# 249 ビット鍵 HyRAL の等価鍵

浅野 優貴　　柳原 慎吾　　岩田 哲

名古屋大学大学院工学研究科計算理工学専攻
464-8603 名古屋市千種区不老町
{y_asano@echo.nuee, s_yanagi@echo.nuee, iwata@cse}.nagoya-u.ac.jp

**あらまし** HyRAL はブロック長が 128 ビットであり，鍵長 $128, 129, \ldots, 256$ ビットをサポートするブロック暗号である．SCIS 2011 において，浅野，柳原，岩田は 256 ビット鍵 HyRAL の等価鍵に関する解析を行い，計算機を用いて実際に等価鍵の具体例を導出した．本論文では，鍵長が 249 ビットの HyRAL について考える．まず，249 ビット鍵 HyRAL に対し，$2^{33.4}$ ペアの等価鍵が存在することを示す．さらに，計算量 $2^{50.8}$ で等価鍵の一例を導出するアルゴリズムを示す．

# Equivalent Keys of 249-Bit Key HyRAL

Yuki Asano　　Shingo Yanagihara　　Tetsu Iwata

Dept. of Computational Science and Engineering, Nagoya University
Furo-cho, Chikusa-ku, Nagoya 464-8603, Japan
{y_asano@echo.nuee, s_yanagi@echo.nuee, iwata@cse}.nagoya-u.ac.jp

**Abstract** HyRAL is a blockcipher whose block length is 128 bits, and it supports the key lengths of $128, 129, \ldots, 256$ bits. At SCIS 2011, Asano, Yanagihara, and Iwata presented the analysis of 256-bit key HyRAL in terms of equivalent keys, and they experimentally derived concrete instances of equivalent keys. In this paper, we consider the 249-bit key version of HyRAL. First, we show that there exist $2^{33.4}$ pairs of equivalent keys. We then show an algorithm that derives an instance of equivalent keys with a time complexity of $2^{50.8}$ encryptions.

## 1　はじめに

HyRAL は，CRYPTREC における電子政府推奨暗号リストの改訂に伴う公募へ提案されたブロック暗号であり，ブロック長は 128 ビット，鍵長は $128, 129, \ldots, 256$ ビットをサポートしている [4, 2]．差分攻撃，線形攻撃，不可能差分攻撃，飽和攻撃，高階差分攻撃などの攻撃に対する安全性評価の結果が報告されており [4, 5, 7, 8, 9, 10, 11, 12, 13, 14, 15]，現在までにこれらの攻撃に対する脆弱性は指摘されていない．

ブロック長 $n$ ビット，鍵長 $k$ ビットのブロック暗号 $E$ に対し，すべての平文 $M \in \{0,1\}^n$ について $E_K(M) = E_{K'}(M)$ が成り立つような互いに異なる鍵のペア $K, K' \in \{0,1\}^k$ を等価鍵という [6]．等価鍵の存在は鍵の全数探索攻撃にかかる計算量の削減を意味するため，その暗号の理論的解読を意味する．

SCIS 2011 において，浅野，柳原，岩田は 256 ビット鍵 HyRAL に対し，$2^{50.0}$ ペアの等価鍵が存在することを示した [1]．256 ビット鍵 HyRAL の鍵空間のサイズは高々 $2^{256} - 2^{50.0}$ であるため，256 ビット鍵 HyRAL は理想的な 256 ビット鍵ブロック暗号に要求される暗号学的強度を有していない．CRYPTREC 暗号方式委員会は，HyRAL について第一次評価までで評価終了とし，次期電子政府推奨暗号リストには掲載しな

いことを発表した [3].

