段数を削減したPRESENTを用いた倍ブロック長圧縮関数に対する衝突攻撃

小林　哲也†*　　廣瀬　勝一†

Collision Attack on Double-Block-Length Compression Function Using Round-Reduced PRESENT

Tetsuya KOBAYASHI†* and Shoichi HIROSE†

あらまし　我々は，軽量ブロック暗号 PRESENT を用いて構成した倍ブロック長圧縮関数に対する衝突攻撃の検討を行った．本論文では，段数を 10 段に削減した PRESENT を用いた倍ブロック長圧縮関数に対して，計算量 2^{60} で衝突攻撃が行えることを示す．また段数を 8 段に削減した PRESENT を用いた倍ブロック長圧縮関数に対する衝突攻撃の計算機実験の結果を示す．更に計算量の理論値と実験値の比較を行う．

キーワード　ハッシュ関数，倍ブロック長圧縮関数，衝突攻撃，PRESENT

1. まえがき

(a) 背　　景

ハッシュ関数は任意長の系列を固定長の系列に変換する関数であり，情報セキュリティにおいて重要な基本的要素として，改ざんの検知，メッセージ認証，擬似乱数生成などに用いられている．ハッシュ関数に要求される主な性質として，衝突計算困難性，原像計算困難性，第二原像計算困難性の三つが挙げられる．これらはハッシュ関数の出力長を n としたとき，衝突，原像，第二原像を見つけるためにそれぞれ $2^{n/2}$，2^n，2^n の計算量が必要であることを要求する．衝突攻撃は，ハッシュ関数を h としたとき，$h(m) = h(\tilde{m})$ を満たすような相異なる m，$\tilde{m}$ を見つける攻撃である．

現在広く利用されているハッシュ関数は，圧縮関数を用いて構成される．圧縮関数は，固定長のメッセージブロックと連鎖値を入力とし，固定長の値を出力する．入力メッセージはパディング処理され，固定長のメッセージブロックに分割される．圧縮関数をメッセージブロックごとに繰り返し適用することでハッシュ値の計算を行う．

圧縮関数はブロック暗号を用いて構成することができる．PRESENT [4] は Bogdanov らによって提案された軽量の共通鍵ブロック暗号であり，RFID タグやセンサネットワークなどのメモリや計算能力に制約があるような環境での利用を想定して設計されている．PRESENT は SPN 構造を有する 64 ビットのブロック暗号であり，80 ビットまたは 128 ビット鍵が利用できる．

Bogdanov らは，ブロック暗号 PRESENT を用いた軽量ハッシュ関数の構成法を検討している [5]．Davies-Meyer 方式を用いると，ハッシュ値の長さがブロック暗号のブロック長と等しい圧縮関数を構成できる．この方式で PRESENT を用いてハッシュ関数を構成すると，ハッシュ値の長さは 64 ビットとなり，衝突計算困難性を要求するアプリケーションに対しては十分な安全性を提供できない．一方，[7] に示された構成法を用いるとブロック長の 2 倍の長さのハッシュ値を出力する倍ブロック長圧縮関数を構成できる．PRESENT を用いた場合のハッシュ値の長さは 128 ビットとなる．

(b) 成　　果

本論文では PRESENT を用いた倍ブロック長圧縮関数に対する衝突攻撃について述べる．段数を 10 段に削減した PRESENT を用いた倍ブロック長圧縮関数に対して，計算量 2^{60} で衝突攻撃が行えることを示す．本攻撃では攻撃者は連鎖値（または初期値）の値

† 福井大学大学院工学研究科，福井市
Graduate School of Engineering, University of Fukui, Fukui-shi, 910–8507 Japan
* 現在，アイシン・エィ・ダブリュ株式会社

を自由に決めることができない．また，段数を 8 段に削減した PRESENT を用いた倍ブロック長圧縮関数に対する衝突攻撃の計算機実験の結果を示し，計算量の理論値と実験値の比較を行う．

筆者らの知る限りにおいて，これまでのところ，PRESENT を用いた倍ブロック長圧縮関数に対する衝突攻撃に関する報告はなされていない．

(c) 関 連 研 究

ブロック暗号 PRESENT に対する攻撃の既存研究には次のものがある．Wang は 16 段の PRESENT に対し 2^{64} の選択平文と 2^{65} のメモリアクセスで差分解読が行えることを示した [10]．Albrecht らは，19 段の PRESENT に対し 2^{113} の計算量で差分攻撃が行えることを示した [1]．大熊は 24 段の PRESENT に対し $2^{63.5}$ の既知平文で線形攻撃が行えることを示した [9]．Cho は 26 段の PRESENT に対し 2^{64} の既知平文と 2^{72} の計算量で線形攻撃が行えることを示した [6]．

Biryukov らは，ブロック暗号 Camellia [2] の変形版である byte-Camellia を用いた倍ブロック長圧縮関数に対し，ランダム関数との識別攻撃が行える差分特性が存在することを示した [3]．Wei らは，ブロック暗号 IDEA [8] を用いた種々の単ブロック長，倍ブロック長圧縮関数の脆弱性を指摘した [11]．小山らは，PRESENT を用いた Davies-Meyer 方式による圧縮関数について，12 段の PRESENT を用いた場合に対して衝突攻撃と第二原像攻撃が可能であること，20 段の PRESENT を用いた場合に対して識別攻撃が可能であることを示した [12]．

(d) 本論文の構成

本論文の構成は次のとおりである．**2.** では，ブロック暗号 PRESENT と倍ブロック長圧縮関数について述べる．**3.** では，10 段の PRESENT を用いた倍ブロック長圧縮関数への衝突攻撃を示す．**4.** では，8 段の PRESENT に対する計算機実験の結果を示し，計算量の理論値と実験値の比較を行う．**5.** ではまとめを述べる．

2. 準　　備

2.1 PRESENT の仕様

以下では $\oplus$ はビットごとの排他的論理和を表し，$\|$ はビット列の連接を表す．また，$\lll_\ell$ は ℓ ビットの左巡回シフトを表す．

PRESENT のブロック長は 64 ビットであり，鍵長は 80 ビットまたは 128 ビットである．本論文では 80 ビット鍵の PRESENT を対象とする．PRESENT は SPN (Substitution Permutation Network) 構造を有し，各段で 3 種類の変換 (addRoundKey，sBoxlayer，pLayer) を行う．図 1 にラウンド変換を示す．暗号化ではこの変換を 31 回繰り返した後に，post-whitening の addRoundKey 変換が行われる．

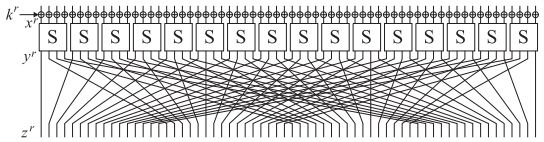

図 1　PRESENT のラウンド変換
Fig. 1　Round transformation of PRESENT.

表 1　PRESENT の S-box
Table 1　S-box of PRESENT.

