L-022

共通鍵ブロック暗号 HyRAL の不能差分攻撃について

Impossible Differential Attack on HyRAL

芝山 直喜* 五十嵐 保隆† 金子 敏信† 半谷 精一郎*
Naoki Shibayama Yasutaka Igarashi Toshinobu Kaneko Seiichiro Hangai

1 はじめに

多くのブロック暗号に対する攻撃法で最もよく知られており，かつ，強力なものに 1990 年に Biham らによって提案された差分攻撃 [7] と 1993 年に松井によって提案された線形攻撃 [8] がある．これらの攻撃法は，ブロック暗号に対する最も汎用的な攻撃法である．そのため，差分攻撃と線形攻撃に対する安全性を保証することは，ブロック暗号の設計において重要な課題である．しかしながら，他の攻撃法が適用できる可能性があるため，差分攻撃及び線形攻撃に対する安全性だけではブロック暗号に対する安全性が保証されるわけではない．

不能差分攻撃 [9] は，1998 年に Knudsen によって提案された差分攻撃から派生した攻撃法であり，成立確率が 0 である入力差分と出力差分のペア (以下，不能差分という．) を利用することで，間違った鍵の候補を棄却していく手法である．データ攪拌部の構造に依存した不能差分が用いられることが多く，特に一般化 Feistel 構造に対して脅威となる攻撃である．

2007 年に角尾らは変形 Feistel 構造のブロック暗号に対する不能差分特性探索法を提案した [5]．角尾らの手法は，Feistel 構造の暗号で F 関数が全単射であれば必ず 5 ラウンドの不能差分が存在することを基とし，変形 Feistel 構造へ拡張したものである．また，角尾らはこの手法を HIGHT へ適用し，HIGHT 提案者の自己評価結果である 14 ラウンドの不能差分よりも長い 15 ラウンドの不能差分があることを示した．

HyRAL は 2010 年に (株) ローレルインテリジェントシステムズの平田によって提案された一般化 Feistel 構造のブロック暗号である [1]．演算要素としてバイト単位の転置，換字処理及び XOR で構成されており，データブロック長は 128bit，秘密鍵長は 128，192 及び 256bit をサポートしている．これまでに，HyRAL は差分攻撃及び線形攻撃に対し，十分な耐性をもつと報告 [2][3] されているが，不能差分攻撃に対する耐性は未知である．

本稿では，角尾らによって提案された不能差分特性探索法を HyRAL へ適用し，HyRAL の不能差分特性探索を行うとともに，この結果を用いた不能差分攻撃に対する安全性を評価する．

* 東京理科大学工学研究科電気工学専攻,Department of Electrical Engineering, Faculty of Engineering, Tokyo University of Science.
† 東京理科大学理工学研究科電気工学専攻,Department of Electrical Engineering, Faculty of Science and Technology, Tokyo University of Science.

2 HyRAL の仕様

図 1 に (a)128bit HyRAL と (b)192/256bit HyRAL のデータ攪拌部を示す．HyRAL は G_1, G_2, F_1 及び F_2 の 4 つの関数から構成されている．$RK_1 \sim RK_9$ 並びに $IK_1 \sim IK_6$ は 128bit の副鍵を表し，$\oplus$ は XOR を表す．

図 2 に G_1, G_2 関数，図 3 に F_1, F_2 関数を示す．図 2(a) において，$X_j^{(1)}$ と $X_j^{(5)}$ $(1 \leq j \leq 4)$ は G_1 関数の

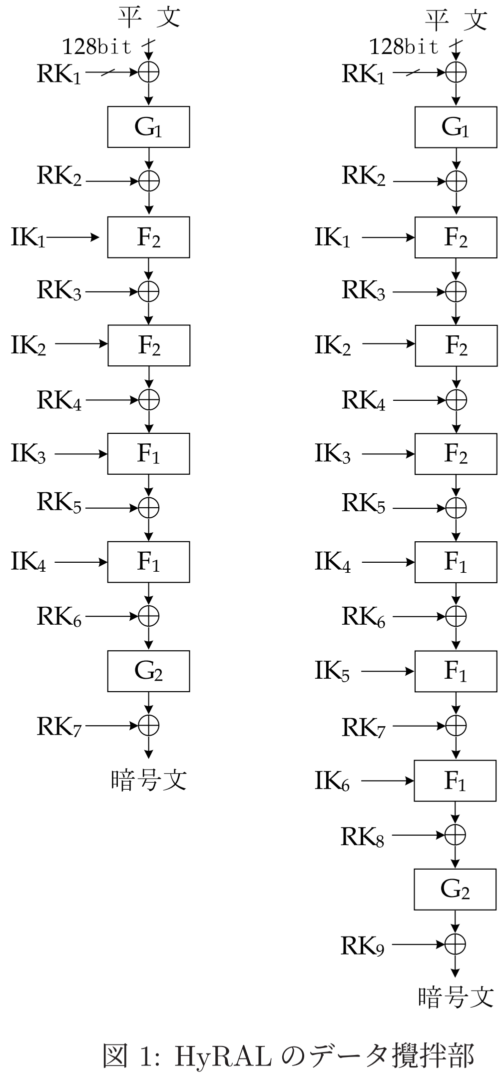
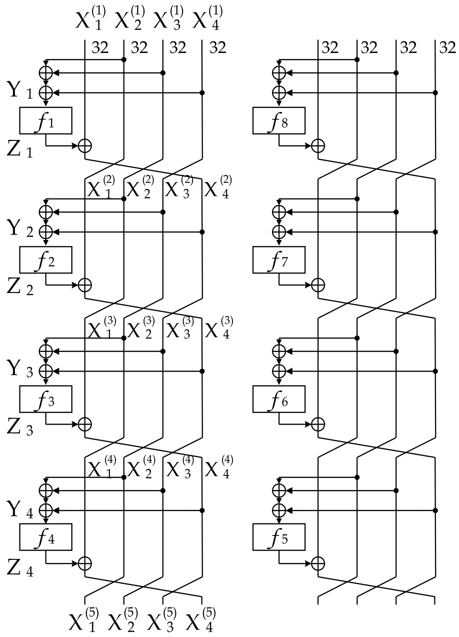
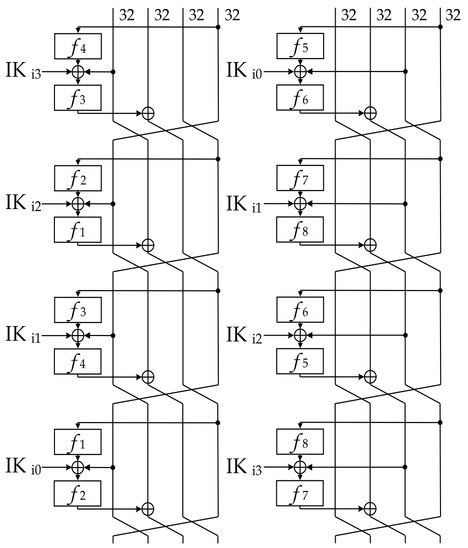


