「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

伊藤 竜馬
（国立研究開発法人情報通信研究機構）

2022 年 4 月 13 日

目次

第 1 章 本報告書の目的と構成概要 3

1.1 目的 . . . 3
1.2 構成概要 . . . 3
1.3 本報告書のレビューについて . . . 4
1.4 謝辞 . . . 4

第 2 章 調査結果の概要 5

2.1 軽量ブロック暗号の安全性解析状況に関する調査結果 . . . 5
2.2 軽量ストリーム暗号の安全性解析状況に関する調査 . . . 6
2.3 軽量ハッシュ関数の安全性解析状況に関する調査 . . . 6
2.4 軽量 MAC の安全性解析状況に関する調査 . . . 6
2.5 軽量認証暗号の安全性解析状況に関する調査 . . . 7

第 3 章 軽量ブロック暗号の安全性解析状況 8

3.1 CLEFIA . . . 9
3.2 LED . . . 11
3.3 Midori . . . 13
3.4 Piccolo . . . 15
3.5 PRESENT . . . 17
3.6 PRINCE . . . 18
3.7 Simon . . . 20
3.8 Speck . . . 23
3.9 TWINE . . . 25
3.10 LEA . . . 26

第 4 章 軽量ストリーム暗号の安全性解析状況 30

4.1 ChaCha . . . 30
4.2 Enocoro . . . 32
4.3 Grain v1 . . . 33

4.4 MICKEY 2.0 . . . 35
4.5 Trivium . . . 36

第 5 章 軽量ハッシュ関数の安全性解析状況査 39
5.1 Keccak . . . 39
5.2 PHOTON . . . 41
5.3 QUARK . . . 42
5.4 SPONGENT . . . 44
5.5 Lesamnta-LW . . . 45

第 6 章 軽量 MAC の安全性解析状況 48
6.1 SipHash . . . 48
6.2 Chaskey . . . 50
6.3 LightMAC . . . 52
6.4 Tsudik's keymode . . . 54

第 7 章 軽量認証暗号の安全性解析状況 55
7.1 ACORN . . . 55
7.2 ASCON . . . 57
7.3 AES-JAMBU . . . 59
7.4 AES-OTR . . . 60
7.5 CLOC and SILC . . . 60
7.6 Deoxys . . . 61
7.7 Joltik . . . 64
7.8 Ketje . . . 65
7.9 Minalpher . . . 68
7.10 OCB . . . 69
7.11 PRIMATEs . . . 70
7.12 AEGIS . . . 71
7.13 COLM . . . 73
7.14 Grain-128A . . . 74

参考文献 77

付録 A 本報告書のレビュー 108

第 1 章

本報告書の目的と構成概要

1.1 目的

2017 年 3 月に公開された CRYPTREC 暗号技術ガイドライン（軽量暗号） [68, 69]（以下、「2016 年度ガイドライン」という）では、「実装性能と安全性のトレードオフを勘案した上で、従来の暗号技術に対して特定の性能指標で優位性（軽量性）を持つように設計された共通鍵暗号技術」をスコープとし、軽量暗号の活用例、代表的な軽量暗号の性能比較、代表的な軽量暗号に関する基本情報について紹介している。しかしながら、暗号方式に対する安全性評価技術は日進月歩であり、2016 年度ガイドラインの公開から 5 年以上が経っているため、2016 年度ガイドラインには記載されていない、軽量暗号の安全性を脅かす新たな脅威が生じている可能性は十分に考えられる。そこで本報告書では、2016 年度ガイドラインで紹介された暗号方式を中心とした代表的な軽量暗号の安全性評価に関する動向調査を行うことを目的とし、2021 年 9 月の時点でこれらの軽量暗号に対して現実的な脅威に繋がる脆弱性が指摘されているか否かを明らかにする。

1.2 構成概要

代表的な軽量暗号の安全性解析状況について、最初に 2016 年度ガイドラインの公開時点における安全性解析状況を明らかにする（例：第 3.1.1 節）。次に、2016 年度ガイドラインで紹介された暗号方式を中心とした代表的な軽量暗号の安全性評価に関する動向調査を行い、2021 年 9 月の時点でこれらの軽量暗号に対して現実的な脅威に繋がる脆弱性が指摘されているか否かを明らかにする。具体的には、攻撃可能段数、攻撃種別、計算量、データ量、メモリ量、参考文献について表にまとめ、表から最良の攻撃を明らかにするとともに、その概要について簡単に紹介する（例：第 3.1.2 節）。最後に、2021 年 9 月現在における代表的な軽量暗号の安全性解析状況についてまとめる（例：第 3.1.3 節）。本報告書の構成概要は以下のとおりである。

- 第 2 章では、本報告書における調査結果の概要を述べる。
- 第 3 章では、2016 年度ガイドライン [68, 69] の第 4.1 節に記載された代表的な軽量ブロック暗号 CLEFIA、LED、Midori、Piccolo、PRESENT、PRINCE、Simon、Speck、TWINE の安全

性解析状況に関する調査結果をまとめる。さらに、軽量ブロック暗号に関係する ISO/IEC 規格 (ISO/IEC 29192-2) [1] で採択されている LEA も調査対象とする。

- 第 4 章では、2016 年度ガイドライン [68, 69] の第 4.2 節に記載された代表的な軽量ストリーム暗号 ChaCha、Enocoro、Grain v1、MICKEY 2.0、Trivium の安全性解析状況に関する調査結果をまとめる。
- 第 5 章では、2016 年度ガイドライン [68, 69] の第 4.3 節に記載された代表的な軽量ハッシュ関数 Keccak、PHOTON、QUARK、SPONGENT の安全性解析状況に関する調査結果をまとめる。さらに、軽量ハッシュ関数に関係する ISO/IEC 規格 (ISO/IEC 29192-5) [4] で採択されている Lesamnta-LW も調査対象とする。
- 第 6 章では、2016 年度ガイドライン [68, 69] の第 4.4 節に記載された代表的な軽量 MAC SipHash の安全性解析状況に関する調査結果をまとめる。さらに、軽量 MAC に関係する ISO/IEC 規格 (ISO/IEC 29192-6) [2] で採択されている Chaskey、LightMAC、Tsudik's keymode も調査対象とする。
- 第 7 章では、2016 年度ガイドライン [68, 69] の第 4.5 節に記載された代表的な軽量認証暗号 ACORN、ASCON、AES-JAMBU、AES-OTR、CLOC and SILC、Deoxys、Joltik、Ketje、Minalpher、OCB、PRIMATEs の安全性解析状況に関する調査結果をまとめる。さらに、CAESAR final portfolio に選出されている AEGIS と COLM、軽量認証暗号に関係する ISO/IEC 規格 (ISO/IEC 29192-8) [3] で採択される予定の Grain-128A も調査対象とする。

1.3　本報告書のレビューについて

2021 年度、暗号技術評価委員会の了承のもと、本報告書のレビューを日本電気株式会社の峯松一彦様にご担当いただいた。レビューの細部は付録 A のとおり。

1. 筆者が 2021 年 9 月時点までの安全性解析状況をまとめたドラフト版に対して、峯松様にその内容を確認していただいた。
2. 筆者は峯松様から受けた指摘事項に基づきドラフト版を修正し、峯松様にその修正内容を再度確認していただいた。

上記の過程を経て、本報告書が対象とする範囲、安全性評価内容、および記述内容が「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として妥当であるとの結論をいただいた。

1.4　謝辞

前述のとおり、本報告書を作成するにあたり、峯松様に本報告書の内容についてご確認いただくとともに、筆者の認識誤りについてご指摘いただきました。峯松様に深く感謝申し上げます。

第 2 章

調査結果の概要

本章では、代表的な軽量暗号の安全性解析状況に関する調査結果（2021 年 9 月現在）を概説する。

2.1 軽量ブロック暗号の安全性解析状況に関する調査結果

第 3 章において、2016 年度ガイドライン [68, 69] の第 4.1 節に記載された代表的な軽量ブロック暗号 CLEFIA、LED、Midori、Piccolo、PRESENT、PRINCE、Simon、Speck、TWINE の安全性解析状況に関する調査結果をまとめた。調査結果の概要は次のとおりである。

- CLEFIA、LED、Simon、Speck に対しては、仕様段数において秘密鍵の全数探索よりも効率的に実行可能な攻撃が存在しない。
- Midori、Piccolo、PRESENT、PRINCE、TWINE に対しては、ある特定の場合（弱鍵を使用している場合、related-key setting の場合、known-key setting の場合、バイクリーク攻撃[*1]とその派生攻撃の手法を使用している場合、など）を除き、仕様段数において秘密鍵の全数探索よりも効率的に実行可能な攻撃が存在しない。

また、CLEFIA、PRESENT、LEA が軽量ブロック暗号に関係する ISO/IEC 規格 (ISO/IEC 29192-2) [1] に採択されている状況を鑑み、2016 年度ガイドラインに記載されていない LEA も調査対象とした。LEA の安全性解析状況に関する調査結果の概要は次のとおりである。

- LEA に対しては、仕様段数において秘密鍵の全数探索よりも効率的に実行可能な攻撃が存在しない。

[*1] バイクリーク攻撃とはバイクリークと呼ばれる性質を利用して鍵の全数探索と同等の計算量を要する処理が必要な攻撃のことを指すものであり、バイクリークの性質を利用した攻撃であってもバイクリーク攻撃とは異なるものもあることに注意されたい。

2.2　軽量ストリーム暗号の安全性解析状況に関する調査

第 4 章において、2016 年度ガイドライン [68,69] の第 4.2 節に記載された代表的な軽量ストリーム暗号 ChaCha、Enocoro、Grain v1、MICKEY 2.0、Trivium の安全性解析状況に関する調査結果をまとめた。調査結果の概要は次のとおりである。

- ChaCha、Enocoro、Trivium に対しては、仕様段数において秘密鍵の全数探索よりも効率的に実行可能な攻撃が存在しない。
- Grain v1、MICKEY 2.0 に対しては、仕様段数において秘密鍵の全数探索よりも効率的に実行可能な攻撃が存在する。なお、Grain v1、MICKEY 2.0 に対してそれぞれ最良の攻撃を実行した場合、一般的な秘密鍵の全数探索と比較して $2^{3.3}$ 倍、$2^{1.0}$ 倍の効率化が可能となる。

2.3　軽量ハッシュ関数の安全性解析状況に関する調査

第 5 章において、2016 年度ガイドライン [68,69] の第 4.3 節に記載された代表的な軽量ハッシュ関数 Keccak、PHOTON、QUARK、SPONGENT の安全性解析状況に関する調査結果をまとめた。調査結果の概要は次のとおりである。

- Keccak、PHOTON、QUARK、SPONGENT に対しては、仕様においてハッシュ関数の安全性基準を脅かす攻撃が存在しない。

また、PHOTON、SPONGENT、Lesamnta-LW が軽量ハッシュ関数に関係する ISO/IEC 規格 (ISO/IEC 29192-5) [4] に採択されている状況を鑑み、2016 年度ガイドラインに記載されていない Lesamnta-LW も調査対象とした。Lesamnta-LW の安全性解析状況に関する調査結果の概要は次のとおりである。

- Lesamnta-LW に対しては、仕様においてハッシュ関数の安全性基準を脅かす攻撃が存在しない。

2.4　軽量 MAC の安全性解析状況に関する調査

第 6 章において、2016 年度ガイドライン [68,69] の第 4.4 節に記載された代表的な軽量 MAC SipHash の安全性解析状況に関する調査結果をまとめた。調査結果の概要は次のとおりである。

- SipHash に対しては、仕様において秘密鍵の全数探索よりも効率的に実行可能な攻撃が存在しない。

また、Chaskey、LightMAC、Tsudik's keymode が軽量 MAC に関係する ISO/IEC 規格 (ISO/IEC

29192-6) [2] に採択されている状況を鑑み、2016 年度ガイドラインに記載されていない Chaskey、LightMAC、Tsudik's keymode も調査対象とした。Chaskey、LightMAC、Tsudik's keymode の安全性解析状況に関する調査結果の概要は次のとおりである。

- Tsudik's keymode に対しては、仕様において秘密鍵の全数探索よりも効率的に実行可能な攻撃が存在しない。
- Chaskey、LightMAC に対しては、ある特定の場合（弱鍵を使用している場合、related-key setting の場合、基礎となるブロック暗号として Simeck32/64 を使用した場合、など）を除き、仕様において効率的に実行可能な攻撃が存在しない。

2.5　軽量認証暗号の安全性解析状況に関する調査

第 7 章において、2016 年度ガイドライン [68,69] の第 4.5 節に記載された代表的な軽量認証暗号 ACORN、ASCON、AES-JAMBU、AES-OTR、CLOC and SILC、Deoxys、Joltik、Ketje、Minalpher、OCB、PRIMATEs の安全性解析状況に関する調査結果をまとめた。調査結果の概要は次のとおりである。

- ACORN、ASCON、AES-OTR、CLOC and SILC、Deoxys、Joltik、Ketje、Minalpher、OCB1、OCB3、PRIMATEs に対しては、仕様において効率的に実行可能な攻撃が存在しない。
- OCB2、AES-JAMBU に対しては、仕様において効率的に実行可能な攻撃が存在する。OCB2 に対しては、現実的な普遍的偽造攻撃と平文回復攻撃が実行可能である。AES-JAMBU に対しては、認証の安全性レベルとして n ビットが想定されているところ、nonce-misuse scenario において $2^{n/2}$ 回の暗号化による攻撃が実行可能である。

また、AEGIS と COLM が CAESAR final portfolio に選出されている状況を鑑み、2016 年度ガイドラインに記載されていない AEGIS と COLM も調査対象とした。加えて、Grain-128A が RFID に関係する ISO/IEC 規格 (ISO/IEC 29167-13) [5] で採択されるとともに、軽量認証暗号に関係する ISO/IEC 規格 (ISO/IEC 29192-8) [3] での採択プロセスが進行中であるという状況を鑑み、2016 年度ガイドラインに記載されていない Grain-128A も調査対象とした。AEGIS、COLM、Grain-128A の安全性解析状況に関する調査結果の概要は次のとおりである。

- AEGIS、COLM_{127} に対しては、仕様において効率的に実行可能な攻撃が存在しないものの、解析論文が少ないため潜在的な脆弱性を含んでいる可能性があることに注意されたい。
- COLM_0 に対しては、ある特定の場合（タグが未検証の場合において平文が得られる状況を想定した場合）を除き、仕様において効率的に実行可能な攻撃が存在しない。
- Grain-128A に対しては、仕様において秘密鍵の全数探索よりも効率的に実行可能な攻撃が存在する。なお、Grain-128A に対して最良の攻撃を実行した場合、一般的な秘密鍵の全数探索と比較して $2^{12.6}$ 倍の効率化が可能となる。

第 3 章

軽量ブロック暗号の安全性解析状況

本章では、2016 年度ガイドライン [68, 69] の第 4.1 節に記載された代表的な軽量ブロック暗号 CLEFIA、LED、Midori、Piccolo、PRESENT、PRINCE、Simon、Speck、TWINE の安全性解析状況に関する調査結果をまとめる。また、CLEFIA、PRESENT、LEA が軽量ブロック暗号に関係する ISO/IEC 規格 (ISO/IEC 29192-2) [1] で採択されている状況を鑑み、2016 年度ガイドラインに記載されていない LEA も調査対象とした。なお、LEA に関しては安全性解析状況に関する調査結果だけでなく、その仕様（設計者、発表年、仕様参照先、特徴、主な実装性能評価結果、標準化状況）についても簡単にまとめる。

ここで、ブロック暗号に対する汎用的な安全性解析手法であるバイクリーク (Biclique) 攻撃 [44] とその派生攻撃に関し、本報告書での取扱いについて議論する。バイクリーク攻撃が提案された暗号方式に関し、この攻撃を一律に最良の攻撃としてラベル付けを行うことは誤解を招く可能性があると考え、本報告書ではバイクリーク攻撃を除いた解析手法の中から最大の攻撃可能ラウンド数を達成するものを最良の攻撃としてラベル付けを行うこととする。例えば、最初のバイクリーク攻撃である single-key setting における AES への攻撃を AES に対する最良の攻撃として取り扱う場合、「AES は破られている」と言う端的な結論になるが、Bogdanov らの解析論文 [44] の発表以来 10 年が経過しても、NIST は AES の安全性が危殆化したとはみなしていない。これは NISTIR 8319 [206] に記載されている以下の文章から読み取れる：

> Biclique attacks perform an exhaustive search over a reduced number of rounds of the cipher and can, therefore, only outperform exhaustive search over all rounds by a small constant factor. It is well known that slight improvements over exhaustive search are always possible (e.g., the “distributive technique” and “early abort technique” [11]); however, biclique attacks provide further speedups that do not apply to every block cipher.
> In NIST SP 800-57 Part 1, Revision 5 [2], “security strength” is defined in terms of the number of “operations” to break a cryptographic algorithm. If “operations” can be elementary operations rather than “full-round encryptions”, then

> biclique attacks do not affect the security strength of a cipher, as biclique attacks still perform exhaustive search over a reduced number of rounds.

このような見解に至る背景として、バイクリーク攻撃が本質的に秘密鍵の全数探索における計算量をわずかに改善するものであり、解析手法を発展させたとしても大きな計算量削減が見込まれないという予想があると考える。なお、CRYPTREC の見解は 2011 年に発表[*1]されており、次の文章から NIST の見解と同様であることが読み取れる：

> AES の解読（暗号鍵の推定）に必要な計算量は、鍵の総当たり（すべての鍵を試す場合）の計算量よりも若干小さくなっています。しかし、解読には大量のデータをあらかじめ用意する必要があるため、直ちに現実的な脅威につながることはないものと考えられます。

以上より、バイクリーク攻撃とその派生攻撃が提案された軽量ブロック暗号（本報告書では Midori、Piccolo、PRESENT、TWINE が該当）に関し、これらの攻撃が提案された事実については記載するものの、これらの攻撃を除いた解析手法の中から最大の攻撃可能ラウンド数を達成するものを最良の攻撃としてラベル付けを行うこととする。

3.1　CLEFIA

3.1.1　2016 年度ガイドラインに記載されている安全性解析状況

2016 年度ガイドライン [69] の第 4.1 節によると、以下のとおり記載されている。

> 様々な解析論文が発表されているが、仕様段数においては全数探索より効率的な攻撃は知られていない。13 段に簡略化した CLEFIA-128、14 段に簡略化した CLEFIA-192、15 段に簡略化した CLEFIA-256 に対してはそれぞれ全数探索より効率的な攻撃が知られている [43, 196]。

なお、CLEFIA-128、CLEFIA-192、CLEFIA-256 における仕様段数はそれぞれ 18、22、26 段である。

3.1.2　上記以降の安全性解析状況（2021 年 9 月現在）

Bogdanov ら [43] による零相関線形攻撃 (Zero-correlation linear attack) と Mala ら [196] による不能差分攻撃 (Impossible differential attack) に関する解析論文が発表されて以降、以下で示すような解析論文が発表されている。

- Boura ら [50] による不能差分攻撃
- Li ら [162] による切り詰め差分攻撃 (Truncated differential attack)

[*1] https://www.cryptrec.go.jp/topics/cryptrec-er-0001-2011.html

表 3.1　CLEFIA の安全性解析状況（CPs: 選択平文、KPs: 既知平文）

Cipher	Rounds	Attack type	Time	Data	Memory	Ref.
CLEFIA-128	12	Integral	$2^{116.7}$	$2^{113.0}$ CPs	N/A	[170]
	13	Impossible Differential	$2^{121.2}$	$2^{117.8}$ CPs	$2^{86.8}$	[196]
	13	Impossible Differential	$2^{114.6}$	$2^{116.2}$ CPs	$2^{83.2}$	[50]
	13	Truncated Differential	$2^{99.0}$	$2^{99.0}$ CPs	$2^{80.0}$	[162]
	14	Truncated Differential	$2^{108.0}$	$2^{100.0}$ CPs	$2^{101.3}$	[162]
CLEFIA-192	13	Impossible Differential	$2^{146.0}$	$2^{119.8}$ CPs	$2^{120.0}$	[260]
	13	Integral	$2^{180.5}$	$2^{113.0}$ CPs	N/A	[170]
	14	Zero-correlation Linear	$2^{180.2}$	$2^{127.5}$ KPs	$2^{115.0}$	[43]
	14	Impossible Differential	$2^{177.6}$	$2^{118.9}$ CPs	N/A	[250]
	14	Zero-correlation Linear	$2^{173.9}$	$2^{124.5}$ KPs	N/A	[280]
	14	Integral	$2^{166.7}$	$2^{128.0}$ CPs	N/A	[280]
	14	Truncated Differential	$2^{135.0}$	$2^{100.0}$ CPs	$2^{131.0}$	[162]
CLEFIA-256	14	Impossible Differential	$2^{212.0}$	$2^{120.3}$ CPs	$2^{121.0}$	[260]
	14	Integral	$2^{244.5}$	$2^{113.0}$ CPs	N/A	[170]
	15	Zero-correlation Linear	$2^{244.2}$	$2^{127.5}$ KPs	$2^{115.0}$	[43]
	15	Impossible Differential	$2^{242.1}$	$2^{119.3}$ CPs	N/A	[250]
	15	Zero-correlation Linear	$2^{237.9}$	$2^{124.5}$ KPs	N/A	[280]
	15	Integral	$2^{230.7}$	$2^{128.0}$ CPs	N/A	[280]
	15	Truncated Differential	$2^{203.0}$	$2^{100.0}$ CPs	$2^{139.0}$	[162]

- Tezcan と Selçuk [250] による不能差分攻撃
- Yi ら [280] による積分攻撃 (Integral attack) と零相関線形攻撃

表 3.1 は文献 [162] の Table 1 と文献 [280] の Table 1 に基づき、CLEFIA に対する安全性解析状況についてまとめたものである。表 3.1 から、全てのバリエーションにおいて Li ら [162] による切り詰め差分攻撃が最良の攻撃であることがわかる。

Li ら [162] は切り詰め差分特性を探索するための中間一致手法を提案し、Feistel 型ブロック暗号に対する汎用的な攻撃手法として一般化した上で、提案手法を CLEFIA の全てのバリエーションに適用した。その結果、Li らは CLEFIA に 10 段の切り詰め差分特性が存在することを明らかにし、発見した 10 段の切り詰め差分特性を使用して 18 段のうち 14 段に簡略化した CLEFIA-128、22 段のうち 14 段に簡略化した CLEFIA-192、26 段のうち 15 段に簡略化した CLEFIA-256 に対し、秘密鍵の全数探索よりも効率的に鍵回復攻撃が実行できることを示した。

3.1.3　安全性解析状況のまとめ

2021 年 9 月現在、様々な解析論文 [43, 50, 162, 170, 196, 250, 260, 280] が発表されているが、仕様段数において秘密鍵の全数探索よりも効率的に実行可能な攻撃は発表されていない。

CLEFIA に対する最良の攻撃は Li ら [162] によって提案された切り詰め差分攻撃であり、18 段のうち 14 段に簡略化した CLEFIA-128、22 段のうち 14 段に簡略化した CLEFIA-192、26 段のうち 15 段に簡略化した CLEFIA-256 に対しては、それぞれ秘密鍵の全数探索よりも効率的に鍵回復攻撃が実行できる。

3.2　LED

3.2.1　2016 年度ガイドラインに記載されている安全性解析状況

2016 年度ガイドライン [69] の第 4.1 節によると、以下のとおり記載されている。

> いくつかの解析論文が発表されているが、仕様段数においては全数探索より効率的な攻撃は知られていない。12 段に簡略化した LED-64、および 32 段に簡略化した LED-128 に対しては全数探索より効率的な攻撃が知られている [89]。

なお、LED-64、LED-128 における仕様段数はそれぞれ 32、48 段である。

3.2.2　上記以降の安全性解析状況（2021 年 9 月現在）

Dinur ら [89] による Even-Mansour 暗号への汎用的な攻撃に関する解析論文が発表されて以降、以下で示すような解析論文が発表されている。

- Nikolic ら [213] によるスライド攻撃 (Slidex attack)
- Soleimany [236] による確率的スライド攻撃 (Probabilistic slide attack)
- Dinur ら [90] による中間一致攻撃 (Meet-in-the-Middle attack)
- Sun ら [244] による積分識別攻撃 (Integral distinguishing attack)

表 3.2 と表 3.3 は文献 [89] の Table 1、文献 [236] の Table 1、文献 [90] の Table 1 に基づき、それぞれ single-key setting と related-key setting における LED の安全性解析状況についてまとめたものである。表 3.2 と表 3.3 から、single-key setting において Dinur ら [89] による Even-Mansour 暗号への汎用的な攻撃が最良の攻撃であり、related-key setting において Mendel ら [200] による差分攻撃が最良の攻撃であることがわかる。また、Sun ら [244] による積分識別攻撃の攻撃可能ステップ数は 1.5 steps であり、既存攻撃を改善しているとは言えない。

以上より、2021 年 9 月現在において、2016 年度ガイドラインに記載されている Dinur ら [89] の攻撃よりも効率的な攻撃が提案されていない。

表 3.2　Single-key setting における LED の安全性解析状況（CPs: 選択平文、KPs: 既知平文）

Cipher	Steps	Attack type	Time	Data	Memory	Ref.
LED-64	2	Meet-in-the-Middle	$2^{56.0}$	$2^{8.0}$ CPs	$2^{11.0}$	[140]
	2	Probabilistic Slide	$2^{51.5}$	$2^{41.5}$ KPs	$2^{42.5}$	[236]
	2	Meet-in-the-Middle	$2^{48.0}$	$2^{16.0}$ CPs	$2^{17.0}$	[90]
	2	Meet-in-the-Middle	$2^{48.0}$	$2^{48.0}$ KPs	$2^{48.0}$	[90]
	2	Probabilistic Slide	$2^{46.5}$	$2^{45.5}$ KPs	$2^{46.5}$	[236]
	3	Generic	$2^{60.2}$	$2^{49.0}$ KPs	$2^{60.0}$	[89]
LED-128	4	Meet-in-the-Middle	$2^{112.0}$	$2^{16.0}$ CPs	$2^{19.0}$	[140]
	4	Differential	$2^{96.0}$	$2^{64.0}$ KPs	$2^{64.0}$	[200]
	4	Slidex	$2^{96.0}$	$2^{32.0}$ KPs	$2^{32.0}$	[213]
	6	Slidex	$2^{124.4}$	$2^{59.0}$ KPs	$2^{59.0}$	[213]
	6	Generic	$2^{124.5}$	$2^{45.0}$ KPs	$2^{60.0}$	[89]
	8	Generic	$2^{123.8}$	$2^{49.0}$ KPs	$2^{60.0}$	[89]

表 3.3　Related-key setting における LED の安全性解析状況（CPs: 選択平文、KPs: 既知平文）

Cipher	Steps	Attack type	Time	Data	Memory	Ref.
LED-64	3	Differential	$2^{60.0}$	$2^{60.0}$	$2^{60.0}$	[200]
	3	Meet-in-the-Middle	$2^{49.0}$	$2^{49.0}$	$2^{59.0}$	[90]
	4	Differential	$2^{63.0}$	$2^{63.0}$	$2^{63.0}$	[200]

3.2.3　安全性解析状況のまとめ

2021 年 9 月現在、様々な解析論文 [89, 90, 140, 200, 213, 236, 244] が発表されているが、仕様段数において秘密鍵の全数探索よりも効率的に実行可能な攻撃は発表されていない。

Single-key setting において、LED に対する最良の攻撃は Dinur ら [89] によって提案された Even-Mansour 暗号への汎用的な攻撃であり、8 ステップのうち 3 ステップに簡略化した LED-64、および 12 ステップのうち 8 ステップに簡略化した LED-128 に対しては、それぞれ秘密鍵の全数探索よりも効率的に鍵回復攻撃が実行できる。

Related-key setting において、LED に対する最良の攻撃は Mendel ら [200] によって提案された差分攻撃であり、8 ステップのうち 4 ステップに簡略化した LED-64 に対しては、秘密鍵の全数探索よりも効率的に鍵回復攻撃が実行できる。

3.3 Midori

3.3.1 2016 年度ガイドラインに記載されている安全性解析状況

2016 年度ガイドライン [69] の第 4.1 節によると、以下のとおり記載されている。

> いくつかの解析論文が発表されているが、仕様段数においては全数探索より効率的な攻撃は知られていない。Midori64 については弱鍵が存在し、その弱鍵を使用している場合、仕様段数であっても効率的な攻撃が行える [111, 112]。また、12 段に簡略化した Midori64 に対してはより効率的な攻撃が知られている [173, 174]。

なお、Midori64、Midori128 における仕様段数はそれぞれ 16、20 段である。

3.3.2 上記以降の安全性解析状況（2021 年 9 月現在）

Guo ら [111, 112] による不変量部分空間攻撃 (Invariant subspace attack) と Lin ら [173, 174] による中間一致攻撃 (Meet-in-the-Middle attack) に関する解析論文が発表されて以降、以下で示すような解析論文が発表されている。

- Chen ら [58] による不能差分攻撃 (Impossible differential attack)
- Gérault と Lafourcade [107] による関連鍵差分攻撃 (Related-key differential attack)
- Tolba ら [257] による切り詰め差分攻撃 (Truncated differential attack)
- Todo ら [254, 255] による非線形不変量攻撃 (Nonlinear invariant attack)

その他、Midori を対象とした様々な解析論文が発表されている [12,26,32,33,117,243,244,289,290]。

表 3.4 と表 3.5 は文献 [107] の Table 1 と文献 [117] の Table 1 に基づき、single-key setting と related-key setting における Midori の安全性解析状況についてまとめたものである。表 3.4 から、single-key setting では Midori64 に対する中間一致攻撃 [173, 174] と Midori128 に対する切り詰め差分攻撃 [257] が最良の攻撃であることがわかる。なお、弱鍵を使用している場合には、Midori64 に対する不変部分空間攻撃 [111, 112] と非線形不変攻撃 [254, 255] が最良の攻撃となる。また、表 3.5 から、related-key setting では関連鍵差分攻撃 [107] が最良の攻撃であることがわかる。

Tolba ら [257] は Midori128 における S-box と MDS transformation の性質を詳細に分析し、確率 2^{-118} となる 10 段の切り詰め差分特性と確率 2^{-230} となる 13 段の切り詰め差分特性を発見した。また、発見した 13 段の切り詰め差分特性を使用し、20 段のうち 13 段に簡略化した Midori128 に対し、秘密鍵の全数探索よりも効率的に鍵回復攻撃が実行できることを示した。

Todo ら [254, 255] は Midori64 における S-box と MDS transformation の性質を詳細に分析することで、従来では不可能とみなされていた非線形近似手法の利用が可能であることを示した。Todo ら [254, 255] はこの攻撃を非線形不変量攻撃と呼び、この攻撃を適用することで Midori64 に弱鍵が 2^{64} 個あることを示すとともに、フルスペックの Midori64 を CBC、CFB、OFB、CTR

表 3.4　Single-key setting における Midori の安全性解析状況

Cipher	Rounds	Attack type	Time	Data	Ref.
Midori64	10	Meet-in-the-Middle	$2^{99.5}$	$2^{61.5}$	[173, 174]
	11	Meet-in-the-Middle	$2^{122.0}$	$2^{53.0}$	[173, 174]
	12	Meet-in-the-Middle	$2^{125.5}$	$2^{55.5}$	[173, 174]
	16 (full)	Invariant Subspace $(2^{32})^{a)}$	$2^{16.0}$	2	[111, 112]
	16 (full)	Nonlinear Invariant $(2^{64})^{a)}$	$2^{16.0}$	2	[254, 255]
Midori128	10	Impossible Differential	$2^{119.0}$	$2^{118.6}$	[58]
	10	Impossible Differential	$2^{116.7}$	$2^{116.1}$	[58]
	13	Truncated Differential	$2^{125.7}$	$2^{115.7}$	[257]
	13	Truncated Differential	$2^{119.0}$	$2^{119.0}$	[257]

[a)] Note that this attack only works if a key from the weak class is used.

表 3.5　Related-key setting における Midori の安全性解析状況

Cipher	Rounds	Attack type	Time	Data	Ref.
Midori64	14	Differential	$2^{59.0}$	$2^{116.0}$	[97]
	16 (full)	Differential	$2^{23.8}$	$2^{35.8}$	[107]
Midori128	20 (full)	Differential	$2^{43.7}$	$2^{43.7}$	[107]

モードで利用する場合に各ブロック 64 ビットのうち 32 ビットの平文を復元できることを示した。

Gérault と Lafourcade [107] は制約プログラミング (Constraint Programming) を用いて関連鍵差分特性を探索し、Midori64 において確率 2^{-14} となる 15 段の差分特性と確率 2^{-16} となる 16 段の差分特性を発見するとともに、Midori128 において確率 2^{-38} となる 19 段の差分特性と確率 2^{-40} となる 20 段の差分特性を発見した。さらに、Midori64 における 15 段の差分特性と Midori128 における 19 段の差分特性を使用し、フルスペックの Midori64/128 に対し、秘密鍵の全数探索よりも効率的に鍵回復攻撃が実行できることを示した。

3.3.3　安全性解析状況のまとめ

2021 年 9 月現在、様々な解析論文 [12, 26, 32, 33, 58, 107, 111, 112, 117, 173, 174, 243, 244, 254, 255, 257, 289, 290] が発表されているが、弱鍵を使用している場合と related-key setting の場合を除き、仕様段数において秘密鍵の全数探索よりも効率的に実行可能な攻撃は発表されていない。

Single-key setting において、Midori64 に対する最良の攻撃は Lin ら [173, 174] によって提案された中間一致攻撃であり、16 段のうち 12 段に簡略化した Midori64 に対しては、秘密鍵の全数探索よりも効率的に鍵回復攻撃が実行できる。Midori128 に対する最良の攻撃は Tolba ら [257] によって提案された切り詰め差分攻撃であり、20 段のうち 13 段に簡略化した Midori128 に対して

は、秘密鍵の全数探索よりも効率的に鍵回復攻撃が実行できる。また、Midori64 については弱鍵が存在し、弱鍵を使用している場合には仕様段数であっても効率的な鍵回復攻撃 [111, 112] とメッセージ復元攻撃 [254, 255] が可能となる。

Related-key setting において、Midori64/128 に対する最良の攻撃は Gérault と Lafourcade [107] によって提案された関連鍵差分攻撃であり、それぞれ仕様段数であっても秘密鍵の全数探索より効率的に鍵回復攻撃が実行できる。

3.4　Piccolo

3.4.1　2016 年度ガイドラインに記載されている安全性解析状況

2016 年度ガイドライン [69] の第 4.1 節によると、以下のとおり記載されている。

> いくつかの解析論文が発表されているが、仕様段数においては全数探索より効率的な攻撃は知られていない。14 段に簡略化した Piccolo-80、および 21 段に簡略化した Piccolo-128 に対してはより効率的な攻撃 [235]、および関連鍵攻撃 [202] が知られている。

なお、Piccolo-80、Piccolo-128 における仕様段数はそれぞれ 25、31 段である。

3.4.2　上記以降の安全性解析状況（2021 年 9 月現在）

Shibutani ら [235] による安全性解析と Minier [202] による関連鍵不能差分攻撃 (Related-key impossible differential attack) に関する解析論文が発表されて以降、以下で示すような解析論文が発表されている。

- Isobe と Shibutani [140] による中間一致攻撃 (Meet-in-the-Middle attack)
- Azimi ら [17] による不能差分攻撃 (Impossible differential attac)
- Tolba ら [256] による中間一致攻撃
- Liu ら [182] による中間一致攻撃

その他、Piccolo を対象としたバイクリーク攻撃 (Biclique attack) に関するいくつかの解析論文 [116, 237] も発表されている。

表 3.6 と表 3.7 は文献 [256] の Table 1 と Table 2、文献 [116] の Table 2、文献 [182] の Table 1 に基づき、single-key setting と related-key setting における Piccolo の安全性解析状況についてまとめたものである。表 3.6 と表 3.7 から、single-key setting において Isobe と Shibutani [140] と Liu ら [182] による中間一致攻撃が最良の攻撃であり、related-key setting において Minier [202] による関連鍵不能差分攻撃が最良の攻撃であることがわかる。

Isobe と Shibutani [140] は既存手法 (*partial matching*、*splice and cut*, *initial structure*) と新しい手法 (*equivalent transformation*) を組み合わせた中間一致攻撃を提案し、提案手法を XTEA、

表 3.6　Single-key setting における Piccolo の安全性解析状況（CCs: 選択暗号文、CPs: 選択平文）

Cipher	Rounds	Attack type	Time	Data	Memory	Ref.
Piccolo-80	12	Impossible Differential	$2^{55.2}$	$2^{36.4}$ CCs	$2^{63.0}$	[17]
	13	Impossible Differential	$2^{69.7}$	$2^{43.3}$ CPs	$2^{62.0}$	[17]
	14	Meet-in-the-Middle	$2^{75.4}$	$2^{43.3}$ CPs	$2^{73.5}$	[256]
	14	Meet-in-the-Middle[a)]	$2^{73.0}$	$2^{64.0}$	$2^{5.0}$	[140]
	14	Meet-in-the-Middle	$2^{67.4}$	$2^{52.0}$ CPs	$2^{64.9}$	[182]
Piccolo-128	15	Impossible Differential	$2^{125.4}$	$2^{58.7}$ CPs	$2^{61.0}$	[17]
	16	Meet-in-the-Middle	$2^{123.0}$	$2^{48.0}$ CPs	$2^{113.5}$	[256]
	17	Meet-in-the-Middle	$2^{126.9}$	$2^{48.0}$ CPs	$2^{126.0}$	[256]
	18	Meet-in-the-Middle	$2^{126.6}$	$2^{52.0}$ CPs	$2^{125.3}$	[182]
	21	Meet-in-the-Middle[a)]	$2^{121.0}$	$2^{64.0}$	$2^{6.0}$	[140]

[a)] Note that this attack requires the full codebook or more.

