LeMac-0/LeMacの偽造攻撃に対する安全性評価

名古屋 太一[1,a)]　白矢 琢朗[2,b)]　髙 和真[2,3]　石川 達也[2]　阪本 光星[2,4]　伊藤 竜馬[2,3]
五十部 孝典[2,3]

概要：LeMac-0 および LeMac は，ToSC 2024 で提案された AES ベースのユニバーサルハッシュ関数に基づいて設計された，現時点で最速のメッセージ認証コードである．本稿では，これらに対して充足可能性問題（SAT）を用いた複数の衝突攻撃に関する安全性評価を行う．具体的には，内部状態やタグの衝突を対象としたビット単位およびバイト単位での差分解析により，各ラウンドにおける active S-box 数の下界を導出し，偽造攻撃に対する耐性を明らかにする本研究は LeMac-0 および LeMac に対して，active S-box を用いた各ラウンドでの偽造攻撃耐性評価を初めて実施したものである．

キーワード：AES 命令，衝突攻撃, LeMac, 差分攻撃, 充足可能性問題

Security Evaluation Against Forgery Attacks on LeMac-0 and LeMac

Taichi Nagoya[1,a)]　Takuro Shiraya[2,b)]　Kazuma Taka[2,3]　Tatsuya Ishikawa[2]
Kosei Sakamoto[2,4]　Ryoma Ito[2,3]　Takanori Isobe[2,3]

Abstract: LeMac-0 and LeMac are the fastest message authentication codes to date, designed based on the AES-based universal hash function proposed in ToSC 2024. In this paper, we conduct a security evaluation of these schemes against several collision attacks using satisfiability (SAT). Specifically, by performing bit-wise and byte-wise differential analysis targeting internal state and tag collisions, we derive lower bounds on the number of active S-boxes in each round and clarify their resistance against forgery attacks. To the best of our knowledge, this is the first work that evaluates the forgery resistance of LeMac-0 and LeMac through round-wise analysis of active S-boxes.

Keywords: AES Instructions, forgery attacks, LeMac, SAT solver, active Sbox

1. はじめに

1.1 背景

2008 年に Intel 社が発表した AES-NI （Advanced Encryption Standard New Instructions） [1] [2] は，NIST によって標準化されたブロック暗号 AES を高速に実行可能にする命令セットである．Intel / AMD 製プロセッサに広く搭載されており，ARM 製プロセッサにも同等機能が存在するため，AES-NI を活用することで高速なソフトウェア実装が可能になる．その利点を活かし，認証暗号（AEGIS [3]，Rocca [4], [5]）やハッシュ関数（Simpira [6], Areion [7]）などの高速暗号が設計されている．

ToSC 2024 にて，Bariant らは AES-NI と XOR のみを用いた高速な Universal Hash Function （UHF） ベースのメッセージ認証コード（MAC）として LeMac を提案した [8]．UHF の設計時には，混合整数線形計画法（MILP）を用いてバイト単位衝突小激大勢の評価をしている．また MAC 全体の衝突耐性は，ラウンド関数として使用する

[1] 兵庫県立大学
University of Hyogo
[2] 大阪大学
The University of Osaka
[3] NICT
National Institute of Information and Communications Technology
[4] 三菱電機株式会社
Mitsubishi Electric Corporation
[a)] taichi.758.goya@gmail.com
[b)] takurou.shiraya727@gmail.com

UHF と AES の安全性に基づき保証しているため，詳細な安全性評価は実施されていない．なお安全性評価を行うコードに誤りがあったとして，設計者は修正版である正しい候補を LeMac とし，以前提案された候補は LeMac-0 に改名された [9]．本研究ではこの命名規則に従い，正しい候補を LeMac ，修正前の候補を LeMac-0 として扱う．

1.2 貢献

本研究では，LeMac-0 および LeMac に対する偽造攻撃耐性を，第三者として初めて評価する．具体的には，これらの暗号に対して，内部衝突を引き起こすようなメッセージ差分を探索する．この探索を行うために，充足可能性問題（SAT: Boolean Satisfiability Problem）を活用し，専用ソルバーを用いて，バイト単位およびビット単位での active S-box 数の下界を導出する．なお，LeMac-0 および LeMac は AES のラウンド関数と XOR 演算のみで構成されており，Sun らの提案手法 [10], [11] を応用することで，これらの構造を効率的にモデリングすることができる．

LeMac-0 および LeMac で内部衝突を引き起こすために，States and Registers Collision（ **図 3**），States Collision（ **図 4**），そして Tag Collision（ **図 5**）という 3 つの攻撃手法を提案する．各攻撃手法での評価結果は次のとおりである（詳細は **表 1** のとおり）．