図 1: HyRAL のデータ攪拌部



(a) G１関数　　(b) G２関数

図 2: G_1, G_2 関数



(a) F１関数　　(b) F２関数

図 3: F_1, F_2 関数

入出力 32bit を表し，Y_i と Z_i は f_i 関数 $(1 \leq i \leq 4)$ の入出力 32bit を表す．図 3 における IK_{ij} は 32bit 副鍵を表し，次式で定義される．

$$IK_i = IK_{i0}||IK_{i1}||IK_{i2}||IK_{i3} \tag{1}$$

ここで，$||$ はデータの連結を表す．G_1, G_2, F_1 及び F_2 の 4 つの関数の構成要素はともに XOR と f_i 関数 $(1 \leq i \leq 8)$ である．

図 2(a) において，f_i 関数を含み，$(X_1^{(i)}, X_2^{(i)}, X_3^{(i)}, X_4^{(i)})$ から $(X_1^{(i+1)}, X_2^{(i+1)}, X_3^{(i+1)}, X_4^{(i+1)})$ に至る回路をラウンドと定義すると，G_1 関数は 4 ラウンドといえる．他の 3 つの関数も同様に定義すると，これらも 4 ラウンドといえる．これより，128bit HyRAL は 24 ラウンド，192/256bit HyRAL は 32 ラウンドといえる．

図 4 に f_i 関数を示す．入出力は 8bit×4 であり，構成要素は添字 i 依存のバイト転置，S 層，P 層及び定数加算 CST_j である ($\mathrm{CST}_0 = 0x11$, $\mathrm{CST}_1 = 0x22$, $\mathrm{CST}_2 = 0x44$, $\mathrm{CST}_3 = 0x88$)．S 層は 8bit 入出力の S-box からなる 4 並列回路であり，P 層は最小分岐数 5 の非巡回型 MDS 行列である．

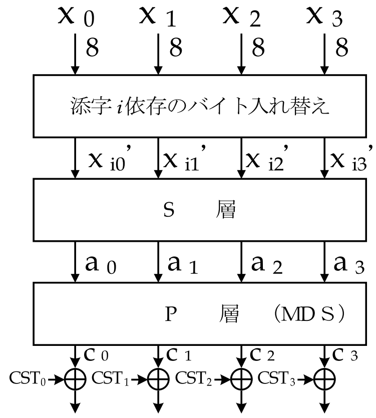


図 4: f_i 関数

添字 i 依存のバイト転置では $\boldsymbol{x} = (x_0||x_1||x_2||x_3)$ が入力されると，転置後のバイト列 $\boldsymbol{x}_i' = (x_{i0}'||x_{i1}'||x_{i2}'||x_{i3}')$ は次式で与えられる．

$$\begin{aligned}
\boldsymbol{x}_1' &= (x_0||x_1||x_2||x_3)\\
\boldsymbol{x}_2' &= (x_1||x_2||x_3||x_0)\\
\boldsymbol{x}_3' &= (x_2||x_3||x_0||x_1)\\
\boldsymbol{x}_4' &= (x_3||x_0||x_1||x_2)\\
\boldsymbol{x}_5' &= (x_3||x_2||x_1||x_0)\\
\boldsymbol{x}_6' &= (x_2||x_1||x_0||x_3)\\
\boldsymbol{x}_7' &= (x_1||x_0||x_3||x_2)\\
\boldsymbol{x}_8' &= (x_0||x_3||x_2||x_1)
\end{aligned} \tag{2}$$

3　不能差分特性探索法

ここでは，角尾らが提案した不能差分特性探索法 [5] を HyRAL に適用した探索法について説明する．差分要素，f_i 関数の入出力差分要素の関係，XOR による差分要素の変化及び不能差分を決定する差分要素の特性 (以下，不能差分特性という．) について述べ，不能差分特性の探索アルゴリズムについて示す．

