Piccolo-typeブロック暗号のラウンド置換の改良

内海 潮音[1,a)]　中橋 元輝[1]　阪本 光星[1]　五十部 孝典[1,2]

概要：Piccolo は，16 ビットワード単位の 4-line Generalized Feistel 構造をベースとした軽量ブロック暗号である．Piccolo では，拡散性能を向上させるため通常のワード単位ではなくバイト単位のラウンド置換 (RP) を採用している．本研究では，バイト単位の RP に対して，安全性の観点でその最適性を検証する．具体的には，すべてのバイト単位の RP に対して，差分・線形，不能差分，Integral 攻撃の耐性を混合整数線形計画法 (MILP) での評価により実施した．結果として，Piccolo の RP がこれらの攻撃に対する安全性を保障するラウンド数の観点で最適であることを明らかにした．また MILP での評価の結果，線形攻撃に対しては，設計者評価より 1 ラウンド短い 7 ラウンドで安全であることを示し，Integral 評価については初めて安全性を保障可能なラウンド数を導出した．さらに，不能差分に対する安全性が Piccolo と比較して，1 ラウンド少ない 7 ラウンドで達成可能な 2 つのクラスの構成を示す．これらの構成は差分/線形攻撃に対する安全性を保障するためにはそれぞれ 7/9 と 8/8 ラウンドが必要な構成であり，Piccolo よりも多くのラウンド数を要する．しかし，本研究のでの差分/線形攻撃への評価は，差分/線形確率が最も高い遷移のみを仮定した設計者にとってワーストケースでの評価であり，実際に 8 ラウンドもしくは 7 ラウンドで識別可能かは不明である．よって，実際に 7 ラウンドの不能差分識別子のある Piccolo のものよりも，新しい PR の方が安全性の観点で優れている可能性も十分高い．

キーワード：軽量ブロック暗号，Piccolo，差分攻撃，線形攻撃，　不能差分攻撃，　Integral 攻撃，MILP

Round Permutation of Piccolo-type Block Cipher Revisited

Shion Utsumi[1,a)]　Motoki Nkahashi[1]　Kosei Sakamoto[1]　Tkanori Isobe[1,2]

Abstract: Piccolo is a lightweight block cipher based on a 16-bit word 4-line Generalized Feistel structure. Piccolo adopts byte-based Round Permutation (RP) instead of the usual word-based RP to improve the diffusion property. In this paper, we explore the optimally of byte-based RP from the viewpoint of security. Specifically, for all byte-by-byte RPs, we evaluate the security of differential, linear, impossible differential, and integral attacks by Mixed Integer Linear Programming (MILP). We show that Piccolo's RP is optimal in terms of the number of rounds to guarantee the security against these attacks. In addition, we show new two classes of RPs those are secure against impossible differentials in 7 rounds, which is one round less than in Piccolo. On the other hand, these require 7/9 and 8/8 rounds to guarantee security against differential/linear attacks, respectively, and require more rounds than Poccolo.

Keywords: lightweight block cipher, Piccolo, differential attack, linear attack, impossible differential attack, Integral attack, MILP

1. はじめに

近年，RFID タグやセンサーノードなどの低リソースデバイスの大量導入や，それらのデバイス間のセキュリティ提供の需要が高まる中，軽量暗号が注目されている．

[1] 兵庫県立大学, University of Hyogo, Japan
[2] 国立研究開発法人情報通信研究機構, National Institute of Information and Communications Technology, Japan
[3] 国立研究開発法人科学技術振興機構, PRESTO, Japan Science and Technology Agency, Japan
[a)] ad22p011@u-hyogo.ac.jp

表 1 安全性を保証するために必要なラウンド数の比較

	Piccolo	RP-1	RP-2
差分攻撃	7 [1]	7	8
線形攻撃	**7** (本論文)/8 [1]	9	8
不能差分攻撃	8 [1]	**7**	**7**
Integral 攻撃	**7** (本論文)/ None[1]	7	7
順方向 Full Diffusion	4 [1]	4	4
逆方向 Full Diffusion	4 [1]	4	4

CHES 2011 において，ハードウェアで低回路規模で実装可能な軽量ブロック暗号 Piccolo が提案された [1]．Piccolo は Generalized Feistel 構造や軽量関数 (F 関数，鍵スケジュール関数) で構成されており， 少ないゲート数で実装可能であり，ハードウェアリソースに制約がある状況でも高い安全性を確保できる．特に，ラウンド置換 (RP) 部が通常のワード単位の置換とは異なり，Piccolo の場合は， 8 ビット (1 バイト) 単位のバイト置換を行うことで拡散性能を向上させ，通常のワード置換のものよりも早いラウンドでの安全性達成を実現している．

本稿では Piccolo のアルゴリズムの RP 部を変更した Piccolo-type 構造を定義し, Piccolo の RP の最適性に安全性の観点について検証する．具体的には, Piccolo-type 構造について差分/線形，不能差分，Integral 攻撃に対する安全性評価を混合整数線形計画法を用いて行い，RP 毎に安全性を保証する最低ラウンド数を求める．ハードウェアのラウンド実装においては，RP の変更は実装面に影響を及ぼさないため，安全性の観点で最適な RP は，実装と安全性の観点でも最適な RP を意味する．また，本評価では，設計者評価で実施されていない Active S-box(AS) による差分・線形攻撃評価と Integral 攻撃の評価をニブル単位で実施し，安全性を厳密に見積もる．

