非0を0, 1で置き換え　$\rightarrow 0000_2 \sim 1111_2$

$$\lambda X = \hat{x}_0 \mid \hat{x}_1 \mid \hat{x}_2 \mid \hat{x}_3 \qquad \hat{x}_i = \begin{cases} 0 & (x_i = 0^8) \\ 1 & (x_i \ne 0^8) \end{cases}$$

情報量の低下が抑えられるため，より厳密な評価が可能

3. 2種類のS-boxの区別

- 従来手法では全てのactiveなS-boxがS_0であるとして評価

- 新手法ではS_0, S_1を分けてカウント
  - 最大差分/線形確率の小さいS_1を考慮
  - Byte Truncateにより，S_0, S_1どちらがactiveであるかを評価可能

例．差分評価においてS_0, S_1のactive数がそれぞれ16, 9のとき(合計25)

- 従来手法（全てS_0とする）

$$DCP \leq (2^{-4.678})^{25} = 2^{-116.950}$$

- 新手法（S_0 , S_1を区別）

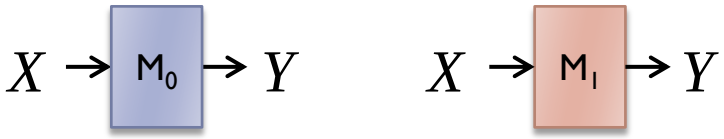
$$DCP \leq (2^{-4.678})^{16} \times (2^{-6})^{9} = 2^{-128.848} < 2^{-128}$$

	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}

従来よりactive S-box数が少なくても，特性確率が2^{-128}以下を達成

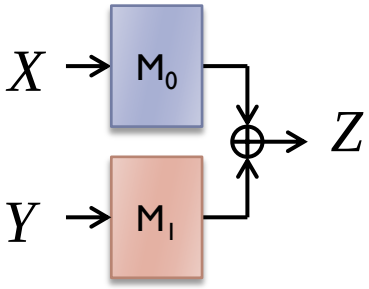
4. パス遷移条件(従来手法)

- MDS行列の入出力重みによる条件



$$\begin{cases} \delta Y = 0 & (\delta X = 0) \\ \delta X + \delta Y \geq 5 & (\delta X \neq 0) \end{cases}$$

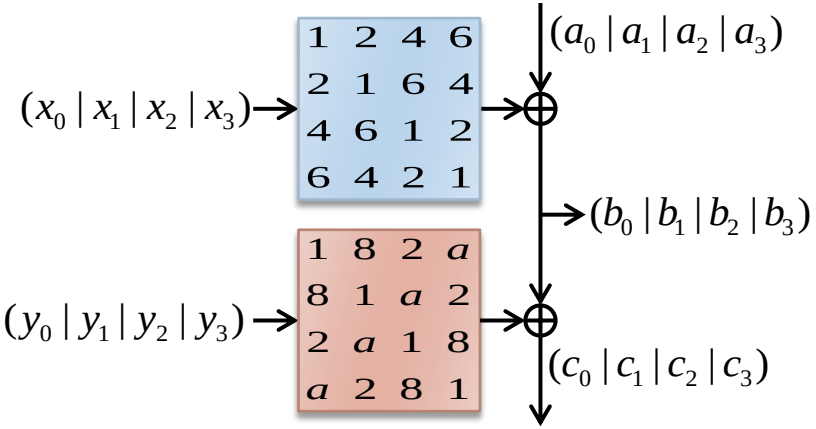
- DSMを考慮した条件



$$\begin{cases} \delta Z = 0 & (\delta X = \delta Y = 0) \\ \delta X + \delta Y + \delta Z \geq 5 & (else) \end{cases}$$

4. パス遷移条件(新手法)

- 拡散行列の値に着目
  - 下左図の差分値に対し，下右図の方程式が成り立つ(GF(2^8))



$$\begin{pmatrix} 1&2&4&6&0&0&0&0&1&0&0&0&1&0&0&0&0&0&0&0 \\ 2&1&6&4&0&0&0&0&0&1&0&0&0&1&0&0&0&0&0&0 \\ 4&6&1&2&0&0&0&0&0&0&1&0&0&0&1&0&0&0&0&0 \\ 6&4&2&1&0&0&0&0&0&0&0&1&0&0&0&1&0&0&0&0 \\ 0&0&0&0&1&8&2&a&0&0&0&0&1&0&0&0&1&0&0&0 \\ 0&0&0&0&8&1&a&2&0&0&0&0&0&1&0&0&0&1&0&0 \\ 0&0&0&0&2&a&1&8&0&0&0&0&0&0&1&0&0&0&1&0 \\ 0&0&0&0&a&2&8&1&0&0&0&0&0&0&0&1&0&0&0&1 \end{pmatrix} \begin{pmatrix} {}^t(x_0,x_1,x_2,x_3) \\ {}^t(y_0,y_1,y_2,y_3) \\ {}^t(a_0,a_1,a_2,a_3) \\ {}^t(b_0,b_1,b_2,b_3) \\ {}^t(c_0,c_1,c_2,c_3) \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

  - 各バイト毎の0, 非0を考慮
    - 各byte truncate値に対する遷移の判定が可能
  - さらに複数ラウンド間の行列に対しても同様
  - 線形も同様に判定が可能

⇒ 従来より厳密な条件を与えたパス遷移を導出

新手法評価結果

- 評価手法に変更を加え，厳密な特性確率を導出

$-\log_2$(最大差分特性確率)

ラウンド	従来手法	新手法
1	0	0
2	4.678	4.678
3	9.356	10.678
4	28.068	32.034
5	37.424	41.390
6	56.136	62.746
7	65.492	73.424
8	84.204	101.492
9	93.560	110.136
10	102.916	119.492
11	112.272	134.848
12	130.984	151.526

$-\log_2$(最大線形特性確率)

ラウンド	従来手法	新手法
1	0	0
2	4.385	4.385
3	21.925	21.925
4	26.310	29.540
5	43.850	47.080
6	65.775	70.620
7	70.160	82.620
8	78.930	98.545
9	87.700	113.775
10	100.855	121.390
11	114.010	134.085
12	131.550	144.470

変更点	従来手法	新手法
依存段数	3ラウンド	5ラウンド
データ表現	ハミング重み	Byte truncate
S-box	S_0	S_0,S_1
遷移判定	入出力重み	代数的条件

⇒ 11ラウンドで安全性基準を達成

まとめ

- CLEFIAの差分/線形特性確率の厳密な評価を行った
  1. パス遷移の依存ラウンド数の増加
  2. 各系列のデータ表現を変更
  3. 2種類のS-boxの区別
  4. パス遷移条件の詳細化

- 11ラウンドで差分/線形特性確率が2^{-128}以下となることを示した
  - 従来では12ラウンド
  - 差分/線形特性を利用した差分/線形攻撃に対して，セキュリティマージンが1ラウンド増加したことを示す