3.1　差分要素，f_i 関数の入出力差分要素の関係及び XOR による差分要素の変化

暗号化処理において，k 系列 Feistel 構造の入力差分 α=(α_0, α_1, $\cdots$, α_{k-1}) が与えられたとき，α が持つ特性を $\boldsymbol{a}$=($\boldsymbol{a}_0$, $\boldsymbol{a}_1$, $\cdots$, $\boldsymbol{a}_{k-1}$) と表記する．また，入力差分 α が与えられたとき，r ラウンド後の出力差分を $\alpha^{(r)}$=($\alpha_0^{(r)}$, $\alpha_1^{(r)}$, $\cdots$, $\alpha_{k-1}^{(r)}$) とし，$\alpha^{(r)}$ が持つ特性を $\boldsymbol{a}^{(r)}$=($\boldsymbol{a}_0^{(r)}$, $\boldsymbol{a}_1^{(r)}$, $\cdots$, $\boldsymbol{a}_{k-1}^{(r)}$) と表記する．ここで，$\boldsymbol{a}_i$ と

$\boldsymbol{a}_i^{(r)}(0 \leq i \leq k-1)$ を差分要素といい，(3) 式及び (4) 式で定義する．

$$\boldsymbol{a}_i = \begin{cases} \mathbf{Z}ero & \text{if} \quad \alpha_i = 0 \quad : \text{差分 } 0 \\ \mathbf{F}ix & \text{otherwise} \quad : \text{非 } 0 \text{ の固定差分} \end{cases} \tag{3}$$

$$\boldsymbol{a}_i^{(r)} = \begin{cases} \mathbf{Z}ero & : \text{差分 } 0 \\ \mathbf{F}ix & : \text{非 } 0 \text{ の固定差分} \\ \mathbf{D}elta & : \text{非 } 0 \text{ の非固定差分 } (\mathbf{Z}ero \text{ を除く}) \\ \mathbf{R}andom & : \text{非固定差分 } (\mathbf{Z}ero \text{ を含む}) \end{cases} \tag{4}$$

以下，差分要素は Z，F，D，R のいずれかで表記するものとする．なお，復号処理の場合は α, α_i, $\alpha^{(r)}$, $\alpha_i^{(r)}$, $\boldsymbol{a}$, $\boldsymbol{a}_i$, $\boldsymbol{a}^{(r)}$, $\boldsymbol{a}_i^{(r)}$ の代わりに β, β_i, $\beta^{(r)}$, $\beta_i^{(r)}$, $\boldsymbol{b}$, $\boldsymbol{b}_i$, $\boldsymbol{b}^{(r)}$, $\boldsymbol{b}_i^{(r)}$ と表記する．

HyRAL の f_i 関数 $(1 \leq i \leq 8)$ はバイト転置部を除けばすべて同じ構造であり，S-box は全単射，かつ，MDS 行列は正則であるから，f_i 関数は全単射性[1]をもつ．また，f_i 関数が非線形な全単射関数であるとき，その入出力差分 Δx，$\Delta y = f_i(\Delta x)$ における差分要素の関係は表 1 で与えられる．例えば，f_i 関数への入力差分要素 Δx が F のとき，出力差分要素 Δy は D となることを表している．

表 1: f_i 関数 $(1 \leq i \leq 8)$ の入出力差分要素の関係

入力差分	出力差分
Z	Z
F	D
D	D
R	R

XOR による差分要素の変化を表 2 に示す．例えば，XOR 演算 $\Delta x \oplus \Delta y = \Delta z$ において，Δx の差分要素が Z で Δy の差分要素が D であるとき，Δz の差分要素は D となる．

表 2: XOR による差分要素の変化

	Z	F	D	R
Z	Z	F	D	R
F	F	Z	R	R
D	D	R	R	R
R	R	R	R	R

3.2 不能差分特性

不能差分特性は全単射型不能差分特性 (以下，全単射型という．) 及び中間不一致型不能差分特性 (以下，不一致型という．) の 2 つのタイプが存在する．以下に，不一致型及び全単射型について説明する．

全単射型

HyRAL の f_i 関数 $(1 \leq i \leq 8)$ の全単射性を利用した不能差分特性である．

例として，HyRAL の F_2 関数の 1 ラウンド目における全単射型について説明する．暗号化方向に計算された r_e ラウンド後の出力差分要素を $\boldsymbol{a}^{(r_e)}=(\boldsymbol{a}_0^{(r_e)}, \boldsymbol{a}_1^{(r_e)}, \boldsymbol{a}_2^{(r_e)}, \boldsymbol{a}_3^{(r_e)})$, 復号方向に計算された r_d ラウンド後の出力差分要素を $\boldsymbol{b}^{(r_d)}=(\boldsymbol{b}_0^{(r_d)}, \boldsymbol{b}_1^{(r_d)}, \boldsymbol{b}_2^{(r_d)}, \boldsymbol{b}_3^{(r_d)})$ としたとき，次の関係式が成り立つ．

$$\begin{cases} \boldsymbol{b}_0^{(r_d)} = \boldsymbol{a}_3^{(r_e)} & (5) \\ \boldsymbol{b}_1^{(r_d)} = \boldsymbol{a}_0^{(r_e)} & (6) \\ \boldsymbol{b}_2^{(r_d)} = \boldsymbol{a}_1^{(r_e)} \oplus f_6\left(f_5(\boldsymbol{a}_3^{(r_e)}) \oplus \boldsymbol{a}_2^{(r_e)}\right) & (7) \\ \boldsymbol{b}_3^{(r_d)} = \boldsymbol{a}_2^{(r_e)} & (8) \end{cases}$$