結果として，Piccolo-type 構造の場合， 8 ラウンドでこれらの安全性を保証するものが最適であることを明らかにする．Piccolo も 8 ラウンドで安全性を保証可能であるため, Piccolo の RP 部はこの観点では最適であることを明らかにする．MILP での評価の結果，線形攻撃に対しては，設計者評価より 1 ラウンド短い 7 ラウンドで安全であることを示し，Integral 評価については初めて安全性を保障可能なラウンド数を導出した．さらに，不能差分に対する安全性が Piccolo と比較して，1 ラウンド少ない 7 ラウンドで達成可能な構成が 128 通りあることを示す．しかしながら，このうち 32 通りの構成は，差分/線形攻撃に対する安全性が Piccolo と比較して，1 ラウンド増える構成であり，Piccolo と同様に安全性を保証するには 8 ラウンド必要である．また，別の 64 通りについては線形攻撃に対する安全性が Piccolo と比較して，2 ラウンド増える構成であり，Piccolo と同様に安全性を保証するには 9 ラウンド必要である．それぞれのクラスを RP-1，RP-2 と定義し，表 1 に不能差分識別子が 7 ラウンドまでの RP の候補で，差分/線形，Integral 攻撃についての安全性が保障されるラウンドを示す．しかし，AS 評価は S-box での最も確率の高い線形遷移を用いた緩い評価であり，実際に 7，8 ラウンドで識別可能かは不明である．一方，不能差分攻撃では実際に 7 段の識別子が構成可能であり， 現在 Piccolo に対する解析では不能差分攻撃が最も効果的な攻撃である [2][3] ことから，新しい RP-1 と RP-2 の方が安全性の観点で優れている可能性がある．また，新しい構成では，Piccolo と比較し不能差分攻撃について安全となるラウンド数が 1 ラウンド少なくなった原因についても考察する．

本稿の構成を以下に示す．2 章で差分/線形攻撃，不能差分，Integral 攻撃について攻撃方法の概要と，その MILP を用いた評価方法について説明する．3 章では，ブロック暗号 Piccolo の仕様と，設計者による安全性評価についての説明を述べる．4 章では Piccolo の RP 部を変更した Piccolo-type 構造を定義し，Piccolo の安全性評価を改良する Piccol-type 構造の探索方法について説明する．5 章では評価結果について Piccolo と比較を交えて説明する．6, 7 章では考察を述べ，最後にまとめを述べる．

2. 準備

本章では，本研究に関する予備知識として，active S-box(AS) による差分/線形攻撃の安全性評価と不能差分攻撃，Integral 攻撃の安全性評価について説明する．

2.1 差分/線形攻撃

差分攻撃では，2 つの平文間の差分 Δx の伝搬を調べ，その出力差分 Δy から差分確率 DP_f を導出する．線形攻撃では暗号の入力マスク Γx と出力マスク Γy の線形相関から線形確率 LP_f を導出する．この操作をすべての入出力差分/マスクパターンで行い，最大差分/線形確率 DP_{fmax}, LP_{fmax} を導出する．ブロック長が b bits のブロックの暗号である場合，$DP_{fmax} \leq 2^{-b}$, $LP_{fmax} \leq 2^{-b}$ であればランダムな置換と識別がつかないため，差分/線形攻撃に対して安全であると言える．DP_f, LP_f, DP_{fmax}, LP_{fmax} は以下の式で定義される．

$$DP_f(\Delta x, \Delta y) = \frac{\#\{x \in \{0,1\}^b | f(x) \oplus f(x \oplus \Delta x) = \Delta y\}}{2^b}$$

$$LP_f(\Gamma x, \Gamma y) = \left(2\frac{\#\{x \in \{0,1\}^b | x \bullet \Gamma x = f(x) \bullet \Gamma y\}}{2^b} - 1\right)^2$$

$$DP_{max} = \max_{\Delta x \neq 0} \quad DP_f(\Delta x, \Delta y)$$

$$LP_{max} = \max_{\Gamma x \neq 0} \quad LP_f(\Gamma x, \Gamma y)$$

比較的ブロック長 b が小さい場合，最大差分確率を求めることは容易であるが，現在提案されている多くのブロック暗号が持つブロック長 64/128 ビットにおいては現実的な時間で最大差分/線形確率を導出することができない．そこで，実際の評価の際は最大差分/線形確率の近似値として，最大差分/線形特性確率 DCP_{fmax}，LCP_{fmax} が用いられる．最大差分/線形特性確率は各ラウンドの差分/線形確率の積で定義される差分/線形特性確率 DCP_f，LCP_f の最大値として定義される．r ラウンド目の入力差分/マスクを Δx_r，Γx_r その出力差分/マスクを Δx_{r+1}，Γx_{r+1} として，以下の式で定義される．

$$DCP_f = \prod_{R=1}^{r} DP_f(\Delta x_R, \Delta x_{R+1})$$

$$LCP_f = \prod_{R=1}^{r} LP_f(\Gamma x_R, \Gamma x_{R+1})$$

$$DCP_{fmax} = \max_{\substack{\Delta x_1 \neq 0 \\ \Delta x_2, \ldots, \Delta x_{r+1}}} DCP_f$$

$$LCP_{fmax} = \max_{\substack{\Delta x_1 \neq 0 \\ \Delta x_2, \ldots, \Delta x_{r+1}}} LCP_f$$