[1] では鍵長が 256 ビットの場合のみを解析している．そこで本論文では，

「鍵長が 256 ビット未満の HyRAL に
対し，等価鍵は存在するか?」

という問題を考える．鍵長が 256 ビット未満の HyRAL では，$128, 129, \ldots, 255$ ビットの合計 128 通りの鍵長が考えられ，本論文ではこのうち，鍵長が 249 ビットの場合を考える．

まず 249 ビット鍵 HyRAL に対し，$2^{33.4}$ ペアの等価鍵が存在することを示す．[1] において示されている $2^{50.0}$ ペアの 256 ビット鍵 HyRAL の等価鍵のうち，$2^{33.4}$ ペアについては最下位 7 ビットが 0 であることを指摘する．249 ビット鍵 HyRAL は，256 ビット鍵 HyRAL の秘密鍵の最下位 7 ビットを 0 に固定することにより得られる．したがって，最下位 7 ビットが 0 である $2^{33.4}$ ペアの等価鍵は，256 ビット鍵 HyRAL の等価鍵であると同時に，249 ビット鍵 HyRAL の等価鍵でもある．

さらに，[1] にある 256 ビット鍵 HyRAL に対する等価鍵導出アルゴリズムにおいて，鍵探索の際に最下位 7 ビットを 0 に固定することにより，計算量 $2^{50.8}$ で等価鍵の一例を導出するアルゴリズムを示す．また，名古屋大学情報基盤センターのスーパーコンピュータシステムを用いてそのアルゴリズムを実行した場合に要する計算時間，及び金額的コストの予測を示す．

## 2　249 ビット鍵 HyRAL の仕様

**全体構造:** 249 ビット鍵 HyRAL の全体構造を図 1 に示す．入力は秘密鍵 $K \in \{0,1\}^{249}$ と平文 $M \in \{0,1\}^{128}$ であり，出力は暗号文 $C \in \{0,1\}^{128}$ である．249 ビット鍵 HyRAL は鍵生成アルゴリズム (KGA: Key Generation Algorithm)，鍵割り当てアルゴリズム (KAA: Key Assignment Algorithm)，データ撹拌アルゴリズム (DPA: Data Processing Algorithm) を内部で用いる．鍵生成アルゴリズムは 2 回使用し，それぞれ $\mathrm{KGA}_1$, $\mathrm{KGA}_2$ と表記する．秘密鍵 $K \in \{0,1\}^{249}$ と平文 $M \in \{0,1\}^{128}$ に対し，以下のように暗号化を行う．

1. $K$ の最下位に 7 ビットの 0 を連結し $(K, 0^7)$ とし，その上位 128 ビットを $OK_1$，下位 128 ビットを $OK_2$ とする．ただし，$0^7$ は 7 ビットの 0 を表す．
2. 鍵生成アルゴリズム $\mathrm{KGA}_1$, $\mathrm{KGA}_2$ にそれぞれ $OK_1, OK_2$ を入力し，中間データ $(Y_4, Y_5, Y_6, Y_7)$, $(Z_4, Z_5, Z_6, Z_7)$ を生成する．$Y_i$, $Z_i \in \{0,1\}^{128}$ である．
3. $KM = (KM_1, KM_3, KM_2, KM_4) \leftarrow (Y_4 \oplus Z_4, Y_5 \oplus Z_5, Y_6 \oplus Z_6, Y_7 \oplus Z_7)$ を計算する．$KM_i \in \{0,1\}^{128}$ である．
4. $KM$ を鍵割り当てアルゴリズム KAA に入力し，$(RK_1, \ldots, RK_9, IK_1, \ldots, IK_6)$ を計算する．$RK_i, IK_i \in \{0,1\}^{128}$ である．
5. $(RK_1, \ldots, RK_9, IK_1, \ldots, IK_6)$ 及び平文 $M$ をデータ撹拌アルゴリズム DPA に入力し，暗号文 $C$ を計算する．

KAA 及び DPA の詳細な定義は [4] にある．

**鍵生成アルゴリズム $\mathrm{KGA}_1$，$\mathrm{KGA}_2$:** 図 1 に $\mathrm{KGA}_1$, $\mathrm{KGA}_2$ の構造も示す．これらは内部で入出力 128 ビットの $G_1$ 関数，$G_2$ 関数を用いる．また，$\mathrm{KGA}_1$ は内部で定数 $\mathrm{CST}_1 \in \{0,1\}^{128}$ を用い，$\mathrm{KGA}_2$ では $\mathrm{CST}_2 \in \{0,1\}^{128}$ を用いる．これらの定数の値は [4] にある．$\mathrm{KGA}_1$ の入力は $OK_1 \in \{0,1\}^{128}$，出力は $(Y_4, Y_5, Y_6, Y_7) \in \{0,1\}^{512}$，$\mathrm{KGA}_2$ の入力は $OK_2 \in \{0,1\}^{128}$，出力は $(Z_4, Z_5, Z_6, Z_7) \in \{0,1\}^{512}$ である．

