低遅延暗号 Gleeok の差分攻撃に対する安全性評価

森田 健斗[1,a)]　石川 達也[2]　白矢 琢朗[2]　阪本 光星[2,3]　伊藤 竜馬[2,4]　五十部 孝典[2]

概要：本稿では，CHES2024 で提案された低遅延擬似乱数関数である Gleeok-128 および Gleeok-256 に対し，差分攻撃に対する安全性評価を行う．具体的には，設計論文では計算量上の制約により実施できなかった，高ラウンドにおける差分特性確率の評価に取り組む．最大差分特性確率を示す差分伝搬から得られる特徴を制約として SAT ソルバーに導入することで探索空間を効率的に削減し，Gleeok-128 の Branch1 および Branch2，ならびに Gleeok-256 の各 Branch において，高ラウンドにおける最良の差分特性を特定する．さらに，Gleeok-128 の Branch3 については，設計論文では未評価であったフルラウンドにおける最大差分特性確率を初めて示す．識別攻撃の観点では、Gleeok-128 に関して全ての Branch で既存結果を上回る攻撃を示し、Gleeok-256 に関しても Branch3 で従来を上回る攻撃を実現する．

キーワード：疑似乱数関数，差分解析，差分特性確率，SAT ソルバー，識別攻撃

Security Evaluation of the Low-Latency Cipher Gleeok Against Differential Attacks

Kento Morita[1,a)]　Tatsuya Ishikawa[2]　Takuro Shiraya[2]　Kosei Sakamoto[2,3]　Ryoma Ito[2,4]
Takanori Isobe[2]

Abstract: This paper evaluates the security of Gleeok128 and Gleeok256, low-latency pseudorandom functions proposed at CHES 2024, against differential attacks. Specifically, we investigate the differential characteristic probabilities for a higher number of rounds than was computationally feasible in the original design paper. By incorporating features derived from the differential propagation that exhibits the maximum differential characteristic probability as constraints for a SAT solver, we efficiently prune the search space. This approach allows us to identify the best differential characteristics for high-round variants of Gleeok128's Branch1 and Branch2, as well as for each Branch of Gleeok256. Furthermore, for Branch3 of Gleeok128, we present the first-ever maximum differential characteristic probability for the full number of rounds, which was not evaluated in the original paper. In the context of distinguishing attacks, we demonstrate attacks on all Branches of Gleeok128 that outperform existing results, and we also achieve an improved attack on Branch3 of Gleeok256.

Keywords: Pseudorandom Function, Differential Cryptanalysis, Differential Characteristic Probability, SAT Solver, Distinguishing Attack

1. はじめに

1.1 背景

IoT デバイスやリアルタイム制御システムなどの普及に伴い，低遅延で動作する暗号技術の重要性が増しており，PRINCE [7],QARMA [2],QARMAv2[3],Mantis [5],Orthros [4] など多くの低遅延暗号が提案されている．

[1] 兵庫県立大学
University of Hyogo, Japan
[2] 大阪大学
The University of Osaka, Japan
[3] 三菱電機株式会社
Mitsubishi Electric Corporation, Japan
[4] NICT
NICT, Japan
[a)] moritakent0515@gmail.com

表 1: 本研究における差分特性確率の重みのまとめ．青字は 4.1 節の探索よる最大差分特性確率の重み，赤字は 6.1 節の探索による差分特性確率の下限値の重みを示す．

Variant	Branch	Rounds																Ref.
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	
Gleeok-128	Branch1	2	8	24	50	≤ 67	69	75	100	-	-	-	-	-	-	-	-	[1]
		2	8	24	50	**81**	**115**	-	-	-	-	-	-	-	-	-	-	4.1 節/6.1 節
	Branch2	2	8	24	50	≤ 66	69	75	100	-	-	-	-	-	-	-	-	[1]
		2	8	24	50	**81**	**115**	-	-	-	-	-	-	-	-	-	-	4.1 節/6.1 節
	Branch3	2	8	20	32	36	48	52	64	-	-	-	-	-	-	-	-	[1]
		2	8	20	32	36	48	52	64	68	80	84	96	100	112	116	128	4.1 節
Gleeok-256	Branch1	2	8	26	≤ 66	68	74	92	132	-	-	-	-	-	-	-	-	[1]
		2	8	26	**80**	**154**	-	-	-	-	-	-	-	-	-	-	-	4.1 節/6.1 節
	Branch2	2	8	26	≤ 65	67	73	91	128	-	-	-	-	-	-	-	-	[1]
		2	8	26	**80**	**154**	-	-	-	-	-	-	-	-	-	-	-	4.1 節/6.1 節
	Branch3	2	8	20	39	61	≤ 71	74	81	-	-	-	-	-	-	-	-	[1]
		2	8	20	39	61	**95**	**130**	**174**	-	-	-	-	-	-	-	-	4.1 節/6.1 節