一般的に差分/線形攻撃に対する安全性の評価を行う際，AS による安全性の評価が行われる．S-box への入力差分/マスクが非 0 であるとき，その S-box を active S-box と呼ぶ．差分/線形特性確率は系全体の AS の最大差分/線形確率の積で抑えられる．遷移する可能性のあるすべての差分/マスクの伝搬を考慮し，AS 数の下界を評価することで，差分/線形特性確率の上界を評価することができる．一般的に，ブロック暗号に含まれる AS の数を保証する方法には 2 種類ある．1 つ目は理論的な証明などで示された AS 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，AS 数の下界を評価する方法である．本稿では 2 つ目の探索アルゴリズムにより，AS 数の下界を評価する方法を用いる．

2.2 不能差分攻撃

差分攻撃では，ある入力差分 Δx に対してより高い確率で伝搬する出力差分 Δy を探索する．一方，不能差分攻撃ではある入力差分 Δx に対して確率 0 で伝搬する出力差分 Δy を探索する．r ラウンドでこの入出力差分のペアが見つかったとき，それを r ラウンドにおける不能差分特性と呼び，識別攻撃が成功したとみなす．

2.3 Integral 攻撃

Integral 攻撃は，Daeman ら [4] によって初めて提案され，2002 年に Knudsen と Wagner[5] によって定式化された．Integral 攻撃は，特定の平文集合に属するすべての平文を複数ラウンド暗号化した際の中間状態の和が 0 である特性 (Integral 特性) を用いた攻撃である．Integral 攻撃では，平文集合と暗号文集合を Integral Property と呼ばれる以下の 4 つの特性に分類し，その伝搬を調べる．

- ALL($\mathcal{A}$): 取り得る全ての値が同数回出現する．
- BALANCE($\mathcal{B}$): 全ての値を XOR すれば 0 となる．
- CONSTANT($\mathcal{C}$): 全ての値が等しい．
- UNKNOWN($\mathcal{U}$): 全ての値がランダムに出現する．

その伝搬より，選択平文集合に対応する暗号文集合に現れる BALANCE($\mathcal{B}$) の特性を用い，識別攻撃を行う．2015 年，藤堂らによって提案された Division Property[6] は Integral 特性を一般化したものであり，これによって，従来より優れた Integral 識別子の構成が可能になった．Division property は以下のように定義される．

定義 1 (Division Property)．$\mathbb{X}$ を $\mathbb{F}_2^n$ の値をとる要素の多重集合とする．多重集合 $\mathbb{X}$ が Division Property$\mathcal{D}_k^n$ $(0 \leq k \leq n)$ の特性の場合，以下の条件を満たす．

$$\bigoplus_{\boldsymbol{x} \in \mathbb{X}} \pi_{\boldsymbol{u}}(\boldsymbol{x}) = \begin{cases} unknown & if\ w(u) \geq k \\ 0 & otherwise \end{cases}$$

2.4 MILP を用いた安全性評価

混合整数線形計画法 (MILP) は，ある変数について線形式で与えられた制約条件の下，線形式で与えられた目的関数を最適化（最大化もしくは最小化）する変数の値を効率的に探索することができる．MILP は，共通鍵暗号に対する様々な攻撃手法や安全性評価に適用されている．

差分/線形攻撃に対する安全性評価

AS 数の下界の評価は，MILP を用いて効率的に行うことができる．本稿では MILP ソルバーとして Gurobi Optimizer[7] を用い，提案するブロック暗号に対して，Mouha らと同様の手法 [8] を用いて，安全性の評価を行う．Mouha らが提案した手法 [8] では，まず暗号内部の各演算を線形式で表現し，制約式として MILP モデルに与える．そして目的関数として AS の合計数を MILP モデルに与え，最小化することにより AS の最小数を得る．

不能差分攻撃に対する安全性評価

不能差分攻撃に対する安全性評価手法としては，AS 評価と同様に暗号内部の各演算における差分伝搬を線形式で表現し，制約式として MILP モデルに与える．次に，入出力

差分を制約式で固定し，目的関数を与えずにこの MILP モデルを解く．与えた入出力差分に対して実行可能解が存在した時，この入出力差分の伝搬は有効であり，実行可能解が存在しない時，この入出力差分の伝搬は存在しない．したがって，与えた入出力差分の実行可能解が存在しない時，この入出力差分ペアでの不能差分識別子を発見したと言える．これを各入出力差分の組み合わせに対して行い，不能差分識別子が存在する最大ラウンド数を探索する．

Integral 攻撃に対する安全性の評価

本稿では Integral 攻撃に対する安全性の評価方法として，Division Property の伝搬を MILP に適用する方法を用いて評価を行う．まず，Division Property の伝搬を線形不等式で表現し，制約式として与える．そして，平文に任意の Division Property を与え，BALANCE の探索を行う．この時，制約式として，入力に任意の Division Property を与え，任意の出力 1 ビットに Division Property を与え，それ以外のビットを 0 とする．この整数計画モデルが実行不可能であれば，BALANCE 特性である．安全性評価を行う際は，最長ラウンドの実行不可能な整数計画モデルを考える．