- LeMac-0 / LeMac の Satas and Registers Collision に対するビット単位評価での active S-box 数の下界は，それぞれ少なくとも 33 個 / 35 個であることを明らかにした．AES S-box の最大差分確率が 2^{-6} であることを踏まえると，LeMac-0 / LeMac の最大差分確率は高々 $2^{-6\cdot 33} = 2^{-198}/2^{-6\cdot 35} = 2^{-210}$ となる．
- LeMac-0 / LeMac の Satas Collision に対するビット単位評価での active S-box 数の下界は，それぞれ少なくとも 33 個 / 35 個であることを明らかにした．AES S-box の最大差分確率が 2^{-6} であることを踏まえると，LeMac-0 / LeMac の最大差分確率は高々 $2^{-6\cdot 33} = 2^{-198}/2^{-6\cdot 35} = 2^{-210}$ となる．
- LeMac-0 / LeMac の Tag Collision に対するビット単位評価での active S-box 数の下界は，それぞれ少なくとも 34 個 / 52 個であることを明らかにした．AES S-box の最大差分確率が 2^{-6} であることを踏まえると，LeMac-0 / LeMac の最大差分確率は高々 $2^{-6\cdot 34} = 2^{-204}/2^{-6\cdot 52} = 2^{-312}$ となる．

1.3 論文構成

本稿の構成は以下の通りである．まず，2 章で偽造/衝突攻撃とその攻撃に利用する差分特性の説明をし，数理最適化ソルバーによる自動探索手法と充足可能性問題を用いた安全性評価の説明をする．次に，3 章では本研究の評価対象である LeMac-0/LeMac の説明をする．次に，4 章では具体的な安全性評価方法を説明し，5 章で安全性評価結果を示す．最後に，6 章でまとめを述べる．

2. 準備

本章では，偽造/衝突攻撃, 攻撃に利用する差分特性, 数理最適化ソルバーによる自動探索手法と充足可能性問題を用いた安全性評価の順番で説明する．

2.1 偽造/衝突攻撃

暗号 MAC に対する脅威の一つとして偽造攻撃が挙げられるが，式 (1) に示すように受信者が期待するタグを攻撃者が同一の鍵 K と元のメッセージ M/ナンス N とは異なる M'/N' を用いて生成する．本稿ではこの偽造攻撃をベースとした安全性評価を行う．

$$Tag_K(M, N) = Tag_K(M', N') \tag{1}$$

またその中でも，内部衝突を起こすことで異なるメッセージから同一 MAC 値を生成することを目標とした衝突攻撃を利用した安全性評価も行う．LeMac-0 / LeMac [8], [9] は衝突耐性の高い UHF を使用することで，安全性を保証している．

偽造/衝突攻撃を実行するにあたり，本研究ではメッセージおよびナンスを利用する．ただし，メッセージおよびナンスの具体的な内容には依存しないものとする．このような条件下において内部状態の衝突が生じた場合，MAC の偽造が可能となる．本攻撃では，2.2 節で説明する差分特性を利用する．評価方法の詳細については，4 節で述べる．

2.2 差分特性

差分特性として差分が非線形層を通過する場合のみ，確率的に伝播することが知られている．本研究の評価対象である LeMac-0 / LeMac は AES のラウンド関数と XOR のみで構成されており，非線形関数は AES の SubBytes で使用される S-box のみであるため，S-box を通過する場合のみ差分特性確率が減少する．差分が 0 ではない S-box は active S-box と呼ばれ，active S-box の数を n，S-box の差分確率を DP_s，ラウンド関数全体の差分特性確率を DP_{F_R} とすると，式 (2) に示すように全ての active S-box における差分特性確率の積によって全体の差分特性確率を推定できる．

$$DP_{F_R} = \prod_{i=1}^{n} DP_s. \tag{2}$$

衝突攻撃に対する安全性評価を行う場合，ある時点において差分が 0 になるような最大差分特性確率を導出する必要があり，この確率は active S-box 数の下界を導出することで算出可能となる．active S-box 数の下界を m，S-box の差分確率を DP_{smax}，最大差分特性確率を DP_{F_Rmax} と

すると，最大差分特性確率は式 (3) で導出できる．

$$DP_{F_R max} = \prod_{i=1}^{m} DP_{smax}. \quad (3)$$

2.3 数理最適化ソルバーによる自動探索手法

自動探索手法は，暗号の安全性評価を目的とした暗号解読に広く利用されている．代表的な数理最適化手法として，混合整数線形計画法 （MILP），充足可能性問題 （SAT），および背景理論付き充足可能性問題 （SMT）があり，これらを用いて暗号内部のビット 演算や S-box 処理を数理モデル化し，ソルバーで最適解または下界を求める手法がある．

本節では active S-box 数の下界評価に用いる，MILP ソルバーと SAT / SMT ソルバーについてそれぞれの評価手法の違いを述べる．MILP を用いた手法では暗号の内部演算を線形式で表現し，制約式として定式化する．目的関数は ative S-box の合計数とし，これを制約条件の下で最小化することにより，active S-box 数の下界を求める．一方，SAT / SMT を用いた手法では，暗号の内部演算をブール式で表現する．さらに active S-box の合計数を特定の値以下になるように制限するようなブール式を追加し，充足可能か判定する．この制約が充足可能でない場合，ative S-box の合計数を制限している閾値を拡大し，再度充足可能か判定する．この操作を充足可能となるまで繰り返すことで，active S-box 数の下界を求める．本研究では後者の SAT ソルバーを安全性評価に適用する．