表 3.7　Related-key setting における Piccolo の安全性解析状況

Cipher	Rounds	Attack type	Time	Data	Ref.
Piccolo-80	14	Impossible Differential[a)]	$2^{68.2}$	$2^{68.2}$	[202]
Piccolo-128	21	Impossible Differential[a)]	$2^{117.8}$	$2^{117.8}$	[202]

[a)] Note that this attack requires the full codebook or more.

LED、Piccolo に適用した。結果として、25 段のうち 14 段に簡略化した Piccolo-80 と 31 段のうち 21 段に簡略化した Piccolo-128 に対し、秘密鍵の全数探索よりも効率的に鍵回復攻撃が実行できることを示した。なお、攻撃にかかるデータ量がフルコードブックであることに注意されたい。

Liu ら [182] は Piccolo の key schedule と MDS matrix を詳細に分析し、δ-set と呼ばれる概念を用いて Piccolo-80 に対する 5 段の識別子と Piccolo-128 に対する 7 段の識別子を構成できることを示した。さらに、これらの識別子を用いて 25 段のうち 14 段に簡略化した Piccolo-80 と 31 段のうち 18 段に簡略化した Piccolo-128 に対し、秘密鍵の全数探索よりも効率的に鍵回復攻撃が実行できることを示した。

3.4.3　安全性解析状況のまとめ

2021 年 9 月現在、様々な解析論文 [17, 116, 140, 182, 202, 235, 237, 256] が発表されているが、仕様段数において秘密鍵の全数探索よりも効率的に実行可能な攻撃は発表されていない。

Single-key setting において、Piccolo-80/128 に対する最良の攻撃は Isobe と Shibutani [140] と Liu ら [182] によって提案された中間一致攻撃であり、25 段のうち 14 段に簡略化した Piccolo-80

と 31 段のうち 21 段に簡略化した Piccolo-128 に対しては、それぞれ秘密鍵の全数探索よりも効率的に鍵回復攻撃が実行できる。

Related-key setting において、Piccolo-80/128 に対する最良の攻撃は Minier [202] によって提案された関連鍵不能差分攻撃であり、25 段のうち 14 段に簡略化した Piccolo-80 と 31 段のうち 21 段に簡略化した Piccolo-128 に対しては、それぞれ秘密鍵の全数探索よりも効率的に鍵回復攻撃が実行できる。

3.5　PRESENT

3.5.1　2016 年度ガイドラインに記載されている安全性解析状況

2016 年度ガイドライン [69] の第 4.1 節によると、以下のとおり記載されている。

> 様々な解析論文が発表されているが、仕様段数においては全数探索より効率的な攻撃は知られていない。26 段に簡略化した PRESENT-80/128 に対してはより効率的な攻撃が知られている [39, 59]。

なお、PRESENT-80/128 における仕様段数は 31 段である。

3.5.2　上記以降の安全性解析状況（2021 年 9 月現在）

Blondeau と Nyberg [39] による切り詰め差分 (Truncated differential) 特性と多次元線形 (Multidimentional linear) 特性との関係性を利用した安全性解析と Cho [59] による線形攻撃 (Linear attack) に関する解析論文が発表されて以降、以下で示すような解析論文が発表されている。

- Blondeau ら [41] による中間一致 (Meet-in-the-Middle) 手法を用いた切り詰め差分攻撃
- Zheng と Zhang [292] による多次元線形攻撃
- Blondeau と Nyberg [40] による多次元線形攻撃
- Bogdanov ら [46] による多次元線形攻撃
- Flórez-Gutiérrez と Naya-Plasencia [102] による多次元線形攻撃

なお、Blondeau ら [41] の攻撃は known-key setting において実行可能であり、PRESENT-80/128 に対しては仕様段数であっても効率的に識別子を構成可能であると示されている。その他、PRESENT を対象としたバイクリーク攻撃 (Biclique attack) に関するいくつかの解析論文 [8, 143, 144] も発表されている。

表 3.8 は文献 [102] の Table 3 に基づき、single-key setting における PRESENT の安全性解析状況についてまとめたものである。表 3.8 から、single-key setting において Flórez-Gutiérrez と Naya-Plasencia [102] による多次元線形攻撃が最良の攻撃であることがわかる。

Flórez-Gutiérrez と Naya-Plasencia [102] は Collard ら [24] によって提案された線形攻撃のた

表 3.8　Single-key setting における PRESENT の安全性解析状況（KPs: 既知平文）

Cipher	Rounds	Attack type	Time	Data	Memory	Ref.
PRESENT-80	26	Multidimentional Linear	$2^{72.0}$	$2^{64.0}$ KPs	$2^{32.0}$	[59]
	26	Multidimentional Linear	$2^{72.0}$	$2^{63.8}$ KPs	$2^{32.0}$	[40, 59]
	26	Multidimentional Linear	$2^{71.8}$	$2^{60.8}$ KPs	$2^{44.0}$	[102]
	26	Multidimentional Linear	$2^{68.6}$	$2^{63.0}$ KPs	$2^{48.0}$	[46]
	26	Multidimentional Linear	$2^{68.2}$	$2^{61.1}$ KPs	$2^{44.0}$	[102]
	27	Multidimentional Linear	$2^{77.3}$	$2^{63.8}$ KPs	$2^{48.0}$	[46]
	27	Multidimentional Linear	$2^{74.0}$	$2^{64.0}$ KPs	$2^{67.0}$	[292]
	27	Multidimentional Linear	$2^{72.0}$	$2^{63.4}$ KPs	$2^{44.0}$	[102]
	28	Multidimentional Linear	$2^{77.4}$	$2^{64.0}$ KPs	$2^{51.0}$	[102]
PRESENT-128	28	Multidimentional Linear	$2^{122.0}$	$2^{64.0}$ KPs	$2^{84.6}$	[102]

めのアルゴリズムにインスピレーションを受け、このアルゴリズムの鍵回復パートを改善するとともに、秘密鍵と key schedule の依存関係を考慮したアルゴリズムを提案した。結果として、31 段のうち 28 段に簡略化した PRESENT-80/128 に対し、秘密鍵の全数探索よりも効率的に鍵回復攻撃が実行できることを示した。なお、攻撃にかかるデータ量がフルコードブックであることに注意されたい。

3.5.3　安全性解析状況のまとめ

2021 年 9 月現在、様々な解析論文 [8, 39, 40, 41, 46, 59, 102, 143, 144, 292] が発表されているが、known-key setting の場合を除き、仕様段数において秘密鍵の全数探索よりも効率的に実行可能な攻撃は発表されていない。

Single-key setting において、PRESENT-80/128 に対する最良の攻撃は Flórez-Gutiérrez と Naya-Plasencia [102] によって提案された多次元線形攻撃であり、31 段のうち 28 段に簡略化した PRESENT-80/128 に対しては、秘密鍵の全数探索よりも効率的に鍵回復攻撃が実行できる。

Known-key setting において、PRESENT-80/128 に対する最良の攻撃は Blondeau ら [41] によって提案された中間一致手法を用いた切り詰め差分攻撃であり、それぞれ仕様段数であっても効率的に識別攻撃を実行できる。

3.6　PRINCE

3.6.1　2016 年度ガイドラインに記載されている安全性解析状況

2016 年度ガイドライン [69] の第 4.1 節によると、以下のとおり記載されている。

> いくつかの解析論文が発表されているが、仕様段数においては全数探索より効率的

表 3.9　PRINCE の安全性解析状況（CPs: 選択平文、KPs: 既知平文）

Rounds	Attack type	Time	Data	Memory	Ref.
4	Integral	$2^{64.0}$	$2^{4.0}$ CPs	$2^{4.0}$	[142]
4	Meet-in-the-Middle	$2^{43.3}$	$2^{5.0}$ KPs	$2^{26.7}$	[79]
6	Meet-in-the-Middle	$2^{101.1}$	$2^{6.0}$ KPs	$2^{34.0}$	[79]
6	Integral	$2^{41.0}$	$2^{18.6}$ CPs	$2^{16.0}$	[142]
6	Meet-in-the-Middle	$2^{33.7}$	$2^{16.0}$ CPs	$2^{31.9}$	[78, 79]
6	Differential	$2^{32.9}$	$2^{14.9}$ CPs	$2^{27.0}$	[78, 79]
8	Sieve-in-the-Middle	$2^{124.0}$	$2^{1.0}$ KPs	2^{20}	[54]
8	Meet-in-the-Middle	$2^{60.0}$	$2^{53.0}$ CPs	$2^{30.0}$	[161]
8	Meet-in-the-Middle	$2^{50.7}$	$2^{16.0}$ CPs	$2^{84.9}$	[78, 79]
10	Meet-in-the-Middle	$2^{68.0}$	$2^{57.0}$ CPs	$2^{41.0}$	[78, 79]
10	Multiple differential	$2^{60.6}$	$2^{57.9}$ CPs	$2^{61.5}$	[52]

な攻撃は知られていない。10 段に簡略化した PRINCE に対してはより効率的な攻撃が知られている [52]。

なお、PRINCE における仕様段数は 12 段である。

3.6.2　上記以降の安全性解析状況（2021 年 9 月現在）

Canteaut ら [52] による多重差分攻撃 (Multiple differential attack) に関する解析論文が発表されて以降、以下で示すような解析論文が発表されている。

- Derbez と Perrin [78, 79] による差分攻撃 (Differential attack) と中間一致攻撃 (Meet-in-the-Middle attack)

その他、PRINCE を対象としたいくつかの解析論文 [12, 110, 142, 222] が発表されている。なお、文献 [142, 222] ではフルスペックの PRINCE に対する鍵回復攻撃が示されているものの、これらの解析結果はバイクリーク攻撃 (Biclique attack) 手法を使用するなど秘密鍵の全数探索における計算量をわずかに改善するものであることに注意されたい。

表 3.9 は文献 [222] の Table 1 に基づき、single-key setting における PRINCE の安全性解析状況についてまとめたものである。表 3.9 から、Canteaut ら [52] による多重差分攻撃が最良の攻撃であることがわかる。つまり、2021 年 9 月現在において、2016 年度ガイドラインに記載されている Canteaut ら [52] の攻撃よりも効率的な攻撃が提案されていない。

3.6.3　安全性解析状況のまとめ

2021 年 9 月現在、様々な解析論文 [12, 52, 54, 78, 79, 102, 110, 142, 161, 222] が発表されている。

Single-key setting において、PRINCE に対する最良の攻撃は Canteaut ら [52] による多重差分攻撃であり、12 段のうち 10 段に簡略化した PRINCE に対しては、秘密鍵の全数探索よりも効率的に鍵回復攻撃が実行できる。

3.7　Simon

3.7.1　2016 年度ガイドラインに記載されている安全性解析状況

2016 年度ガイドライン [69] の第 4.1 節によると、以下のとおり記載されている。

> 様々な解析論文が発表されているが、仕様段数においては全数探索より効率的な攻撃は知られていない。23、25、31、38、53 段に簡略化したブロック長 32、48、64、96、128-bit の Simon に対してはより効率的な攻撃が知られている [55]。

なお、Simon32、Simon48、Simon64、Simon96、Simon128 における仕様段数はそれぞれ最大で 32、36、44、54、72 段である[*2]。

3.7.2　上記以降の安全性解析状況（2021 年 9 月現在）

Chen と Wang [55] による線形攻撃 (Linear attack) に関する解析論文が発表されて以降、以下で示すような解析論文が発表されている。

- Derbez と Fouque [77] による不能差分攻撃 (Impossible differential attack)
- Qiao ら [218] による差分攻撃 (Differential attack)
- Hao と Meier [122] による切り詰め差分攻撃 (Truncated differential attack)
- Rohit と Gong [226] による Correlated sequence attack
- Wang ら [264] による差分攻撃
- Chu ら [61] による積分攻撃 (Integral attack)
- Lee ら [155] による関連鍵線形攻撃 (Related-key linear attack)
- Leurent ら [158] による差分攻撃と線形攻撃

その他、Simon を対象とした様々な解析論文 [22, 131, 132, 133, 151, 189, 190, 269] が発表されている。なお、Hao と Meier [122] の攻撃は known-key setting において実行可能であり、29、32、37、47、63 段に簡略化した Simon32/48/64/96/128 に対し、それぞれ効率的に識別子を構成可能

[*2] 鍵長によってさらに細分化される。例えば、Simon64 において 96 ビット秘密鍵を使用する場合と 128 ビット秘密鍵を使用する場合の仕様段数はそれぞれ 42、44 段である。

表 3.10　Single-key setting における Simon の安全性解析状況

Cipher	Rounds	Attack type	Time	Data	Ref.
Simon32	20	Impossible Differential	$2^{62.8}$	$2^{32.0}$	[77]
	21	Differential	$2^{55.3}$	$2^{31.0}$	[264]
	22	Differential	$2^{58.8}$	$2^{32.0}$	[218]
	23	Linear	$2^{61.8}$	$2^{31.2}$	[55]
	24	Integral	$2^{63.0}$	$2^{32.0}$	[61]
	24	Correlated Sequence	$2^{61.8}$	$2^{31.2}$	[226]
	25	Correlated Sequence	$2^{61.8}$	$2^{31.2}$	[226]
	26	Correlated Sequence	$2^{61.8}$	$2^{31.2}$	[226]
	27	Correlated Sequence	$2^{61.8}$	$2^{31.2}$	[226]
Simon48	24	Integral	$2^{71.0}$	$2^{48.0}$	[61]
	24	Linear	$2^{67.9}$	$2^{47.9}$	[55]
	25	Integral	$2^{95.0}$	$2^{48.0}$	[61]
	25	Linear	$2^{89.9}$	$2^{47.9}$	[55]
Simon64	30	Linear	$2^{93.6}$	$2^{63.5}$	[55]
	31	Linear	$2^{120.0}$	$2^{63.5}$	[55]
Simon96	37	Linear	$2^{88.0}$	$2^{95.2}$	[55]
	38	Linear	$2^{136.0}$	$2^{95.2}$	[55]
	45	Linear	$2^{136.5}$	$2^{95.0}$	[158]
Simon128	49	Linear	$2^{120.0}$	$2^{127.6}$	[55]
	51	Linear	$2^{184.0}$	$2^{127.6}$	[55]
	53	Linear	$2^{248.0}$	$2^{127.6}$	[55]
	56	Linear	$2^{249.0}$	$2^{126.0}$	[158]

であると示されている。

表 3.10 と表 3.11 は文献 [55] の Table 1、文献 [226] の Table 1、文献 [61] の Table 1、文献 [155] の Table 1、文献 [158] の Table 1 に基づき、single-key setting と related-key setting における Simon の安全性解析状況についてまとめたものである。表 3.10 と表 3.11 から、single-key setting において Chen と Wang [55] による線形攻撃、Rohit と Gong [226] による Correlated sequence attack、Leurent ら [158] による線形攻撃が最良の攻撃であり、related-key setting において Lee ら [155] による関連鍵線形攻撃が最良の攻撃であることがわかる。

Rohit と Gong [226] は各ラウンドにおける内部状態 (sequence) とラウンド鍵との関係性について詳細に分析し、これらの相関性を利用して秘密鍵を復元するための新しい攻撃手法である correlated sequence attack を提案した。結果として、32 段のうち 27 段に簡略化した Simon32 に

表 3.11　Related-key setting における Simon の安全性解析状況

Cipher	Rounds	Attack type	Time	Data	Ref.
Simon32	23	Linear	$2^{46.7}$	$2^{46.3}$	[155]
Simon48	28	Linear	$2^{71.1}$	$2^{70.9}$	[155]
Simon64	34	Linear	$2^{95.5}$	$2^{95.3}$	[155]
Simon128	55	Linear	$2^{175.0}$	$2^{174.7}$	[155]
	62	Linear	$2^{190.8}$	$2^{190.4}$	[155]

対し、秘密鍵の全数探索よりも効率的に鍵回復攻撃が実行できることを示した。

Leurent ら [158] は既存研究 [9, 25, 37, 55, 149, 150, 189, 218, 269] で示された Simon に対する差分攻撃と線形攻撃のための強力なクラスタリング効果にインスピレーションを受け、さらに強力なクラスタリング効果を調査するためのフレームワークを提案した。結果として、提案手法を応用することで既存のものよりも高い確率となる差分特性と線形特性が得られることを明らかにするとともに、既存の鍵回復攻撃手法 [102, 218, 264] を応用することで 54 段のうち 45 段に簡略化した Simon96 と 72 段のうち 56 段に簡略化した Simon128 に対し、秘密鍵の全数探索よりも効率的に鍵回復攻撃が実行できることを示した。

Lee ら [155] はラウンド鍵（関連鍵）の情報を含めて線形近似する手法を提案し、Matsui's Algorithm と組み合わせることで関連鍵線形攻撃のための汎用的なフレームワークを提案した。結果として、related-key setting において 23、28、34、62 段に簡略化した Simon32/48/64/128 に対し、秘密鍵の全数探索よりも効率的に鍵回復攻撃が実行できることを示した。

3.7.3　安全性解析状況のまとめ

2021 年 9 月現在、様々な解析論文 [22, 55, 61, 77, 122, 131, 132, 133, 151, 155, 158, 189, 190, 218, 226, 264, 269] が発表されているが、仕様段数において秘密鍵の全数探索よりも効率的に実行可能な攻撃は発表されていない。

Single-key setting において、Simon に対する最良の攻撃は Chen と Wang [55] によって提案された線形攻撃、Rohit と Gong [226] によって提案された Correlated sequence attack、Leurent ら [158] による線形攻撃であり、27、25、31、45、56 段に簡略化した Simon32/48/64/96/128 に対しては、それぞれ秘密鍵の全数探索よりも効率的に鍵回復攻撃が実行できる。

Known-key setting において、Simon に対する最良の攻撃は Hao と Meier [122] によって提案された切り詰め差分攻撃であり、29、32、37、47、63 段に簡略化した Simon32/48/64/96/128 に対しては、それぞれ効率的に識別攻撃が実行できる。

Related-key setting において、Simon に対する最良の攻撃は Lee ら [155] によって提案された線形攻撃であり、23、28、34、62 段に簡略化した Simon32/48/64/128 に対しては、それぞれ秘密鍵の全数探索よりも効率的に鍵回復攻撃が実行できる。

3.8　Speck

3.8.1　2016 年度ガイドラインに記載されている安全性解析状況

2016 年度ガイドライン [69] の第 4.1 節によると、以下のとおり記載されている。

> 様々な解析論文が発表されているが、仕様段数においては全数探索より効率的な攻撃は知られていない。14、15、19、17、19 段に簡略化したブロック長 32、48、64、96、128-bit の Speck に対してはより効率的な攻撃が知られている [88]。

なお、Speck32、Speck48、Speck64、Speck96、Speck128 における仕様段数はそれぞれ最大で 22、23、27、29、34 段である[*3]。

3.8.2　上記以降の安全性解析状況（2021 年 9 月現在）

Dinur [88] による差分攻撃 (Differential attack) に関する解析論文が発表されて以降、以下で示すような解析論文が発表されている。

- Song ら [240] による差分攻撃
- Sun ら [245] による差分・線形特性 (Differential/Linear trails) 探索

その他、Speck を対象とした差分・線形特性などの自動探索に関する解析論文 [38, 104, 136, 137, 148, 186, 187, 188] や深層学習を用いた攻撃に関する解析論文 [22, 28, 56, 57, 109, 262] が発表されている。

表 3.12 は文献 [240] の Table 1 に基づき、single-key setting における Speck の安全性解析状況についてまとめたものである。表 3.12 から、single-key setting において Song ら [240] による差分攻撃が最良の攻撃であることがわかる。また、表 3.13 は文献 [245] の Table 1 に基づき、Speck に対する差分・線形識別子の構成可能段数についてまとめたものである。表 3.13 から、Speck32/48/64 に対しては Sun ら [245] による識別攻撃が最良の攻撃であり、Speck96/128 に対しては Song ら [240] による識別攻撃が最良の攻撃であることがわかる。

Song ら [240] は ARX ブロック暗号に対する差分特性の自動探索手法に着目し、Mouha と Preneel [208] が提案した SMT solver による自動探索手法を改善することで、既存手法よりも効率的な自動探索手法を提案した。結果として、17、20 段に簡略化した Speck96/128 に対し、効率的に識別攻撃が実行できることを示した。また、Dinur [88] と Abed ら [9] が提案したそれぞれの鍵回復攻撃手法を改善し、Speck の全てのバリエーションに対し、既存攻撃 [88] よりも効率的に鍵回復攻撃が実行できることを示した。

[*3] 鍵長によってさらに細分化される。例えば、Speck64 において 96 ビット秘密鍵を使用する場合と 128 ビット秘密鍵を使用する場合の仕様段数はそれぞれ 26、27 段である。

表 3.12　Single-key setting における Speck の安全性解析状況

Cipher	Rounds	Attack type	Time	Data	Ref.
Speck32	14	Differential	$2^{63.0}$	$2^{31.0}$	[88]
	14	Differential	$2^{61.4}$	$2^{29.4}$	[240]
Speck48	14	Differential	$2^{65.0}$	$2^{41.0}$	[88]
	15	Differential	$2^{89.0}$	$2^{41.0}$	[88]
	15	Differential	$2^{68.3}$	$2^{44.3}$	[240]
	16	Differential	$2^{92.3}$	$2^{44.3}$	[240]
Speck64	18	Differential	$2^{93.0}$	$2^{61.0}$	[88]
	19	Differential	$2^{125.0}$	$2^{61.0}$	[240]
	19	Differential	$2^{92.6}$	$2^{60.6}$	[88]
	20	Differential	$2^{124.6}$	$2^{60.6}$	[240]
Speck96	16	Differential	$2^{85.0}$	$2^{85.0}$	[88]
	17	Differential	$2^{133.0}$	$2^{85.0}$	[88]
	20	Differential	$2^{94.9}$	$2^{94.9}$	[240]
	23	Differential	$2^{142.9}$	$2^{94.9}$	[240]
Speck128	17	Differential	$2^{113.0}$	$2^{113.0}$	[88]
	18	Differential	$2^{177.0}$	$2^{113.0}$	[88]
	19	Differential	$2^{241.0}$	$2^{113.0}$	[88]
	23	Differential	$2^{124.4}$	$2^{124.4}$	[240]
	24	Differential	$2^{188.4}$	$2^{124.4}$	[240]
	25	Differential	$2^{252.4}$	$2^{124.4}$	[240]

Sun ら [245] は自動探索ツール SAT solver のための新しいエンコーディング手法を提案し、SAT solver による自動探索の高速化を実現した。結果として、Speck32/48/64 に対しては仕様段数であっても効率的に識別攻撃が実行できることを示した。なお、Sun ら [245] は Speck に対する鍵回復攻撃について言及していない。

3.8.3　安全性解析状況のまとめ

2021 年 9 月現在、様々な解析論文 [22, 28, 38, 56, 57, 88, 104, 109, 136, 137, 148, 186, 187, 188, 240, 245, 262] が発表されているが、仕様段数において秘密鍵の全数探索よりも効率的に実行可能な攻撃は発表されていない。

Single-key setting において、Speck に対する最良の鍵回復攻撃は Song ら [240] によって提案された差分攻撃であり、14、16、20、21、25 段に簡略化した Speck32/48/64/96/128 に対しては、それぞれ秘密鍵の全数探索よりも効率的に鍵回復攻撃が実行できる。また、Speck に対する最良

表 3.13　Speck に対する差分・線形識別子の構成可能段数

Attack type	Speck32	Speck48	Speck64	Speck96	Speck128	Ref.
Differential	10	9	8	7	6	[38]
	10	11	15	**17**	**20**	[240]
	9	11	15	16	19	[104]
	10	12	16	8	8	[188]
	22	**18**	**27**	10	9	[245]
Linear	6	–	–	–	–	[38]
	9	10	13	**15**	**16**	[104]
	22	11	13	9	9	[186]
	22	13	15	9	9	[188]
	22	**23**	**27**	14	10	[245]

の識別攻撃は Song ら [240] によって提案された差分攻撃と Sun ら [245] による線形攻撃であり、Speck32/48/64 に対しては仕様段数であっても効率的に識別攻撃を実行でき、17、20 段に簡略化した Speck96/128 に対してはそれぞれ効率的に識別攻撃を実行できる。

3.9　TWINE

3.9.1　2016 年度ガイドラインに記載されている安全性解析状況

2016 年度ガイドライン [69] の第 4.1 節によると、以下のとおり記載されている。

> いくつかの解析論文が発表されているが、仕様段数においては全数探索より効率的な攻撃は知られていない。

3.9.2　上記以降の安全性解析状況（2021 年 9 月現在）

TWINE [248] が提案されて以降、以下で示すような解析論文が発表されている。

- Lin ら [175] による多次元零相関線形攻撃 (Multidimentional zero-correlation linear attack)

その他、TWINE を対象とした様々な解析論文 [11, 36, 42, 63, 146, 211, 214, 258, 270, 272, 293] が発表されている。なお、文献 [11, 63, 146, 211, 258] ではバイクリーク攻撃 (Biclique attack) 手法、又はその派生攻撃手法が使用されていることに注意されたい。

表 3.14 は文献 [175] の Table 1 に基づき、single-key setting における TWINE の安全性解析状況についてまとめたものである。表 3.14 から、single-key setting において Lin ら [175] による多

表 3.14　Single-key setting における TWINE の安全性解析状況（CPs: 選択平文、KPs: 既知平文）

Cipher	Rounds	Attack type	Time	Data	Memory	Ref.
TWINE-80	23	Impossible Differential	$2^{79.1}$	$2^{57.9}$ CPs	$2^{84.1}$	[293]
	23	Multidim. ZC Linear	$2^{73.0}$	$2^{62.1}$ KPs	$2^{60.0}$	[175]
TWINE-128	25	Meet-in-the-Middle	$2^{124.7}$	$2^{48.0}$ CPs	$2^{109.0}$	[36]
	25	Impossible Differential	$2^{124.5}$	$2^{59.1}$ CPs	$2^{78.1}$	[36]
	25	Multidim. ZC Linear	$2^{122.1}$	$2^{62.1}$ KPs	$2^{60.0}$	[270]
	25	Multidim. ZC Linear	$2^{119.0}$	$2^{62.1}$ KPs	$2^{60.0}$	[175]

次元零相関線形攻撃が最良の攻撃であることがわかる。

Lin ら [175] は、Dunkelman らによって提案された *key-bridging technique* [98,99] にインスピレーションを受け、鍵スケジュールを記述した連立方程式を解くことでブロック暗号の *key-bridges* を自動的に探索するフレームワークを提案した。このフレームワークは *knowledge-propagation phase* と *relation-derivation phase* で構成されている。結果として、36 段のうち 23 段に簡略化した TWINE-80 と 36 段のうち 25 段に簡略化した TWINE-128 に対し、提案したフレームワークと組み合わせて多次元零相関線形攻撃を適用することにより、秘密鍵の全数探索よりも効率的に鍵回復攻撃が実行できることを示した。

3.9.3　安全性解析状況のまとめ

2021 年 9 月現在、様々な解析論文 [11,36,42,63,146,175,211,214,258,270,272,293] が発表されている。

Single-key setting において、TWINE に対する最良の攻撃は Lin ら [175] による多次元零相関線形攻撃であり、36 段のうち 23 段に簡略化した TWINE-80 と 36 段のうち 25 段に簡略化した TWINE-128 に対しては、それぞれ秘密鍵の全数探索よりも効率的に鍵回復攻撃が実行できる。

3.10　LEA

3.10.1　仕様

■設計者　Deukjo Hong[1]、Jung-Keun Lee[1]、Dong-Chan Kim[1]、Daesung Kwon[1]、Kwon Ho Ryu[1]、Dong-Geon Lee[2]

(1: 韓国電子通信研究院 / 韓国、2: 釜山大学校 / 韓国)

■発表年（発表学会等）　2013 (WISA 2013 [129])

■仕様参照先　[129]

表 3.15　LEA の全体構造、ブロック長、鍵長、構成段数

全体構造	Addition-Rotation-XOR (ARX) 型		
ブロック長 [bit]	128		
鍵長 [bit]	128 (LEA-128)	192 (LEA-192)	256 (LEA-256)
構成段数 [段]	24	28	32

表 3.16　LEA のハードウェア実装評価結果

Algorithm	Area [GE]	Cycles/block	Throughput@100KHz [kbps]	Ref.
LEA-128(Enc)	3,826	168	76.19	[129]
LEA-128(Enc)	5,426	24	533.33	[129]

表 3.17　LEA のソフトウェア実装評価結果

Algorithm	ROM [byte]	RAM [byte]	Cycles/byte [Enc/Dec]	Platform	Ref.
LEA-128	590	32	326.94/–	ARM926EJ-S	[129]
LEA-128	–	–	20.06/–	ARM926EJ-S	[129]
LEA-128	–	–	9.29/14.83	Intel Core 2 Quad Q6600	[129]
LEA-128	–	–	9.29/14.52	Intel Core i5-2500	[129]
LEA-128	–	–	8.85/14.50	AMD Phenom II X4 965	[129]
LEA-128	–	–	8.55/14.05	AMD Opteron 6176 SE	[129]
LEA-128	9,674	832	103.59/–	MCF5213	[129]
LEA-128	704	32	829.25/–	MCF5213	[129]

■特徴　設計者らは LEA がソフトウェア実装における高速な暗号化処理が可能であり、オーバーヘッドの軽減による低消費電力性能を持つとともに、コードサイズの小さいコンパクトな実装が可能であると主張している。また、構成段数の設定においては未知の攻撃への対策として 1.5 倍のセキュリティマージンを設けることにより、ブロック暗号に対する全ての既存攻撃に対して十分な安全性を持っていると主張している。LEA の全体構造、ブロック長、鍵長、構成段数については、表 3.15 のとおり。

■主な実装性能評価結果　LEA のハードウェア・ソフトウェア実装評価結果をそれぞれ表 3.16 と表 3.17 に示す。

■標準化状況　ISO/IEC 29192-2 [1]

表 3.18　Single-key setting における LEA の安全性解析状況（CPs: 選択平文）

Cipher	Rounds	Attack type	Time	Data	Memory	Ref.
LEA-128	12	Differential	$2^{84.0}$	$2^{100.0}$ CPs	$2^{84.1}$	[129]
	14	Differential	$2^{124.0}$	$2^{124.0}$ CPs	$2^{22.0}$	[240]
LEA-192	14	Differential	$2^{124.0}$	$2^{124.0}$ CPs	$2^{22.0}$	[240]
LEA-256	15	Differential	$2^{252.0}$	$2^{124.0}$ CPs	$2^{22.0}$	[240]

表 3.19　LEA-128 の差分、線形、差分線形、ブーメラン特性

Cipher	Rounds	Attack type	Probability or Bias	Ref.
LEA-128	13	Differential	$2^{-123.8}$	[240]
	11	Linear	$2^{-62.0}$	[129]
	14	Differential-linear	$2^{-57.0}$	[129]
	14	Boomerang	$2^{-108.0}$	[129]
	16	Boomerang	$2^{-117.1}$	[148]

3.10.2　安全性解析状況（2021 年 9 月現在）

LEA [129] が提案されて以降、以下で示すような解析論文が発表されている。

- Song ら [240] による差分攻撃 (Differential attack)
- Kim ら [148] によるブーメラン特性 (Boomerang characteristics) 探索

その他、LEA を対象としたいくつかの解析論文 [19, 100, 242] が発表されている。

表 3.18 は文献 [240] の Table 1 に基づき、single-key setting における LEA の安全性解析状況についてまとめたものである。表 3.18 から、single-key setting において Song ら [240] による差分攻撃が最良の攻撃であることがわかる。なお、LEA の設計者 [129] は 15、16、17 段に簡略化した LEA-128/192/256 に対してブーメラン攻撃による鍵回復攻撃が実行可能であると主張しているが、攻撃方法の詳細について記述していないため本調査の対象外とする。

また、表 3.19 は文献 [148] の Table 1 に基づき、LEA-128 に対する差分、線形、差分線形、ブーメラン特性についてまとめたものである。表 3.19 から、LEA-128 に対しては Kim ら [148] によるブーメラン攻撃が最良の識別攻撃であることがわかる。

Song ら [240] は ARX ブロック暗号に対する差分特性の自動探索手法に着目し、Mouha と Preneel [208] が提案した SMT solver による自動探索手法を改善することで、既存手法よりも効率的な自動探索手法を提案した。また、Dinur [88] と Abed ら [9] が提案したそれぞれの鍵回復攻撃手法を改善し、14、14、15 段に簡略化した LEA-128/192/256 に対し、秘密鍵の全数探索よりも効率的に鍵回復攻撃が実行できることを示した。

Kim ら [148] は ARX 暗号に対するブーメラン接続表 (Boomerang connectivity table) の新しい生成手法を提案した。ARX 暗号はドメインサイズが大きすぎるため、既存手法をそのまま適用することが困難であるという問題点があった。この問題を解決するために、算術加算におけるビット間の関係性を詳細に分析し、算術加算のためのブーメラン接続確率を計算する効率的な方法を提案することで、ブーメラン接続表の効率的な生成を可能にした。結果として、LEA-128 に対して最良のブーメラン特性を発見した。なお、Kim ら [148] は LEA-128 に対する鍵回復攻撃について言及していないものの、提案手法によって発見したブーメラン特性を利用することで、LEA-128 に対する鍵回復攻撃を改善できる可能性があることに注意されたい。

3.10.3　安全性解析状況のまとめ

2021 年 9 月現在、いくつかの解析論文 [19, 100, 148, 240, 242] が発表されているが、仕様段数において秘密鍵の全数探索よりも効率的に実行可能な攻撃は発表されていない。

Single-key setting において、LEA に対する最良の鍵回復攻撃は Song ら [240] による差分攻撃であり、14、14、15 段に簡略化した LEA-128/192/256 に対しては、それぞれ秘密鍵の全数探索よりも効率的に鍵回復攻撃が実行できる。また、LEA-128 に対する最良の識別攻撃は Kim ら [148] によるブーメラン攻撃であり、24 段のうち 16 段に簡略化した LEA-128 に対しては、効率的に識別攻撃を実行できる。