3. ブロック暗号 Piccolo の仕様

Piccolo は，CHES 2011 で提案されたハードウェアで低回路規模で実装可能な軽量ブロック暗号である [1]．図 1 に，Piccolo のラウンド関数を示す．Piccolo は Generalized Feistel 構造をベースとしており，ブロック長が 64 ビットのブロック暗号で，鍵長は 80 ビットと 128 ビットに対応している．鍵長によってラウンド数は 25，31 ラウンドと異なるものの，両暗号とも鍵スケジュール部とデータ処理部の同様の処理で構成される．本章では，Piccolo の詳細な仕様と今回示す各攻撃の設計者による評価について説明を行う．

3.1 Piccolo の仕様

本節では，Piccolo の仕様について具体的に説明する．まず，図 1 で用いられている表記方法について示し，具体的な Piccolo のアルゴリズムについて説明する．

3.1.1 表記

図 1 で用いられている表記方法について以下に示す．

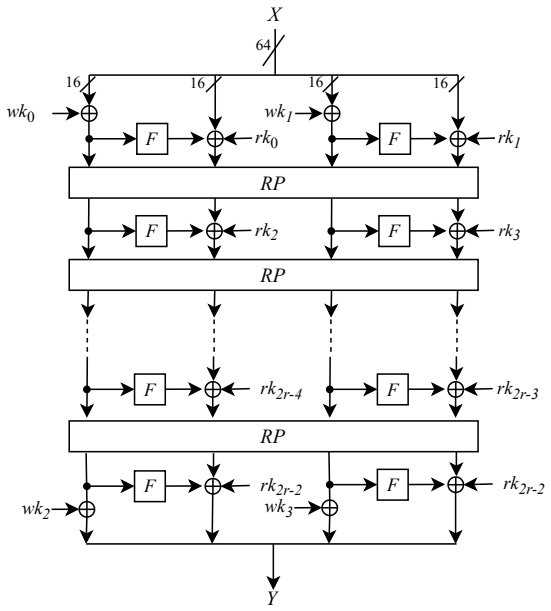

図 1 データ処理部

$a_{(b)}$: b は a のビット長

$a|b$ or $(a|b)$: a と b の連結

$a \leftarrow b$: a の値を b の値で更新

${}^t\boldsymbol{a}$: ベクトルまたは行列 $\boldsymbol{a}$ の転置

$\{a\}_b$: a を b の基数で表現

$X_{64} = (X_{0(16)}, X_{1(16)}, X_{2(16)}, X_{3(16)})$: 関数の入力

Y_{64} : 関数の出力

$F(a)$: a を F 関数に入力

$RP(a)$: ラウンド置換による a の並び替え

3.1.2 データ処理部

Piccolo のデータ処理部のアルゴリズムを図 2 に示す．まず，入力の 64 ビットを 16 ビット毎に 4 分割し，4-line Generalized Feistel 構造により暗号化が行われる．最初のラウンドでは，F 関数の入力の前にホワイトニングキーによる鍵加算処理を行う．F 関数では，2 回の S-box と 1 回の matrix による処理が行われる．通常の 4-line Generalized Feistel 構造では，16 ビット単位での並び替えが行われるが Piccolo の場合は，8 ビット (1 バイト) 単位の RP による並び替えが行われ，次のラウンドの入力に用いられる．これにより，拡散性能を向上させ，16 ビット単位のものよりも早いラウンドでの安全性達成を実現している．最終ラウンドでは，出力の前に再度ホワイトニングキーによる鍵加算処理を行い，64 ビットのビット長で出力する．

F 関数

図 3 に，F 関数の構造を示す．F 関数は，4 並列された 2 層の S-box 層とその 2 層の間の matrix 層で構成される．入力の 16 ビットが 1 層目の 4 並列された 4 ビット S-box に入力され，次に，1 層目の S-box の出力が matrix に入力

Algorithm 1 Piccolo のアルゴリズム

$X_{0(16)}|X_{1(16)}|X_{2(16)}|X_{3(16)} \leftarrow X_{64}$
$X_0 \leftarrow X_0 \oplus wk_0$
$X_2 \leftarrow X_2 \oplus wk_1$
for $i \leftarrow 0$ *to* 15 **do**
  $X_1 \leftarrow X_1 \oplus F(X_0) \oplus rk_{2i}$
  $X_3 \leftarrow X_3 \oplus F(X_2) \oplus rk_{2i+1}$
  $X_0|X_1|X_2|X_3 \leftarrow RP(X_0|X_1|X_2|X_3)$
end for
$X_1 \leftarrow X_1 \oplus F(X_0) \oplus rk_{2r-2}$
$X_3 \leftarrow X_3 \oplus F(X_2) \oplus rk_{2r-1}$
$X_0 \leftarrow X_0 \oplus wk_2$
$X_2 \leftarrow X_2 \oplus wk_3$
$Y_{64} \leftarrow X_0|X_1|X_2|X_3$