(5) 式及び (8) 式より (7) 式は次式で表される．

$$\boldsymbol{a}_1^{(r_e)} = \boldsymbol{b}_2^{(r_d)} \oplus f_6\left(f_5(\boldsymbol{b}_0^{(r_d)}) \oplus \boldsymbol{b}_3^{(r_d)}\right) \tag{9}$$

今，(7) 式及び (9) 式において，$\boldsymbol{a}_1^{(r_e)} = \boldsymbol{b}_2^{(r_d)} \in \{Z, F\}$ のとき，表 1 と表 2 より

$$f_6\left(f_5(a_3^{(r_e)}) \oplus a_2^{(r_e)}\right) = f_6\left(f_5(b_0^{(r_d)}) \oplus b_3^{(r_d)}\right) = \text{Z}, \tag{10}$$

となる．このとき，$f_5(a_3^{(r_e)}) \oplus a_2^{(r_e)} \in \{F, D\}$ または $f_5(b_0^{(r_d)}) \oplus b_3^{(r_d)} \in \{F, D\}$ であれば，(10) 式に矛盾する．このような，差分要素の矛盾を $(r_e + r_d + 1)$ ラウンドの全単射型という．

不一致型

暗号化方向に計算された r_e ラウンド後の出力差分要素 $\boldsymbol{a}^{(r_e)}=(\boldsymbol{a}_0^{(r_e)}, \boldsymbol{a}_1^{(r_e)}, \boldsymbol{a}_2^{(r_e)}, \boldsymbol{a}_3^{(r_e)})$ と復号方向に計算された r_d ラウンド後の出力差分要素 $\boldsymbol{b}^{(r_d)}=(\boldsymbol{b}_0^{(r_d)}, \boldsymbol{b}_1^{(r_d)}, \boldsymbol{b}_2^{(r_d)}, \boldsymbol{b}_3^{(r_d)})$ において，$(\boldsymbol{a}_i^{(r_e)}, \boldsymbol{b}_i^{(r_d)})(0 \leq i \leq 3)$ の差分要素組に 1 つでも矛盾が生じている場合，$(r_e + r_d)$ ラウンドの不一致型という．ここで，矛盾となる差分要素組は (Z, F)，(F, Z)，(Z, D) 及び (D, Z) である．

3.3 探索アルゴリズム

不能差分特性の探索アルゴリズムは次の 3 つのステップで実行される．

Step1：暗号化方向のすべての入力差分要素 $\boldsymbol{a}=(\boldsymbol{a}_0, \boldsymbol{a}_1, \boldsymbol{a}_2, \boldsymbol{a}_3) \in \{$ (Z, Z, Z, F), (Z, Z, F, Z) , $\cdots$, (F, F, F, F)$\}$ における差分要素の伝搬を表 1 と表 2 を用いて探索する．

Step2：復号方向のすべての入力差分要素 $\boldsymbol{b}=(\boldsymbol{b}_0, \boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3) \in \{$ (Z, Z, Z, F), (Z, Z, F, Z) , $\cdots$, (F, F, F, F)$\}$ における差分要素の伝搬を表 1 と表 2 を用いて探索する．

Step3：暗号化方向と復号方向のそれぞれの出力差分要素を比較し，全単射型または不一致型により矛盾が生じている差分要素の組み合わせを不能差分特性として検出する．

4 HyRAL の不能差分特性探索結果

128bit HyRAL において，$\boldsymbol{a}$=(F, F, F, Z)$\not\to$ $\boldsymbol{b}$=(Z, Z, F, Z) の 13(=7+5+1) ラウンドの全単射型，表 3 に示す $\boldsymbol{a} \not\to \boldsymbol{b}$ の 9(=5+4) ラウンドの不一致型が見つかった．13 ラウンドの全単射型の細部結果を図 5 に示す．このとき，8 ラウンド目において，図 6 に示すように，$\boldsymbol{b}^{(5)}$=(D, D,

[1] 入力差分が非 0 のとき，出力差分が非 0 となる．

表 3: 9 ラウンドの不能差分特性 (不一致型)

$\boldsymbol{a}$	$\boldsymbol{b}$
(Z,Z,F,F)	(Z,F,Z,Z)
(Z,F,Z,F)	(Z,F,Z,Z)
(Z,F,F,Z)	(Z,F,Z,Z)
(F,F,Z,F)	(Z,F,Z,Z)
(F,F,F,Z)	(Z,F,Z,Z)

F, Z) を用いると，f_7 関数または f_8 関数の入力差分要素は D となる．一方，◯ 印をつけた $\boldsymbol{a}_1^{(7)}=\boldsymbol{b}_2^{(5)}$=F に着目すると，$f_7$ 関数の出力差分要素は Z でなければならない．これは，f_7 関数または f_8 関数の入力差分要素が D であることに矛盾している．