CHES 2024 で提案された Gleeok [1] は, 量子コンピュータへの耐性を持ちながら低遅延を実現する擬似ランダム関数 (PRF) である．一般に, 低遅延暗号はラウンド数が制限されるため, 差分攻撃に対する安全性を十分に主張することが重要な課題となる．Gleeok はこの課題に対し, 3 つの独立した置換 (Branch) の出力を合成する 3 branch 構造と, ビットレベルで最適化された鍵付き置換の設計という 2 つの戦略を採用している．しかし、3-branch 構造に由来する大規模な内部状態のため、差分特性確率の導出において主流である SAT ソルバーによる全探索評価は計算量的に困難である．さらに、ビット単位の置換を用いるという構造的特徴により、active S-box 数に基づく評価手法の計算量削減効果も限定的であり、安全性の詳細な評価を難しくしている．提案論文 [1] では、**表 1** に示すように、自動探索ツールを用いて各 Branch の最大差分特性確率を評価している．しかし、その計算量の膨大さから評価は限定的であり、多くのバリアントでは小ラウンドに対してのみ正確な値が得られ、それ以上では上界の提示に留まっている．例えば、Gleeok-128 の Branch1 および Branch2 では 5 ラウンド以降、Gleeok-256 の各 Branch では 4 または 6 ラウンド以降の最大差分特性確率が特定されておらず、安全性を議論するには不十分な状況にある．

したがって、十分なラウンド数に対する最大差分特性確率を明らかにし、Gleeok の差分攻撃耐性を具体的に評価することが、重要な未解決問題として残されている．

1.2 貢献

本稿では、Gleeok の差分伝搬特性を詳細に分析し、その知見に基づく効率的な探索手法を提案することで、従来評価が困難であったラウンド数における安全性を明らかにする．このように、暗号の構造的特徴を探索指針として活用し、計算量的に実行可能なサブ問題へ分割する手法は、近年の暗号評価における重要な研究動向である [8].

本研究は二段階のアプローチから成る．第一に、SAT ソルバーを用いた最大差分特性確率の探索を通じて差分伝搬を詳細に分析し、高確率で成立する伝搬が持つ複数の特徴的な構造を特定する．第二に、これらの構造的特徴を探索空間への制約として導入する手法を提案し、全探索が困難なラウンドにおける高確率な差分伝搬の探索を可能にする．

本稿の主要な結果は表 1 に色付き文字で示す．また、**表 2** では提案論文 [1] における識別攻撃の結果と本研究の成果を整理し、新たに得られた結果を赤字で示す．

本稿では，全探索により Gleeok-128 の Branch3 の評価を拡張し, 16 ラウンドまでの最大差分特性確率を示した．また, 提案した効率的探索手法を適用することで, これまで計算量的に評価が不可能であった Gleeok-128 の Branch1 , Branch2 および Gleeok256 の全 Branch において, 特定のラウンドにおける差分特性確率の下限値を初めて導出した．Gleeok-128 に関しては，全てのブランチに置いて既存結果よりも優れた識別攻撃を実現し，Gleeok-256 に関しては Branch3 のみ既存結果を上回る識別攻撃を示した．

これらの結果は, Gleeok に対するより具体的な安全性の指標を提供すると同時に, ビット指向暗号の効率的な評価手法としての本研究のアプローチの有効性を実証するものである．

2. 準備

本章では，差分特性確率の導出を行うための前提知識である差分攻撃について説明する．その後，SAT ソルバーを用いた安全性評価およびそのモデリングについて説明する．

表 2: Gleeok の各 Branch に対する識別攻撃まとめ．赤字は本稿により新たに得られた結果を示す．

variant	Branch	Round	Method	Time/Data	Ref.
Gleeok-128-10	Branch1	4	Integral	2^{-64}	[1]
		4	Differential	2^{-50}	[1]
	Branch2	4	Integral	2^{-64}	[1]
		4	Differential	2^{-50}	[1]
	Branch3	5	Integral	2^{-64}	[1]
		8	Differential	2^{-64}	[1]
Gleeok-128-12	Branch1	6	Integral	2^{-127}	[1]
		6	Differential	2^{-115}	6.1 節
	Branch2	6	Integral	2^{-127}	[1]
		6	Differential	2^{-115}	6.1 節
	Branch3	6	Integral	2^{-127}	[1]
		16	Differential	2^{-128}	4.1 節
Gleeok-256-12	Branch1	5	Integral	2^{-128}	[1]
		4	Differential	2^{-80}	6.1 節
	Branch2	5	Integral	2^{-128}	[1]
		4	Differential	2^{-80}	6.1 節
	Branch3	5	Integral	2^{-128}	[1]
		6	Differential	2^{-95}	6.1 節
Gleeok-256-16	Branch1	6	Integral	2^{-255}	[1]
		5	Differential	2^{-154}	6.1 節
	Branch2	6	Integral	2^{-255}	[1]
		5	Differential	2^{-154}	6.1 節
	Branch3	5	Integral	2^{-255}	[1]
		8	Differential	2^{-174}	6.1 節