**$G_1$ 関数，$G_2$ 関数:** $G_1$ 関数，$G_2$ 関数を図 2 に示す．これらの関数は $(X_1^{(1)}, X_2^{(1)}, X_3^{(1)}, X_4^{(1)}) \in \{0,1\}^{128}$ を入力とし，$(X_1^{(5)}, X_2^{(5)}, X_3^{(5)}, X_4^{(5)}) \in \{0,1\}^{128}$ を出力する．ともに 4 ラウンド，4 系列の一般化 Feistel 型構造であり，$G_1$ 関数は内部で 32 ビット入出力の $f_1, f_2, f_3, f_4$ 関数を用い，$G_2$ 関数は $f_5, f_6, f_7, f_8$ 関数を用いる．$f_i$ 関数の詳細な定義は [4] にある．

## 3　等価鍵の存在

まず [1] に沿って等価鍵の存在についてまとめる．鍵生成アルゴリズム $\mathrm{KGA}_1$, $\mathrm{KGA}_2$ に入

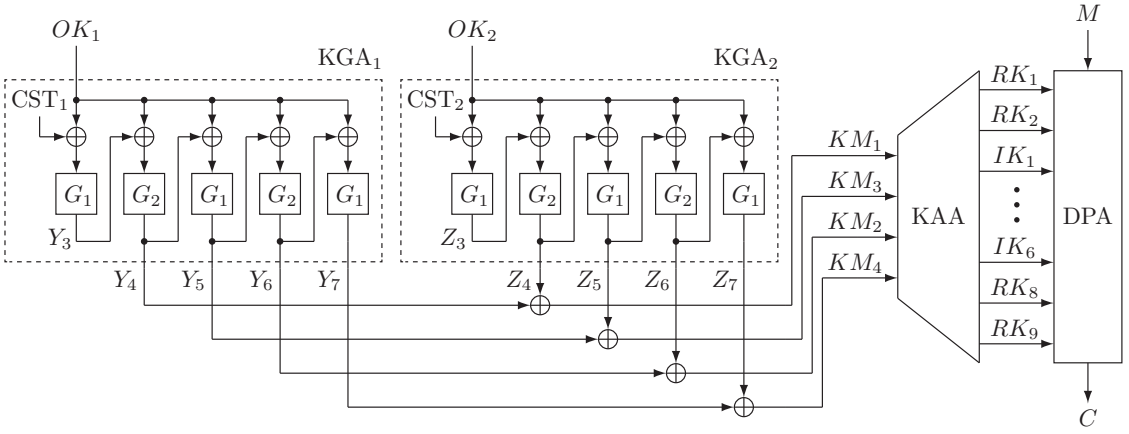


図 1: 249 ビット鍵 HyRAL の全体構造と $\mathrm{KGA}_1$, $\mathrm{KGA}_2$ の構造．秘密鍵 $K \in \{0,1\}^{249}$ に対し，$OK_1$ は $(K, 0^7)$ の上位 128 ビット，$OK_2$ は下位 128 ビットである．

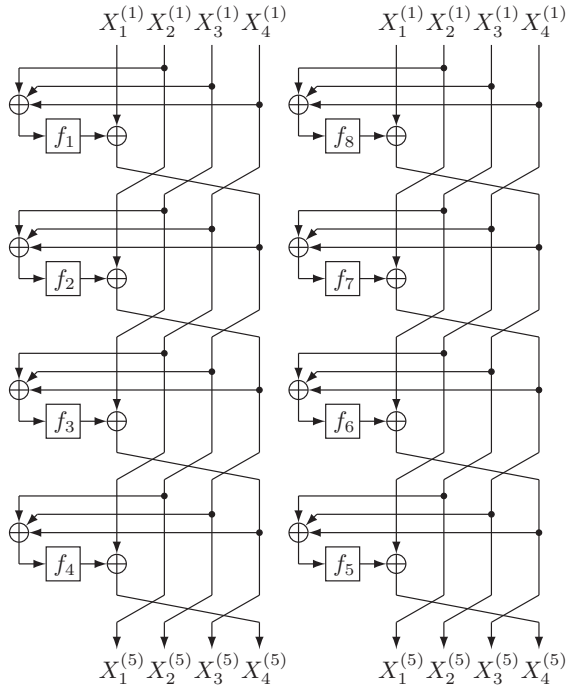


図 2: $G_1$ 関数 (左)，$G_2$ 関数 (右)