2.4 充足可能性問題（SAT）を用いた安全性評価

充足可能性問題（SAT）は，与えられたブール式が充足可能か否かを判定する問題である．ブール式は真と偽の二値をとるブール変数と，論理理演子である AND （∧），OR （∨），NOT （¬）から構成される．全てのブール式は $\bigwedge_{i=0}^{n} \bigvee_{j=0}^{m_i} C_i j$ のような連言標準形（CNF）と呼ばれる形式に変換可能である．ここで，$C_i j$ ($0 \le i \le n, 0 \le j \le m_i$) はリテラルと呼ばれ，論理変数またはその否定である．各リテラルを論理和 （∨） で結合した式が $\bigvee_{j=0}^{m_i} C_i j$ であり，節と呼ばれる．複数の節を論理積 （∧） で結合した式全体が CNF 式である．

本稿では，PySAT [12] で CNF 式を作成する．そして SAT competition 2022 [13]/ SAT competition 2024 [14] で, 高スコアを記録した mallob-kicaliglu [15], [16]/ saoudi-painless-par2 [17] を SAT ソルバーとして採用し，安全性評価を行う．

3. LeMac-0/LeMac

本章では，本稿の評価対象である LeMac-0 / LeMac について説明する．LeMac-0 / LeMac は Bariant らによって提案された MAC [8], [9] であり，AES-NI を用いて高速性を保証している．LeMac-0 / LeMac は入力された鍵からラウンド鍵 K を生成し，初期値を設定する初期化フェーズ，データを入力して内部状態を更新する吸収フェーズ，入力されたナンスを用いて MAC 値を生成する最終フェーズの 3 つのフェーズからなる．また，LeMac-0 / LeMac のラウンド関数をそれぞれ**図 1**/**図 2** に示す．

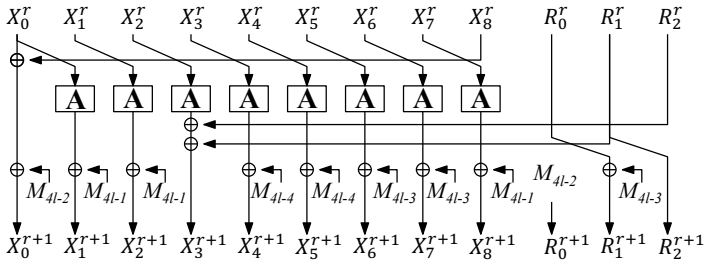

図 1 LeMac-0 のラウンド関数.

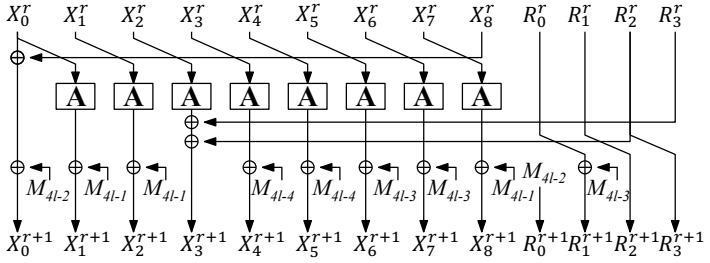

図 2 LeMac のラウンド関数.

3.1 AES-NI

AES-NI（Advanced Encryption Standard New Instructions） [1] [2] は 2008 年に Intel から発表された，AES 暗号化・復号の処理を高速に行うことを目的とした SIMD 命令群の一種である．AES-NI では複雑で時間のかかる AES アルゴリズムを直接ハードウェア上で実装し，ソフトウェア実装より 3 –10 倍程度の高速化を実現している．入力を X，ラウンド鍵を K とすると， AES ラウンド関数は以下の式で定義される．

$$\mathrm{AES}_K(X) = (\mathrm{MixColumns} \circ \mathrm{ShiftRows} \circ \mathrm{SubBytes}(X)) \oplus K$$

LeMac-0 / LeMac で使用される aesenc 命令は，AddKey を除く SubBytes , ShiftRows , MixColumns から構成される AES ラウンド関数の 1 ラウンド分を実行する．また，図 1， 図 2 中の A では内部ステートを鍵として利用することで，aesenc 命令が実行されている．

3.2 LeMac-0/LeMac の構造

LeMac-0 / LeMac では主にステート X_i^r とレジスタ R_i^r を使用する．i, r はそれぞれステートまたはレジスタの番号，ラウンド数を示す．

初期化フェーズ 初期化フェーズでは，吸収フェーズで使用

する初期ステート X_i^0・初期レジスタ R_i^0 を式 (4) のように設ける．R_{init} については 3.3 節にて述べる．また，入力メッセージ M から $l = \lceil (\text{bitlen}\,(M) + 1)/512 \rceil$ を使用して式 (5) のようにパディング処理を行う．

$$X^0 \leftarrow K_{init} \quad R^0 \leftarrow R_{init} \tag{4}$$

$$K_{init} \leftarrow (AES_K(0) \ldots AES_K(8))$$

$$M_0, \ldots, M_{4l-1} \leftarrow M||10^* \quad M_{4l}, \ldots, M_{4l+3} \leftarrow 0 \tag{5}$$

