CRYPTREC Report 2021

令和 4 年 3 月

国立研究開発法人情報通信研究機構
独立行政法人情報処理推進機構

CRYPTREC RP-2000-2021

「暗号技術評価委員会報告」

CRYPTREC Report 2021

暗号技術評価委員会報告書 目次

はじめに

本報告書は、デジタル庁、総務省及び経済産業省が主催する暗号技術検討会の下に設置され運営されている暗号技術評価委員会の 2021 年度活動報告書である。暗号技術評価委員会は、国立研究開発法人情報通信研究機構及び独立行政法人情報処理推進機構が共同で運営している。本委員会の 2021 年度の活動として、主に、1)暗号技術の安全性及び実装に係る監視及び評価、2)推奨候補暗号リストへの追加候補(事務局選出)となる暗号方式の実装評価、3)新しい暗号技術に係る調査および評価について暗号技術検討会より承認を得て実施した。

1)に関しては、多くの国際会議がオンラインで実施される中、国際会議等で発表される暗号の安全性及び実装に係る技術に関する監視を行い、CRYPTREC 暗号リストに掲載されている暗号の危殆化が進んでいないかどうかの判断を行った。2)に関しては、2020 年度に CRYPTREC 暗号リストに追加するための安全性要件を満たしていると判断した EdDSA(署名)に対して実装性能に関する調査及び評価を行い、暗号技術評価委員会としての見解をまとめ、暗号技術検討会に対して EdDSA の CRYPTREC 暗号リスト(推奨候補暗号リスト)への追加を提案した。また、3)に関しては、a)耐量子計算機暗号(Post-Quantum Cryptography)に関するガイドラインを作成するため、暗号技術調査ワーキンググループ(耐量子計算機暗号)を設置し、國廣昇先生に主査をご担当いただき、ガイドライン及びその根拠資料となる調査報告書の作成に関する方針をまとめ、ガイドラインの目次案を決定した。また、公開鍵暗号の安全性に直結する素因数分解の困難性に関する計算量評価や楕円曲線上の離散対数計算の困難性に関する計算量評価に関する予測図の更新を行った。次に、b)高機能暗号(Advanced Cryptography)に関するガイドラインを作成するため、暗号技術調査ワーキンググループ(高機能暗号)を設置し、四方順司先生に主査をご担当いただき、ガイドラインで扱う高機能暗号の定義を行うとともに、高機能暗号の分類やガイドラインに記載する高機能暗号の種類を整理し、ガイドラインの目次案を決定した。次に、c)軽量暗号に関するガイドラインを、2016 年度に公開した「CRYPTREC 暗号技術ガイドライン(軽量暗号)」を更新する形で作成するために、2017 年度以降の技術動向についてガイドラインに掲載されている暗号方式を中心に調査を行った。また、NIST Lightweight コンペティション最終選考で採択された方式及び軽量な方式として ISO に近年採録されたもしくは採録される予定の方式を追加対象として評価及び調査等を行うことを決定した。

2000 年に IT 基本法が制定されたほぼ同時期に発足して以来、22 年間にわたる CRYPTREC 活動は、安全・安心な ICT 社会の実現に貢献してきた。近年のコロナ禍で、テレワークや電子決済等、デジタル技術を積極的に利活用する状況が急速に進んできており、今後も様々な分野においてデジタル化を推進することが期待されている。その中で暗号技術に対する社会のニーズはかつてないほど大きくなっている。今後も、社会の情勢を踏まえ、健全なサイバー空間の実現・維持につなげるべく、暗号技術の安全性という観点から必要とされる活動を展開していきたい。暗号技術評価委員会の活動は暗号技術やその実装及び運用に携わる研究者及び技術者の献身的な協力により成り立っている。末筆ではあるが、本活動に様々な形でご協力頂いている関係者の皆様に深甚なる謝意を表する次第である。

暗号技術評価委員会　委員長　　高木 剛

本報告書の利用にあたって

本報告書の想定読者は、情報セキュリティの基礎知識を有している方である。たとえば、電子政府においてデジタル署名やデータの暗号化等の暗号関連のシステムに関係する業務についている方などを想定している。しかしながら、個別テーマの調査報告等を読むためには、ある程度の暗号技術の知識を備えていることが望まれる。

本報告書の第 1 章は暗号技術評価委員会の活動概要についての説明である。第 2 章は暗号技術評価委員会における監視活動に関する報告である。第 3 章は暗号技術評価委員会のもとで活動している暗号技術調査ワーキンググループの活動報告である。

本報告書の内容は、我が国最高水準の暗号専門家で構成される「暗号技術評価委員会」及びそのもとに設置された「暗号技術調査ワーキンググループ」において審議された結果であるが、暗号技術の特性から、その内容とりわけ安全性に関する事項は将来にわたって保証されたものではなく、今後とも継続して評価・監視活動を実施していくことが必要なものである。

本報告書ならびにこれまでに発行された CRYPTREC 報告書、技術報告書、CRYPTREC 暗号リスト記載の暗号技術の仕様書は、CRYPTREC 事務局（デジタル庁、総務省、経済産業省、国立研究開発法人情報通信研究機構及び独立行政法人情報処理推進機構）が共同で運営する下記の Web サイトで参照することができる。

https://www.cryptrec.go.jp/

本報告書ならびに上記 Web サイトから入手した CRYPTREC 活動に関する情報の利用に起因して生じた不利益や問題について、本委員会及び CRYPTREC 事務局は一切責任をもっていない。

本報告書に対するご意見、お問い合わせは、CRYPTREC 事務局までご連絡いただけると幸いである。

【問合せ先】　info@cryptrec.go.jp

委員会構成

暗号技術評価委員会(以下、「評価委員会」という。)は、デジタル庁、総務省及び経済産業省が共同で主催する暗号技術検討会の下に設置され、国立研究開発法人情報通信研究機構(以下、「NICT」という。)と独立行政法人情報処理推進機構(以下、「IPA」という。)が共同で運営する。評価委員会は、CRYPTREC 暗号リスト(付録 1)に掲載されている暗号技術や電子政府システム等で利用される暗号技術の安全性維持及び信頼性確保の観点から、それらの安全性及び実装に係る監視及び評価を行う等、主として技術的活動を担い、暗号技術検討会に助言を行う。また、暗号技術の安全な利用方法に関する調査や新世代の暗号に関する調査も行う。

暗号技術調査ワーキンググループ(以下、「調査 WG」という。)は、評価委員会の下に設置され、NICT と IPA が共同で運営する。調査 WG は、評価委員会の指示の下、評価委員会活動に必要な項目について調査・検討活動を担当する作業グループである。評価委員会の委員長は、実施する調査・検討項目に適する主査及びメンバーを選出し、調査・検討活動を指示する。主査は、その調査・検討結果を評価委員会に報告する。2021 年度、評価委員会の指示に基づき実施される調査項目は、「暗号技術調査 WG(耐量子計算機暗号)」及び「暗号技術調査 WG(高機能暗号)」にてそれぞれ検討される。

評価委員会と連携して活動する「暗号技術活用委員会」も、評価委員会と同様、暗号技術検討会の下に設置され、NICT と IPA が共同で運営している。

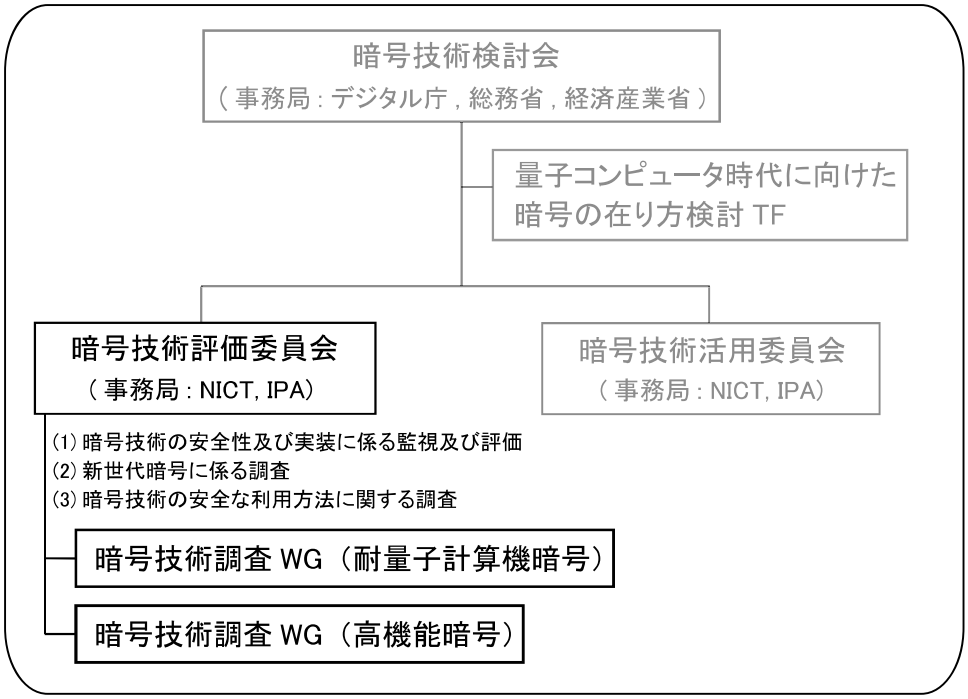

図 0.1：CRYPTREC 体制図

委員名簿

暗号技術評価委員会

委員長	高木 剛	東京大学 教授
委員	青木 和麻呂	文教大学 准教授
委員	岩田 哲	名古屋大学 准教授
委員	上原 哲太郎	立命館大学 教授
委員	大東 俊博	東海大学 准教授
委員	國廣 昇	筑波大学 教授
委員	四方 順司	横浜国立大学　教授
委員	手塚 悟	慶應義塾大学 教授
委員	花岡 悟一郎	国立研究開発法人産業技術総合研究所　首席研究員
委員	藤﨑 英一郎	北陸先端科学技術大学院大学 教授
委員	本間 尚文	東北大学 教授
委員	松本 勉	横浜国立大学 教授
委員	松本 泰	セコム株式会社 マネージャー
委員	山村 明弘	秋田大学 教授

暗号技術調査ワーキンググループ(耐量子計算機暗号)

主査	國廣 昇	筑波大学 教授
委員	青木 和麻呂	文教大学 准教授
委員	伊藤 忠彦	セコム株式会社 主務研究員
委員	草川 恵太	日本電信電話株式会社 主任研究員
委員	下山 武司	国立情報学研究所 特任研究員
委員	高木 剛	東京大学 教授
委員	高島 克幸	早稲田大学 教授
委員	廣瀬 勝一	福井大学 教授
委員	安田 貴徳	岡山理科大学 准教授
委員	安田 雅哉	立教大学 准教授

暗号技術調査ワーキンググループ(高機能暗号)

主査	四方 順司	横浜国立大学 教授
委員	金岡 晃	東邦大学 准教授
委員	国井 裕樹	セコム株式会社 グループリーダー
委員	須賀 祐治	株式会社インターネットイニシアティブ シニアエンジニア
委員	花岡 悟一郎	国立研究開発法人産業技術総合研究所　首席研究員
委員	外園 康智	株式会社野村総合研究所 上級研究員
委員	米山 一樹	茨城大学 教授

オブザーバー

東　隆夫	内閣官房内閣サイバーセキュリティセンター
武藤 健一郎	内閣官房内閣サイバーセキュリティセンター［2021 年 10 月まで］
宮崎 俊一	内閣官房内閣サイバーセキュリティセンター
高橋 元	内閣官房内閣サイバーセキュリティセンター［2021 年 11 月から］
高木 浩光	内閣官房内閣サイバーセキュリティセンター
柏原 陽	個人情報保護委員会 事務局[2021年6月まで]
原田 貴志	個人情報保護委員会 事務局[2021 年 7 月から]
上野 俊介	警察庁 情報通信局情報管理課［2022 年 3 月まで］
鳥越 治	警察庁 長官官房技術企画課［2022 年 4 月から］
千葉 亮輔	デジタル庁 デジタル社会共通機能 G［2022 年 2 月から］
角田 梨翔	デジタル庁 デジタル社会共通機能 G［2022 年 2 月から］
細川 敬太	総務省 自治行政局 住民制度課
梅城 崇師	総務省 サイバーセキュリティ統括官室［2021 年 6 月まで］
山下 恵一	総務省 サイバーセキュリティ統括官室［2021 年 6 月まで］
和田 憲拓	総務省 サイバーセキュリティ統括官室［2021 年 7 月から］
服部 裕史	総務省 サイバーセキュリティ統括官室［2021 年 4 月から］
増田 幸司	総務省 サイバーセキュリティ統括官室［2021 年 7 月から］
佐久間 明彦	外務省 大臣官房
西丸 真生	外務省 大臣官房
大平 浩之	経済産業省 産業技術環境局
村山 裕紀	経済産業省 商務情報政策局
上田 翔太	経済産業省 商務情報政策局［2021 年 6 月まで］
和平 悠希	経済産業省 商務情報政策局［2021 年 7 月から］
小林 圭樹	防衛省 整備計画局
椛木 隆慎	防衛省 整備計画局
伊藤 愼崇	警察大学校
岡原 亮	警察大学校
滝澤 修	国立研究開発法人情報通信研究機構

事務局

国立研究開発法人情報通信研究機構（盛合 志帆、野島 良、篠原 直行、大久保 美也子、黒川 貴司、金森 祥子、吉田 真紀、青野 良範、小川 一人、伊藤 竜馬、高安 敦[2021 年 9 月まで]、笠井 祥、大川 晋司）

独立行政法人情報処理推進機構（瓜生 和久、神田 雅透、石川 誠、木島 慶子、福岡 尊）

第１章　活動の目的

1.1 電子政府システムの安全性確保

電子政府、電子自治体及び重要インフラにおける情報セキュリティ対策は根幹において暗号アルゴリズムの安全性に依存している。情報セキュリティ確保のためにはネットワークセキュリティ、通信プロトコルの安全性、機械装置の物理的な安全性、セキュリティポリシー構築、個人認証システムの脆弱性、運用管理方法の不備を利用するソーシャルエンジニアリングへの対応と幅広く対処する必要があるが、暗号技術は情報システム及び情報通信ネットワークにおける基盤技術であり、暗号アルゴリズムの安全性を確立することなしに情報セキュリティ対策は成り立たない。現在、様々な暗号技術が開発され、それを組み込んだ多くの製品・ソフトウェアが市場に提供されているが、暗号技術を電子政府システム等で利用していくためには、暗号技術の適正な評価が行われ、その評価情報が容易に入手できることが極めて重要となる。

このため CRYPTREC では、「電子政府における調達のために参照すべき暗号のリスト(CRYPTREC 暗号リスト)」[1] を策定し、リストに記載された暗号アルゴリズムを対象として調査・検討を行っている。それに加えて、実導入が進んできている暗号技術の安全性及び実装性について調査し、CRYPTREC 暗号リストへの追加を視野にいれた評価活動も行っている。また、暗号技術に関する安全性について重要な指摘があった場合に対応するため、CRYPTREC の Web サイト上に注意喚起レポートを掲載する活動を実施してきた。

暗号技術に対する解析・攻撃技術の高度化が日夜進展している状況にあることから、今後とも、CRYPTREC によって発信される情報を踏まえて、関係各機関が連携して情報システム及び情報通信ネットワークをより安全なものにしていくための取り組みを実施していくことが非常に重要である。また、過去 21 年間に渡って実施してきた暗号技術の安全性及び信頼性確保のための活動は、最新の暗号研究に関する情報収集・分析に基づいており、引き続き、暗号技術に係る研究者等の多くの関係者の協力が必要不可欠である。

1.2 暗号技術評価委員会

電子政府システムにおいて利用可能な暗号アルゴリズムを評価・選択する活動が2000年度から2002年度まで暗号技術評価委員会において実施された。その結論を考慮して電子政府推奨暗号リスト[2]が総務省・経済産業省において決定された。

電子政府システムの安全性を確保するためには電子政府推奨暗号リストに掲載されている暗号の安全性を常に把握し、安全性を脅かす事態を予見することが重要課題となった。

---

[1] https://www.cryptrec.go.jp/list/cryptrec-ls-0001-2012r4.pdf

[2] https://www.cryptrec.go.jp/list_2003.html

そのため、2007年度に電子政府推奨暗号の安全性に関する継続的な評価、電子政府推奨暗号リストの改訂に関する調査・検討を行うことが重要であるとの認識の下に、暗号技術評価委員会が発展的に改組され、暗号技術検討会の下に暗号技術監視委員会が設置された。設置の目的は、電子政府推奨暗号の安全性を把握し、もし電子政府推奨暗号の安全性に問題点を有する疑いが生じた場合には緊急性に応じて必要な対応を行うこと、また、電子政府推奨暗号の監視活動のほかに、暗号理論の最新の研究動向を把握し、電子政府推奨暗号リストの改訂に技術面から支援を行うことである。

2008 年度において、暗号技術監視委員会では、「電子政府推奨暗号リストの改訂に関する骨子（案)」及び「電子政府推奨暗号リスト改訂のための暗号技術公募要項（2009 年度）(案)」を策定したが、2009 年度からは次期リスト策定のために新しい体制に移行し、名称を「暗号方式委員会」と変更した。電子政府推奨暗号リスト改訂のための暗号技術公募(2009 年度)を受けて、2010 年度からは応募された暗号技術などの安全性評価を開始し、2012 年度に「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト)」[3](付録 1)を策定した。その概要については、CRYPTREC Report 2012 を参照のこと。

2013 年度からは、名称を「暗号方式委員会」から「暗号技術評価委員会」と変更し、暗号技術の安全性に係る監視・評価及び実装に係る技術(暗号モジュールに対する攻撃とその対策も含む)の監視・評価を実施することになった。引き続き、暗号技術評価委員会では、その下に暗号技術調査ワーキンググループを設置し、暗号技術に関する具体的な検討を行っている。2013 年度から 2016 年度まで、暗号技術調査ワーキンググループ（暗号解析評価）及び暗号技術調査ワーキンググループ（軽量暗号）の 2 つのワーキンググループが設置され、2017 年度から 2020 年度までは、暗号技術調査ワーキンググループ（暗号解析評価）が設置された。

そして、2021 年度からは、暗号技術調査ワーキンググループ（耐量子計算機暗号）及び暗号技術調査ワーキンググループ（高機能暗号）の 2 つのワーキンググループが設置されている。2021 年度から設置された暗号技術調査ワーキンググループ（耐量子計算機暗号)及び暗号技術調査ワーキンググループ(高機能暗号)の活動の詳細については、第 3 章を参照のこと。

1.3 CRYPTREC 暗号リスト

2000年度から2002年度のCRYPTRECプロジェクトの集大成として、暗号技術評価委員会で作成された「電子政府推奨暗号リスト（案)」は、2002年度に暗号技術検討会に提出され、同検討会での審議ならびに（総務省・経済産業省による）パブリックコメント募集を経て、「電子政府推奨暗号リスト」として決定された。そして、「各府省の情報システム調達における暗号の利用方針（平成15年2月28日、行政情報システム関係課長連絡会議了承)」において、可能な限り、「電子政府推奨暗号リスト」に掲載された暗号の利

[3] https://www.cryptrec.go.jp/list/cryptrec-ls-0001-2012r4.pdf

用を推進するものとされた。

電子政府推奨暗号リストの技術的な裏付けについては、CRYPTREC Report 2002 暗号技術評価報告書（平成14年度版）に詳しく記載されている。CRYPTREC Report 2002 暗号技術評価報告書（平成14年度版）は、次のURLから入手できる。

https://www.cryptrec.go.jp/rande_cmte.html

2009 年度には、2008 年度に検討した「電子政府推奨暗号リスト改訂のための暗号技術公募要項（2009 年度)」に基づき、電子政府推奨暗号リスト改訂のための暗号技術公募が行われた。2010 年度から 2012 年度にかけて、暗号方式委員会、暗号実装委員会及び暗号運用委員会にて評価が行われ、2012 年度に暗号技術検討会にて電子政府推奨暗号リストの改定が行われた。最終的に、総務省及び経済産業省がパブリックコメント(意見募集)[4]を行い、「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト)」が決定された。選定方法及びその結果については、CRYPTREC Report 2012(暗号技術評価委員会報告)に記載されている。

1.4 活動の方針

暗号技術評価委員会では、主に、暗号技術の安全性評価を中心とした技術的な検討を行う。すなわち、

I) 暗号技術の安全性及び実装に係る監視及び評価

II) 暗号技術の安全な利用方法に関する調査(暗号技術ガイドラインの整備、学術的な安全性の調査・公表等)

を実施する。

I)の内容をさらに詳細に分けると、下記の①～⑤となる。

① CRYPTREC 暗号等の監視：

国際会議等で発表される CRYPTREC 暗号リストの安全性及び実装に係る技術(暗号モジュールに対する攻撃とその対策も含む) に関する監視を行い、会議や ML を通して報告する。

② 電子政府推奨暗号リストからの運用監視暗号リストへの降格、並びに、推奨候補暗号リスト及び運用監視暗号リストからの危殆化が進んだ暗号の削除：

CRYPTREC 暗号リストの安全性に係る監視活動を継続的に行い、急速に危殆化が進んだ暗号技術やその予兆のある暗号技術の安全性について評価を行う。また、リストからの降格や削除、注釈の改訂が必要か検討を行う。

③ CRYPTREC 注意喚起レポートの発行：

CRYPTREC 暗号リストの安全性及び実装に係る技術の監視活動を通じて、国際会議等で発表された攻撃等の概要や想定される影響範囲、対処方法について早期に公開することが望ましいと判断された場合、注意喚起レポートを発行する。

④ 推奨候補暗号リストへの新規暗号（事務局選出）の追加：

[4] https://www.cryptrec.go.jp/topics/cryptrec_201212_listpc.html

標準化動向に鑑み電子政府システム等での利用が見込まれると判断される暗号技術の追加を検討する。

⑤ 新技術等に関する調査及び評価：
将来的に有用になると考えられる技術やリストに関わる技術について、安全性・性能評価を行う。必要に応じて、暗号技術調査ワーキンググループによる調査・評価、または、外部評価による安全性・性能評価などを行う。