力差分 $\Delta OK_1$, $\Delta OK_2$ を入力した時の出力差分をそれぞれ

$$
\begin{aligned}
&(\Delta Y_4, \Delta Y_5, \Delta Y_6, \Delta Y_7) \\
&\quad = \mathrm{KGA}_1(OK_1) \oplus \mathrm{KGA}_1(OK_1 \oplus \Delta OK_1) \\
&(\Delta Z_4, \Delta Z_5, \Delta Z_6, \Delta Z_7) \\
&\quad = \mathrm{KGA}_2(OK_2) \oplus \mathrm{KGA}_2(OK_2 \oplus \Delta OK_2)
\end{aligned}
$$

とする．これらの出力差分が一致し，$(\Delta Y_4, \Delta Y_5, \Delta Y_6, \Delta Y_7) = (\Delta Z_4, \Delta Z_5, \Delta Z_6, \Delta Z_7)$ が成立すると，鍵割り当てアルゴリズム KAA の入力差分 $(\Delta KM_1, \Delta KM_3, \Delta KM_2, \Delta KM_4)$ が 0 となるため，

$$
\begin{aligned}
&(OK_1, OK_2), (OK_1 \oplus \Delta OK_1, OK_2 \oplus \Delta OK_2) \\
&(OK_1 \oplus \Delta OK_1, OK_2 \oplus \Delta OK_2), (OK_1, OK_2) \\
&(OK_1 \oplus \Delta OK_1, OK_2), (OK_1, OK_2 \oplus \Delta OK_2) \\
&(OK_1, OK_2 \oplus \Delta OK_2), (OK_1 \oplus \Delta OK_1, OK_2)
\end{aligned}
$$

はいずれも等価鍵となる．[1] に従い，本論文ではこれを 4 個 (2 ペア) と数える．$\mathrm{KGA}_1, \mathrm{KGA}_2$ は定数を除いて同一のアルゴリズムであるから差分を考える上では両者を同一視でき，以降，$\mathrm{KGA} \in \{\mathrm{KGA}_1, \mathrm{KGA}_2\}$ と表記する．また，KGA の入力差分を $\Delta OK$ をとし，出力差分を $(\Delta Y_4, \Delta Y_5, \Delta Y_6, \Delta Y_7)$ とする．

**256 ビット鍵 HyRAL の等価鍵 [1]:** $\Delta OK = (\delta, \delta, \delta, \delta)$, $\Delta Y_4 = (\delta, \delta, 0, 0)$, $\Delta Y_5 = (0, 0, 0, \delta)$, $\Delta Y_6 = (\delta, \delta, \delta, \delta)$, $\Delta Y_7 = (0, 0, 0, 0)$ とする．ただし，$\delta \in \{0,1\}^{32}$ は任意の非ゼロのビット列である．この入出力差分の [1, 表 1] にある差分パスに対する差分特性確率は $\delta$ のみに依存し，これを $\mathrm{DCP}^{\mathrm{KGA}}(\delta)$ と表記する．$\mathrm{DCP}^{\mathrm{KGA}}(\delta)$ は，次式で与えられる [1].

$$
\begin{aligned}
&\mathrm{DCP}^{\mathrm{KGA}}(\delta) \\
&\quad = \mathrm{DP}^{f_1}(\delta) \cdot \mathrm{DP}^{f_3}(\delta) \cdot \mathrm{DP}^{f_5}(\delta) \cdot \mathrm{DP}^{f_7}(\delta)
\end{aligned}
$$

ただし，

$$
\mathrm{DP}^{f_i}(\delta) = \frac{\#\{I \mid f_i(I) \oplus f_i(I \oplus \delta) = \delta\}}{2^{32}}
$$