第 4 章

軽量ストリーム暗号の安全性解析状況

本章では、2016 年度ガイドライン [68, 69] の第 4.2 節に記載された代表的な軽量ストリーム暗号 ChaCha、Enocoro、Grain v1、MICKEY 2.0、Trivium の安全性解析状況に関する調査結果をまとめる。

4.1 ChaCha

4.1.1 2016 年度ガイドラインに記載されている安全性解析状況

2016 年度ガイドライン [69] の第 4.2 節によると、以下のとおり記載されている。

> 2016 年時点では、ChaCha の安全性を脅かす結果は知られていない。Aumasson ら [14] は差分攻撃を用いて 20 ラウンド中 7 ラウンドについて、鍵の総当たりよりも効率良く解読可能であることを示した。この他にも、Shi ら [233] による評価、Maitra [195] による評価があり、それぞれ Aumasson らの結果を改良しているが、攻撃可能なラウンド数は 7 ラウンドに留まっている。

4.1.2 上記以降の安全性解析状況（2021 年 9 月現在）

Aumasson ら [14]、Shi ら [233]、Maitra [195] による差分攻撃 (Differential attack) に関する解析論文が発表されて以降、以下で示すような解析論文が発表されている。

- Choudhuri と Maitra [60] による差分線形攻撃 (Differential-linear attack)
- Beierle ら [27] による差分線形攻撃
- Coutinho と Neto [64, 65, 66] による差分線形攻撃
- Miyashita ら [203] による差分攻撃

その他、ChaCha を対象とした様々な解析論文 [23, 75, 80, 81, 82, 212] が発表されている。

表 4.1 は文献 [66] の Table 1 と文献 [203] の Table 1 に基づき、ChaCha の安全性解析状況に

表 4.1　ChaCha の安全性解析状況

Rounds	Attack type	Time	Data	Ref.
6	Differential	$2^{139.0}$	$2^{30.0}$	[14]
	Differential	$2^{136.0}$	$2^{28.0}$	[233]
	Differential-linear	$2^{130.0}$	$2^{25.0}$	[60]
	Differential-linear	$2^{127.5}$	$2^{27.5}$	[60]
	Differential-linear	$2^{102.2}$	$2^{56.0}$	[64]
	Differential-linear	$2^{77.4}$	$2^{58.0}$	[27]
7	Differential	$2^{248.0}$	$2^{27.0}$	[14]
	Differential	$2^{246.5}$	$2^{27.0}$	[233]
	Differential-linear	$2^{242.6}$	$2^{69.6}$	[65]
	Differential	$2^{238.9}$	$2^{96.0}$	[195]
	Differential-linear	$2^{237.7}$	$2^{96.0}$	[60]
	Differential-linear	$2^{231.9}$	$2^{50.0}$	[64]
	Differential	$2^{231.6}$	$2^{49.6}$	[203]
	Differential-linear	$2^{230.9}$	$2^{48.8}$	[27]
	Differential-linear [a)]	$2^{228.5}$	$2^{80.5}$	[66]
	Differential-linear [b)]	$2^{224.0}$	$2^{224.0}$	[65, 66]
7.25	Differential	$2^{255.6}$	$2^{37.5}$	[203]
	Differential [c)]	$2^{244.2}$	$2^{69.1}$	[203]

[a)] 文献 [65] の第 4.1 節に “*Since the first version of this paper was published, several independent researches reviewed our results and code. We would like to thank Juan C. G. Vasquez (juan.grados@tii.ae) for identifying an error in the code we made publicly available. [...] After correcting the code, we could not find significant results for* $\Delta_{1,0}^{(3.5)}$, $\Delta_{12,0}^{(3.5)}$ *and* $\Delta_{5,0}^{(3.5)}$ *as previously reported, even considering* 2^{52} *samples.*” と記載されており、この攻撃が成立しないことを示唆している。

[b)] 文献 [65] の第 4.2 節に “*we get* $\epsilon_d(\epsilon_{L_0}, \epsilon_{L_1}, \epsilon_{L_2}, \epsilon_{L_3})^2 \approx 2^{-111.86}$ *which gives us a distinguisher for 7 rounds of ChaCha with complexity less than* 2^{228}.” と記載されているため、この攻撃は識別攻撃に相当する。

[c)] この攻撃は文献 [66] で示された $\Delta_{5,0}^{(3.5)}$ に関する差分特性を利用しているため、[a)] で記載した内容に従うと、この攻撃が成立しないことを示唆している。

ついてまとめたものである。表 4.1 から、鍵回復攻撃に関しては，20 段のうち 7 段に簡略化した ChaCha に対して Beierle ら [27] による差分線形攻撃が最良の攻撃であり、7.25 段に簡略化した ChaCha に対して Miyashita ら [203] による差分攻撃が最良の攻撃であることがわかる。また，識

別攻撃に関しては，20 段のうち 7 段に簡略化した ChaCha に対して Coutinho と Neto [65,66] による差分線形攻撃が最良の攻撃であることがわかる。

Beierle ら [27] は ARX 暗号に特化した差分線形攻撃の新しいフレームワークを提案し、提案したフレームワークを Chaskey と ChaCha に対して適用した。結果として、20 段のうち 7 段に簡略化した ChaCha に対して鍵回復攻撃の改善に成功したが、依然として攻撃可能段数は 7 段に留まっている。

Coutinho と Neto [66] は Beierle ら [27] による ARX 暗号に対する差分線形攻撃の新しいフレームワークにインスパイアを受け、ChaCha に特化した差分線形伝搬を詳細に分析した。結果として、20 段のうち 7 段に簡略化した ChaCha に対して最良の識別攻撃が実行可能であることを示したが、鍵回復攻撃の改善には至っていない。

Miyashita ら [203] は Probabilistic Neutral Bits (PNB) の解析に重点を置いた差分攻撃を提案した。具体的には、既存研究 [14,27,60,64,65,66,195,233] では全て (1) 差分・差分線形伝搬の解析、(2) 差分・差分線形伝搬に基づく PNB の解析、という順序で攻撃を実行していたが、Miyashita ら [203] は (1) PNB の解析、(2) PNB に基づく差分伝搬の解析、という順序で攻撃を実行する手法を提案した。結果として、7 段に簡略化した ChaCha に対して鍵回復攻撃の改善には成功しなかったが、7.25 段に簡略化した ChaCha に対して効率的に鍵回復攻撃が実行できることを示した。

4.1.3　安全性解析状況のまとめ

2021 年 9 月現在、様々な解析論文 [14,23,27,60,64,65,66,75,80,81,82,195,203,212,233] が発表されているが、仕様段数において秘密鍵の全数探索よりも効率的に実行可能な攻撃は発表されていない。

20 段のうち 7 段に簡略化した ChaCha に対する最良の攻撃は Beierle ら [27] によって提案された差分線形攻撃と Coutinho と Neto [65,66] によって提案された差分線形攻撃であり、Beierle ら [27] が提案する攻撃では秘密鍵の全数探索よりも効率的に鍵回復攻撃が実行でき、Coutinho と Neto [65,66] が提案する攻撃では効率的に識別攻撃が実行できる。20 段のうち 7.25 段に簡略化した ChaCha に対する最良の攻撃は Miyashita ら [203] による差分攻撃であり、秘密鍵の全数探索よりも効率的に鍵回復攻撃が実行できる。

4.2　Enocoro

4.2.1　2016 年度ガイドラインに記載されている安全性解析状況

2016 年度ガイドライン [69] の第 4.2 節によると、以下のとおり記載されている。

> Enocoro-80、Enocoro-128v2 のいずれについても、single-key setting での脆弱性は知られていない。その一方で、Enocoro-80、および Enocoro-128v2 の前身である

Enocoro-128v1 は関連鍵攻撃に対して脆弱であることが知られている [85, 271, 297, 298]。たとえば、Ding ら [85] の評価によれば、Enocoro-80 の秘密鍵は確率 2^{-8} で弱鍵であり、2^{17} 個の選択 IV を用いることで、計算量 2^{48} で秘密鍵を復元することができる。なお、Enocoro-128v2 については、関連鍵攻撃の有効性は確認されていない。

4.2.2　上記以降の安全性解析状況（2021 年 9 月現在）

Ding ら [85] による弱鍵を使用した攻撃に関する解析論文が発表されて以降、以下で示すような解析論文が発表されている。

- 船引ら [300] によるキューブ攻撃 (Cube attack)
- 芝山ら [301] による高階差分攻撃

船引ら [300] は Enocoro-128v2 に対して MILP を用いたキューブ攻撃を提案した。結果として、96 段のうち 21 段の Enocoro-128v2 に対して効率的に識別攻撃が実行できることを示すとともに、11 段の Enocoro-128v2 に対して 2^{120} の計算量と 2^{8} のデータ量で鍵回復攻撃が実行できることを示した。

芝山ら [301] は Enocoro-128v2 の高階差分特性を探索するためにその構造を詳細に分析し、22 段の 16 階差分特性を発見した。この高階差分特性を利用することで、96 段のうち 22 段の Enocoro-128v2 に対して効率的に識別攻撃が実行できることを示した。

4.2.3　安全性解析状況のまとめ

2021 年 9 月現在、いくつかの解析論文 [85, 271, 297, 298, 300, 301] が発表されているが、仕様段数において秘密鍵の全数探索よりも効率的に実行可能な攻撃は発表されていない。

Enocoro-80 に対する最良の攻撃は Ding ら [85] によって提案された弱鍵を使用した攻撃であり、Ding ら [85] の評価によれば Enocoro-80 の秘密鍵は確率 2^{-8} で弱鍵が存在し、2^{17} 個の選択 IV を用いることで、計算量 2^{48} で鍵回復攻撃を実行できる。

Enocoro-128v2 に対する最良の攻撃は船引ら [300] によって提案された cube 攻撃と芝山ら [301] によって提案された高階差分攻撃であり、96 段のうち 11 段に簡略化した Enocoro-128v2 に対しては秘密鍵の全数探索よりも効率的に鍵回復攻撃が実行でき、22 段の Enocoro-128v2 に対しては効率的に識別攻撃を実行できる。

4.3　Grain v1

4.3.1　2016 年度ガイドラインに記載されている安全性解析状況

2016 年度ガイドライン [69] の第 4.2 節によると、以下のとおり記載されている。

表 4.2　Grain v1 の安全性解析状況

Rounds	Attack type	Time	Data	Ref.
160 (full)	Fast Near Collision	$2^{86.1}$	$2^{19.0}$	[282]
160 (full)	Fast Correlation	$2^{76.7}$	$2^{75.1}$	[253]

Berbain ら [29] は Grain v1 の前身である Grain について評価を行い、2^{38} bits の鍵ストリームと 2^{43} の計算量で 80-bit の秘密鍵を復元できることを報告している。Grain v1 はこの報告を受けてアルゴリズムを改良したものであり、Berbain らの攻撃をそのまま適用することはできない。また、Dinur ら [92] は Grain v1 の鍵長 128-bit のアルゴリズムについて、初期化が不十分であり 118 bits 分の弱鍵空間があると指摘している。この弱鍵の空間は大きいが、この弱鍵に対して鍵復元攻撃を行うためには 2^{103} 程度の計算量が必要である。

4.3.2　上記以降の安全性解析状況（2021 年 9 月現在）

Dinur ら [92] による弱鍵を使用した攻撃に関する解析論文が発表されて以降、以下で示すような解析論文が発表されている。

- Zhang ら [282] による高速近傍衝突攻撃 (Fast near collision attack)
- Todo ら [253] による高速相関攻撃 (Fast correlation attack)

その他、Grain v1 を対象とした様々な解析論文 [20, 21, 71, 72, 159, 160, 192, 193, 194, 215, 220, 281] が発表されている。

表 4.2 は文献 [253] の Table 1 に基づき、Grain v1 の安全性解析状況についてまとめたものである。表 4.2 から、フルスペックの Grain v1 に対しては Todo ら [253] による高速相関攻撃が最良の攻撃であることがわかる。

Todo ら [253] は高速相関攻撃を改善するための *parity-check equations* と *modified wrong-key hypothesis* と呼ばれる新しいテクニックを提案し、フルスペックの Grain v1、Grain-128、Grain-128A に対して提案手法を適用した。結果として、Grain v1 に対しては仕様段数であっても秘密鍵の全数探索より効率的に内部状態復元攻撃が実行できることを示した。

4.3.3　安全性解析状況のまとめ

2021 年 9 月現在、様々な解析論文 [20, 21, 29, 71, 72, 92, 159, 160, 192, 193, 194, 215, 220, 253, 281, 282] が発表されている。

Grain v1 に対する最良の攻撃は Todo ら [253] によって提案された高速相関攻撃であり、Grain v1 に対しては仕様段数であっても効率的に内部状態復元攻撃が実行できる。なお、設計者が主張

表 4.3　n ビット秘密鍵 ($n \geq 80$) と m ビット IV ($0 < m < n$) を入力とする MICKEY 2.0 の安全性解析状況

Rounds	Attack type	Time (online)	Memory	Data	Time (offline)	Ref.
200 (full)	TMDTO	$2^{47.0}$	$2^{120.0}$	$2^{80.0}$ bits	$2^{120.0}$	[86]
200 (full)	TMDTO ($m = 64$)	$2^{78.0}$	$2^{45.0}$	80 bits	$2^{79.0}$	[83]
200 (full)	TMDTO ($m = 79$)	$2^{79.6}$	$2^{45.0}$	80 bits	$2^{79.0}$	[83]

するセキュリティレベルは Grain v1 において 80 ビットである。本攻撃では、Grain v1 に対して $2^{76.7}$ ($< 2^{80.0}$) の計算量で実行可能であり、一般的な秘密鍵の全数探索と比較して $2^{3.3}$ 倍の効率化に成功した。

4.4　MICKEY 2.0

4.4.1　2016 年度ガイドラインに記載されている安全性解析状況

2016 年度ガイドライン [69] の第 4.2 節によると、以下のとおり記載されている。

> MICKEY 2.0 に対する安全性評価結果は自己評価以外に知られておらず、脆弱性は見つかっていない。

4.4.2　上記以降の安全性解析状況（2021 年 9 月現在）

MICKEY 2.0 [18] が提案されて以降、以下で示すような解析論文が発表されている。

- Ding ら [83, 86] によるタイムメモリデータトレードオフ攻撃 (TMDTO attack)

その他、MICKEY 2.0 を対象としたいくつかの解析論文 [84, 124, 130] が発表されている。

表 4.3 は文献 [83] の Table 2 に基づき、MICKEY 2.0 の安全性解析状況についてまとめたものである。表 4.3 から、フルスペックの MICKEY 2.0 に対しては Ding ら [83] によるタイムメモリデータトレードオフ攻撃が最良の攻撃であることがわかる。

Ding ら [83] は n ビット秘密鍵 ($n \geq 80$) と m ビット IV ($0 < m < n$) を入力とする MICKEY 2.0 に対し、single-key setting においてオンライン計算量、メモリ量、データ量、オフライン計算量が全て 2^n 未満で実行可能な鍵回復攻撃が存在することを証明した。結果として、MICKEY 2.0 に対しては仕様段数であっても秘密鍵の全数探索より効率的に鍵回復攻撃が実行できることを示した。

4.4.3　安全性解析状況のまとめ

2021 年 9 月現在、いくつかの解析論文 [83, 84, 86, 124, 130] が発表されている。

MICKEY 2.0 に対する最良の攻撃は Ding ら [83] によって提案されたタイムメモリデータトレードオフ攻撃であり、MICKEY 2.0 に対しては仕様段数であっても秘密鍵の全数探索より効率的に鍵回復攻撃が実行できる。なお、設計者が主張するセキュリティレベルは MICKEY 2.0 において 80 ビットである。本攻撃では、MICKEY 2.0 に対して $2^{79.0}$ ($< 2^{80.0}$) の計算量で実行可能であり、一般的な秘密鍵の全数探索と比較して $2^{1.0}$ 倍の効率化に成功した。

4.5　Trivium

4.5.1　2016 年度ガイドラインに記載されている安全性解析状況

2016 年度ガイドライン [69] の第 4.2 節によると、以下のとおり記載されている。

> 2016 年時点では、Trivium の安全性を脅かす結果は知られていない。Maximov ら [199] は鍵ストリームから内部状態を推定する攻撃について、$2^{61.5}$ bits の鍵ストリームから、鍵の総当たりを $2^{89.5}$ 回行うのと同等の計算量で内部状態を復元できることが攻撃が可能であることを報告している。Fouque ら [103] は Trivium の初期化に対して cube attack を適用しており、2^{40} 個の IV (と対応する鍵ストリーム) および 2^{62} の総当たりを行うことで、1152 ステップ中 799 ステップまで鍵復元が可能であると報告している。

4.5.2　上記以降の安全性解析状況（2021 年 9 月現在）

Fouque ら [103] によるキューブ攻撃 (Cube attack) に関する解析論文が発表されて以降、以下で示すような解析論文が発表されている。

- Wang ら [118, 267] によるキューブ攻撃
- Fu ら [105] によるキューブ攻撃
- Hao ら [120, 121] によるキューブ攻撃
- Hu ら [134] によるキューブ攻撃

その他、Trivium を対象とした様々な解析論文 [76, 135, 181, 246, 251, 252, 268, 279] が発表されている。

表 4.4 は文献 [121] の Table 1 と Table 2、文献 [134] の Table 2 に基づき、Trivium の安全性解析状況についてまとめたものである。表 4.4 から、Trivium に対しては Hu ら [134] によるキューブ攻撃が最良の攻撃であることがわかる。

Hu ら [134] は文献 [135] で提案した *monomial prediction technique* を発展させ、大規模な superpoly を効率的に復元するための新しいフレームワークを提案した。このフレームワークでは、ターゲットとなる出力ビットを中間ラウンドにおける内部状態のビットの多項式で表現し、多項式の各項に *monomial prediction technique* を適用して、対応する MILP モデルが指定された

表 4.4　Trivium の安全性解析状況

Rounds	Attack type	Time	Data	Ref.
799	Cube	$2^{62.0}$	$2^{38.0}$	[103]
832	Cube	$2^{79.0}$	$2^{72.0}$	[251, 268, 279]
835	Cube	$2^{75.0}$	$2^{35.0}$	[181]
836	Cube [a)]	$2^{79.0}$	–	[118, 267]
839	Cube [a)]	$2^{79.0}$	–	[118, 267]
840	Cube	$2^{79.6}$	$2^{78.0}$	[120, 121]
840	Cube	$2^{77.8}$	$2^{76.6}$	[135]
840	Cube	$2^{76.3}$	$2^{62.0}$	[134]
841	Cube	$2^{78.6}$	$2^{77.0}$	[135]
841	Cube	$2^{78.0}$	$2^{56.0}$	[134]
842	Cube	$2^{78.6}$	$2^{77.0}$	[135]
842	Cube	$2^{78.0}$	$2^{56.0}$	[134]
843	Cube	$2^{79.6}$	$2^{78.0}$	[246]
843	Cube	$2^{77.0}$	$2^{56.0}$	[134]
844	Cube	$2^{79.0}$	$2^{56.0}$	[134]
845	Cube	$2^{79.0}$	$2^{56.0}$	[134]
855	Cube [b)]	$2^{77.0}$	–	[105]

[a)] Attack does not work because of a flaw in the degeneration to distinguisher, which was pointed out in [268, 279].

[b)] Attack does not work because of a flaw in the degree estimation, which was pointed out in [120, 121].

制限時間内で解けるかどうかを決定する。結果として、1152 段のうち 845 段に簡略化した Trivium に対し、秘密鍵の全数探索よりも効率的に鍵回復攻撃が実行できることを示した。

なお、Fu ら [105] は 1152 段のうち 855 段に簡略化した Trivium に対するキューブ攻撃を提案したものの、Hao ら [121] によって Fu ら [105] の攻撃が不正確であることが明らかとなったため、結果として Hu ら [134] によるキューブ攻撃が最良の攻撃となる。

4.5.3　安全性解析状況のまとめ

2021 年 9 月現在、様々な解析論文 [76, 103, 105, 118, 120, 121, 134, 135, 181, 246, 251, 252, 267, 268, 279] が発表されているが、仕様段数において秘密鍵の全数探索よりも効率的に実行可能な攻撃は発表されていない。

Trivium に対する最良の攻撃は Hu ら [134] によって提案されたキューブ攻撃であり、1152 段のうち 845 段に簡略化した Trivium に対しては、秘密鍵の全数探索よりも効率的に鍵回復攻撃が実行できる。

第 5 章

軽量ハッシュ関数の安全性解析状況査

本章では、2016 年度ガイドライン [68, 69] の第 4.3 節に記載された代表的な軽量ハッシュ関数 Keccak、PHOTON、QUARK、SPONGENT の安全性解析状況に関する調査結果をまとめる。また、PHOTON、SPONGENT、Lesamnta-LW が軽量ハッシュ関数に関係する ISO/IEC 規格 (ISO/IEC 29192-5) [4] で採択されている状況を鑑み、2016 年度ガイドラインに記載されていない Lesamnta-LW も調査対象とした。なお、Lesamnta-LW に関しては安全性解析状況に関する調査結果だけでなく、その仕様（設計者、発表年、仕様参照先、特徴、主な実装性能評価結果、標準化状況）についても簡単にまとめる。

5.1 Keccak

5.1.1 2016 年度ガイドラインに記載されている安全性解析状況

2016 年度ガイドライン [69] の第 4.3 節によると、以下のとおり記載されている。

> SHA-3 として標準化された方式に関する解析論文が多数存在するが、現時点では致命的な脆弱性は報告されていない。

なお、これは軽量暗号の観点から Keccak-f[100]、Keccak-f[200]、Keccak-f[400] にのみ着目した結果として記載されたものである。

5.1.2 上記以降の安全性解析状況（2021 年 9 月現在）

軽量暗号の観点から Keccak-f[100]、Keccak-f[200]、Keccak-f[400] に着目すると、以下で示すような解析論文が発表されている。

- Li ら [168] による原像攻撃 (Preimage attack)
- Boissier ら [47] による代数衝突攻撃 (Algebraic collision attack)

その他、SHA-3 として標準化された Keccak を対象とした解析論文 [113, 123, 167, 171, 176, 180,

表 5.1　Keccak の安全性解析状況

Cipher	Rounds	Attack type	Time	Ref.
Keccak-f[200]	2	Algebraic Collision	$2^{52.5}$	[47]
	2	Algebraic Collision	$2^{73.0}$	[47]
Keccak-f[400]	2	Algebraic Collision	$2^{101.5}$	[47]
	3	Preimage	$2^{45.0}$	[168]

219, 221, 238, 239, 241, 247] については多数存在している。

表 5.1 は文献 [168] と文献 [47] の結果に基づき、Keccak の安全性解析状況についてまとめたものである。表 5.1 から、18 段のうち 2 段に簡略化した Keccak-f[200] に対しては Boissier ら [47] による代数衝突攻撃が最良の攻撃であり、20 段のうち 3 段に簡略化した Keccak-f[400] に対しては Li ら [168] による原像攻撃が最良の攻撃であることがわかる。なお、2021 年 9 月現在において、Keccak-f[100] に対する解析論文については発表されていない。

Li ら [168] は *cross-linear structures* と呼ばれる新しい概念を提案した。これは原像攻撃に利用する多項式を可能な限り多く収集するための概念であり、この概念を用いることで原像攻撃を効率化させることができる。結果として、20 段のうち 3 段に簡略化した Keccak-f[400] に対し、効率的に原像攻撃が実行できることを示した。

Boissier ら [47] は Dinur ら [91] が提案した *birthday squeeze attack* にインスピレーションを受け、代数的解析に基づく衝突攻撃を提案した。結果として、18 段のうち 2 段に簡略化した Keccak-f[200]、20 段のうち 2 段に簡略化した Keccak-f[400] に対し、効率的に衝突攻撃が実行できることを示した。

5.1.3　安全性解析状況のまとめ

2021 年 9 月現在、SHA-3 として標準化された方式も含め、様々な解析論文 [47, 113, 123, 167, 168, 171, 176, 180, 219, 221, 238, 239, 241, 247] が発表されているが、仕様においてハッシュ関数の安全性基準を脅かす攻撃は発表されていない。

18 段のうち 2 段に簡略化した Keccak-f[200] と 20 段のうち 2 段に簡略化した Keccak-f[400] に対する最良の攻撃は Boissier ら [47] によって提案された代数衝突攻撃であり、それぞれ全数探索よりも効率的に衝突攻撃が実行できる。また、20 段のうち 3 段に簡略化した Keccak-f[400] に対する最良の攻撃は Li ら [168] によって提案された原像攻撃であり、全数探索よりも効率的に原像攻撃が実行できる。

5.2　PHOTON

5.2.1　2016 年度ガイドラインに記載されている安全性解析状況

2016 年度ガイドライン [69] の第 4.3 節によると、以下のとおり記載されている。

> 現時点では致命的な脆弱性は報告されていないが、解析論文が少ないため潜在的な脆弱性を含んでいる可能性があることに注意。

5.2.2　上記以降の安全性解析状況（2021 年 9 月現在）

PHOTON [114] が提案されて以降、以下で示すような解析論文が発表されている。

- Jean ら [141] によるリバウンド攻撃 (Rebound attack)
- Wang ら [265, 266] によるゼロサム攻撃 (Zero-sum attack)

表 5.2 は文献 [266] の Table 1 に基づき、PHOTON の安全性解析状況についてまとめたものである。表 5.2 から、PHOTON に対しては Wang ら [265, 266] によるゼロサム攻撃が最良の攻撃であることがわかる。なお、2021 年 9 月現在において、PHOTON-256/32/32 に対する解析論文については発表されていない。

Wang ら [265, 266] は MILP を用いた順方向・逆方向関数に対する division property の探索手法を提案した。この提案手法では、PRESENTS-box の脆弱性に基づく *zero-sum partitions* と呼ばれるテクニックと、*subspace trail* と呼ばれる概念を用いて効率化を図っている。結果として、12 段のうち 11 段に簡略化した PHOTON-80/20/16 とフルスペックの PHOTON-128/16/16、PHOTON-160/36/36、PHOTON-224/32/32 に対し、効率的な識別攻撃が実行できることを示した。

5.2.3　安全性解析状況のまとめ

2021 年 9 月現在、いくつかの解析論文 [141, 265, 266] が発表されているが、仕様においてハッシュ関数の安全性基準を脅かす攻撃は発表されていない。

PHOTON に対する最良の攻撃は Wang ら [265, 266] によって提案されたゼロサム攻撃であり、12 段のうち 11 段に簡略化した PHOTON-80/20/16 とフルスペックの PHOTON-128/16/16、PHOTON-160/36/36、PHOTON-224/32/32 に対しては、効率的に識別攻撃を実行できる。なお、PHOTON に対する識別攻撃は原則的にハッシュ関数の必須安全性基準（原像計算困難性、第 2 原像計算困難性、衝突困難性）を脅かすものでは無いことに注意されたい。

表 5.2　PHOTON の安全性解析状況

Cipher	Rounds	Attack type	Time	Ref.
PHOTON-80/20/16	8	Differential Distinguisher	$2^{8.0}$	[114]
	9	Zero-sum Distinguisher	$2^{35.0}$	[265]
	10	Zero-sum Distinguisher	$2^{40.0}$	[265]
	11	Zero-sum Distinguisher	$2^{76.0}$	[265]
PHOTON-128/16/16	8	Differential Distinguisher	$2^{8.0}$	[114]
	9	Zero-sum Distinguisher	$2^{42.0}$	[266]
	10	Zero-sum Distinguisher	$2^{47.0}$	[266]
	11	Zero-sum Distinguisher	$2^{107.0}$	[266]
	12 (full)	Zero-sum Distinguisher	$2^{127.0}$	[266]
PHOTON-160/36/36	8	Differential Distinguisher	$2^{8.0}$	[114]
	9	Zero-sum Distinguisher	$2^{43.0}$	[265]
	10	Zero-sum Distinguisher	$2^{48.0}$	[265]
	11	Zero-sum Distinguisher	$2^{108.0}$	[265]
	12 (full)	Zero-sum Distinguisher	$2^{159.0}$	[265]
PHOTON-224/32/32	8	Differential Distinguisher	$2^{8.0}$	[114]
	9	Rebound Distinguisher	$2^{184.0}$	[141]
	9	Zero-sum Distinguisher	$2^{50.0}$	[265]
	10	Zero-sum Distinguisher	$2^{54.0}$	[265]
	11	Zero-sum Distinguisher	$2^{119.0}$	[265]
	12 (full)	Zero-sum Distinguisher	$2^{184.0}$	[266]

5.3　QUARK

5.3.1　2016 年度ガイドラインに記載されている安全性解析状況

2016 年度ガイドライン [69] の第 4.3 節によると、以下のとおり記載されている。

> 現時点では致命的な脆弱性は報告されていないが、解析論文が少ないため潜在的な脆弱性を含んでいる可能性があることに注意。

5.3.2　上記以降の安全性解析状況（2021 年 9 月現在）

QUARK [15, 16] が提案されて以降、以下で示すような解析論文が発表されている。

表 5.3　QUARK の安全性解析状況

Cipher	Rounds	Attack type	Time	Ref.
U-QUARK	136	Conditional Differential Distinguisher	$2^{27.0}$	[16]
	153	Conditional Differential Distinguisher	$2^{18.0}$	[284]
	155	Conditional Differential Distinguisher	$2^{27.0}$	[265]
D-QUARK	159	Conditional Differential Distinguisher	$2^{27.0}$	[16]
	159	Conditional Differential Distinguisher	$2^{22.0}$	[284]
	166	Conditional Differential Distinguisher	$2^{25.0}$	[265]
S-QUARK	237	Conditional Differential Distinguisher	$2^{27.0}$	[16]
	248	Conditional Differential Distinguisher	$2^{24.0}$	[284]
	259	Conditional Differential Distinguisher	$2^{15.0}$	[265]

- Zhang ら [284] による条件付き差分攻撃 (Conditional differential attack)
- Yang ら [278] による条件付き差分攻撃

表 5.3 は文献 [278] の Table 1 に基づき、QUARK の安全性解析状況についてまとめたものである。表 5.3 から、QUARK に対しては Yang ら [278] による条件付き差分攻撃が最良の攻撃であることがわかる。

Yang ら [278] は条件付き差分攻撃において適切な入力差分を選択するために *symbolic-like computation* という新しい手法を提案した。結果として、544 段のうち 155 段に簡略化した U-QUARK、704 段のうち 166 段に簡略化した D-QUARK、1024 段のうち 259 段に簡略化した S-QUARK に対し、効率的に識別攻撃が実行できることを示した。

5.3.3　安全性解析状況のまとめ

2021 年 9 月現在、いくつかの解析論文 [278, 284] が発表されているが、仕様においてハッシュ関数の安全性基準を脅かす攻撃は発表されていない。

QUARK に対する最良の攻撃は Yang ら [278] によって提案された条件付き差分攻撃であり、544 段のうち 155 段に簡略化した U-QUARK、704 段のうち 166 段に簡略化した D-QUARK、1024 段のうち 259 段に簡略化した S-QUARK に対しては、効率的に識別攻撃を実行できる。なお、QUARK に対する識別攻撃は原則的にハッシュ関数の必須安全性基準（原像計算困難性、第 2 原像計算困難性、衝突困難性）を脅かすものでは無いことに注意されたい。

表 5.4　SPONGENT permutation の安全性解析状況（識別攻撃可能段数）

Cipher	Full rounds	Rounds		
		[45]	[7]	[283]
SPONGENT-88/80/8	88	22	23	30
SPONGENT-88/176/88	264	66	–	77
SPONGENT-128/128/8	136	34	–	43
SPONGENT-128/256/128	384	96	–	109
SPONGENT-160/160/16	176	44	–	53
SPONGENT-160/160/80	240	60	–	69
SPONGENT-160/320/160	480	122	–	132
SPONGENT-224/224/16	240	60	–	69
SPONGENT-224/224/112	336	84	–	95
SPONGENT-224/448/224	672	169	–	181
SPONGENT-256/256/16	272	68	–	78
SPONGENT-256/256/128	384	96	–	109
SPONGENT-256/512/256	768	192	–	205

5.4　SPONGENT

5.4.1　2016 年度ガイドラインに記載されている安全性解析状況

2016 年度ガイドライン [69] の第 4.3 節によると、以下のとおり記載されている。

> 現時点では致命的な脆弱性は報告されていないが、解析論文が少ないため潜在的な脆弱性を含んでいる可能性があることに注意。

5.4.2　上記以降の安全性解析状況（2021 年 9 月現在）

SPONGENT [45] が提案されて以降、以下で示すような解析論文が発表されている。

- Abdelraheem [7] による差分攻撃 (Differential attack) と線形攻撃 (Linear attack)
- Zhang と Liu [283] による中間一致 (Meet-in-the-Middle) 手法を用いた切り詰め差分攻撃 (Truncated differential attack)

表 5.4 は文献 [283] の Table 1 に基づき、SPONGENT の安全性解析状況についてまとめたものである。表 5.4 から、SPONGENT に対しては Zhang と Liu [283] による中間一致手法を用いた切り詰め差分攻撃が最良の攻撃であることがわかる。

Zhang と Liu [283] は Blondeau ら [41] が提案したフルスペックの PRESENT に対する known-key distinguisher を PRESENT-like permutations に適用するための一般化手法を提案した。具体的には、切り詰め差分確率 (truncated differential probability) と多次元線形近似 (multidimentional linear approximation) との強力な関係性を分析し、切り詰め差分識別子の構成に利用できる強力なバイアスを取得する手法を提案した。結果として、簡略化した全てのバリエーションにおける SPONGENT permutations に対し、効率的に識別攻撃が実行できることを示した。

5.4.3　安全性解析状況のまとめ

2021 年 9 月現在、いくつかの解析論文 [7, 283] が発表されているが、仕様においてハッシュ関数の安全性基準を脅かす攻撃は発表されていない。

SPONGENT に対する最良の攻撃は Zhang と Liu [283] によって提案された中間一致手法を用いた切り詰め差分攻撃であり、簡略化した全てのバリエーションにおける SPONGENT permutations に対しては、効率的に識別攻撃が実行できる。なお、SPONGENT に対する識別攻撃は原則的にハッシュ関数の必須安全性基準（原像計算困難性、第 2 原像計算困難性、衝突困難性）を脅かすものでは無いことに注意されたい。

5.5　Lesamnta-LW

5.5.1　仕様

■設計者　Shoichi Hirose[1], Kota Ideguchi[2], Hidenori Kuwakado[3], Toru Owada[2], Bart Preneel[4], and Hirotaka Yoshida[2,4]

(1: University of Fukui / Japan, 2: Hitach, Ltd. / Japan, 3: Kobe University / Japan, 4: Katholieke Universiteit Leuven, Belgium)

■発表年（発表学会等）　2010 (ICISC 2010 [125])

■仕様参照先　[125]

■特徴　Lesamnta-LW は LW1 モードと呼ばれるドメイン拡張型の Merkle-Damgård 構造から成り、その基礎となるコンポーネントは AES ベースのブロック暗号 (Lesamnta-LW-BC) を利用する。出力長は 256 ビットであり、原像攻撃や衝突攻撃に対して 2^{120} のセキュリティレベルを有するよう設計されている。なお、Lesamnta-LW は SHA-3 competition に応募された Lesamnta の軽量版として提案された。

Lesamnta-LW-BC は 4-branch type-1 一般化 Feistel network 型のブロック暗号であり、仕様段数は 64 段、ブロックサイズは 256 ビット、秘密鍵サイズは 128 ビット、ラウンド関数は AES のコンポーネントである MixColumns と SubBytes を使用する。

表 5.5　Lesamnta-LW のハードウェア実装評価結果

	Area [GE]	Clock [MHz]	Throughput@30MHz [Mbit/s]
Lesamnta-LW	8240	188.3	20.00

表 5.6　Lesamnta-LW のソフトウェア実装評価結果

Algorithm	RAM [byte]	Cycles/byte	Platform
Lesamnta-LW	50	1650.9	Renesas H8 (8-bit CPU)
Lesamnta-LW	–	39.5	Intel Core i5 (32-bit CPU)