吸収フェーズ 吸収フェーズでは 図 1， 図 2 のラウンド関数を r ラウンド分実行し，ステートとレジスタを更新する．

$$X^{r+1}, R^{r+1} = RF(X^r, R^r, M^r) \tag{6}$$

$$M^r = (M_{4r}, M_{4r-1}, M_{4r-2}M_{4r-3}) \tag{7}$$

最終フェーズ 吸収フェーズで更新した X に対し，最終フェーズでのラウンド数 R' を $0 \le r' < 10$ の範囲で式 (8) を繰り返す．この時，以下のように鍵 K を決定する．

$$X_i^{r'+1} = \text{AES}_{k_{i+r'}}(X_i^{r'})\ (0 \le r' < 10, 0 \le i < 9) \tag{8}$$

$$k_{i+r'} = \text{AES}_K(9 + i + r')\ (9 \le 9 + i + r' \le 26)$$

最終的に，全ての X_i の XOR の和を

$$h = \bigoplus_{i=0}^{8} X_i \tag{9}$$

として求め, ナンス N とともに以下のように MAC 値 (Tag) を出力する．

$$Tag = AES_k(h \oplus AES_{k'}(N) \oplus N), \tag{10}$$

$$k = \text{AES}_K(28),\ k' = \text{AES}_K(27)$$

3.3 LeMac-0 / LeMac の相違点

両方式の相違点はレジスタ数と変数 n と吸収フェーズのラウンド数にある．LeMac-0 は 3 本のレジスタ（R_0–R_2）を用い $R_{init} \leftarrow (0,0,0)$ とし，吸収フェーズのラウンド数は $0 \le r < l + 3$ とする．一方，LeMac は 4 本のレジスタ（R_0–R_3）を用い $R_{init} \leftarrow (0,0,0,0)$ とし，吸収フェーズのラウンド数は $0 \le r < l + 4$ とする．

4. SAT を用いた衝突攻撃に対する安全性評価

本章では， SAT を活用したモデリング，三つの手法を用いた衝突攻撃，本研究で実施する安全性評価の順番で説明する．

4.1 SAT を活用したモデリング

本評価における SAT モデリングでは, AES ラウンド関数の非線形関数である S-box , 線形関数である ShiftRows および MixColumns , 並びに XOR 演算を論理式として符号化する．S-box および XOR のモデリングには Sun らの手法 [10], [11] を用いる．MixColumns については Maximov の提案 [18] により，92 個の XOR 演算のみで表現されたモデルを採用する．ShiftRows は単なるビット置換であるため，割り当てたブール変数のインデックスを入れ替えることで実装する．また，active S-box の総数や差分特性確率が所定の閾値以下となるように制約を課すために，PySAT の CardEnc モジュールを用いた Sequential Encoding を適用する．なお本研究では関連鍵攻撃を考慮せず鍵の差分は常に 0 となるため，AES ラウンド関数で使用する AddRoundKey は考慮しない．

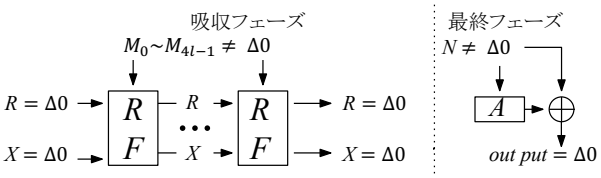

図 3 States and Registers Collision の攻撃概要.

4.2 攻撃手法

本研究では偽造/衝突攻撃を活用した 3 つの攻撃手法を考慮する．各手法の評価方法の説明を以下で行う．

4.2.1 States and Registers Collision

1 つ目の手法は，衝突攻撃を利用して内部ステートとレジスタの衝突に注目する．攻撃の概要を 図 3 に示すように，吸収フェーズでメッセージ差分を入力し，出力される X^r, R^r の差分を 0 にする．加えて，AES に差分のあるナンス N を入力し，出力差分を 0 にする必要がある．この条件下で，吸収フェーズのラウンド数 r の範囲を $0 \le r < l$ で変化させつつ，active S-box 数の下界を探索する．本手法に基づく衝突攻撃を States and Registers Collision と定義する．

4.2.2 States Collision

2 つ目の手法は，衝突攻撃を利用して内部ステートのみの衝突に注目する．攻撃の概要を図 4 に示すように，吸収フェーズでメッセージ差分を入力し，出力される X^r の差分を 0 にする．加えて，AES に差分のあるナンス N を入力し，出力差分を 0 にする必要がある．この時，式 (5) のパディング処理を考慮すると，攻撃者が差分入力可能なメッセージ長は $512 \times l - 1$ ビット である．この条件下において，吸収フェーズのラウンド数 r を LeMac-0 では $0 \le r < l + 3$ で，LeMac では $0 \le r < l + 4$ で変化させ，active S-box 数の下界を探索する．本手法に基づく衝突攻撃を States Collision と定義する．

4.2.3 Tag Collision

3 つ目の手法は，偽造攻撃を利用して最終フェーズで tag 偽造に注目する．攻撃の概要を 図 5 に示すように，攻撃者は差分入力条件として，吸収フェーズのメッセージ最終 512 ビット $\{M_{4l-4}, M_{4l-3}, M_{4l-2}, M_{4l-1}\}$ と最終フェーズ

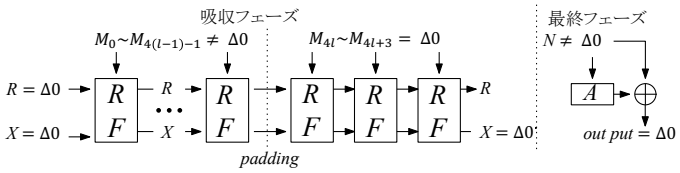

図 4　States Collision の攻撃概要.