図 2 Piccolo のアルゴリズム

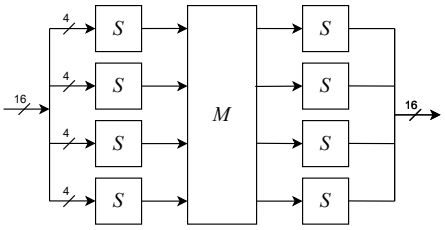

図 3 F 関数

される．matrix の出力が 2 回目の 4 並列された S-box に入力され，その出力が F 関数の出力となる．

matrix 層の入力を $X_{(16)} = x_{0(4)}|x_{1(4)}|x_{2(4)}|x_{3(4)}$，出力を $Y_{(16)} = y_{0(4)}|y_{1(4)}|y_{2(4)}|y_{3(4)}$ とすると matrix 層による演算は以下の通りである．

$$M = \begin{pmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{pmatrix}$$

$$\begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{pmatrix}$$

ラウンド置換

図 4 に RP の内部構造を示す．Piccolo の RP では 1 バイト単位で並び替えを行う．

3.2 設計者の安全性評価

Piccolo への差分/線形攻撃，不能差分攻撃，Integral 攻撃に対する設計者による安全性評価結果について説明する．

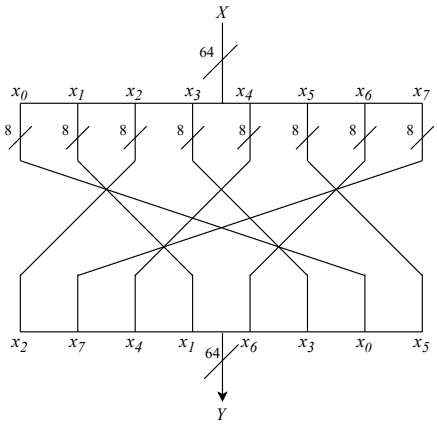

図 4 ラウンド置換

設計者による差分攻撃に対する評価では，AS による評価ではなく，active F 関数 (AF) を用いている．AF では，差分特性確率の評価に S-box の最大差分確率を用いるのではなく，F 関数の最大差分確率を用いる．Piccolo の F 関数の最大差分確率は $2^{-9.3}$ である．また，設計者評価の AF の数によると，6 ラウンドで 6 個，7 ラウンド 7 個，8 ラウンドで 8 個である [1]．したがって，差分攻撃に対して安全と見なすためには，AF の最小数が 7 個以上を満たすラウンドが必要であり，設計者評価より，7 ラウンドで差分攻撃に対する安全性要件を満たしている．

線形攻撃については F 関数の最大線形確率が 2^{-8} であり、線形攻撃に対して安全と見なすためには AF の最小数が 8 個以上を満たすラウンドが必要である．各ラウンドの AF の数は差分攻撃の時と同じであり 8 ラウンドでは 8 個であり，8 ラウンドで線形攻撃に対する安全性要件を満たしている．差分/線形ともに AS による評価は記載されていなかったため，結果ではニブル単位の MILP を用いた自身の評価も参考にする．

不能差分攻撃については最大 7 ラウンドまでの不能差分識別子が示されており、8 ラウンドで不能差分攻撃に対して安全であることが示されている．Integral 攻撃については設計者による安全性評価の詳細は記載されていない．結果ではニブル単位の MILP を用いた自身の評価と比較する．

4. Piccolo のラウンド置換の最適性の検証

Piccolo は RP をバイト単位にすることで拡散性能を高めていた．本章では，Piccolo の RP の最適性について検討する．具体的には，全ての RP の候補に対して，MILP による差分，線形，不能差分と Integral の評価を行い， 最も安全性の高い RP を探索する．ここで，ハードウェア実装で一般的なラウンド実装においては，この RP を変更は、回路規模には影響を及ぼさないので，実装時のオーバーヘッドはない．以下に，RP の探索対象とその評価方法の詳細についてそれぞれ説明する．

4.1 Piccolo-type 構造

Piccolon の RP では，64 ビットを 1 バイト単位で 8 つに分割し，図 4 のように並び替えを行っている．本稿では，全ての 1 バイト単位での並び替えを探索対象とし，全ての探索対象含む構成を Piccolo-type 構造と定義する．並び替えの組み合わせは，8 の順列であるため，$8! = 40320$ 通り存在する．この定義においては，Piccolo は Piccolo-type 構造のインスタンスの一つと分類される．また，Piccolo-type 構造の各インスタンスの違いは RP のみであるため，ハードウェアのラウンド実装においてはインスタンス間での実装上の差はない．

4.2 探索方法

40320 通りの Piccolo-type 構造に対して，差分攻撃，不能差分攻撃，Integaral 攻撃の安全性を，MILP を用いたニブル単位で評価する．しかしながら，全探索対象（$8! = 40320$ 通り）に対して，これら全ての安全性評価を行うのは膨大な計算量を要するため，Piccolo の安全性評価結果と我々の初期評価を元に効率的に探索対象の絞り込みを行う．