そして、具体的に 2021 年度については、上記④において、

- ディジタル署名 EdDSA について、IETF での標準化、TLS 1.3 への実導入などの状況を鑑み、今後、利用が見込まれる暗号技術（署名）であることから、CRYPTREC 暗号リストへの追加を視野に入れ、EdDSA の実装性能評価を行う。また、EdDSA の安全性評価結果(2020 年度外部評価により実施)および実装性能評価の結果から CRYPTREC 暗号リストへ追加するための条件を満たすか否かの検討を行う。

また、次期 CRYPTREC 暗号リストとは別文書として、耐量子計算機暗号、軽量暗号、及び、高機能暗号に関するガイドラインを作成するため、上記⑤において、

- 耐量子計算機暗号に関するガイドラインを作成するため、耐量子計算機暗号に関するワーキンググループを設置する。また、「素因数分解の困難性に関する計算量評価」、「楕円曲線上の離散対数計算の困難性に関する計算量評価」の予測図の更新についても耐量子計算機暗号に関するワーキンググループで検討し、更新を行う。
- 高機能暗号に関するガイドラインを作成するため、高機能暗号に関するワーキンググループを設置する。
- 2016 年度に作成した「CRYPTREC 暗号技術ガイドライン(軽量暗号)」の更新のため、掲載されている暗号方式に関わる安全性解析について、2017 年度以降の技術動向調査を行う。

を実施することが暗号技術検討会において承認された。

監視に関する基本的な考え方は、CRYPTREC Report 2012 までに記載されていた電子政府推奨暗号リスト[5]掲載の暗号技術に対する考え方[6]と基本的に同じである。つまり、暗号技術の安全性及び実装に係る監視及び評価とは、研究集会、国際会議、研究論文誌、インターネット上の情報等を監視すること（情報収集）、CRYPTREC 暗号リストに掲載さ

[5] 2003 年 2 月 20 日に策定されたものを指す。
[6] たとえば、暗号技術検討会 2008 年度報告書を参照のこと。
https://www.cryptrec.go.jp/report/cryptrec-rp-1000-2008.pdf

れている暗号技術の安全性に関する情報を分析し、それを暗号技術評価委員会に報告すること（情報分析）、安全性等において問題が認められた場合、暗号技術評価委員会において内容を審議し、評価結果を決定すること（審議及び決定）、の 3 つの段階からなる。また、仕様書の参照先の変更を検討する際にも、監視に関する基本的な考え方を参考にしている。

また、暗号アルゴリズムの脆弱性に関する CRYPTREC からの情報発信については、下記に示すフローチャート(図 1.1)に基づいて取り扱うことが 2015 年度の暗号技術検討会にて承認されている。

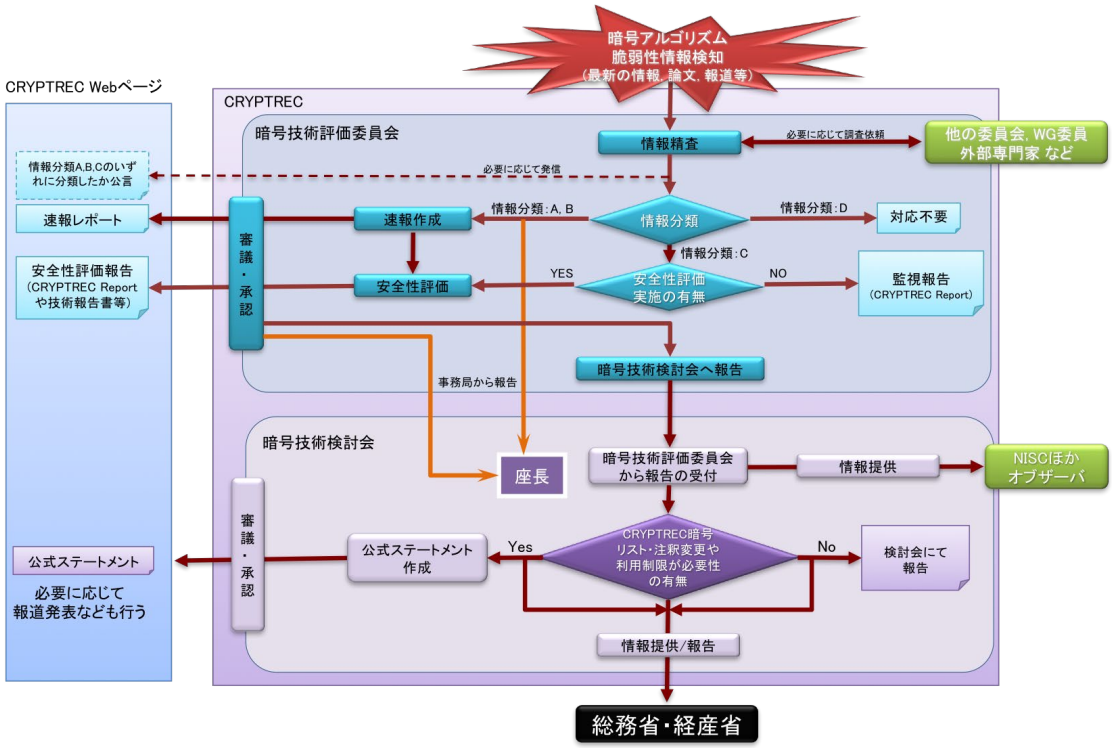

図1.1　暗号アルゴリズムの脆弱性に関する情報発信フロー

[情報発信フローの概要]

（1）　暗号アルゴリズムの脆弱性情報を検知した後、CRYPTREC において参照している仕様に対する攻撃成功に関する情報か、もしくは攻撃成功までは到達していないが攻撃に必要となる計算量の著しい低下につながる結果であるか否かについて判断をし、以下のいずれに属する情報であるかを分類する。

A) 暗号アルゴリズムの完全な危殆化による緊急対応

B) 正確で信頼性の高い情報を発信することによる過剰反応防止

C) 長期的なシステムの安全性維持のための対策喚起

D) 対応不要

（2）　上記の分類のうち、A)もしくは B)に分類される脆弱性情報については、速報を

公開し、また、安全性評価を実施し、その評価結果を公開する。C)に分類される脆弱性情報については、必要に応じて C)に分類された情報であることの公表や安全性評価を実施する。ここで、速報とは、外部で公開されている情報に基づき記載するもので、CRYPTREC では自ら詳細評価は行っていないが、信頼に足る機関・組織等から得た情報に基づくものとする。また、安全性評価報告とは、CRYPTREC として安全性評価を実施しその評価結果をまとめたものとする。

（３） 取り扱う暗号アルゴリズムの範囲は、CRYPTREC 暗号リストに掲載されている暗号技術、および CRYPTREC 暗号リストに掲載されていないが、影響度が高いと暗号技術評価委員会で認められた暗号技術を対象とする。

（４） 速報および安全性評価結果は暗号技術評価委員会の審議に基づき公開される。また、これら脆弱性情報は、暗号技術評価委員会から暗号技術検討会に報告される。

第２章 委員会の活動

2.1. 監視活動報告

電子政府推奨暗号の安全性評価について 2021 年度の報告時点では収集した全ての情報が引き続き「情報収集」、「情報分析」フェーズに留まり、「審議及び決定」には至らず、電子政府推奨暗号の安全性に懸念を持たせるような事態は生じていないと判断した。以降、収集、分析した主たる情報について報告する。

2.1.1. 共通鍵暗号に関する安全性評価について

2021 年度は、2020 年度に引き続き、共通鍵暗号に関する解読について大きな進展はなかったものの、既存の暗号アルゴリズムへの攻撃について、攻撃に必要な計算量の削減等の進展があった。ここでは主な発表を紹介する。

AES については、二つの暗号解析論文が注目される。一つ目は、Eurocrypt 2021 で、AES 鍵スケジュールに対する新しい表現とそれを活用した AES-128 に対する不能差分攻撃（impossible-differential attacks）の改善を報告した。INDOCRYPT 2010 で報告された攻撃、及びその亜種が今までの最善の攻撃であったが、本提案手法はそれよりも約 2.3 倍計算量を改善している。この論文は Eurocrypt 2021 Best paper award を受賞した。二つ目は、同じく Eurocrypt 2021 にて、AES-128 ハッシュモードの 8 段に対する最初の攻撃を報告した。これは、攻撃探索問題を混合整数線形計画法における制約条件のもとでの最適化問題に変換することで攻撃の探索範囲を拡大し、より攻撃に有効な経路を発見できることを利用している。このように、AES に対する攻撃は 2021 年度も進展は見られたが、セキュリティマージンはまだ十分にあり、AES の安全性に直ちに影響を与えるものではない。

その他の暗号については、Eurocrypt 2021 で、ARX（Addition, Rotation, and XOR）ベースの暗号に対する差分線形解析の改良が発表された。ストリーム暗号の一種である ChaCha がこのタイプに属し、結果として時間計算量が $2^{228.51}$、データ計算量が $2^{80.51}$ となるラウンド数 7 の ChaCha に対する攻撃が発表された。この結果は、CRYPTO 2020 で発表された今まで最良の攻撃計算量（時間計算量 $2^{230.86}$、データ計算量 $2^{48.4}$）よりも削減され、攻撃が進展したことを示している [1]。ただ、ChaCha のラウンド数 20 にはまだマージンがあり、早急な対策が必要となるものではない。

2.1.2. 公開鍵暗号に関する安全性評価について

公開鍵暗号の一種である RSA については、部分的に秘密鍵が分かっている場合の新規

[1] Cryptology ePrint Archive に投稿された論文（Paper 2021/224）において、Eurocrypt 2021 で発表された攻撃手法が成立しないと提案者自らが訂正していることに注意されたい。

の素因数分解アルゴリズム（Partial Key Exposure Attack）が Asiacrypt 2021 において提案された。素因数分解する数を N として、今までは CRT-RSA 指数のサイズが $N^{0.122}$ 以下のときの多項式時間攻撃が提案されていたが、本攻撃は CRT-RSA 指数の最下位ビット（LSB：Least Significant Bit）の部分的な知識を仮定して、サイズが $N^{0.122}$ 以上 $N^{0.5}$ 以下の場合の攻撃を実現している。

また、格子と暗号理論との関係についての招待講演が Ducas 氏により PKC 2021 にて行われた。その中で Schnorr 氏の Eurocrypt'91 の論文における格子を用いた素因数分解について述べられた。最近、1991 年の攻撃手法を改良した論文が Schnorr 氏によって Cryptology ePrint Archive に投稿され(Paper 2021/232[取り下げ]、2021/933[訂正版])、注目を集めたところである。Ducas 氏自身によるものを含めいくつかの検証実験が行われた結果、大きなビット長が素因数分解できた結果は報告されていない。そのため、Schnorr 氏の攻撃手法が直ちに RSA の危殆化につながることはないと考えられる。

2.1.3. その他の注視すべき技術動向

・耐量子計算機暗号(PQC: Post-Quantum Cryptography)の動向

NIST による、量子計算機による解読に耐性を持つ暗号「耐量子計算機暗号(PQC:Post-Quantum Cryptography)」の標準化では、NIST PQC 3rd Standardization Conference において、NIST は「格子に基づかない汎用的電子署名スキームに関心がある」とした上で、第 3 ラウンド終了後、新たな提案募集を行う予定を明らかにした。応募期間は 6 ヵ月から 1 年の予定であり、特に構造付き格子（structured lattice）以外の汎用的電子署名スキームに興味を示している。第 3 ラウンドにおけるセレクションは未だ継続中であり、更に続く第 4 ラウンドもまた 12～18 ヵ月かけて行われる見通しである。最終的な標準化については、2024 年に最終版を提出する予定であるという。

2.2. 注意喚起レポートについて

今年度は、注意喚起の対象となるイベントが発生しなかったため注意喚起レポートの発行は行わなかった。

2.3. 推奨候補暗号リストへの新規暗号（事務局選出）の追加

ディジタル署名 EdDSA は、RFC8032[2]で規定され、TLS1.3 で採用された（RFC 8446[3]）署名アルゴリズムである。EdDSA は、TLS1.2 のような TLS1.3 より前のバージョンおいて、ECDSA と同じ暗号スイートを使っても利用可能である（RFC8422[4]）。

ディジタル署名 EdDSA の安全性評価について、2020 年度に評価を行い、EdDSA の曲線

[2] RFC8032, "Edwards-Curve Digital Signature Algorithm (EdDSA) ", Jan. 2017
[3] RFC8446, "The Transport Layer Security (TLS) Protocol Version 1.3", Aug. 2018
[4] RFC8422, "Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS) Versions 1.2 and Earlier", Aug. 2018

および方式の構成いずれについても安全性に問題は見つからなかったことから、「国際標準化等の実績がある」ことを根拠とした事務局で選出する暗号アルゴリズムの候補として、CRYPTREC 暗号リストへの追加を視野に入れて評価を行うことが承認された。

2021 年度は、EdDSA の実装性能について調査・評価を実施した。

2.3.1. 調査・評価概要

下記のように、公開されている第三者の測定結果および本調査による測定結果の範囲では、Ed25519 は ECDSA P-256 と同等の安全性でありながら高速であると評価でき、Ed448 は ECDSA P-384 より高い安全性でありながら同等または高速であると評価できた。詳しくは、付録 4 を参照のこと。

- 特徴
- EdDSA は ECDSA と同様に射影座標系を使用可能であるため、有限体上の乗法逆元の演算を用いずに演算可能であることから、高速な実装が可能である。
- EdDSA で推奨される twisted-Edwards 曲線は無限遠点を例外的に扱うための分岐が不要なため、ECDSA で使われる Weierstrass 形式の楕円曲線と比較して実装しやすい。
- EdDSA で推奨される Edwards 楕円曲線は，異なる点の加算と同一の点の加算(2 倍算)を同じ処理で計算できるため、実装するアルゴリズムが 1 つでよく、点が異なるかどうかの条件分岐を考慮する必要がないため，Weierstrass 形式の楕円曲線と比較して Side Channel Attack (SCA) 対策に有利である。
- 性能測定結果
- C 言語 4 種類、Java 2 種類の OSS の暗号ライブラリを Windows、Linux、Mac の 3 つの OS 上でそれぞれ動かした計 18 種類の環境で実際に性能測定を行い、各環境の結果は以下のようになった。
- Ed25519
  - 鍵ペア生成
    - 17 環境で ECDSA P-256 より高スループットだった。1 環境では ECDSA P-256 より低スループットだったが 50%未満の極端な差はなかった。
  - 署名生成
    - 12 環境で ECDSA P-256 より高スループットだった。6 環境では ECDSA P-256 より低スループットだったが 50%未満の極端な差はなかった。
  - 署名検証
    - 15 環境で ECDSA P-256 より高スループットだった。3 環境では ECDSA P-256 より低スループットだったが 50%未満の極端な差はなかった。
- Ed448

- 鍵ペア生成
  - 15 環境で ECDSA P-384 より高スループットだった。3 環境では ECDSA P-384 より低スループットだったが 50%未満の極端な差はなかった。18 環境で ECDSA P-521 より高スループットだった。
- 署名生成
  - 15 環境で ECDSA P-384 より高スループットだった。3 環境では ECDSA P-384 より低スループットだったが 50%未満の極端な差はなかった。18 環境で ECDSA P-521 より高スループットだった。
- 署名検証
- 15 環境で ECDSA P-384 より高スループットだった。3 環境では ECDSA P-384 より低スループットだったが 50%未満の極端な差はなかった。18 環境で ECDSA P-521 より高スループットだった。

2.3.2. CRYPTREC 暗号リストへの追加について

CRYPTREC 暗号リストへ追加するためには、安全性評価および実装性能評価を実施する必要がある。ディジタル署名 EdDSA については、2020 年度に安全性評価を実施し、暗号技術評価委員会として下記の見解を得た。

- 曲線に関する安全性評価について

  EdDSA での使用が見込まれる二つの曲線 Curve25519 及び Curve448 における ECDLP に対する古典計算機（従来の計算機）を用いた現時点での最良のアルゴリズムは ρ 法であるため、その安全性は現在使用されている楕円曲線暗号の場合と同じく、結果として主に基礎体の大きさで決定される。従って、Curve25519 の場合はほぼ 128 ビットセキュリティ、Curve448 の場合はほぼ 224 ビットセキュリティの安全性を持つと判断する。また、それらの曲線上の演算も効率よく実行できることを確認した。

- 方式の構成に関する安全性評価について

  評価報告書において、現実的な脅威に結びつくような脆弱性は指摘されておらず、また、ECDSA と比較してもその安全性に劣る点はないと考えられる。他、複数の観点から安全性に関わる考察が示されており、いずれも安全性に問題を与える点はないと考えられる。以上より、評価報告書により示された評価結果を総合し、EdDSA の構成については、現実的な利用シーンにおける安全性に問題はないと判断する。

そして、2021 年度は、前節の通り、EdDSA の実装性能評価を行い、十分な実装性能があることを確認した。2020 年度に実施した安全性評価および今年度実施した実装性能評価の結果に基づき、EdDSA はディジタル署名として十分な安全性及び実装性能を有し

ていると判断したので、CRYPTREC 暗号リストの推奨候補暗号リスト（技術分類：公開鍵暗号_署名）へ追加することを暗号技術検討会に提案した。

2.4. 仕様書の参照先の変更について

今年度は、仕様書の参照先の変更を行わなかった。

2.5. 軽量暗号に関するガイドラインの作成について

2020 年度第 2 回暗号技術検討会にて、2016 年度に作成した「CRYPTREC 暗号技術ガイドライン（軽量暗号）」（以下、2016 年度版ガイドラインと呼ぶ）の更新のため、2021 年度は、掲載されている暗号方式に関わる安全性解析について、2017 年度以降の技術動向調査を行い、2023 年度中を目途に現ガイドラインを更新することが承認された。

2016 年度版ガイドラインに掲載されている暗号方式に関わる安全性解析について、2017 年度以降の技術動向調査を行った。また、現ガイドラインの更新方針を決定した。

2.5.1. 軽量暗号に関する技術動向調査

2021 年 9 月の時点で脅威に繋がる脆弱性が指摘されているか否かについて調査を実施した。調査報告書は、技術調査報告書として CRYPTREC ホームページに公開する。

調査概要は下記の通り。

- 調査対象
  - 2017 年 3 月に公開した「CRYPTREC 暗号技術ガイドライン（軽量暗号）」に掲載されている方式について、2017 年 3 月以降に大幅な安全性の劣化につながる脆弱性が見つかっているか否かについて調査。
  - 軽量暗号に関わる ISO/IEC 29192 シリーズに近年採録されたもしくは採録される予定の方式について、「CRYPTREC 暗号技術ガイドライン（軽量暗号）」における掲載の有無およびそれらの安全性について調査。
  - 「CRYPTREC 暗号技術ガイドライン（軽量暗号）」公開時に CAESAR プロジェクトが終了していなかったことから、CAESAR プロジェクトで最終的に選ばれたポートフォーリオ 6 方式について、「CRYPTREC 暗号技術ガイドライン（軽量暗号）」における掲載の有無およびそれらの安全性について調査。
- 実施方法
  - 事務局により調査を行い、調査報告書を執筆し、外部有識者による調査報告書のレビューを実施した。
- 調査結果概要

  各方式の安全性解析状況について、次のとおり表にまとめた。

	分類１	分類２	分類３
ブロック暗号	CLEFIA,LED,Simon,Speck, LEA	Piccolo,Midori, PRESENT,PRINCE, TWINE	
ストリーム暗号	ChaCha,Enocoro,Trivium		Grain v1, MICKEY 2.0
ハッシュ関数	Keccak,PHOTON,QUARK 、SPONGENT,Lesamnta-LW		
MAC	SipHash, Tsudik’s keymode	Chaskey, LightMAC	
認証暗号	ACORN,ASCON,AES-OTR,CLOC and SILC,Deoxys,Joltik, Ketje,Minalpher,OCB1, OCB3,PRIMATEs,AEGIS, $COLM_{127}$	$COLM_0$	OCB2,AES-JAMBU, Grain-128A

分類１：仕様段数において安全性を脅かす攻撃が存在しない方式

- ✧ 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方式
- ✧ 安全性基準を脅かす攻撃が存在しない方式

分類２:特定の場合を除き仕様段数において安全性を脅かす攻撃が存在しない方式

- ✧ 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方式

分類３：仕様段数において安全性基準を満たさない方式

- ✧ 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方式
- ✧ 安全性基準を脅かす攻撃が存在する方式

2.5.2. 軽量暗号ガイドラインの更新に関する方針

下記の通り更新を行うことを決定した。

- ➢ 更新形態

2016 年度版ガイドラインに新規情報を追加・更新した文書を 2023 年度版ガイドラインとして公開する。

- ・ 主たる追加は、2016 年度版ガイドラインの 4 章「代表的な軽量暗号」に相当する軽量暗号方式の紹介とする。
- ・ 既に 4 章に掲載されている方式については、今年度実施した軽量暗号に関する技術動向調査[5]を基に更新する。

[5] 詳しくは、付録 3 参照のこと。

- 1 章～3 章は、2016 年度版ガイドラインをそのまま用いる。ただし、4 章に新規追加・更新する方式に関わる情報は、適切な章に節を追加し、掲載する。
- 付録を追加し、関連情報を掲載する。

➢ タイトル
- 「CRYPTREC 暗号技術ガイドライン（軽量暗号)」2023 年度版

➢ 追加情報の対象
- NIST Lightweight コンペティション最終選考で採択された方式
- 軽量な方式として ISO に近年採録されたもしくは採録される予定の方式

➢ 主な追加内容
- 1 章　はじめに
  - ✓ 追記箇所を説明する文章を追加する。
- 2 章 軽量暗号とその活用法
  - ✓ 節を追加し、2017 年以降の標準化動向を掲載する。
- 3 章 軽量暗号の性能比較
  - ✓ 節を追加し、″追加情報の対象″ の方式に関する安全性や実装性能に関わる評価・調査結果（2022 年度実施予定）を掲載する。
- 4 章 代表的な軽量暗号
  - ✓ 2016 年度版ガイドライン掲載暗号について、今年度実施した軽量暗号に関わる調査報告書[5]を基に追記・更新する。
  - ✓ ″追加情報の対象″の方式について、掲載方式と同等の情報を掲載する。(2022 年度外部評価の実施結果を反映する)
- 付録(新規)
  - ✓ NIST　Lightweight コンペティションファイナリスト(最終選考で採択されなかった方式)
  - ✓ CAESAR のスケジュールが後ろ倒しにずれ込み、最終選考が完結する前に 2016 年度版ガイドラインを公開することとなった。後に、CAESAR プロジェクトの最終選考により、3 ケース各 2 方式(計 6 方式）が選ばれた。Use case 1: Lightweight applications について選ばれた 2 方式はすでに掲載していたが、Use case 2: High-performance applications および Use case 3: Defense in depth については、2 方式中 1 方式は掲載しているが、各 1 方式は掲載していない。ここで、未掲載の 2 方式を紹介する。