は $f_i$ 関数の入出力差分がともに $\delta$ となる確率である．[1] において，$\mathrm{DCP}^{\mathrm{KGA}}(\delta) > 2^{-128}$ となる非ゼロの $\delta$ が 89938 通り存在することが示されている．表 1 にこの一部を示す．

表 1: $\mathrm{DCP}^{\mathrm{KGA}}(\delta) > 2^{-128}$ となる $\delta$ の例と個数 [1]

| $\mathrm{DCP}^{\mathrm{KGA}}(\delta)$ | $\delta$ の例 | $\delta$ の個数 |
|---|---|---|
| $2^{-103}$ | 0xd7d7d0d7 | 1 |
| $2^{-104}$ | 0xc5c5d254 | 1 |
| ⋮ | ⋮ | ⋮ |
| $2^{-111}$ | 0x0101e818 | 7685 |
| $2^{-112}$ | 0x01010520 | 80471 |

[1] において，$\mathrm{DCP}^{\mathrm{KGA}}(\delta) > 2^{-128}$ となる $\delta$ の存在は，等価鍵の存在を意味することが示されている．

**249 ビット鍵 HyRAL の等価鍵:** 次に 249 ビット鍵 HyRAL について考える．例えば $\delta =$ 0xd7d7d0d7，$\Delta OK_1 = \Delta OK_2 = (\delta, \delta, \delta, \delta)$ の場合，$2^{50}$ 通りの $(OK_1, OK_2)$ に対し，$(K, K') = ((OK_1, OK_2), (OK_1 \oplus \Delta OK_1, OK_2 \oplus \Delta OK_2))$ は 256 ビット鍵 HyRAL の等価鍵である．

ここで $\delta$ の最下位 7 ビットに 1 が存在するため，$OK_2$ あるいは $OK_2 \oplus \Delta OK_2$ の最下位 7 ビットには必ず 1 が存在し，したがってこの $\delta$ から得られる 256 ビット鍵 HyRAL の等価鍵には，249 ビット鍵 HyRAL の等価鍵は存在しない．

一方，表 1 にある 89938 通りの $\delta$ の中には，最下位 7 ビットが 0 である $\delta$ が存在する．そのような $\delta$ は表 1 を $\delta$ についてソートすることで得られ，実際に 398 通り存在する．$\delta$ の例と個数を表 2 にまとめる．

例えば $\delta =$ 0xe00ce080，$\Delta OK_1 = \Delta OK_2 = (\delta, \delta, \delta, \delta)$ の場合，$2^{38}$ 通りの $(OK_1, OK_2)$ に対し，$(K, K') = ((OK_1, OK_2), (OK_1 \oplus \Delta OK_1, OK_2 \oplus \Delta OK_2))$ は 256 ビット鍵 HyRAL の等価鍵である．

この $2^{38}$ 通りの $(OK_1, OK_2)$ のうち，$2^{38} \times 2^{-7} = 2^{31}$ 通りの $(OK_1, OK_2)$ に対しては $OK_2$ の最下位 7 ビットが 0 であると期待でき，この場合 $OK_2 \oplus \Delta OK_2$ の最下位 7 ビットも 0 である．したがってこれらは 256 ビット鍵 HyRAL の等価鍵であると同時に，249 ビット鍵 HyRAL の等価鍵でもある．

表 2: 最下位 7 ビットが 0 である $\delta$ の例と個数

| $\mathrm{DCP}^{\mathrm{KGA}}(\delta)$ | $\delta$ の例 | $\delta$ の個数 |
|---|---|---|
| $2^{-109}$ | 0xe00ce080 | 1 |
| $2^{-110}$ | 0x3f4ba680 | 8 |
| $2^{-111}$ | 0x078e2a80 | 39 |
| $2^{-112}$ | 0x01348f80 | 350 |

以上の議論と表 2，及び重複を考慮すると，249 ビット鍵 HyRAL の等価鍵の個数は

$$\frac{4(2^{31} \cdot 1 + 2^{29} \cdot 8 + 2^{27} \cdot 39 + 2^{25} \cdot 350)}{4} \geq 2^{34.4}$$