■主な実装性能評価結果　ハードウェア (90nm Logic Process)・ソフトウェア実装評価結果 [125] をそれぞれ表 5.5 と表 5.6 に示す。

■標準化状況　ISO/IEC 29192-5 [4]

5.5.2　安全性解析状況（2021 年 9 月現在）

Lesamnta-LW [125, 126] が提案されて以降、以下で示すような解析論文が発表されている。

- Hirose ら [128] による差分攻撃 (Differential attack)
- Shiba ら [234] による積分攻撃 (Integral attack) と不能差分攻撃 (Impossible differential attack)

その他、SHA-3 competition に応募された Lesamnta を対象としたいくつかの解析論文 [49, 231] が発表されている。

表 5.7 は文献 [234] の Table 1 に基づき、Lesamnta-LW-BC の安全性解析状況についてまとめたものである。表 5.7 から、Lesamnta-LW-BC に対しては Hirose ら [128] による差分攻撃と Shiba ら [234] による積分攻撃が最良の攻撃であることがわかる。

Hirose ら [128] は MILP を用いた差分攻撃により Lesamnta-LW-BC の active S-box を厳密に評価した。結果として、64 段のうち 18 段に簡略化した Lesamnta-LW-BC の active S-box が 25、29 段に簡略化した Lesamnta-LW-BC の active S-box が 42 であることを明らかにし、1 つの active S-box につき最大差分確率を 2^{-6} として評価することで、29 段に簡略化した Lesamnta-LW-BC に対し、効率的に識別攻撃が実行できることを示した。

Shiba ら [234] は MILP を用いた Lesamnta-LW-BC に対する積分攻撃と不能差分攻撃を示した。結果として、64 段のうち 20 段に簡略化した Lesamnta-LW-BC に対し、秘密鍵の全数探索よりも効率的に鍵回復攻撃が実行できることを示した。また、known-key setting において、64 段のうち 47 段に簡略化した Lesamnta-LW-BC に対し、効率的に識別攻撃が実行可能であることを示した。

表 5.7　Lesamnta-LW-BC の安全性解析状況

Rounds	Attack type	Time	Data	Ref.
11	Impossible Differential/Distinguisher	–	–	[126]
18	Differential/Distinguisher	$2^{150.0}$	$2^{150.0}$	[128]
18	Integral/Distinguisher	$2^{63.0}$	$2^{63.0}$	[234]
19	Integral/Distinguisher	$2^{127.0}$	$2^{127.0}$	[234]
21	Impossible Differential/Distinguisher	–	–	[234]
25	Integral/Distinguisher	$2^{255.0}$	$2^{255.0}$	[234]
29	Differential/Distinguisher	$2^{252.0}$	$2^{252.0}$	[128]
25	Zero-sum/Known-key Distinguisher	$2^{63.0}$	$2^{63.0}$	[234]
29	Zero-sum/Known-key Distinguisher	$2^{127.0}$	$2^{127.0}$	[234]
47	Zero-sum/Known-key Distinguisher	$2^{255.0}$	$2^{255.0}$	[234]
19	Impossible Differential/Key Recovery	$2^{123.8}$	$2^{123.0}$	[234]
20	Integral/Key Recovery	$2^{95.0}$	$2^{63.0}$	[234]

5.5.3　安全性解析状況のまとめ

2021 年 9 月現在、いくつかの解析論文 [49, 128, 231, 234] が発表されているが、仕様においてハッシュ関数の安全性基準を脅かす攻撃は発表されていない。

Single-key setting において、Lesamnta-LW-BC に対する最良の攻撃は Shiba ら [234] によって提案された積分攻撃であり、64 段のうち 20 段に簡略化した Lesamnta-LW-BC に対しては、秘密鍵の全数探索よりも効率的に鍵回復攻撃が実行できる。また、Hirose ら [128] によって提案された差分攻撃では、29 段に簡略化した Lesamnta-LW-BC に対して効率的に識別攻撃が実行できる。

Known-key setting において、Lesamnta-LW-BC に対する最良の攻撃は Shiba ら [234] によって提案されたゼロサム攻撃であり、64 段のうち 47 段に簡略化した Lesamnta-LW-BC に対しては、効率的に識別攻撃が実行できる。なお、Lesamnta-LW-BC に対する識別攻撃は原則的にハッシュ関数の必須安全性基準（原像計算困難性、第 2 原像計算困難性、衝突困難性）を脅かすものでは無いことに注意されたい。

第 6 章

軽量 MAC の安全性解析状況

本章では、2016 年度ガイドライン [68,69] の第 4.4 節に記載された代表的な軽量 MAC SipHash の安全性解析状況に関する調査結果をまとめる。また、Chaskey、LightMAC、Tsudik's keymode が軽量 MAC に関係する ISO/IEC 規格 (ISO/IEC 29192-6) [2] で採択されている状況を鑑み、2016 年度ガイドラインに記載されていない Chaskey、LightMAC、Tsudik's keymode も調査対象とした。なお、Chaskey、LightMAC、Tsudik's keymode に関しては安全性解析状況に関する調査結果だけでなく、その仕様（設計者、発表年、仕様参照先、特徴、主な実装性能評価結果、標準化状況）についても簡単にまとめる。

6.1 SipHash

6.1.1 2016 年度ガイドラインに記載されている安全性解析状況

2016 年度ガイドライン [69] の第 4.4 節によると、以下のとおり記載されている。

> 2016 年時点において、SipHash の脆弱性は知られていない。第三者による評価として、Dobraunig ら [94] による結果がある。彼らは差分特性確率が $2^{-236.3}$ の差分パスを発見している。しかし、SipHash の鍵長は 128-bit であり、鍵の総当たり攻撃の方がはるかに効率的であるので、この結果は SipHash の安全性を脅かすものではない。

6.1.2 上記以降の安全性解析状況（2021 年 9 月現在）

Dobraunig ら [94] による差分攻撃 (Differential attack) に関する解析論文が発表されて以降、以下で示すような解析論文が発表されている。

- Xin ら [275] による差分攻撃と巡回シフト XOR 攻撃 (Rotational-XOR attack)
- Liu ら [185] による巡回シフト差分線形攻撃 (Rotational differential-linear attack)

表 6.1　SipHash の安全性解析状況

Instance	Attack type	# of message blocks	Probability	Ref.
SipHash-1-x	Differential/Internal Collision	1	0	[275]
	Differential/Internal Collision	2	0	[275]
	Differential/Internal Collision	3	$2^{-169.0}$	[94]
	Differential/Internal Collision	4	$2^{-278.0}$	[275]
	Rotational-XOR/Internal Collision	1	0	[275]
	Rotational-XOR/Internal Collision	2	$2^{-280.0}$	[275]
SipHash-2-x	Differential/Internal Collision	1	$2^{-242.0}$	[94]
	Differential/Internal Collision	1	$2^{-241.0}$	[275]
SipHash-2-4	Differential/Probability	–	$2^{-498.0}$	[13]
	Differential/Probability	–	$2^{-236.3}$	[94]

なお、Liu ら [185] は SipHash に対する識別攻撃の細部を明確にしていない。

表 6.1 は文献 [94] の Table 1 と文献 [275] の Table 1 に基づき、SipHash の安全性解析状況についてまとめたものである。表 6.1 から、フルスペックの SipHash-2-4 に対しては Dobraunig ら [94] による差分攻撃が最良の攻撃であることがわかる。また、圧縮フェーズのみの簡略化した SipHash-1-x と SipHash-2-x に対しては Xin ら [275] による差分攻撃が最良の攻撃であることがわかる。

Xin ら [275] は差分攻撃を用いた内部衝突特性を探索するためのモデルを作成し、SMT ベースの自動探索ツールを用いて内部衝突特性を探索した。結果として、最終処理フェーズを除いた圧縮フェーズのみの簡略化した SipHash-1-x と SipHash-2-x に対し、メッセージブロック長が短い場合に高い内部衝突特性があることを示した。

6.1.3　安全性解析状況のまとめ

2021 年 9 月現在、いくつかの解析論文 [94, 185, 275] が発表されているが、仕様において秘密鍵の全数探索よりも効率的に実行可能な攻撃は発表されていない。

フルスペックの SipHash-2-4 に対する最良の鍵回復攻撃は Dobraunig ら [94] によって提案された差分攻撃である。Dobraunig ら [94] は差分特性確率が $2^{-236.3}$ の差分パスを発見しているものの、SipHash の鍵長は 128-bit であり、鍵の総当たり攻撃の方がはるかに効率的であるので、この結果は SipHash の安全性を脅かすものではない。また、圧縮フェーズのみの簡略化した SipHash-1-x と SipHash-2-x に対する最良の攻撃は Xin ら [275] によって提案された差分攻撃であり、SipHash-1-x と SipHash-2-x において高い内部衝突特性があることを示したが。この結果においても SipHash の安全性を脅かすものではない。

表 6.2　Chaskey のソフトウェア実装評価結果

Data [byte]	ROM [byte]	Cycles/byte	Platform
16	414	21.8	Cortex-M0
16	1308	21.3	Cortex-M0
128	414	16.9	Cortex-M0
128	1308	18.3	Cortex-M0
16	402	16.1	Cortex-M3/M4
16	908	10.6	Cortex-M3/M4
128	402	11.2	Cortex-M3/M4
128	908	7.0	Cortex-M3/M4

6.2　Chaskey

6.2.1　仕様

■設計者　Nicky Mouha[1], Bart Mennink[1], Anthony Van Herrewege[1], Dai Watanabe[2], Bart Preneel[1], and Ingrid Verbauwhede[1]

(1: Katholieke Universiteit Leuven / Belgium, 2: Hitach, Ltd. / Japan)

■発表年（発表学会等）　2014 (SAC 2014 [207])、2015 (Cryptology ePrint Archive [205])

■仕様参照先　[205, 207]

■特徴　Chaskey は算術加算、排他的論理和、巡回シフトの組み合わせで構成される暗号学的置換を用いたメッセージ認証コードアルゴリズムである。暗号学的置換の仕様段数は 8 段、鍵長とブロックサイズは 128 ビット、タグ長は 64 ビット以上が推奨されている。32 ビットワードを単位として演算が実行されることから、32 ビット演算をサポートするマイクロコントローラー上で効率的に動作する。また、全ての演算にかかる実行時間が一定であり、サイクル数がメッセージ長のみに依存するため、Chaskey はタイミング攻撃に対して安全である。

7 段に簡略化した Chaskey に対して鍵回復攻撃が可能であることが報告され [157]、セキュリティマージンを確保する観点で仕様段数を 12 段に増やした Chaskey-12 [205] が提案されている。セキュリティマージンの観点で Chaskey-12 は優れているものの、Chaskey と比較すると 32-bit ARM Cortex-M microcontrollers で 15% 低速である。

■主な実装性能評価結果　Chaskey のソフトウェア実装評価結果を表 6.2 に示す。

■標準化状況　ISO/IEC 29192-6 [2]

表 6.3　Single-key setting における Chaskey の安全性解析状況

Rounds	Attack type	Time	Data	Ref.
6	Differential-linear	$2^{28.6}$	$2^{25.0}$	[157]
7	Differential-linear	$2^{67.0}$	$2^{48.0}$	[157]
7	Differential-linear	$2^{51.2}$	$2^{40.2}$	[27]
7	Differential-linear	$2^{50.0}$	$2^{39.0}$	[51]
7.5	Differential-linear	$2^{77.0}$	$2^{48.0}$	[51]

6.2.2　安全性解析状況（2021 年 9 月現在）

Chaskey [207] が提案されて以降、以下で示すような解析論文が発表されている。

- Mavromati [198] による衝突攻撃 (Collision attack)
- Leurent [157] による差分線形攻撃 (Differential-linear attack)
- Beierle ら [27] による差分線形攻撃
- Kraleva ら [152] による巡回シフト攻撃 (Rotational attack)
- Broll ら [51] による差分線形攻撃
- Xu ら [276] による巡回シフト線形攻撃 (Rotational-linear attack)

表 6.3 は文献 [27] の Table 1 と文献 [51] の Table 1 に基づき、Chaskey の安全性解析状況についてまとめたものである。表 6.3 から、single-key setting において Broll ら [51] による差分線形攻撃撃が最良の攻撃であることがわかる。

Broll ら [51] は *partitioning techniques* と *LLR statistics techniques* と呼ばれるテクニックを応用することにより、Leurent [157] と Beierle ら [27] が提案した差分線形攻撃を改善した。結果として、8 段のうち 7.5 段に簡略化した Chaskey に対し、秘密鍵の全数探索よりも効率的に鍵回復攻撃が実行できることを示した。

Related-key setting においては Kraleva ら [152] による弱鍵を利用した巡回シフト攻撃が最良の攻撃であり、8 段のうち 6 段に簡略化した Chaskey に対して 2^{42} のデータ量で識別攻撃が実行でき、フルスペックの Chaskey-12 に対して 2^{86} のデータ量で実行可能な偽造攻撃と 2^{120} のデータ量で実行可能な鍵回復攻撃が示されている。また、Xu ら [276] は related-key setting における巡回シフト線形攻撃を提案し、フルスペックの Chaskey-12 に対して $2^{60.4}$ のデータ量で実行可能な識別攻撃を示したが、フルスペックの Chaskey-12 に対して鍵回復攻撃を実行できないことを示した（12 段のうち 7 段に簡略化した Chaskey-12 に対して $2^{46.8}$ の計算量と $2^{38.8}$ のデータ量で鍵回復攻撃が実行可能であることを示した）。

Mavromati [198] は single-user mode と multi-user mode における衝突攻撃を提案しており、フルスペックの Chaskey に対して single-user mode では 2^{64} のデータ量で鍵回復攻撃が実行で

き、multi-user mode では 2^{43} ユーザと各ユーザごと 2^{43} のデータ量で鍵回復攻撃が実行できることを示した[*1]。

6.2.3　安全性解析状況のまとめ

2021 年 9 月現在、いくつかの解析論文 [27, 51, 152, 157, 198, 276] が発表されている。

Single-key setting において、Chaskey に対する最良の鍵回復攻撃は Broll ら [51] によって提案された差分線形攻撃であり、8 段のうち 7.5 段に簡略化した Chaskey に対しては、秘密鍵の全数探索よりも効率的に鍵回復攻撃が実行できる。

Chaskey については弱鍵が存在し、related-key setting においてその弱鍵を使用している場合、Chaskey-12 に対しては仕様段数であっても効率的に鍵回復攻撃と偽造攻撃が実行できる [152]。

6.3　LightMAC

6.3.1　仕様

■設計者　Atul Luykx[1,2], Bart Preneel[1,2], Elmar Tischhauser[3], Kan Yasuda[4]

(1: Katholieke Universiteit Leuven / Belgium, 2: iMinds / Belgium, 3: Technical University of Denmark / Denmark, 4: NTT Corporation / Japan)

■発表年（発表学会等）　2016 (FSE 2016 [191])

■仕様参照先　[191]

■特徴　LightMAC はブロック暗号を利用した暗号利用モードによるメッセージ認証コードアルゴリズムである。従来のメッセージ認証技術では、ブロック長の短い軽量ブロック暗号を利用した場合、大きなデータを処理すると安全性が低下してしまうという課題があったが、LightMAC ではブロック暗号に対して独特の繰り返し方法を用いることにより、この課題を解決した。これにより LightMAC は既存の軽量ブロック暗号の実装を有効活用しつつ必要な安全性を確保することができる（参考記事：NTT 持株会社ニュースリリース [299]）。

■主な実装性能評価結果　LightMAC のソフトウェア実装評価結果を表 6.4 に示す。なお、数値は cycles/byte である。

■標準化状況　ISO/IEC 29192-6 [2]

[*1] Mavromati [198] が述べているように、single-user mode における攻撃は Chaskey の設計者が主張する安全性証明と矛盾するものではないことに注意されたい。一方で、Chaskey の設計者は multi-user mode における安全性限界を示していないため、Mavromati [198] の結果は安全性限界のタイトネスを示したものであると解釈できる。

表 6.4　LightMAC のソフトウェア実装評価結果

Underlying Block Cipher	Rate	Message length [bytes]						
		128	256	512	1024	2048	4096	8192
PRESENT	1/2	25.50	23.67	22.75	22.32	22.08	21.97	21.92
PRESENT	2/3	25.70	21.21	20.17	19.03	18.09	17.80	17.80
PRESENT	7/8	20.31	18.34	14.65	13.48	–	–	–
AES	1/2	1.33	1.29	1.27	1.26	1.26	1.26	1.25
AES	2/3	1.37	1.31	1.12	1.04	0.95	0.95	0.92
AES	15/16	1.38	1.00	0.82	0.80	0.72	–	–

6.3.2　安全性解析状況（2021 年 9 月現在）

LightMAC [191] が提案されて以降、以下で示すような解析論文が発表されている。

- Darumaya と Susanti [73] による偽造攻撃 (Forgery attack)
- Windarta ら [273] による存在的偽造攻撃 (Existential forgery attack)

その他、LightMAC の派生版である LightMAC_Plus や LightMAC_Plus2 の安全性証明に関する研究論文 [209, 210] が発表されている。

Darumaya と Susanti [73] は Simeck32/64 を LightMAC の基礎となるブロック暗号に選択した場合、選択的偽造攻撃 (Selective forgery attack)、存在的偽造攻撃 (Existential forgery attack)、普遍的偽造攻撃 (Universal forgery attack) がそれぞれ 2^{16} の計算量で実行できることを示した。

Windarta ら [273] は同様に Simeck32/64 を LightMAC の基礎となるブロック暗号に選択した場合、存在的偽造攻撃が 2^{12}–2^{15} の計算量で実行できる場合があることを示した。

なお、Simeck32/64 以外のブロック暗号を利用した LightMAC に関する解析論文は発表されていない。

6.3.3　安全性解析状況のまとめ

2021 年 9 月現在、いくつかの解析論文 [73, 209, 210, 273] が発表されている。

基礎となるブロック暗号として Simeck32/64 を利用した LightMAC に対し、3 種類の偽造攻撃が現実的な計算量で実行可能であることが報告されている [73, 273]。なお、これらの攻撃の有効性を検証するためにブロック暗号として Simeck32/64 を利用したのであり、他のブロック暗号を利用した場合でもこれらの攻撃が成立する可能性があることに注意されたい。

6.4　Tsudik's keymode

6.4.1　仕様

■設計者　Gene Tsudik (University of Southern California, USA)

■発表年（発表学会等）　1992 (ACM SIGCOMM 1992 [259])

■仕様参照先　[259]

■特徴　Tsudik's keymode は一方向性ハッシュ関数を用いたメッセージ認証コードアルゴリズムであり、提案論文では MD4 を用いてアルゴリズムを紹介している。Tsudik's keymode では、通信相手との間で事前に乱数 R を共有しておき、R を MD4 への入力におけるシークレットプレフィックス又はシークレットサフィックスとして扱う。つまり、メッセージ M のメッセージダイジェストを MD4$(R||M)$ 又は MD4$(M||R)$ として扱う。

■主な実装性能評価結果　Tsudik's keymode の実装性能はその基礎となる一方向性ハッシュ関数に依存する。

■標準化状況　ISO/IEC 29192-6 [2]

6.4.2　安全性解析状況（2021 年 9 月現在）

提案論文 [259] において、Tsudik's keymode の安全性はその基礎となる一方向性ハッシュ関数の安全性に帰着されると主張している。その他、Tsudik's keymode 自身の安全性解析に関する論文が報告されていない。

6.4.3　安全性解析状況のまとめ

Tsudik's keymode の安全性はその基礎となる一方向性ハッシュ関数の安全性に帰着される。

第 7 章

軽量認証暗号の安全性解析状況

本章では、2016 年度ガイドライン [68, 69] の第 4.5 節に記載された代表的な軽量認証暗号 ACORN、ASCON、AES-JAMBU、AES-OTR、CLOC and SILC、Deoxys、Joltik、Ketje、Minalpher、OCB、PRIMATEs の安全性解析状況に関する調査結果をまとめる。また、AEGIS と COLM が CAESAR final portfolio に選出されている状況を鑑み、2016 年度ガイドラインに記載されていない AEGIS と COLM も調査対象とした。加えて、Grain-128A が RFID に関係する ISO/IEC 規格 (ISO/IEC 29167-13) [5] で採択されるとともに、軽量認証暗号に関係する ISO/IEC 規格 (ISO/IEC 29192-8) [3] での採択プロセスが進行中であるという状況を鑑み、2016 年度ガイドラインに記載されていない Grain-128A も調査対象とした。なお、AEGIS、COLM、Grain-128A に関しては安全性解析状況に関する調査結果だけでなく、その仕様（設計者、発表年、仕様参照先、特徴、主な実装性能評価結果）についても簡単にまとめる。

7.1 ACORN

ACORN は CAESAR final portfolio for use case 1: Lightweight applications に選出された。

7.1.1 2016 年度ガイドラインに記載されている安全性解析状況

2016 年度ガイドライン [69] の第 4.5 節によると、以下のとおり記載されている。

> Salam ら [229] による、初期攪拌回数を短くした場合の攻撃と、Nonce 重複を許した場合のフルスペックの解析が存在する。後者は $2^{72.8}$ の計算量と報告されている。そのほかいくつかの解析結果が存在する（例えば [154]）が、いずれも鍵総当たりより大きい計算量、あるいは鍵を既知とした場合の構造解析などであり。直接的な攻撃とはなっていない。
>
> 2016 年 12 月に、Roy ら [228] により、2^{40} という現実的な計算量における内部状態回復攻撃が提案された。ただし、この結果は ePrint への投稿であり、査読などの検証を未だ経ていないものであることを付記しておく。

表 7.1　ACORN v3 の安全性解析状況

Rounds	Attack type	Time	Ref.
503	Cube / Key Recovery	Practical	[229]
704	Cube / Key Recovery	$2^{122.0}$	[251, 252]
721	Cube / Distinguisher	$2^{95.0}$	[87]
750	Cube / Key Recovery	$2^{120.9}$	[118, 267]
772	Cube / Key Recovery [a)]	$2^{127.5}$	[277]
773	Cube / Key Recovery	$2^{127.0}$	[120, 121]
774	Cube / Key Recovery	$2^{127.0}$	[120, 121]
775	Cube / Key Recovery	$2^{127.0}$	[120, 121]

[a)] Attack does not work because of a flaw in the degeneration to distinguisher, which was pointed out in [120, 121].

7.1.2　上記以降の安全性解析状況（2021 年 9 月現在）

CAESAR final portfolio として選ばれたバージョンは ACORN v3 [30] であるが、上記の解析論文 [154, 228, 229] は全て ACORN v1 または ACORN v2 を対象とした評価であることに注意されたい。

ACORN v3 [30] が提案されて以降、以下で示すような解析論文が発表されている。

- Zhang と Lin [286] による nonce-misuse scenario での内部状態復元攻撃 (State recovery attack)
- Hao ら [120, 121] によるキューブ攻撃 (Cube attack)

その他、ACORN を対象とした様々な解析論文 [87, 118, 119, 147, 267, 277] が発表されている。

表 7.1 は文献 [277] の Table 1、文献 [121] の Table 1 と Table 2 に基づき、ACORN v3 の安全性解析状況についてまとめたものである。表 7.1 から、ACORN v3 に対しては Hao ら [121] によるキューブ攻撃が最良の攻撃であることがわかる。

Hao ら [121] は Wang ら [268] によって提案された three-subset division property のための新しい MILP モデリング手法を提案し、簡略化した ACORN v3 に対して提案手法を適用した。結果として、1792 段のうち 775 段に簡略化した ACORN v3 に対し、秘密鍵の全数探索よりも効率的に鍵回復攻撃が実行できることを示した。

また、Zhang と Lin [286] は平文の選択方法を詳細に分析することでキーストリームと内部状態で構築される線形式を従来手法より多く取得できることを明らかにした。結果として、3 つの異なる平文に対する暗号化において同じ nonce を再利用した場合、取得した線形式を解くことにより

$2^{120.6} \cdot c$ の計算量で内部状態を復元できることを示した。ここで、c は線形式を解くための計算量である。Nonce-misuse scenario を想定した場合、Zhang と Lin [286] はフルスペックの ACORN v3 に対して秘密鍵の全数探索よりも効率的に内部状態復元攻撃が実行できると主張しているが、線形式を解くための計算量 c については具体的に示していないことに注意されたい。

7.1.3　安全性解析状況のまとめ

2021 年 9 月現在、様々な解析論文 [87, 118, 119, 120, 121, 147, 154, 228, 229, 267, 277, 286] が発表されているが、仕様において秘密鍵の全数探索よりも効率的に実行可能な攻撃は発表されていない。

ACORN v3 に対する最良の攻撃は Hao ら [121] によって提案されたキューブ攻撃であり、1792 段のうち 775 段に簡略化した ACORN v3 に対しては、秘密鍵の全数探索よりも効率的に鍵回復攻撃が実行できる。

7.2　ASCON

ASCON は CAESAR final portfolio for use case 1: Lightweight applications に選出された。

7.2.1　2016 年度ガイドラインに記載されている安全性解析状況

2016 年度ガイドライン [69] の第 4.5 節によると、以下のとおり記載されている。

> 内部の置換の段数短縮に対する提案者らによる評価が存在する [93]。初期撹拌を 5 段（フルスペックは 12 段）にした場合、現実的な計算量 $\mathcal{O}(2^{35})$ で鍵導出が可能、同様に 6 段であれば $\mathcal{O}(2^{66})$ の攻撃計算量と報告されている。フルスペックに対する攻撃報告はない。

7.2.2　上記以降の安全性解析状況（2021 年 9 月現在）

CAESAR final portfolio として選ばれたバージョンは ASCON v1.2 [30] であるが、上記の解析論文 [93] は ASCON v1 を対象とした評価であることに注意されたい。

ASCON v1.2 [30] が提案されて以降、以下で示すような解析論文が発表されている。

- Tezcan [249] による切り詰め差分攻撃 (Truncated differential attack)
- Li ら [172] による条件付きキューブ攻撃 (Conditional cube attack)
- Li ら [169] によるキューブライク攻撃 (Cube-like attack)
- Rohit ら [227] によるキューブ攻撃と積分攻撃 (Integral attack)
- Gerault ら [108] による差分攻撃 (Differential attack)

表 7.2　ASCON v1.2 の安全性解析状況

Rounds	Attack type	Time	Data	Ref.
ASCON permutation				
5	Truncated Differential/Distinguisher	$2^{33.0}$	$2^{33.0}$	[93]
6	Algebraic/Distinguisher	$2^{33.0}$	$2^{33.0}$	[93]
7	Integral/Distinguisher	$2^{60.0}$	$2^{60.0}$	[227]
ASCON-128/ASCON-128A				
6	Cube-like/Key Recovery	$2^{66.0}$	$2^{66.0}$	[93]
7	Conditional Cube/Key Recovery[a)]	$2^{103.9}$	$2^{77.2}$	[172]
7	Cube-like/Key Recovery[b)]	$2^{97.0}$	$2^{33.0}$	[169]
7	Cube/Key Recovery	$2^{123.0}$	$2^{64.0}$	[227]
3	Differential/Forgery	$2^{33.0}$	$2^{33.0}$	[93]
3	Differential/Forgery	$2^{20.0}$	–	[108]
4	Differential/Forgery	$2^{96.6}$	–	[108]
6	Cube-like/Forgery[b)]	$2^{33.0}$	$2^{33.0}$	[169]
ASCON-Hash				
2	Differential/Collision	$2^{125.0}$	–	[295]
2	Differential/Collision	$2^{103.0}$	–	[108]

[a)] Invalid as the required data is beyond 2^{64}.

[b)] Invalid as the nonce is repeaded.

表 7.2 は文献 [227] の Table 1、文献 [108] の Table 1 に基づき、ASCON v1.2 の安全性解析状況についてまとめたものである。なお、文献 [108] の Table 1 では non-black-box distinguishers に関する安全性解析状況がまとめられているものの、本調査の対象外とする。表 7.2 から、ASCON v1.2 に対しては Li ら [169] によるキューブライク攻撃、Rohit ら [227] によるキューブ攻撃、Gerault ら [108] による衝突攻撃が最良の攻撃であることがわかる。

Li ら [169] は ASCON v1.2 の内部構造を詳細に分析し、適切なキューブ変数を導出するための性質を発見した。結果として、nonce-misuse setting において、12 段のうち 6 段に簡略化した ASCON v1.2 に対する偽造攻撃と 12 段のうち 7 段に簡略化した ASCON v1.2 に対する鍵回復攻撃を示した。

Rohit ら [227] は *partial polynomial multiplication* と呼ばれるキューブ攻撃において superpoly を効率的に復元する汎用的な手法を提案し、簡略化した ASCON v1.2 に対して提案手法を適用した。結果として、nonce-respecting setting において、12 段のうち 7 段に簡略化した ASCON v1.2 に対する鍵回復攻撃と識別攻撃を示した。

Gerault ら [108] は制約プログラミング (Constraint Programming) を使用して ASCON v1.2

における最良の差分特性を自動的に探索する方法を示し、既存の偽造攻撃や衝突攻撃を改善することが可能な差分特性を発見した。結果として、nonce-respecting setting において、12 段のうち 4 段に簡略化した ASCON v1.2 に対する偽造攻撃と 12 段のうち 2 段に簡略化した ASCON-Hash に対する衝突攻撃を示した。

7.2.3　安全性解析状況のまとめ

2021 年 9 月現在、いくつかの解析論文 [93, 108, 169, 172, 227] が発表されているが、仕様において秘密鍵の全数探索よりも効率的に実行可能な攻撃は発表されていない。

Nonce-respecting setting において、ASCON v1.2 に対する最良の攻撃は Rohit ら [227] によるキューブ攻撃、Gerault ら [108] による差分攻撃であり、12 段のうち 7 段に簡略化した ASCON v1.2 に対する鍵回復攻撃と識別攻撃、12 段のうち 4 段に簡略化した ASCON v1.2 に対する偽造攻撃、12 段のうち 2 段に簡略化した ASCON-Hash に対する衝突攻撃が実行できる。

Nonce-misuse setting において、ASCON v1.2 に対する最良の攻撃は Li ら [169] によるキューブライク攻撃であり、12 段のうち 6 段に簡略化した ASCON v1.2 に対する偽造攻撃と 12 段のうち 7 段に簡略化した ASCON v1.2 に対する鍵回復攻撃が実行できる。

7.3　AES-JAMBU

AES-JAMBU は CAESAR 3rd round candidates の 1 方式である。

7.3.1　2016 年度ガイドラインに記載されている安全性解析状況

2016 年度ガイドライン [69] の第 4.5 節によると、以下のとおり記載されている。

> 一般的な暗号利用モードとは異なり、ブロック暗号の計算量的安全性に基づく安全性帰着を提案者は示していない。提案者の主張では k ビット鍵、$2n$ ビットブロック暗号のときに、暗号化の安全性で k ビット、認証の安全性で n ビットとしている。Peyrin ら [217] により、Nonce-misuse scenario において $2^{n/2}$ 回の暗号化による攻撃と、Nonce-respecting scenario における CCA2 安全性に対する計算量 $2^{3n/2}$ の攻撃が報告されている。

なお、CCA2 とは適応的選択暗号文攻撃 (*Adaptive Chosen-Ciphertext Attack*) のことである。

7.3.2　上記以降の安全性解析状況（2021 年 9 月現在）

Peyrin ら [217] による解析論文の他、nonce-respecting と nonce-misuse scenarios での安全性証明に関する論文が Wang ら [263] によって発表されているが、nonce-misuse scenario において Peyrin らと同じ結果であることが示されている。

7.3.3　安全性解析状況のまとめ

2021 年 9 月現在、Peyrin ら [217] による解析論文の他、目立った解析論文は発表されていない。

一般的な暗号利用モードとは異なり、ブロック暗号の計算量的安全性に基づく安全性帰着を提案者は示していない。提案者の主張では k ビット鍵、$2n$ ビットブロック暗号のときに、暗号化の安全性で k ビット、認証の安全性で n ビットとしている。Peyrin ら [217] により、nonce-misuse scenario において $2^{n/2}$ 回の暗号化による攻撃と、nonce-respecting scenario における CCA2 (Adaptive Chosen-Ciphertext Attack) 安全性に対する計算量 $2^{3n/2}$ の攻撃が報告されている。なお、$n = 64$ である。

7.4　AES-OTR

AES-OTR は CAESAR 3rd round candidates の 1 方式である。

7.4.1　2016 年度ガイドラインに記載されている安全性解析状況

2016 年度ガイドライン [69] の第 4.5 節によると、以下のとおり記載されている。

> 提案論文にて、OTR の安全性がブロック暗号の擬似ランダム性（Pseudorandomness）へ帰着可能なことが示されている。n ビットブロック暗号の利用において $n/2$ ビットの証明可能安全性を有する。なお Bost ら [48] により内部のマスク生成における安全性証明との齟齬が指摘され、提案者の修正版が提案されている。

7.4.2　上記以降の安全性解析状況（2021 年 9 月現在）

Bost ら [48] による解析論文の他、目立った解析論文は発表されていない。

7.4.3　安全性解析状況のまとめ

2021 年 9 月現在、Bost ら [48] による解析論文の他、目立った解析論文は発表されていない。

提案論文にて、OTR の安全性がブロック暗号の擬似ランダム性（Pseudorandomness）へ帰着可能なことが示されている。n ビットブロック暗号の利用において $n/2$ ビットの証明可能安全性を有する。なお、Bost ら [48] により内部のマスク生成における安全性証明との齟齬が指摘され、提案者の修正版が提案されている。

7.5　CLOC and SILC

CLOC と SILC は CAESAR 3rd round candidates の 1 方式である。

7.5.1　2016 年度ガイドラインに記載されている安全性解析状況

2016 年度ガイドライン [69] の第 4.5 節によると、以下のとおり記載されている。

> 提案論文にて、CLOC と SILC の安全性が用いるブロック暗号の擬似ランダム性に帰着可能であることが示されている。n ビットブロック暗号を用いたとき $n/2$ ビットの安全性を有する。Nonce を誤って暗号化で重複させた場合でも暗号文の改ざんに対する安全性が保証されている。

7.5.2　上記以降の安全性解析状況（2021 年 9 月現在）

目立った解析論文は発表されていない。

7.5.3　安全性解析状況のまとめ

2021 年 9 月現在、目立った解析論文は発表されていない。

提案論文にて、CLOC と SILC の安全性が用いるブロック暗号の擬似ランダム性に帰着可能であることが示されている。n ビットブロック暗号を用いたとき $n/2$ ビットの安全性を有する。Nonce を誤って暗号化で重複させた場合でも暗号文の改ざんに対する安全性が保証されている。

7.6　Deoxys

Deoxys のバリエーションの 1 つである Deoxys-II は CAESAR final portfolio for use case 3: Defense in depth に選出された。

7.6.1　2016 年度ガイドラインに記載されている安全性解析状況

2016 年度ガイドライン [69] の第 4.5 節によると、以下のとおり記載されている。

> 提案論文にて、Deoxys-BC の安全性に帰着可能であり、TAE モードで 128 ビット安全性を持つことが示されている。SCT モードの安全性は [216] にて証明されている。

なお、TAE モードとは Liskov ら [177, 178] らによって提案された *Tweakable Authenticated Encryption* モードのことであり、SCT モードとは Peyrin と Seurin [216] によって提案された *Synthetic Counter in Tweak* モードのことである。

7.6.2　上記以降の安全性解析状況（2021 年 9 月現在）

CAESAR final portfolio として選ばれたバージョンは Deoxys v1.41 (Deoxys-II) [30] であるが、上記の解析論文 [216] は Deoxys v1.3 を対象とした評価であることに注意されたい。なお、Deoxys-I は Nonce-Respecting Mode、Deoxys-II は Nonce-Misuse Resistance Mode である。

Peyrin と Seurin [216] による安全性証明に関する解析論文が発表されて以降、以下で示すような解析論文が発表されている。

- Zhao ら [287] によるブーメラン攻撃 (Boomerang attack) と矩形攻撃 (Rectangle attack)
- Zhao ら [288] による矩形攻撃
- Liu ら [183] による中間一致攻撃 (Meet-in-the-Middle attack)
- Li と Chen [164] による中間一致攻撃

その他、Deoxys を対象とした様々な解析論文 [62, 96, 165, 204, 230, 296] が発表されている。

表 7.3 は文献 [287] の Table 1、文献 [288] の Table 1、文献 [164] の Table 1 に基づき、related-tweakkey setting における Deoxys v1.41 の安全性解析状況についてまとめたものである。表 7.3 から、related-tweakkey setting における Deoxys v1.41 に対しては Zhao ら [287] と Zhao ら [288] による矩形攻撃が最良の攻撃であることがわかる。

Zhao ら [287] は Cid ら [62] が提案した MILP モデリング手法を改良するとともに、*Boomerang Difference Table* と呼ばれる手法を応用し、簡略化した Deoxys v1.41 に対して提案手法を適用した。結果として、14 段のうち 10 段に簡略化した Deoxys-I-128-128 に対し、秘密鍵の全数探索よりも効率的に鍵回復攻撃が実行できることを示した。

Zhao ら [288] は Deoxys v1.41 の切り詰め差分特性を探索するために新しい MILP モデルを構築し、tweakey 差分の探索を行った。また、related-tweakey setting における矩形攻撃を実行するために、Zhao ら [287] と同様に *Boomerang Difference Table* と呼ばれる手法を応用し、簡略化した Deoxys v1.41 に対して提案手法を適用した。結果として、14 段のうち 13 段に簡略化した Deoxys-BC-256、16 段のうち 14 段に簡略化した Deoxys-BC-384、16 段のうち 13 段に簡略化した Deoxys-I-256-128 に対し、それぞれ秘密鍵の全数探索よりも効率的に鍵回復攻撃が実行できることを示した。

なお、2021 年 9 月現在、Deoxys-BC と Deoxys-I に関する様々な解析論文 [62, 96, 164, 165, 183, 204, 216, 230, 287, 288, 296] が発表されているのに対し、CAESAR final portfolio に選定された Deoxys-II に関する解析論文は発表されていない。また、文献 [287] において、提案された矩形攻撃は Deoxys-II に対して適用することができないと記述されている。

表 7.3　Related-tweakkey setting における Deoxys v1.41 の安全性解析状況

Cipher	Rounds	Attack type	Time	Data	Memory	Ref.
Deoxys-BC-256	9	Impossible Diff.	$2^{118.0}$	$2^{118.0}$	$2^{118.0}$	[204]
	9	Boomerang	$2^{112.0}$	$2^{98.0}$	$2^{17.0}$	[230]
	10	Meet-in-the-Middle	$2^{228.0}$	$2^{113.0}$	$2^{226.0}$	[165]
	10	Rectangle[a)]	$2^{204.0}$	$2^{127.6}$	$2^{127.6}$	[62]
	10	Impossible Diff.[a)]	$2^{173.0}$	$2^{135.0}$	–	[296]
	10	Boomerang[a)]	$2^{170.0}$	$2^{98.0}$	$2^{98.0}$	[230]
	10	Rectangle	$2^{114.2}$	$2^{114.2}$	$2^{112.2}$	[287]
	10	Boomerang	$2^{109.1}$	$2^{98.4}$	$2^{88.0}$	[287]
	11	Meet-in-the-Middle	$2^{251.0}$	$2^{113.0}$	$2^{226.0}$	[164]
	11	Rectangle[a)]	$2^{249.9}$	$2^{122.1}$	$2^{128.2}$	[287]
	12	Rectangle	$2^{208.0}$	$2^{115.0}$	$2^{113.0}$	[287]
	13	Rectangle	$2^{186.7}$	$2^{125.2}$	$2^{136.0}$	[288]
Deoxys-BC-384	12	Boomerang	$2^{148.0}$	$2^{100.0}$	$2^{100.0}$	[230]
	12	Rectangle	$2^{127.0}$	$2^{127.0}$	$2^{127.0}$	[62]
	12	Rectangle[a)]	$2^{114.0}$	$2^{114.0}$	$2^{112.0}$	[287]
	12	Boomerang[a)]	$2^{98.0}$	$2^{98.0}$	$2^{64.0}$	[287]
	12	Rectangle	$2^{208.0}$	$2^{115.0}$	$2^{113.0}$	[287]
	13	Rectangle[a)]	$2^{270.0}$	$2^{127.0}$	$2^{144.0}$	[62]
	13	Boomerang	$2^{191.3}$	$2^{125.0}$	$2^{136.0}$	[287]
	13	Rectangle	$2^{186.7}$	$2^{125.2}$	$2^{136.0}$	[288]
	14	Rectangle[a)]	$2^{286.2}$	$2^{127.0}$	$2^{136.0}$	[287]
	14	Rectangle[a)]	$2^{282.7}$	$2^{125.2}$	$2^{136.0}$	[288]
Deoxys-I-128-128	9	Rectangle	$2^{118.0}$	$2^{117.0}$	$2^{117.0}$	[62]
	10	Rectangle	$2^{114.2}$	$2^{114.2}$	$2^{112.2}$	[287]
Deoxys-I-256-128	12	Rectangle	$2^{236.0}$	$2^{126.0}$	$2^{124.0}$	[62]
	12	Rectangle	$2^{208.0}$	$2^{115.0}$	$2^{113.0}$	[287]
	13	Rectangle	$2^{186.7}$	$2^{125.2}$	$2^{136.0}$	[288]

[a)] This is not an attack on Deoxys with recommended parameters.