➢ 編集方法
- 事務局で取りまとめ・編集を行い、更新版を作成し、暗号技術評価委員会にて審議いただく。

➢ 今後のスケジュール

- 2022年：
  NIST Lightweight コンペティションファイナリストを対象とした安全性および実装性能に関わる調査・評価
- 2023年：
  事務局によりガイドラインの更新案を編集し、ドラフト版について外部有識者にガイドラインとして、掲載内容の適切性や情報の過不足などについてレビュー頂き、完成版を暗号技術評価委員会にて審議する

2.6. 学会等参加状況

国内外の学術会議に参加し、暗号解読技術に関する情報収集を実施した。参加した国際会議は、表 2.4 に示す通りである。

表 2.4 国際会議への参加状況

学会名・会議名		開催国・都市	期間
PQCrypto 2021	The 12th International Conference on Post-Quantum Cryptography	(Virtual Conference)	2021年7月20日～7月22日
Crypto 2021	The 41st Annual International Cryptology Conference	(Virtual Conference)	2021年8月16日～8月20日
CHES 2021	Conference on Cryptographic Hardware and Embedded Systems	(Virtual Conference)	2021年9月13日～9月17日
FDTC 2021	Fault Tolerance and Diagnosis in Cryptography	(Virtual Conference)	2021年9月17日
Eurocrypt 2021	The 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques	(Virtual Conference)	2021 年 10 月 17 日～10月21日
TCC 2021	The Theory of Cryptography 19th International Conference	(Virtual Conference)	2021 年 11 月 8 日～11 月 11 日
Asiacrypt 2021	The 27th Annual International Conference on the Theory and Application of Cryptology and Information Security	(Virtual Conference)	2021 年 12 月 6 日～12 月 10 日

以下に、国際学会等に発表された論文を中心に、暗号解読技術の最新動向を示す。詳しくは、付録 5 を参照のこと。

2.6.1. 共通鍵暗号の解読技術

・New Representations of the AES Key Schedule [Eurocrypt 2021, Awarded paper]

Gaëtan Leurent, Clara Pernot

本論文では、AES 鍵スケジュールの新しい表現と、AES ベースのスキームの安全性へのいくつかの示唆が提示される。特に、AES-128 鍵スケジュールは、32 ビットのチャンクで動作する 4 つの独立した並列計算に分割でき、線形変換まで可能であることが示される。この性質は 20 年以上にわたる AES の解析を経て初めて示されたものである。さらに、この新しい表現は AES ベースのスキームに対するこれまでの暗号解読結果を改善するために使用され、2 つの新しい結果が得られている。まず著者らは、奇数回の鍵スケジュールラウンドを繰り返すと、短いサイクルを持つ関数が生成されることを確認し

た。この結果を利用することで、NIST Lightweight Cryptography コンペティションの第 2 ラウンド候補である mixFeed に対して Khairallah が示した観測結果を説明することが可能となる。著者らの解析によると、Khairallah が示した mixFeed に対する偽造攻撃は 0.44 の確率で成功することがわかった（データ量は 220GB)。また、同じ観測結果から、AES ベースの AEAD 方式である ALE に対する新たな攻撃も発見された。また、著者らが提示する新しい表現により、最初のサブキーの情報と最後のサブキーの情報を組み合わせて、対応するマスターキーを再構成する効率的な方法が示されている。特に、これらの解析手法を使用し、AES-128 に対する従来の不可能差分攻撃（impossible-differential attacks）を改善することが可能となる。

・Automatic Search of Meet-in-the-Middle Preimage Attacks on AES-like Hashing [Eurocrypt 2021]

Zhenzhen Bao, Xiaoyang Dong, Jian Guo, Zheng Li, Danping Shi, Siwei Sun, Xiaoyun Wang

中間一致原像攻撃（MITM 原像攻撃）は、フル MD5、HAVAL、Tiger、縮小 SHA-0/1/2 など、多くのハッシュ関数の原像攻撃の耐性を破るのに極めて有効である。なお、2011 年に Sasaki は AES ライクなハッシュ関数に対してもこの攻撃が脅威であると示している。近年、AES のハッシュモードに対する MITM 原像攻撃は、内部状態を自由に選択できる仮定を利用するとともに、メッセージを自由に選択できる仮定を利用するなど、様々な攻撃手法が提案されている。しかしながら、MITM 原像攻撃を実行するために考えられる構成が多すぎるため、従来の解析結果は提案者の直感と経験に依存するところが大きく、必ずしも最適な解であるとは限らないという問題があった。

本論文では、先行研究における人為的な制限を取り除き、攻撃の構成に関する本質的なアイデアを明確に定式化し、最適な解を探索するため混合整数線形プログラミング（MILP）モデルにおける制約条件の下で最適化問題に変換する。MILP モデルを構築し、市販のソルバーを使用することで、最適な解を網羅的に探索することができる。その結果、Haraka-512 v2 の完全版（5 ラウンド）と拡張版（5.5 ラウンド)、および AES-128 ハッシュモードの 8 ラウンドに対する攻撃を初めて示すとともに、Haraka-256 v2 および AES と Rijndael のハッシュモードにおける他のメンバーへの攻撃を改善した。

・Improved Linear Approximations to ARX Ciphers and Attacks Against ChaCha [Eurocrypt 2021]

Murilo Coutinho Silva, Tertuliano C. de Souza Neto

本論文では、ARX 暗号においてより良い線形近似を求めるために用いることができる新しい技術が紹介される。この技術を用いることで、ChaCha の 3 ラウンドと 4 ラウンドに対して初めて明示的に導き出された線形近似を提示し、その結果として、ChaCha に

対する最近の攻撃を改善することが可能となった。さらに、ChaCha の 3 ラウンドと 3.5 ラウンドに対する新しい差分を提示し、提案手法と組み合わせることで、ChaCha に対する差分線形攻撃の計算量をさらに向上させることに成功している。

2.6.2. 公開鍵暗号の解読技術

・Partial Key Exposure Attack on Short Secret Exponent CRT-RSA [Asiacrypt 2021]

Alexander May, Julian Nowakowski, Santanu Sarkar

(N,e) を RSA 公開鍵とし、 N=pq をビットサイズの等しい素数 p,q の積とする。d_p, d_q は対応する秘密の CRT-RSA 指数とする。Coppersmith 型攻撃により、Takayasu, Lu and Peng (TLP) は最近、$d_p, d_q \leq N^{0.122}$ であれば、多項式時間で N の因数分解を得ることができることを示した。

本論文では、TLP 攻撃に基づいて、短い秘密指数を持つ CRT-RSA に対する最初の Partial Key Exposure 攻撃が示される。すなわち、$N^{0.122} \leq d_p, d_q \leq N^{0.5}$ のとき、d_p, d_q の両方の既知の定数割合の下位ビット (LSBs) があれば、多項式時間で N を因数分解するのに十分であることを示す。当然ながら、d_p, d_q が大きくなればなるほど、より多くの下位ビットが必要となる。例えば、d_p, d_q が $N^{0.13}$ のサイズであればその約 1/5 の下位ビット、$N^{0.2}$ のサイズならその約 2/3 の下位ビット、d_p, d_q がフルサイズ $N^{0.5}$ であればその全てを知る必要がある。この結果の副産物として、入力 (N, e, d_p, d_q) に対するヒューリスティックな決定論的多項式時間因数分解アルゴリズムが得られることに注目する。

2.6.3. その他の暗号技術の解読技術

・Quantum Collision Attacks on Reduced SHA-256 and SHA-512 [CRYPTO 2021]

Akinori Hosoyamada, Yu Sasaki

本論文では、SHA-256 と SHA-512 に対する専用の量子衝突攻撃法が初めて示される。

この攻撃はそれぞれ 38 ステップと 39 ステップに達し、古典的な 31 ステップと 27 ステップの攻撃を大幅に改善した。両攻撃とも、多数の semi-free-start 衝突を 2 ブロック衝突に変換する先行研究の枠組みを採用し、計算時間と計算空間の間のトレードオフのコスト指標において汎用攻撃より高速であることが確認された。必要な semi-free-start 衝突の数は、量子設定において削減できることが観測されており、この観測結果に基づき、従来の古典的な 38 ステップ、39 ステップの semi-free-start 衝突を一つの衝突に変換することが可能となった。著者らは、この攻撃の基本となる考え方が単純であるため、他の暗号学的ハッシュ関数にも適用可能であると報告している。

・A Deeper Look at Machine Learning-Based Cryptanalysis [Eurocrypt 2021]

Adrien Benamira, David Gerault, Thomas Peyrin, Quan Quan Tan

機械学習を用いた共通鍵暗号に対する解析論文である。

CRYPTO 2019 で Gohr は、機械学習アルゴリズムを活用した新しい暗号解析手法を提案した。この解析手法ではディープニューラルネットワークを利用しており、ブロック暗号 SPECK のメンバーの 1 つである SPECK-32/64 に対し、最先端の暗号解読を上回る識別器（distinguisher）を構築することに成功した（この識別器は鍵回復攻撃に応用できる可能性がある）。しかしながら、この識別器が実際にどのように機能するのか、機械学習アルゴリズムがどのような情報を推論しているのか、という問題（ディープニューラルネットワークの解釈可能性）はよく知られた困難な問題であることも加わり、まだ明らかになっていない。

本論文では、この新しい識別器に対して詳細な分析と徹底的な解説を行う。まず、分類済みのデータセットを使用し、Gohr の結果をよりよく理解するための指針となる様々なパターンの発見を試みた。実験により、この識別器は一般的に暗号文ペアに関する差分分布に依存しているが、最後から 2 番目と 3 番目のラウンド（penultimate and antepenultimate rounds）における差分分布にも依存していることが明らかとなった。この実験結果を検証するため、ニューラルネットワークを使用しない暗号解析手法に基づいて SPECK の識別器を構築し、Gohr の識別器と基本的に同じ精度と効率性を達成することに成功している（したがって、この結果は Gohr の識別器が従来の識別器よりも改善できていることを明らかにしている）。さらに別のアプローチとして、Gohr のディープニューラルネットワークを必要最低限にまで縮小した機械学習ベースの識別器を提供する。著者らは、標準的な機械学習ツールを用いるだけで Gohr の識別器に非常に近い精度を維持できることを示した。また、Gohr は識別器を構成するために学習段階で対象となる暗号方式の差分分布表（DDT）に関する非常に優れた近似表を作成し、この情報を使って暗号文ペアを直接分類していることを示す。この結果は、識別器の完全な解釈可能性を可能にするとともに、ディープニューラルネットワークの解釈可能性に向けた興味深い貢献となる。最後に、Gohr の研究を改善するための方法と、識別器の構成に関する新しい可能性が提案されている。すべての結果は、SPECK ブロック暗号で実施した実験により確認されている。

・On the hardness of the NTRU problem [Asiacrypt 2021]

Alice Pellet-Mary, Damien Stehlé

25 年前の NTRU 問題は、公開鍵暗号における重要な計算の前提となっている。しかし、ユークリッド格子上の他の問題と比較した場合、削減の観点からその相対的な難しさはよく分かっていない。その決定版は探索 Ring-LWE 問題に還元されるが、これは困難性の上界を与えるに過ぎない。

本論文は、NTRU 問題の困難性に関する漸化式の証拠を提供するという、長年の未解決問題に対する 2 つの解答を提供する。まず、理想格子上の最悪ケースの近似最短ベクトル問題を、NTRU 問題の平均ケース探索変種問題に帰着する。次に、NTRU 問題の別の平均ケース探索変種問題を、決定 NTRU 問題に還元する。

・A Geometric Approach to Linear Cryptanalysis [Asiacrypt 2021]

Tim Beyne

線形解読法に関する新しい解釈を提案する論文である。「幾何学的アプローチ」（geometric approarch）は、線形解読法における全ての一般的なバリエーションを統一するとともに、様々な特性の間にリンクが存在することを明らかにし、線形解読法のさらなる一般化を提案する。例えば、相関行列の非実数固有値に対応する不変量に対する新しい洞察や、ゼロ相関攻撃と積分攻撃の間のリンクに関する一般化が得られる。幾何学的直感は、固定鍵による piling-up 原理の動機付けにつながり、これは不変量と線形近似に関連する従来の結果の説明と一般化によって説明される。ランク 1 近似は、セル指向暗号（cell-oriented cipher）を分析するために提案され、FSE 2019 で Beierle、Canteaut、Leander によって提起された未解決問題を解決するために使用される。特に、このような近似がリーマン最適化を用いて自動的に解析される方法を示す。

2.7. 委員会開催記録

2021 年度に暗号技術評価委員会は、表 2.5 の通り 2 回開催された。各会合の開催日及び主な議題は以下の通りである。

表 2.5　暗号技術評価委員会の開催状況

回	開催日	議案
第 1 回	2021 年 7 月 6 日	■ 暗号技術評価委員会活動計画の具体的な進め方についての審議 ■ 外部評価（ディジタル署名EdDSAの実装性能に関する調査）実施についての審議 ■ 暗号技術調査ワーキンググループ（耐量子計算機暗号）の活動計画案の審議 ■ 暗号技術調査ワーキンググループ（高機能暗号）の活動計画案の審議 ■ 軽量暗号に関するガイドライン係る技術動向調査及び更新方針策定案の審議
第 2 回	2022 月 2 月 22 日	■ 暗号技術評価委員会活動報告（案）についての審議 ■ ディジタル署名EdDSAの実装性能に関する調査結果の報告と暗号技術評価委員会としての見解について審議 ■ 暗号技術調査ワーキンググループ（耐量子計算機暗号）の活動内容の報告 ■ 暗号技術調査ワーキンググループ（高機能暗号）の活動内容の報告 ■ 軽量暗号ガイドラインに係る技術動向調査結果の報告及び更新方針の決定

2.8. 暗号技術調査ワーキンググループ開催記録

2021 年度、暗号技術調査ワーキンググループ(耐量子計算機暗号)は、表 2.6 の通り 2 回開催された。

表 2.6　暗号技術調査ワーキンググループ(耐量子計算機暗号)の開催状況

回	開催日	議案
第 1 回	2021 年 9 月 7 日	■ 暗号技術評価委員会活動計画及び暗号技術調査ワーキンググループ（耐量子計算機暗号）の活動計画の報告 ■ 耐量子計算機暗号ガイドラインに関する記載すべき項目・章立て、執筆方針及び執筆スケジュールに関する審議
第 2 回	2022 月 1 月 28 日	■ 耐量子計算機暗号ガイドラインに関する執筆担当者及びスケジュールに関する審議 ■ 耐量子計算機暗号に関する調査内容の報告（導入、活用方法、格子に基づく暗号技術、符号に基づく暗号技術、多変数多項式に基づく暗号技術、同種写像に基づく暗号技術、ハッシュ関数に基づく署名技術） ■ 耐量子計算機暗号ガイドラインに関する執筆方針案に関する審議 ■ 「素因数分解の困難性に関する計算量評価」、「楕円曲線上の離散対数計算の困難性に関する計算量評価」の予測図に関する審議 ■ 2021年度暗号技術調査WG(耐量子計算機暗号)活動報告案に関する審議

また、暗号技術調査ワーキンググループ(高機能暗号暗号)は、表 2.7 の通り 3 回開催された。各会合の開催日及び主な議題は以下の通りである。

表 2.7　暗号技術調査ワーキンググループ(高機能暗号暗号)の開催状況

回	開催日	議案
第 1 回	2021 年 8 月 3 日	■ 暗号技術評価委員会活動計画及び暗号技術調査ワーキンググループ（高機能暗号）の活動計画の報告 ■ 想定するガイドラインの目次についての審議 ■ 高機能暗号の定義についての審議 ■ ガイドライン執筆に関する作業方針と作業分担についての審議
第 2 回	2021 月 12 月 8 日	■ 高機能暗号技術に関する現状調査に関する報告 ■ アプリケーション・活用法に関するヒアリング先に関する検討 ■ ガイドライン目次案についての審議
第 3 回	2022 年 2 月 8 日	■ ガイドライン執筆方針案についての審議 ■ アプリケーション・活用法に関するヒアリング先に関する検討 ■ 2021年度暗号技術調査WG(高機能暗号)活動報告案に関する審議

第３章　暗号技術調査ワーキンググループの活動

暗号技術評価委員会では、その下に暗号技術調査ワーキンググループを設置し、暗号技術に関する具体的な検討を行っている。そして、2021 年度からは、暗号技術調査ワーキンググループ（耐量子計算機暗号）及び暗号技術調査ワーキンググループ（高機能暗号）の 2 つのワーキンググループが設置されている。暗号技術調査ワーキンググループ（耐量子計算機暗号）及び暗号技術調査ワーキンググループ（高機能暗号）の活動について以下に示す。

3.1.　暗号技術調査ワーキンググループ（耐量子計算機暗号）

3.1.1. 活動報告の概要

大規模な量子コンピュータが実用化されたとしても安全性を保つことができると期待される暗号（耐量子計算機暗号:PQC）の研究開発及び標準化などが各国で進められている。そこで、2021 年度、暗号技術評価委員会では、耐量子計算機暗号に関するガイドライン（以下「耐量子計算機ガイドライン」という）を作成するためにワーキンググループを設置することが承認されていたことから、「新技術等に関する調査及び評価」の活動として暗号技術調査ワーキンググループ（耐量子計算機暗号）（以下「耐量子計算機暗号 WG」という）を設置した。以下が主な検討項目である。

- 耐量子計算機暗号の研究動向調査をもとに、主要な耐量子計算機暗号についてのガイドラインを2021年度から2022年度にかけて作成する。
- 「素因数分解の困難性に関する計算量評価」、「楕円曲線上の離散対数計算の困難性に関する計算量評価」の予測図を更新する。

これらの成果（3.1.3.～3.1.4.節）は 2021 年度第 2 回暗号技術評価委員会にて報告され、了承された。

【2021 年度のスケジュール】

・2021 年 9 月 7 日 第 1 回 耐量子計算機暗号 WG
　耐量子計算機暗号ガイドラインに関する記載すべき項目・章立て、執筆方針及び執筆スケジュールに関する審議

・2022 年 1 月 28 日　第 2 回 耐量子計算機暗号 WG
　耐量子計算機暗号ガイドラインに関する執筆担当者及びスケジュールに関する審議、「素因数分解の困難性に関する計算量評価」、「楕円曲線上の離散対数計算の困難性に関する計算量評価」の予測図に関する審議

3.1.2. 委員構成（敬称略）

主査：國廣 昇　　（筑波大学）
委員：青木 和麻呂　　（文教大学）
委員：伊藤 忠彦　　（セコム株式会社）
委員：草川 恵太　　（NTT）

委員：下山 武司　　(国立情報学研究所)
委員：高木 剛　　(東京大学)
委員：高島 克幸　　(早稲田大学)
委員：廣瀬 勝一　　(福井大学)
委員：安田 貴徳　　(岡山理科大学)
委員：安田 雅哉　　(立教大学)

3.1.3. 耐量子計算機暗号に関するガイドラインの作成方針

<u>ガイドライン及び調査報告書の作成</u>

耐量子計算機暗号ガイドラインは、暗号理論に精通していない利用者を対象とし、耐量子計算機暗号に関する調査報告書は、暗号理論の研究者や技術者を対象としている。基本的には耐量子計算機暗号ガイドラインは調査報告書から技術的詳細を削除し、その一部を抜粋したものとする。ただし、暗号理論に精通していない利用者のために、耐量子計算機暗号の活用方法を耐量子計算機暗号ガイドラインでは記載するが、調査報告書には記載しない。

<u>ガイドライン及び調査報告書に記載する暗号方式の選定基準及び候補について</u>

主要な公開鍵暗号方式（NIST PQC 標準化への提案方式等）を記載するが、対象となる暗号方式は執筆担当委員が選定する。

<u>記載すべき項目及び章立て</u>

i. 導入
ii. PQC の活用方法（ガイドラインにのみ記載）
iii. 格子に基づく暗号技術
iv. 符号に基づく暗号技術
v. 多変数多項式に基づく暗号技術
vi. 同種写像に基づく暗号技術
vii. ハッシュ関数に基づく署名技術

- iii 章以降：章内部の詳細な構成（A 章の場合）

A.1. 安全性の根拠となる問題の説明（例：LWE 問題、シンドローム復号問題）
A.2. 代表的な暗号方式の構成法（例：Regev 暗号、McEliece 暗号）
A.3. 主要な暗号方式
A.3.1. 暗号方式 1（例：CRYSTALS-KYBER, Classic McEliece）
A.3.2. 暗号方式 2
A.3.3. 暗号方式 3
・・・
A.4. まとめ

3.1.4. 「素因数分解の困難性に関する計算量評価」、「楕円曲線上の離散対数計算の困難性に関する計算量評価」の予測図の更新

「素因数分解の困難性に関する計算量評価」、「楕円曲線上の離散対数計算の困難性に関する計算量評価」の予測図（以下単に「予測図」という。）は公開鍵暗号方式のセキュリティパラメータの選択について検討を行うため、2006 年度に設置された暗号技術調査 WG（公開鍵暗号）において作成された。当時、米国 NIST は「NIST SP 800-57 Part 1 (Revised)(May,2006)」において暗号技術の鍵サイズに関して「80 ビットセキュリティの利用期限を 2010 年まで」と推奨していた。現在では「NIST SP 800-57 Part 1 (Revision 5)(May,2020)」において「112 ビットセキュリティの利用期限を 2030 年まで」と推奨している。

これらの状況を踏まえ、2019 年度暗号技術評価委員会において、今後の予測図の取扱いについて審議し、下記のとおりの対応方針を決定した。

<u>今後の予測図の取扱いについて</u>

これまでの暗号の鍵長の推奨値は、いわゆるムーアの法則（集積回路上のトランジスタ数が 18 ヶ月毎に 2 倍になる）を主な根拠として設定されてきた。ところが、近年、計算機の性能向上は以前と比べて鈍化してきている。今後の予測図のあり方に対して、以下のとおり、対応方針を決定した。