2.1 差分攻撃

差分攻撃 [6] は Biham および Shamir によって提案されたブロック暗号に対する攻撃手法である．入力差分を変化させたときの出力差分の偏りを利用した攻撃であり，ブロック暗号は差分攻撃に対して安全であることが求められている．差分とは 2 つの入力の排他的論理和を取ったものであり，差分 Δx をブロック長が n ビット入出力の関数 f に入力したとき，出力が $\Delta x'$ になるような確率を差分確率という．

差分確率 DP_f の定義を以下に示す．

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

差分攻撃に対する安全性評価を行う際は，全ての入出力差分の組み合わせに対する差分確率の最大値である最大差分確率を求める．入力ビット数が小さいものであれば最大差分確率を求めることは容易であるが，256 ビットや 512 ビットのような入力長が大きい暗号の場合，計算量が膨大になってしまうため最大差分確率を求めることは困難である．そのため，最大差分確率の近似値である最大差分特性確率を用いて安全性評価を行うことが一般的である．差分特性確率 DCP_f とその最大値である最大差分特性確率 DCP_{max} の定義を以下に示す．ここで，Δx_r と Δx_{r+1} はそれぞれ r ラウンド目の入力差分と出力差分を示している．

$$DCP_f = \prod_{r=0}^{R-1} DP_f(\Delta x_r, \Delta x_{r+1})$$

$$DCP_{\max} = \max_{\substack{\Delta x_0 \neq 0 \\ \Delta x_2, \ldots, \Delta x_R}} DCP_f$$

2.2 SAT ソルバーを用いた安全性評価

共通鍵暗号に対する安全性評価の手法の一つとして，数理ソルバーを用いた方法がある．本稿では，2022 年に Sun らによって充足可能性問題 (SAT) を用いた自動探索手法が提案された手法を用いる [10]．この SAT ソルバーを用いた手法は，これまで計算量の問題で探索範囲を限定していた評価に対して，全探索範囲による解析が可能である．

2.3 SAT モデリング

SAT とはバイナリ変数により与えられたブール式が真となる変数割り当てが存在するかどうかを判定する問題であり，ブール式は連言標準形 (CNF) 表現で与えられる．SAT ソルバーを差分解析に用いるには，Sbox や XOR などの暗号を構成する論理式を CNF 表現に変換してブール式を作成する必要があり，XOR などの基礎的な演算やブール基数制約の CNF モデリングは Sun らにより提案されている [10]．また，最大差分特性確率はインクリメント変数 k を用意し，k を差分特性確率の制約する．そして，発生した差分特性確率が k 以下となるまで k を増加させることで導出できる．最大差分特性確率の導出に関する CNF モデリングは，PySAT[9] のモジュールである CardEnc によって容易に作成できる．また，本稿では，ラウンド関数の入力に対するハミング重みを縛る制約を用いている．これは，各ラウンド関数の入力として割り振られた論理変数を，PySAT[9] のモジュールである CardEnc の equals 関数に引数として渡すことで容易に導入が可能である．

3. 評価対象

本章では, 評価対象である Gleeok のバリアントやその構造, 鍵スケジュールについて紹介し，主張されている安全性や既存の安全性評価を把握する．

3.1 Gleeok のバリアント

Gleeok には大きく 4 つのバリアントがある．まず, ブロック長が 128 ビットの Gleeok-128 と 256 ビットの Gleeok-256 がある．さらにその中で，データ量が制限された使用環境を想定した Gleeok-128-10 （データ量が 2^{64} 以下）と Gleeok-256-12（データ量が 2^{128} 以下），フルラウンドである Gleeok-128-12 と Gleeok-256-16 の 4 つのバリアントが設定されている．

3.2 Gleeok-128 および Gleeok-256 の構造

Gleeok の全体構造は, 3 つの独立した鍵付き置換, すなわち Branch1, Branch2, Branch3 の出力を XOR することにより, 最終的な暗号文を生成する.Gleeok-128 および Gleeok-256 ではこの各 Branch のブロック長が 128 ビット, 256 ビットである．

各 Branch は SPN 構造を持つ．ラウンド関数 R は, 非線

表 3: Branch1 , Branch2 , Branch3 における S-box.