4.2.1 探索対象の絞り込み方法

Piccolo の提案論文 [1] より，Piccolo では不能差分識別子が 7 ラウンドまで示されており，8 段以上で安全性を達成していた．一方，差分攻撃と線形に対しては，それぞれ 7 と 8 ラウンドで安全性が保障されている．差分/線形攻撃に対する設計者による評価では AF で行われており，本論文では，より詳細な解析のため F 関数の中身まで考慮したニブル単位の AS による評価を行った．その結果，差分と線形攻撃に対しては，それぞれ 7 ラウンドで安全性が保障されるという結果になり，線形攻撃に対して安全性を保証するためのラウンド数を 1 ラウンド更新した．Integral 攻撃に関しては設計者評価は実施されていないため，MILP を用いたニブル単位で評価を行ったところ，6 ラウンドまでの Integral 識別子を発見した．

このことより，差分攻撃，不能差分攻撃，Integaral 攻撃の中で，Piccolo に対して最もラウンド数が長い攻撃方法は不能差分攻撃である．最も攻撃可能なラウンド数の長い攻撃方法において改善が出来ない限り，攻撃可能な最大ラウンド数は変化しないため，最初に Piccolo-type 構造に対して，不能差分攻撃に対する安全性評価により探索対象の絞り込みを行った上で，他の攻撃の評価を行うアプローチをとる．

4.2.2 効率的な探索手順

Piccolo では，7 ラウンドの不能差分識別子が存在するため，そのラウンド数より少ない 6 ラウンドまでしか不能差分識別子がない候補の探索を MILP 評価により，初めに行う．次に、不能差分特性が改良された構成に対して Integral 攻撃の評価として，MILP を用いた Division Property の評価を行う．Piccolo では，6 ラウンドまでの Integaral 識別子を発見したので，Piccolo-type 構造では同じ 6 ラウンドもしくはそれ以下までのラウンドの識別子を持つ構成を探索する．

差分攻撃の評価についても，不能差分が改良された構成に対して AS の評価を行う．具体的には Piccolo の S-box の最大差分確率は 2^{-2} であり，AS 数が 32 個以上になるラウンドを調べる．Piccolo は，7 ラウンドで差分攻撃に対して安全性が保障されているので [1]，Piccolo-type 構造では同じ 7 ラウンド，もしくはそれ以下のラウンドで AS が 32 個以上になる構成を探索する．

線形攻撃の評価についても，不能差分が改良された構成に対して MILP を用いた評価を行う．差分攻撃の評価と同様 AS による評価で行う．S-box の最大線形確率は 2^{-2} であり，AS が 32 個以上になるラウンドを調べる．Piccolo の AS を用いた評価では 7 ラウンドで線形攻撃に対する安全性が保障されると分かったので，Piccolo-type 構造では同じ 7 ラウンド，もしくはそれ以下までのラウンドで AS が 32 個以上になる構成を探索する．

5. 探索結果

本章では，Piccolo-type 構造に行った差分，線形攻撃，不能差分攻撃，Integral 攻撃に対する安全性評価の結果と最適な RP の探索結果について示す．

5.1 各攻撃に対する探索結果

各攻撃に対する評価による最適な探索の結果について説明する．4.2 で述べた通り，効率的な探索のため，不能差分攻撃による絞り込みを行った上で，それ以外の評価を実施する．

不能差分攻撃に対する安全性評価結果

不能差分攻撃に対する評価では，不能差分特性が最大 6 ラウンドの構成を 128 通り発見した．これは，オリジナルの Piccolo よりも最大不能差分特性が 1 ラウンド少ない結果である．この 128 のラウンド置換の集合を RP-id と定義する．

Integral 攻撃に対する安全性評価結果

128 通りの RP-id について Integral 攻撃について評価した結果，128 通りのすべての候補の Integral 識別子が最大 6 ラウンドであった．

差分攻撃に対する安全性評価結果

128 通りの RP-id に差分攻撃に対する評価を行った結果，7 ラウンドで AS が 35 個となる RP を 64 通り発見した．

線形攻撃に対する安全性評価結果

128 通りの RP-id に差分攻撃に対する評価を行った結果，8 ラウンドで安全性が保障される構成は 32 通りであった．一方，差分攻撃に対して 7 ラウンドで安全な 64 通りの RP では，線形攻撃に対して 9 ラウンドで

安全性が保障される結果になった．一方，線形攻撃に対して 8 ラウンドで安全な 32 通りの RP では，差分攻撃に対しても 8 ラウンドで安全性が保障される結果になった．R-id の集合のなかで差分/線形攻撃に対して，7/9 ラウンドで安全性が保障される構成を RP-1 と定義する．また，RP-id の集合のなかで差分/線形攻撃に対して，8/8 ラウンドで安全性が保障される構成を RP-2 と定義する．図 5 と図 6 に，それぞれ探索の結果得られた不能差分についての評価が改善された RP-1 と RP-2 の一例を示す．

5.2 最適な RP について

表 1 に Piccolo と本研究で調査した Piccolo-type 構造の RP-1 と RP-2 について，各攻撃に対して安全となるラウンド数を示す．表 1 より，Piccolo-type 構成の安全性を確保できる最小ラウンドが 8 ラウンドであることがわかる．Piccolo も 8 ラウンドで安全性を保証可能であるため，Piccolo の RP 部はこの観点では最適であることを明らかにした．一方，RP-1 と RP-2 は不能差分に対する安全性が Piccolo と比較して，1 ラウンド少ない 7 ラウンドで達成可能である．一方，線形攻撃や差分攻撃に対する安全性を保証するためのラウンド数が増加している．