対応方針

〈今後の予測図の取扱い〉

(1) 予測図を従来通り、いわゆるムーアの法則を仮定して外挿線を年度末から20年後まで直線で引き[1]、評価に大きな変動がないと考えられる限りにおいては、安全サイドに倒した評価として当面の間更新していく。なお、予測図は各国・国際標準化機関等により示されている主要な暗号技術の安全性基準と比較すると、より現状に則した評価であり、危殆化時期がそれらよりも先に延びるものとなっている。

〈今後の公開鍵暗号のパラメータ選択〉

(2) 公開鍵暗号のパラメータ選択に関する対応方針については、安全性以外にも相互接続性など、運用上の観点もあるため、暗号技術評価委員会だけではなく、暗号技術検討会、暗号技術活用委員会や関係各所などを含めて検討する。

<u>予測図の更新について</u>

素因数分解問題の困難性および楕円曲線上の離散対数問題の困難性に関する計算量評価に大幅な進展はなかったため、TOP500.org における 2021 年 6 月・11 月のベンチマーク結果を追加して予測図の更新を行った（図 3.2-1 及び図 3.2-2）。

[1] 2020 年度暗号技術評価委員会にて、直線の外挿範囲を「年度末から 20 年後」と変更した。

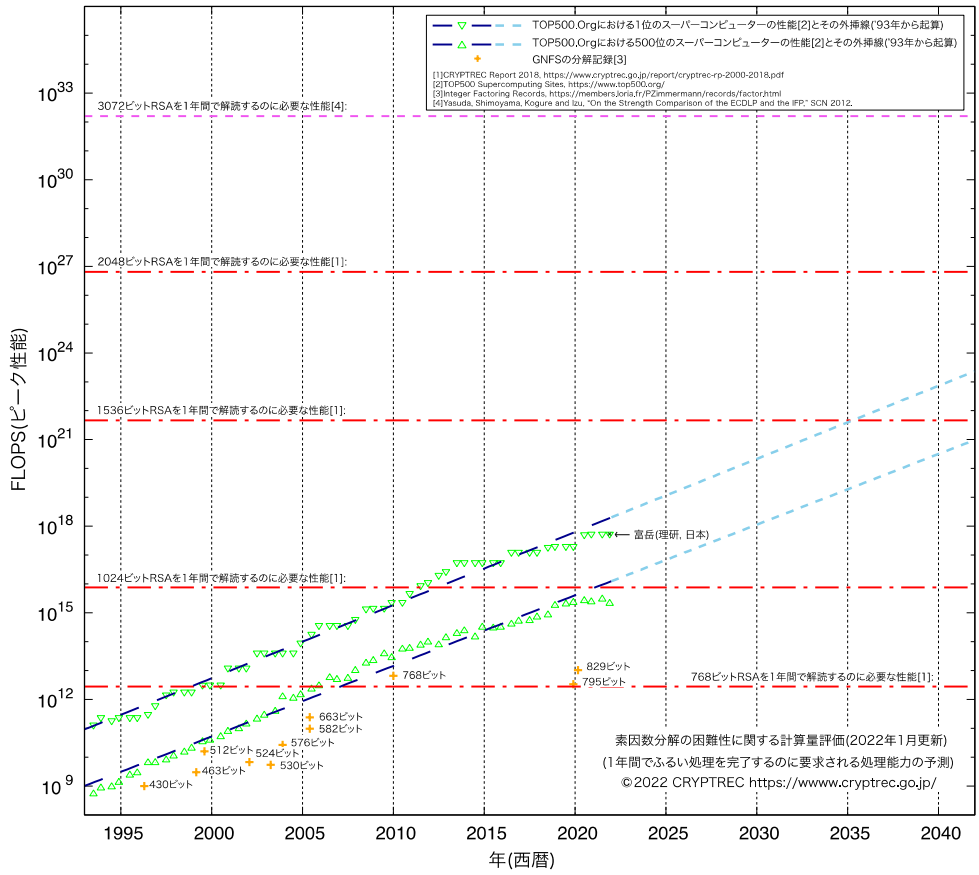

図 3.2-1：素因数分解の困難性に関する計算量評価（2022 年 1 月更新）[2]

[2] スーパーコンピューターの性能の伸びに関する外挿線は僅かであるが鈍化してきている。

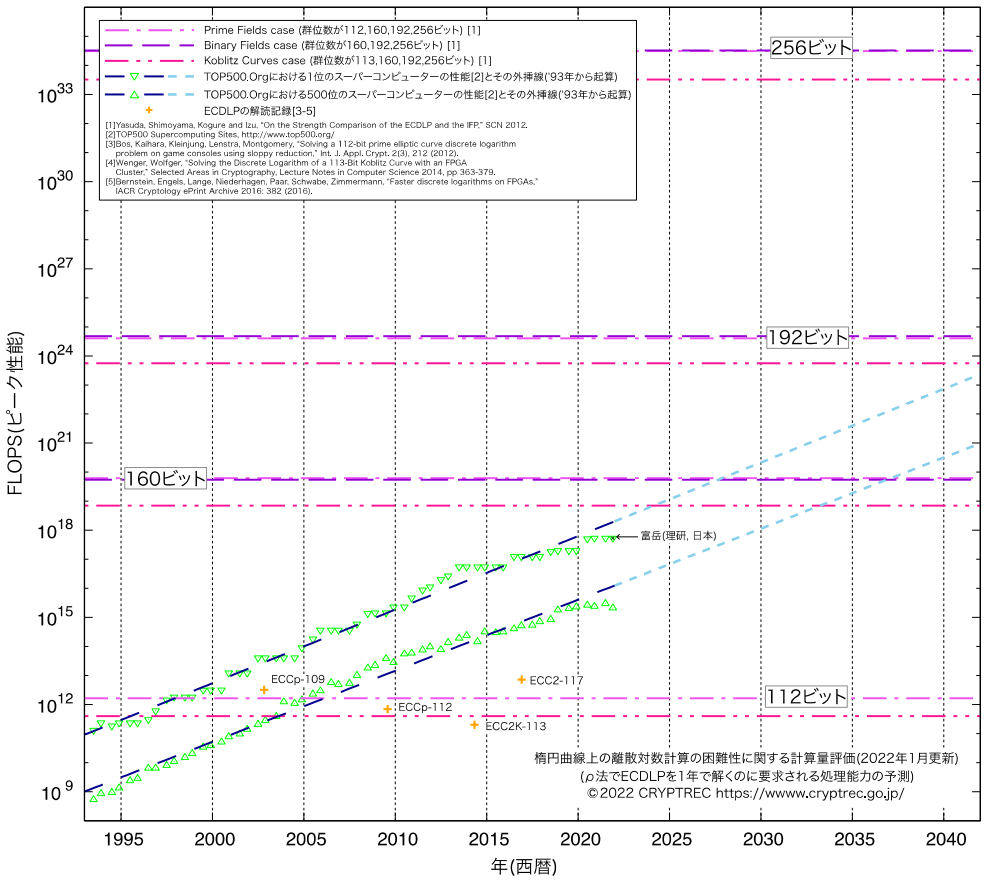

図 3.2-2：楕円曲線上の離散対数計算の困難性に関する計算量評価（2022 年 1 月更新）[3]

[3] スーパーコンピューターの性能の伸びに関する外挿線は僅かであるが鈍化してきている。

3.2　暗号技術調査ワーキンググループ（高機能暗号）

3.2.1　活動報告の概要

公開鍵暗号は、アプリケーションが多様となりその活用が広まっている。その中で、従来の公開鍵暗号よりも機能が向上した高機能暗号を利用してアプリケーションに適用することが有効と考えられている。そこで、高機能暗号ガイドラインを作成するために、2020 年度の暗号技術検討会において、暗号技術評価委員会の下に暗号技術調査ワーキンググループ（高機能暗号）（以下、高機能暗号 WG）を設置することが承認された。

そして、2021 年度暗号技術評価委員会において、2021 年度の高機能暗号 WG の活動として下記 3 点について実施する活動計画が承認された。

(1) 高機能暗号のスコープの明確化
(2) 高機能暗号技術に関する現状調査
(3) 高機能暗号のアプリケーションに関する調査

【2021 年度のスケジュール】

- 2021 年 8 月 3 日　第 1 回高機能暗号 WG
  高機能暗号のスコープの議論により、高機能暗号に関するガイドラインに掲載する高機能暗号のスコープを決定
- 2021 年 12 月 8 日　第 2 回高機能暗号 WG
  高機能暗号に関するガイドラインの目次案を議論し決定
- 2022 年 2 月 8 日　第 3 回高機能暗号 WG
  高機能暗号に関するガイドラインの執筆方針案を議論し決定

3.2.2　委員構成（敬称略）

主査：四方 順司　　（横浜国立大学）
委員：金岡 晃　　（東邦大学）
委員：国井 裕樹　　（セコム）
委員：須賀 祐治　　（インターネットイニシアティブ）
委員：花岡 悟一郎　　（国立研究開発法人産業技術総合研究所）
委員：外園 康智　　（野村総合研究所）
委員：米山 一樹　　（茨城大学）

3.2.3　高機能暗号のスコープの明確化

「高機能暗号」に対して一般的に合意されている定義がない。そこで、本ガイドラインで記載する高機能暗号が何を指すものか定義する必要がある。このため、第 1 回高機能暗号 WG において、本ガイドラインで扱う高機能暗号のスコープを議論した。そして、本ガイドラインでは、高機能暗号を「従来の暗号技術に対して、機能が追加・向上されるなどの優位性を主張する暗号、および、従来の暗号技術では困難であった事象を解決できるなどの新規機能を有することを主張する暗号技術」とした。

さらに、第 1 回高機能暗号 WG において、ガイドラインに掲載する可能性がある高機能暗号を列挙するとともに、高機能暗号を

- 守秘
- 認証・署名
- その他

の 3 つに分類した。そして、調査すべき高機能暗号の対象を

- 守秘
  - ID ベース暗号、属性ベース暗号、放送型暗号、しきい値暗号、準同型暗号、プロキシ再暗号化
- 認証・署名
  - ID ベース署名、属性ベース署名、集約署名・MAC・マルチ署名、グループ署名、リング署名、しきい値署名
- その他
  - マルチパーティ計算－秘密分散ベース、マルチパーティ計算－Garbled Circuit ベース、ゼロ知識証明、検索可能暗号、Private Information Retrieval、Oblivious RAM

の 18 項目とした。

第 1 回高機能暗号 WG の議論に基づき、第 2 回高機能暗号 WG において、ガイドラインの目次案を決定した。

目次案

3.2.4　高機能暗号技術に関する現状調査

高機能暗号に関する現在のアルゴリズムを調査し、現状を情報共有するとともに、将来的に利用される可能性がある高機能暗号を精査する。

第 1 回高機能暗号 WG の中の、高機能暗号のスコープの明確化により定められた、3 分類 18 項目の暗号技術に対し、“技術”について調査することした。調査は各委員が分担して行うこととした。調査内容は、第 2 回、第 3 回高機能暗号 WG において報告された。

【2021 年度のスケジュール】

- 2021 年 8 月 3 日　第 1 回高機能暗号 WG
  高機能暗号の技術に関する現状調査について、作業方針・分担を議論
- 2021 年 12 月 8 日　第 2 回高機能暗号 WG
  高機能暗号の技術に関する現状調査について中間報告
- 2022 年 2 月 8 日　第 3 回高機能暗号 WG
  2021 年度調査内容の確認
  高機能暗号ガイドラインの執筆方針に関する議論

3.2.5　高機能暗号のアプリケーションに関する調査

高機能暗号に関する現在の活用事例、標準化動向を調査し、現状を情報共有するとともに、将来的に利用される可能性がある高機能暗号を精査する。

第 1 回高機能暗号 WG の中の、高機能暗号のスコープの明確化により定められた、3 分類 18 項目の暗号技術に対し、“活用事例”、“標準化動向”について調査することした。調査は各委員が分担して行うこととした。調査内容は、第 2 回、第 3 回高機能暗号 WG において報告された。

また、エンドユーザのヒアリングの候補を以下の 4 件に決定した。

- 秘密分散を利用した医療データ活用
- 検索可能暗号＆属性ベース暗号
- 属性ベース暗号を利用した放送サービスの拡張
- マルチパーティ計算を利用した秘密情報を秘匿したデータ分析

このうち 2 件を選び、2022 年度にヒアリングを行うこととした。ヒアリングは、2022 年度の第 1 回、第 2 回高機能暗号 WG において、発表、質疑形式で行う予定である。

このヒアリング内容は、本ガイドラインの応用事例に掲載することとするが、ヒアリング先である企業、団体、個人の宣伝とはならないように、できるだけ、企業、団体、個人名などを削除できるようにし、ヒアリング先に了解を得ることとした。

【2021 年度のスケジュール】

- 2021 年 8 月 3 日　第 1 回高機能暗号 WG
  高機能暗号のアプリケーションに関する現状調査について、作業方針・分担を議論
  高機能暗号のアプリケーションについて、エンドユーザのヒアリング先の検討
- 2021 年 12 月 8 日　第 2 回高機能暗号 WG
  高機能暗号のアプリケーションに関する現状調査について中間報告
  ヒアリングに関する中間報告
- 2022 年 2 月 8 日　第 3 回高機能暗号 WG
  ヒアリング先に関する候補者選定
  ヒアリング方法について決定
  高機能暗号ガイドラインの執筆方針に関する議論

3.2.6　高機能暗号ガイドラインの執筆方針

想定する読者：

高機能暗号ガイドラインは、高機能暗号を導入することを考えられている技術開発者や、コンソーシアム・標準化団体に関与する技術者などを読者として想定し、暗号理論に精通していない方々を対象として執筆する。

記載する暗号方式の選定基準及び候補：

主要な高機能暗号方式として、対象となる暗号方式は執筆担当委員が選定する。

付録１

CRYPTREC LS-0001-2012R7

電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リスト）

平成２５年３月１日
デジタル庁・総務省・経済産業省
（最終更新：令和4年3月30日）

電子政府推奨暗号リスト

暗号技術検討会[1]及び関連委員会（以下、「CRYPTREC」という。）により安全性及び実装性能が確認された暗号技術[2]について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリスト。なお、利用する鍵長について、「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」[5]の規定に合致しない鍵長を用いた場合には、電子政府推奨暗号リストの暗号技術を利用しているとは見なされないことに留意すること。

技術分類		暗号技術
公開鍵暗号	署名	DSA
		ECDSA
		RSA-PSS(注1)
		RSASSA-PKCS1-v1_5(注1)
	守秘	RSA-OAEP(注1)
	鍵共有	DH
		ECDH
共通鍵暗号	64ビットブロック暗号(注2)	該当なし
	128ビットブロック暗号	AES
		Camellia
	ストリーム暗号	KCipher-2
ハッシュ関数		SHA-256
		SHA-384
		SHA-512
暗号利用モード	秘匿モード	CBC
		CFB
		CTR
		OFB
	認証付き秘匿モード(注13)	CCM
		GCM(注4)
メッセージ認証コード		CMAC
		HMAC
認証暗号		該当なし
エンティティ認証		ISO/IEC 9798-2
		ISO/IEC 9798-3

[1]デジタル庁統括官、総務省サイバーセキュリティ統括官及び経済産業省商務情報政策局長が有識者の参集を求め、暗号技術の普及による情報セキュリティ対策の推進を図る観点から、専門家による意見等を聴取することにより、デジタル庁、総務省及び経済産業省における施策の検討に資することを目的として開催。

[2] 暗号利用モード、メッセージ認証コード、エンティティ認証は、他の技術分類の暗号技術と組み合わせて利用することとされているが、その場合、CRYPTREC暗号リストに掲載されたいずれかの暗号技術と組み合わせること。

[5] CRYPTREC, 暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準, https://www.cryptrec.go.jp/list.html

（注1） 「政府機関の情報システムにおいて使用されている暗号アルゴリズムSHA-1及びRSA1024に係る移行指針」（平成20年４月情報セキュリティ政策会議決定、平成24年10月情報セキュリティ対策推進会議改定）を踏まえて利用すること 。https://www.nisc.go.jp/pdf/policy/general/angou_ikoushishin.pdf
（平成25年３月１日現在）

（注2） CRYPTREC暗号リストにおいて、64ビットブロック暗号により、同一の鍵を用いて暗号化する場合、2^{20}ブロックまで、同一の鍵を用いてCMACでメッセージ認証コードを生成する場合、2^{21}ブロックまでとする。

（注4） 初期化ベクトル長は96ビットを推奨する。

（注13） CRYPTREC暗号リスト掲載のブロック暗号を、認証付き秘匿モードと組み合わせて、「認証暗号」として使うことができる。

推奨候補暗号リスト

CRYPTRECにより安全性及び実装性能が確認され、今後、電子政府推奨暗号リストに掲載される可能性のある暗号技術[3]のリスト。なお、本リストに記載されている暗号技術を利用する際は、「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」[6]の規定に合致する鍵長を用いることが求められることに留意すること。

技術分類		暗号技術
公開鍵暗号	署名	EdDSA
	守秘	該当なし
	鍵共有	PSEC-KEM(注5)
共通鍵暗号	64ビットブロック暗号(注6)	CIPHERUNICORN-E
		Hierocrypt-L1
		MISTY1
	128ビットブロック暗号	CIPHERUNICORN-A
		CLEFIA
		Hierocrypt-3
		SC2000
	ストリーム暗号	Enocoro-128v2
		MUGI
		MULTI-S01(注7)
ハッシュ関数		SHA-512/256
		SHA3-256
		SHA3-384
		SHA3-512
		SHAKE128(注12)
		SHAKE256(注12)
暗号利用モード	秘匿モード	XTS(注17)
	認証付き秘匿モード(注14)	該当なし
メッセージ認証コード		PC-MAC-AES
認証暗号		ChaCha20-Poly1305
エンティティ認証		ISO/IEC 9798-4

（注5） KEM (Key Encapsulating Mechanism) - DEM (Data Encapsulating Mechanism) 構成における利用を前提とする。

（注6） CRYPTREC暗号リストにおいて、64ビットブロック暗号により、同一の鍵を用いて暗号化する場合、2^{20}ブロックまで、同一の鍵を用いてCMACでメッセージ認証コードを生成する場合、2^{21}ブロックまでとする。

（注7） 平文サイズは64ビットの倍数に限る。

（注12） ハッシュ長は256ビット以上とすること。

（注14） CRYPTREC暗号リスト掲載のブロック暗号を、認証付き秘匿モードと組み合わせて、「認証暗号」として使うことができる。

（注17） ブロック暗号には、CRYPTREC暗号リスト掲載128ビットブロック暗号を使う。利用用途はストレージデバイスの暗号化に限り、実装方法はNIST SP800-38Eに従うこと。

[3] 暗号利用モード、メッセージ認証コード、エンティティ認証は、他の技術分類の暗号技術と組み合わせて利用することとされているが、その場合、CRYPTREC暗号リストに掲載されたいずれかの暗号技術と組み合わせること。

[6] CRYPTREC, 暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準, https://www.cryptrec.go.jp/list.html

運用監視暗号リスト

実際に解読されるリスクが高まるなど、推奨すべき状態ではなくなったとCRYPTRECにより確認された暗号技術[4]のうち、互換性維持のために継続利用を容認するもののリスト。互換性維持[7]以外の目的での利用は推奨しない。なお、本リストに記載されている暗号技術を利用する際は、「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」[8]の規定に合致する鍵長を用いることが求められることに留意すること。

技術分類		暗号技術
公開鍵暗号	署名	該当なし
	守秘	RSAES-PKCS1-v1_5（注8）（注9）
	鍵共有	該当なし
共通鍵暗号	64ビットブロック暗号（注15）	3-key Triple DES
	128ビットブロック暗号	該当なし
	ストリーム暗号	該当なし
ハッシュ関数		RIPEMD-160
		SHA-1（注8）
暗号利用モード	秘匿モード	該当なし
	認証付き秘匿モード（注16）	該当なし
メッセージ認証コード		CBC-MAC（注11）
認証暗号		該当なし
エンティティ認証		該当なし

（注8） 「政府機関の情報システムにおいて使用されている暗号アルゴリズムSHA-1及びRSA1024に係る移行指針」（平成20年4月 情報セキュリティ政策会議決定、平成24年10月情報セキュリティ対策推進会議改定）を踏まえて利用すること。https://www.nisc.go.jp/pdf/policy/general/angou_ikoushishin.pdf
（平成25年3月1日現在）

（注9） TLS 1.0, 1.1, 1.2で利用実績があることから当面の利用を認める。

（注11） 安全性の観点から、メッセージ長を固定して利用すべきである。

（注15） CRYPTREC暗号リストにおいて、64ビットブロック暗号により、同一の鍵を用いて暗号化する場合、2^{20}ブロックまで、同一の鍵を用いてCMACでメッセージ認証コードを生成する場合、2^{21}ブロックまでとする。

（注16） CRYPTREC暗号リスト掲載のブロック暗号を、認証付き秘匿モードと組み合わせて、「認証暗号」として使うことができる。

[4] 暗号利用モード、メッセージ認証コード、エンティティ認証は、他の技術分類の暗号技術と組み合わせて利用することとされているが、その場合、CRYPTREC暗号リストに掲載されたいずれかの暗号技術と組み合わせること。
[7] 既に稼働中のシステムやアプリケーション等との間での相互運用を継続すること
[8] CRYPTREC, 暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準, https://www.cryptrec.go.jp/list.html