(a) S-box S_3.

x	0	1	2	3	4	5	6	7
$S_3(x)$	0	5	3	2	6	1	4	7

(b) S-box S_4.

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$S_4(x)$	1	0	2	4	3	8	6	d	9	a	b	e	f	c	7	5

(c) S-box S_5.

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$S_5(x)$	0	5	a	b	14	11	16	17	9	c	3	2	d	8	f	e
x	10	11	12	13	14	15	16	17	18	19	1a	1b	1c	1d	1e	1f
$S_5(x)$	12	15	18	1b	6	1	4	7	1a	1d	10	13	1e	19	1c	1f

形層である S-box (S), 線形層である 3 入力 XOR (θ) とビット置換 (π), および鍵加算 (RK_{xor}) と定数加算 (RC_{xor}) から構成され, 以下の式で表現される.

$$R = RC_{xor} \circ RK_{xor} \circ \pi \circ \theta \circ S$$

各層の仕様は以下の通りである.

- **S-box (S):** S-box の構成は Branch ごとに異なる. Branch1 と Branch2 では 3 ビット S-box (S_3) と 5 ビット S-box (S_5) が交互に適用される. 一方, Branch3 では 4 ビット S-box (S_4) が一律に適用される. S-box の詳細は**表 3** に示す.
- **3-input XOR (θ):** 内部状態から 3 つの異なる位置のビットを XOR する演算であり, XOR の入力値はブロック長や Branch ごとに異なる.
- **Permutation (π):** ビット単位の置換であり, そのパターンはブロック長や Branch ごとに異なるパラメータで定義される.

いずれにおいても, 最終ラウンドでは線形層が省略される.

3.2.1 Gleeok-128 および Gleeok-256 の鍵スケジュール

Gleeok-128 および Gleeok-256 では, 置換ベースの鍵スケジュール関数を採用している. Gleeok-128 では, 256 ビット鍵 K が, 各 Branch で異なる方法で 2 つの 128 ビット鍵, すなわち K_0 と K_1 に分割され, それぞれが交互に置換に適用されてラウンド鍵を生成する. また, Gleeok-256 では, 256 ビット鍵がそのまま各ラウンドで置換に適用されてラウンド鍵を生成する.

3.3 差分攻撃に対して主張している安全性

Gleeok-128 と Gleeok-256 は、それぞれ確率が 2^{-128} および 2^{-256} 未満となる差分特性を持つように, 4 つのバリアントにおけるラウンド数が設定されている.

3.4 差分攻撃に対する既存の安全性評価

提案論文 [1] における安全性評価では, SAT ソルバーを用いた自動探索ツールにより, ビットレベルでの最大差分特性確率が探索された. その結果を表 1 に示す. 探索された最大差分特性確率は黒字で, 複数ラウンドの積によって求められた上界値は灰色で示している. 表 1 が示すように, 提案論文 [1] における評価は限定的である.

具体的には, Gleeok-128 において, Branch1 および Branch2 では 4 ラウンドまでの最大差分特性確率が算出されているものの, 5 ラウンド目についてはそれぞれ $DCP \leq 2^{-67}$ および $DCP \leq 2^{-66}$ という上界値が示されているに過ぎない. また, Branch3 では 8 ラウンドまでの最大差分特性確率が報告されているが, 8 ラウンド目における最大差分特性確率は 2^{-64} と依然として高く, 安全性を論じるには不十分である. それにもかかわらず, それ以上のラウンドでは評価が行われていない.

Gleeok-256 においても同様の課題が見られ, Branch1 と Branch2 および Branch3 において, 4 ラウンドおよび 6 ラウンド目以降は, それぞれ $DCP \leq 2^{-66}$, $DCP \leq 2^{-65}$, $DCP \leq 2^{-65}$ という上界値が示されるに留まっている. したがって, いずれのバリアントにおいても, 十分な安全性マージンを保証するラウンド数が明確に示されているとは言えない状況である.

4. 差分伝搬特性の分析

本章では, Gleeok の差分伝搬特性を分析し, 効率的な安全性評価に繋がる知見を得ることを目的とする. まず, 各 Branch における最大差分特性確率を探索し, 現実的な計算量の範囲内で評価可能なラウンド数を特定する. 次に, その探索で得られた最大差分特性確率を導出する差分伝搬をハミング重み (HW) に注目して, 分析する.

4.1 最大差分特性確率の探索

提案論文 [1] と同様の条件下で, Gleeok の各 Branch における最大差分特性確率 (DCP) を探索する. その結果を表 1 に青字で示す.