7.6.3　安全性解析状況のまとめ

2021 年 9 月現在、様々な解析論文 [62, 96, 164, 165, 183, 204, 216, 230, 287, 288, 296] が発表されているが、仕様において秘密鍵の全数探索よりも効率的に実行可能な攻撃は発表されていない。

Related-tweakey setting において、Deoxys v1.41 に対する最良の攻撃は Zhao ら [287] と Zhao ら [288] によって提案された矩形攻撃であり、14 段のうち 13 段に簡略化した Deoxys-BC-256、16 段のうち 14 段に簡略化した Deoxys-BC-384、14 段のうち 10 段に簡略化した Deoxys-I-128-128、16 段のうち 13 段に簡略化した Deoxys-I-256-128 に対しては、それぞれ秘密鍵の全数探索よりも効率的に鍵回復攻撃が実行できる。

なお、Deoxys-BC と Deoxys-I に関する解析論文がいくつか発表されているが、CAESAR final portfolio に選定された Deoxys-II に関する解析論文は発表されていない。

7.7　Joltik

Joltik は CAESAR 2nd round candidates の 1 方式である。

7.7.1　2016 年度ガイドラインに記載されている安全性解析状況

2016 年度ガイドライン [69] の第 4.5 節によると、以下のとおり記載されている。

> 提案論文にて、Joltik-BC の安全性に帰着可能、TAE モードで 64 ビット安全性を有することが示されている。

なお、TAE モードとは Liskov ら [177, 178] らによって提案された *Tweakable Authenticated Encryption* モードのことである。

7.7.2　上記以降の安全性解析状況（2021 年 9 月現在）

Joltik [30] が発表されて以降、以下で示すような解析論文が発表されている。

- Zong と Dong [294] による不能差分攻撃 (Impossible differential attack)
- Li ら [166] による中間一致攻撃 (Meet-in-the-Middle attack)
- Liu ら [184] による中間一致攻撃
- Li と Chen [163] による中間一致攻撃

表 7.4 は文献 [163] の Table 1 に基づき、Joltik の安全性解析状況についてまとめたものである。表 7.4 から、single-key setting における Joltik-BC に対しては Li ら [166] による中間一致攻撃、related-tweakkey setting における Joltik-BC に対しては Li と Chen [163] による中間一致攻撃がそれぞれ最良の攻撃であることがわかる。

Li ら [166] は *freedom of the tweak* と *differential enumeration technique* と呼ばれる手法を応用した中間一致攻撃を構成した。結果として、single-key setting において、24 段のうち 8 段の Joltik-BC-128、32 段のうち 10 段の Joltik-BC-192 に対し、それぞれ秘密鍵の全数探索よりも効率的に鍵回復攻撃が実行できることを示した。

Li と Chen [163] は Liu ら [184] が提案した *subtweakey difference cancellation*、*tweak differ-*

表 7.4　Joltik の安全性解析状況（SK: single-key setting、RK: related-tweakey setting）

Cipher	Rounds	Attack type	Time	Data	Memory	Ref.
Joltik-BC-128	8	SK/Meet-in-the-Middle	$2^{53.6}$	$2^{53.5}$	$2^{53.0}$	[166]
	9	RK/Impossible Diff.	$2^{61.7}$	$2^{60.0}$	$2^{50.0}$	[294]
	9	RK/Meet-in-the-Middle	$2^{56.6}$	$2^{53.0}$	$2^{52.9}$	[184]
	9	RK/Meet-in-the-Middle	$2^{54.1}$	$2^{53.0}$	$2^{52.9}$	[163]
Joltik-BC-192	10	SK/Meet-in-the-Middle	$2^{126.5}$	$2^{56.1}$	$2^{123.5}$	[166]
	11	RK/Meet-in-the-Middle	$2^{123.0}$	$2^{53.0}$	$2^{114.0}$	[163]

ence、*differential enumeration technique* と呼ばれる手法を改良し、新たな中間一致攻撃手法を提案した。結果として、related-tweakey setting において、24 段のうち 9 段の Joltik-BC-128、32 段のうち 11 段の Joltik-BC-192 に対して本攻撃を適用することにより、それぞれ秘密鍵の全数探索よりも効率的に鍵回復攻撃が実行できることを示した。

7.7.3　安全性解析状況のまとめ

2021 年 9 月現在、いくつかの解析論文 [163, 166, 184, 294] が発表されているが、仕様において秘密鍵の全数探索よりも効率的に実行可能な攻撃は発表されていない。

Single-key setting において、Joltik に対する最良の攻撃は Li ら [166] によって提案された中間一致攻撃であり、24 段のうち 8 段の Joltik-BC-128、32 段のうち 10 段の Joltik-BC-192 に対しては、それぞれ秘密鍵の全数探索よりも効率的に鍵回復攻撃が実行できる。Related-tweakey setting において、Joltik に対する最良の攻撃は Li と Chen [163] によって提案された中間一致攻撃であり、24 段のうち 9 段の Joltik-BC-128、32 段のうち 11 段の Joltik-BC-192 に対しては、それぞれ秘密鍵の全数探索よりも効率的に鍵回復攻撃が実行できる。

なお、Joltik-BC に関する解析論文がいくつか発表されているが、認証暗号としての Joltik に関する解析論文は発表されていない。

7.8　Ketje

Ketje は CAESAR 3rd round candidates の 1 方式である。

7.8.1　2016 年度ガイドラインに記載されている安全性解析状況

2016 年度ガイドライン [69] の第 4.5 節によると、以下のとおり記載されている。

> 内部の暗号学的置換が公開ランダム置換とした場合の安全性証明が存在する [70]。Keccak-p 置換に対しては、提案者らはベースとする Keccak-f の安全性評価結果の

大部分が引き継げるため安全としている。

7.8.2　上記以降の安全性解析状況（2021 年 9 月現在）

Ketje [30] が発表されて以降、以下で示すような解析論文が発表されている。

- Fuhr ら [106] による内部状態復元攻撃 (State recovery attack)
- Song と Guo [238] によるキューブ攻撃 (Cube attack)
- Song ら [239] による条件付きキューブ攻撃 (Conditional cube attack)
- Li ら [171] による条件付きキューブ攻撃
- Zhao ら [291] によるキューブ攻撃

その他、Ketje を対象としたいくつかの解析論文 [35, 95] が発表されている。

表 7.5 は文献 [106] の Table 1、文献 [238] の Table 1、文献 [239] の Table 2、文献 [171] の Table 1、文献 [291] の Table 1 に基づき、Ketje の安全性解析状況についてまとめたものである。なお、Ketje Jr v1 と Ketje Jr v2 の鍵長は 96 ビットが推奨されているため、鍵長が 96 ビットではない場合の安全性解析状況については対象外とした。表 7.5 から、Ketje に対しては Fuhr ら [106] による内部状態復元攻撃、Song と Guo [238] によるキューブ攻撃、Song ら [239] による条件付きキューブ攻撃、Li ら [171] による条件付きキューブ攻撃、Zhao ら [291] による条件付きキューブ攻撃がそれぞれ最良の攻撃であることがわかる。

Fuhr ら [106] はメッセージ処理フェーズにおいて生成される 3 つの連続したキーストリームブロックを使用することで、*divide-and-conquer strategy* による内部状態復元攻撃が実行できることを示した。結果として、ビットレートが 40 の Ketje Jr v1 と Ketje Jr v2 に対し、仕様段数であっても秘密鍵の全数探索より効率的に内部状態復元攻撃が実行できることを示した。なお、Ketje Jr におけるビットレートは 16 が推奨されており、この場合には仕様段数であっても秘密鍵の全数探索より効率的に内部状態復元攻撃が実行できないことに注意されたい。

Song と Guo [238] は Keccak-based keyed constructions に対するキューブ攻撃のための新しい MILP モデリング手法を提案し、Ketje Jr と Ketje Sr に対して提案手法を適用した。結果として、12 段のうち 5 段の Ketje Jr、12 段のうち 7 段の Ketje Sr に対し、それぞれ秘密鍵の全数探索よりも効率的に鍵回復攻撃が実行できることを示した。

Song ら [239] は Keccak のラウンド関数における S-box レイヤと linear レイヤの関係性を詳細に分析し、Keccak-based keyed constructions に対する条件付きキューブ攻撃のための新しい MILP モデリング手法を提案した。結果として、12 段のうち 7 段の Ketje Sr v1、Ketje Minor、Ketje Minor に対し、それぞれ秘密鍵の全数探索よりも効率的に鍵回復攻撃が実行できることを示した。

Li ら [171] は *kernel quadratic term technique* と呼ばれる手法を利用した新しい条件付きキューブ攻撃を提案した。結果として、12 段のうち 7 段の Ketje Sr に対し、それぞれ秘密鍵の全

表 7.5　Ketje の安全性解析状況

Cipher	Key size	Rounds	Attack type	Time	Ref.
Ketje Jr v1	96	5	Cube	$2^{56.0}$	[95]
		5	Cube	$2^{36.9}$	[238]
		12 (full)	State Recovery (Rate: 16)	$2^{152.0}$	[106]
		12 (full)	State Recovery (Rate: 24)	$2^{128.0}$	[106]
		12 (full)	State Recovery (Rate: 32)	$2^{104.0}$	[106]
		12 (full)	State Recovery (Rate: 40)	$2^{80.0}$	[106]
Ketje Jr v2	96	5	Cube	$2^{50.3}$	[95]
		5	Cube	$2^{34.9}$	[238]
		5	Cube	$2^{30.5}$	[291]
		12 (full)	State Recovery (Rate: 16)	$2^{152.0}$	[106]
		12 (full)	State Recovery (Rate: 24)	$2^{128.0}$	[106]
		12 (full)	State Recovery (Rate: 32)	$2^{104.0}$	[106]
		12 (full)	State Recovery (Rate: 40)	$2^{82.0}$	[106]
Ketje Sr v1	128	7	Cube	$2^{115.3}$	[95]
		7	Cube	$2^{114.0}$	[238]
		7	Conditional Cube	$2^{91.0}$	[239]
		7	Conditional Cube	$2^{75.0}$	[171]
Ketje Sr v2	128	7	Cube	$2^{113.9}$	[95]
		7	Cube	$2^{99.0}$	[238]
		7	Conditional Cube	$2^{77.0}$	[171]
Ketje Minor	128	7	Cube	$2^{113.0}$	[35]
		7	Conditional Cube	$2^{73.0}$	[239]
Ketje Major	128	7	Cube	$2^{94.0}$	[35]
		7	Conditional Cube	$2^{71.2}$	[239]

数探索よりも効率的に鍵回復攻撃が実行できることを示した。

Zhao ら [291] は Song と Guo [238] が提案した MILP モデリング手法を改良し、Ketje Jr に対して提案手法を適用した。結果として、12 段のうち 5 段の Ketje Jr v2 に対し、それぞれ秘密鍵の全数探索よりも効率的に鍵回復攻撃が実行できることを示した。

7.8.3　安全性解析状況のまとめ

2021 年 9 月現在、いくつかの解析論文 [35, 95, 106, 171, 238, 239, 291] が発表されているが、仕様において秘密鍵の全数探索よりも効率的に実行可能な攻撃は発表されていない。

Ketje に対する最良の攻撃は Song と Guo [238] によって提案されたキューブ攻撃、Song ら [239] によって提案されたキューブ攻撃、Li ら [171] によって提案された条件付きキューブ攻撃、Zhao ら [291] によって提案されたキューブ攻撃であり、12 段のうち 5 段に簡略化した Ketje Jr、12 段のうち 7 段に簡略化した Ketje Sr、Ketje Minor、Ketje Major に対しては、それぞれ秘密鍵の全数探索よりも効率的に鍵回復攻撃が実行できる。また、Ketje Jr に対する内部状態復元攻撃が Fuhr ら [106] によって提案され、ビットレートが 40 の場合には仕様段数であっても秘密鍵の全数探索より効率的に内部状態復元攻撃が実行できるものの、推奨パラメータであるビットレートが 16 の場合には秘密鍵の全数探索より効率的に内部状態復元攻撃が実行できない。

7.9　Minalpher

Minalpher は CAESAR 2nd round candidates の 1 方式である。

7.9.1　2016 年度ガイドラインに記載されている安全性解析状況

2016 年度ガイドライン [69] の第 4.5 節によると、以下のとおり記載されている。

> TEM ブロック暗号の安全性に帰着可能であり、128 ビット安全性を持つことが示されている。Minalpher-P は全部で 17.5 段の構造であるが、安全性評価として、CAESAR 提案書 [30] (Minalpher v1.0) にて 5.5 段まで短縮したときに攻撃が可能であることが示されている。

なお、TEM とは *Tweakable Even-Mansour* モードのことである。

7.9.2　上記以降の安全性解析状況（2021 年 9 月現在）

最新版の CAESAR 提案書 [30] (Minalpher v1.1) では、17.5 段のうち 6.5 段に簡略化した Minalpher-P に対する不能差分攻撃 (Impossible differential attack) が示されている。

Minalpher [30] が発表されて以降、以下で示すような解析論文が発表されている。

- Sasaki と Todo [232] による不能差分攻撃

その他、Minalpher を対象としたいくつかの解析論文 [53, 115] が発表されている。

Sasaki と Todo [232] は 8 ビット S-box の差分伝搬を制約式として表現することが従来では困難とされていたものの、任意のサイズの S-box に対して効率的に制約式を表現する手法を考案し、

制約式を微修正するだけで差分特性と不能差分特性を探索できる汎用的な MILP ツールを提案した。結果として、17.5 段のうち 7.5 段に簡略化した Minalpher に対し、効率的に識別攻撃が実行できることを示した。

7.9.3　安全性解析状況のまとめ

2021 年 9 月現在、いくつかの解析論文 [53, 115, 232] が発表されているが、仕様において秘密鍵の全数探索よりも効率的に実行可能な攻撃は発表されていない。

Minalpher に対する最良の攻撃は Sasaki と Todo [232] によって提案された不能差分攻撃であり、17.5 段のうち 7.5 段に簡略化した Minalpher に対しては、効率的に識別攻撃を実行できる。

7.10　OCB

OCB は CAESAR final portfolio for use case 2: High-performance applications に選出された。なお、OCB には 3 種類のバリエーション（OCB1、OCB2、OCB3）があるが、CAESAR への提案方式は OCB3 である。

7.10.1　2016 年度ガイドラインに記載されている安全性解析状況

2016 年度ガイドライン [69] の第 4.5 節によると、以下のとおり記載されている。

> 提案論文 [153, 223, 224, 225] にて、OCB の安全性がブロック暗号の強擬似ランダム性 (Strong Pseudorandomness) へ帰着可能なことが示されている。n ビットブロック暗号の利用において $n/2$ ビットの証明可能安全性を有する。

7.10.2　上記以降の安全性解析状況（2021 年 9 月現在）

OCB [153, 223, 224, 225] が発表されて以降、以下で示すような解析論文が発表されている。

- Inoue ら [138, 139] による OCB2 への普遍的偽造攻撃 (Universal forgery attack) と平文回復攻撃 (Full plaintext recovery attack)

その他、OCB を対象とした integrity security や INT-RUP security に関するいくつかの解析論文 [34, 127, 285] が発表されている。

Inoue ら [138, 139] は OCB2 で採用されている tweakable ブロック暗号 XEX* の欠陥と提案論文 [223] に記載された安全性証明の欠陥を指摘するとともに、OCB2 に対して現実的な普遍的偽造攻撃と平文回復攻撃が実行できることを示した。結果として、OCB2 は ISO 規格から除外されることとなった [6]。なお、OCB1 と OCB3 には影響がないことに注意されたい。

7.10.3　安全性解析状況のまとめ

2021 年 9 月現在、いくつかの解析論文 [34, 127, 138, 139, 285] が発表されている。

提案論文 [153, 223, 224, 225] にて、OCB の安全性がブロック暗号の強擬似ランダム性 (Strong Pseudorandomness) へ帰着可能なことが示されている。n ビットブロック暗号の利用において $n/2$ ビットの証明可能安全性を有する。

一方、Inoue ら [138, 139] は OCB2 の基礎となる tweakable ブロック暗号 XEX* に欠陥があることを示すとともに、既存の安全性証明にも欠陥があることを示した。これらの欠陥を悪用することにより、OCB2 に対しては現実的な攻撃として普遍的偽造攻撃と平文回復攻撃が実行できる。結果として、OCB2 が ISO/IEC19772:2009-02 規格から除外された [6]。

7.11　PRIMATEs

PRIMATEs は CAESAR 2nd round candidates の 1 方式である。

7.11.1　2016 年度ガイドラインに記載されている安全性解析状況

2016 年度ガイドライン [69] の第 4.5 節によると、以下のとおり記載されている。

> HANUMAN に対して、Associated Data がないときの処理の問題点を利用した現実的な偽造作成攻撃が報告されている [261]。提案者による修正が提案されている。

なお、PRIMATEs には、パラメータなどの設定の違いによって APE、GIBBON、HANUMAN という 3 種類の方式がある。

7.11.2　上記以降の安全性解析状況（2021 年 9 月現在）

PRIMATEs [30] が発表されて以降、以下で示すような解析論文が発表されている。

- Jovanovic ら [145] による多重衝突 (Multi-collision) に基づく汎用的攻撃

Jovanovic ら [145] は Sponge-based constructions をベースとした認証暗号に対する安全性証明を行った。この安全性証明では、*multi-collision probabilities* と呼ばれる確率を厳密に計算するとともに、多重衝突に基づく汎用的な攻撃手法を提案し、Sponge-based constructions をベースとした認証暗号に本攻撃を適用した。結果として、いくつかのパラメータ設定が保守的であり、パラメータを変更することで効率性を大幅に向上できることを示した。

7.11.3　安全性解析状況のまとめ

HANUMAN に対して、Associated Data がないときの処理の問題点を利用した現実的な偽造作成攻撃が報告されている [261]。その他、2021 年 9 月現在において目立った解析論文は発表されていない。

7.12　AEGIS

AEGIS のバリエーションの 1 つである AEGIS-128 は CAESAR final portfolio for use case 2: High-performance applications に選出された。

7.12.1　仕様

■設計者　Hongjun Wu[1] and Bart Preneel[2]
(1: Nanyang Technological University / Singapore, 2: Katholieke Universiteit Leuven / Belgium)

■発表年（発表学会等）　2013 (SAC 2013 [274])

■仕様参照先　[274]

■特徴　AEGIS は AEGIS-128L、AEGIS-128、AEGIS-256 の 3 種のバリエーションが提案されており、AEGIS-128 が final portfolio for use case 2: High-performance applications に選出された。AEGIS-128 は 640 (128 × 5) ビットの内部状態を持ち、5 つの AES ラウンド関数を並列に実行することで内部状態を更新する。鍵長、ナンス長、タグ長はそれぞれ 128 ビットを推奨している。また、ソフト・ハード両面での高速性が特徴として挙げられる。

■主な実装性能評価結果　2016 年度ガイドライン [69] の第 4.5 節に記載された方針に従い、ソフトウェア実装評価値 (SW) については eBACS 内の Supercop ベンチマークシステム [31] での十分長いメッセージ処理の結果、ハードウェア実装評価値 (HW) については ATHENA ベンチマークシステム [67] の結果を示す。

(SW)　AEGIS-128、Intel Core i5-1030NG7 (Icelake 4 × 1.1 GHz) で 0.41 cycle/byte。
(HW)　AEGIS-128L、Virtex 6 で 1,025 slices、fmax 320.8 MHz。

7.12.2　安全性解析状況（2021 年 9 月現在）

AEGIS [274] が発表されて以降、以下で示すような解析論文が発表されている。

- Minaud [201] による線形攻撃 (Linear attack)

表 7.6　AEGIS の安全性解析状況（線形特性）

Model	AEGIS-128	AEGIS-256	AEGIS-128L	Ref.
Manual Model	$c^{-2} \leq 2^{154}$	$c^{-2} \leq 2^{178}$		[201]
Truncated Model	$2^{92} \leq c^{-2}$	$2^{116} \leq c^{-2}$	$2^{114} \leq c^{-2} \leq 2^{172}$	[101]
Improved Model	$2^{102} \leq c^{-2} \leq 2^{140}$	$2^{120} \leq c^{-2}$		[101]
Bitwise Model	$2^{132} \leq c^{-2} \leq 2^{140}$	$2^{152} \leq c^{-2} \leq 2^{162}$	$2^{140} \leq c^{-2} \leq 2^{152}$	[101]

表 7.7　Weak-key setting における AEGIS-128 の安全性解析状況

Rounds	Attack type	Time	Data	Memory	Ref.
5	Integral/Distinguisher	$2^{32.0}$	$2^{32.0}$	–	[179]
5	Integral/Key Recovery	$2^{72.0}$	$2^{32.0}$	2^{25}	[179]

- Eichlseder ら [101] による線形攻撃
- Liu ら [179] による積分攻撃 (Integral attack)

表 7.6 は文献 [101] の Table 1 に基づき、AEGIS の線形特性に関する安全性解析状況についてまとめたものである。Eichlseder ら [101] は Minaud [201] が示した AEGIS のキーストリームに関する線形特性探索にインスピレーションを受け、MILP モデリング手法を用いて AEGIS のキーストリームに関する線形特性を再評価した。3 つのモデル (Truncated、Improved、Bitwise models) を構築して評価した結果、線形特性の上界と下界を厳密に評価したことを示すとともに、AEGIS-256 に対しては仕様段数であっても効率的に識別攻撃が実行できることを示した。

表 7.7 は文献 [179] の Table 1 に基づき、weak-key setting における AEGIS-128 の安全性解析状況についてまとめたものである。Liu ら [179] は AES ラウンド関数の積分特性について詳細に分析し、10 段のうち 5 段に簡略化した AEGIS-128 について弱鍵が存在することを明らかにした。この弱鍵を用いることで、10 段のうち 5 段に簡略化した AEGIS-128 に対し、効率的に鍵回復攻撃と識別攻撃が実行できることを示した。

7.12.3　安全性解析状況のまとめ

2021 年 9 月現在、いくつかの解析論文 [101, 179, 201] が発表されているが、仕様において秘密鍵の全数探索よりも効率的に実行可能な攻撃は発表されていない。

Single-key setting において、AEGIS に対する最良の攻撃は Eichlseder ら [101] によって提案された線形攻撃であり、AEGIS-256 に対しては仕様段数であっても効率的に識別攻撃を実行できる。なお、AEGIS-128 に対しては仕様段数であっても $2^{132} \leq c^{-2} \leq 2^{140}$ の計算量で識別攻撃を実行できる。

Weak-key setting において、AEGIS-128 に対する最良の攻撃は Liu ら [179] によって提案された積分攻撃であり、10 段のうち 5 段に簡略化した AEGIS-128 に対しては、効率的に鍵回復攻撃と

識別攻撃を実行できる。

7.13　COLM

COLM は CAESAR final portfolio for use case 3: Defense in depth に選出された。

7.13.1　仕様

■設計者　Elena Andreeva[1], Andrey Bogdanov[2], Nilanjan Datta[3], Atul Luykx[1], Bart Mennink[1], Mridul Nandi[3], Elmar Tischhauser[2], Kan Yasuda[4]

(1: Katholieke Universiteit Leuven / Belgium, 2: DTU Compute / Denmark, 3: Indian Statistical Institute / India, 4: NTT / Japan)

■発表年（発表学会等）　2016 [30]

■仕様参照先　[30]

■特徴　COLM は COLM_0 と COLM_{127} の 2 種のバリエーションが提案されており、いずれも final portfolio for use case 3: Defense in depth に選出された。当初、CAESAR submissions として AES-COPA と ELmD が投稿されたが、それぞれの長所を生かした形として COLM が設計された。COLM はブロック暗号ベースの Encrypt-Linearmix-Encrypt 構造を採用しており、ブロック暗号として AES-128 を利用する。鍵長とタグ長は 128 ビット、ナンス長は 64 ビットが推奨されている。COLM_0 と COLM_{127} の主な違いはタグ生成の手順であり、COLM_{127} では暗号化処理の途中で中間タグ値を生成した後、これらの中間タグ値を用いてタグ生成が実行される。

■主な実装性能評価結果　2016 年度ガイドライン [69] の第 4.5 節に記載された方針に従い、ソフトウェア実装評価値 (SW) については eBACS 内の Supercop ベンチマークシステム [31] での十分長いメッセージ処理の結果、ハードウェア実装評価値 (HW) については ATHENA ベンチマークシステム [67] の結果を示す。

(SW)　COLM_0、Intel Core i5-1030NG7 (Icelake 4 × 1.1 GHz) で 1.10 cycle/byte。
(SW)　COLM_{127}、Intel Core i5-1030NG7 (Icelake 4 × 1.1 GHz) で 30.06 cycle/byte。
(HW)　COLM_0、Virtex 6 で 2,060 slices、fmax 241.8 MHz。

7.13.2　安全性解析状況（2021 年 9 月現在）

COLM [30] が発表されて以降、以下で示すような解析論文が発表されている。

- Datta ら [74] による偽造攻撃 (Forgery attack)

なお、Datta ら [74] による解析論文が 2016 年に公開されて以降、COLM の安全性解析に関する

表 7.8　COLM の安全性解析状況

Mixing	Nonce	Complexity (ignoring constants)			Ref.
		Encrypt	Decrypt	Length [blocks]	
XOR	respecting	1	2	$2n$	[74]
any	misusing	$4n$	$4n$	$3n$	[74]
any	respecting	1	$2n$	$(n+1)n$	[74]

論文は発表されていない。

表 7.8 は文献 [74] の Table 1 に基づき、COLM の安全性解析状況についてまとめたものであり、n はブロックサイズである。Datta ら [74] は COLM type structure (COLM$_0$、COPA、ELmE、ELmD) に対する Release of Unverified Plaintext (RUP) security の評価を実施した。RUP では、タグが未検証の場合において平文が得られることを仮定する。結果として、nonce-respecting setting における COPA への偽造攻撃と nonce-misuse setting における 任意の COLM type structure への偽造攻撃が実行可能であることを示すとともに、nonce-misuse setting における偽造攻撃を nonce-respecting setting における 偽造攻撃へと拡張する方法について示した。なお、これらの偽造攻撃については COLM$_{127}$ には影響しないことに注意されたい。

7.13.3　安全性解析状況のまとめ

2021 年 9 月現在、Datta ら [74] の他、目立った解析論文は発表されていない。

Datta ら [74] は COLM タイプの認証暗号に対し、nonce-misuse setting と nonce-respecting setting における INT-RUP 攻撃について議論した。n をブロックサイズとすると、nonce-misuse setting において暗号化・復号クエリが各 $4n$ 回、メッセージブロックサイズが $3n$ ブロックの場合に偽造攻撃が成立し、nonce-respecting setting において暗号化クエリが 1 回、復号クエリが $2n$ 回、メッセージブロックサイズが $(n+1)n$ ブロックの場合に偽造攻撃が成立する。なお、これらの偽造攻撃については COLM$_{127}$ に影響しない。

7.14　Grain-128A

Grain-128A は RFID に関係する ISO/IEC 規格 (ISO/IEC 29167-13) で採択されるとともに、軽量暗号に関係する ISO/IEC 規格 (ISO/IEC 29192-8) での採択プロセスが進行中である。

7.14.1　仕様

■設計者　Martin Agren[1], Martin Hell[1], Thomas Johansson[1], Willi Meier[2]

(1: Lund University / Sweden, 2: FHNW / Switzerland)

表 7.9　Grain-128A のハードウェア実装評価結果

# of parallel	Frequency [GHz]	Throughput [Gbps]	Area [μm^2]	Power [μW]
1	2.1	1.1	5,876	96.9
2	2.0	2.0	6.972	106.1
4	2.0	4.0	8,299	120.6
8	1.9	7.6	10,778	176.4
16	1.7	13.6	15,709	247.8
32	1.5	24.0	23,430	417.9

■発表年（発表学会等）　2011 [10]

■仕様参照先　[10]

■特徴　Grain-128A は eSTREAM portfolio に選ばれた Grain v1、その派生版である Grain-128 と同様の構造を有するハードウェア実装向けのストリーム暗号であるが、認証機能をサポートしていることが大きな違いである。初期化フェーズは 256 段、鍵長は 128 ビット、ナンス長は 96 ビットであり、タグ長は任意に設定できるものの 32 ビットが推奨されている。Grain-128A は Grain-128 に対する既存の攻撃に耐性を持つよう非線形関数が改良されている。なお、NIST LWC finalists の 1 つである Grain-128AEAD についても同様の構造を有しており、Grain-128A に対する既存の攻撃に耐性を持つようさらに改良が施されている。

■主な実装性能評価結果　ハードウェア実装評価結果 (Cadence RTL Compiler, TSMC 90 nm ASIC) [197]。なお、全てオリジナル実装の結果である。

7.14.2　安全性解析状況（2021 年 9 月現在）

Grain-128A [10] が発表されて以降、以下で示すような解析論文が発表されている。

- Wang ら [118, 267] によるキューブ攻撃 (Cube attack)
- Todo ら [253] による高速相関攻撃 (Fast correlation attack)

その他、Grain-128A を対象としたいくつかの解析論文 [156, 251, 252] が発表されている。

表 7.10 は文献 [118] の Table 1、文献 [253] の Table 1 に基づき、Grain-128A の安全性解析状況についてまとめたものである。表 7.10 から、Grain-128A に対しては Todo ら [253] による高速相関攻撃が最良の攻撃であることがわかる。

Todo ら [253] は高速相関攻撃を改善するための *parity-check equations* と *modified wrong-key hypothesis* と呼ばれる新しいテクニックを提案し、フルスペックの Grain v1、Grain-128、Grain-128A に対して提案手法を適用した。結果として、Grain-128A に対しては仕様段数であっても効率

表 7.10　Grain-128A の安全性解析状況

Rounds	Attack type	Time	Ref.
177	Cube	Practical	[156]
182	Cube	$2^{106.0}$	[251, 252]
182	Cube	$2^{102.0}$	[118, 267]
183	Cube	$2^{108.0}$	[251, 252]
183	Cube	$2^{108.0} - 2^{96.1}$	[118, 267]
184	Cube	$2^{116.0}$	[118, 267]
184	Cube	$2^{109.6}$	[118, 267]
256 (full)	Fast Correlation	$2^{115.4}$	[253]

的に内部状態復元攻撃を実行できることが示されている。

7.14.3　安全性解析状況のまとめ

2021 年 9 月現在、いくつかの解析論文 [118, 156, 251, 252, 253, 267] が発表されている。

Grain-128A に対する最良の攻撃は Todo ら [253] によって提案された高速相関攻撃であり、Grain-128A に対しては仕様段数であっても秘密鍵の全数探索より効率的に内部状態復元攻撃が実行できる。なお、設計者が主張するセキュリティレベルは Grain-128A において 128 ビットである。本攻撃では、Grain-128A に対して $2^{115.4}$ $(< 2^{128.0})$ の計算量で実行可能であり、一般的な秘密鍵の全数探索と比較して $2^{12.6}$ 倍の効率化に成功した。

参考文献

[1] Information security – Lightweight cryptography – Part 2: Block ciphers (ISO/IEC 29192-2:2019). https://www.iso.org/standard/78477.html.