変更履歴情報

変更日付	変更箇所	変更前の記述	変更後の記述
平成27年3月27日	（注10）	128-bit RC4は、SSL（TLS1.0以上）に限定して利用すること。	互換性維持のために継続利用をこれまで容認してきたが、今後は極力利用すべきでない。SSL/TLSでの利用を含め、電子政府推奨暗号リストに記載された暗号技術への移行を速やかに検討すること。
平成28年3月29日	推奨候補暗号リスト（技術分類：ハッシュ関数）	該当なし	SHA-512/256 SHA3-256 SHA3-384 SHA3-512 SHAKE256（注12）
	（注12）	[新規追加]	ハッシュ長は256ビット以上とすること。
平成29年3月30日	推奨候補暗号リスト（技術分類：ハッシュ関数）	SHA-512/256 SHA3-256 SHA3-384 SHA3-512 SHAKE256（注12）	SHA-512/256 SHA3-256 SHA3-384 SHA3-512 SHAKE128（注12） SHAKE256（注12）
平成30年3月29日	（注2） （注6）	より長いブロック長の暗号が利用できるのであれば、128ビットブロック暗号を選択することが望ましい。	CRYPTREC暗号リストにおいて、64ビットブロック暗号により、同一の鍵を用いて暗号化する場合、2^{20}ブロックまで、同一の鍵を用いてCMACでメッセージ認証コードを生成する場合、2^{21}ブロックまでとする。
	（注15）	[新規追加]	
	電子政府推奨暗号リスト（技術分類：共通鍵暗号）	3-key Triple DES（注3）	該当なし
	（注3）	3-key Triple DESは、以下の条件を考慮し、当面の利用を認める。 1） NIST SP 800-67として規定されていること。 2） デファクトスタンダードとしての位置を保っていること。	[削除]
	運用監視暗号リスト（技術分類：共通鍵暗号）	該当なし	3-Key Triple DES（注15）
	電子政府推奨暗号リスト	[技術分類の新設]	技術分類：認証暗号 暗号技術：該当なし
	推奨候補暗号リスト		技術分類：認証暗号 暗号技術：ChaCha20-Poly1305
	運用監視暗号リスト		技術分類：認証暗号 暗号技術：該当なし

	（注13） （注14） （注16）	[新規追加]	CRYPTREC暗号リスト掲載のブロック暗号を、認証付き秘匿モードと組み合わせて、「認証暗号」として使うことができる。
	電子政府推奨暗号リスト（見出し）	名称	暗号技術
	推奨候補暗号リスト（見出し）		
	運用監視暗号リスト（見出し）		
令和２年12月21日	推奨候補暗号リスト（技術分類：暗号利用モード　秘匿モード）	該当なし	XTS（注17）
	（注17）	[新規追加]	ブロック暗号には、CRYPTREC暗号リスト掲載128ビットブロック暗号を使う。利用用途はストレージデバイスの暗号化に限り、実装方法はNIST SP800-38Eに従うこと。
令和３年4月1日	運用監視暗号リスト（技術分類：共通鍵暗号）	128-bit RC4（注10）	該当なし
	（注10）	互換性維持のために継続利用をこれまで容認してきたが、今後は極力利用すべきでない。TLSでの利用を含め、電子政府推奨暗号リストに記載された暗号技術への移行を速やかに検討すること。	[削除]
令和4年3月30日	文書クレジット	総務省・経済産業省	デジタル庁・総務省・経済産業省
	推奨候補暗号リスト（技術分類：公開鍵暗号　署名）	該当なし	EdDSA
	電子政府推奨暗号リスト（本文）	暗号技術検討会及び関連委員会（以下、「CRYPTREC」という。）により安全性及び実装性能が確認された暗号技術について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリスト。	暗号技術検討会及び関連委員会（以下、「CRYPTREC」という。）により安全性及び実装性能が確認された暗号技術について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリスト。なお、利用する鍵長について、「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」の規定に合致しない鍵長を用いた場合には、電子政府推奨暗号リストの暗号技術を利用しているとは見なされないことに留意すること。

	電子政府推奨暗号リスト（本文）	「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」	「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」[5]
	電子政府推奨暗号リスト（脚注）	該当なし	[5] CRYPTREC, 暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準, https://www.cryptrec.go.jp/list.html
	推奨候補暗号リスト（本文）	CRYPTRECにより安全性及び実装性能が確認され、今後、電子政府推奨暗号リストに掲載される可能性のある暗号技術のリスト。	CRYPTRECにより安全性及び実装性能が確認され、今後、電子政府推奨暗号リストに掲載される可能性のある暗号技術のリスト。なお、本リストに記載されている暗号技術を利用する際は、「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」の規定に合致する鍵長を用いることが求められることに留意すること。
	推奨候補暗号リスト（本文）	「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」	「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」[6]
	推奨候補暗号リスト（脚注）	該当なし	[6] CRYPTREC, 暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準, https://www.cryptrec.go.jp/list.html
	運用監視暗号リスト（本文）	実際に解読されるリスクが高まるなど、推奨すべき状態ではなくなったとCRYPTRECにより確認された暗号技術のうち、互換性維持のために継続利用を容認するもののリスト。互換性維持以外の目的での利用は推奨しない。	実際に解読されるリスクが高まるなど、推奨すべき状態ではなくなったとCRYPTRECにより確認された暗号技術のうち、互換性維持のために継続利用を容認するもののリスト。互換性維持以外の目的での利用は推奨しない。なお、本リストに記載されている暗号技術を利用する際は、「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」の規定に合致する鍵長を用いることが求められることに留意すること。
	運用監視暗号リスト（本文）	互換性維持	互換性維持[7]
	運用監視暗号リスト（脚注）	該当なし	[7] 既に稼働中のシステムやアプリケーション等との間での相互運用を継続すること
	運用監視暗号リスト（本文）	「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」	「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」[8]
	運用監視暗号リスト（脚注）	該当なし	[8] CRYPTREC, 暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準, https://www.cryptrec.go.jp/list.html

付録２

CRYPTREC 暗号リスト掲載暗号技術の問合せ先一覧

電子政府推奨暗号リスト

1. 公開鍵暗号

暗号名	DSA
関連情報	仕様
・ NIST Federal Information Processing Standards Publication 186-4 (July 2013), Digital Signature Standard (DSS) で規定されたもの。 ・ 参照 URL https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf	

暗号名	ECDSA (Elliptic Curve Digital Signature Algorithm)
関連情報 1	公開ホームページ
和文： https://www.fujitsu.com/jp/about/research/external-activities/crypto/ 英文： https://www.fujitsu.com/global/about/research/external-activities/crypto/ ・ 参照 URL SEC 1: Elliptic Curve Cryptography (September 20, 2000 Version 1.0) https://www.secg.org/SEC1-Ver-1.0.pdf	
問い合わせ先 1	
富士通株式会社 電子政府推奨暗号 問い合わせ窓口 E-MAIL：fj-soft-crypto-ml@dl.jp.fujitsu.com	
関連情報 2	仕様
・ ANS X9.62-2005, Public Key Cryptography for The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA) で規定されたもの。 ・ 参照 URL https://www.x9.org/	

暗号名	RSA Public-Key Cryptosystem with Probabilistic Signature Scheme (RSA-PSS)
関連情報	仕様　公開ホームページ
	・ PKCS#1 RSA Cryptography Standard Version 2.2 ・ 参照 URL https://tools.ietf.org/html/rfc8017 和文：なし

暗号名	RSASSA-PKCS1-v1_5
関連情報	仕様　公開ホームページ
	・ PKCS#1 RSA Cryptography Standard Version 2.2 ・ 参照 URL https://tools.ietf.org/html/rfc8017 和文：なし

暗号名	RSA Public-Key Cryptosystem with Optimal Asymmetric Encryption Padding (RSA-OAEP)
関連情報	仕様　公開ホームページ
	・ PKCS#1 RSA Cryptography Standard Version 2.2 ・ 参照 URL https://tools.ietf.org/html/rfc8017 和文：なし

暗号名	DH
関連情報 1	仕様
	・ ANSI X9.42-2003, Public Key Cryptography for The Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography で規定されたもの。 ・ 参照 URL https://www.x9.org/
関連情報 2	仕様
	・ NIST Special Publication 800-56A Revision 2 (May 2013), Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography において、FCC DH プリミティブとして規定されたもの。 ・ 参照 URL https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar2.pdf

暗号名	ECDH (Elliptic Curve Diffie-Hellman Scheme)
関連情報 1	公開ホームページ
和文： https://www.fujitsu.com/jp/about/research/external-activities/crypto/ 英文： https://www.fujitsu.com/global/about/research/external-activities/crypto/ ・ 参照 URL SEC 1: Elliptic Curve Cryptography (September 20, 2000 Version 1.0) https://www.secg.org/SEC1-Ver-1.0.pdf	
問い合わせ先 1	
富士通株式会社 電子政府推奨暗号 問い合わせ窓口 E-MAIL：fj-soft-crypto-ml@dl.jp.fujitsu.com	
関連情報 2	仕様
・ NIST Special Publication SP 800-56A Revision 2(May 2013), Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography において、C(2e,0s,ECC CDH)として規定されたもの。 ・ 参照 URL https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar2.pdf	

2. 共通鍵暗号

暗号名	AES
関連情報	仕様
・ NIST FIPS PUB 197, Specification for the ADVANCED ENCRYPTION STANDARD (AES), November 26, 2001 ・ 参照 URL https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf	

暗号名	Camellia
関連情報	公開ホームページ
和文：https://info.isl.ntt.co.jp/crypt/camellia/ 英文：https://info.isl.ntt.co.jp/crypt/eng/camellia/	
問い合わせ先	〒180-8585 東京都武蔵野市緑町 3-9-11
日本電信電話株式会社　NTT 社会情報研究所 Camellia 問い合わせ窓口　担当 E-MAIL: camellia-ml@hco.ntt.co.jp　FAX:0422-59-2971	

暗号名	KCipher-2
関連情報	公開ホームページ 和文：https://www.kddi-research.jp/products/kcipher2.html 英文：https://www.kddi-research.jp/english/products/kcipher2.html
問い合わせ先	〒356-8502 埼玉県ふじみ野市大原 2-1-15 株式会社 KDDI 総合研究所 執行役員　清本 晋作 TEL:049-278-7638, FAX:049-278-7510 E-MAIL: kiyomoto@kddi-research.jp

3. ハッシュ関数

暗号名	SHA-256, SHA-384, SHA-512
関連情報	仕様 ・ NIST FIPS PUB 180-4, Secure Hash Standard (SHS), August 2015 ・ 参照 URL https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf

4. 暗号利用モード(秘匿モード)

暗号名	CBC, CFB, CTR, OFB
関連情報	仕様 ・ NIST SP 800-38A, Recommendation for Block Cipher Modes of Operation: Methods and Techniques 2001 Edition ・ 参照 URL https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf

5. 暗号利用モード(認証付き秘匿モード)

暗号名	CCM
関連情報	仕様
	・ NIST SP 800-38C, Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, May 2004 (errata update 07-20-2007; corrected value of parameter B on p.19) ・ 参照 URL https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38c.pdf

暗号名	GCM
関連情報	仕様
	・ NIST SP 800-38D, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, November 2007 ・ 参照 URL https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38d.pdf

6. メッセージ認証コード

暗号名	CMAC
関連情報	仕様
	・ NIST FIPS SP 800-38B, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, May 2005 (Updated Oct. 2016) ・ 参照 URL https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38b.pdf

暗号名	HMAC
関連情報	仕様
	・ NIST FIPS PUB 198-1, The Keyed-Hash Message Authentication Code (HMAC), July 2008 ・ 参照 URL https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.198-1.pdf

7. エンティティ認証

暗号名	ISO/IEC 9798-2
関連情報	仕様
	・ ISO/IEC 9798-2:2008, Information technology - Security techniques - Entity Authentication - Part 2: Mechanisms using symmetric encipherment algorithms, 2008. 及び ISO/IEC 9798-2:2008/Cor.1:2010, Information technology - Security techniques - Entity Authentication - Part 2: Mechanisms using symmetric encipherment algorithms. Technical Corrigendum 1, 2010 で規定されたもの。なお、同規格書は日本規格協会(https://www.jsa.or.jp/)から入手可能である。

暗号名	ISO/IEC 9798-3
関連情報	仕様
	・ ISO/IEC 9798-3:1998, Information technology - Security techniques - Entity Authentication - Part 3: Mechanisms using digital signature techniques, 1998. 及び ISO/IEC 9798-3:1998/Amd.1:2010, Information technology - Security techniques - Entity Authentication - Part 3: Mechanisms using digital signature techniques. Amendment 1, 2010 で規定されたもの。なお、同規格書は日本規格協会(https://www.jsa.or.jp/)から入手可能である。

推奨候補暗号リスト

1. 公開鍵暗号

暗号名	PSEC-KEM Key agreement
関連情報	公開ホームページ 和文：https://info.isl.ntt.co.jp/crypt/psec/ 英文：https://info.isl.ntt.co.jp/crypt/eng/psec/
問い合わせ先	〒180-8585 東京都武蔵野市緑町 3-9-11 日本電信電話株式会社　NTT 社会情報研究所 PSEC-KEM 問い合わせ窓口　担当 E-MAIL: publickey-ml@hco.ntt.co.jp　FAX: 0422-59-2971

2. 共通鍵暗号

暗号名	CIPHERUNICORN-E
関連情報	公開ホームページ 和文：https://jpn.nec.com/secureware/sdk/cipherunicorn-e.html 英文：https://jpn.nec.com/secureware/sdk/cipherunicorn-e-en.html
問い合わせ先	〒211-8666 神奈川県川崎市中原区下沼部 1753 日本電気株式会社　サイバーセキュリティ事業統括部 E-MAIL: nec-pki@security.jp.nec.com

暗号名	Hierocrypt-L1
関連情報	公開ホームページ 和文：https://www.global.toshiba/jp/technology/corporate/rdc/security.html 英文：https://www.global.toshiba/ww/technology/corporate/rdc/security.html
問い合わせ先	〒212-8582 神奈川県川崎市幸区小向東芝町 1 株式会社東芝 研究開発センター サイバーセキュリティ技術センター 電子政府推奨暗号 問い合わせ窓口 E-MAIL: rdc-crypt-info@ml.toshiba.co.jp

暗号名	MISTY1
関連情報	公開ホームページ
https://www.mitsubishielectric.co.jp/corporate/randd/list/info_tel/a41/misty01_b.html	
問い合わせ先	〒247-8520 神奈川県鎌倉市上町屋 325 番地 三菱電機株式会社 インフォメーションシステム統括事業部 MISTY1 問合せ窓口 E-MAIL：misty1_info@mf.MitsubishiElectric.co.jp

暗号名	CIPHERUNICORN-A
関連情報	公開ホームページ 和文：https://jpn.nec.com/secureware/sdk/cipherunicorn-a.html 英文：https://jpn.nec.com/secureware/sdk/cipherunicorn-a-en.html
問い合わせ先	〒211-8666 神奈川県川崎市中原区下沼部 1753 日本電気株式会社　サイバーセキュリティ事業統括部 E-MAIL: nec-pki@security.jp.nec.com

暗号名	CLEFIA
関連情報	公開ホームページ 和文：https://www.sony.co.jp/Products/cryptography/clefia/ 英文：https://www.sony.net/Products/cryptography/clefia/
問い合わせ先	ソニー株式会社 CLEFIA 問い合わせ窓口 E-MAIL: clefia-q@jp.sony.com

暗号名	Hierocrypt-3
関連情報	公開ホームページ 和文：https://www.global.toshiba/jp/technology/corporate/rdc/security.html 英文：https://www.global.toshiba/ww/technology/corporate/rdc/security.html
問い合わせ先	〒212-8582 神奈川県川崎市幸区小向東芝町 1 株式会社東芝 研究開発センター サイバーセキュリティ技術センター 電子政府推奨暗号 問い合わせ窓口 E-MAIL: rdc-crypt-info@ml.toshiba.co.jp

暗号名	SC2000
関連情報	公開ホームページ
和文： https://www.fujitsu.com/jp/about/research/external-activities/crypto/ 英文： https://www.fujitsu.com/global/about/research/external-activities/crypto/	
問い合わせ先	富士通株式会社 電子政府推奨暗号 問い合わせ窓口
E-MAIL： fj-soft-crypto-ml@dl.jp.fujitsu.com	

暗号名	MUGI
関連情報	公開ホームページ
和文：https://www.hitachi.co.jp/rd/yrl/crypto/mugi/ 英文：https://www.hitachi.com/rd/yrl/crypto/mugi/	
問い合わせ先	
株式会社日立製作所　情報セキュリティリスク統括本部 情報セキュリティマネジメント本部　サイバーリスクマネジメント部 担当部長 栗田 博司 TEL：070-3854-4514, FAX ： 03-5471-2343 E-MAIL：hiroshi.kurita.wp@hitachi.com	

暗号名	Enocoro-128v2
関連情報	公開ホームページ
和文:https://www.hitachi.co.jp/rd/yrl/crypto/enocoro/index.html 英文:https://www.hitachi.com/rd/yrl/crypto/enocoro/index.html	
問い合わせ先	
株式会社日立製作所　研究開発グループ　サービスシステムイノベーションセンタ セキュリティ・トラスト研究部　主任研究員　渡辺 大 E-MAIL: dai.watanabe.td@hitachi.com	

暗号名	MULTI-S01
関連情報	公開ホームページ 和文：https://www.hitachi.co.jp/rd/yrl/crypto/s01/ 英文：https://www.hitachi.com/rd/yrl/crypto/s01/
問い合わせ先	株式会社日立製作所　情報セキュリティリスク統括本部 情報セキュリティマネジメント本部　サイバーリスクマネジメント部 担当部長 栗田 博司 TEL：070-3854-4514, FAX ： 03-5471-2343 E-MAIL：hiroshi.kurita.wp@hitachi.com

3. ハッシュ関数

暗号名	SHA-512/256
関連情報	仕様 ・ NIST FIPS PUB 180-4, Secure Hash Standard (SHS), August 2015 ・ 参照 URL https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf

暗号名	SHA3-256, SHA3-384, SHA3-512, SHAKE128, SHAKE256
関連情報	仕様 ・ NIST FIPS PUB 202, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, August 2015 ・ 参照 URL https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf

4. 暗号利用モード（秘匿モード）

暗号名	XTS
関連情報	仕様 ・ NIST SP 800-38E, Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices, January 2010 ・ 参照 URL https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38e.pdf

5. メッセージ認証コード

暗号名	PC-MAC-AES
関連情報	仕様
参照 URL：https://jpn.nec.com/rd/crl/code/research/pcmacaes.html	
問い合わせ先	〒211-8666 神奈川県川崎市中原区下沼部 1753 日本電気株式会社　セキュアシステム研究所　主席研究員 峯松 一彦 TEL：080-8823-8882 E-MAIL: k-minematsu@nec.com

6. 認証暗号

暗号名	ChaCha20-Poly1305
関連情報	仕様 ・ Internet Research Task Force (IRTF), Request for Comments (RFC) 7539, ChaCha20 and Poly1305 for IETF Protocols, May 2015 で規定されたもの。 ・ 参照 URL https://tools.ietf.org/html/rfc7539

7. エンティティ認証

暗号名	ISO/IEC 9798-4
関連情報	仕様 ・ ISO/IEC 9798-4:1999, Information technology - Security techniques - Entity Authentication - Part 4: Mechanisms using a cryptographic check function, 1999.及び ISO/IEC 9798-4:1999/Cor.1:2009, Information technology - Security techniques - Entity Authentication - Part 3: Mechanisms using a cryptographic check function. Technical Corrigendum 1, 2009 で規定されたもの。なお、同規格書は日本規格協会(https://www.jsa.or.jp/)から入手可能である。

運用監視暗号リスト

1. 公開鍵暗号

暗号名	RSAES-PKCS1-v1_5
関連情報	仕様
	・ PKCS#1 RSA Cryptography Standard Version 2.2 ・ 参照 URL https://tools.ietf.org/html/rfc8017 和文：なし

2. 共通鍵暗号

暗号名	Triple DES
関連情報	仕様
	・ NIST SP 800-67 Revision 2, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, November 2017 ・ 参照 URL https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-67r2.pdf

3. ハッシュ関数

暗号名	RIPEMD-160
関連情報	仕様
・ 参照 URL https://www.esat.kuleuven.ac.be/~bosselae/ripemd160.html	

暗号名	SHA-1
関連情報	仕様
・ NIST FIPS PUB 180-4, Secure Hash Standard (SHS), August 2015 ・ 参照 URL https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf	

4. メッセージ認証コード

暗号名	CBC-MAC
関連情報	仕様
・ ISO/IEC 9797-1:1999, Information technology - Security techniques - Message Authentication Codes(MACs) - Part 1: Mechanisms using a block cipher, 1999 で規定されたもの。なお、同規格書は日本規格協会(https://www.jsa.or.jp/)から入手可能である。	

付録３

「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（エグゼクティブサマリー）[*1]

伊藤 竜馬
（国立研究開発法人情報通信研究機構）

2022 年 3 月

[*1] 原文は、CRYPTREC EX-3101-2021
https://www.cryptrec.go.jp/exreport/cryptrec-ex-3101-2021.pdf
から入手可能。なお、本エグゼクティブサマリーでの章立てについては原文のとおり記載している。

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。

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 *Symposium on Cryptography and Information Security, 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４

ディジタル署名アルゴリズム EdDSAの実装性能調査 (エグゼクティブサマリー)*1

株式会社インフォーズ
2021年12月

*1 原文は、CRYPTREC EX-3102-2021
https://www.cryptrec.go.jp/exreport/cryptrec-ex-3102-2021.pdf
から入手可能。

エグゼクティブサマリー

本報告書はディジタル署名Edwards-curve Digital Signature Algorithm (EdDSA)の実装性能に関する評価結果を報告するものである.

EdDSAとは, 2011年9月にDaniel J. Bernsteinらによって“High-speed high-security signatures”[1]で発表され, Internet Research Task Force (IRTF) のRequest for Comments (RFC) 8032 [2]で規定されるディジタル署名のことであり, 有限体上のtwisted Edwards曲線 [3] [4]といわれる楕円曲線上のSchnorr署名 [5] [6]の署名内部乱数（ノンス）を署名者の秘密情報と署名されるメッセージのハッシュ値に置き換えた確定的 (deterministic) 版のSchnorr署名である. EdDSAで推奨されるtwisted Edwards曲線はIRTFのRFC7748 [7]で規定されるものでありedwards25519, edwards448と記述される.

以下, 評価結果の概要を述べる.

- EdDSAの技術的な特徴として以下を確認できた.
  - EdDSAはECDSAと同様に射影座標系を使用可能であるため, 有限体上の乗法逆元の演算を用いずに演算可能であることから, 高速な実装が可能である.
  - EdDSAで推奨されるtwisted-Edwards曲線は無限遠点を例外的に扱うための分岐が不要なため, ECDSAで使われるWeierstrass形式の楕円曲線と比較して実装しやすい.
  - EdDSAで推奨されるEdwards楕円曲線は, 異なる点の加算と同一の点の加算(2倍算)を同じ処理で計算できるため, 実装するアルゴリズムが1つでよく, 点が異なるかどうかの条件分岐を考慮する必要がないため, Weierstrass形式の楕円曲線と比較してSide Channel Attack (SCA) 対策に有利である.