Gleeok-128 の Branch1 と Branch2 及び Gleeok-256 の各 Branch における探索では, 計算量の膨大さから, 提案論

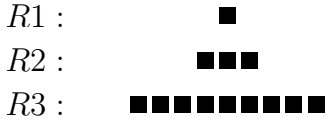

図 1: Gleeok-256 Branch1 の 3 ラウンドで観察された HW 遷移 ($1 \to 3 \to 9$).

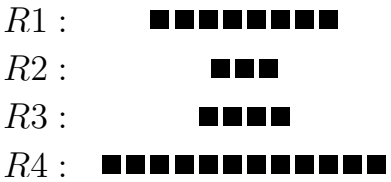

図 2: Gleeok-128 Branch1 の 4 ラウンドで観察された HW 遷移 ($8 \to 3 \to 4 \to 12$).

文 [1] の結果 (表 1) と同様の評価に留まった．一方で，Gleeok-128 の Branch3 では 16 ラウンドまでの最大差分特性確率を導出できた．

これらの探索により，Gleeok-128 の Branch3 以外の Branch においては，大きなラウンドにおける最大差分特性確率を導出することが計算量の膨大さにより困難であることが明らかになった．

4.2 差分伝搬の分析

Gleeok-128 の Branch3 以外の Branch を対象に，4.1 節で得られた最大差分特性確率を導出する差分伝搬について，そのハミング重み（HW）に着目して分析する．初めに差分伝搬の観察結果を述べ，次に観察から見出された特徴的な構造を抽出し定義する．本分析の目的は，より高い確率を有する差分特性を探索するための知見を得ることである．

4.2.1 最大差分特性確率を導出する差分伝搬の観察

4.1 節で得られた差分伝搬について，各ラウンドにおける差分値の HW の遷移を観察した結果，いくつかの特徴的な遷移が確認された．まず，Gleeok-128 の Branch1, Branch2 および Gleeok-256 の Branch1, Branch2 の 1-3 ラウンドと，Gleeok-256 の Branch3 の 1-2 ラウンドでは，**図 1** のとおり，入力差分の HW が 1 からラウンドの経過とともに増加するような差分伝搬が観察された．

次に，Gleeok-128 の Branch1, Branch2 の 4 ラウンドと，Gleeok-256 の Branch3 の 3-4 ラウンドでは，**図 2** および **図 3** に示すように，HW が一度減少した後に再び増加する遷移が観察された．さらに，Gleeok-256 の Branch3 の 5 ラウンドにおいては，**図 4** に示すように，HW が複数ラウンドにわたり一定の値で維持される遷移が観察された．

4.2.2 構造の定義

観察から得られた特徴的な構造をそれぞれ以下のように定義する．

拡散構造　HW が 1 など小さい値から始まり，ラウンドを経るごとに単調に増加する構造 (図 1 参照).

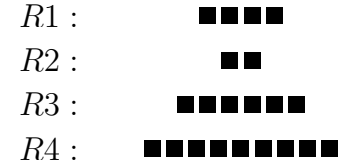

図 3: Gleeok-256 Branch3 の 4 ラウンドで観察された HW 遷移 ($4 \to 2 \to 6 \to 9$).

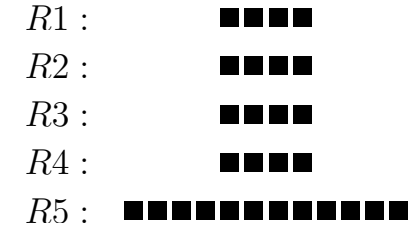

図 4: Gleeok-256 Branch3 の 5 ラウンドで観察された HW 遷移 ($4 \to 4 \to 4 \to 4 \to 12$).

くびれ構造　伝搬の途中ラウンドで HW が一時的に減少し，その後再び増加する遷移パターンを持つ構造 (図 2, 図 3 参照).

プラトー構造　中間ラウンドで HW が特定の値のまま，複数ラウンドにわたって維持される構造 (図 4 参照).