次に，192/256bit HyRAL に対する実験結果として，$\boldsymbol{a}$=(F, F, F, Z)$\not\to$ $\boldsymbol{b}$ =(Z, F, Z, Z) の 12(=7+4+1) ラウンドの全単射型，表 3 に示した $\boldsymbol{a} \not\to \boldsymbol{b}$ の 9(=5+4) ラウンドの不一致型が見つかった．なお，12 ラウンドの全単射型は図 5 において，F_1 関数を除いた G_1 関数及び F_2 関数の部分からなる．

5 HyRAL の不能差分攻撃

ここでは，今回見つかった中で最もラウンド数が大きい 128bit HyRAL の 13 ラウンド，192/256bit HyRAL の 12 ラウンドの不能差分特性を用い，HyRAL に対する不能差分攻撃に必要な選択平文数及び計算量の見積もりを行う．

128bit HyRAL の 14 ラウンド鍵回復

前章より，13 ラウンドの不能差分特性は $\boldsymbol{a}$=(F, F, F, Z)$\not\to$ $\boldsymbol{b}$=(Z, Z, F, Z) であったので，14 ラウンド後の出力差分要素は (Z, D, Z, F) となる (図 7 参照)．i ラウンド後の出力差分を $\Delta C^{(i)}$=($\Delta C_0^{(i)}$, $\Delta C_1^{(i)}$, $\Delta C_2^{(i)}$, $\Delta C_3^{(i)}$) と表記したとき，差分が (α, α, α, 0) である平文組に対応した暗号文組の中から，($\Delta C_0^{(14)}$, $\Delta C_1^{(14)}$, $\Delta C_2^{(14)}$, $\Delta C_3^{(14)}$)=(0, β, 0, α) となる暗号文組を選ぶ．ただし，$\alpha \in \{0,1\}^{32}$ は非 0 の固定差分，$\beta \in \{0,1\}^{32}$ は非 0 の非固定差分である．α を定めたとき，$\Delta C_0^{(14)}$=0, $\Delta C_2^{(14)}$=0, $\Delta_3^{(14)}$=α となる確率はそれぞれ $\frac{1}{2^{32}}$ であり，$\Delta C_1^{(14)}$=β となる確率は $\frac{2^{32}-1}{2^{32}}$ である．したがって，($\Delta C_0^{(14)}$, $\Delta C_1^{(14)}$, $\Delta C_2^{(14)}$, $\Delta C_3^{(14)}$)=(0, β, 0, α) となる暗号文組が得られる確率は

$$\left(\frac{1}{2^{32}}\right)^3 \cdot \left(\frac{2^{32}-1}{2^{32}}\right) \simeq 2^{-96}, \qquad (11)$$

である．ここで，図 7 より，$\Delta C^{(13)}$ と $\Delta C^{(14)}$ の間には次の関係式が成り立つ．

$$\begin{cases} \Delta C_0^{(14)} = \Delta C_3^{(13)} & (12) \\ \Delta C_1^{(14)} = \Delta C_0^{(13)} \oplus f_1\left(f_2(\Delta C_2^{(13)}) \oplus \Delta C_3^{(13)} \oplus IK_{32}\right) & (13) \\ \Delta C_2^{(14)} = \Delta C_1^{(13)} & (14) \\ \Delta C_3^{(14)} = \Delta C_2^{(13)} & (15) \end{cases}$$

($\Delta C_0^{(14)}$, $\Delta C_1^{(14)}$, $\Delta C_2^{(14)}$, $\Delta C_3^{(14)}$)=(0, β, 0, α) となる暗号文組のうち，13 ラウンドの不能差分特性より，