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$S(x)$	c	5	6	b	9	0	a	d	3	e	f	8	4	7	1	2

PRESENT の r 段目 ($r = 1, 2, \ldots$) のラウンド鍵を k^r と表記し，k^r の下位から j 番目のビットを $k^r[j]$ と表記する．ここで，$j \in \{0, 1, \ldots, 63\}$ であり，$k^r[0]$ が最下位ビットである．$k^r[j]$ から $k^r[l]$ まで ($j < l$) のビット列を $k^r[j..l]$ と表記する．また k^r を 4 ビットごとに区切り，$k^r = k^r_{15} \| k^r_{14} \| \cdots \| k^r_0$ とする．$k^r_i[j]$ ($j \in \{0, 1, 2, 3\}$) は k^r_i の下位から j 番目のビットを表す．同様に，sBoxlayer 変換の直前の状態（addRoundKey 変換後の状態）を x^r，sBoxlayer 変換後の状態を y^r，pLayer 変換後の状態を z^r と表記する．ただし z^0 を平文とする．x^r_i を r 段目の右から i 番目の S-box の入力とする．また鍵レジスタの状態を κ^r と表記する．

（1） addRoundKey 変換では，ラウンド鍵 k^r の排他的論理和が行われる．

$$x^r = z^{r-1} \oplus k^r \ .$$

（2） sBoxlayer 変換では，表 1 に示す 4 ビット入出力の S-box $S(\cdot)$ による非線形変換が行われる．

$$y^r_i = S(x^r_i) \ \text{ for } i \in \{0, \ldots, 15\} \ .$$

（3） pLayer 変換では，ビットごとの並べ換えが行われる．

$$z^r[P(j)] = y^r[j] \ \text{ for } j \in \{0, 1, \ldots, 63\} \ .$$

ここで，

$$P(j) = \begin{cases} 16\,j \bmod 63 & \text{if } j \in \{0,\ldots,62\} \\ 63 & \text{if } j = 63 \end{cases}$$

である．

鍵スケジュールにより秘密鍵から各段の addRoundKey 変換で用いられるラウンド鍵が生成される．まず 80 ビットの鍵レジスタに秘密鍵 K をストアする ($\kappa^1 = K$)．鍵レジスタの上位 64 ビットを r 段目のラウンド鍵として取り出す ($k^r = \kappa^r[16..79]$)．その後，次の手順で鍵レジスタを更新する．

（1） $\kappa^{r+1} = \kappa^r \lll_{61}$ ．

（2） $\kappa^{r+1}[76..79] = S(\kappa^{r+1}[76..79])$ ．

（3） $\kappa^{r+1}[15..19] = \kappa^{r+1}[15..19] \oplus r$ ．

本攻撃では，PRESENT の段数を削減する際に，最後の post-whitening を省略しない．なお，本攻撃は差分攻撃であり，秘密鍵に差分がない場合を考えるため，post-whitening の有無は攻撃に影響を与えない．

2.2 差分攻撃

本攻撃はビットごとの XOR 差分を考える差分攻撃であり，差分の伝搬は非線形関数で確率的となる．δ_{I} を入力差分，δ_{O} を出力差分とするとき，

$$S(x \oplus \delta_{\mathrm{I}}) \oplus S(x) = \delta_{\mathrm{O}} \tag{1}$$

を満たす解 x を δ_{I}，δ_{O} に対する許容値と呼ぶ．δ_{I}，δ_{O} の組合せにより，許容値の個数は 0 個，2 個，4 個のいずれかである．許容値が 0 個の場合を除くと，S-box への入力がランダムに決まるとき，2^{-3} または 2^{-2} の確率で許容値が入力される．また，入力差分が 0 でない S-box を活性 S-box と呼ぶ．

2.3 H-PRESENT

本研究は図 2 に示す倍ブロック長圧縮関数 [7] を対象とする．この圧縮関数はブロック暗号 E を用いて構成され，連鎖値 G，H 及び，メッセージブロック M を入力とし，出力 G'，H' を次のように計算する．

$$\begin{aligned} G' &= f_{\mathrm{U}}(G,K) = E_K(G) \oplus G \ , \\ H' &= f_{\mathrm{L}}(G,K) = E_K(G \oplus c) \oplus G \oplus c \ . \end{aligned} \tag{2}$$

ここで $K = M \| H$ であり，c は非零の定数である．

この倍ブロック長圧縮関数のブロック暗号 E に 80 ビット鍵の PRESENT を用いたものを，H-PRESENT と呼ぶ．H-PRESENT の出力は 128 ビットである．

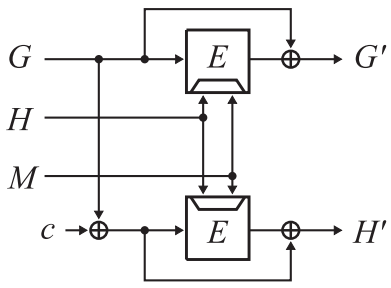

図 2　倍ブロック長圧縮関数
Fig. 2　Double-block-length compression function.

3. 10 段の H-PRESENT に対する衝突攻撃

本章では，10 段の PRESENT を用いた H-PRESENT に対する衝突攻撃を示す．

以下では，内部状態の変数に関する差分を Δx のように Δ を付けて表す．また f_{L} の内部状態を表す変数に $\hat{x}$ のように ^ を付けて表す．

3.1 概　　要

G に関する差分を ΔG，K に関する差分を ΔK とするとき，f_{U}，f_{L} の出力に関する衝突をそれぞれ次のように表すことができる．

$$f_{\mathrm{U}}(G,K) = f_{\mathrm{U}}(G \oplus \Delta G, K \oplus \Delta K) \ . \tag{3}$$

$$f_{\mathrm{L}}(G,K) = f_{\mathrm{L}}(G \oplus \Delta G, K \oplus \Delta K) \ . \tag{4}$$

本研究で提案する衝突攻撃では $\Delta G \neq \mathbf{0}$，$\Delta K = \mathbf{0}$ である衝突が得られる．

(G,K) が式 (3) と式 (4) の両式を満たすとき，H-PRESENT の圧縮関数の出力が衝突する．すなわち E に関して，

$$\begin{cases} E_K(G) \oplus E_K(G \oplus \Delta G) = \Delta G \\ E_K(G \oplus c) \oplus E_K(G \oplus \Delta G \oplus c) = \Delta G \end{cases} \tag{5}$$

を満たす (G,K) が見つかったとき，圧縮関数の衝突が生じている．

本攻撃は，まず f_{U} で衝突が起こる (G,K) を見つけ，その (G,K) について f_{L} でも衝突が起こるかを確認する．f_{U} と f_{L} の両方で衝突が起こる (G,K) を見つけるまでこれを繰り返す．

3.2 攻撃方法

本攻撃では，f_{U} と f_{L} の両方で表 2 と図 3 に示された 10 段の差分経路を用いる．これは，入力差分と出力差分が等しくかつ各段の活性 S-box の個数が 2 以下（ただし 1 段目については 2）となる 10 段の差分経路のうち，差分確率が最大の差分経路である．また，後述のように 1 段目から 3 段目までの活性 S-box の

表 2　10 段の差分経路とその確率
Table 2　10-round differential path and its probabilities.