となり，ペア数はこの 1/2 である $2^{33.4}$ となる．以上より，次の補題を得る．

**補題 3.1** 249 ビット鍵 HyRAL には $2^{34.4}$ 個 ($2^{33.4}$ ペア) の等価鍵が存在する．

## 4 等価鍵導出アルゴリズム

**表記法:** 前章と同様，$\mathrm{KGA} \in \{\mathrm{KGA}_1, \mathrm{KGA}_2\}$ とし，$G_1$ 関数，$G_2$ 関数の 1 ラウンドを KGA の 1 ラウンドとする．KGA の入力を $OK \in \{OK_1, OK_2\}$，定数を $\mathrm{CST} \in \{\mathrm{CST}_1, \mathrm{CST}_2\}$ とし，$OK = (K_1, K_2, K_3, K_4) \in \{0,1\}^{128}$ と書き，$\mathrm{CST} = (C_1, C_2, C_3, C_4) \in \{0,1\}^{128}$ と書く．KGA は 20 ラウンドの関数であり，$r = 1, 2, \ldots, 20$ に対し，$r$ ラウンドにある $f_i$ 関数を $f_i^{(r)}$ とし，その入出力をそれぞれ $I_i^{(r)}, O_i^{(r)} \in \{0,1\}^{32}$ と書く．

**等価鍵導出アルゴリズム:** $\delta =$ 0xe00ce080 の場合を考える．この $\delta$ に対し，$\mathrm{DP}^{f_1}(\delta) = 2^{-28}$, $\mathrm{DP}^{f_3}(\delta) = 2^{-28}$, $\mathrm{DP}^{f_5}(\delta) = 2^{-26}$, $\mathrm{DP}^{f_7}(\delta) = 2^{-27}$ である．したがって，$i \in \{1, 3, 5, 7\}$ に対し $f_i(I_i) \oplus f_i(I_i \oplus \delta) = \delta$ を満たす $I_i$ のリストを $\mathcal{I}_i$ とすると，それぞれのサイズは $\#\mathcal{I}_1 = 16$, $\#\mathcal{I}_3 = 16$, $\#\mathcal{I}_5 = 64$, $\#\mathcal{I}_7 = 32$ となる．

$I_1^{(1)} \in \mathcal{I}_1$, $I_7^{(6)} \in \mathcal{I}_7$, $I_3^{(11)} \in \mathcal{I}_3$, $I_5^{(16)} \in \mathcal{I}_5$ を満たす $OK = (K_1, K_2, K_3, K_4)$ は，等価鍵

の一部 ($OK_1$ または $OK_2$) である．$I_1^{(1)} \in \mathcal{I}_1$, $I_7^{(6)} \in \mathcal{I}_7$ を両方満たす $(K_1, K_2, K_3, K_4)$ を導出できることが示されている [1]．

**補題 4.1 ([1])** 任意に固定された $\tilde{K}_1, I_1^{(1)}, I_8^{(5)}, I_7^{(6)}$ に対する $(K_1, K_2, K_3, K_4)$ を導出できる．ただし，$\tilde{K}_1 = K_1 \oplus K_3$ である．

この補題を用いて，249 ビット鍵 HyRAL の等価鍵導出アルゴリズムを示す．

**$OK_1$ の導出：** $OK_1$ を出力する等価鍵導出アルゴリズムは，用いるリスト $\mathcal{I}_1, \mathcal{I}_3, \mathcal{I}_5, \mathcal{I}_7$ が異なる点を除いて，256 ビット鍵 HyRAL の等価鍵導出アルゴリズムと同一である．