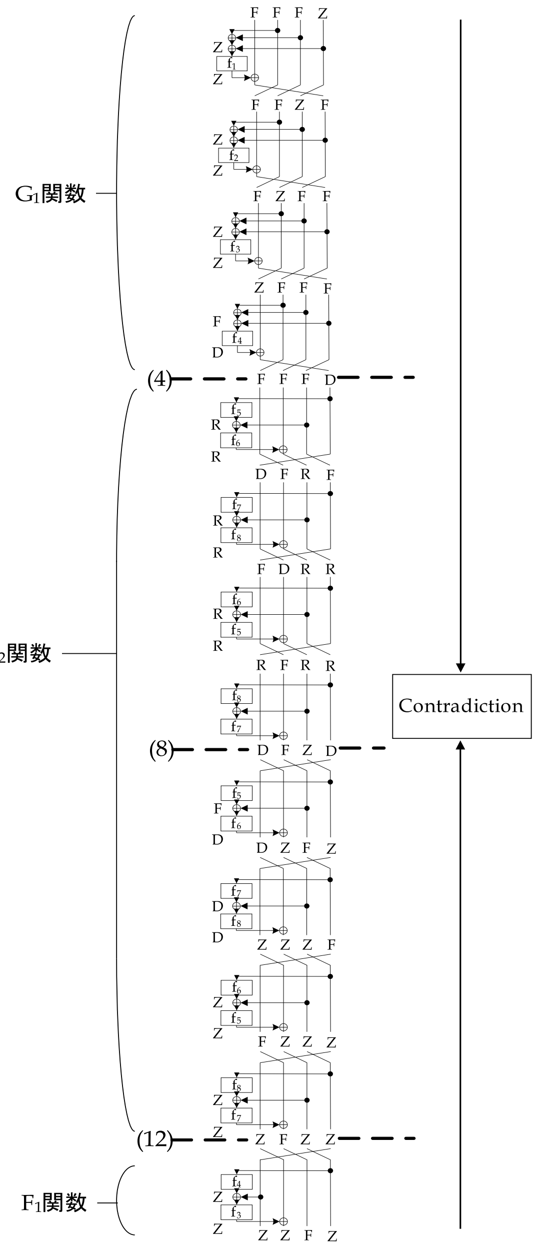


図 5: 128bit HyRAL の 13 ラウンドの不能差分特性

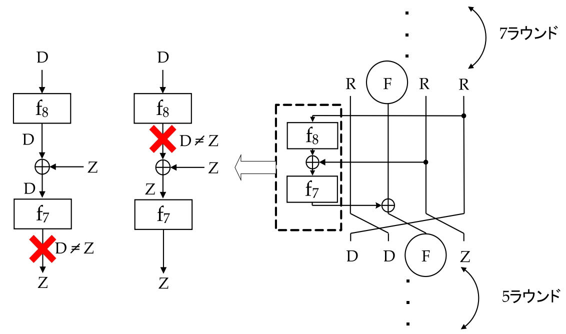


図 6: 128bit HyRAL の 8 ラウンド目で生じる差分要素の矛盾

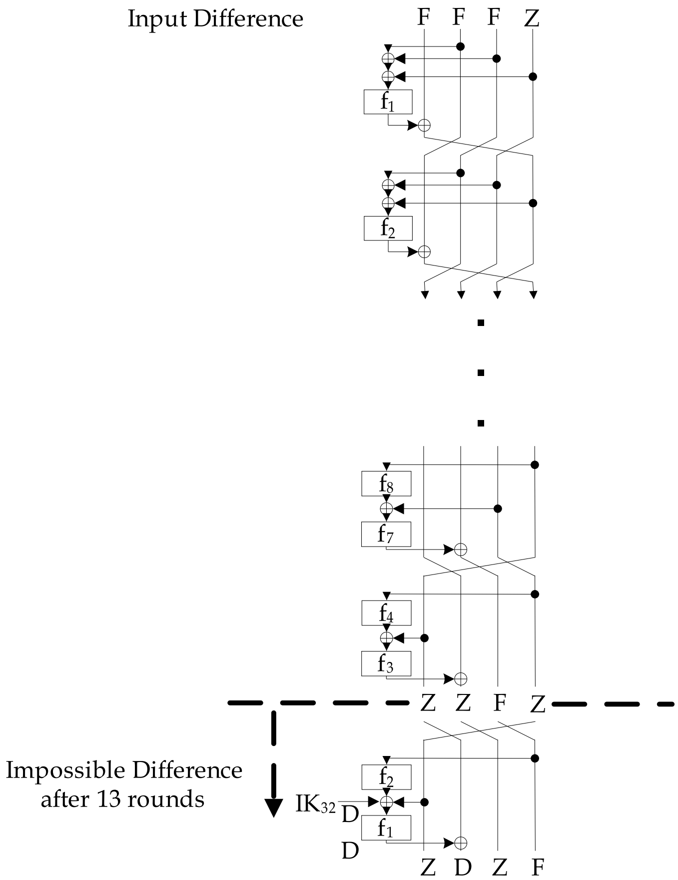


図 7: 128bit HyRAL の 14 ラウンド後の差分要素

$(\Delta C_0^{(13)},\ \Delta C_1^{(13)},\ \Delta C_2^{(13)},\ \Delta C_3^{(13)})$=(0, 0, α, 0) となる IK_{32} は鍵の候補から棄却される．このとき，(13) 式において，$\Delta C_0^{(13)} = \Delta C_3^{(13)} = 0$ であるから，次式を満たす IK_{32} は誤った鍵である．

$$f_1\left(f_2(\Delta C_2^{(13)}) \oplus IK_{32}\right) \oplus \Delta C_1^{(14)} = 0, \qquad (16)$$

(16) 式において，f_1 関数の出力差分は入力差分に対し，一様分布に従うと仮定したとき，14 ラウンド目の f_1 関数の出力差分を用いて，推測した 32bit の IK_{32} が誤りである確率は 2^{-32} である．よって，IK_{32} を正しい鍵に絞り込むのに必要な暗号文組の数 N は次式より，約 $2^{36.5}$ となる．

$$2^{32}\left(1-2^{-32}\right)^N = 1 \qquad (17)$$

解読に必要な平文組の数 $\frac{2^{36.5}}{2^{-96}} = 2^{132.5}$ において，平文 $(X_0,\ X_1,\ X_2,\ X_3)$ の X_3 を固定した 2^{96} 個の平文の中から，異なる 2 つを選ぶと差分が $(\alpha,\ \alpha,\ \alpha,\ 0)$ となる平文組を

$$\frac{2^{96}\left(2^{32}-1\right)}{2} \simeq 2^{127}, \qquad (18)$$

通り作ることができる．つまり，$2^{132.5-127} = 2^{5.5}$ 個の平文組を選択すれば，解読に必要な暗号文組を得ることができる．したがって，解読に必要な選択平文数は