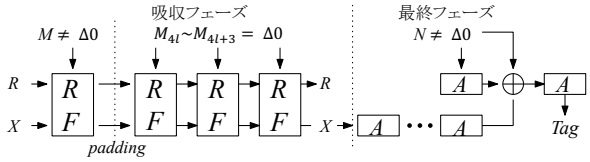

図 5　Tag Collision の攻撃概要.

のナンスに差分を入力する．この条件のもと，式 (8), (9) により出力された $X_i^{r'}(0 \leq i < 9)$ と h を用いて式 (10) より出力される Tag の差分が 0 である必要がある．この時，式 (5) のパディング処理を考慮すると，攻撃者が差分入力可能なメッセージはパディング処理前の $512-1$ ビットである．この条件下において，最終フェーズのラウンド数 r' の範囲を $0 \leq r' < 10$ で変化させながら active S-box の下界を探索する．本手法に基づく衝突攻撃を Tag Collision と定義する．

4.3　安全性評価

4.1 節で説明したモデリングを用いて，4.2 節で述べた三つの衝突攻撃に対する安全性評価を実施する．関連鍵差分攻撃は考慮せず，攻撃者はメッセージおよびナンス空間を操作可能と仮定して評価を行う．評価粒度をバイトおよびビットとして差分特性の伝播を探索し，1 ラウンドから 8 ラウンドまでの active S-box 数の下界を探索する．

5.　評価結果

本章では，各衝突攻撃に対してバイト単位/ビット単位の安全性評価結果と同一ナンス利用時の結果を示す．各手法のラウンド毎のバイト単位/ビット単位での active S-box 数の下界評価結果を 表 1 にまとめ，最小の active S-box 数を達成したラウンドにおける結果を太字で示す．

5.1　States and Registers Collision

LeMac-0　ビット単位の評価により，active S-box 数が少なくとも 33 個存在することを明らかにした．AES S-box の最大差分確率が 2^{-6} であることを踏まえると，LeMac-0 の最大差分確率は高々 $2^{-6\cdot 33} = 2^{-198}$ となるため，本攻撃に対する 128 ビット安全性を保証すると言える．

LeMac　ビット単位の評価により，active S-box 数が少なくとも 35 個存在することを明らかにした．同様に，LeMac の最大差分確率は高々 $2^{-6\cdot 35} = 2^{-210}$ となるため，本攻撃に対する 128 ビット安全性を保証すると言える．

5.2　States Collision

LeMac-0　ビット単位の評価により，active S-box 数が少なくとも 33 個であることを明らかにした．AES S-box の最大差分確率が 2^{-6} であることを踏まえると，LeMac-0 の最大差分確率は高々 $2^{-6\cdot 33} = 2^{-198}$ となるため，本攻撃に対する 128 ビット安全性を保証すると言える．

LeMac　ビット単位の評価により，active S-box 数が少なくとも 35 個存在することを明らかにした．同様に，LeMac の最大差分確率は高々 $2^{-6\cdot 35} = 2^{-210}$ となるため，本攻撃に対する 128 ビット安全性を保証すると言える．

5.3　Tag Collision

LeMac-0　ビット単位の評価により，active S-box 数が少なくとも 34 個存在することを明らかにした．AES S-box の最大差分確率が 2^{-6} であることを踏まえると，LeMac-0 の最大差分確率は高々 $2^{-6\cdot 34} = 2^{-204}$ となるため，本攻撃に対する 128 ビット安全性を保証すると言える．

LeMac　ビット単位の評価により，active S-box 数が少なくとも 52 個存在することを明らかにした．同様に，LeMac の最大差分確率は高々 $2^{-6\cdot 52} = 2^{-312}$ となるため，本攻撃に対する 128 ビット安全性を保証すると言える．

5.4　同一ナンスの利用時

Tag collision ではナンスの衝突条件を考慮するため，ここでは States and Register collision / States collision 攻撃において，同一ナンスが用いられる場合を考える．この時ナンス差分は 0 となり，ナンスによる衝突は発生しない 図 6/ 図 7 よりナンスの衝突により active S-box は 8 個存在するため，同一ナンスの利用時，active S-box は 8 個減少する．それでも LeMac-0 / LeMac では active S-box が少なくとも 25 個 / 27 個存在するため，最大差分確率は高々 $2^{-6\cdot 25} = 2^{-150}/2^{-6\cdot 27} = 2^{-162}$ である．したがって，同一ナンスの利用時でも 128 ビットの安全性が保証される．