段	差分	確率
1	$\Delta x_0^1 = 5,\ \Delta x_8^1 = 5$	
	$\Delta y_0^1 = 1,\ \Delta y_8^1 = 1$	2^{-6}
2	$\Delta x_0^2 = 1,\ \Delta x_2^2 = 1$	
	$\Delta y_0^2 = 9,\ \Delta y_2^2 = 9$	2^{-4}
3	$\Delta x_0^3 = 5,\ \Delta x_{12}^3 = 5$	
	$\Delta y_0^3 = 4,\ \Delta y_{12}^3 = 4$	2^{-6}
4	$\Delta x_8^4 = 1,\ \Delta x_{11}^4 = 1$	
	$\Delta y_8^4 = 9,\ \Delta y_{11}^4 = 9$	2^{-4}
5	$\Delta x_2^5 = 9,\ \Delta x_{14}^5 = 9$	
	$\Delta y_2^5 = 4,\ \Delta y_{14}^5 = 4$	2^{-4}
6	$\Delta x_8^6 = 4,\ \Delta x_{11}^6 = 4$	
	$\Delta y_8^6 = 5,\ \Delta y_{11}^6 = 5$	2^{-4}
7	$\Delta x_2^7 = 9,\ \Delta x_{10}^7 = 9$	
	$\Delta y_2^7 = 9,\ \Delta y_{10}^7 = 4$	2^{-4}
8	$\Delta x_8^8 = 4,\ \Delta x_{10}^8 = 4$	
	$\Delta y_8^8 = 5,\ \Delta y_{10}^8 = 5$	2^{-4}
9	$\Delta x_2^9 = 5,\ \Delta x_{10}^9 = 5$	
	$\Delta y_2^9 = 1,\ \Delta y_{10}^9 = 1$	2^{-6}
10	$\Delta x_0^{10} = 4,\ \Delta x_2^{10} = 4$	
	$\Delta y_0^{10} = 5,\ \Delta y_2^{10} = 5$	2^{-4}
	$\Delta z_0^{10} = 5,\ \Delta z_8^{10} = 5$	

入力を常に許容値とするため，4 段目以降の差分確率が大きくなることなどを考慮して選択した．この差分経路の入力差分は

$$\Delta G = \texttt{0x0000 0005 0000 0005}$$

である．この差分経路には 20 個の活性 S-box が含まれ，これらで差分の伝搬が確率的となる．この差分経路全体の差分確率は 2^{-46} である．入力差分と出力差分が等しいため，f_{U} と f_{L} のフィードフォワードで差分がキャンセルされることにより衝突が得られる．

本攻撃では，f_{U} の 1 段目から 3 段目に存在する 6 個の活性 S-box S_0^1，S_8^1，S_0^2，S_2^2，S_0^3，S_{12}^3 と，f_{L} の 1 段目から 3 段目に存在する 6 個の活性 S-box $\hat{S}_0^1$，$\hat{S}_8^1$，$\hat{S}_0^2$，$\hat{S}_2^2$，$\hat{S}_0^3$，$\hat{S}_{12}^3$ の入力をそれぞれ差分経路の差分の許容値で固定することで，これらの S-box での差分の伝搬を確率 1 で行う．これにより，表 2 と図 3 に示された 10 段の差分経路の差分確率を 2^{-30} とすることができ，誕生日攻撃よりも効率の良い衝突攻撃が可能となる．

3. 2. 1　S_0^1，S_8^1 について

x_0^1，x_8^1 をそれぞれ入力差分 0x5，出力差分 0x1 に対する許容値 0x3，0x6 のどちらかで固定することで，

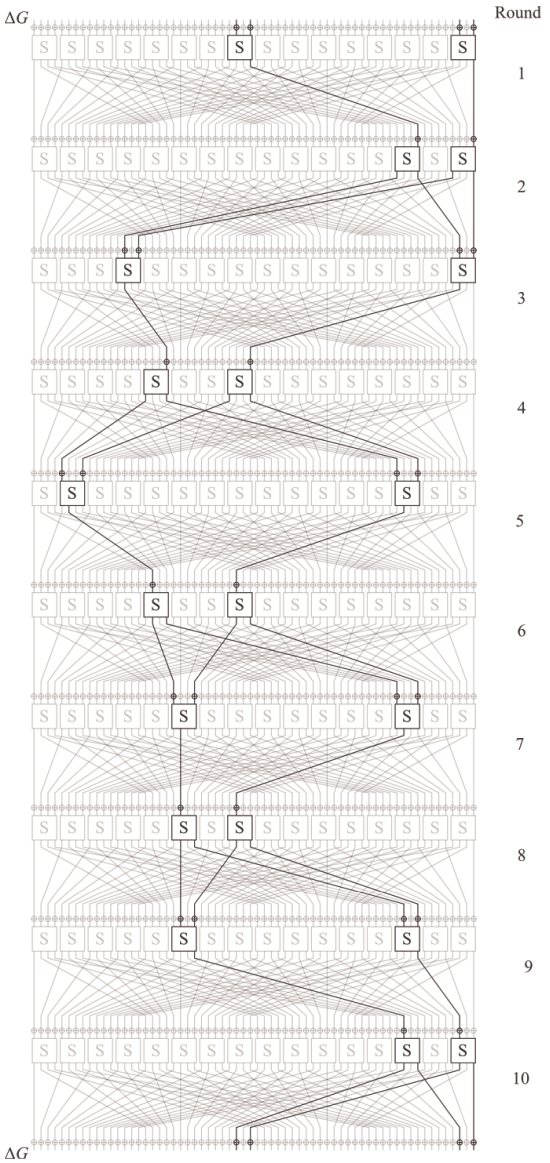

図 3　10 段の差分経路
Fig. 3　10-round differential path.

S_0^1，S_8^1 の入力を常に許容値にできる．

3. 2. 2　c の影響について

本攻撃では f_{U} で衝突が起こる (G, K) を見つけ，その (G, K) について f_{L} でも衝突が起こるかどうかを調べる．このとき，f_{U} の 1 段目から 3 段目に存在する 6 個の活性 S-box に常に許容値が入力されるよう攻撃を行う．このため f_{L} では，c の影響により，1 段目から 3 段目の活性 S-box に許容値が入力されるのが確

率的になる可能性があるが，本攻撃ではこれらの活性 S-box にも常に許容値が入力されるよう攻撃を行うため，攻撃が適用可能な c の値が制限される．以下では，本攻撃が適用可能であるための c に関する十分条件について考察する．

ここでは $E_K(G)$ と $E_K(G \oplus c)$ の内部状態の XOR 差分を考える．c を 4 ビットごとに，$c = c_{15} \| c_{14} \| \cdots \| c_0$ と表記する．1 段目の S-box について，$x_i^1 \oplus \hat{x}_i^1 = c_i$ $(i \in \{0, \ldots, 15\})$ である．