$$2^{5.5} \cdot 2^{96} = 2^{101.5}, \qquad (19)$$

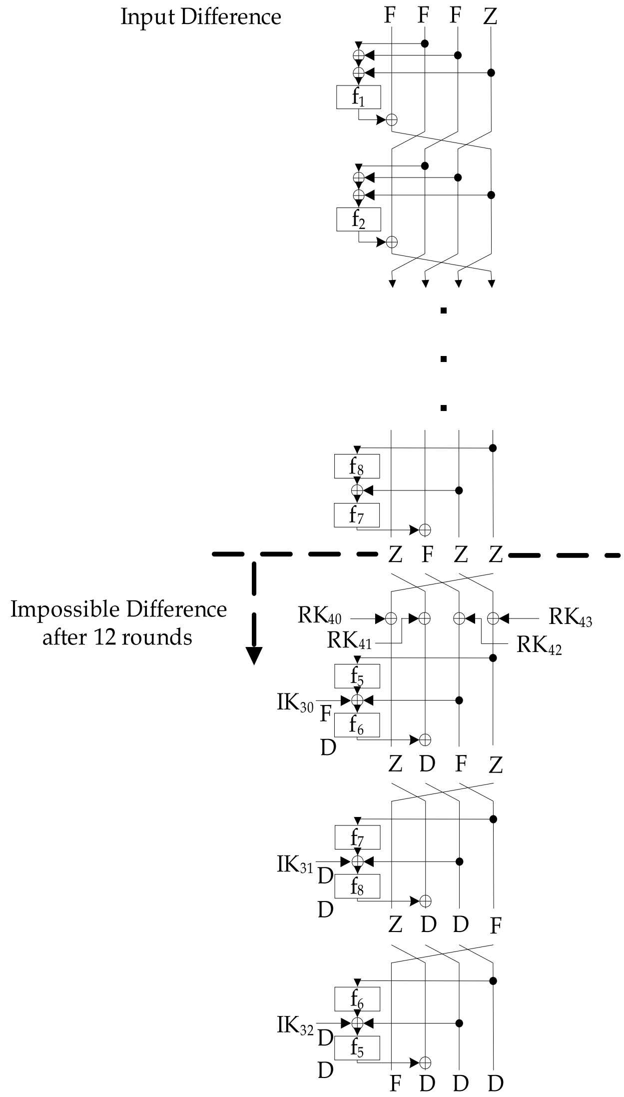


図 8: 192/256bit HyRAL の 15 ラウンド後の差分要素

となる．

次に，解読に必要な計算量は

1. 暗号文を求める計算量：$2^{101.5}$(暗号化)
2. 鍵を絞り込む計算量：$2^{36.5} \cdot 2^{32}$(F_1 関数のラウンド関数)$< 2^{65}$(暗号化)

したがって，解読に必要な計算量は

$$2^{101.5} + 2^{65} \simeq 2^{102}, \qquad (20)$$

となる．

192/256bit HyRAL の 13 ラウンド鍵回復

前章より，12 ラウンドの不能差分特性は $\boldsymbol{a}$=(F, F, F, Z)$\not\rightarrow$ $\boldsymbol{b}$=(Z, F, Z, Z) であったので，13 ラウンド後の出力差分要素は (Z, D, F, Z) となる (図 8 参照)．i ラウンド後の出力差分を $\Delta C^{(i)}$=$(\Delta C_0^{(i)}, \Delta C_1^{(i)}, \Delta C_2^{(i)}, \Delta C_3^{(i)})$ と表記したとき，差分が $(\alpha,\ \alpha,\ \alpha,\ 0)$ である平文組に対応した暗号文組の中から，$(\Delta C_0^{(13)},\ \Delta C_1^{(13)},$

$\Delta C_2^{(13)}$, $\Delta C_3^{(13)}$)=(0, β, α, 0) となる暗号文組を選ぶ．ただし，$\alpha \in \{0,1\}^{32}$ は非 0 の固定差分，$\beta \in \{0,1\}^{32}$ は非 0 の非固定差分である．α を定めたとき，$\Delta C_0^{(13)}$=0, $\Delta C_2^{(13)}$=α, $\Delta_3^{(13)}$=0 となる確率はそれぞれ $\frac{1}{2^{32}}$ であり，$\Delta C_1^{(14)}$=β となる確率は $\frac{2^{32}-1}{2^{32}}$ である．したがって，($\Delta C_0^{(13)}$, $\Delta C_1^{(13)}$, $\Delta C_2^{(13)}$, $\Delta C_3^{(13)}$)=(0, β, α, 0) となる暗号文組が得られる確率は

$$\left(\frac{1}{2^{32}}\right)^3 \cdot \left(\frac{2^{32}-1}{2^{32}}\right) \simeq 2^{-96}, \tag{21}$$

である．($\Delta C_0^{(13)}$, $\Delta C_1^{(13)}$, $\Delta C_2^{(13)}$, $\Delta C_3^{(13)}$)=(0, β, α, 0) となる暗号文組のうち，12 ラウンドの不能差分特性より，($\Delta C_0^{(12)}$, $\Delta C_1^{(12)}$, $\Delta C_2^{(12)}$, $\Delta C_3^{(12)}$)=(0, α, 0, 0) となる $RK_{42} \oplus IK_{30}$(以下，IK'_{30} という．) は正しい値の候補から棄却される．このとき，図 8 より，$\Delta C^{(12)}$ と $\Delta C^{(13)}$ の間に成立する関係式及び $\Delta C_0^{(12)} = \Delta C_2^{(12)} = 0$ から得られる次式を満たす IK'_{30} は誤った値である．

$$f_6\left(\Delta C_1^{(12)} \oplus IK'_{30}\right) \oplus \Delta C_1^{(13)} = 0, \tag{22}$$