[2] Information security – Lightweight cryptography – Part 6: Message authentication codes (MACs) (ISO/IEC 29192-6:2019). https://www.iso.org/standard/71116.html.

[3] Information security – Lightweight cryptography – Part 8: Authenticated encryption (ISO/IEC DIS 29192-8). https://www.iso.org/standard/71116.html.

[4] Information security – Security techniques – Lightweight cryptography – Part 5: Hash-functions (ISO/IEC 29192-5:2016). https://www.iso.org/standard/67173.html.

[5] Information technology – Automatic identification and data capture techniques – Part 13: Crypto suite Grain-128A security services for air interface communications (ISO/IEC 29167-13: 2015). https://www.iso.org/standard/60682.html.

[6] ISO/IEC JTC 1/SC 27 STATEMENT ON OCB2.0 – Major weakness found in a standardised cipher scheme (2019-01-09, press release). https://www.din.de/blob/321470/da3d9bce7116deb510f6aded2ed0b4df/20190107-press-release-19772-2009-1st-ed-ocb2-0-data.pdf.

[7] Mohamed Ahmed Abdelraheem. Estimating the Probabilities of Low-Weight Differential and Linear Approximations on PRESENT-Like Ciphers. In Taekyoung Kwon, Mun-Kyu Lee, and Daesung Kwon, editors, *Information Security and Cryptology - ICISC 2012 - 15th International Conference, Seoul, Korea, November 28-30, 2012, Revised Selected Papers*, volume 7839 of *Lecture Notes in Computer Science*, pages 368–382. Springer, 2012.

[8] Farzaneh Abed, Christian Forler, Eik List, Stefan Lucks, and Jakob Wenzel. Biclique Cryptanalysis of the PRESENT and LED Lightweight Ciphers. *IACR Cryptol. ePrint Arch.*, 2012:591, 2012.

[9] Farzaneh Abed, Eik List, Stefan Lucks, and Jakob Wenzel. Differential Cryptanalysis of Round-Reduced Simon and Speck. In Carlos Cid and Christian Rechberger, editors, *Fast Software Encryption - 21st International Workshop, FSE 2014, London, UK, March 3-5, 2014. Revised Selected Papers*, volume 8540 of *Lecture Notes in Computer Science*,

pages 525–545. Springer, 2014.

[10] Martin Ågren, Martin Hell, Thomas Johansson, and Willi Meier. Grain-128a: a new version of Grain-128 with optional authentication. *Int. J. Wirel. Mob. Comput.*, 5(1):48–59, 2011.

[11] Siavash Ahmadi, Zahra Ahmadian, Javad Mohajeri, and Mohammad Reza Aref. Biclique Cryptanalysis of Block Ciphers LBlock and TWINE-80 with Practical Data Complexity. *ISC Int. J. Inf. Secur.*, 11(1):57–74, 2019.

[12] Ralph Ankele and Stefan Kölbl. Mind the Gap - A Closer Look at the Security of Block Ciphers against Differential Cryptanalysis. In Carlos Cid and Michael J. Jacobson Jr., editors, *Selected Areas in Cryptography - SAC 2018 - 25th International Conference, Calgary, AB, Canada, August 15-17, 2018, Revised Selected Papers*, volume 11349 of *Lecture Notes in Computer Science*, pages 163–190. Springer, 2018.

[13] Jean-Philippe Aumasson and Daniel J. Bernstein. SipHash: A Fast Short-Input PRF. In Steven D. Galbraith and Mridul Nandi, editors, *Progress in Cryptology - INDOCRYPT 2012, 13th International Conference on Cryptology in India, Kolkata, India, December 9-12, 2012. Proceedings*, volume 7668 of *Lecture Notes in Computer Science*, pages 489–508. Springer, 2012.

[14] Jean-Philippe Aumasson, Simon Fischer, Shahram Khazaei, Willi Meier, and Christian Rechberger. New Features of Latin Dances: Analysis of Salsa, ChaCha, and Rumba. In Kaisa Nyberg, editor, *Fast Software Encryption, 15th International Workshop, FSE 2008, Lausanne, Switzerland, February 10-13, 2008, Revised Selected Papers*, volume 5086 of *Lecture Notes in Computer Science*, pages 470–488. Springer, 2008.

[15] Jean-Philippe Aumasson, Luca Henzen, Willi Meier, and María Naya-Plasencia. Quark: A Lightweight Hash. In Stefan Mangard and François-Xavier Standaert, editors, *Cryptographic Hardware and Embedded Systems, CHES 2010, 12th International Workshop, Santa Barbara, CA, USA, August 17-20, 2010. Proceedings*, volume 6225 of *Lecture Notes in Computer Science*, pages 1–15. Springer, 2010.

[16] Jean-Philippe Aumasson, Luca Henzen, Willi Meier, and María Naya-Plasencia. Quark: A Lightweight Hash. *J. Cryptol.*, 26(2):313–339, 2013.

[17] Seyyed Arash Azimi, Zahra Ahmadian, Javad Mohajeri, and Mohammad Reza Aref. Impossible differential cryptanalysis of Piccolo lightweight block cipher. In *11th International ISC Conference on Information Security and Cryptology, ISCISC 2014, Tehran, Iran, September 3-4, 2014*, pages 89–94. IEEE, 2014.

[18] Steve Babbage and Matthew Dodd. The MICKEY Stream Ciphers. In Matthew J. B. Robshaw and Olivier Billet, editors, *New Stream Cipher Designs - The eSTREAM Finalists*, volume 4986 of *Lecture Notes in Computer Science*, pages 191–209. Springer, 2008.

[19] Elnaz Bagherzadeh and Zahra Ahmadian. MILP-based automatic differential search for LEA and HIGHT block ciphers. *IET Inf. Secur.*, 14(5):595–603, 2020.

[20] Subhadeep Banik. Some Insights into Differential Cryptanalysis of Grain v1. In Willy Susilo and Yi Mu, editors, *Information Security and Privacy - 19th Australasian Conference, ACISP 2014, Wollongong, NSW, Australia, July 7-9, 2014. Proceedings*, volume 8544 of *Lecture Notes in Computer Science*, pages 34–49. Springer, 2014.

[21] Subhadeep Banik. Conditional differential cryptanalysis of 105 round Grain v1. *Cryptogr. Commun.*, 8(1):113–137, 2016.

[22] Zhenzhen Bao, Jian Guo, Meicheng Liu, Li Ma, and Yi Tu. Conditional Differential-Neural Cryptanalysis. *IACR Cryptol. ePrint Arch.*, 2021:719, 2021.

[23] Stefano Barbero, Emanuele Bellini, and Rusydi H. Makarim. Rotational analysis of ChaCha permutation. *IACR Cryptol. ePrint Arch.*, 2020:1049, 2020.

[24] Baudoin Collard and François-Xavier Standaert and Jean-Jacques Quisquater. Improving the time complexity of matsui's linear cryptanalysis. In Kil-Hyun Nam and Gwangsoo Rhee, editors, *Information Security and Cryptology - ICISC 2007, 10th International Conference, Seoul, Korea, November 29-30, 2007, Proceedings*, volume 4817 of *Lecture Notes in Computer Science*, pages 77–88. Springer, 2007.

[25] Christof Beierle. Pen and Paper Arguments for SIMON and SIMON-like Designs. In Vassilis Zikas and Roberto De Prisco, editors, *Security and Cryptography for Networks - 10th International Conference, SCN 2016, Amalfi, Italy, August 31 - September 2, 2016, Proceedings*, volume 9841 of *Lecture Notes in Computer Science*, pages 431–446. Springer, 2016.

[26] Christof Beierle, Anne Canteaut, and Gregor Leander. Nonlinear Approximations in Cryptanalysis Revisited. *IACR Trans. Symmetric Cryptol.*, 2018(4):80–101, 2018.

[27] Christof Beierle, Gregor Leander, and Yosuke Todo. Improved Differential-Linear Attacks with Applications to ARX Ciphers. In Daniele Micciancio and Thomas Ristenpart, editors, *Advances in Cryptology - CRYPTO 2020 - 40th Annual International Cryptology Conference, CRYPTO 2020, Santa Barbara, CA, USA, August 17-21, 2020, Proceedings, Part III*, volume 12172 of *Lecture Notes in Computer Science*, pages 329–358. Springer, 2020.

[28] Adrien Benamira, David Gérault, Thomas Peyrin, and Quan Quan Tan. A Deeper Look at Machine Learning-Based Cryptanalysis. In Anne Canteaut and François-Xavier Standaert, editors, *Advances in Cryptology - EUROCRYPT 2021 - 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17-21, 2021, Proceedings, Part I*, volume 12696 of *Lecture Notes in Computer Science*, pages 805–835. Springer, 2021.

[29] Côme Berbain, Henri Gilbert, and Alexander Maximov. Cryptanalysis of Grain. In

Matthew J. B. Robshaw, editor, *Fast Software Encryption, 13th International Workshop, FSE 2006, Graz, Austria, March 15-17, 2006, Revised Selected Papers*, volume 4047 of *Lecture Notes in Computer Science*, pages 15–29. Springer, 2006.

[30] Daniel J. Bernstein. CAESAR: Competition for Authenticated Encryption: Security, Applicability, and Robustness. http://competitions.cr.yp.to/caesar.html.

[31] Daniel J. Bernstein. eBACS: ECRYPT Benchmarking of Cryptographic Systems. http://bench.cr.yp.to/results-caesar.html/.

[32] Tim Beyne. Block Cipher Invariants as Eigenvectors of Correlation Matrices. In Thomas Peyrin and Steven D. Galbraith, editors, *Advances in Cryptology - ASIACRYPT 2018 - 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2-6, 2018, Proceedings, Part I*, volume 11272 of *Lecture Notes in Computer Science*, pages 3–31. Springer, 2018.

[33] Tim Beyne. Block Cipher Invariants as Eigenvectors of Correlation Matrices. *J. Cryptol.*, 33(3):1156–1183, 2020.

[34] Ritam Bhaumik and Mridul Nandi. Improved Security for OCB3. In Tsuyoshi Takagi and Thomas Peyrin, editors, *Advances in Cryptology - ASIACRYPT 2017 - 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part II*, volume 10625 of *Lecture Notes in Computer Science*, pages 638–666. Springer, 2017.

[35] Wenquan Bi, Xiaoyang Dong, Zheng Li, Rui Zong, and Xiaoyun Wang. MILP-aided cube-attack-like cryptanalysis on Keccak Keyed modes. *Des. Codes Cryptogr.*, 87(6):1271–1296, 2019.

[36] Alex Biryukov, Patrick Derbez, and Léo Perrin. Differential Analysis and Meet-in-the-Middle Attack Against Round-Reduced TWINE. In Gregor Leander, editor, *Fast Software Encryption - 22nd International Workshop, FSE 2015, Istanbul, Turkey, March 8-11, 2015, Revised Selected Papers*, volume 9054 of *Lecture Notes in Computer Science*, pages 3–27. Springer, 2015.

[37] Alex Biryukov, Arnab Roy, and Vesselin Velichkov. Differential Analysis of Block Ciphers SIMON and SPECK. In Carlos Cid and Christian Rechberger, editors, *Fast Software Encryption - 21st International Workshop, FSE 2014, London, UK, March 3-5, 2014. Revised Selected Papers*, volume 8540 of *Lecture Notes in Computer Science*, pages 546–570. Springer, 2014.

[38] Alex Biryukov, Vesselin Velichkov, and Yann Le Corre. Automatic Search for the Best Trails in ARX: Application to Block Cipher Speck. In Thomas Peyrin, editor, *Fast Software Encryption - 23rd International Conference, FSE 2016, Bochum, Germany, March 20-23, 2016, Revised Selected Papers*, volume 9783 of *Lecture Notes in Computer Science*, pages 289–310. Springer, 2016.

[39] Céline Blondeau and Kaisa Nyberg. Links between Truncated Differential and Multidimensional Linear Properties of Block Ciphers and Underlying Attack Complexities. In Phong Q. Nguyen and Elisabeth Oswald, editors, *Advances in Cryptology - EUROCRYPT 2014 - 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, May 11-15, 2014. Proceedings*, volume 8441 of *Lecture Notes in Computer Science*, pages 165–182. Springer, 2014.

[40] Céline Blondeau and Kaisa Nyberg. Improved Parameter Estimates for Correlation and Capacity Deviates in Linear Cryptanalysis. *IACR Trans. Symmetric Cryptol.*, 2016(2):162–191, 2016.

[41] Céline Blondeau, Thomas Peyrin, and Lei Wang. Known-Key Distinguisher on Full PRESENT. In Rosario Gennaro and Matthew Robshaw, editors, *Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part I*, volume 9215 of *Lecture Notes in Computer Science*, pages 455–474. Springer, 2015.

[42] Andrey Bogdanov, Christina Boura, Vincent Rijmen, Meiqin Wang, Long Wen, and Jingyuan Zhao. Key Difference Invariant Bias in Block Ciphers. In Kazue Sako and Palash Sarkar, editors, *Advances in Cryptology - ASIACRYPT 2013 - 19th International Conference on the Theory and Application of Cryptology and Information Security, Bengaluru, India, December 1-5, 2013, Proceedings, Part I*, volume 8269 of *Lecture Notes in Computer Science*, pages 357–376. Springer, 2013.

[43] Andrey Bogdanov, Huizheng Geng, Meiqin Wang, Long Wen, and Baudoin Collard. Zero-Correlation Linear Cryptanalysis with FFT and Improved Attacks on ISO Standards Camellia and CLEFIA. In Tanja Lange, Kristin E. Lauter, and Petr Lisonek, editors, *Selected Areas in Cryptography - SAC 2013 - 20th International Conference, Burnaby, BC, Canada, August 14-16, 2013, Revised Selected Papers*, volume 8282 of *Lecture Notes in Computer Science*, pages 306–323. Springer, 2013.

[44] Andrey Bogdanov, Dmitry Khovratovich, and Christian Rechberger. Biclique Cryptanalysis of the Full AES. In Dong Hoon Lee and Xiaoyun Wang, editors, *Advances in Cryptology - ASIACRYPT 2011 - 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011. Proceedings*, volume 7073 of *Lecture Notes in Computer Science*, pages 344–371. Springer, 2011.

[45] Andrey Bogdanov, Miroslav Knezevic, Gregor Leander, Deniz Toz, Kerem Varici, and Ingrid Verbauwhede. spongent: A Lightweight Hash Function. In Bart Preneel and Tsuyoshi Takagi, editors, *Cryptographic Hardware and Embedded Systems - CHES 2011 - 13th International Workshop, Nara, Japan, September 28 - October 1, 2011. Proceedings*, volume 6917 of *Lecture Notes in Computer Science*, pages 312–325. Springer, 2011.

[46] Andrey Bogdanov, Elmar Tischhauser, and Philip S. Vejre. Multivariate Profiling of Hulls for Linear Cryptanalysis. *IACR Trans. Symmetric Cryptol.*, 2018(1):101–125, 2018.

[47] Rachelle Heim Boissier, Camille Noûs, and Yann Rotella. Algebraic Collision Attacks on Keccak. *IACR Trans. Symmetric Cryptol.*, 2021(1):239–268, 2021.

[48] Raphael Bost and Olivier Sanders. Trick or Tweak: On the (In)security of OTR's Tweaks. In Jung Hee Cheon and Tsuyoshi Takagi, editors, *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*, volume 10031 of *Lecture Notes in Computer Science*, pages 333–353, 2016.

[49] Charles Bouillaguet, Orr Dunkelman, Gaëtan Leurent, and Pierre-Alain Fouque. Attacks on Hash Functions Based on Generalized Feistel: Application to Reduced-Round *Lesamnta* and *SHAvite-3*$_{512}$. In Alex Biryukov, Guang Gong, and Douglas R. Stinson, editors, *Selected Areas in Cryptography - 17th International Workshop, SAC 2010, Waterloo, Ontario, Canada, August 12-13, 2010, Revised Selected Papers*, volume 6544 of *Lecture Notes in Computer Science*, pages 18–35. Springer, 2010.

[50] Christina Boura, María Naya-Plasencia, and Valentin Suder. Scrutinizing and Improving Impossible Differential Attacks: Applications to CLEFIA, Camellia, LBlock and Simon. In Palash Sarkar and Tetsu Iwata, editors, *Advances in Cryptology - ASIACRYPT 2014 - 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, R.O.C., December 7-11, 2014. Proceedings, Part I*, volume 8873 of *Lecture Notes in Computer Science*, pages 179–199. Springer, 2014.

[51] Marek Broll, Federico Canale, Nicolas David, Antonio Flórez-Gutiérrez, Gregor Leander, María Naya-Plasencia, and Yosuke Todo. Further Improving Differential-Linear Attacks: Applications to Chaskey and Serpent. *IACR Cryptol. ePrint Arch.*, 2021:820, 2021.

[52] Anne Canteaut, Thomas Fuhr, Henri Gilbert, María Naya-Plasencia, and Jean-René Reinhard. Multiple Differential Cryptanalysis of Round-Reduced PRINCE. In Carlos Cid and Christian Rechberger, editors, *Fast Software Encryption - 21st International Workshop, FSE 2014, London, UK, March 3-5, 2014. Revised Selected Papers*, volume 8540 of *Lecture Notes in Computer Science*, pages 591–610. Springer, 2014.

[53] Anne Canteaut, Eran Lambooij, Samuel Neves, Shahram Rasoolzadeh, Yu Sasaki, and Marc Stevens. Refined Probability of Differential Characteristics Including Dependency Between Multiple Rounds. *IACR Trans. Symmetric Cryptol.*, 2017(2):203–227, 2017.

[54] Anne Canteaut, María Naya-Plasencia, and Bastien Vayssière. Sieve-in-the-Middle: Improved MITM Attacks. In Ran Canetti and Juan A. Garay, editors, *Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part I*, volume 8042 of *Lecture Notes in Computer*

Science, pages 222–240. Springer, 2013.

[55] Huaifeng Chen and Xiaoyun Wang. Improved Linear Hull Attack on Round-Reduced Simon with Dynamic Key-Guessing Techniques. In Thomas Peyrin, editor, *Fast Software Encryption - 23rd International Conference, FSE 2016, Bochum, Germany, March 20-23, 2016, Revised Selected Papers*, volume 9783 of *Lecture Notes in Computer Science*, pages 428–449. Springer, 2016.

[56] Yi Chen and Hongbo Yu. Bridging Machine Learning and Cryptanalysis via EDLCT. *IACR Cryptol. ePrint Arch.*, 2021:705, 2021.

[57] Yi Chen and Hongbo Yu. Improved Neural Aided Statistical Attack for Cryptanalysis. *IACR Cryptol. ePrint Arch.*, 2021:311, 2021.

[58] Zhan Chen, Huaifeng Chen, and Xiaoyun Wang. Cryptanalysis of Midori128 Using Impossible Differential Techniques. In Feng Bao, Liqun Chen, Robert H. Deng, and Guojun Wang, editors, *Information Security Practice and Experience - 12th International Conference, ISPEC 2016, Zhangjiajie, China, November 16-18, 2016, Proceedings*, volume 10060 of *Lecture Notes in Computer Science*, pages 1–12, 2016.

[59] Joo Yeon Cho. Linear Cryptanalysis of Reduced-Round PRESENT. In Josef Pieprzyk, editor, *Topics in Cryptology - CT-RSA 2010, The Cryptographers' Track at the RSA Conference 2010, San Francisco, CA, USA, March 1-5, 2010. Proceedings*, volume 5985 of *Lecture Notes in Computer Science*, pages 302–317. Springer, 2010.

[60] Arka Rai Choudhuri and Subhamoy Maitra. Significantly Improved Multi-bit Differentials for Reduced Round Salsa and ChaCha. *IACR Trans. Symmetric Cryptol.*, 2016(2):261–287, 2016.

[61] Zhihui Chu, Huaifeng Chen, Xiaoyun Wang, Xiaoyang Dong, and Lu Li. Improved Integral Attacks on SIMON32 and SIMON48 with Dynamic Key-Guessing Techniques. *Secur. Commun. Networks*, 2018:5160237:1–5160237:11, 2018.

[62] Carlos Cid, Tao Huang, Thomas Peyrin, Yu Sasaki, and Ling Song. A Security Analysis of Deoxys and its Internal Tweakable Block Ciphers. *IACR Trans. Symmetric Cryptol.*, 2017(3):73–107, 2017.

[63] Mustafa Çoban, Ferhat Karakoç, and Özkan Boztas. Biclique Cryptanalysis of TWINE. In Josef Pieprzyk, Ahmad-Reza Sadeghi, and Mark Manulis, editors, *Cryptology and Network Security, 11th International Conference, CANS 2012, Darmstadt, Germany, December 12-14, 2012. Proceedings*, volume 7712, pages 43–55. Springer, 2012.

[64] Murilo Coutinho and T. C. Souza Neto. New Multi-bit Differentials to Improve Attacks Against ChaCha. *IACR Cryptol. ePrint Arch.*, 2020:350, 2020.

[65] Murilo Coutinho and T. C. Souza Neto. Improved Linear Approximations to ARX Ciphers and Attacks Against ChaCha. *IACR Cryptol. ePrint Arch.*, page 224, 2021.

[66] Murilo Coutinho and Tertuliano C. Souza Neto. Improved Linear Approximations to

ARX Ciphers and Attacks Against ChaCha. In Anne Canteaut and François-Xavier Standaert, editors, *Advances in Cryptology - EUROCRYPT 2021 - 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17-21, 2021, Proceedings, Part I*, volume 12696 of *Lecture Notes in Computer Science*, pages 711–740. Springer, 2021.

[67] Cryptographic Engineering Research Group at George Mason University. ATHENa: Automated Tools for Hardware EvaluatioN. https://cryptography.gmu.edu/athena/.

[68] CRYPTREC Lightweight Cryptography Working Group. CRYPTREC Cryptographic Technology Guideline (Lightweight Cryptography) (Document ID: CRYPTREC GL-2003-2016EN), 2017. https://www.cryptrec.go.jp/report/cryptrec-gl-2003-2016en.pdf.

[69] CRYPTREC 軽量暗号ワーキンググループ. CRYPTREC 暗号技術ガイドライン（軽量暗号）（文書番号：CRYPTREC GL-2003-2016JP）, 2017. https://www.cryptrec.go.jp/report/cryptrec-gl-2003-2016jp.pdf.

[70] Joan Daemen. Permutation-based encryption, authentication and authenticated encryption. DIAC - Directions in Authenticated Ciphers, 2012. http://hyperelliptic.org/DIAC/.

[71] Deepak Kumar Dalai, Subhamoy Maitra, Santu Pal, and Dibyendu Roy. Distinguisher and non-randomness of Grain-v1 for 112, 114 and 116 initialisation rounds with multiple-bit difference in IVs. *IET Inf. Secur.*, 13(6):603–613, 2019.

[72] Deepak Kumar Dalai and Santu Pal. Recovering Internal States of Grain-v1. In Swee-Huay Heng and Javier López, editors, *Information Security Practice and Experience - 15th International Conference, ISPEC 2019, Kuala Lumpur, Malaysia, November 26-28, 2019, Proceedings*, volume 11879 of *Lecture Notes in Computer Science*, pages 325–337. Springer, 2019.

[73] T A Darumaya and B H Susanti. Forgery Attack on LightMAC Hash Function Scheme using SIMECK 32/64 Lightweight Block Cipher. *IOP Conference Series: Materials Science and Engineering*, 453:012014, nov 2018.

[74] Nilanjan Datta, Atul Luykx, Bart Mennink, and Mridul Nandi. Understanding RUP Integrity of COLM. *IACR Trans. Symmetric Cryptol.*, 2017(2):143–161, 2017.

[75] Kakumani K. C. Deepthi and Kunwar Singh. Cryptanalysis for reduced round Salsa and ChaCha: revisited. *IET Inf. Secur.*, 13(6):591–602, 2019.

[76] Stephanie Delaune, Patrick Derbez, Arthur Gontier, and Charles Prudhomme. A Simpler Model for Recovering Superpoly on Trivium. *IACR Cryptol. ePrint Arch.*, 2021:1191, 2021. (accepted on *Selected Areas in Cryptography - 28th International Workshop, SAC 2021*).

[77] Patrick Derbez and Pierre-Alain Fouque. Automatic Search of Meet-in-the-Middle and

Impossible Differential Attacks. In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part II*, volume 9815 of *Lecture Notes in Computer Science*, pages 157–184. Springer, 2016.

[78] Patrick Derbez and Léo Perrin. Meet-in-the-middle attacks and structural analysis of round-reduced PRINCE. In Gregor Leander, editor, *Fast Software Encryption - 22nd International Workshop, FSE 2015, Istanbul, Turkey, March 8-11, 2015, Revised Selected Papers*, volume 9054 of *Lecture Notes in Computer Science*, pages 190–216. Springer, 2015.

[79] Patrick Derbez and Léo Perrin. Meet-in-the-Middle Attacks and Structural Analysis of Round-Reduced PRINCE. *J. Cryptol.*, 33(3):1184–1215, 2020.

[80] Sabyasachi Dey and Santanu Sarkar. Improved analysis for reduced round Salsa and Chacha. *Discret. Appl. Math.*, 227:58–69, 2017.

[81] Sabyasachi Dey and Santanu Sarkar. Proving the biases of Salsa and ChaCha in differential attack. *Des. Codes Cryptogr.*, 88(9):1827–1856, 2020.

[82] Sabyasachi Dey and Santanu Sarkar. A theoretical investigation on the distinguishers of Salsa and ChaCha. *Discret. Appl. Math.*, 302:147–162, 2021.

[83] Lin Ding, Dawu Gu, and Lei Wang. New Key Recovery Attack on the MICKEY Family of Stream Ciphers. In Bazhong Shen, Baocang Wang, Jinguang Han, and Yong Yu, editors, *International Conference on Frontiers in Cyber Security - FCS 2019*, volume 1105 of *Communications in Computer and Information Science*, pages 239–249. Springer, 2019.

[84] Lin Ding and Jie Guan. Cryptanalysis of MICKEY family of stream ciphers. *Secur. Commun. Networks*, 6(8):936–941, 2013.

[85] Lin Ding, Chenhui Jin, and Jie Guan. Slide attack on standard stream cipher Enocoro-80 in the related-key chosen IV setting. *Pervasive Mob. Comput.*, 24:224–230, 2015.

[86] Lin Ding, Chenhui Jin, Jie Guan, and Chuanda Qi. New Treatment of the BSW Sampling and Its Applications to Stream Ciphers. In David Pointcheval and Damien Vergnaud, editors, *Progress in Cryptology - AFRICACRYPT 2014 - 7th International Conference on Cryptology in Africa, Marrakesh, Morocco, May 28-30, 2014. Proceedings*, volume 8469 of *Lecture Notes in Computer Science*, pages 136–146. Springer, 2014.

[87] Lin Ding, Lei Wang, Dawu Gu, Chenhui Jin, and Jie Guan. Algebraic Degree Estimation of ACORN v3 Using Numeric Mapping. *Secur. Commun. Networks*, 2019:7429320:1–7429320:5, 2019.

[88] Itai Dinur. Improved Differential Cryptanalysis of Round-Reduced Speck. In Antoine Joux and Amr M. Youssef, editors, *Selected Areas in Cryptography - SAC 2014 - 21st International Conference, Montreal, QC, Canada, August 14-15, 2014, Revised Selected*

Papers, volume 8781 of *Lecture Notes in Computer Science*, pages 147–164. Springer, 2014.

[89] Itai Dinur, Orr Dunkelman, Nathan Keller, and Adi Shamir. Key Recovery Attacks on 3-round Even-Mansour, 8-step LED-128, and Full AES2. In Kazue Sako and Palash Sarkar, editors, *Advances in Cryptology - ASIACRYPT 2013 - 19th International Conference on the Theory and Application of Cryptology and Information Security, Bengaluru, India, December 1-5, 2013, Proceedings, Part I*, volume 8269 of *Lecture Notes in Computer Science*, pages 337–356. Springer, 2013.

[90] Itai Dinur, Orr Dunkelman, Nathan Keller, and Adi Shamir. Improved Linear Sieving Techniques with Applications to Step-Reduced LED-64. In Carlos Cid and Christian Rechberger, editors, *Fast Software Encryption - 21st International Workshop, FSE 2014, London, UK, March 3-5, 2014. Revised Selected Papers*, volume 8540 of *Lecture Notes in Computer Science*, pages 390–410. Springer, 2014.

[91] Itai Dinur, Orr Dunkelman, and Adi Shamir. Collision Attacks on Up to 5 Rounds of SHA-3 Using Generalized Internal Differentials. In Shiho Moriai, editor, *Fast Software Encryption - 20th International Workshop, FSE 2013, Singapore, March 11-13, 2013. Revised Selected Papers*, volume 8424 of *Lecture Notes in Computer Science*, pages 219–240. Springer, 2013.

[92] Itai Dinur and Adi Shamir. Breaking grain-128 with dynamic cube attacks. In Antoine Joux, editor, *Fast Software Encryption - 18th International Workshop, FSE 2011, Lyngby, Denmark, February 13-16, 2011, Revised Selected Papers*, volume 6733 of *Lecture Notes in Computer Science*, pages 167–187. Springer, 2011.

[93] Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer. Cryptanalysis of Ascon. In Kaisa Nyberg, editor, *Topics in Cryptology - CT-RSA 2015, The Cryptographer's Track at the RSA Conference 2015, San Francisco, CA, USA, April 20-24, 2015. Proceedings*, volume 9048 of *Lecture Notes in Computer Science*, pages 371–387. Springer, 2015.

[94] Christoph Dobraunig, Florian Mendel, and Martin Schläffer. Differential Cryptanalysis of SipHash. In Antoine Joux and Amr M. Youssef, editors, *Selected Areas in Cryptography - SAC 2014 - 21st International Conference, Montreal, QC, Canada, August 14-15, 2014, Revised Selected Papers*, volume 8781 of *Lecture Notes in Computer Science*, pages 165–182. Springer, 2014.

[95] Xiaoyang Dong, Zheng Li, Xiaoyun Wang, and Ling Qin. Cube-like Attack on Round-Reduced Initialization of Ketje Sr. *IACR Trans. Symmetric Cryptol.*, 2017(1):259–280, 2017.

[96] Xiaoyang Dong, Lingyue Qin, Siwei Sun, and Xiaoyun Wang. Key Guessing Strategies for Linear Key-Schedule Algorithms in Rectangle Attacks. *IACR Cryptol. ePrint Arch.*,

2021:856, 2021.

[97] Xiaoyang Dong and Yanzhao Shen. Cryptanalysis of Reduced-Round Midori64 Block Cipher. *IACR Cryptol. ePrint Arch.*, 2016:676, 2016.

[98] Orr Dunkelman, Nathan Keller, and Adi Shamir. Improved single-key attacks on 8-round AES-192 and AES-256. In Masayuki Abe, editor, *Advances in Cryptology - ASIACRYPT 2010 - 16th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 5-9, 2010. Proceedings*, volume 6477 of *Lecture Notes in Computer Science*, pages 158–176. Springer, 2010.

[99] Orr Dunkelman, Nathan Keller, and Adi Shamir. Improved single-key attacks on 8-round AES-192 and AES-256. *J. Cryptol.*, 28(3):397–422, 2015.

[100] Ashutosh Dhar Dwivedi and Gautam Srivastava. Differential Cryptanalysis of Round-Reduced LEA. *IEEE Access*, 6:79105–79113, 2018.

[101] Maria Eichlseder, Marcel Nageler, and Robert Primas. Analyzing the Linear Keystream Biases in AEGIS. *IACR Trans. Symmetric Cryptol.*, 2019(4):348–368, 2019.

[102] Antonio Flórez-Gutiérrez and María Naya-Plasencia. Improving Key-Recovery in Linear Attacks: Application to 28-Round PRESENT. In Anne Canteaut and Yuval Ishai, editors, *Advances in Cryptology - EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10-14, 2020, Proceedings, Part I*, volume 12105 of *Lecture Notes in Computer Science*, pages 221–249. Springer, 2020.

[103] Pierre-Alain Fouque and Thomas Vannet. Improving Key Recovery to 784 and 799 Rounds of Trivium Using Optimized Cube Attacks. In Shiho Moriai, editor, *Fast Software Encryption - 20th International Workshop, FSE 2013, Singapore, March 11-13, 2013. Revised Selected Papers*, volume 8424 of *Lecture Notes in Computer Science*, pages 502–517. Springer, 2013.

[104] Kai Fu, Meiqin Wang, Yinghua Guo, Siwei Sun, and Lei Hu. MILP-Based Automatic Search Algorithms for Differential and Linear Trails for Speck. In Thomas Peyrin, editor, *Fast Software Encryption - 23rd International Conference, FSE 2016, Bochum, Germany, March 20-23, 2016, Revised Selected Papers*, volume 9783 of *Lecture Notes in Computer Science*, pages 268–288. Springer, 2016.

[105] Ximing Fu, Xiaoyun Wang, Xiaoyang Dong, and Willi Meier. A Key-Recovery Attack on 855-round Trivium. In Hovav Shacham and Alexandra Boldyreva, editors, *Advances in Cryptology - CRYPTO 2018 - 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2018, Proceedings, Part II*, volume 10992 of *Lecture Notes in Computer Science*, pages 160–184. Springer, 2018.

[106] Thomas Fuhr, María Naya-Plasencia, and Yann Rotella. State-Recovery Attacks on Modified Ketje Jr. *IACR Trans. Symmetric Cryptol.*, 2018(1):29–56, 2018.

[107] David Gérault and Pascal Lafourcade. Related-Key Cryptanalysis of Midori. In Orr Dunkelman and Somitra Kumar Sanadhya, editors, *Progress in Cryptology - INDOCRYPT 2016 - 17th International Conference on Cryptology in India, Kolkata, India, December 11-14, 2016, Proceedings*, volume 10095 of *Lecture Notes in Computer Science*, pages 287–304, 2016.

[108] David Gérault, Thomas Peyrin, and Quan Quan Tan. Exploring differential-based distinguishers and forgeries for ASCON. *IACR Cryptol. ePrint Arch.*, 2021:1103, 2021. accepted to *IACR Trans. Symmetric Cryptol., 2021(3)*.

[109] Aron Gohr. Improving Attacks on Round-Reduced Speck32/64 Using Deep Learning. In Alexandra Boldyreva and Daniele Micciancio, editors, *Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2019, Proceedings, Part II*, volume 11693 of *Lecture Notes in Computer Science*, pages 150–179. Springer, 2019.

[110] Lorenzo Grassi and Christian Rechberger. Practical Low Data-Complexity Subspace-Trail Cryptanalysis of Round-Reduced PRINCE. In Orr Dunkelman and Somitra Kumar Sanadhya, editors, *Progress in Cryptology - INDOCRYPT 2016 - 17th International Conference on Cryptology in India, Kolkata, India, December 11-14, 2016, Proceedings*, volume 10095 of *Lecture Notes in Computer Science*, pages 322–342, 2016.

[111] Jian Guo, Jérémy Jean, Ivica Nikolic, Kexin Qiao, Yu Sasaki, and Siang Meng Sim. Invariant Subspace Attack Against Midori64 and The Resistance Criteria for S-box Designs. *IACR Trans. Symmetric Cryptol.*, 2016(1):33–56, 2016.

[112] Jian Guo, Jérémy Jean, Ivica Nikolic, Yu Sasaki, and Siang Meng Sim. Invariant Subspace Attack Against Midori64 and The Resistance Criteria for S-box Designs. *IACR Cryptol. ePrint Arch.*, 2016:973, 2016.