(i) S_i^1，c_i $(i \in \{1, \ldots, 7, 9, \ldots, 15\})$ について

2 段目と 3 段目の活性 S-box $\hat{S}_0^2$，$\hat{S}_2^2$，$\hat{S}_0^3$，$\hat{S}_{12}^3$ の入力は，1 段目の全ての S-box の出力の最下位ビットにのみ依存している．したがって，c によりこれらの値が変化しなければ，$\hat{S}_0^2$，$\hat{S}_2^2$，$\hat{S}_0^3$，$\hat{S}_{12}^3$ には常に許容値が入力される．

PRESENT の S-box の差分特性より，0x1 と 0x8 以外の全ての入力差分には，最下位ビットが 0 となる出力差分が存在する．したがって，$c_i \neq$ 0x1 かつ $c_i \neq$ 0x8 のとき，$\hat{S}_0^2$，$\hat{S}_2^2$，$\hat{S}_0^3$，$\hat{S}_{12}^3$ に常に許容値を入力することができ，本攻撃が適用可能となる．

(ii) S_i^1，c_i $(i \in \{0, 8\})$ について

1 段目の活性 S-box $\hat{S}_0^1$，$\hat{S}_8^1$ にも常に許容値が入力されるよう攻撃を行う．

$$\hat{x}_0^1 = x_0^1 \oplus c_0 \ , \quad \hat{x}_8^1 = x_8^1 \oplus c_8$$

より，活性 S-box S_0^1，S_8^1，$\hat{S}_0^1$，$\hat{S}_8^1$ の入力 x_0^1，x_8^1，$\hat{x}_0^1$，$\hat{x}_8^1$ が全て許容値（0x3 または 0x6）であるためには，c_0，c_8 の値は 0x0 または 0x5 でなければならない．更に，$\hat{S}_0^3$，$\hat{S}_{12}^3$ の入力は，$\hat{S}_0^2$，$\hat{S}_2^2$ を介して，$\hat{S}_0^1$，$\hat{S}_8^1$ の両方の出力に依存している．このため，ΔG による $\hat{S}_0^1$，$\hat{S}_8^1$ の入力差分が 0x5 であることから，$c_0 = c_8$ とすれば，S_0^3，S_{12}^3 と同様に $\hat{S}_0^3$，$\hat{S}_{12}^3$ にも許容値を入力できる．

以上 (i)，(ii) の二つの場合をまとめると，本攻撃が適用可能であるための $c = c_{15} \| c_{14} \| \cdots \| c_0$ に関する十分条件は以下のとおりである．

- $c_0 = c_8 =$ 0x0 または $c_0 = c_8 =$ 0x5.
- c_0，c_8 以外の全ての c_i について，$c_i \neq$ 0x1 かつ $c_i \neq$ 0x8.

この条件を満たす c の値の個数は $14^{14} \times 2 - 1 \simeq 2^{54.3}$ であり，これは c の値の総数 $(2^{64} - 1)$ のおよそ 0.12%である．

3.2.3 S_0^2，S_2^2，S_0^3，S_{12}^3 について

ここまでで $x_1^1, \ldots, x_{15}^1$ のうち，値を決めていなかったものに値をランダムに割り当て，1 段目の sBoxlayer と pLayer を計算し，2 段目の addRoundKey 変換の直前の状態 z^1 を求める．ここでラウンド鍵を用いて x_0^2，x_2^2 を常に許容値とすることで，活性 S-box S_0^2，S_2^2 での差分の伝搬を確率 1 で行う．x_0^2，x_2^2 が入力差分 0x1，出力差分 0x9 に対する許容値 0x0，0x1，0x4，0x5 のいずれかになるように k_0^2，k_2^2 を決める．

更に 3 段目の活性 S-box S_0^3，S_{12}^3 の入力 x_0^3，x_{12}^3 は，y_0^2，y_1^2，y_2^2，y_3^2 に依存しているため，ラウンド鍵によって x_0^3，x_{12}^3 を固定するためには，これらをあらかじめ求める必要がある．このために k_1^2，k_3^2 の値をランダムに決め，先に決めた k_0^2，k_2^2 を用いて，S_0^2，S_1^2，S_2^2，S_3^2 の出力 y_0^2，y_1^2，y_2^2，y_3^2 を求める．

ここまでで $k_0^2, \ldots, k_3^2$ の値が決まったため，κ^2[16..31] の値が決まる．鍵更新を考えると κ^3[0..12]，κ^3[77..79] の値が決まったことになる．

$x_0^2, \ldots, x_3^2$ について sBoxlayer と pLayer を計算し，z_0^2，z_{12}^2 を求める．3 段目の活性 S-box S_0^3，S_{12}^3 でも 2 段目と同様に，x_0^3，x_{12}^3 が，入力差分 0x5，出力差分 0x4 に対する許容値 0x8，0xd になるよう k_0^3，k_{12}^3 を決める．これにより κ^3[16..19]，κ^3[64..67] の値が決まる．

ここまでで値が決まっていなかった κ^3[13..15]，κ^3[20..63]，κ^3[68..76] の 56 ビットの値をランダムに決める．この時点で，鍵レジスタと，メッセージ撹拌部の状態が一意に定まるため，(G, K) と暗号文を計算することができる．

この (G, K) について f_{U} で衝突が起こるかを確認する．更に f_{U} で衝突が起こるとき，その (G, K) について f_{L} でも衝突が起こるかを確認する．f_{U} と f_{L} の両方で衝突が起これば，それは圧縮関数の衝突である．

この攻撃では，値をランダムに割り当てた鍵レジスタの 64 ビットが攻撃の自由度となる．

攻撃の手順を以下にまとめる．

（1） S_0^1，S_8^1 の入力を許容値で固定する．

（2） c の値に応じて，x_i^1 の値を固定する．

（3） S_0^2，S_2^2，S_0^3，S_{12}^3 の入力をラウンド鍵を用いて固定する．

（4） κ^3[13..15]，κ^3[20..63]，κ^3[68..76] に値をランダムに割り当てる．

（5） (G, K) を求め，この (G, K) について f_{U} で衝突が起こるかを確認する．衝突していなければ Step 1 に戻る．

（6） Step 5 までで求めた (G, K) について f_{L} で

も衝突が起こるかを確認する．衝突していなければ Step 1 に戻る．

3.3 計 算 量

本攻撃では，差分確率が 2^{-46} の差分経路に存在する 20 個の活性 S-box のうち，f_{U} と f_{L} のそれぞれ 1 段目から 3 段目に存在する 6 個の活性 S-box への入力が常に許容値となるように攻撃を行う．したがって，f_{U} で衝突が見つかる確率と，f_{L} で衝突が見つかる確率は共に，$2^{-46+16} = 2^{-30}$ となる．

ここで攻撃の計算量の 1 単位を 1 回の圧縮関数呼出しとする．Step 1 から Step 5 の 1 回の実行では，$f_{\mathrm{U}}(G, K)$ と $f_{\mathrm{U}}(G \oplus \Delta G, K)$ を計算するので，1 回の圧縮関数呼出しの計算量に相当する．同様に，Step 6 の 1 回の実行も 1 回の圧縮関数呼出しの計算量に相当する．したがって，攻撃計算量は $2^{60} + 2^{30} \simeq 2^{60}$ と見積もられる．