6.　結論

本稿では，LeMac-0 / LeMac に対し，バイト単位/ビット単位での衝突攻撃に対する安全性評価を行った．評価に際しては，States and Registers Collision ，States Collision ，Tag Collision の三つの手法を用い，SAT ソルバーによって各ラウンドにおける active S-box 数の下界を探索した．結果として，各手法で各ラウンドでの active S-box 数の下界を初めて導出し，両対象が設計者の主張する 128 ビットに対する 128 ビット安全性を保証すると言える．5 ラウンドでの States and Registers Collision の差分伝搬を図 **6** と図 **7** に示す．

表 1　衝突攻撃に対する active S-box を用いた下界評価

評価対象	衝突攻撃手法	1R	2R	3R	4R	5R	6R	7R	8R	Reference
LeMac-0	States and Registers Collision	–	–	39	**28**	28	28	28	28	byte AS
		–	–	63	**33**	33	33	33	33	bit AS
LeMac		–	–	39	35	**32**	32	32	32	byte AS
		–	–	78	42	**35**	35	35	35	bit AS
LeMac-0	States Collision	–	44	**28**	28	28	28	28	28	byte AS
		–	54	43	**33**	33	33	33	33	bit AS
LeMac		–	65	39	**32**	32	32	32	32	byte AS
		–	68	57	42	**35**	35	35	35	bit AS
LeMac-0	Tag Collision	**32**	53	61	69	89	97	102	107	byte AS
		34	55	63	72	92	99	107	111	bit AS
LeMac		**48**	58	67	85	102	108	117	135	byte AS
		52	59	67	87	102	109	117	137	bit AS

安全性を満たすことを確認した.

謝辞

本研究は, JSPS 科研費 JP24H00696 と JST AIP 加速課題 JPMJCR24U1 の支援を受けたものである.

参考文献

[1] intrinsics guide. Official webpage, I. C. I.: `https://www.intel.com/content/www/us/en/docs/intrinsics-guide/index.html`.

[2] Gueron, S.: Intel Advanced Encryption Standard(AES) New Instructions Set (2010).

[3] Wu, H. and Preneel, B.: AEGIS: A Fast Authenticated Encryption Algorithm, *Selected Areas in Cryptography - SAC 2013 - 20th International Conference, Burnaby, BC, Canada, August 14-16, 2013, Revised Selected Papers* (Lange, T., Lauter, K. E. and Lisonek, P., eds.), Lecture Notes in Computer Science, Vol. 8282, Springer, pp. 185–201 (online), DOI: 10.1007/978-3-662-43414-7_10 (2013).

[4] Sakamoto, K., Liu, F., Nakano, Y., Kiyomoto, S. and Isobe, T.: Rocca: An Efficient AES-based Encryption Scheme for Beyond 5G, *IACR Trans. Symmetric Cryptol.*, Vol. 2021, No. 2, pp. 1–30 (online), DOI: 10.46586/tosc.v2021.i2.1-30 (2021).

[5] Sakamoto, K., Liu, F., Nakano, Y., Kiyomoto, S. and Isobe, T.: Rocca: An Efficient AES-based Encryption Scheme for Beyond 5G (Full version), *IACR Cryptol. ePrint Arch.*, p. 116 (online), available from ⟨https://eprint.iacr.org/2022/116⟩ (2022).

[6] Gueron, S. and Mouha, N.: Simpira v2: A Family of Efficient Permutations Using the AES Round Function, *Advances in Cryptology - ASIACRYPT 2016 - 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part I* (Cheon, J. H. and Takagi, T., eds.), Lecture Notes in Computer Science, Vol. 10031, pp. 95–125 (online), DOI: 10.1007/978-3-662-53887-6_4 (2016).

[7] Isobe, T., Ito, R., Liu, F., Minematsu, K., Nakahashi, M., Sakamoto, K. and Shiba, R.: Areion: Highly-Efficient Permutations and Its Applications to Hash Functions for Short Input, *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, Vol. 2023, No. 2, pp. 115–154 (online), DOI: 10.46586/TCHES.V2023.I2.115-154 (2023).

[8] Bariant, A., Baudrin, J., Leurent, G., Pernot, C., Perrin, L. and Peyrin, T.: Fast AES-Based Universal Hash Functions and MACs Featuring LeMac and PetitMac, *IACR Trans. Symmetric Cryptol.*, Vol. 2024, No. 2, pp. 35–67 (online), DOI: 10.46586/TOSC.V2024.I2.35-67 (2024).

[9] Bariant, A., Baudrin, J., Leurent, G., Pernot, C., Perrin, L. and Peyrin, T.: Corrigendum to Fast AES-Based Universal Hash Functions and MACs, *IACR Trans. Symmetric Cryptol.*, Vol. 2025, No. 1, pp. 623–628 (online), DOI: 10.46586/TOSC.V2025.I1.623-628 (2025).