- EdDSAの標準化での採用状況としては, RFC8032 [2]として標準化され, Draft版を含め参照する標準も増えつつあることが分かった. Open Source Software (OSS) での採用状況としては, 少なくとも20件のOSSの暗号ライブラリが採用していることが分かった. ただし, 224ビットセキュリティのEdDSAであるEd448は128ビットセキュリティのEdDSAであるEd25519よりも採用数は少なかった. 今後, EdDSAの実装の品質や高速化技法が洗練され, 安全性の高いEd448も性能が高まると採用が進むことが期待できる.

- 公開されている第三者の測定結果および本調査での実装評価として, 4つのC言語実装および2つのJava言語実装のOSSに対して, Windows, Linux, Macの環境でそれぞれでの性能測定を実施した.その結果は以下のとおりである.
  - Ed255519

- 鍵ペア生成
  - ほぼ全ての環境においてECDSA P-256より高スループットであった.
- 署名生成
  - 半数以上の環境でECDSA P-256より高スループットであり，それ以外の環境において半分以下のスループットとなることはなかった.
- 署名検証
  - ほぼ全てのECDSA P-256より高スループットであった.

➢ Ed448

- 鍵ペア生成
  - ほぼ全ての環境でECDSA P-384より高スループットであり，全環境でECDSA P-521より高スループットであった.
- 署名生成
  - ほぼ全ての環境でECDSA P-384より高スループットであり，全環境でECDSA P-521より高スループットであった.
- 署名検証
  - ほぼ全ての環境でECDSA P-384より高スループットであり，全環境でECDSA P-521より高スループットであった.

以上から，EdDSAは，方式そのものに安全性担保，高速化，実装がしやすい特性があると評価でき，実際にOSSとして実装された暗号ライブラリの性能は，同程度の安全性のECDSAや高い安全性のECDSAと比べても遜色のないものであった．実装されたOSSの品質，高速化技法は洗練されているとは言い切れない部分もあるが，歴史のあるECDSAと比べても性能で劣ることはないと考えられる.

参考文献

[1] Daniel J. Bernstein, Niels Duif, Tanja Lange, Peter Schewabe , Bo-Yin Yang, “High-speed high-security signatures,” 2011.

[2] Internet Research Task Force (IRTF), “RFC8032 Edwards-Curve Digital Signature Algorithm (EdDSA),” 2017.

[3] Harold M. Edwards, “A normal form for elliptic curves,” In Bulletin of the American Mathematical Society, 2007.

[4] Daniel J. Bernstein , Tanja Lange, “Faster addition and doubling on elliptic curves,” 2007.

[5] Claus P. Schnorr, “Efficient Identification and Signatures for Smart Cards,” 1990.

[6] 新保 淳, 岡田 光司 , 丹羽 朗人, “ECDSA 評価報告書,” 2001.

[7] Internet Research Task Force (IRTF), “RFC7748 Elliptic Curves for Security,” 2016.

[8] 藤﨑 英一郎, “ディジタル署名 EdDSA の構成の安全性に関する調査および評価,” 2020.

[9] 安田 雅哉, “ディジタル署名EdDSAで使われている曲線の安全性に関する調査及び評価,” 2020.

[10] Steven D. Galbraith, “CRYPTREC Review of EdDSA,” 2020.

[11] John M. Pollard, “Monte carlo methods for index computation (mod p),” *Mathematics of computation, 第32巻 143号,* p. 918-924, 7 1978.

[12] National Institute of Standards and Technology, “FIPS Pub 186-5 (Draft) Digital Signature Standard (DSS),” 2019.

[13] National Institute of Standards and Technology, “SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions FIPS PUB 202,” 2015.

[14] Internet Engineering Task Force (IETF), “RFC6234 US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF),” 2011.

[15] Huseyin Hisil, Kenneth Koon-Ho Wong, Gary Carter , Ed Dawson, “Twisted Edwards Curves Revisited,” Springer-Verlag, 2008.

[16] VAMPIRE lab, “SUPERCOP,” https://bench.cr.yp.to/supercop.html.

付録５

学会等での主要攻撃論文発表等一覧

目次

1. 具体的な暗号の攻撃に関する発表

表 1 に具体的な暗号の攻撃に関する発表のリストをカテゴリー別に示す。★は電子政府推奨暗号の安全性に直接関わる技術動向、☆はその他の注視すべき技術動向である。

表 1 具体的な暗号の攻撃に関する発表

	公開鍵暗号	頁
	SimS: a Simplification of SiGamal [PQCrypto 2021]	107
	A Practical Adaptive Key Recovery Attack on the LGM (GSW-like) Cryptosystem [PQCrypto 2021]	109
	How to Meet Ternary LWE Keys [CRYPTO2021]	110
	Improved torsion-point attacks on SIDH variants [CRYPTO 2021]	110
★	Partial Key Exposure Attack on Short Secret Exponent CRT-RSA [Asiacrypt2021]	125
☆	On the hardness of the NTRU problem [Asiacrypt 2021]	124
	Fault-Injection Attacks against NIST's Post-Quantum Cryptography Round 3 KEM Candidates [Asiacrypt 2021]	125
	A formula for disaster: a unified approach to elliptic curve special-point-based attacks [Asiacrypt 2021]	126
	On the non-tightness of measurement-based reductions for key encapsulation mechanism in the quantum random oracle model [Asiacrypt 2021]	127
	NTRU Fatigue: How Stretched is Overstretched? [Asiacrypt 2021]	133
	Faster Dual Lattice Attacks for Solving LWE -- with applications to CRYSTALS [Asiacrypt 2021]	133
	Lattice sieving via quantum random walks [Asiacrypt 2021]	134
	A Systematic Approach and Analysis of Key Mismatch Attacks on Lattice-Based NIST Candidate KEMs [Asiacrypt 2021]	134
	ブロック暗号	
	Linear Cryptanalysis of FF3-1 and FEA [CRYPTO 2021]	109
☆	Differential-Linear Cryptanalysis from an Algebraic Perspective [CRYPTO 2021]	112
	Cryptanalysis of Full LowMC and LowMC-M with Algebraic Techniques [CRYPTO 2021]	113
	Meet-in-the-Middle Attacks Revisited: Key-recovery, Collision, and Preimage Attacks [CRYPTO 2021]	113
★	New Representations of the AES Key Schedule [Eurocrypt 2021]	117
★	Automatic Search of Meet-in-the-Middle Preimage Attacks on AES-like Hashing [Eurocrypt 2021]	118
	Rotational Cryptanalysis From a Differential-Linear Perspective - Practical Distinguishers for Round-reduced FRIET, Xoodoo, and Alzette [Eurocrypt 2021]	119

2. PQCrypto 2021 の発表

2.1. PQCrypto 2021 の発表(1 日目)

・Decoding Supercodes of Gabidulin Codes and Applications to Cryptanalysis [PQCrypto 2021]

Maxime Bombar, Alain Couvreur

本論文は、Gabidulin符号の復号について述べ、復号半径の大幅な減少と引き換えに、通常の復号器を Gabidulin 符号の任意のスーパーコードに拡張する方法を示している。この復号器を用いて、ランクによる距離を用いた暗号方式である RAMESSES と LIGA に対する多項式時間攻撃を提供する。

・ Classical and Quantum algorithms for generic Syndrome Decoding problems and applications to the Lee metric [PQCrypto 2021]

Thomas Debris-Alazard, André Chailloux, Simona Etinski

コードベース暗号の安全性は、通常、ハミング重みに対するシンドローム復号(Syndrome Decoding、SD)問題の困難性に依存している。最も優れた汎用アルゴリズムは、いずれもPrangeによる古いアルゴリズムの改良版であり、Information Set Decoding (ISD) アルゴリズムの名で知られている。

本論文では、基礎となる重み関数と SD のアルファベットサイズを変更することにより、ISD アルゴリズムの適用範囲を拡大することが目的である。より正確には、ISD の枠組みで Wagner のアルゴリズムを使うことで、広範囲の重み関数に対する SD を解く方法が示される。また、ISD アルゴリズムの漸近的な複雑さを、古典的な場合と量子的な場合の両方について計算される。次に、現在注目されている Lee 測度に対して、著者らの結果が適用される。復号が最も困難と思われる Lee ウェイトに対するSDのパラメータを提供することにより、著者らの研究は、特に量子敵対者に対する符号ベースの暗号システムの設計とその安全性解析に対するいくつかの応用を持つことが報告される。

・Improving Thomae-Wolf Algorithm for Solving Underdetermined Multivariate Quadratic Polynomial Problem [PQCrypto 2021]

Hiroki Furue, Shuhei Nakamura and Tsuyoshi Takagi

多変数二次多項式問題(MQ 問題)は、ポスト量子暗号における基本的な計算問題である。有限体 Fq 上の n 変数における m 個の二次多項式の MQ 問題を MQ(q, n, m)と表す。PKC 2012 では、Thomae と Wolf により、劣決定(すなわち n>m の場合)の MQ(2^r, n, m)を解く効率的なアルゴリズムが提案された(TW アルゴリズム)。具体的には、α 個の二次多項式の交差積項を線形化により除去することで、MQ(2^r, n, m)は MQ(2^r, m − k − α, m − α)(k は TW アルゴリズム適用後のハイブ

リッドアプローチで固定される変数の数)に還元することが可能である。そして、このアルゴリズムは、α のうち最大の線形化係数$\alpha = \lfloor n/m \rfloor - 1$に対して最小の MQ 問題をもたらす。

本論文では、ハイブリッドアプローチと TW アルゴリズムを組み合わせることにより、線形化係数 α を改善するアルゴリズムが提案される。提案アルゴリズムは、MQ(2^r, n, m)を、線形化係数$\alpha_k = \lfloor (n-k)/(m-k) \rfloor - 1$で、MQ($2^r$, m-k-$\alpha_k$, m-$\alpha_k$)に削減することが可能である。$\alpha_k \geq \alpha$ なので、提案アルゴリズムはいくつかのパラメータセットに対して TW アルゴリズムよりも効率的である。さらにバイナリケース(r = 1)の場合に、自明ではない改良されたアルゴリズムを提供し、適切な k に対してより大きな線形化係数$\beta_k = \lfloor (n-1)/(m-k-1) \rfloor - 1$を与える。

・On the Effect of Projection on Rank Attacks in Multivariate Cryptography [PQCrypto 2021]

Morten øygarden, Daniel Smith-Tone and Javier Verbel

多変数暗号方式 HFEv-は、かつてポスト量子署名システムの有望な候補とみなされていた。2000 年代初頭に初めて提案されたこの方式は、現在進行中の NIST のポスト量子標準化プロセスの第 3 ラウンドに進出している。2020 年後半、この方式は Tao, Petzoldt, そして Ding による効率的なランク攻撃を受けた。本論文では、この最近のランク攻撃がプロジェクション変形(projection modification)によってどのような影響を受けるかを検証している。この変形は、署名方式 PFLASH を先行者の攻撃から保護するために導入された。本論文では、新しい攻撃の下での projected HFEv- (pHFEv-)と PFLASH のランクの上界を示した。著者らが行った実験結果ではこれらの値に近い結果を得ている。このプロジェクション手法は、最近の暗号解読から守るための有用なツールになりうると結論付ける。

・Quantum Key Search for Ternary LWE [PQCrypto 2021]

Iggy van Hoof, Elena Kir shanova, Alexander May

3 値 LWE(ternary LWE)、すなわち秘密と誤差ベクトルの係数を{-1, 0, 1}から取った LWE は、NTRU 型暗号や BLISS や GLP などの一部の署名方式でよく使われている。

本論文は、3 値 LWE に対する量子組み合わせ攻撃について検討する。提案アルゴリズムは、Magniez-Nayak-Roland-Santha の量子ウォークの枠組みをベースに、部分和問題のアルゴリズムに登場する表現技法(representation technique)と呼ばれる組合せ論的な手法を 3 値 LWE に適用している。LWE 鍵の探索空間を S で表すと、表現攻撃の漸近的計算量は$S^{0.24}$(古典)から$S^{0.19}$(量子)にまで低下する。これは、NTRU-HRSS [CHES 2017] や NTRU Prime [SAC 2017] などの具体的な NTRU インスタンスに対する顕著な攻撃速度の向上となる。提案されたアルゴリズムは、NTRU や他の 3 値 LWE ベースのスキームの現在の安全性を損なうものではないが、LWE に対するハイブリッド攻撃内部の組み合わせサブルーチンの改良のための基礎となりうる。

・A Fusion Algorithm for Solving the Hidden Shift Problem in Finite Abelian Groups [PQCrypto 2021]

Wouter Castryck, Ann Dooms, Carlo Emerencia, Alexander Lemmens

有限アーベル群 G における隠れシフト問題に関する論文である。

2014 年の Friedl, Ivanyos, Magniez, Santha and Sen による結果から、任意の(小さな)固定整数 m > 0 に対して、任意の有限アーベル群 G における隠れシフト問題を時間計算量 $poly(log\,|G|) \cdot 2O\left(\sqrt{m|G|}\right)$で解く量子アルゴリズムが存在することが分かる。これは一方向性群作用をもつ等質空間に対する Pohlig-Hellman 型の控えめな主張と見なすことができる。

本論文では、m = 2t*p(t は任意の非負整数、p は任意の素数)で同じ実行時間を達成するやや単純なアルゴリズムで、さらにメモリ要件はおおむね量子ランダムアクセス古典メモリの観点に収まるものを構成する。実際に、格納する必要がある量子ビットの量は poly(log |G|)である。著者らは、Peikert による Kuperberg の平行ふるいの適応を任意の有限アーベル群に拡張し、前述の時間で商群 G/(2t*p)G の隠れシフト問題へと問題を帰着する。帰着された問題は、Friedl らによる p-ねじれ群に対する方法と、Bonnetain と Naya-Plasencia による 2t-ねじれ群に対する方法を組み合わせることにより、多項式時間で取り組むことができる。

・Differential Power Analysis of the Picnic Signature Scheme [PQCrypto 2021]

Tim Gellersen, Okan Seker, Thomas Eisenbarths

本論文では、NIST 耐量子コンペティションの候補である Picnic 署名スキームの差分サイドチャネル解析を初めて行ったものである。LowMC ブロック暗号のマルチパーティ実装(MPC-LowMC)のサイドチャネル解析に成功し、アルゴリズムの 2 つの異なる部分を利用することでサイドチャネル情報から秘密鍵全体を復元する方法を示した。LowMC の鍵回復により、Picnic の署名を偽造することができる。本論文では、FRDM-K66F 開発ボードで実行される NIST 参照実装を対象とした。鍵の復元は 1000 以下の LowMC トレースで成功するが、これは観測された 30 個以下の Picnic 署名から得ることができるものである。

2.2. PQCrypto 2021 の発表(2 日目)

・SimS: a Simplification of SiGamal [PQCrypto 2021]

Tako Boris Fouotsa, Christophe Petit

Asiacrypt 2020 で Moriya らにより提案された、SiGamal と C-SiGamal に関する暗号解析論文である。これらは 2 つの新しい IND-CPA 安全な超特異性ベースの公開鍵暗号化(PKE)プロトコルである。SIKE や CSIDH から正規化された PKE とは異なり、新しいプロトコルはランダムオラクルを用いずに IND-CPA の安全性を実現している。しかし、SiGamal と C-SiGamal は IND-CCA 安全ではない。また Moriya らは IND-CCA 安全性を持つ SiGamal の変種を提案したが、その研究は未解決のまま

残された部分があった。

本論文では、Moriya らが提案したプロトコルを再検討する。まず、Moriya らが IND-CCA 安全性のために提案した SiGamal の変形が、実際には IND-CCA 安全性でないことを明らかにする。次に、SiGamal を単純化した InSIDH と名付けた新しい同種ベースの PKE プロトコルを提案する。In-SIDH は(C-)SiGamal よりも公開鍵、暗号文が小さく、効率的である。さらに、CSIDH の安全性仮定と、本論文で導入される Knowledge-of-Exponent 型の仮定の下で、InSIDH が IND-CCA 安全であることを証明する。興味深いことに、InSIDH は CSIDH プロトコルに非常に近く、SiGamal と CSIDH の比較を容易にする。

2.3. PQCrypto 2021 の発表(3 日目)

・Generating Cryptographically-Strong Random Lattice Bases and Recognizing Rotations of $\mathbb{Z}^n$ [PQCrypto 2021]

Tamar Blanks, Stephen Miller

格子暗号は、完全な簡約が困難なランダムな基底の生成に依存している。

本論文では、GL(n, Z)のランダムな要素をサンプリングする様々な方法の強さを比較し、Zn 格子を回転として捉える問題に関して、ある方法が他の方法より強いことを発見した。特に、(Magma の RandomSLnZ コマンドで実装されている)ユニポテント行列を掛け合わせる標準的なアルゴリズムにより生成されるものは、1,500 に近い次元でもこの最後の問題のインスタンスで効率的に破ることができる。また、NIST のポスト量子暗号コンペティションに提出されたランダム基底生成法(DRS)も効率的に破ることができる。

・Attacks on Beyond-Birthday-Bound MACs in the Quantum Setting [PQCrypto 2021]

Tingting Guo, Peng Wang, Lei Hu, Dingfeng Ye

本論文では、攻撃者が MAC への量子クエリアクセスを持つ Q2 モデルにおいて、12 の誕生日攻撃耐性 MAC(BBB MAC)の安全性を系統的に研究している。その結果、少なくとも $O(2^{2n/3})$ クエリまでは安全であることが証明された(古典的な攻撃では $O(2^{3n/4})$ クエリが必要)。さらに著者らは、SUM-ECBC および PMAC Plus に似た MAC に対する秘密状態回復と、PMAC Plus に似た MAC に対する鍵回復を検討し、どちらの攻撃も偽造を成功させた。これらは、BBB MAC に対する初の量子攻撃である。mPMAC+-f、mPMAC+-p1、mPMAC+-p2 のような最適安全 MAC に対しても、本攻撃は有効であると報告された。

・An Algebraic Approach to the Rank Support Learning Problem [PQCrypto 2021]

Magali Bardet, Pierre Briaud

階数距離符号ベースの暗号は、階数距離においてランダムな線形符号の復号が困難であること

に依存している。その変種である階数サポート学習問題(Rank Support Learning, RSL)とは、同じサポートをエラーとして持つ N 個の復号インスタンスに攻撃者がアクセスし、そのうちどれか 1 つを解こうとするものである。この問題は Durandal 署名方式で用いられている。

本論文では、この問題を解くために、従来の攻撃を明らかに上回る RSL に対する代数的な攻撃を提案する。本論文では、MinRank と RD を解くために同様の技術を用いた既存研究を基に、RSL に対する代数的攻撃を提案する。しかしながら、著者らの分析はより単純であり、したがってその攻撃は標準的な Gröbner 基底攻撃と比較して非常に単純な仮定に依存する。また、Durandal に対する鍵回復攻撃は、これまで考えられていたよりもはるかに効率的であることも、本研究で示唆された。

・A Practical Adaptive Key Recovery Attack on the LGM (GSW-like) Cryptosystem [PQCrypto 2021]

Prastudy Fauzi, Martha Norberg Hovd, Håvard Raddum

本論文では、Li, Galbraith and Ma (ProvSec 2016) が提案した Leveled 準同型暗号に対する、適応的(adaptive)鍵回復攻撃が紹介される。この方式自体は、復号ごとに異なる秘密鍵の線形結合を使用することで鍵回復攻撃に抵抗するように設計された GSW 暗号の修正版である。著者らは、統計的な攻撃を用いて、現実的なパラメータの選択に対して、効率的に秘密鍵を復元することができた。これは特に、Li, Galbraith, Ma の戦略は適応的な鍵回復攻撃を防ぐことができないことを意味する。

3. Crypto 2021 の発表

3.1. Crypto 2021 の発表(2 日目)

・Linear Cryptanalysis of FF3-1 and FEA [CRYPTO 2021]

Tim Beyne

本論文は、ラウンド微調整(round tweaks)を交互に適用する汎用小領域 Feistel 暗号(generic small-domain Feistel cipher) に対して線形解読法を用いて解析した結果を提示している。結果として、米国の形式保存暗号(format-preserving encryption)規格である FF3-1、韓国の規格である FEA-1 と FEA-2 に対する実用的な識別攻撃とメッセージ回復攻撃を実現している。FF3-1 と FEA-1 に対する提案攻撃のデータ量は$O\left(N^{r/2-1.5}\right)$である;ここで N^2 はドメインサイズ、r はラウンド数である。例えば、$N=10^3$ の FF3-1 は、2^{23} の暗号化クエリを用いることで、1/10 以上の成功率(advantage)で理想的な調整値付き (tweakable) ブロック暗号と区別することが可能である。同じ成功率でメッセージの左半分を復元するためには、2^{24} 個のデータが必要である。FF3-1 の解析は、群$\mathbb{Z}/N\mathbb{Z}$上の(一般化)線形解読法の興味深い実世界への応用として役立っている。

・Efficient Key Recovery for all HFE Signature Variants [CRYPTO 2021]

Chengdong Tao, Albrecht Petzoldt, Jintai Ding

HFE 暗号は、最もよく知られた多変数暗号方式の一つである。特に電子署名の分野では、HFEv-亜種は短い署名と高い性能を提供する。最近、GeMSS と呼ばれる HFEv-署名方式のインスタンスが、NIST のポスト量子暗号(PQC)標準化プロジェクトの第 3 ラウンドで、署名方式の代替候補の 1 つに選出された。

本論文では、HFEv-署名方式に対する新たな鍵回復攻撃を提案される。本攻撃は、Minus と Vinegar のいずれの変形も基本 HFE 方式の安全性を大きく向上させないことを示す。このことは、HFE をベースとした安全かつ効率的な署名方式を構築することが非常に困難であることを示している。特に、提案した GeMSS 方式のパラメータが主張するほど安全でないことが示される。

・How to Meet Ternary LWE Keys [CRYPTO2021]