なお，Step 1 から Step 5 の 1 回の実行では，$f_{\mathrm{U}}(G, K)$ のみを計算して各活性 S-box に許容値が入力されているかどうかを確認することにより，$f_{\mathrm{U}}(G \oplus \Delta G, K)$ を計算することなく衝突を得ることも可能である．更に，この場合，活性 S-box に許容値が入力されないことが分かった時点で計算を打ち切ることにより，更に計算量を削減することも可能である．このような手法は Step 6 にも適用できる．

4. 8 段の H-PRESENT に対する衝突攻撃

計算機実験を行うために，8 段の PRESENT を用いた H-PRESENT に対する衝突攻撃を検討する．

4.1 概 要

攻撃に用いた 8 段の PRESENT の差分経路を表 3 と図 4 に示す．これは，入力差分と出力差分が等しくかつ各段の活性 S-box の個数が 2 以下（ただし 1 段目については 2）となる 8 段の差分経路のうち，差分確率が最大の差分経路である．また，後述のように 1 段目から 3 段目までの活性 S-box の入力を常に許容値とするため，4 段目以降の差分確率が大きくなることなどを考慮して選択した．この差分経路の入力差分と出力差分は

$$\Delta G = \texttt{0x0500 0000 0000 0500}$$

であり，全体の差分確率は 2^{-36} である．今回，

$$c = \texttt{0x0030 0000 0000 0000}$$

として攻撃を行った．このとき $c_{13} = x^1_{13} \oplus \hat{x}^1_{13} = \texttt{0x3}$ となる．この経路でも，1 段目の全ての S-box の最下位ビットが 2 段目から 3 段目に存在する 4 個の活性 S-box $\hat{S}^2_0$，$\hat{S}^2_3$，$\hat{S}^3_0$，$\hat{S}^3_8$ の入力に影響を与えるため，$y^1_{13} \oplus \hat{y}^1_{13}$ に最下位ビットが 0 である値 0x4 を選ぶ．$x^1_{13} = \texttt{0x4}$ のとき，$y^1_{13} \oplus \hat{y}^1_{13} = \texttt{0x4}$ となる．

攻撃の手順を以下に示す．

（i） S^1_2，S^1_{14}，S^2_0，S^2_3，S^3_0，S^3_8 の入力を許容値で，x^1_{13} を 0x4 で固定し，f_{U} で衝突を見つける．

（ii） Step i で見つけた (G, K) について f_{L} で衝突が起こるかを確認する．衝突していなければ Step i に戻る．

この攻撃では f_{U} と f_{L} のそれぞれで，1 段目から 3 段目に存在する 6 個の活性 S-box の入力を許容値で固定するため，衝突が起こる確率は共に $2^{-36+14} = 2^{-22}$ となる．したがって圧縮関数の衝突を見つけるために必要な計算量を 2^{44} と見積もることができる．

表 3 8 段の差分経路とその確率
Table 3 8-round differential path and its probabilities.

段	差分	確率
1	$\Delta x^1_2 = 5,\ \Delta x^1_{14} = 5$	
	$\Delta y^1_2 = 1,\ \Delta y^1_{14} = 1$	2^{-6}
2	$\Delta x^2_0 = 4,\ \Delta x^2_3 = 4$	
	$\Delta y^2_0 = 5,\ \Delta y^2_3 = 5$	2^{-4}
3	$\Delta x^3_0 = 9,\ \Delta x^3_8 = 9$	
	$\Delta y^3_0 = 4,\ \Delta y^3_8 = 4$	2^{-4}
4	$\Delta x^4_8 = 1,\ \Delta x^4_{10} = 1$	
	$\Delta y^4_8 = 9,\ \Delta y^4_{10} = 9$	2^{-4}
5	$\Delta x^5_2 = 5,\ \Delta x^5_{14} = 5$	
	$\Delta y^5_2 = 1,\ \Delta y^5_{14} = 1$	2^{-6}
6	$\Delta x^6_0 = 4,\ \Delta x^6_3 = 4$	
	$\Delta y^6_0 = 5,\ \Delta y^6_3 = 5$	2^{-4}
7	$\Delta x^7_0 = 9,\ \Delta x^7_8 = 9$	
	$\Delta y^7_0 = 4,\ \Delta y^7_8 = 4$	2^{-4}
8	$\Delta x^8_8 = 1,\ \Delta x^8_{10} = 1$	
	$\Delta y^8_8 = 9,\ \Delta y^8_{10} = 9$	2^{-4}
	$\Delta z^{10}_2 = 5,\ \Delta z^{10}_{14} = 5$	

4.2 実 験 結 果

計算機実験において，圧縮関数の衝突を 1 組見つけるのに要した計算量の平均は，およそ $2^{33.71}$ であった．これは計算量の見積り 2^{44} と明らかに異なっている．

計算機実験において，f_{U} で衝突を見つけるために Step i を実行した回数の平均は，$2^{21.34}$ であった．これは，3 段目の pLayer 後の差分 Δz^3 から最後の差分 ΔG に至る差分経路が，この差分経路以外にも存在す

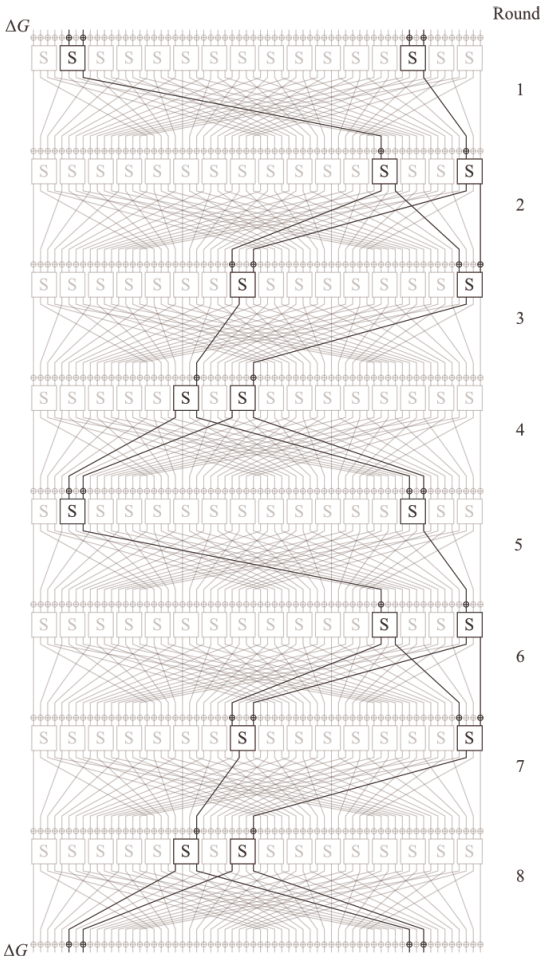

図 4　8 段の差分経路
Fig. 4　8-round differential path.