**$OK_2$ の導出：** $OK_2$ の導出では，$K_4$ の最下位 7 ビットが 0 となるようにアルゴリズムを修正する．$OK_2$ の導出アルゴリズムを以下に示す．

1. $I_1^{(1)} \in \mathcal{I}_1$, $I_7^{(6)} \in \mathcal{I}_7$ を満たす $I_1^{(1)}$, $I_7^{(6)}$ を任意に固定し，$O_1^{(1)} = f_1(I_1^{(1)})$ を計算する．
2. $I_8^{(5)}$ を任意に固定し，$O_8^{(5)} = f_8(I_8^{(5)})$ を計算する．
3. $O_2^{(2)} = \tilde{C}_5 \oplus I_8^{(5)} \oplus O_8^{(5)}$ を計算する．ただし，$\tilde{C}_5 = C_1 \oplus C_2 \oplus O_1^{(1)} \oplus I_7^{(6)}$ である．
4. $\tilde{K}_2 = f_2^{-1}(O_2^{(2)}) \oplus \tilde{C}_1$ を計算する．ただし，$\tilde{C}_1 = C_1 \oplus C_3 \oplus C_4 \oplus O_1^{(1)}$ である．
5. $\tilde{K}_2$ と最下位 7 ビットが等しい $\tilde{K}_1$ を任意に固定する．すべての $\tilde{K}_1$ を探索したらステップ 2 へ戻る．
6. 補題 4.1 により $(K_1, K_2, K_3, K_4)$ を求める．
7. $(K_1, K_2, K_3, K_4)$ より $I_3^{(11)}$ を求め，$I_3^{(11)} \in \mathcal{I}_3$ が成り立てばステップ 8 へ進む．そうでなければステップ 5 へ戻る．
8. $(K_1, K_2, K_3, K_4)$ より $I_5^{(16)}$ を求め，$I_5^{(16)} \in \mathcal{I}_5$ が成り立てば $(K_1, K_2, K_3, K_4)$ を出力して終了する．そうでなければステップ 5 へ戻る．

[1] より $K_4 = \tilde{K}_1 \oplus \tilde{K}_2$ であるため，ステップ 5 において $OK_2$ の最下位 7 ビットは 0 となる．

**計算量：** $OK_1, OK_2$ それぞれに対し，$I_3^{(11)}, I_5^{(16)}$ が $\{0,1\}^{32}$ 上を一様に分布すると仮定すると，$I_3^{(11)} \in \mathcal{I}_3$, $I_5^{(16)} \in \mathcal{I}_5$ が両方成立する確率は $(16/2^{32}) \times (64/2^{32}) = 2^{-54}$ なので，$2^{54}$ 通りの $(I_8^{(5)}, \tilde{K}_1)$ を探索すれば $(K_1, K_2, K_3, K_4)$ が出力されると期待できる．

$OK_1$ に対し，$2^{54}$ 通りの $(I_8^{(5)}, \tilde{K}_1)$ を探索する際に，$2^{22}$ 通りの $I_8^{(5)}$ を探索し，各 $I_8^{(5)}$ に対して $2^{32}$ 通りの $\tilde{K}_1$ を探索すると，$5 \times 2^{54}$ 回の $f_i$ 関数の計算でアルゴリズムを実行できる．

$OK_2$ に対しては最下位 7 ビットを 0 に固定するため，$\tilde{K}_1$ は $2^{32}$ 通りの値を取ることはできない．そのため，$2^{29}$ 通りの $I_8^{(5)}$ を探索し，各 $I_8^{(5)}$ に対して $2^{25}$ 通りの $\tilde{K}_1$ を探索する．この場合も，$5 \times 2^{54}$ 回の $f_i$ 関数の計算でアルゴリズムを実行できる．

$OK_1, OK_2$ を両方導出するための計算量は合計で $10 \times 2^{54}$ 回の $f_i$ 関数の計算であり，249 ビット鍵 HyRAL の暗号化関数には 96 個の $f_i$ 関数があることから，これは暗号化関数を $2^{50.8}$ 回実行する計算量に相当する．

**計算時間，金額的コスト：** 計算機として名古屋大学情報基盤センターのスーパーコンピュータシステム (HX600) を利用して，249 ビット鍵 HyRAL の等価鍵導出アルゴリズムを実行する場合にかかる計算時間，及び金額的コストの予測を表 3 に示す．

表 3 において，16 コアを用いてアルゴリズムの一部を実行して得たデータを「16 コア (実測)」の欄に示す．$(I_8^{(5)} \times \tilde{K}_1)$ は探索した $(I_8^{(5)}, \tilde{K}_1)$ の個数を表し，計算時間は実測，金額は HX600 の使用料 (16 コアの場合 1 秒あたり 0.06 円) と実測した計算時間から算出した．