Alexander May

LWE 問題とその環を変えた変種は、量子コンピュータに耐える効率的な公開鍵暗号を構築するための最も有力な候補である。NTRU 暗号は、LWE 問題の変形で、最大ノルムの秘密が小さく、通常、集合 $\{-1, 0, 1\}$ の三項係数を使用する。これらの方式に対する最良の攻撃は、格子削減技術と Odlyzko の Meet-in-the-Middle アプローチを組み合わせたハイブリッド攻撃と推定される。Odlyzko のアルゴリズムは古典的な組み合わせ攻撃であり、鍵空間のサイズSに対して時間で$S^{0.5}$実行される。

本論文では、部分和アルゴリズムで開発された表現技法(representation technique)を用いて、この Meet-in-the-Middle アプローチが大幅に改善される。漸近的には、著者のヒューリスティックな Meet-in-the-Middle 攻撃はおよそ $S^{0.25}$ の時間で実行されるが、これは最もよく知られた量子アルゴリズムの $S^{1/3}$ 計算量を上回るものである。

NIST のラウンド 3 ポスト量子暗号 NTRU-Encrypt と NTRU-Prime に対しては、著者らの攻撃の非漸近的な実装を、計算量およそ$S^{0.35}$で得ることができた。他の組み合わせ攻撃とは対照的に、著者らの攻撃はより大きな LWE フィールドサイズ q からアドバンテージを得ている。例えば、BLISS 署名では $S^{0.31}$から$S^{0.35}$の間で、GLP 署名では$S^{0.3}$で非漸近的な組合せ攻撃が得られる。

著者の攻撃は、前述の方式の安全性の主張を無効化するものではない。しかし、その安全性に対して改善された組み合わせ論的な上界を確立している。著者の新しい Meet-in-the-Middle 攻撃と格子削減を組み合わせることで、ハイブリッド攻撃を高速化できるかどうかは未解決の問題である。

・Improved torsion-point attacks on SIDH variants [CRYPTO 2021]

Victoria de Quehen, Peter Kutas, Chris Leonardi, Chloe Martindale, Lorenz Panny, Christophe Petit, Katherine E. Stange

SIDH は、超特異楕円曲線間の同種写像を見つけることが困難であるという推定に基づく耐量子

鍵交換アルゴリズムである。しかし、SIDH が依拠する厳密な困難性の仮定は純粋な同種写像問題ではない。攻撃者は実際に、秘密同種写像を曲線の部分群として与えるという制限を受ける。Petit はこの情報を利用して、SIDH の overstretched variants を多項式時間で破っており、ねじれ点の情報を利用することで、ある場合には効率的な攻撃ができることを実証している。

本論文の貢献は 2 つある。まず、Petit の手法を再検討し、双対とフロベニウス同種から来る情報を追加で利用する方法を示す。また、著者らの攻撃が適用されるパラメータの全範囲を示し、特に興味深い例として n-party group key agreement を挙げる。6 人以上のパーティの場合、本攻撃は多項式時間で実行され、3 人以上のパーティの場合、本量子攻撃は最もよく知られた漸近的計算量を向上させる。また、6 パーティに対する本攻撃の Magma 実装も提供する。

第二に、本攻撃に対して弱く設計された SIDH 変種を構築した。これには、開始曲線のトラップドアの選択と基礎体の標数のトラップドアの選択が含まれる。ただし著者らの結果は、NIST 提出の SIKE の弱点を明らかにしてはいない。

・Towards faster polynomial-time lattice reduction [CRYPTO2021]

Paul Kirchner, Thomas Espitau, Pierre-Alain Fouque

LLL アルゴリズムは、指数関数的な近似係数を持つ d 次元格子を簡約する多項式時間アルゴリズムである。現在、最も効率の良い Neumaier and Stehl'e による LLL の変形は、$d^4 \cdot B^{1+o(1)}$ (B はエントリのビット長)の理論実行時間を持っているが、実装されてはいなかった。

本論文では、漸近的に高速な並列かつヒューリスティックな削減アルゴリズムとその最適化実装が紹介される。このアルゴリズムは再帰的であり、高速なブロック行列の乗算を十分に利用することができる。再帰的ステップで浮動小数点精度を注意深く制御することにより、ランク d のユークリッド格子を時間 $\tilde{O}(d^{\omega c})$ 、すなわちほぼ一定数の行列乗算で削減できることを実験的に実証した。ここで、ω は行列の乗算の指数、C は行列の条件数の対数である。これにより、最新実装 fplll の実行時間が$d^2 \cdot B$のオーダーで改善される。さらに、ナップザック格子と呼ばれる構造的格子(structured lattice)を、漸近的な簡約により、時間 $\tilde{O}\left(d^{(\omega-1)c}\right)$で削減することができることを示す。他にも著者らの実装は、4 百万ビットを持つ 2230 次元の大きな整数に基づく完全準同型暗号方式のいくつかのインスタンスを破ることができる。

3.2. Crypto 2021 の発表(3 日目)

・Provable Security Analysis of FIDO2 [CRYPTO 2021]

Manuel Barbosa, Alexandra Boldyreva, Shan Chen, Bogdan Warinschi

本論文は、FIDO Alliance が提案するパスワードレスユーザー認証の標準規格である FIDO2 プロトコルについて、初めて証明可能な安全性解析を実施している。著者らの分析は、W3C の Web Authentication (WebAuthn) 仕様と新しい Client-to-Authenticator Protocol (CTAP2) という FIDO2 のコアコンポーネントを対象としている。

WebAuthnとCTAP2について、順番に、意図されたセキュリティ目標を捉えることを目的とした適切なセキュリティモデルを提案し、そのモデルを用いてセキュリティを分析する。最初に著者らは、WebAuthnの認証の安全性を証明することで確認する。次に、CTAP2が弱い意味での安全性しか証明できないことを示す。その一方で、一連の設計上の欠陥を特定し、改善のための提案を提供する。さらに、より強力かつ現実的な敵に対抗するため、sPACA と呼ばれる汎用プロトコルを提案し、その強い安全性を証明する。適切なインスタンス化により、sPACA は CTAP2 よりも効率的である。最後に、FIDO2 と WebAuthn+sPACA が提供する全体的なセキュリティ保証を、それらの構成要素のセキュリティに基づいて分析する。著者らは、著者らのモデルと証明可能なセキュリティ結果によって、FIDO2プロトコルのセキュリティ保証が明らかになることを期待している。また、CTAP2の代替プロトコルとして、より強固なセキュリティと高い性能を両立する著者らによる sPACA プロトコルを採用することを提唱している。

・Quantum Collision Attacks on Reduced SHA-256 and SHA-512 [CRYPTO 2021]

Akinori Hosoyamada, Yu Sasaki

本論文では、SHA-256とSHA-512に対する専用の量子衝突攻撃法が初めて示される。

この攻撃はそれぞれ 38 ステップと 39 ステップに達し、古典的な 31 ステップと 27 ステップの攻撃を大幅に改善した。両攻撃とも、多数の semi-free-start 衝突を 2 ブロック衝突に変換する先行研究の枠組みを採用し、計算時間と計算空間の間のトレードオフのコスト指標において汎用攻撃より高速であることが確認された。必要な semi-free-start 衝突の数は、量子設定において削減できることが観測されており、この観測結果に基づき、従来の古典的な 38 ステップ、39 ステップの semi-free-start 衝突を一つの衝突に変換することが可能となった。著者らは、この攻撃の基本となる考え方が単純であるため、他の暗号学的ハッシュ関数にも適用可能であると報告している。

3.3. Crypto 2021 の発表(4 日目)

・Differential-Linear Cryptanalysis from an Algebraic Perspective [CRYPTO 2021]

Meicheng Liu, Xiaojuan Lu, Dongdai Lin

差分線形解読法(differential-linear cryptanalysis)は、暗号技術における重要な暗号解析手段であり、1994 年に Langford と Hellman によって発見されて以来、盛んに研究されている。それにもかかわらず、差分トレイルと線形トレイルが接続する中間部分を研究する方法は非常に少ない。

本論文では、代数学的な観点から差分線形解読法を研究する。まず、差分線形解読法のためのDATF(Differential Algebraic Transitional Form)という技術を紹介し、次に差分線形バイアスの推定に関する新しい理論と差分線形解読法における鍵回復のための技術を開発する。

CAESARとLWCの最終候補であるASCON、AESの最終候補であるSerpent、eSTREAMの最終候補であるGrain v1に対して本技術を適用し、ASCONとSerpentに対する差分線形近似のバイアスを

推定した。バイアスの理論的な推定値は、差分線形接続表（Differential-Linear Connectivity Table）（Bar-On et al., EUROCRYPT 2019）で得られる値よりも正確であり、ラウンド数が多くても適用可能な技術であることがわかる。著者らの一般的な技術は、差分解読法における Grain v1 のバイアスを推定するためにも使用でき、暗号に合わせた Differential Engine ツールよりも明らかに優れた性能を持つ。次に、これらの暗号のラウンド数を削減した亜種に対する改良型鍵回復攻撃法も提案される。これらは、Serpent の暗号解析として、また、ASCON の差分線形解読法、Grain v1 の初期化フェーズの解析として、現時点で最もよく知られているものである。特に、Serpent の安全性解析は、過去 20 年間における差分線形解読法の最も重要な応用例の 1 つである。2003 年に示された Biham, Dunkelman, Keller の結果と比較すると、Serpent-128 と Serpent-256 に対する差分線形解読法では提案手法を使用することで攻撃可能ラウンド数を 1 ラウンド増やすことに成功した。

・Cryptanalysis of Full LowMC and LowMC-M with Algebraic Techniques [CRYPTO 2021]

Fukang Liu, Takanori Isobe, Willi Meier

本論文では、LowMC の差分列挙(difference enumeration)の技術を再検討し、新しい代数的技術を開発して、無視できるほどのメモリ計算量で効率的な鍵回復攻撃を実現する。ブロックサイズが鍵サイズよりはるかに大きい場合、本技術によって LowMC に対する攻撃を大幅に改善することが可能となり、結果としてフルスペックの LowMC を解読することに成功した。提案する鍵回復技術を用いると、特定の差分トレイルを有する単一の入出力メッセージペアのみが与えられた状況において完全な鍵を回復する時間計算量を大幅に改善することが可能である。両方の技術を組み合わせることで、2 つの選択平文のみで、ブロックサイズ 129、192、255 ビットのフル S-Box 層を採用した LowMC に対してそれぞれ 4 ラウンドのバージョンを解読することができる。これら 3 つパラメータは、NIST PQC コンペティションにおける第 3 ラウンド候補である Picnic3 の推奨パラメータである。Picnic のユースケースは非常に異なっており、攻撃者は具体的な LowMC インスタンスに対して暗号化する 2 つの平文を自由に選択することができないため、提案攻撃は Picnic3 が解読されることを示すものではない。しかし、最新の LowMC では、このようなパラメータは安全であるとみなされていた。また、Peyrin と Wang が CRYPTO 2020 で提案したバックドア暗号 LowMC-M の 7 インスタンスのうち、許可された 2^{64} データをフル活用することでバックドアを見つけることなく、はるかに多くのラウンドを解読できることも示している。上記の攻撃は、いずれも無視可能なメモリ量で実現された。

・Meet-in-the-Middle Attacks Revisited: Key-recovery, Collision, and Preimage Attacks [CRYPTO 2021]

Xiaoyang Dong, Jialiang Hua, Siwei Sun, Zheng Li, Xiaoyun Wang, Lei Hu

EUROCRYPT 2021 で Bao らは、中間一致(MITM)原像攻撃の構成空間を系統的に探索する自動手法を提案した。

本論文は、Bao らの手法を制約ベースのフレームワークに拡張し、鍵回復攻撃と衝突攻撃の両方のシナリオにおける微妙な特殊性を考慮することで、攻撃に利用可能な MITM 特性を見出す。さらに、従来にない非線形制約を持つ neutral words を用いて MITM 特性を利用した攻撃を行うために、対応する非線形方程式を解くことなく、また攻撃全体の時間的計算量を増やすことなく、neutral words の解空間を導出する手順を提示する。本手法を、SKINNY、ForkSkinny、Romulus、Saturnin、Grostl、Whirlpool といった具体的な共通鍵暗号プリミティブに適用した。その結果、単一鍵モデルにおいて、SKINNY-n-3n に対する初の 23 ラウンド鍵回復攻撃と ForkSkinny-n-3n に対する初の 24 ラウンド鍵回復攻撃を極めて少ないメモリで実行できることを示した。さらに、Whirlpool と Grostl に対する改良された(擬似)原像攻撃や衝突攻撃も実行できることを示した。これらの攻撃を実行するためのソースコードは公開されている。

・Revisiting the Security of DbHtS MACs: Beyond-Birthday-Bound in the Multi-User Setting [CRYPTO 2021]

Yaobin Shen, Lei Wang, Dawu Gu, Jian Weng

Double-block Hash-then-Sum(DbHtS)MACs は誕生日攻撃耐性を目指す MACs で、 SUM-ECBC、PMAC_Plus、3kf9、LightMAC_Plus などがある。最近、Datta ら(FSE 2019)と Kim ら(Eurocrypt 2020)は、単一ユーザー設定において DbHtS MACs が誕生日攻撃耐性を有することを証明した。しかし、彼らの結果はマルチユーザー設定においては成り立たない。

本論文では、マルチユーザー設定における DbHtS MACs の安全性が再検討され、誕生日攻撃耐性を証明するためのフレームワークが提案される。このフレームワークの有用性を、2k-SUM-ECBC、2k-PMAC_Plus、2k-LightMAC_Plus をはじめとした、鍵削減を施した DbHtS MACs のバリエーションに適用して実証する。これらの構成は、ユーザー数が増えても安全性が低下しないことが示された。一方、先行研究で解析を簡略化するために用いられている領域分離(domain separation)を追加することなく、シングルユーザーおよびマルチユーザーの設定において、これらの構成が誕生日攻撃耐性を持つことも示した。

さらに、Datta ら(FSE 2019)が誕生日攻撃耐性を証明した 2kf9 に重大な欠陥があることを見いだした。具体的には、クエリを実行することなく確率 1 でタグの偽造に成功する。

4. FDTC 2021 の発表

・Are Cold Boot Attacks Still Feasible: A Case Study on Raspberry Pi With Stacked Memory [FDTC2021]

Yoo-Seung Won and Shivam Bhasin

コールドブートアタックは、パスワード、暗号鍵、PIN といった機微なユーザー情報を漏洩させる、10 年以上にわたってコンピュータシステムの脅威となってきた semi-invasive attack の一種である。本論文では、人気がありすでに数百万台が出荷されている Internet-of-Thins (IoT) デバ

イスである Raspberry Pi (model B+) を調査している。Raspberry Pi はプロセッサの上に stacked memory を搭載し、プロセッサから RAM を分離することを物理的に不可能にしている。著者らは Raspberry Pi に対するコールドブートアタックの減衰モデルを研究した。その結果によれば、減衰率は 0.00027%と、以前の研究から考えられていたよりも桁違いに低く、ほぼ完全なデータ復元を可能にするほどである。さらに、Raspberry Pi 上の dm-crypt を使用したディスク暗号化の鍵 (AES-XTS-512 の 512 ビットマスター鍵) の復元に成功したことも示している。

5. CHES 2021 の発表

5.1. CHES 2021 の発表(1 日目)

・Online Template Attacks: Revisited [CHES2021]

Alejandro Cabrera Aldaya and Billy Bob Brumley

Online Template Attack (OTA)は、楕円曲線のスカラー倍アルゴリズムの攻撃に以前から使用されていた強力な手法である。この攻撃は、処理している値に関係した信号が漏洩する電力消費と電磁場サイドチャネルの領域でのみ分析されてきた。しかし、マイクロアーキテクチャの信号にはそのような性質はなく、これまでの OTA に関する研究に基づく仮定は適用できない。
本論文では、以前からの OTA の手法を再検討し、一般的なフレームワークと任意のサイドチャネル信号のための評価基準を提案している。

この点について、著者らは、OTA が逆方向に実行できることを示す。これによって、Naccache, Smart and Stern による提案 (Eurocrypt 2004) に関して augmented projective coordinate attack を実行することができる。このことは、以前の研究で信じられていたように、ターゲットアルゴリズムの初期ステートをランダム化することがこの攻撃を防ぐことができないことを示している。

著者らは libgcrypt、mbedTLS、wolfSSL の 3 個のライブラリを、2 つのマイクロアーキテクチャサイドチャネルを使用して解析した。libgcrypt では、ツイスト曲線 Curve25519 を使用した EdDSA 実装を標的とする。曲線 secp256r1 を使用した mbedTLS と wolfSSL に対しても同様の結果を得ている。各ライブラリに対して、すべてのケースで 1 個のトレースを使用して、スカラーを完全に復元することができる広範囲の攻撃例を実行した。

この研究は、マイクロアーキテクチャへの OTA もこのシナリオでは非常に強力であり、漏洩モデルを知らずに秘密情報を復元できることを示している。これは「必要に応じて修正する」のではなく「デフォルトでセキュア」であるように開発することの重要性を際立たせる。

・RASSLE: Return Address Stack based Side-channel LEakage [CHES2021]

Anirban Chakraborty, Sarani Bhattacharya, Manaar Alam, SikharPatranabis and Debdeep Mukhopadhyay

マイクロアーキテクチャに対する攻撃はしばしば基礎となるアーキテクチャにある小さなアーティ

ファクトに由来する。本論文では、毎回のサブルーチンコールのリターンアドレスを格納することにより分岐予測ミスペナルティを軽減するために現代のプロセッサに実装されている小さなハードウェアスタックであるリターンアドレススタック（RAS）に注目する。RAS は、典型的な分岐予測ユニットでは精度よく予測できない RET 命令に対する分岐予測の扱いに特に役立つ。特に、著者らは、RAS を任意のリターンアドレスで満杯にすることで RAS にオーバーフローコンディションを意図的に作り出し、並行して動くプロセスを攻撃してそれらの間でタイミングサイドチャネル攻撃を確立するスパイプロセスを想定する。著者らはこの攻撃原理を”RASSLE”(Return Address Stack based Side-channel Leakage)と呼び、これによって、確立したタイミングチャネルを悪用する一般的な手法を使用して最初に RAS をリバースエンジニアリングすることによって最新のプロセッサに攻撃を行うことができる。続いて、3 つの具体的な攻撃シナリオを示している。i)スパイプロセスが他の共存しているプロセスとの間に秘密のチャネルをいかにして確立するか。ii)OpenSSL (v1.1.1 ライブラリ)の P-384 曲線の秘密鍵を確定するのに RASSLE がいかにして利用できるか。iii)RASSLE の助力によって部分的に漏洩した nonce への Lattice Attack を使用することにより OpenSSL の P-256 曲線の ECDSA の秘密鍵をいかにして暴露できるか。この攻撃において、この曲線でのスカラー乗算の OpenSSL での実装が、add-and-sub 関数呼び出し回数が秘密のスカラービットに依存して変化することを著者らは示している。何回かの実験を通して、add-and-sub 関数呼び出しの回数が秘密のビットをテンプレート化することができ、RASSLE の原理を利用したスパイプロセスによってそれを拾い上げることができることを著者らは示している。最後に、著者らは P-256 曲線のパラメータを使用した OpenSSL の ECDSA に対する最初から最後までの完全な攻撃を示している。RASSLE による実験のこの部分では、deadline scheduler policy を悪用することでスパイプロセスと標的プロセスの間の完全な同期を、標的プロセスのコードから同期を誘発することの助けを得ることなく達成している。RASSLE を通じたこの同期とタイミングリーケージは、署名生成に使用される一時的な nonce の MSB を復元するのに十分であり、これによって、Hidden Number Problem を適用することによって、送信者の秘密の署名鍵を復元することが可能になる。

・Minerva: The curse of ECDSA nonces: Systematic analysis of lattice attacks on noisy leakage of bit-length of ECDSA nonces [CHES2021]

Ján Jančár, Vladimír Sedláček, Petr Švenda, and Marek Sýs

ECDSA の実装(FIPS140-2 認証されたスマートカード用 IC チップである Atmel 社製 AT90SC、および 5 個のソフトウェア暗号ライブラリ)に、サイドチャネル攻撃の一種であるタイミングアタックに対する脆弱性を発見した。ECDSA では、署名生成 1 回ごとに nonce が必要だが、nonce のビット長がサイドチャネル情報として(ノイズは大きいが)洩れる場合に、それを利用して秘密鍵を復元する手法を示し、実際の認証製品や暗号ライブラリに対する具体的な攻撃の結果も示している。EdDSA は、nonce が決定論的に生成され、また nonce が長いことから、この攻撃に耐性がある。

・When one vulnerable primitive turns viral: Novel single-trace attacks on ECDSA

and RSA [CHES2021]

Alejandro Cabrera Aldaya and Billy Bob Brumley

本論文では、TLS の実装のひとつである mbedTLS の binary GCD アルゴリズムのセキュリティを分析している。SGX エンクレーブを基にした mbedTLS に対して、SGX-Step というフレームワークを使用したサイドチャネル攻撃に対する脆弱性があることを示している。このライブラリのこのアルゴリズムにおけるあるユースケースのセキュリティを分析し、この実装に対する単一トレースによる攻撃を許す新たな脆弱性を、ECDSA のコードパス中に発見する結果を得た。

また、直行するユースケースにもカバーし、mbedTLS の RSA の、秘密鍵をロードするときの CRT パラメータの計算中のコードパスの内部も対象にしている。この攻撃は binary GCD 実装の脅威も悪用しており、1 個の脆弱なプリミティブがいかに複数のセキュリティ脅威になるかを示している。著者らは両方のセキュリティ脅威を各 1000 回の試行による完全な攻撃で示し、両方のケースにおいて 100%に近い成功率でシングルトレース攻撃を達成できることを示している。

5.2. CHES 2021 の発表(5 日目)

・Persistent Fault Attack in Practice [CHES2021]

Fan Zhang, Yiran Zhang, Huilong Jiang, Xiang Zhu, Shivam Bhasin, Xinjie Zhao, Zhe Liu, Dawu Gu and Kui Ren

Persistent Fault Attack の実用的な適用可能性についての発表である。Persistent Fault Attack は、暗号実装ハードウェアに対して持続的なフォールトを起こす(例えば、S-Box 計算用テーブルを 1 バイト書き換え、1 ブロックの暗号演算中は誤ったテーブルが参照されるようにする)攻撃で、CHES 2018 に初めてその原理が発表された。本発表では、AES の実装に対するこの攻撃手法を改良し、1641 個の暗号文を取得することで AES の鍵を復元できることをしており、これは以前の研究より 28%の改良となっている。さらに、軽量暗号のひとつである PRESENT に対しても適用できることを示した。