しかし，AS 評価は S-box での最も確率の高い線形遷移を用いた緩い評価であり， 実際に 7，8 ラウンドで識別可能かは不明である．さらに，Piccolo の不能差分攻撃では実際に 7 段の識別子が構成可能であり， 現在 Piccolo に対する解析では不能差分攻撃が最も効果的な攻撃である [2][3] ことから，新しい RP-1 と RP-2 の方が安全性の観点で優れている可能性がある興味深いクラスである．

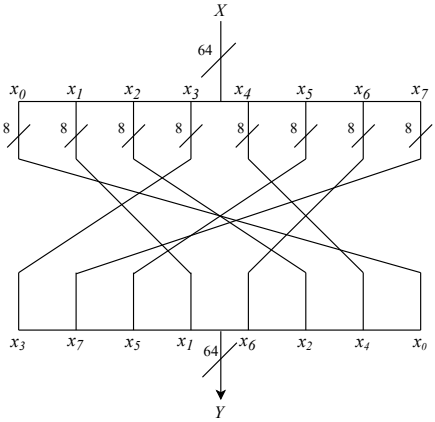

図 5 RP-1 の一例

6. 考察

攻撃可能な最大ラウンド数は変化しなかったものの，不能差分については不能差分特性が 1 ラウンド少ない構成を発見した．不能差分が改良された構成に対して，不能差分

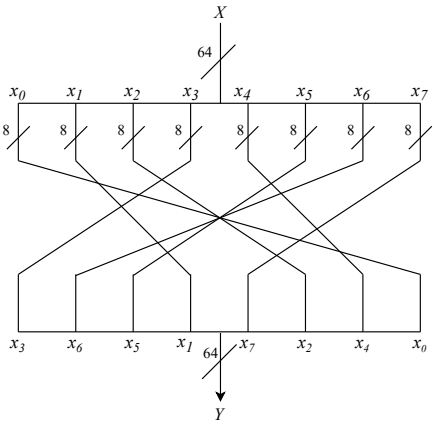

図 6 RP-2 の一例

特性が 1 ラウンド少ない結果になった理由について考察する．

初めに不能差分特性と関連性がある Full Diffusion(FD) 評価を用った．Full Diffusion とは，入力 1 か所に差分が入ったとき，差分が出力すべてに広がる最小ラウンドのことであり，すべての入力個所に対して最大のラウンドである．入力方向，出力方向の FD を調べ，そのラウンド数の和が大きいほど，不能差分特性が見つかるラウンドも大きくなる傾向がある．しかしながら，追加検証の結果，Piccolo，Piccolo-type 構造のどちらの入力方向，出力方向の FD の特性も 4 ラウンドのであり，FD 特性での差異は見つからなかった．

そこで，詳しく不能差分における差分の伝搬の内部構造レベルの解析を実施した．入力の差分に対する出力の差分の発生確率が 0 である場合、不能差分特性として評価される． そのため，不能差分特性を探索する際は，入力方向と出力方向から差分の伝搬を考え，任意の中間値で矛盾が生じたときに不能差分特性とする．実際に，Piccolo と Piccolo-type 構造の違いである 7 ラウンドでの Piccolo の不能差分があるパスの構造を解析し，Piccolo-type 構造ではそれがなぜ発生しないのかを調べる．

図 7 は Piccolo の入力方向，出力方向からの 4 ラウンド目の出力の差分の状態の一例を記した図である．図中の A は差分が active であることを示す．U_1 は U_1 単体で考えると差分の状態は不定であるが，U_1 の中では差分が 2 つ以上含む条件を示す．U_2 も同様に U_2 単体で考えると差分の状態は不定であるが，U_2 の中では差分が 3 つ以上含む条件を示す．Piccolo の 7 ラウンドにおける不能差分は偶数ブランチの入出力に差分を固定した時に不能差分識別子が長いラウンドで見つかりやすく，その時に，中間値で偶数ブランチのどちらかのブランチの入力側と出力側から見た差分がすべて 0 で固定される図 7 のような結果に陥る．図 7 では左から 2 番目のブランチの入出力に差分がないという条件であるが，F 関数には必ず差分が入力され出力に差分が現れるため，不能差分となる．

一方，Piccolo-type 構造では偶数ブランチの入力側，出力側から見た差分がばらけやすく図 8 のような中間値に帰着する．この差分状態の場合は伝搬が起こり得る確率があるため，不能差分とならない．以上より FD 特性は同じ 4 ラウンドのであるが，今回発見した Piccolo-type 構造の方が，不能差分特性が出にくい並び替えであることが考えられる．