[10] Sun, L., Wang, W. and Wang, M.: More Accurate Differential Properties of LED64 and Midori64, *IACR Trans. Symmetric Cryptol.*, Vol. 2018, No. 3, pp. 93–123 (online), DOI: 10.13154/tosc.v2018.i3.93-123 (2018).

[11] Sun, L., Wang, W. and Wang, M.: Accelerating the Search of Differential and Linear Characteristics with the SAT Method, *IACR Trans. Symmetric Cryptol.*, Vol. 2021, No. 1, pp. 269–315 (online), DOI: 10.46586/tosc.v2021.i1.269-315 (2021).

[12] Ignatiev, A., Morgado, A. and Marques-Silva, J.: PySAT: A Python Toolkit for Prototyping with SAT Oracles, *SAT*, pp. 428–437 (2018).

[13] Balyo, T., Heule, M., Iser, M., Järvisalo, M. and Suda, M.(eds.): *Proceedings of SAT Competition 2022: Solver and Benchmark Descriptions*, Department of Computer Science Series of Publications B, Department of Computer Science, University of Helsinki, Finland (2022).

[14] Heule, M., Iser, M., Järvisalo, M. and Suda, M.(eds.): *Proceedings of SAT Competition 2024: Solver, Benchmark and Proof Checker Descriptions*, Department of Computer Science Report Series B, Department of Computer Science, University of Helsinki, Finland (2024).

[15] Schreiber, D. and Sanders, P.: Scalable SAT Solving in the Cloud, *International Conference on Theory and Applications of Satisfiability Testing*, Springer, pp. 518–534 (2021).

[16] Sanders, P. and Schreiber, D.: Decentralized Online Scheduling of Malleable NP-hard Jobs, *International European Conference on Parallel and Distributed Computing*, Springer, pp. 119–135 (2022).

[17] Saoudi, M., Baarir, S., Sopena, J. and Lejemble, T.: D-Painless: A Framework for Distributed Portfolio SAT Solving, *Tools and Algorithms for the Construction and Analysis of Systems* (Gurfinkel, A. and Heule, M., eds.), Cham, Springer Nature Switzerland, pp. 45–64 (2025).

[18] Maximov, A.: AES MixColumn with 92 XOR gates, *IACR Cryptol. ePrint Arch.*, p. 833 (online), available from ⟨https://eprint.iacr.org/2019/833⟩ (2019).