(22) 式において，f_6 関数の出力差分は入力差分に対し，一様分布に従うと仮定したとき，13 ラウンド目の f_6 関数の出力差分を用いて，推測した 32bit の IK'_{30} が誤りである確率は 2^{-32} である．よって，IK'_{30} を正しい値に絞り込むのに必要な暗号文組の数 N は次式より，約 $2^{36.5}$ となる．

$$2^{32}\left(1-2^{-32}\right)^N = 1, \tag{23}$$

解読に必要な平文組の数 $\dfrac{2^{36.5}}{2^{-96}} = 2^{132.5}$ において，平文 (X_0, X_1, X_2, X_3) の X_3 を固定した 2^{96} 個の平文の中から，異なる 2 つを選ぶと差分が (α, α, α, 0) となる平文組を

$$\frac{2^{96}\left(2^{32}-1\right)}{2} \simeq 2^{127}, \tag{24}$$

通り作ることができる．つまり，$2^{132.5-127} = 2^{5.5}$ 個の平文組を選択すれば，解読に必要な暗号文組を得ることができる．したがって，解読に必要な選択平文数は

$$2^{5.5} \cdot 2^{96} = 2^{101.5}, \tag{25}$$

となる．

次に，解読に必要な計算量は

1. 暗号文を求める計算量：$2^{101.5}$(暗号化)
2. 鍵を絞り込む計算量：$2^{36.5} \cdot 2^{32}$(f_6 関数)$< 2^{64}$(暗号化)

したがって，解読に必要な計算量は

$$2^{101.5} + 2^{64} \simeq 2^{102}, \tag{26}$$

となる．

同様に，192/256bit HyRAL の 14 ラウンド及び $\mathbf{RK_4}$ 無しの 15 ラウンド鍵回復に必要な選択平文数と計算量の算出を行った．HyRAL に対する不能差分攻撃の攻撃可能段数及び攻撃に必要な選択平文数及び計算量をまとめたものを表 4 に示す．

表 4: HyRAL に対する不能差分攻撃の結果

段数	鍵長	選択平文数	計算量	備考
14	128	$2^{101.5}$	2^{102}	
13	192,256	$2^{101.5}$	2^{102}	
14	192,256	$2^{103.5}$	2^{158}	
15	256	$2^{103.1}$	2^{196}	$\mathbf{RK_4}$ 無

6　まとめ

角尾らによって提案された不能差分特性探索法を HyRAL へ適用し，HyRAL の不能差分特性探索を行った結果，128bit HyRAL は 13 ラウンド，192/256bit HyRAL は 12 ラウンドの不能差分特性があることが分かった．この結果を用い，HyRAL に不能差分攻撃を適用した結果，14 ラウンドの 128bit HyRAL に対して選択平文数 $2^{101.5}$，計算量 2^{102}，14 ラウンドの 192/256bit HyRAL に対して選択平文数 $2^{103.5}$，計算量 2^{158} で不能差分攻撃が可能である．しかしながら，HyRAL のラウンド数は 128bit HyRAL の場合は 24，192/256bit HyRAL の場合は 32 ラウンドであるので，本稿の結果が HyRAL の安全性に影響を与えることはない．

今後は，MDS 行列の特性を考慮した不能差分特性探索を行うとともに，その結果を利用した不能差分攻撃法の解読に必要な選択平文数及び計算量の詳細な検討を行う予定である．

参考文献

[1] 平田耕藏, “共通鍵 128 ビットブロック暗号 HyRAL”, SCIS2010-1D1-1, 2010.

[2] 高木幸弥，五十嵐保隆，金子敏信，“共通鍵ブロック暗号 HyRAL の差分攻撃耐性評価”，SCIS2010-1D1-2, 2010.

[3] 五十嵐保隆，高木幸弥，金子敏信，“共通ブロック暗号 HyRAL の線形攻撃耐性評価”, SCIS2010-1D1-3, 2010.

[4] J. Kim, S. Hong, J. Sung, C. Lee, and S. Lee, “Impossible Differential Cryptanalysis for Block Cipher Structures”, INDOCRYPT’03, LNCS 2904, pp.82-96, Springer-Verlag, 2003.

[5] 角尾幸保，辻原悦子，中嶋浩貴，久保博靖，“変形 Feistel 構造を持つブロック暗号の不可能差分”，SCIS2007-4A2-2, 2007.

[6] 中嶋浩貴，辻原悦子，茂真紀，川幡剛嗣，角尾幸保，“不能差分特性探索手法の改良”, SCIS2008-2A4-1, 2008.

[7] E. Biham and A. Shamir, “Differential Cryptanalysis of DES-like Cryptosysytems”, CRYPTO’90, LNCS 573, pp.2-21, Springer-Verlag, 1990.

[8] M. Matsui, “Linear Cryptanalysis Method for DES Cipher”, EUROCRYPT’93, LNCS 765, pp.386-397, Springer-Verlag, 1994.

[9] E. Biham, A. Biryukov, and A. Shamir, “Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials.” in *Proceedings of Eurocrypt’99* (J. Stern, ed), no.1592 in LNCS, pp.12-23, Spriger-Verlag, 1999.

[10] 辻原悦子，茂真紀，洲崎智保，川崎剛嗣，角尾幸保，“CLEFIA の新たな不能差分”，信学技法，vol.108, no38, ISEC2008-3, pp15-22, 2008 年 5 月．