るからである．我々は，表 3 の差分経路以外にも，差分確率が 2^{-38}，2^{-40}，2^{-43}，2^{-45} である経路をそれぞれ 2 個，1 個，1 個，1 個見つけた．これらの経路のうち，差分がどの経路を通過しても f_{U} で衝突が起こるため，これらの差分経路の確率の合計 $2^{-35.35}$ が，全体の確率となる．したがって，f_{U} で衝突を 1 組見つけるために必要な Step i の実行回数は $2^{35.35-14} = 2^{21.35}$ と見積もることができ，この値は実験値とほぼ一致する．

ここでは簡単のため，f_{U} において差分が表 3 の差分経路を通り，衝突が起こる場合だけを考える．その確率は $2^{-36+14} = 2^{-22}$ と見積もることができる．一方，計算機実験では，表 3 の差分経路を通り衝突が起こる確率は，$2^{-22.01}$ であった．この理論値は実験値とほぼ一致する．

表 4　許容値が入力される確率の見積りと実験結果
Table 4　Estimated and measured probabilities that admissible inputs are given.

活性 S-box	見積り	実験値
$\hat{S}_8^4$	2^{-2}	1
$\hat{S}_{10}^4$	2^{-2}	1
$\hat{S}_2^5$	2^{-3}	$2^{-1.26}$
$\hat{S}_{14}^5$	2^{-3}	$2^{-0.39}$
$\hat{S}_0^6$	2^{-2}	$2^{-1.56}$
$\hat{S}_3^6$	2^{-2}	$2^{-1.55}$
$\hat{S}_0^7$	2^{-2}	$2^{-1.99}$
$\hat{S}_8^7$	2^{-2}	$2^{-2.00}$
$\hat{S}_8^8$	2^{-2}	$2^{-2.02}$
$\hat{S}_{10}^8$	2^{-2}	$2^{-1.98}$

計算機実験において，表 3 の差分経路を通り f_{U} で衝突が起こったときの (G, K) について f_{L} で衝突が起こる確率は $2^{-12.70}$ であり，これは理論値の 2^{-22} と大きく異なっている．このときの f_{L} の 4 段目から 8 段目に存在する 10 個の活性 S-box に許容値が入力された確率の実験値を表 4 に示す．

4.3 考　　察

f_{U} と f_{L} のどちらでも 1 段目から 3 段目までに存在する活性 S-box には常に許容値が入力されるように攻撃を行ったため，これらの活性 S-box で差分が伝搬する確率は 1 である．表 4 に示した実験結果より，4 段目から 6 段目の活性 S-box $\hat{S}_8^4$，$\hat{S}_{10}^4$，$\hat{S}_2^5$，$\hat{S}_{14}^5$，$\hat{S}_0^6$，$\hat{S}_3^6$ で，許容値が入力される確率の見積りと実験値が異なっている．最初の見積りでは，各活性 S-box の入力がランダムであると仮定して確率の計算を行っている．しかし，f_{L} ではこれらの活性 S-box の入力に偏りが生じていると考えられる．

f_{U} で衝突が起こるとき，f_{U} の全ての活性 S-box には許容値が入力されている．この攻撃では f_{U} で衝突が起こる (G, K) を見つけ，その (G, K) について f_{L} で衝突が起こるかを確認する．このとき，c の影響で f_{L} の各活性 S-box への入力が f_{U} のときとは異なってくるが，c の影響の広がりが遅く，初期の段の S-box では許容値が入力されやすくなっていると考えられる．そこで c が各活性 S-box の入力に与える影響について考える．

4.3.1　$\hat{S}_8^4$，$\hat{S}_{10}^4$，$\hat{S}_2^5$，$\hat{S}_{14}^5$ について

以下では，c によって生じる f_{U} と f_{L} の内部状態の XOR 差分を ∇ で表す．

$c_{13} = 0\mathrm{x}3$ より，$\hat{S}_{13}^1$ について $\nabla x_{13}^1 = 0\mathrm{x}3$ である．

これに対する出力の差分が $\nabla y^1_{13} = 0\text{x}4$ となるように攻撃を行ったため，次の段の $\hat{S}^2_{11}$ の入力について常に $\nabla x^2_{11} = 0\text{x}2$ となる．$\hat{x}^2_{11}$ がランダムに決まるとき，∇y^2_{11} はそれぞれ 1/8 の確率で 0x3，0x6，0xa，0xc，0xd，0xe となり，1/4 の確率で 0x5 となる．$\hat{y}^2_{11}$ は 3 段目の $\hat{S}^3_2$，$\hat{S}^3_6$，$\hat{S}^3_{10}$，$\hat{S}^3_{14}$ の入力 $\hat{x}^3_2[3]$，$\hat{x}^3_6[3]$，$\hat{x}^3_{10}[3]$，$\hat{x}^3_{14}[3]$ に対応する．すなわち，∇y^2_{11} の値により $\nabla\hat{x}^3_2[3]$，$\nabla\hat{x}^3_6[3]$，$\nabla\hat{x}^3_{10}[3]$，$\nabla\hat{x}^3_{14}[3]$ のうち 2 個ないし 3 個が 1 となる．

次に 4 段目の $\hat{S}^4_8$，$\hat{S}^4_9$，$\hat{S}^4_{10}$，$\hat{S}^4_{11}$ に対する影響を考える．これらの入力はそれぞれ，$\hat{S}^3_2$，$\hat{S}^3_6$，$\hat{S}^3_{10}$，$\hat{S}^3_{14}$ の出力 $\hat{y}^3_2[2]$，$\hat{y}^3_6[2]$，$\hat{y}^3_{10}[2]$，$\hat{y}^3_{14}[2]$ に依存している．

ここで $\hat{S}^4_8$，$\hat{S}^4_{10}$ の入力 $\hat{x}^4_8$，$\hat{x}^4_{10}$ は，

$$\hat{x}^4_8 = (\hat{y}^3_3[2]\|\hat{y}^3_2[2]\|\hat{y}^3_1[2]\|\hat{y}^3_0[2]) \oplus \hat{k}^4_8 \ ,$$
$$\hat{x}^4_{10} = (\hat{y}^3_{11}[2]\|\hat{y}^3_{10}[2]\|\hat{y}^3_9[2]\|\hat{y}^3_8[2]) \oplus \hat{k}^4_{10}$$

である．x^4_8，x^4_{10} の値は常に許容値 (0x0，0x1，0x4，0x5) であるため，$\nabla y^3_2[2] = 1$，$\nabla y^3_{10}[2] = 1$ であっても，$\hat{x}^4_8$，$\hat{x}^4_{10}$ は許容値 (0x0，0x1，0x4，0x5) となる．したがって，$\hat{S}^4_8$，$\hat{S}^4_{10}$ で ΔG による差分が伝搬する確率は 1 となり，表 4 の実験値と一致する．

S-box の差分特性より，入力差分が 0x8 のとき，入力がランダムに決まるならば，出力差分の下位から 2 番目（最下位ビットは 0 番目）のビットが 1 になる確率は 1/2 である．すなわち，c による差分で $\hat{S}^3_2$，$\hat{S}^3_6$，$\hat{S}^3_{10}$，$\hat{S}^3_{14}$ が活性となるとき，それぞれ 1/2 の確率で，$\hat{S}^4_8$，$\hat{S}^4_9$，$\hat{S}^4_{10}$，$\hat{S}^4_{11}$ が活性となり，そのときの入力差分は 0x4 である．