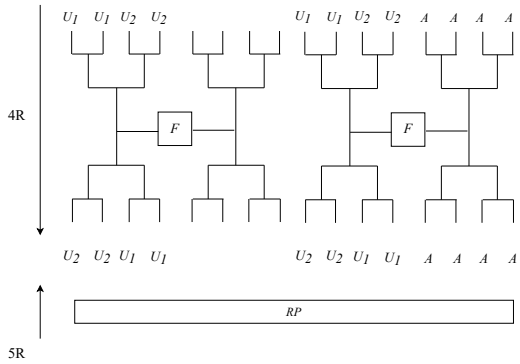

図 7 Piccolo 不能差分伝搬の例

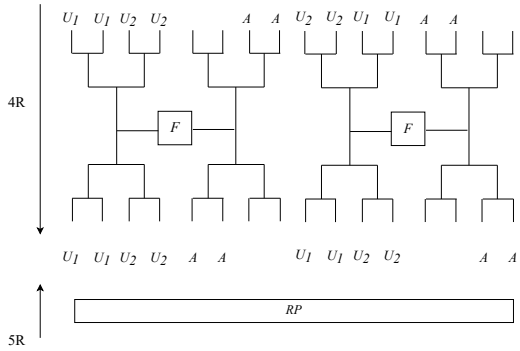

図 8 Piccolo-type 構造の差分伝搬の例

7. まとめ

本稿では，RP の変更による Piccolo-type 構造で，差分/線形攻撃，不能差分攻撃，Integral 攻撃に対して評価を行い．安全性の観点でバイト単位での RP の最適性の検証を行った．結果として，Piccolo の RP がこれらの攻撃に対する安全性を保障するラウンド数の観点で最適であることを明らかにした．さらに、不能差分に対する安全性が Piccolo と比較して，1 ラウンド少ない 7 ラウンドで達成可能な 2 つのクラスの構成を示した．これらの構成は差分/線形攻撃に対する安全性を保障するためにはそれぞれ 7/9 と 8/8 ラウンドが必要な構成であり， Poccolo よりも多くのラウンド数を要する．しかし，本研究のでの差分/線形攻撃への評価は， 差分/線形確率が最も高い遷移のみを仮定した設計者にとってワーストケースでの評価であり，実際に 8 ラウンドもしくは 7 ラウンドで識別可能かは不明である．よって，実際に 7 ラウンドの不能差分識別子のある Piccolo のものよりも，新しい PR の方が安全性の観点で優れている可能性も十分高い．

今後の課題としては，Piccolo-type 構造の差分/線形攻撃に対する詳細な評価や，Piccolo の RP をバイト単位ではなくニブル/ビット単位での並び替えに変更した構成を考え，その構成に対して Piccolo の RP が最適であるのか，もしくは安全性評価が改善 RP があるのかを調査が挙げられる．

謝辞 本研究は，総務省の「電波資源拡大のための研究開発（JPJ000254）」における委託研究「安全な無線通信サービスのための新世代暗号技術に関する研究開発」の成果の一部である．本研究は JST さきがけ（JPMJPR2031）の助成を受けたものである．本研究は科研費特別研究員奨励費（20J23526）の助成を受けたものである．

参考文献

[1] Shibutani, K., Isobe, T., Hiwatari, H., Mitsuda, A., Akishita, T. and Shirai, T.: Piccolo: An Ultra-Lightweight Blockcipher, *Cryptographic Hardware and Embedded Systems – CHES 2011* (Preneel, B. and Takagi, T., eds.), Berlin, Heidelberg, Springer Berlin Heidelberg, pp. 342–357 (2011).

[2] 伊藤竜馬：CRYPTREC　暗号技術ガイドライン（軽量暗号）」掲載の暗号方式に関する安全性評価の動向調査, https://www.cryptrec.go.jp/exreport/cryptrec-ex-3101-2021.pdf (2022).

[3] Azimi, S. A., Ahmadian, Z., Mohajeri, J. and Aref, M. R.: Impossible differential cryptanalysis of Piccolo lightweight block cipher, *2014 11th International ISC Conference on Information Security and Cryptology*, pp. 89–94 (online), DOI: 10.1109/ISCISC.2014.6994028 (2014).

[4] Daemen, J., Knudsen, L. R. and Rijmen, V.: The Block Cipher Square, *FSE '97* (Biham, E., ed.), Lecture Notes in Computer Science, Vol. 1267, Springer, pp. 149–165 (online), DOI: 10.1007/BFb0052343 (1997).

[5] Knudsen, L. R. and Wagner, D. A.: Integral Cryptanalysis, *FSE 2002* (Daemen, J. and Rijmen, V., eds.), Lecture Notes in Computer Science, Vol. 2365, Springer, pp. 112–127 (online), DOI: 10.1007/3-540-45661-9_9 (2002).

[6] Todo, Y.: Structural Evaluation by Generalized Integral Property, *EUROCRYPT 2015* (Oswald, E. and Fischlin, M., eds.), Lecture Notes in Computer Science, Vol. 9056, Springer, pp. 287–314 (online), DOI: 10.1007/978-3-662-46800-5_12 (2015).

[7] Inc., G. O.: Gurobi Optimizer 6.5, Official webpage, `http://www.gurobi.com/` (2015).

[8] Mouha, N., Wang, Q., Gu, D. and Preneel, B.: Differential and Linear Cryptanalysis Using Mixed-Integer Linear Programming, *Inscrypt 2011* (Wu, C., Yung, M. and Lin, D., eds.), Lecture Notes in Computer Science, Vol. 7537, Springer, pp. 57–76 (online), DOI: 10.1007/978-3-642-34704-7_5 (2011).