5. 効率的な差分特性の探索手法の提案

本章では，前章の差分伝搬の分析に基づき，探索空間を削減する探索手法を提案する．本手法の目的は，計算コストを抑制しつつ，全探索が困難な大きなラウンドにおける差分伝搬を効率的に探索することにある．

5.1 提案手法の方針

提案手法の基本的な方針は，その Branch において，4.1 節で探索した中で最大ラウンドの「最大差分特性確率を導出する差分伝搬の HW 遷移」を制約として用いることで探索空間を削減することである．ただし，この方針では，すべての探索空間の評価を実施していないため，導出した差分特性確率が最大差分特性確率であるかは不明である．

そこで本稿では，その制約された構造から，最大差分特性確率の本質を捉える「エッセンス」に注目し，探索空間を段階的に可能な限り広げていくことで，最大差分特性確率との差を抑制することを目指す．

5.2 エッセンスの定義

差分特性確率を高く維持する目的において，アクティブ S-box 数を少なくするために，全体的な HW を低く維持することが理想的である．この観点から，最大差分特性確率を導出する差分伝搬構造において，全体的な HW を低く維持するために最も重要となる部分を「エッセンス」として定義する．各構造のエッセンスは，既知の最大差分特性を

与える差分伝搬に基づき, 以下のように定義される.

- **拡散構造:** 入力差分 HW が最小であることがその後の拡散 HW 数の抑制につながるため, 差分伝搬の入力 HW をエッセンスとする.
- **くびれ構造:** くびれ部分の HW が最小であることが減少ラウンドや拡散ラウンドにおける HW 数の抑制につながるため, 差分伝搬のくびれ部分の HW をエッセンスとする.
- **プラトー構造:** 複数ラウンドにわたり低い HW を維持することが重要であるため, 同一 HW を維持する部分をエッセンスとする.

5.3 具体的な探索手法

本稿の探索は, 以下の 4 ステップで実行される.

(1) **基本探索パターンの定義:** まず, 各 Branch において, 4.1 節で探索した中で最大ラウンドの「最大差分特性確率を導出する差分伝搬の HW 遷移」を基本探索パターンとして定義する.

(2) **サブパターンの階層的導出:** 次に, この基本パターンから 5.2 節で定義したエッセンスを除く HW 制約を段階的に緩和し, 制約強度の異なる複数のサブパターンを階層的に導出する. 例えば, 4 ラウンドの HW 遷移パターン $(h_1 \to h_2 \to h_3 \to h_4)$ からは, より制約の緩い 3 ラウンドパターン $(h_1 \to h_2 \to h_3)$ や, 単一ラウンドの HW (h_2) といったサブパターンが得られる.

(3) **最適なパターンの選出:** 最終的に, 全パターンの探索結果から, 未評価ラウンドを評価できたもののうち最も制約の緩いパターンを本稿の評価で使用する制約とする.

(4) **結果の導出:** 選出された制約を用いて，計算が可能な限り差分特性確率を導出する.

本アプローチは, 計算量的に許容される最も緩い制約下での評価値を採用することにより, 特定の強い制約下でのみ現れる局所解を避け, より信頼性の高い評価を得ることを目的とする.

5.4 各 Branch における制約の設定

本節では，前節で提案した探索手法の (3) 最適なパターンの選出までを行い，各 Branch において適切な制約を設定する.

5.4.1 Gleeok-128 Branch1 と Branch2 の探索

(1) **基本探索パターンの定義:** 4.1 節で探索可能であった中で，最大ラウンドである 4 ラウンドで最大差分特性確率を与えた差分伝搬が HW 遷移 $(8 \to 3 \to 4 \to 12)$ を持つ「くびれ構造」(図 2) であったことから, これを基本探索パターンとして定義する.

(2) **サブパターンの設定と探索:** 次に, 基本パターンから制約を段階的に緩和した以下の 4 つのサブパターンを設定し, それぞれの条件下で探索を実行する.

パターン A: 連続 4 ラウンドの HW 遷移を $(8 \to 3 \to 4 \to 12)$ に制約.

パターン B: 連続 3 ラウンドの HW 遷移を $(8 \to 3 \to 4)$ に制約.

パターン C: 連続 2 ラウンドの HW 遷移を $(8 \to 3)$ または $(3 \to 4)$ に制約.

パターン D: 1 ラウンドの HW を 3 に制約（エッセンスに相当）.

(3) **制約の選出:** パターン D では計算資源の制約から評価ラウンドの探索が困難であった. そのため, 評価可能であったパターンのうち最も制約の緩いパターン C を用いる.

5.4.2 Gleeok-256 Branch1 と Branch2 の具体的な探索

(1) **基本探索パターンの定義:** 4.1 節で探索可能であった中で，最大ラウンドである 3 ラウンドで最大差分特性確率を与えた差分伝搬が HW 遷移 $(1 \to 3 \to 9)$ を持つ「拡散構造」(図 1) であったことから, これを基本探索パターンとして定義する.

(2) **サブパターンの設定と探索:** 次に, 基本パターンから制約を段階的に緩和した以下の 3 つのサブパターンを設定し, それぞれの条件下で探索を実行する.

パターン F: 入力から 3 ラウンドの HW 遷移を $(1 \to 3 \to 9)$ に制約.