次に，$\hat{S}^5_2$，$\hat{S}^5_{14}$ の入力は $\hat{S}^4_8$，$\hat{S}^4_9$, $\hat{S}^4_{10}$，$\hat{S}^4_{11}$ の出力に依存し，

$$\hat{x}^5_2 = (\hat{y}^4_{11}[0]\|\hat{y}^4_{10}[0]\|\hat{y}^4_9[0]\|\hat{y}^4_8[0]) \oplus \hat{k}^5_2 \ ,$$
$$\hat{x}^5_{14} = (\hat{y}^4_{11}[3]\|\hat{y}^4_{10}[3]\|\hat{y}^4_9[3]\|\hat{y}^4_8[3]) \oplus \hat{k}^5_{14}$$

である．

$\hat{S}^4_8$，$\hat{S}^4_{10}$ には先ほど示したとおり，常に差分経路の許容値 (0x0，0x1，0x4，0x5) のいずれかが入力されている．S-box の差分特性として，入力差分が 0x4 のとき，0x0，0x1，0x4，0x5 が入力されると，出力差分は 0x5 になる．すなわち，$\hat{S}^4_8$，$\hat{S}^4_{10}$ が c による差分で活性となるときは常に，$\hat{S}^5_2$ について $\nabla x^5_2[0] = 1$ となり，$\hat{S}^5_{14}$ について $\nabla x^5_{14}[0] = 0$ となる．

$\hat{S}^4_9$，$\hat{S}^4_{11}$ について，S-box の差分特性より，入力差分 0x4 のとき，入力がランダムに決まるならば，出力差分の最上位ビットが 1 になる確率と，最下位ビットが 1 になる確率は共に 1/2 である．

表 5　$\hat{S}^5_2$，$\hat{S}^5_{14}$ に許容値が入力される確率
Table 5　Probabilities that admissible inputs are given to $\hat{S}^5_2$ and $\hat{S}^5_{14}$.

$\hat{S}^2_{11}$の出力差分 ∇y^2_{11}	許容値（0x3 または 0x6）が入力される確率	
	$\hat{S}^5_2$	$\hat{S}^5_{14}$
3	$\frac{1}{8} \times (\frac{1}{2} \times \frac{3}{4})$	$\frac{1}{8} \times \frac{3}{4}$
5	$\frac{1}{4} \times (\frac{1}{2} \times \frac{1}{2} + \frac{1}{2} \times \frac{1}{2})$	$\frac{1}{4} \times 1$
6	$\frac{1}{8} \times (\frac{1}{2} \times \frac{3}{4})$	$\frac{1}{8} \times \frac{3}{4}$
a	$\frac{1}{8} \times (\frac{3}{4} \times \frac{3}{4})$	$\frac{1}{8} \times (\frac{3}{4} \times \frac{3}{4})$
c	$\frac{1}{8} \times (\frac{3}{4} \times \frac{1}{2})$	$\frac{1}{8} \times \frac{3}{4}$
d	$\frac{1}{8} \times (\frac{3}{4} \times \frac{1}{2} \times \frac{1}{2} + \frac{3}{4} \times \frac{1}{2} \times \frac{1}{2})$	$\frac{1}{8} \times \frac{3}{4}$
e	$\frac{1}{8} \times (\frac{3}{4} \times \frac{1}{2} \times \frac{3}{4})$	$\frac{1}{8} \times (\frac{3}{4} \times \frac{3}{4})$
合計	$2^{-1.26}$	$2^{-0.39}$

$\hat{S}^5_2$，$\hat{S}^5_{14}$ への入力が許容値 (0x3，0x6) となるのは，c による入力の差分が 0x0 または 0x5 の場合である．この確率を表 5 にまとめる．この表より，$\hat{S}^5_2$ に許容値が入力される確率は $2^{-1.26}$，$\hat{S}^5_{14}$ に許容値が入力される確率は $2^{-0.39}$ となり，表 4 の実験値と一致する．ただし，この表の確率は各 S-box の入力がランダムかつ独立に選択されることを仮定して計算されており，PRESENT の構造を考えるとこの仮定は適切ではない．一方で，$\hat{S}^3_2$，$\hat{S}^3_6$，$\hat{S}^3_{10}$，$\hat{S}^3_{14}$ はすべて 2 段目の同じ 4 個の S-box から入力を得ているものの，ここでは $\hat{S}^3_2$，$\hat{S}^3_6$，$\hat{S}^3_{10}$，$\hat{S}^3_{14}$ それぞれの出力の下位から 2 番目のビットにのみ着目している．更に，$\hat{S}^4_8$，$\hat{S}^4_9$，$\hat{S}^4_{10}$，$\hat{S}^4_{11}$ のそれぞれが入力を得ている 3 段目の 4 個の S-box の集合は互いに素である．これらを考慮すると，各 S-box の入力がランダムかつ独立に選択されるという仮定は幾らかの妥当性を有していると考えられる．

表 5 に示された確率の計算の例を以下に二つ示す．他の場合についても同様に計算できる．

まず，$\nabla y^2_{11} = 0\text{x}5$ かつ $\hat{S}^5_2$ に許容値が入力される確率を考える．$\nabla y^2_{11} = 0\text{x}5$ のとき，c の差分による 3 段目の活性 S-box は $\hat{S}^3_{10}$ と $\hat{S}^3_2$ であり，活性となり得る 4 段目の S-box は $\hat{S}^4_{10}$ と $\hat{S}^4_8$ である．$\hat{S}^5_2$ への入力が許容値となるのは，∇x^5_2 が 0x0 または 0x5 の場合，すなわち，$\nabla y^4_{10}[0]$，$\nabla y^4_8[0]$ がともに 0 または共に 1 の場合である．$\nabla y^4_8[0] = 0$ となるのは，$\nabla y^3_2[2] = 0$ または，$\nabla y^3_2[2] = 1$ かつ $\nabla y^4_8[0] = 0$ のときである．一方，$\nabla y^3_2[2] = 1$ ならば $\nabla y^4_8[0] = 1$ なので

$$\Pr[\nabla y^4_8[0] = 0] = \Pr[\nabla y^3_2[2] = 0] = \frac{1}{2}$$

である．同様に $\Pr[\nabla y_{10}^4[0]=0]=1/2$ である．したがって，$\nabla y_{11}^2=$ 0x5 かつ $\hat{S}_2^5$ に許容値が入力される確率は

$$\begin{aligned}&\Pr[\nabla y_{11}^2=\text{0x5}]\left(\Pr[\nabla y_{10}^4[0]=\nabla y_8^4[0]=0]\right.\\&\qquad\left.+\Pr[\nabla y_{10}^4[0]=\nabla y_8^4[0]=1]\right)\\&=\frac{1}{4}\times\left(\frac{1}{2}\times\frac{1}{2}+\frac{1}{2}\times\frac{1}{2}\right)\end{aligned}$$