[113] Jian Guo, Guohong Liao, Guozhen Liu, Meicheng Liu, Kexin Qiao, and Ling Song. Practical Collision Attacks against Round-Reduced SHA-3. *J. Cryptol.*, 33(1):228–270, 2020.

[114] Jian Guo, Thomas Peyrin, and Axel Poschmann. The PHOTON Family of Lightweight Hash Functions. In Phillip Rogaway, editor, *Advances in Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings*, volume 6841 of *Lecture Notes in Computer Science*, pages 222–239. Springer, 2011.

[115] Zhiyuan Guo, Wenling Wu, Renzhang Liu, and Liting Zhang. Multi-key Analysis of Tweakable Even-Mansour with Applications to Minalpher and OPP. *IACR Trans. Symmetric Cryptol.*, 2016(2):288–306, 2016.

[116] Guoyong Han and Wenying Zhang. Improved Biclique Cryptanalysis of the Lightweight Block Cipher Piccolo. *Secur. Commun. Networks*, 2017:7589306:1–7589306:12, 2017.

[117] Guoyong Han, Wenying Zhang, Zhaohui Xing, Hongluan Zhao, and Jian Lian. Unbalanced biclique cryptanalysis of a full round Midori. *IET Commun.*, 13(5):505–511, 2019.

[118] Yonglin Hao, Takanori Isobe, Lin Jiao, Chaoyun Li, Willi Meier, Yosuke Todo, and Qingju Wang. Improved Division Property Based Cube Attacks Exploiting Algebraic Properties of Superpoly. *IEEE Trans. Computers*, 68(10):1470–1486, 2019.

[119] Yonglin Hao, Lin Jiao, Chaoyun Li, Willi Meier, Yosuke Todo, and Qingju Wang. Links between Division Property and Other Cube Attack Variants. *IACR Trans. Symmetric Cryptol.*, 2020(1):363–395, 2020.

[120] Yonglin Hao, Gregor Leander, Willi Meier, Yosuke Todo, and Qingju Wang. Modeling for Three-Subset Division Property Without Unknown Subset - Improved Cube Attacks Against Trivium and Grain-128AEAD. In Anne Canteaut and Yuval Ishai, editors, *Advances in Cryptology - EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10-14, 2020, Proceedings, Part I*, volume 12105 of *Lecture Notes in Computer Science*, pages 466–495. Springer, 2020.

[121] Yonglin Hao, Gregor Leander, Willi Meier, Yosuke Todo, and Qingju Wang. Modeling for Three-Subset Division Property without Unknown Subset. *J. Cryptol.*, 34(3):22, 2021.

[122] Yonglin Hao and Willi Meier. Truncated differential based known-key attacks on round-reduced SIMON. *Des. Codes Cryptogr.*, 83(2):467–492, 2017.

[123] Le He, Xiaoen Lin, and Hongbo Yu. Improved Preimage Attacks on 4-Round Keccak-224/256. *IACR Trans. Symmetric Cryptol.*, 2021(1):217–238, 2021.

[124] Tor Helleseth, Cees J. A. Jansen, Oleksandr Kazymyrov, and Alexander Kholosha. State space cryptanalysis of the MICKEY cipher. In *2013 Information Theory and Applications Workshop, ITA 2013, San Diego, CA, USA, February 10-15, 2013*, pages 1–10. IEEE, 2013.

[125] Shoichi Hirose, Kota Ideguchi, Hidenori Kuwakado, Toru Owada, Bart Preneel, and Hirotaka Yoshida. A Lightweight 256-Bit Hash Function for Hardware and Low-End Devices: Lesamnta-LW. In Kyung Hyune Rhee and DaeHun Nyang, editors, *Information Security and Cryptology - ICISC 2010 - 13th International Conference, Seoul, Korea, December 1-3, 2010, Revised Selected Papers*, volume 6829 of *Lecture Notes in Computer Science*, pages 151–168. Springer, 2010.

[126] Shoichi Hirose, Kota Ideguchi, Hidenori Kuwakado, Toru Owada, Bart Preneel, and Hirotaka Yoshida. An AES Based 256-bit Hash Function for Lightweight Applications: Lesamnta-LW. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, 95-A(1):89–99, 2012.

[127] Shoichi Hirose, Yu Sasaki, and Kan Yasuda. Rate-One AE with Security Under RUP. In Phong Q. Nguyen and Jianying Zhou, editors, *Information Security - 20th International Conference, ISC 2017, Ho Chi Minh City, Vietnam, November 22-24, 2017, Proceedings*, volume 10599 of *Lecture Notes in Computer Science*, pages 3–20. Springer, 2017.

[128] Shoichi Hirose, Yu Sasaki, and Hirotaka Yoshida. Lesamnta-LW Revisited: Improved Security Analysis of Primitive and New PRF Mode. In Mauro Conti, Jianying Zhou, Emiliano Casalicchio, and Angelo Spognardi, editors, *Applied Cryptography and Network Security - 18th International Conference, ACNS 2020, Rome, Italy, October 19-22, 2020, Proceedings, Part I*, volume 12146 of *Lecture Notes in Computer Science*, pages 89–109. Springer, 2020.

[129] Deukjo Hong, Jung-Keun Lee, Dong-Chan Kim, Daesung Kwon, Kwon Ho Ryu, and Donggeon Lee. LEA: A 128-Bit Block Cipher for Fast Encryption on Common Processors. In Yongdae Kim, Heejo Lee, and Adrian Perrig, editors, *Information Security Applications - 14th International Workshop, WISA 2013, Jeju Island, Korea, August 19-21, 2013, Revised Selected Papers*, volume 8267 of *Lecture Notes in Computer Science*, pages 3–27. Springer, 2013.

[130] Jin Hong and Woo-Hwan Kim. TMD-Tradeoff and State Entropy Loss Considerations of Streamcipher MICKEY. In Subhamoy Maitra, C. E. Veni Madhavan, and Ramarathnam Venkatesan, editors, *Progress in Cryptology - INDOCRYPT 2005, 6th International Conference on Cryptology in India, Bangalore, India, December 10-12, 2005, Proceedings*, volume 3797 of *Lecture Notes in Computer Science*, pages 169–182. Springer, 2005.

[131] Zezhou Hou, Jiongjiong Ren, and Shaozhen Chen. Cryptanalysis of Round-Reduced SIMON32 Based on Deep Learning. *IACR Cryptol. ePrint Arch.*, 2021:362, 2021.

[132] Zezhou Hou, Jiongjiong Ren, and Shaozhen Chen. Improve Neural Distinguisher for Cryptanalysis. *IACR Cryptol. ePrint Arch.*, 2021:1017, 2021.

[133] Zezhou Hou, Jiongjiong Ren, and Shaozhen Chen. SAT-based Method to Improve Neural Distinguisher and Applications to SIMON. *IACR Cryptol. ePrint Arch.*, 2021:452, 2021.

[134] Kai Hu, Siwei Sun, Yosuke Todo, Meiqin Wang, and Qingju Wang. Massive Superpoly Recovery with Nested Monomial Predictions. *IACR Cryptol. ePrint Arch.*, 2021:1225, 2021. (accepted on *Advances in Cryptology - ASIACRYPT 2021 - 27th International Conference on the Theory and Application of Cryptology and Information Security)*.

[135] Kai Hu, Siwei Sun, Meiqin Wang, and Qingju Wang. An Algebraic Formulation of the Division Property: Revisiting Degree Evaluations, Cube Attacks, and Key-Independent Sums. In Shiho Moriai and Huaxiong Wang, editors, *Advances in Cryptology - ASIACRYPT 2020 - 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7-11, 2020, Proceedings, Part I*, volume 12491 of *Lecture Notes in Computer Science*, pages 446–476.

Springer, 2020.

[136] Mingjiang Huang and Liming Wang. Automatic Tool for Searching for Differential Characteristics in ARX Ciphers and Applications. In Feng Hao, Sushmita Ruj, and Sourav Sen Gupta, editors, *Progress in Cryptology - INDOCRYPT 2019 - 20th International Conference on Cryptology in India, Hyderabad, India, December 15-18, 2019, Proceedings*, volume 11898 of *Lecture Notes in Computer Science*, pages 115–138. Springer, 2019.

[137] Mingjiang Huang and Liming Wang. Automatic Search for the Linear (Hull) Characteristics of ARX Ciphers: Applied to SPECK, SPARX, Chaskey, and CHAM-64. *Secur. Commun. Networks*, 2020:4898612:1–4898612:14, 2020.

[138] Akiko Inoue, Tetsu Iwata, Kazuhiko Minematsu, and Bertram Poettering. Cryptanalysis of OCB2: Attacks on Authenticity and Confidentiality. In Alexandra Boldyreva and Daniele Micciancio, editors, *Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2019, Proceedings, Part I*, volume 11692 of *Lecture Notes in Computer Science*, pages 3–31. Springer, 2019.

[139] Akiko Inoue, Tetsu Iwata, Kazuhiko Minematsu, and Bertram Poettering. Cryptanalysis of OCB2: Attacks on Authenticity and Confidentiality. *J. Cryptol.*, 33(4):1871–1913, 2020.

[140] Takanori Isobe and Kyoji Shibutani. Security Analysis of the Lightweight Block Ciphers XTEA, LED and Piccolo. In Willy Susilo, Yi Mu, and Jennifer Seberry, editors, *Information Security and Privacy - 17th Australasian Conference, ACISP 2012, Wollongong, NSW, Australia, July 9-11, 2012. Proceedings*, volume 7372 of *Lecture Notes in Computer Science*, pages 71–86. Springer, 2012.

[141] Jérémy Jean, María Naya-Plasencia, and Thomas Peyrin. Improved Rebound Attack on the Finalist Grøstl. In Anne Canteaut, editor, *Fast Software Encryption - 19th International Workshop, FSE 2012, Washington, DC, USA, March 19-21, 2012. Revised Selected Papers*, volume 7549 of *Lecture Notes in Computer Science*, pages 110–126. Springer, 2012.

[142] Jérémy Jean, Ivica Nikolic, Thomas Peyrin, Lei Wang, and Shuang Wu. Security Analysis of PRINCE. In Shiho Moriai, editor, *Fast Software Encryption - 20th International Workshop, FSE 2013, Singapore, March 11-13, 2013. Revised Selected Papers*, volume 8424 of *Lecture Notes in Computer Science*, pages 92–111. Springer, 2013.

[143] Kitae Jeong, HyungChul Kang, Changhoon Lee, Jaechul Sung, and Seokhie Hong. Biclique Cryptanalysis of Lightweight Block Ciphers PRESENT, Piccolo and LED. *IACR Cryptol. ePrint Arch.*, 2012:621, 2012.

[144] K. B. Jithendra and Shahana Thottathikkulam Kassim. New Biclique Cryptanalysis on

Full-Round PRESENT-80 Block Cipher. *SN Comput. Sci.*, 1(2):94, 2020.

[145] Philipp Jovanovic, Atul Luykx, Bart Mennink, Yu Sasaki, and Kan Yasuda. Beyond Conventional Security in Sponge-Based Authenticated Encryption Modes. *J. Cryptol.*, 32(3):895–940, 2019.

[146] Ferhat Karakoç, Hüseyin Demirci, and A. Emre Harmanci. Biclique cryptanalysis of LBlock and TWINE. *Inf. Process. Lett.*, 113(12):423–429, 2013.

[147] Abhishek Kesarwani, Dibyendu Roy, Santanu Sarkar, and Willi Meier. New cube distinguishers on NFSR-based stream ciphers. *Des. Codes Cryptogr.*, 88(1):173–199, 2020.

[148] Dongyeong Kim, Dawoon Kwon, and Junghwan Song. Efficient Computation of Boomerang Connection Probability for ARX-Based Block Ciphers with Application to SPECK and LEA. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, 103-A(4):677–685, 2020.

[149] Stefan Kölbl, Gregor Leander, and Tyge Tiessen. Observations on the SIMON Block Cipher Family. In Rosario Gennaro and Matthew Robshaw, editors, *Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part I*, volume 9215 of *Lecture Notes in Computer Science*, pages 161–185. Springer, 2015.

[150] Stefan Kölbl and Arnab Roy. A Brief Comparison of Simon and Simeck. In Andrey Bogdanov, editor, *Lightweight Cryptography for Security and Privacy - 5th International Workshop, LightSec 2016, Aksaray, Turkey, September 21-22, 2016, Revised Selected Papers*, volume 10098 of *Lecture Notes in Computer Science*, pages 69–88. Springer, 2016.

[151] Bonwook Koo, Younghoon Jung, and Woo-Hwan Kim. Rotational-XOR Rectangle Cryptanalysis on Round-Reduced Simon. *Secur. Commun. Networks*, 2020:5968584:1–5968584:12, 2020.

[152] Liliya Kraleva, Tomer Ashur, and Vincent Rijmen. Rotational Cryptanalysis on MAC Algorithm Chaskey. In Mauro Conti, Jianying Zhou, Emiliano Casalicchio, and Angelo Spognardi, editors, *Applied Cryptography and Network Security - 18th International Conference, ACNS 2020, Rome, Italy, October 19-22, 2020, Proceedings, Part I*, volume 12146 of *Lecture Notes in Computer Science*, pages 153–168. Springer, 2020.

[153] Ted Krovetz and Phillip Rogaway. The Software Performance of Authenticated-Encryption Modes. In Antoine Joux, editor, *Fast Software Encryption - 18th International Workshop, FSE 2011, Lyngby, Denmark, February 13-16, 2011, Revised Selected Papers*, volume 6733 of *Lecture Notes in Computer Science*, pages 306–327. Springer, 2011.

[154] Frédéric Lafitte, Liran Lerman, Olivier Markowitch, and Dirk Van Heule. SAT-based cryptanalysis of ACORN. *IACR Cryptol. ePrint Arch.*, 2016:521, 2016.

[155] Jung-Keun Lee, Bonwook Koo, and Woo-Hwan Kim. A General Framework for the Related-Key Linear Attack Against Block Ciphers with Linear Key Schedules. In Kenneth G. Paterson and Douglas Stebila, editors, *Selected Areas in Cryptography - SAC 2019 - 26th International Conference, Waterloo, ON, Canada, August 12-16, 2019, Revised Selected Papers*, volume 11959 of *Lecture Notes in Computer Science*, pages 194–224. Springer, 2019.

[156] Michael Lehmann and Willi Meier. Conditional Differential Cryptanalysis of Grain-128a. In Josef Pieprzyk, Ahmad-Reza Sadeghi, and Mark Manulis, editors, *Cryptology and Network Security, 11th International Conference, CANS 2012, Darmstadt, Germany, December 12-14, 2012. Proceedings*, volume 7712, pages 1–11. Springer, 2012.

[157] Gaëtan Leurent. Improved Differential-Linear Cryptanalysis of 7-Round Chaskey with Partitioning. In Marc Fischlin and Jean-Sébastien Coron, editors, *Advances in Cryptology - EUROCRYPT 2016 - 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, May 8-12, 2016, Proceedings, Part I*, volume 9665 of *Lecture Notes in Computer Science*, pages 344–371. Springer, 2016.

[158] Gaetan Leurent, Clara Pernot, and Andre Schrottenloher. Clustering Effect in Simon and Simeck. *IACR Cryptol. ePrint Arch.*, 2021:1198, 2021. (accepted on *Advances in Cryptology - ASIACRYPT 2021 - 27th International Conference on the Theory and Application of Cryptology and Information Security)*.

[159] Jun-Zhi Li and Jie Guan. Advanced conditional differential attack on Grain-like stream cipher and application on Grain v1. *IET Inf. Secur.*, 13(2):141–148, 2019.

[160] Junzhi Li and Jie Guan. Improved Conditional Differential Attacks on Round-Reduced Grain v1. *KSII Trans. Internet Inf. Syst.*, 12(9):4548–4559, 2018.

[161] Leibo Li, Keting Jia, and Xiaoyun Wang. Improved Meet-in-the-Middle Attacks on AES-192 and PRINCE. *IACR Cryptol. ePrint Arch.*, 2013:573, 2013.

[162] Leibo Li, Keting Jia, Xiaoyun Wang, and Xiaoyang Dong. Meet-in-the-Middle Technique for Truncated Differential and Its Applications to CLEFIA and Camellia. In Gregor Leander, editor, *Fast Software Encryption - 22nd International Workshop, FSE 2015, Istanbul, Turkey, March 8-11, 2015, Revised Selected Papers*, volume 9054 of *Lecture Notes in Computer Science*, pages 48–70. Springer, 2015.

[163] Manman Li and Shaozhen Chen. Improved meet-in-the-middle attacks on reduced-round Joltik-BC. *IET Information Security*, 15(3):247–255, 2021.

[164] Manman Li and Shaozhen Chen. Improved Meet-in-the-Middle Attacks on Reduced-Round Tweakable Block Cipher Deoxys-BC. *The Computer Journal*, 06 2021.

[165] Rongjia Li and Chenhui Jin. Meet-in-the-middle attacks on round-reduced tweakable block cipher Deoxys-BC. *IET Inf. Secur.*, 13(1):70–75, 2019.

[166] Rongjia Li, Chenhui Jin, and Hongchen Pan. Key recovery attacks on reduced-round Joltik-BC in the single-key setting. *Inf. Process. Lett.*, 151, 2019.

[167] Ting Li and Yao Sun. Preimage Attacks on Round-Reduced Keccak-224/256 via an Allocating Approach. In Yuval Ishai and Vincent Rijmen, editors, *Advances in Cryptology - EUROCRYPT 2019 - 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19-23, 2019, Proceedings, Part III*, volume 11478 of *Lecture Notes in Computer Science*, pages 556–584. Springer, 2019.

[168] Ting Li, Yao Sun, Maodong Liao, and Dingkang Wang. Preimage Attacks on the Round-reduced Keccak with Cross-linear Structures. *IACR Trans. Symmetric Cryptol.*, 2017(4):39–57, 2017.

[169] Yanbin Li, Guoyan Zhang, Wei Wang, and Meiqin Wang. Cryptanalysis of round-reduced ASCON. *Sci. China Inf. Sci.*, 60(3):38102, 2017.

[170] Yanjun Li, Wenling Wu, and Lei Zhang. Improved Integral Attacks on Reduced-Round CLEFIA Block Cipher. In Souhwan Jung and Moti Yung, editors, *Information Security Applications - 12th International Workshop, WISA 2011, Jeju Island, Korea, August 22-24, 2011. Revised Selected Papers*, volume 7115 of *Lecture Notes in Computer Science*, pages 28–39. Springer, 2011.

[171] Zheng Li, Xiaoyang Dong, Wenquan Bi, Keting Jia, Xiaoyun Wang, and Willi Meier. New Conditional Cube Attack on Keccak Keyed Modes. *IACR Trans. Symmetric Cryptol.*, 2019(2):94–124, 2019.

[172] Zheng Li, Xiaoyang Dong, and Xiaoyun Wang. Conditional Cube Attack on Round-Reduced ASCON. *IACR Trans. Symmetric Cryptol.*, 2017(1):175–202, 2017.

[173] Li Lin and Wenling Wu. Meet-in-the-Middle Attacks on Reduced-Round Midori-64. *IACR Cryptol. ePrint Arch.*, 2015:1165, 2015.

[174] Li Lin and Wenling Wu. Meet-in-the-Middle Attacks on Reduced-Round Midori64. *IACR Trans. Symmetric Cryptol.*, 2017(1):215–239, 2017.

[175] Li Lin, Wenling Wu, and Yafei Zheng. Automatic Search for Key-Bridging Technique: Applications to LBlock and TWINE. In Thomas Peyrin, editor, *Fast Software Encryption - 23rd International Conference, FSE 2016, Bochum, Germany, March 20-23, 2016, Revised Selected Papers*, volume 9783 of *Lecture Notes in Computer Science*, pages 247–267. Springer, 2016.

[176] Xiaoen Lin, Le He, and Hongbo Yu. Improved Preimage Attacks on 3-Round Keccak-224/256. *IACR Trans. Symmetric Cryptol.*, 2021(3):84–101, 2021.

[177] Moses D. Liskov, Ronald L. Rivest, and David A. Wagner. Tweakable Block Ciphers. In Moti Yung, editor, *Advances in Cryptology - CRYPTO 2002, 22nd Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 2002,*

Proceedings, volume 2442 of *Lecture Notes in Computer Science*, pages 31–46. Springer, 2002.

[178] Moses D. Liskov, Ronald L. Rivest, and David A. Wagner. Tweakable Block Ciphers. *J. Cryptol.*, 24(3):588–613, 2011.

[179] Fukang Liu, Takanori Isobe, Willi Meier, and Kosei Sakamoto. Weak Keys in Reduced AEGIS and Tiaoxin. *IACR Trans. Symmetric Cryptol.*, 2021(2):104–139, 2021.

[180] Guozhen Liu, Weidong Qiu, and Yi Tu. New Techniques for Searching Differential Trails in Keccak. *IACR Trans. Symmetric Cryptol.*, 2019(4):407–437, 2019.

[181] Meicheng Liu, Jingchun Yang, Wenhao Wang, and Dongdai Lin. Correlation Cube Attacks: From Weak-Key Distinguisher to Key Recovery. In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part II*, volume 10821 of *Lecture Notes in Computer Science*, pages 715–744. Springer, 2018.

[182] Ya Liu, Liang Cheng, Zhiqiang Liu, Wei Li, Qingju Wang, and Dawu Gu. Improved meet-in-the-middle attacks on reduced-round Piccolo. *Sci. China Inf. Sci.*, 61(3):032108:1–032108:13, 2018.

[183] Ya Liu, Bing Shi, Dawu Gu, Fengyu Zhao, Wei Li, and Zhiqiang Liu. Improved Meet-in-the-Middle Attacks on Reduced-Round Deoxys-BC-256. *Comput. J.*, 63(12):1859–1870, 2020.

[184] Ya Liu, Yifan Shi, Dawu Gu, Zhiqiang Zeng, Fengyu Zhao, Wei Li, Zhiqiang Liu, and Yang Bao. Improved Meet-in-the-Middle Attacks on Reduced-Round Kiasu-BC and Joltik-BC. *Comput. J.*, 62(12):1761–1776, 2019.

[185] Yunwen Liu, Siwei Sun, and Chao Li. Rotational Cryptanalysis from a Differential-Linear Perspective - Practical Distinguishers for Round-Reduced FRIET, Xoodoo, and Alzette. In Anne Canteaut and François-Xavier Standaert, editors, *Advances in Cryptology - EUROCRYPT 2021 - 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17-21, 2021, Proceedings, Part I*, volume 12696 of *Lecture Notes in Computer Science*, pages 741–770. Springer, 2021.

[186] Yunwen Liu, Qingju Wang, and Vincent Rijmen. Automatic Search of Linear Trails in ARX with Applications to SPECK and Chaskey. In Mark Manulis, Ahmad-Reza Sadeghi, and Steve A. Schneider, editors, *Applied Cryptography and Network Security - 14th International Conference, ACNS 2016, Guildford, UK, June 19-22, 2016. Proceedings*, volume 9696 of *Lecture Notes in Computer Science*, pages 485–499. Springer, 2016.

[187] Yunwen Liu, Glenn De Witte, Adrián Ranea, and Tomer Ashur. Rotational-XOR Crypt-

analysis of Reduced-round SPECK. *IACR Trans. Symmetric Cryptol.*, 2017(3):24–36, 2017.

[188] Zhengbin Liu, Yongqiang Li, Lin Jiao, and Mingsheng Wang. A New Method for Searching Optimal Differential and Linear Trails in ARX Ciphers. *IEEE Trans. Inf. Theory*, 67(2):1054–1068, 2021.

[189] Zhengbin Liu, Yongqiang Li, and Mingsheng Wang. Optimal Differential Trails in SIMON-like Ciphers. *IACR Trans. Symmetric Cryptol.*, 2017(1):358–379, 2017.

[190] Jinyu Lu, Yunwen Liu, Tomer Ashur, Bing Sun, and Chao Li. Rotational-XOR Cryptanalysis of Simon-Like Block Ciphers. In Joseph K. Liu and Hui Cui, editors, *Information Security and Privacy - 25th Australasian Conference, ACISP 2020, Perth, WA, Australia, November 30 - December 2, 2020, Proceedings*, volume 12248 of *Lecture Notes in Computer Science*, pages 105–124. Springer, 2020.

[191] Atul Luykx, Bart Preneel, Elmar Tischhauser, and Kan Yasuda. A MAC Mode for Lightweight Block Ciphers. In Thomas Peyrin, editor, *Fast Software Encryption - 23rd International Conference, FSE 2016, Bochum, Germany, March 20-23, 2016, Revised Selected Papers*, volume 9783 of *Lecture Notes in Computer Science*, pages 43–59. Springer, 2016.

[192] Zhen Ma, Tian Tian, and Wen-Feng Qi. Improved conditional differential attacks on Grain v1. *IET Inf. Secur.*, 11(1):46–53, 2017.

[193] Zhen Ma, Tian Tian, and Wen-Feng Qi. Internal state recovery of Grain v1 employing guess-and-determine attack. *IET Inf. Secur.*, 11(6):363–368, 2017.

[194] Zhen Ma, Tian Tian, and Wenfeng Qi. A New Distinguishing Attack on Grain-V1 with 111 Initialization Rounds. *J. Syst. Sci. Complex.*, 32(3):970–984, 2019.

[195] Subhamoy Maitra. Chosen IV cryptanalysis on reduced round ChaCha and Salsa. *Discret. Appl. Math.*, 208:88–97, 2016.

[196] Hamid Mala, Mohammad Dakhilalian, and Mohsen Shakiba. Impossible Differential Attacks on 13-Round CLEFIA-128. *J. Comput. Sci. Technol.*, 26(4):744–750, 2011.

[197] Shohreh Sharif Mansouri and Elena Dubrova.

[198] Chrysanthi Mavromati. Key-Recovery Attacks Against the MAC Algorithm Chaskey. In Orr Dunkelman and Liam Keliher, editors, *Selected Areas in Cryptography - SAC 2015 - 22nd International Conference, Sackville, NB, Canada, August 12-14, 2015, Revised Selected Papers*, volume 9566 of *Lecture Notes in Computer Science*, pages 205–216. Springer, 2015.

[199] Alexander Maximov and Alex Biryukov. Two Trivial Attacks on Trivium. In Carlisle M. Adams, Ali Miri, and Michael J. Wiener, editors, *Selected Areas in Cryptography, 14th International Workshop, SAC 2007, Ottawa, Canada, August 16-17, 2007, Revised Selected Papers*, volume 4876 of *Lecture Notes in Computer Science*, pages 36–55. Springer,

2007.

[200] Florian Mendel, Vincent Rijmen, Deniz Toz, and Kerem Varici. Differential Analysis of the LED Block Cipher. In Xiaoyun Wang and Kazue Sako, editors, *Advances in Cryptology - ASIACRYPT 2012 - 18th International Conference on the Theory and Application of Cryptology and Information Security, Beijing, China, December 2-6, 2012. Proceedings*, volume 7658 of *Lecture Notes in Computer Science*, pages 190–207. Springer, 2012.

[201] Brice Minaud. Linear Biases in AEGIS Keystream. In Antoine Joux and Amr M. Youssef, editors, *Selected Areas in Cryptography - SAC 2014 - 21st International Conference, Montreal, QC, Canada, August 14-15, 2014, Revised Selected Papers*, volume 8781 of *Lecture Notes in Computer Science*, pages 290–305. Springer, 2014.

[202] Marine Minier. On the Security of Piccolo Lightweight Block Cipher against Related-Key Impossible Differentials. In Goutam Paul and Serge Vaudenay, editors, *Progress in Cryptology - INDOCRYPT 2013 - 14th International Conference on Cryptology in India, Mumbai, India, December 7-10, 2013. Proceedings*, volume 8250 of *Lecture Notes in Computer Science*, pages 308–318. Springer, 2013.

[203] Shotaro Miyashita, Ryoma Ito, and Atsuko Miyaji. PNB-focused Differential Cryptanalysis of ChaCha Stream Cipher. *IACR Cryptol. ePrint Arch.*, 2021:1537, 2021.

[204] Farokhlagha Moazami, Alireza Mehrdad, and Hadi Soleimany. Impossible Differential Cryptanalysis on Deoxys-BC-256. *ISC Int. J. Inf. Secur.*, 10(2):93–105, 2018.

[205] Nicky Mouha. Chaskey: a MAC Algorithm for Microcontrollers - Status Update and Proposal of Chaskey-12 -. *IACR Cryptol. ePrint Arch.*, 2015:1182, 2015.

[206] Nicky Mouha. Review of the Advanced Encryption Standard. 2021.

[207] Nicky Mouha, Bart Mennink, Anthony Van Herrewege, Dai Watanabe, Bart Preneel, and Ingrid Verbauwhede. Chaskey: An Efficient MAC Algorithm for 32-bit Microcontrollers. In Antoine Joux and Amr M. Youssef, editors, *Selected Areas in Cryptography - SAC 2014 - 21st International Conference, Montreal, QC, Canada, August 14-15, 2014, Revised Selected Papers*, volume 8781 of *Lecture Notes in Computer Science*, pages 306–323. Springer, 2014.

[208] Nicky Mouha and Bart Preneel. Towards Finding Optimal Differential Characteristics for ARX: Application to Salsa20. *IACR Cryptol. ePrint Arch.*, 2013:328, 2013.

[209] Yusuke Naito. Blockcipher-Based MACs: Beyond the Birthday Bound Without Message Length. In Tsuyoshi Takagi and Thomas Peyrin, editors, *Advances in Cryptology - ASIACRYPT 2017 - 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part III*, volume 10626 of *Lecture Notes in Computer Science*, pages 446–470. Springer, 2017.

[210] Yusuke Naito. Improved Security Bound of LightMAC_Plus and Its Single-Key Variant.

In Nigel P. Smart, editor, *Topics in Cryptology - CT-RSA 2018 - The Cryptographers' Track at the RSA Conference 2018, San Francisco, CA, USA, April 16-20, 2018, Proceedings*, volume 10808 of *Lecture Notes in Computer Science*, pages 300–318. Springer, 2018.

[211] Seyed Reza Hoseini Najarkolaei, Mohammad Zare Ahangarkolaei, Siavash Ahmadi, and Mohammad Reza Aref. Biclique cryptanalysis of Twine-128. In *13th International Iranian Society of Cryptology Conference on Information Security and Cryptology, ISCISC 2016, Tehran, Iran, September 7-8, 2016*, pages 46–51. IEEE, 2016.

[212] Samuel Neves and Filipe Araújo. An observation on NORX, BLAKE2, and ChaCha. *Inf. Process. Lett.*, 149:1–5, 2019.

[213] Ivica Nikolic, Lei Wang, and Shuang Wu. Cryptanalysis of Round-Reduced LED. In Shiho Moriai, editor, *Fast Software Encryption - 20th International Workshop, FSE 2013, Singapore, March 11-13, 2013. Revised Selected Papers*, volume 8424 of *Lecture Notes in Computer Science*, pages 112–129. Springer, 2013.

[214] Chao Niu, Muzhou Li, Siwei Sun, and Meiqin Wang. Zero-Correlation Linear Cryptanalysis with Equal Treatment for Plaintexts and Tweakeys. In Kenneth G. Paterson, editor, *Topics in Cryptology - CT-RSA 2021 - Cryptographers' Track at the RSA Conference 2021, Virtual Event, May 17-20, 2021, Proceedings*, volume 12704 of *Lecture Notes in Computer Science*, pages 126–147. Springer, 2021.

[215] Senshan Pan, Yueping Wu, and Liangmin Wang. Optimizing Fast Near Collision Attack on Grain Using Linear Programming. *IEEE Access*, 7:181191–181201, 2019.

[216] Thomas Peyrin and Yannick Seurin. Counter-in-Tweak: Authenticated Encryption Modes for Tweakable Block Ciphers. In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part I*, volume 9814 of *Lecture Notes in Computer Science*, pages 33–63. Springer, 2016.

[217] Thomas Peyrin, Siang Meng Sim, Lei Wang, and Guoyan Zhang. Cryptanalysis of JAMBU. In Gregor Leander, editor, *Fast Software Encryption - 22nd International Workshop, FSE 2015, Istanbul, Turkey, March 8-11, 2015, Revised Selected Papers*, volume 9054 of *Lecture Notes in Computer Science*, pages 264–281. Springer, 2015.

[218] Kexin Qiao, Lei Hu, and Siwei Sun. Differential Analysis on Simeck and SIMON with Dynamic Key-Guessing Techniques. In Olivier Camp, Steven Furnell, and Paolo Mori, editors, *Information Systems Security and Privacy - Second International Conference, ICISSP 2016, Rome, Italy, February 19-21, 2016, Revised Selected Papers*, volume 691 of *Communications in Computer and Information Science*, pages 64–85. Springer, 2016.

[219] Kexin Qiao, Ling Song, Meicheng Liu, and Jian Guo. New Collision Attacks on Round-Reduced Keccak. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *Advances*

in Cryptology - EUROCRYPT 2017 - 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30 - May 4, 2017, Proceedings, Part III, volume 10212 of *Lecture Notes in Computer Science*, pages 216–243, 2017.

[220] Majid Rahimi, Mostafa Barmshory, Mohammad Hadi Mansouri, and Mohammad Reza Aref. Dynamic cube attack on Grain-v1. *IET Inf. Secur.*, 10(4):165–172, 2016.

[221] Mahesh Sreekumar Rajasree. Cryptanalysis of Round-Reduced KECCAK Using Non-linear Structures. In Feng Hao, Sushmita Ruj, and Sourav Sen Gupta, editors, *Progress in Cryptology - INDOCRYPT 2019 - 20th International Conference on Cryptology in India, Hyderabad, India, December 15-18, 2019, Proceedings*, volume 11898 of *Lecture Notes in Computer Science*, pages 175–192. Springer, 2019.

[222] Shahram Rasoolzadeh and Håvard Raddum. Cryptanalysis of PRINCE with Minimal Data. In David Pointcheval, Abderrahmane Nitaj, and Tajjeeddine Rachidi, editors, *Progress in Cryptology - AFRICACRYPT 2016 - 8th International Conference on Cryptology in Africa, Fes, Morocco, April 13-15, 2016, Proceedings*, volume 9646 of *Lecture Notes in Computer Science*, pages 109–126. Springer, 2016.

[223] Phillip Rogaway. Efficient Instantiations of Tweakable Blockciphers and Refinements to Modes OCB and PMAC. In Pil Joong Lee, editor, *Advances in Cryptology - ASIACRYPT 2004, 10th International Conference on the Theory and Application of Cryptology and Information Security, Jeju Island, Korea, December 5-9, 2004, Proceedings*, volume 3329 of *Lecture Notes in Computer Science*, pages 16–31. Springer, 2004.

[224] Phillip Rogaway, Mihir Bellare, and John Black. OCB: A block-cipher mode of operation for efficient authenticated encryption. *ACM Trans. Inf. Syst. Secur.*, 6(3):365–403, 2003.

[225] Phillip Rogaway, Mihir Bellare, John Black, and Ted Krovetz. OCB: a block-cipher mode of operation for efficient authenticated encryption. In Michael K. Reiter and Pierangela Samarati, editors, *CCS 2001, Proceedings of the 8th ACM Conference on Computer and Communications Security, Philadelphia, Pennsylvania, USA, November 6-8, 2001*, pages 196–205. ACM, 2001.

[226] Raghvendra Rohit and Guang Gong. Correlated Sequence Attack on Reduced-Round Simon-32/64 and Simeck-32/64. *IACR Cryptol. ePrint Arch.*, 2018:699, 2018.

[227] Raghvendra Rohit, Kai Hu, Sumanta Sarkar, and Siwei Sun. Misuse-Free Key-Recovery and Distinguishing Attacks on 7-Round Ascon. *IACR Trans. Symmetric Cryptol.*, 2021(1):130–155, 2021.

[228] Dibyendu Roy and Sourav Mukhopadhyay. Some results on ACORN. *IACR Cryptol. ePrint Arch.*, 2016:1132, 2016.