パターン G: 入力から 2 ラウンドの HW 遷移を $(1 \to 3)$ に制約.

パターン H: 入力ラウンドの HW を 1 に制約（エッセンスに相当）.

ただし，4.2 節でラウンド数の増加によりくびれ構造への変化も確認されることから，本 Branch ではくびれ構造に注目した探索も有効であると考えられる．Gleeok-256 (Branch1,Branch2) と Gleeok-128 (Branch1,Branch2) は同じ非線形層を持つため，くびれ構造をとらえた探索を行う目的でパターン C を含めた探索を行う.

(3) **制約の選出:** 「拡散構造」に注目した探索の中で評価可能なパターンの内，最も制約の緩いパターン H であったが，パターン C の方が高い差分特性確率を得られたため，パターン C を用いる.

この結果は当該ラウンドにおいて拡散構造よりくびれ構造の方が高い差分特性確率を与えることを示唆する.

5.4.3 Gleeok-256 Branch3 の具体的な探索

(1) **基本探索パターンの定義:** 4.1 節で探索可能であった中で, 最大ラウンドである 5 ラウンドで最大差分特性確率を与えた差分伝搬が HW 遷移 $(4 \to 4 \to 4 \to 4 \to 12)$ を持つ「プラトー構造」であったことから, これを基本探索パターンとして定義する.

(2) **サブパターンの設定と探索:** 次に, 基本パターンから

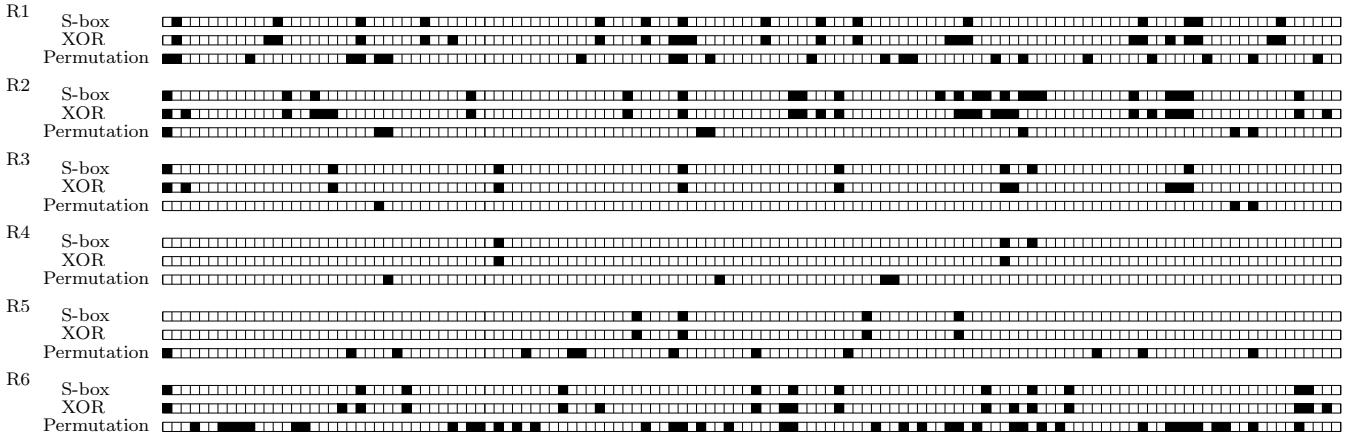

図 5: 6.1 節で得られた Gleeok-256 Branch1 の 5 ラウンドの差分伝搬.

制約を段階的に緩和した以下の 2 つのサブパターンを設定し, それぞれの条件下で探索を実行する.

パターン I: 連続 5 ラウンドの HW 遷移を $(4 \to 4 \to 4 \to 4 \to 12)$ に制約.

パターン J: 連続 4 ラウンドの HW 遷移を $(4 \to 4 \to 4 \to 4)$ に制約（エッセンスに相当）.

(3) **制約の選出:** 評価可能であったパターンのうち最も制約の緩いパターン J を用いる.

6. 結果

本章では，5.4 節で設定した制約を各 Branch に適用し，これまで全探索が計算量的に困難であったラウンド数における差分特性確率 (DCP) の下限値を評価した結果を報告し，さらに 4 章における差分伝搬分析に対する考察を述べる.

6.1 評価結果

5.4 節で設定した制約を適用し，探索した結果を，提案論文 [1] と比較する形で表 1 に赤字で示す.

表 1 に示す通り, 提案手法を用いることで, 多くの Branch において提案論文 [1] では評価されていなかったラウンドの差分特性確率の下限値を得ることに成功した．例として Gleeok256 Branch1 の 5 ラウンドで得られた差分伝搬を図 5 に示す.