1024 コアを用いてアルゴリズム全体を実行した場合にかかる計算時間，及び金額的コストの予測を「1024 コア (予測)」の欄に示す．$(I_8^{(5)} \times \tilde{K}_1)$ は探索する $(I_8^{(5)}, \tilde{K}_1)$ の個数を表し，計算時間はこの個数と 16 コアの計算時間から算出した予測である．また，$OK_1, OK_2$ の計算時間はそれぞれ 12.155 日，11.982 日に相当する．金額は HX600 の使用料 (1024 コアの場合 1 秒あたり 0.96 円) と予測した計算時間から算出した．

表 3: HX600 を用いた場合にかかる計算時間と金額的コスト

| | 16 コア (実測) | | | 1024 コア (予測) | | |
|---|---|---|---|---|---|---|
| | $(I_8^{(5)} \times \tilde{K}_1)$ | 計算時間 (秒) | 金額 (円) | $(I_8^{(5)} \times \tilde{K}_1)$ | 計算時間 (秒) | 金額 (千円) |
| $OK_1$ | $2^8 \times 2^{32}$ | 4102.2 | 247 | $2^{22} \times 2^{32}$ | $1.0502 \times 10^6$ | 1008.2 |
| $OK_2$ | $2^{15} \times 2^{25}$ | 4044.1 | 243 | $2^{29} \times 2^{25}$ | $1.0353 \times 10^6$ | 993.87 |

## 5 まとめ

本論文ではまず，249 ビット鍵 HyRAL に対し，$2^{33.4}$ ペアの等価鍵が存在することを示した．この結果は 249 ビット鍵 HyRAL の理論的解読を意味する．さらに，計算量が $2^{50.8}$ である等価鍵導出アルゴリズムを示し，その実行に要する計算時間，及び金額的コストの予測を示した．

## 謝辞

計算機実験には名古屋大学情報基盤センターのスーパーコンピュータシステムを利用した．本研究の一部は科研費若手研究 (A) (課題番号 22680001) の助成を受けた．

## 参考文献

[1] 浅野優貴, 柳原慎吾, 岩田哲, “256 ビット鍵 HyRAL の等価鍵,” SCIS 2011, 2B2-3, 2011.

[2] CRYPTREC, http://www.cryptrec.go.jp/index.html

[3] CRYPTREC, “CRYPTREC Report 2010 暗号方式委員会報告書,” 2011.

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

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

[6] Lars R. Knudsen, “Cryptanalysis of LOKI,” ASIACRYPT ’91, LNCS 739, pp. 22–35, 1993.

[7] 芝山直喜, 五十嵐保隆, 金子敏信, 半谷精一郎, “共通鍵ブロック暗号 HyRAL の不能差分攻撃について,” FIT 2010, L-022, 2010.

[8] 芝山直喜, 五十嵐保隆, 金子敏信, 半谷精一郎, “共通鍵ブロック暗号 HyRAL の MDS 行列の分岐数を利用した不能差分特性について,” 2010 年電子情報通信学会基礎・境界ソサイエティ大会, A-7-8, 2010.

[9] 芝山直喜, 五十嵐保隆, 金子敏信, 半谷精一郎, “共通鍵ブロック暗号 HyRAL の飽和攻撃耐性評価,” SITA 2010, 10.1, 2010.

[10] 芝山直喜, 五十嵐保隆, 金子敏信, 半谷精一郎, “共通鍵ブロック暗号 HyRAL に対する高階差分攻撃,” 信学技報, ISEC 2010-123, pp. 341–347, 2011.

[11] 芝山直喜, 五十嵐保隆, 金子敏信, 半谷精一郎, “共通鍵ブロック暗号 HyRAL の飽和攻撃耐性評価 (II),” 信学技報, ISEC 2011-19, pp. 103–109, 2011.

[12] 多賀文吾, 田中秀磨, “共通鍵ブロック暗号 HyRAL の高階差分特性,” SCIS 2011, 2B2-2, 2011.

[13] 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,” SCIS 2010, 1D1-2, 2010.

[14] 山口洋平, 五十嵐保隆, 金子敏信, “共通鍵ブロック暗号 HyRAL の高階差分特性,” 第 63 回電気関係学会九州支部連合大会, 02-1A-06, 2010.

[15] Heung Youl YOUM, Jung Hwan Song, and Sun Young Lee, “Security Analysis of HyRAL,” CRYPTREC 技術報告書, 2011.