[229] Md. Iftekhar Salam, Harry Bartlett, Ed Dawson, Josef Pieprzyk, Leonie Simpson, and Kenneth Koon-Ho Wong. Investigating Cube Attacks on the Authenticated Encryp-

tion Stream Cipher ACORN. In Lynn Batten and Gang Li, editors, *Applications and Techniques in Information Security - 6th International Conference, ATIS 2016, Cairns, QLD, Australia, October 26-28, 2016, Proceedings*, volume 651 of *Communications in Computer and Information Science*, pages 15–26, 2016.

[230] Yu Sasaki. Improved Related-Tweakey Boomerang Attacks on Deoxys-BC. In Antoine Joux, Abderrahmane Nitaj, and Tajjeeddine Rachidi, editors, *Progress in Cryptology - AFRICACRYPT 2018 - 10th International Conference on Cryptology in Africa, Marrakesh, Morocco, May 7-9, 2018, Proceedings*, volume 10831 of *Lecture Notes in Computer Science*, pages 87–106. Springer, 2018.

[231] Yu Sasaki and Kazumaro Aoki. Improved Integral Analysis on Tweaked Lesamnta. In Howon Kim, editor, *Information Security and Cryptology - ICISC 2011 - 14th International Conference, Seoul, Korea, November 30 - December 2, 2011. Revised Selected Papers*, volume 7259 of *Lecture Notes in Computer Science*, pages 1–17. Springer, 2011.

[232] Yu Sasaki and Yosuke Todo. New Impossible Differential Search Tool from Design and Cryptanalysis Aspects - Revealing Structural Properties of Several Ciphers. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *Advances in Cryptology - EUROCRYPT 2017 - 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30 - May 4, 2017, Proceedings, Part III*, volume 10212 of *Lecture Notes in Computer Science*, pages 185–215, 2017.

[233] Zhenqing Shi, Bin Zhang, Dengguo Feng, and Wenling Wu. Improved Key Recovery Attacks on Reduced-Round Salsa20 and ChaCha. In Taekyoung Kwon, Mun-Kyu Lee, and Daesung Kwon, editors, *Information Security and Cryptology - ICISC 2012 - 15th International Conference, Seoul, Korea, November 28-30, 2012, Revised Selected Papers*, volume 7839 of *Lecture Notes in Computer Science*, pages 337–351. Springer, 2012.

[234] Rentaro Shiba, Kosei Sakamoto, Fukang Liu, Kazuhiko Minematsu, and Takanori Isobe. Integral and Impossible Differential Attacks on the Reduced-Round Lesamnta-LW-BC. In **暗号と情報セキュリティシンポジウム**, *SCIS2021, 1B1-2*, 2021.

[235] Kyoji Shibutani, Takanori Isobe, Harunaga Hiwatari, Atsushi Mitsuda, Toru Akishita, and Taizo Shirai. Piccolo: An Ultra-Lightweight Blockcipher. In Bart Preneel and Tsuyoshi Takagi, editors, *Cryptographic Hardware and Embedded Systems - CHES 2011 - 13th International Workshop, Nara, Japan, September 28 - October 1, 2011. Proceedings*, volume 6917 of *Lecture Notes in Computer Science*, pages 342–357. Springer, 2011.

[236] Hadi Soleimany. Probabilistic Slide Cryptanalysis and Its Applications to LED-64 and Zorro. In Carlos Cid and Christian Rechberger, editors, *Fast Software Encryption - 21st International Workshop, FSE 2014, London, UK, March 3-5, 2014. Revised Selected Papers*, volume 8540 of *Lecture Notes in Computer Science*, pages 373–389. Springer, 2014.

[237] Junghwan Song, Kwanhyung Lee, and HwanJin Lee. Biclique cryptanalysis on lightweight block cipher: HIGHT and Piccolo. *Int. J. Comput. Math.*, 90(12):2564–2580, 2013.

[238] Ling Song and Jian Guo. Cube-Attack-Like Cryptanalysis of Round-Reduced Keccak Using MILP. *IACR Trans. Symmetric Cryptol.*, 2018(3):182–214, 2018.

[239] Ling Song, Jian Guo, Danping Shi, and San Ling. New MILP Modeling: Improved Conditional Cube Attacks on Keccak-Based Constructions. In Thomas Peyrin and Steven D. Galbraith, editors, *Advances in Cryptology - ASIACRYPT 2018 - 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2-6, 2018, Proceedings, Part II*, volume 11273 of *Lecture Notes in Computer Science*, pages 65–95. Springer, 2018.

[240] Ling Song, Zhangjie Huang, and Qianqian Yang. Automatic Differential Analysis of ARX Block Ciphers with Application to SPECK and LEA. In Joseph K. Liu and Ron Steinfeld, editors, *Information Security and Privacy - 21st Australasian Conference, ACISP 2016, Melbourne, VIC, Australia, July 4-6, 2016, Proceedings, Part II*, volume 9723 of *Lecture Notes in Computer Science*, pages 379–394. Springer, 2016.

[241] Ling Song, Guohong Liao, and Jian Guo. Non-full Sbox Linearization: Applications to Collision Attacks on Round-Reduced Keccak. In Jonathan Katz and Hovav Shacham, editors, *Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part II*, volume 10402 of *Lecture Notes in Computer Science*, pages 428–451. Springer, 2017.

[242] Ling Sun, Wei Wang, and Meiqin Wang. Automatic Search of Bit-Based Division Property for ARX Ciphers and Word-Based Division Property. In Tsuyoshi Takagi and Thomas Peyrin, editors, *Advances in Cryptology - ASIACRYPT 2017 - 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part I*, volume 10624 of *Lecture Notes in Computer Science*, pages 128–157. Springer, 2017.

[243] Ling Sun, Wei Wang, and Meiqin Wang. More Accurate Differential Properties of LED64 and Midori64. *IACR Trans. Symmetric Cryptol.*, 2018(3):93–123, 2018.

[244] Ling Sun, Wei Wang, and Meiqin Wang. MILP-aided bit-based division property for primitives with non-bit-permutation linear layers. *IET Inf. Secur.*, 14(1):12–20, 2020.

[245] Ling Sun, Wei Wang, and Meiqin Wang. Accelerating the Search of Differential and Linear Characteristics with the SAT Method. *IACR Trans. Symmetric Cryptol.*, 2021(1):269–315, 2021.

[246] Yao Sun. Cube Attack against 843-Round Trivium. *IACR Cryptol. ePrint Arch.*, page 547, 2021.

[247] Sahiba Suryawanshi, Dhiman Saha, and Satyam Sachan. New Results on the SymSum

Distinguisher on Round-Reduced SHA3. In Abderrahmane Nitaj and Amr M. Youssef, editors, *Progress in Cryptology - AFRICACRYPT 2020 - 12th International Conference on Cryptology in Africa, Cairo, Egypt, July 20-22, 2020, Proceedings*, volume 12174 of *Lecture Notes in Computer Science*, pages 132–151. Springer, 2020.

[248] Tomoyasu Suzaki, Kazuhiko Minematsu, Sumio Morioka, and Eita Kobayashi. TWINE: A Lightweight Block Cipher for Multiple Platforms. In Lars R. Knudsen and Huapeng Wu, editors, *Selected Areas in Cryptography, 19th International Conference, SAC 2012, Windsor, ON, Canada, August 15-16, 2012, Revised Selected Papers*, volume 7707 of *Lecture Notes in Computer Science*, pages 339–354. Springer, 2012.

[249] Cihangir Tezcan. Truncated, Impossible, and Improbable Differential Analysis of ASCON. In Olivier Camp, Steven Furnell, and Paolo Mori, editors, *Proceedings of the 2nd International Conference on Information Systems Security and Privacy, ICISSP 2016, Rome, Italy, February 19-21, 2016*, pages 325–332. SciTePress, 2016.

[250] Cihangir Tezcan and Ali Aydin Selçuk. Improved improbable differential attacks on ISO standard CLEFIA: Expansion technique revisited. *Inf. Process. Lett.*, 116(2):136–143, 2016.

[251] Yosuke Todo, Takanori Isobe, Yonglin Hao, and Willi Meier. Cube Attacks on Non-Blackbox Polynomials Based on Division Property. In Jonathan Katz and Hovav Shacham, editors, *Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part III*, volume 10403 of *Lecture Notes in Computer Science*, pages 250–279. Springer, 2017.

[252] Yosuke Todo, Takanori Isobe, Yonglin Hao, and Willi Meier. Cube Attacks on Non-Blackbox Polynomials Based on Division Property. *IEEE Trans. Computers*, 67(12):1720–1736, 2018.

[253] Yosuke Todo, Takanori Isobe, Willi Meier, Kazumaro Aoki, and Bin Zhang. Fast Correlation Attack Revisited - Cryptanalysis on Full Grain-128a, Grain-128, and Grain-v1. In Hovav Shacham and Alexandra Boldyreva, editors, *Advances in Cryptology - CRYPTO 2018 - 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2018, Proceedings, Part II*, volume 10992 of *Lecture Notes in Computer Science*, pages 129–159. Springer, 2018.

[254] Yosuke Todo, Gregor Leander, and Yu Sasaki. Nonlinear Invariant Attack - Practical Attack on Full SCREAM, iSCREAM, and Midori64. In Jung Hee Cheon and Tsuyoshi Takagi, editors, *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 II*, volume 10032 of *Lecture Notes in Computer Science*, pages 3–33, 2016.

[255] Yosuke Todo, Gregor Leander, and Yu Sasaki. Nonlinear Invariant Attack: Practical

Attack on Full SCREAM, iSCREAM, and Midori64. *J. Cryptol.*, 32(4):1383–1422, 2019.

[256] Mohamed Tolba, Ahmed Abdelkhalek, and Amr M. Youssef. Meet-in-the-Middle Attacks on Reduced Round Piccolo. In Tim Güneysu, Gregor Leander, and Amir Moradi, editors, *Lightweight Cryptography for Security and Privacy - 4th International Workshop, LightSec 2015, Bochum, Germany, September 10-11, 2015, Revised Selected Papers*, volume 9542 of *Lecture Notes in Computer Science*, pages 3–20. Springer, 2015.

[257] Mohamed Tolba, Ahmed Abdelkhalek, and Amr M. Youssef. Truncated and Multiple Differential Cryptanalysis of Reduced Round Midori128. In Matt Bishop and Anderson C. A. Nascimento, editors, *Information Security - 19th International Conference, ISC 2016, Honolulu, HI, USA, September 3-6, 2016, Proceedings*, volume 9866 of *Lecture Notes in Computer Science*, pages 3–17. Springer, 2016.

[258] Mohamed Tolba and Amr M. Youssef. Generalized MitM attacks on full TWINE. *Inf. Process. Lett.*, 116(2):128–135, 2016.

[259] Gene Tsudik. Message Authentication with One-Way Hash Functions. In *Proceedings IEEE INFOCOM '92, The Conference on Computer Communications, Eleventh Annual Joint Conference of the IEEE Computer and Communications Societies, One World through Communications, Florence, Italy, May 4-8, 1992*, pages 2055–2059. IEEE Computer Society, 1992.

[260] Yukiyasu Tsunoo, Etsuko Tsujihara, Maki Shigeri, Teruo Saito, Tomoyasu Suzaki, and Hiroyasu Kubo. Impossible differential cryptanalysis of CLEFIA. In Kaisa Nyberg, editor, *Fast Software Encryption, 15th International Workshop, FSE 2008, Lausanne, Switzerland, February 10-13, 2008, Revised Selected Papers*, volume 5086 of *Lecture Notes in Computer Science*, pages 398–411. Springer, 2008.

[261] Damian Vizár. Ciphertext Forgery on HANUMAN. *IACR Cryptol. ePrint Arch.*, page 697, 2016.

[262] Gao Wang and Gaoli Wang. Improved Differential-ML Distinguisher: Machine Learning Based Generic Extension for Differential Analysis. In Debin Gao, Qi Li, Xiaohong Guan, and Xiaofeng Liao, editors, *Information and Communications Security - 23rd International Conference, ICICS 2021, Chongqing, China, November 19-21, 2021, Proceedings, Part II*, volume 12919 of *Lecture Notes in Computer Science*, pages 21–38. Springer, 2021.

[263] Geng Wang, Haiyang Zhang, and Fengmei Liu. Security Proof of JAMBU under Nonce Respecting and Nonce Misuse Cases. *IACR Cryptol. ePrint Arch.*, 2017:831, 2017.

[264] Ning Wang, Xiaoyun Wang, Keting Jia, and Jingyuan Zhao. Differential attacks on reduced SIMON versions with dynamic key-guessing techniques. *Sci. China Inf. Sci.*, 61(9):098103:1–098103:3, 2018.

[265] Qingju Wang, Lorenzo Grassi, and Christian Rechberger. Zero-Sum Partitions of PHO-

TON Permutations. *IACR Cryptol. ePrint Arch.*, 2017:1211, 2017.

[266] Qingju Wang, Lorenzo Grassi, and Christian Rechberger. Zero-Sum Partitions of PHOTON Permutations. In Nigel P. Smart, editor, *Topics in Cryptology - CT-RSA 2018 - The Cryptographers' Track at the RSA Conference 2018, San Francisco, CA, USA, April 16-20, 2018, Proceedings*, volume 10808 of *Lecture Notes in Computer Science*, pages 279–299. Springer, 2018.

[267] Qingju Wang, Yonglin Hao, Yosuke Todo, Chaoyun Li, Takanori Isobe, and Willi Meier. Improved Division Property Based Cube Attacks Exploiting Algebraic Properties of Superpoly. In Hovav Shacham and Alexandra Boldyreva, editors, *Advances in Cryptology - CRYPTO 2018 - 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2018, Proceedings, Part I*, volume 10991 of *Lecture Notes in Computer Science*, pages 275–305. Springer, 2018.

[268] Senpeng Wang, Bin Hu, Jie Guan, Kai Zhang, and Tairong Shi. MILP-aided Method of Searching Division Property Using Three Subsets and Applications. In Steven D. Galbraith and Shiho Moriai, editors, *Advances in Cryptology - ASIACRYPT 2019 - 25th International Conference on the Theory and Application of Cryptology and Information Security, Kobe, Japan, December 8-12, 2019, Proceedings, Part III*, volume 11923 of *Lecture Notes in Computer Science*, pages 398–427. Springer, 2019.

[269] Xuzi Wang, Baofeng Wu, Lin Hou, and Dongdai Lin. Automatic Search for Related-Key Differential Trails in SIMON-like Block Ciphers Based on MILP. In Liqun Chen, Mark Manulis, and Steve A. Schneider, editors, *Information Security - 21st International Conference, ISC 2018, Guildford, UK, September 9-12, 2018, Proceedings*, volume 11060 of *Lecture Notes in Computer Science*, pages 116–131. Springer, 2018.

[270] Yanfeng Wang and Wenling Wu. Improved Multidimensional Zero-Correlation Linear Cryptanalysis and Applications to LBlock and TWINE. In Willy Susilo and Yi Mu, editors, *Information Security and Privacy - 19th Australasian Conference, ACISP 2014, Wollongong, NSW, Australia, July 7-9, 2014. Proceedings*, volume 8544 of *Lecture Notes in Computer Science*, pages 1–16. Springer, 2014.

[271] Dai Watanabe, Toru Owada, Kazuto Okamoto, Yasutaka Igarashi, and Toshinobu Kaneko. Update on Enocoro stream cipher. In *Proceedings of the International Symposium on Information Theory and its Applications, ISITA 2010, 17-20 October 2010, Taichung, Taiwan*, pages 778–783. IEEE, 2010.

[272] Yuechuan Wei, Peng Xu, and Yisheng Rong. Related-key impossible differential cryptanalysis on lightweight cipher TWINE. *J. Ambient Intell. Humaniz. Comput.*, 10(2):509–517, 2019.

[273] Susila Windarta, Kalamullah Ramli, and Dodi Sudiana. Security Evaluation of LIGHT-MAC: Second Preimage Attack using Existential Forgery. In *2020 1st International*

Conference on Information Technology, Advanced Mechanical and Electrical Engineering (ICITAMEE), pages 265–269. IEEE, 2020.

[274] Hongjun Wu and Bart Preneel. AEGIS: A Fast Authenticated Encryption Algorithm. In Tanja Lange, Kristin E. Lauter, and Petr Lisonek, editors, *Selected Areas in Cryptography - SAC 2013 - 20th International Conference, Burnaby, BC, Canada, August 14-16, 2013, Revised Selected Papers*, volume 8282 of *Lecture Notes in Computer Science*, pages 185–201. Springer, 2013.

[275] Wenqian Xin, Yunwen Liu, Bing Sun, and Chao Li. Improved Cryptanalysis on SipHash. In Yi Mu, Robert H. Deng, and Xinyi Huang, editors, *Cryptology and Network Security - 18th International Conference, CANS 2019, Fuzhou, China, October 25-27, 2019, Proceedings*, volume 11829 of *Lecture Notes in Computer Science*, pages 61–79. Springer, 2019.

[276] Yaqi Xu, Baofeng Wu, and Dongdai Lin. Rotational-Linear Attack: A New Framework of Cryptanalysis on ARX Ciphers with Applications to Chaskey. In Debin Gao, Qi Li, Xiaohong Guan, and Xiaofeng Liao, editors, *Information and Communications Security - 23rd International Conference, ICICS 2021, Chongqing, China, November 19-21, 2021, Proceedings, Part II*, volume 12919 of *Lecture Notes in Computer Science*, pages 192–209. Springer, 2021.

[277] Jingchun Yang, Meicheng Liu, and Dongdai Lin. Cube Cryptanalysis of Round-Reduced ACORN. In Zhiqiang Lin, Charalampos Papamanthou, and Michalis Polychronakis, editors, *Information Security - 22nd International Conference, ISC 2019, New York City, NY, USA, September 16-18, 2019, Proceedings*, volume 11723 of *Lecture Notes in Computer Science*, pages 44–64. Springer, 2019.

[278] Jingchun Yang, Meicheng Liu, Dongdai Lin, and Wenhao Wang. Symbolic-Like Computation and Conditional Differential Cryptanalysis of QUARK. In Atsuo Inomata and Kan Yasuda, editors, *Advances in Information and Computer Security - 13th International Workshop on Security, IWSEC 2018, Sendai, Japan, September 3-5, 2018, Proceedings*, volume 11049 of *Lecture Notes in Computer Science*, pages 244–261. Springer, 2018.

[279] Chen-Dong Ye and Tian Tian. Revisit Division Property Based Cube Attacks: Key-Recovery or Distinguishing Attacks? *IACR Trans. Symmetric Cryptol.*, 2019(3):81–102, 2019.

[280] Wentan Yi, Baofeng Wu, Shaozhen Chen, and Dongdai Lin. Improved Integral and Zero-correlation Linear Cryptanalysis of CLEFIA Block Cipher. In Kefei Chen, Dongdai Lin, and Moti Yung, editors, *Information Security and Cryptology - 12th International Conference, Inscrypt 2016, Beijing, China, November 4-6, 2016, Revised Selected Papers*, volume 10143 of *Lecture Notes in Computer Science*, pages 33–46. Springer, 2016.

[281] Bin Zhang, Zhenqi Li, Dengguo Feng, and Dongdai Lin. Near Collision Attack on the

Grain v1 Stream Cipher. In Shiho Moriai, editor, *Fast Software Encryption - 20th International Workshop, FSE 2013, Singapore, March 11-13, 2013. Revised Selected Papers*, volume 8424 of *Lecture Notes in Computer Science*, pages 518–538. Springer, 2013.

[282] Bin Zhang, Chao Xu, and Willi Meier. Fast Near Collision Attack on the Grain v1 Stream Cipher. In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part II*, volume 10821 of *Lecture Notes in Computer Science*, pages 771–802. Springer, 2018.

[283] Guoyan Zhang and Meicheng Liu. A distinguisher on PRESENT-like permutations with application to SPONGENT. *Sci. China Inf. Sci.*, 60(7):72101, 2017.

[284] Kai Zhang, Jie Guan, and Xuliang Fei. Improved conditional differential cryptanalysis. *Secur. Commun. Networks*, 8(9):1801–1811, 2015.

[285] Ping Zhang, Peng Wang, Honggang Hu, Changsong Cheng, and Wenke Kuai. INT-RUP Security of Checksum-Based Authenticated Encryption. In Tatsuaki Okamoto, Yong Yu, Man Ho Au, and Yannan Li, editors, *Provable Security - 11th International Conference, ProvSec 2017, Xi'an, China, October 23-25, 2017, Proceedings*, volume 10592 of *Lecture Notes in Computer Science*, pages 147–166. Springer, 2017.

[286] Xiaojuan Zhang and Dongdai Lin. Cryptanalysis of Acorn in Nonce-Reuse Setting. In Xiaofeng Chen, Dongdai Lin, and Moti Yung, editors, *Information Security and Cryptology - 13th International Conference, Inscrypt 2017, Xi'an, China, November 3-5, 2017, Revised Selected Papers*, volume 10726 of *Lecture Notes in Computer Science*, pages 342–361. Springer, 2017.

[287] Boxin Zhao, Xiaoyang Dong, and Keting Jia. New Related-Tweakey Boomerang and Rectangle Attacks on Deoxys-BC Including BDT Effect. *IACR Trans. Symmetric Cryptol.*, 2019(3):121–151, 2019.

[288] Boxin Zhao, Xiaoyang Dong, Keting Jia, and Willi Meier. Improved Related-Tweakey Rectangle Attacks on Reduced-Round Deoxys-BC-384 and Deoxys-I-256-128. In Feng Hao, Sushmita Ruj, and Sourav Sen Gupta, editors, *Progress in Cryptology - INDOCRYPT 2019 - 20th International Conference on Cryptology in India, Hyderabad, India, December 15-18, 2019, Proceedings*, volume 11898 of *Lecture Notes in Computer Science*, pages 139–159. Springer, 2019.

[289] Hongluan Zhao and Guoyong Han. Biclique cryptanalysis on Midori block cipher. *Int. J. Embed. Syst.*, 11(2):229–239, 2019.

[290] Hongluan Zhao, Guoyong Han, Letian Wang, and Wen Wang. MILP-Based Differential Cryptanalysis on Round-Reduced Midori64. *IEEE Access*, 8:95888–95896, 2020.

[291] Zishen Zhao, Shiyao Chen, Meiqin Wang, and Wei Wang. Improved cube-attack-like cryptanalysis of reduced-round Ketje-Jr and Keccak-MAC. *Inf. Process. Lett.*, 171:106124, 2021.

[292] Lei Zheng and Shao-Wu Zhang. FFT-based multidimensional linear attack on PRESENT using the 2-bit-fixed characteristic. *Secur. Commun. Networks*, 8(18):3535–3545, 2015.

[293] Xuexin Zheng and Keting Jia. Impossible Differential Attack on Reduced-Round TWINE. In Hyang-Sook Lee and Dong-Guk Han, editors, *Information Security and Cryptology - ICISC 2013 - 16th International Conference, Seoul, Korea, November 27-29, 2013, Revised Selected Papers*, volume 8565 of *Lecture Notes in Computer Science*, pages 123–143. Springer, 2013.

[294] Rui Zong and Xiaoyang Dong. MILP-Aided Related-Tweak/Key Impossible Differential Attack and its Applications to QARMA, Joltik-BC. *IEEE Access*, 7:153683–153693, 2019.

[295] Rui Zong, Xiaoyang Dong, and Xiaoyun Wang. Collision Attacks on Round-Reduced Gimli-Hash/Ascon-Xof/Ascon-Hash. *IACR Cryptol. ePrint Arch.*, 2019:1115, 2019.

[296] Rui Zong, Xiaoyang Dong, and Xiaoyun Wang. Related-tweakey impossible differential attack on reduced-round Deoxys-BC-256. *Sci. China Inf. Sci.*, 62(3):32102:1–32102:12, 2019.

[297] 五十嵐保隆，岡本和人，金子敏信. 関連鍵攻撃による Enocoro の弱鍵復元の検討. In **電子情報通信学会技術研究報告**, *ISEC*, pages 275–280, 2010.

[298] 五十嵐 保隆，岡本 和人，金子 敏信. 関連鍵攻撃による Enocoro-128v1.1 の弱鍵復元の検討 (II). In **電子情報通信学会総合大会講演論文集**, 2010.

[299] 日本電信電話株式会社. NTT 持株会社ニュースリリース – IoT 向けメッセージ認証技術 LightMAC が ISO 標準に採択 –. https://www.ntt.co.jp/news2019/1910/191004a.html.

[300] 船引悠生，藤堂洋介，五十部孝典，森井昌克. Enocoro-128v2 の Cube 攻撃に対する安全性評価. In **暗号と情報セキュリティシンポジウム**, *SCIS2019, 2B1-1*, 2019.

[301] 芝山直喜，五十嵐保隆，金子敏信. ストリーム暗号 Enocoro-128v2 の高階差分特性. In **暗号と情報セキュリティシンポジウム**, *SCIS2021, 1B1-4*, 2021.

付録 A

本報告書のレビュー

2021 年度、暗号技術評価委員会の了承のもと、本報告書のレビューを日本電気株式会社の峯松一彦様にご担当いただいた。峯松様のレビューについては次頁以降を参照されたい。なお、レビューで頂いたコメントについては本報告書に全て反映済みである。

CRYPTREC 軽量暗号動向調査報告書に関するレビュー

峯松　一彦（日本電気株式会社）

2021 年 12 月 22 日

概要

本報告書は、CRYPTREC の活動内容の一つである「「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」（以下、軽量暗号動向調査報告書）についてその内容のレビューを行い、報告するものである。本報告書では軽量暗号動向調査報告書が対象とする範囲、安全性評価内容、および記述内容の妥当性をレビューしている。結果としていくつかの検討事項が挙げられるが、基本的な記述内容は妥当であるとの結論を得た。

1 はじめに

本報告書は CRYPTREC の活動内容の一つである「「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」（以下、軽量暗号動向調査報告書）についてその内容のレビューを行い、報告するものである。軽量暗号動向調査報告書では、2016 年度に策定した CRYPTREC 暗号技術ガイドライン（軽量暗号）に掲載された暗号方式、およびガイドライン出版時には掲載されなかったいくつかの軽量暗号方式について、最新の研究論文を元に安全性評価を行っている。本報告書では軽量暗号動向調査報告書が対象とする範囲、安全性評価内容、および記述内容の妥当性をレビューした。以下、章ごとに評価内容を記す。

2 軽量ブロック暗号の安全性評価

記載された評価対象の軽量ブロック暗号については妥当と考えられる。それらの安全性評価についてはいくつかの指摘事項を以下に記すが、基本的に次節で触れる Biclique 攻撃の扱いを除けば評価は妥当と考える。

2.1 Biclique 攻撃の評価について

軽量暗号動向調査報告書においては、攻撃の種類を単一鍵（Single-key）と関連鍵（Related-key）の二つのシナリオに分類し、それぞれアタック可能なラウンド数の最大値を達成した攻撃を最良の攻撃として記述している。この評価は直感的であり、また多くの論文で見受けられる流儀である一方、Biclique 攻撃を含んだ場合にも広く適用することについては、学術的なコンセンサスがあるとは言えないという状況である。例えば最初の Biclique 攻撃である Single-key AES への攻撃を AES への現時点の最良攻撃とすると、「AES は破られている」という端的な結論になるが、Bogdanov らの論文 [BKR11] 発表後 10 年を経ても、NIST は AES の安全性が危殆化したとはみなしていない模様である。NIST IR 8319 [Mou21] の該当箇所を引用する:

> Biclique attacks perform an exhaustive search over a reduced number of rounds of the cipher and can, therefore, only outperform exhaustive search over all rounds by a small constant factor. It is well known that slight improvements over exhaustive search are always possible (e.g., the “distributive technique” and “early abort technique” [11]); however, biclique attacks provide further speedups that do not apply to every block cipher. In NIST SP 800-57 Part 1, Revision 5 [2], “security strength” is defined in terms of the number of “operations” to break a cryptographic algorithm. If “operations” can be elementary operations rather than “full-round encryptions,” then biclique attacks do not affect the security strength of a cipher, as biclique attacks still perform exhaustive search over a reduced number of rounds.

このような見解に至る背景としては、Biclique 攻撃が本質的に鍵総当たりのコストを細かく改善するものであり、攻撃方法を発展させても大きな計算量削減が見込まれないという予想があるだろう。

例えば Tweak 付ブロック暗号の Skinny について設計者が攻撃のコンペティションを開催したとき [Pey16] には、Biclique 攻撃などの “accelerated brute force” 攻撃が示されたときにはそのほかの攻撃とは別の判断を行う、としている（そして実際に文献 [ZW16] では Skinny への Biclique 攻撃が示されている）。

以上の現状認識を元に考えると、Biclique 攻撃が提案された暗号に関してこれを一律に最良攻撃としてラベル付けを行うことは誤解を招く可能性があると考える。評価者の一案としては、Biclique および Biclique との類似性が論文中に述べられている攻撃（例えば文献 [RR16, TY16]）についてはその旨注記を行い、それらを除いた中から最大のアタック可能ラウンド数をもつ最良攻撃をリストする、などが考えられる[*1]。Biclique 攻撃には Single-key と Related-key 双方があり得るが、いずれも同様の注記が必要と考える。

なお Biclique 攻撃が実際に愚直な総当たり攻撃より速いのか否かという問題については、例えば文献 [BKP+12] が HW 実装、文献 [GS13] が SW 実装のケースなどを考え、いずれも高速化ができるという結論を得ている。

2.1.1 未記載の Biclique 攻撃

Piccolo については、軽量暗号動向調査報告書に未記載の （筆者が見る限り Single-key の） Biclique 攻撃を報告している論文 [HZ17] があった。

2.2 そのほかのコメント

- x が極めて小さいケースも「2^x 倍もの効率化に成功した」と表現しており、一律「2^x 倍の効率化に成功した」のほうが自然にみえる。
- 3.10.2 “LEA の全てのバリエーションに対し、秘密鍵の全数探索よりも効率的に鍵回復攻撃が実行できることを示した”はこの部分だけを見るとフルラウンド攻撃ができたように誤読されうる。
- 3.8.2 Speck への識別攻撃とそれによるフルラウンド鍵回復への言及は少し意味が読み取りづらい。識別攻撃の意味を少し補足したほうがよいように思われる。また、最後の Speck32,48,64 への言及「... 提案手法によって発見した新しい差分・線形特性を利用することで、Speck32/48/64 に対し、仕様段数であっても効率的に鍵回復攻撃が実行可能になりうることに注意されたい」についてはフルラウンド攻撃発見の可能性が高いということを伝えたいのか、意図が若干不明瞭であった。

3 軽量ストリーム暗号の安全性評価

全体を通して大きな指摘事項は見つからなく、評価候補の選定、安全性評価の内容ともに妥当と思われる。

3.1 そのほかのコメント

- Chacha の攻撃 [65] は ePrint/2021/224 の最新版を見ると 7 段攻撃が Time 2^{224}, Data 2^{224} の攻撃のみになっている。当初の内容から更新された模様。

4 軽量ハッシュ関数の安全性評価

「仕様段数において秘密鍵の全数探索よりも効率的に実行可能な攻撃は発表されていない」という表現がいくつかあるが、修正が必要と思われる。内部でブロック暗号を使っている場合なら解釈可能であるが、Keccak

[*1] もちろんこの方法も何をもって Biclique“らしい” 攻撃とするかで判断が分かれる可能性や、古典的な差分/線形攻撃などにおいてフルコードブックを使う場合などの扱いは変えなくてよいのか、などの議論の余地がある。

など暗号学的置換をベースとする場合は鍵入力がない。

4.1 そのほかのコメント

- 5.2 PHOTON について、識別攻撃は原則的にはハッシュ関数の必須安全性基準（衝突安全性、現像攻撃安全性）との直接的な関係がないため、注記が必要と思われる。5.3 QUARK, 5.4 SPONGENT の distinguisher にも同様のことが言えると思われる。
- 5.2.2 タイポ：ゼロサム攻撃（Zro-sum attack）

5 軽量 MAC の安全性評価

全体を通して大きな指摘事項は見つからなく、評価候補の選定、安全性評価の内容ともに妥当と思われる。

5.1 そのほかのコメント

- 6.2.2 Chaskey について、Mavromati [194] は、著者が述べているように少なくとも single-user mode はオリジナルの安全性証明バウンドとは矛盾しない。一方オリジナルでは Multi-user でのバウンドは示されていない。Mavromati の結果はバウンドのタイトネスを示す結果という解釈が可能である。
- 6.3.2 LightMAC について、Windarta [236] は MAC としての攻撃になっているか？（第 2 現像攻撃はハッシュ関数の安全性基準）
- 6.4.1 Tsudik's keymode については報告書にあるとおり提案論文以降の評価は特に発見できていないが、極めて古くシンプルなため何らかの外部評価が望まれるところである。

6 軽量認証暗号の安全性評価

全体を通して大きな指摘事項は見つからなく、評価候補の選定、安全性評価の内容ともに妥当と思われる。

6.1 そのほかのコメント

- 7.1.2 ACORN v3 の解析について、文献 [DWG+19] があった。短縮段（最長 721 段）での攻撃を示している。
- 7.6 Deoxys は Deoxys-II のみが CAESAR portfolio に選出されている（7.6.2 で触れられてはいるが冒頭で示しておくほうがよい）。
- 7.10 CAESAR に提案されたのは OCB3 [KR11] であるが、提案者は OCB という名前で提案している。

7 まとめ

軽量暗号動向調査報告書のいずれの章においても、調査範囲、調査内容、報告書の見解について、2.1 節に記した Biclique とその派生攻撃に関する扱いを除けば、大きな問題はなく、全般に見解は妥当と思われる。

参考文献

[BKP+12] Andrey Bogdanov, Elif Bilge Kavun, Christof Paar, Christian Rechberger, and Tolga Yalcin. Better than brute-force — optimized hardware architecture for efficient biclique attacks on aes-128. SHARCS, 2012.

[BKR11] Andrey Bogdanov, Dmitry Khovratovich, and Christian Rechberger. Biclique cryptanalysis of the full AES. In Dong Hoon Lee and Xiaoyun Wang, editors, *ASIACRYPT 2011*, volume 7073 of *LNCS*, pages 344–371. Springer, Heidelberg, December 2011.

[DWG+19] Lin Ding, Lei Wang, Dawu Gu, Chenhui Jin, and Jie Guan. Algebraic Degree Estimation of ACORN v3 Using Numeric Mapping. *Secur. Commun. Networks*, 2019:7429320:1–7429320:5, 2019.

[GS13] David Gstir and Martin Schläffer. Fast software encryption attacks on AES. In Amr Youssef, Abderrahmane Nitaj, and Aboul Ella Hassanien, editors, *AFRICACRYPT 13*, volume 7918 of *LNCS*, pages 359–374. Springer, Heidelberg, June 2013.

[HZ17] Guoyong Han and Wenying Zhang. Improved Biclique Cryptanalysis of the Lightweight Block Cipher Piccolo. *Secur. Commun. Networks*, 2017:7589306:1–7589306:12, 2017.

[KR11] Ted Krovetz and Phillip Rogaway. The software performance of authenticated-encryption modes. In Antoine Joux, editor, *FSE 2011*, volume 6733 of *LNCS*, pages 306–327. Springer, Heidelberg, February 2011.

[Mou21] Nicky Mouha. Review of the advanced encryption standard. NIST IR 8319, 2021.

[Pey16] Thomas Peyrin. The skinny family of tweakable block ciphers. Asian Symmetric-key Workshop (ASK), 2016.

[RR16] Shahram Rasoolzadeh and Håvard Raddum. Cryptanalysis of PRINCE with minimal data. In David Pointcheval, Abderrahmane Nitaj, and Tajjeeddine Rachidi, editors, *AFRICACRYPT 16*, volume 9646 of *LNCS*, pages 109–126. Springer, Heidelberg, April 2016.

[TY16] Mohamed Tolba and Amr M. Youssef. Generalized mitm attacks on full TWINE. *Inf. Process. Lett.*, 116(2):128–135, 2016.

[ZW16] Yafei Zheng and Wenling Wu. Biclique Attack of Block Cipher SKINNY. In *Inscrypt*, volume 10143 of *Lecture Notes in Computer Science*, pages 3–17. Springer, 2016.