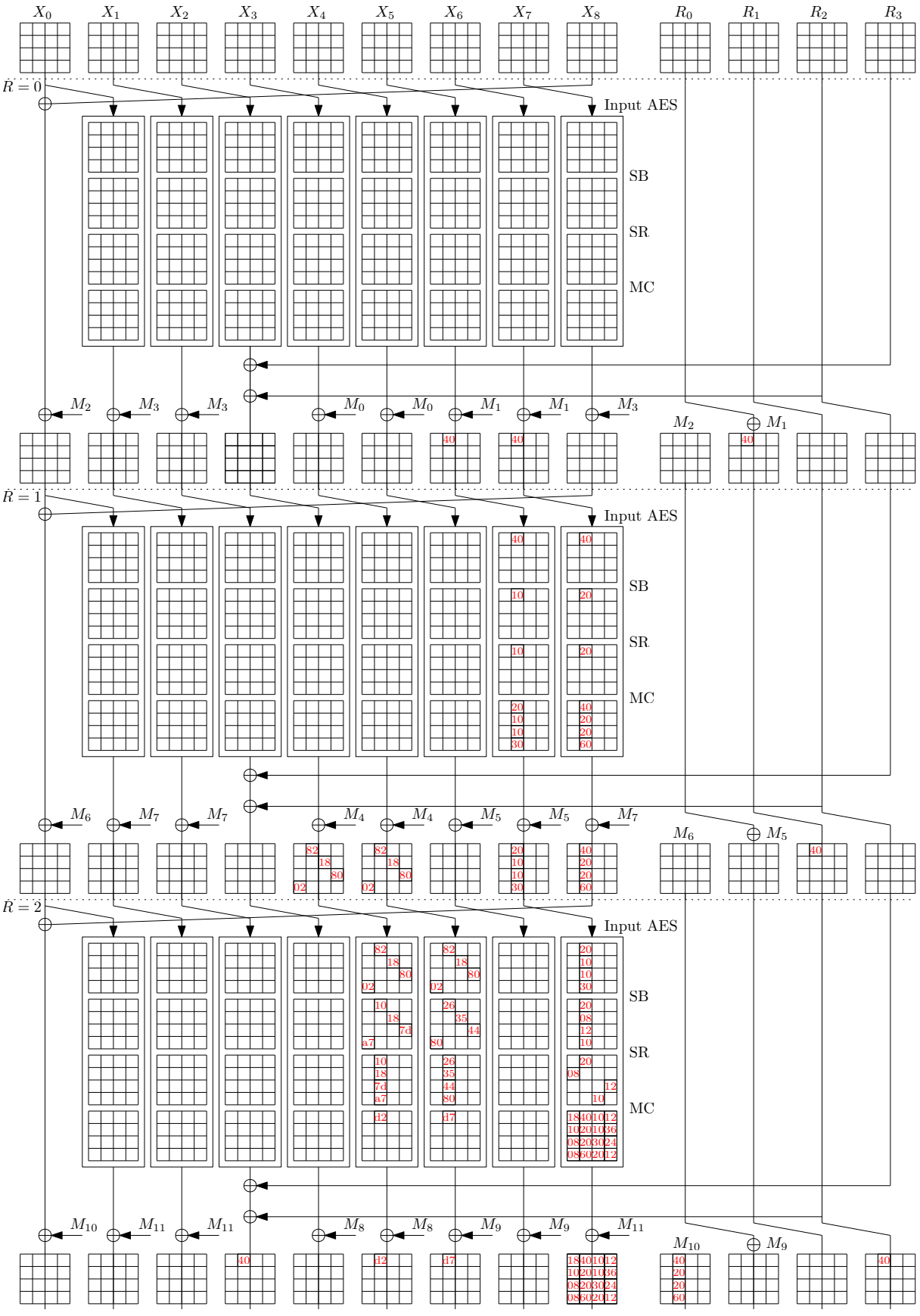

図 6 LeMac の 5 ラウンドでの States and Registers Collision の差分伝搬 (1–3 ラウンド)

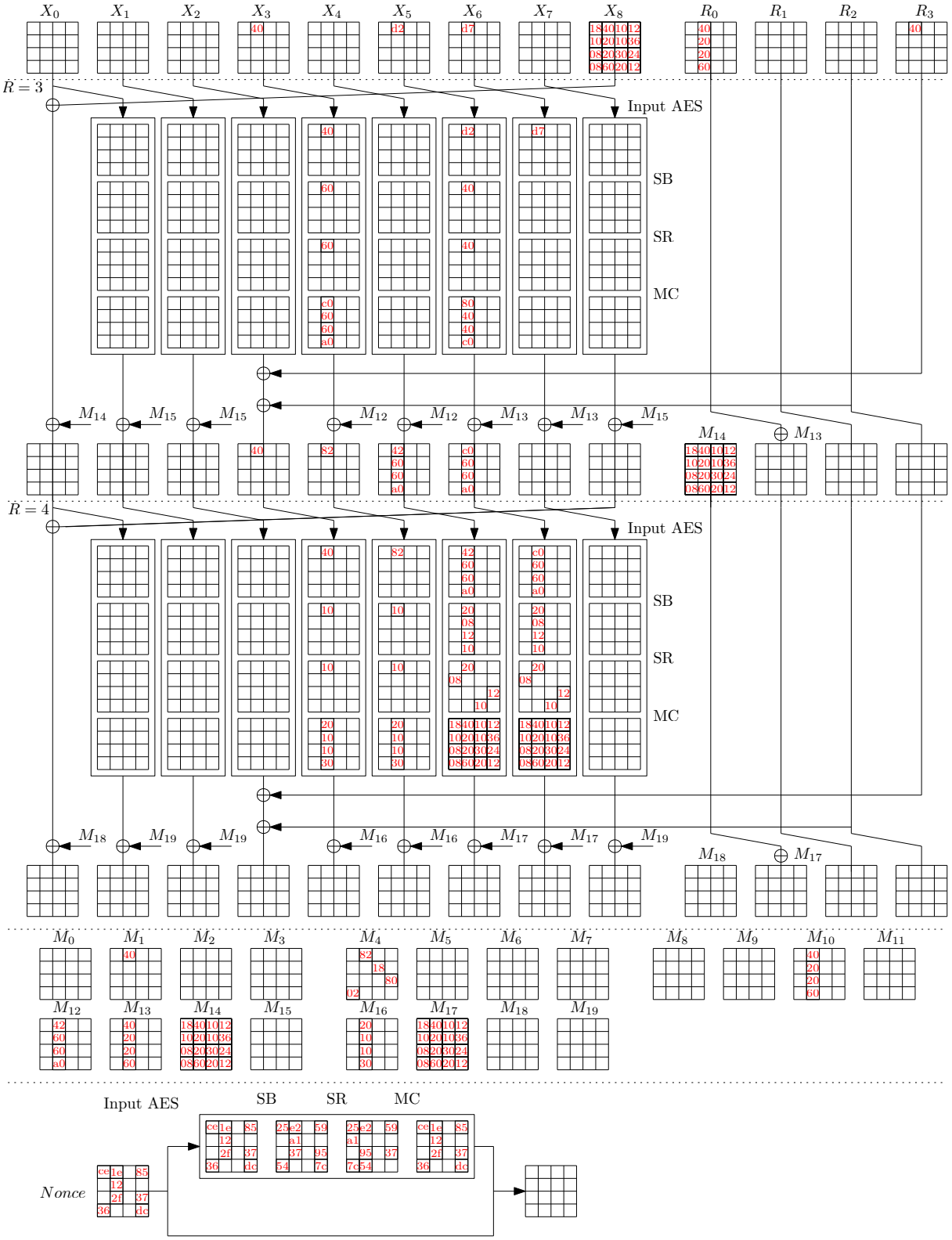

図 7 LeMac の 5 ラウンドでの States and Registers Collision の差分伝搬 (4–5 ラウンド)