となる．

次に，$\nabla y_{11}^2=$ 0xd かつ $\hat{S}_2^5$ に許容値が入力される確率を考える．$\nabla y_{11}^2=$ 0xd のとき，3 段目の活性 S-box は $\hat{S}_{14}^3$，$\hat{S}_{10}^3$，$\hat{S}_2^3$ であり，活性となり得る 4 段目の S-box は $\hat{S}_{11}^4$，$\hat{S}_{10}^4$，$\hat{S}_8^4$ である．$\hat{S}_2^5$ への入力が許容値となるのは，∇x_2^5 が 0x0 または 0x5 の場合，すなわち，$\nabla y_{11}^4[0]=0$ かつ $\nabla y_{10}^4[0]=\nabla y_8^4[0]$ の場合である．$\nabla y_{11}^4[0]=0$ となるのは，$\nabla y_{14}^3[2]=0$ または $\nabla y_{14}^3[2]=1$ かつ $\nabla y_{11}^4[0]=0$ のときであり，

$$\begin{aligned}&\Pr[\nabla y_{11}^4[0]=0]\\&\quad=\Pr[\nabla y_{14}^3[2]=0]\\&\qquad+\Pr[\nabla y_{14}^3[2]=1]\Pr[\nabla y_{11}^4[0]=0]\\&\quad=\frac{1}{2}+\frac{1}{2}\times\frac{1}{2}=\frac{3}{4}\end{aligned}$$

である．したがって，$\nabla y_{11}^2=$ 0xd かつ $\hat{S}_2^5$ に許容値が入力される確率は

$$\begin{aligned}&\Pr[\nabla y_{11}^2=\text{0xd}]\\&\quad\left(\Pr[\nabla y_{11}^4[0]=0]\Pr[\nabla y_{10}^4[0]=\nabla y_8^4[0]=0]\right.\\&\quad\left.+\Pr[\nabla y_{11}^4[0]=0]\Pr[\nabla y_{10}^4[0]=\nabla y_8^4[0]=1]\right)\\&=\frac{1}{8}\times\left(\frac{3}{4}\times\frac{1}{2}\times\frac{1}{2}+\frac{3}{4}\times\frac{1}{2}\times\frac{1}{2}\right)\end{aligned}$$

となる．

以上のとおり，$\hat{S}_8^4$，$\hat{S}_{10}^4$，$\hat{S}_2^5$，$\hat{S}_{14}^5$ について，その入力に偏りが生じていることを確認した．10 段の PRESENT を用いた H-PRESENT に対する攻撃についても，実際の計算量と理論値との間に同様の差異が生じているものと考えられる．なお暗号化の処理が進むにつれて，c による差分の影響が広がり，活性 S-box に許容値が入力される確率は，活性 S-box の入力がランダムであると仮定して見積もる理論値に近づくと考えられる．

4.4 衝突の例

8 段の H-PRESENT の衝突の例を表 6 に示す．

表 6　衝突の例（ここで $\Delta H=\mathbf{0}$，$\Delta M=\mathbf{0}$）
Table 6　Example of collision.

G	e5ca bff5 4076 c36d
ΔG	0500 0000 0000 0500
c	0030 0000 0000 0000
H	4682 abff 5e37 30e9
M	f725
G'	2b55 a3c1 6117 815a
H'	a117 c5b6 317a 5f65

5. むすび

本論文では，10 段の H-PRESENT に対し，2^{60} の計算量で攻撃ができることを示した．また 8 段の H-PRESENT に対する衝突攻撃の計算機実験の結果を示し，攻撃の計算量の理論値と実験値の比較を行い，これらに生じる差異は活性 S-box の入力の偏りが原因であることを確認した．

謝辞　本論文に関して有益なコメントを下さった査読者の方々に感謝致します．本研究の一部は JSPS 科研費 21240001 の助成を受けています．

文　献

[1] M.R. Albrecht and C. Cid, “Algebraic techniques in differential cryptanalysis,” FSE 2009, LNCS, vol.5665, pp.193–208, Springer, 2009.

[2] 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 — Design and analysis,” SAC 2000, LNCS, vol.2012, pp.39–56, Springer, 2000.

[3] A. Biryukov and I. Nikolić, “Automatic search for related-key differential characteristics in byte-oriented block ciphers: Application to AES, Camellia, Khazad and others,” EUROCRYPT 2010, LNCS, vol.6110, pp.322–344, Springer, 2010.

[4] A. Bogdanov, L.R. Knudsen, G. Leander, C. Paar, A. Poschmann, M.J.B. Robshaw, Y. Seurin, and C. Vikkelsoe, “PRESENT: An ultra-lightweight block cipher,” CHES 2007, LNCS, vol.4727, pp.450–466, Springer-Verlag, 2007.

[5] A. Bogdanov, G. Leander, C. Paar, A. Poschmann, M.J.B. Robshaw, and Y. Seurin, “Hash functions and RFID tags: Mind the gap,” CHES 2008, LNCS, vol.5154, pp.283–299. Springer-Verlag, 2008.

[6] J.Y. Cho, “Linear cryptanalysis of reduced-round PRESENT,” CT-RSA 2010, LNCS, vol.5985, pp.302–317, Springer, 2010.

[7] S. Hirose, “Some plausible constructions of double-block-length hash functions,” FSE 2006, LNCS, vol.4047, pp.210–225, Springer, 2006.

[8] X. Lai and J.L. Massey, “A proposal for a new block encryption standard,” EUROCRYPT 1990, LNCS,

vol.473, pp.389–404, Springer, 1991.
[9] K. Ohkuma, “Weak keys of reduced-round PRESENT for linear cryptanalysis,” SAC 2009, LNCS, vol.5867, pp.249–265, Springer, 2009.
[10] M. Wang, “Differential cryptanalysis of reduced-round PRESENT,” AFRICACRYPT 2008, LNCS, vol.5023, pp.40–49, Springer, 2008.
[11] L. Wei, T. Peyrin, P. Sokolowski, S. Ling, J. Pieprzyk, and H. Wang, “On the (in)security of IDEA in various hashing modes,” FSE 2012, LNCS, vol.7549, pp.163–179, 2012.
[12] 小山卓麻，佐々木悠，國廣　昇，“DM-PRESENT の差分特性の考察,” 2013 年暗号と情報セキュリティシンポジウム，3B4-4, 2013.

（平成 24 年 10 月 31 日受付，25 年 3 月 4 日再受付）

小林　哲也　（正員）

2010 福井大・工・電気・電子卒．2012 同大大学院工学研究科電気・電子工学専攻博士前期課程了．在学中，暗号及び情報セキュリティに関する研究に従事．

廣瀬　勝一　（正員）

1988 京大・工・情報工学卒．1990 同大大学院工学研究科情報工学専攻修士課程了．1995 博士（工学）．1990 京大・工・助手．1998 京大院・情報学研究科・講師．2005 福井大・工・助教授．2009 福井大院・工学研究・教授，現在に至る．暗号及び情報セキュリティに関する研究に従事．