これらの結果は，提案した構造ベースの探索が，未知のラウンドに対する効率的な安全性評価に有効であることを実証しており，第 4 章で特定した構造が長いラウンドでも重要な要素であることを強く示唆している.

6.2 差分伝搬に関する考察

本稿で分析した構造は, ラウンド数の増加に応じて, 差分確率の全体的な低下を抑制する上で最も有利な差分伝搬へと変化するために生じると考えられる.

まず, 小さいラウンドでの「拡散構造」は, 入力差分 HW が小さいほど初期ラウンドにおけるアクティブ S-box 数が抑制され, 差分確率の低下が緩やかになるため有利である.

次に, より大きいラウンドにおける「くびれ構造」は,「拡散構造」をとり，終盤の高 HW から拡散を開始するよりも, 序盤で一度 HW を減少させる方が全体的な確率低下を抑制できるため有利になる.

最後に「プラトー構造」は, ラウンド数がさらに増えることで「くびれ構造」における HW の減少と再増加のコストが大きくなり, 結果として一定の HW を維持する方が有利になるために生じると考えられる.

7. まとめ

本章で示した一連の結果は, 第 5 章で提案した探索手法の有効性を示すものである．「拡散構造」や「くびれ構造」,「プラトー構造」という構造的特徴に着目し，高い差分特性確率を導出する差分伝搬を効率的に探索することができた.

特に, 既知の最大ラウンドにおける最大差分特性を持つ差分伝搬の HW 遷移を初期制約として利用し, それを段階的に緩和していくアプローチは, 計算コストを抑制しつつ, より広範な探索を可能にした.

ただし, 本手法の性能は初期制約として用いる差分伝搬の品質に依存する可能性があり, 本手法で発見されなかった構造を持つ，より高確率な差分特性が存在する可能性がある点は今後の課題である．とはいえ, 本研究で提案した手法は, 従来法では評価が困難であったラウンドに対して, より信頼性の高い差分特性確率の下限値を与えるための有効なアプローチであると結論付けられる.

参考文献

[1] R. Anand, S. Banik, A. Caforio, T. Ishikawa, T. Isobe, F. Liu, K. Minematsu, M. Rahman, and K. Sakamoto. Gleeok: A family of low-latency prfs and its applications to authenticated encryption. *IACR Transactions on Cryptographic Hardware and*

Embedded Systems, 2024(2):545–587, 2024.

[2] R. Avanzi. The QARMA block cipher family – almost MDS matrices over rings with zero divisors, nearly symmetric even-mansour constructions with non-involutory central rounds, and search heuristics for low-latency s-boxes. Cryptology ePrint Archive, Paper 2016/444, 2016.

[3] R. Avanzi, S. Banik, O. Dunkelman, M. Eichlseder, S. Ghosh, M. Nageler, and F. Regazzoni. The QARMAv2 family of tweakable block ciphers. Cryptology ePrint Archive, Paper 2023/929, 2023.

[4] S. Banik, T. Isobe, F. Liu, K. Minematsu, and K. Sakamoto. Orthros: A low-latency PRF. Cryptology ePrint Archive, Paper 2021/390, 2021.

[5] C. Beierle, J. Jean, S. Kölbl, G. Leander, A. Moradi, T. Peyrin, Y. Sasaki, P. Sasdrich, and S. M. Sim. The skinny family of block ciphers and its low-latency variant mantis. In *Annual international cryptology conference*, pages 123–153. Springer, 2016.

[6] E. Biham and A. Shamir. Differential cryptanalysis of des-like cryptosystems. *Journal of CRYPTOLOGY*, 4(1):3–72, 1991.

[7] J. Borghoff, A. Canteaut, T. Güneysu, E. B. Kavun, M. Knezevic, L. R. Knudsen, G. Leander, V. Nikov, C. Paar, C. Rechberger, et al. Prince–a low-latency block cipher for pervasive computing applications. In *International conference on the theory and application of cryptology and information security*, pages 208–225. Springer, 2012.

[8] J. Erlacher, F. Mendel, and M. Eichlseder. Bounds for the security of ascon against differential and linear cryptanalysis. *IACR Transactions on Symmetric Cryptology*, 2022(1):64–87, Mar. 2022.

[9] A. Ignatiev, A. Morgado, and J. Marques-Silva. PySAT: A Python toolkit for prototyping with SAT oracles. In *SAT*, pages 428–437, 2018.

[10] L. Sun, W. Wang, and M. Wang. Accelerating the search of differential and linear characteristics with the SAT method. *IACR Trans. Symmetric Cryptol.*, 2021(1):269–315, 2021.