6. Eurocrypt 2021 の発表

6.1. Eurocrypt 2021 の発表(1 日目)

・New Representations of the AES Key Schedule [Eurocrypt 2021]

Gaëtan Leurent, Clara Pernot

本論文では、AES 鍵スケジュールの新しい表現と、AES ベースのスキームの安全性へのいくつかの示唆が提示される。特に、AES-128 鍵スケジュールは、32 ビットのチャンクで動作する 4 つの独立した並列計算に分割でき、線形変換まで可能であることが示される。この性質は 20

年以上にわたる AES の解析を経て初めて示されたものである。さらに、この新しい表現は AES ベースのスキームに対するこれまでの暗号解読結果を改善するために使用され、2 つの新しい結果が得られている。まず著者らは、奇数回の鍵スケジュールラウンドを繰り返すと、短いサイクルを持つ関数が生成されることを確認した。この結果を利用することで、NIST Lightweight Cryptography コンペティションの第 2 ラウンド候補である mixFeed に対して Khairallah が示した観測結果を説明することが可能となる。著者らの解析によると、Khairallah が示した mixFeed に対する偽造攻撃は 0.44 の確率で成功することがわかった(データ量は 220GB)。また、同じ観測結果から、AES ベースの AEAD 方式である ALE に対する新たな攻撃も発見された。また、著者らが提示する新しい表現により、最初のサブキーの情報と最後のサブキーの情報を組み合わせて、対応するマスターキーを再構成する効率的な方法が示されている。特に、これらの解析手法を使用し、AES-128 に対する従来の不可能差分攻撃(impossible-differential attacks)を改善することが可能となる。

・Automatic Search of Meet-in-the-Middle Preimage Attacks on AES-like Hashing [Eurocrypt 2021]

Zhenzhen Bao, Xiaoyang Dong, Jian Guo, Zheng Li, Danping Shi, Siwei Sun, Xiaoyun Wang

中間一致原像攻撃(MITM 原像攻撃)は、フル MD5、HAVAL、Tiger、縮小 SHA-0/1/2 など、多くのハッシュ関数の原像攻撃の耐性を破るのに極めて有効である。なお、2011 年に Sasaki は AES ライクなハッシュ関数に対してもこの攻撃が脅威であると示している。近年、AES のハッシュモードに対する MITM 原像攻撃は、内部状態を自由に選択できる仮定を利用するとともに、メッセージを自由に選択できる仮定を利用するなど、様々な攻撃手法が提案されている。しかしながら、MITM 原像攻撃を実行するために考えられる構成が多すぎるため、従来の解析結果は提案者の直感と経験に依存するところが大きく、必ずしも最適な解であるとは限らないという問題があった。

本論文では、先行研究における人為的な制限を取り除き、攻撃の構成に関する本質的なアイデアを明確に定式化し、最適な解を探索するため混合整数線形プログラミング(MILP)モデルにおける制約条件の下で最適化問題に変換する。このような MILP モデルを構築し、市販のソルバーを使用することで、最適な解を網羅的に探索することができる。その結果、Haraka-512 v2 の完全版(5 ラウンド)と拡張版(5.5 ラウンド)、および AES-128 ハッシュモードの 8 ラウンドに対する攻撃を初めて示すとともに、Haraka-256 v2 および AES と Rijndael のハッシュモードにおける他のメンバーへの攻撃を改善した。

・Improved Linear Approximations to ARX Ciphers and Attacks Against ChaCha [Eurocrypt 2021]

Murilo Coutinho Silva, Tertuliano C. de Souza Neto

本論文では、ARX 暗号においてより良い線形近似を求めるために用いることができる新しい技術

が紹介される。この技術を用いることで、ChaCha の 3 ラウンドと 4 ラウンドに対して初めて明示的に導き出された線形近似を提示し、その結果として、ChaCha に対する最近の攻撃を改善することが可能となった。さらに、ChaCha の 3 ラウンドと 3.5 ラウンドに対する新しい差分を提示し、提案手法と組み合わせることで、ChaCha に対する差分線形攻撃の計算量をさらに向上させることに成功している。

・Rotational Cryptanalysis From a Differential-Linear Perspective - Practical Distinguishers for Round-reduced FRIET, Xoodoo, and Alzette [Eurocrypt 2021]

Yunwen Liu, Siwei Sun, Chao Li

差分線形識別器の偏りを評価する厳密な公式(JoC2017)から、差分部分と線形部分の切り替えの依存性を扱う差分線形接続表(DLCT)技術(EUROCRYPT2019)、そして ARX プリミティブの暗号解読の文脈での改良(CRYPTO2020)まで、この 4 年間で差分線形攻撃は大きな発展を見せている。本論文では、攻撃の差分部分を回転型 xor(rotational-xor)差分に置き換えることで、この枠組みをさらに拡張している。さらに、FRIET、Xoodoo、Alzette、SipHash に含まれる並べ換えに対して著者らの技術を適用した。これにより、既存の暗号解析結果を大幅に改善することができ、また、理論的根拠のない従来の実験的識別器の説明を行うことができる。本解析の妥当性を確認するため、実用的な計算量を持つすべての識別器の実験的検証も行われている。

・A Deeper Look at Machine Learning-Based Cryptanalysis[Eurocrypt 2021]

Adrien Benamira, David Gerault, Thomas Peyrin, Quan Quan Tan

機械学習を用いた共通鍵暗号に対する解析論文である。

CRYPTO 2019 で Gohr は、機械学習アルゴリズムを活用した新しい暗号解析を提案した。この解析手法ではディープニューラルネットワークを利用しており、ブロック暗号 SPECK のメンバーの 1 つである SPECK-32/64 に対し、最先端の暗号解読を上回る識別器(distinguisher)を構築することに成功した(この識別器は鍵回復攻撃に応用できる可能性がある)。しかしながら、この識別器が実際にどのように機能するのか、機械学習アルゴリズムがどのような情報を推論しているのか、という問題(ディープニューラルネットワークの解釈可能性)はよく知られた困難な問題であることも加わり、まだ明らかになっていない。

本論文では、この新しい識別器に対して詳細な分析と徹底的な解説を行う。まず、分類済みのデータセットを使用し、Gohr の結果をよりよく理解するための指針となる様々なパターンの発見を試みた。実験により、この識別器は一般的に暗号文ペアに関する差分分布に依存しているが、最後から 2 番目と 3 番目のラウンド(penultimate and antepenultimate rounds)における差分分布にも依存していることが明らかとなった。この実験結果を検証するため、ニューラルネットワークを使用しない暗号解析手法に基づいて SPECK の識別器を構築し、Gohr の識別器と基本的に同じ精度と効率性を達成することに成功している(したがって、この結果は Gohr の識別器が従来の識別器よりも改善できていることを明らかにしている)。さらに別のアプ

ローチとして、Gohr のディープニューラルネットワークを必要最低限にまで縮小した機械学習ベースの識別器を提供する。著者らは、標準的な機械学習ツールを用いるだけで Gohr の識別器に非常に近い精度を維持できることを示した。また、Gohr は識別器を構成するために学習段階で対象となる暗号方式の差分分布表(DDT)に関する非常に優れた近似表を作成し、この情報を使って暗号文ペアを直接分類していることを示す。この結果は、識別器の完全な解釈可能性を可能にするとともに、ディープニューラルネットワークの解釈可能性に向けた興味深い貢献となる。最後に、Gohr の研究を改善するための方法と、識別器の構築に関する新しい可能性が提案されている。すべての結果は、SPECK ブロック暗号で実施した実験により確認されている。

・Three Third Generation Attacks on the Format Preserving Encryption Scheme FF3[Eurocrypt 2021]

Ohad Amon, Orr Dunkelman, Nathan Keller, Eyal Ronen, Adi Shamir

FPE(Format Preserving Encryption)方式は、社会保障番号や生年月日などの有限な値の集合から平文を受け取り、同じ集合に属する暗号文を生成する方式である。既存のデータベースや通信パケットの形式を変えずに暗号化できるため、実用上非常に有用である。業界の要望により、NIST は 2016 年に FF1 および FF3 と呼ばれる 2 つのこのような暗号化方式を標準化していた。これらは攻撃計算量の減少とともに、すぐに暗号解読の対象として大きな注目を集めた。FF3 の Feistel 構築に対して現在知られている最高の攻撃は、入力がサイズ $N \times N$のドメインに属する場合、データとメモリの複雑さが$O(N^{11/6})$、時間の複雑さが$O(N^{17/6})$になる。

本論文では, FF3 に対する 3 つの改良型攻撃法を提案し, 実験的に検証する. 本論文で提案する攻撃法は、任意の$t \leq 0.5$に対し、トレードオフ曲線$D = M = \tilde{O}(N^{2-t}), T = \tilde{O}(N^{2+t})$を実現するものである。特に、データ量とメモリ量を実用的な$\tilde{O}(N^{1.5})$に低減し、同時に時間量を$\tilde{O}(N^{2.5})$に低減することが可能である。また、FPE 方式に対するもう一つの攻撃ベクトルである related-domain 攻撃を識別する。敵対者に異なるドメインで同じ鍵の暗号にアクセスさせることで強力な攻撃を行う方法を示し、FF3 インスタンスと FF3-1 インスタンスを効率的に区別するための適用方法を示す。

・Cryptanalysis of the GPRS Encryption Algorithms GEA-1 and GEA-2 [Eurocrypt 2021]

Christof Beierle, Patrick Derbez, Gregor Leander, Gaetan Leurent, Havard Raddum, Yann Rotella, David Rupprecht, Lukas Stennes

本論文では、GEA-1 および GEA-2 アルゴリズムに対する初めての公開された暗号解読法を紹介する。64 ビットの完全なセキュリティを提供する代わりに、GEA-1 の初期状態を、わずか 65 ビットの(少なくとも 1 フレームごとに 24 ビットである)既知のキーストリームから、2^{40}回の GEA-1 評価と 44.5

GiB のメモリを使用して回復することができることを示した。GEA-1 への攻撃は、配置された LFSR と鍵の初期化との例外的な相互作用に基づいており、偶然に起こる可能性は極めて低いものである。この異常なパターンは、設計上セキュリティレベルを 40 ビットに制限するために、弱点を意図的に隠していることを示している。一方、GEA-2 については、同様の意図的な弱点は発見されなかった。しかし、代数的手法とリストマージアルゴリズムの組み合わせにより、依然として $2^{45.1}$ 回の GEA-2 評価で GEA-2 を破ることが可能である。主な実用上のハードルは、1600 バイトのキーストリームの知識が要求される点となる。

6.2. Eurocrypt 2021 の発表(2 日目)

・Mind the Middle Layer: The HADES Design Strategy Revisited [Eurocrypt 2021]

Nathan Keller, Asaf Rosemarin

HADES は古典的な SPN 構成と部分的な SPN (PSPN) 構成を組み合わせて設計されている。PSPN 構成とは、各暗号化ラウンドにおいて内部状態の一部にのみ非線形層を適用した構成のことである。統計的な攻撃手法に対する HADES の安全性については、PSPN 構成の部分を除外し、SPN 構成の部分のみに着目されている。このような仮定を用いているため、設計者は線形演算として使用する MDS 行列についていかなる制限も課していない。

本論文では、MDS 行列の選択が HADES 設計のセキュリティレベルに大きく影響することを示されている。さらに、HADES 設計のバリエーションである Starkad と Poseidon における解析結果も紹介され、適切でない MDS 行列を選択した場合、Starkad と Poseidon の安全性を破ることができると示されている。本報告を受け、Starkad と Poseidon の設計者は、MDS 行列が適切に選択されていることを保証する要件を追加し、設計を修正済みである。

・Advanced Lattice Sieving on GPUs, with Tensor Cores [Eurocrypt 2021]

Léo Ducas, Marc Stevens, Wessel van Woerden

本論文は、General Sieve Kernel (G6K, Albrecht et al. 2019)の内部で、格子のための様々な最先端のふるい分けアルゴリズム(Becker-Gama-Joux 2015, Becker-Ducas-Gama-Laarhoven 2016, Herold-Kirshanova 2017)の GPU 実装を研究している。特に、最近導入された Tensor Core(元々はレイトレーシングや機械学習用に設計されている)を広範囲に活用し、目下の暗号解読タスクへの適合性を実証する。また、G6K の重要な要素である短いリフトドベクトルの発見を高速化するために、「リフトに値する」(='lift-worthy')ペアを効率的に検出する新しいデュアルハッシュ技術を提案する。筆者らは、SVP Darmstadt Challenge において、従来の 155 次元の記録を更新する 180 次元の計算量を達成し、新記録を達成した。この計算は、4 つの NVIDIA Turing GPU と 1.5TB の RAM を搭載したサーバーで 51.6 日間実行された。これは、実測時間やエネルギー効率の点で、これまでの記録より約 2 桁も優れている。

・On Bounded Distance Decoding with Predicate: Breaking the "Lattice Barrier" for the Hidden Number Problem [Eurocrypt 2021]

Martin R. Albrecht, Nadia Heninger

暗号解読における格子ベースのアルゴリズムは、整数の線形制約を満たすターゲットベクトルを、ある格子における最短または最接近のベクトルとして探索することが多い。本研究では、これらの定式化が、ターゲットベクトルが一意に近い、あるいは短いとは言い難い場合でも、ターゲットベクトルを区別するために用いることができる基礎となるアプリケーションからの非線形情報を破棄する可能性があることを観察する。著者らは、ターゲットベクトルを区別する述語による格子問題の定式化を行い、これらの問題のインスタンスを解くためのアルゴリズムを提供する。本技術をサイドチャネル攻撃で DSA や ECDSA の秘密鍵を復元する際によく用いられる秘匿数問題の格子ベースの解法に適用し、これまで格子アプローチでは解けないと考えられていた事例でも本アルゴリズムが署名鍵の復元に成功することを実証する。また、著者らの推定・解法フレームワークを用いた広範な実験を行い、その結果も併せて公開している。

・On the ideal shortest vector problem over random rational primes [Eurocrypt 2021]

Yanbin Pan, Jun Xu, Nick Wadleigh, Qi Cheng

数体における非自明なイデアルは素イデアルの積に分解できる。本論文では、素イデアルの最短ベクトル問題(SVP)の計算量とその分解群の間の関係性について研究する。得られた結果を、二べきの円分体など、格子に基づく暗号システムでよく用いられる数体に適用したところ、有理素数(rational prime)の大部分は、SVP の多項式時間アルゴリズムを認める素イデアルに属することが示された。理想格子の最短ベクトル問題は Ring-LWE 暗号の安全性を支えているが、安全性の低下は最悪の場合の理想 SVP から平均的な場合の Ring-LWE への一方通行であるため、この研究は Ring-LWE を破るものではない。

6.3. Eurocrypt 2021 の発表(3 日目)

・The Nested Subset Differential Attack: A Practical Direct Attack Against LUOV which Forges a Signature within 210 Minutes [Eurocrypt 2021]

Jintai Ding, Joshua Deaton, Vishakha, Bo-Yin Yang

2017 年、Ward Beullens らが Patarin による Unbalanced Oil and Vinegar を修正した耐量子署名スキーム Lifted Unbalanced Oil and Vinegar(LUOV)を提出した。その後 Ding らは Subfield Differential Attack を提案したが、これは NIST のポスト量子標準化コンペティションの第 2 ラウンドで LUOV の作者がパラメータを変更するきっかけとなった。

本論文では、提案されたパラメータセットの半分を完全に破る、Subfield Differential Attack を改良した Nested Subset Differential Attack を提案する。また、この攻撃が理論上

の攻撃ではなく、レベルⅠのセキュリティパラメータに対して 210 分以内で実際に可能であることを実験により示す。Nested Subset Differential Attack は、Subfield Differential Attack を大きく改良したものであり、実環境で使用可能である。著者らは、LUOV の「lifted」構造と呼ばれるもののみを使用しており、その攻撃は「lifted」二次方程式を解くことの発展形と考えることができる。

・Improved cryptanalysis of UOV and Rainbow [Eurocrypt 2021]

Ward Beullens

本論文の貢献は 2 つある。一つに、Unbalanced Oil and Vinegar 方式(UOV)とその変形である Rainbow 方式の記述を簡略化し、既存の攻撃を理解しやすくしたことである。二つに、UOV と Rainbow の署名方式に対して、UOV と Rainbow の両方に適用できる交叉攻撃と、Rainbow のみに適用できる長方形 MinRank 攻撃という 2 つの新しい攻撃を与えたことである。これらは既存の攻撃よりも強力であり、特に、NIST PQC 標準化プロジェクトの第 2 ラウンドに提出された、セキュリティレベルⅠ、Ⅲ、Ⅴをそれぞれ対象とするパラメータセットに対して、従来知られている攻撃と比較して、鍵回復のコストを 2^{17}、2^{53}、2^{73} 倍削減すると推定している。第 3 ラウンドのパラメータでは、コストはそれぞれ 2^{20}、2^{40}、2^{55} で減少している。これらのパラメータセットはすべて、NIST が定めたセキュリティ要件を満たさない。

7. TCC 2021 の発表

・Simple Constructions from (Almost) Regular One-Way Functions [TCC 2021]

Noam Mazor, Jiapeng Zhang

一方向性関数から構成できる暗号プリミティブとして、擬似乱数生成器(pseudorandom generators、PRG)と普遍的一方向性ハッシュ関数(universal one-way hash functions、UOWHF)の 2 つが有用である。これらを実際に実装するためには、その構成の効率性を考慮する必要がある。効率性の指標としては、シード長、一方向性関数への呼び出し計算量、そしてこれらの呼び出しの適応性の 3 つが挙げられる。しかし、これらの構成における最適な効率はまだ十分に理解されておらず、ブラックボックス構成における既知の上限と既知の下限の間にギャップが存在する。未知の正則一方向性関数(unknown-regular one-way functions)と呼ばれる一方向性関数の特殊なクラスは、よりよく理解されている。Haitner, Harnik and Reingold (CRYPTO 2006)は、ランダム化反復子と呼ばれる手法に基づき、半線形(semi-linear)シード長および線形呼び出し回数の PRG 構成について発表した。Ames, Gennaro and Venkitasubramaniam (TCC 2012)は、同様のパラメータで、同様のアイデアを用いた UOWHF の構築を示した。一方、Holenstein and Sinha (FOCS 2012) と Barhum and Holenstein (TCC 2013) は、一方向性関数から PRG と UOWHF のブラックボックス構成に対して、ほぼ線形な呼び出し計算量の下界を示した。したがって、Haitner ら

とAmesらは、通常の一方向性関数からPRGとUOWHFを(シード長と呼び出し回数の点から)厳密に構成することに成功した。しかし、これらの構成は適応的である。

本研究では、HolensteinとSinha、BarhumとHolensteinが示した最適な呼び出し回数と一致する、両プリミティブの非適応的な構成法を提示する。構成は単純かつ非適応的であることに加え、ほぼ正則な一方向性関数に対してもロバストである。

・Relationships between quantum IND-CPA notions [TCC 2021]

Tore V. Carstens, Ehsan Ebrahimi, Gelo N. Tabia, Dominique Unruh

攻撃者が選んだ 2 つのメッセージの暗号を見分けることができない安全性、選択平文攻撃に対する識別不可能性(indistinguishable under chosen plaintext attack、IND-CPA)と呼ばれる。この定義には他のバリエーションがあるが、古典的なケースではすべて等価であることがわかっている。

本論文では、対称型暗号化方式におけるIND-CPAの様々な定義について、量子環境下での包括的な概観を示している。また、これらの概念の関係を調査し、これらの概念の間の様々な等価性、含意、非等価性、非含意についての証明が行われる。

8. Asiacrypt 2021 の発表

8.1. Asiacrypt 2021 の発表(1 日目)

・On the hardness of the NTRU problem [Asiacrypt 2021]

Alice Pellet-Mary, Damien Stehlé

25 年前の NTRU 問題は、公開鍵暗号における重要な計算の前提となっている。しかし、ユークリッド格子上の他の問題と比較した場合、削減の観点からその相対的な難しさはよく分かっていない。その決定版は探索Ring-LWE問題に還元されるが、これは困難性の上界を与えるに過ぎない。

本論文は、NTRU 問題の困難性に関する漸化式の証拠を提供するという、長年の未解決問題に対する 2 つの解答を提供する。まず、理想格子上の最悪ケースの近似最短ベクトル問題を、NTRU問題の平均ケース探索変種問題に帰着する。次に、NTRU 問題の別の平均ケース探索変種問題を、決定NTRU問題に還元する.

・A Geometric Approach to Linear Cryptanalysis [Asiacrypt 2021, Award Paper]

Tim Beyne

線形暗号法に関する新しい解釈を提案する論文である。「幾何学的アプローチ」(geometric approach)は、線形暗号法における全ての一般的なバリエーションを統一するとともに、様々な特性の間にリンクが存在することを明らかにし、線形解読法のさらなる一般化を提案する。例えば、相

関行列の非実数固有値に対応する不変量に対する新しい洞察や、ゼロ相関攻撃と積分攻撃の間のリンクに関する一般化が得られる。幾何学的直感は、固定鍵による piling-up 原理の動機付けにつながり、これは不変量と線形近似に関連する従来の結果の説明と一般化によって説明される。ランク 1 近似は、セル指向暗号(cell-oriented cipher)を分析するために提案され、FSE 2019 で Beierle、Canteaut、Leander によって提起された未解決問題を解決するために使用される。特に、このような近似がリーマン最適化を用いて自動的に解析される方法を示す。

・Partial Key Exposure Attack on Short Secret Exponent CRT-RSA [Asiacrypt 2021]

Alexander May, Julian Nowakowski, Santanu Sarkar

(N, e)を RSA 公開鍵とし、N=pq をビットサイズの等しい素数 p, q の積とする。d_p, d_qは対応する秘密の CRT-RSA 指数とする。Coppersmith 型攻撃により、Takayasu, Lu and Peng(TLP)は最近、$d_p, d_q \leq N^{0.122}$であれば、多項式時間で N の因数分解を得ることができることを示した。

本論文では、TLP 攻撃に基づいて、短い秘密指数を持つ CRT-RSA に対する最初の Partial Key Exposure 攻撃が示される。すなわち、$N^{0.122} \leq d_p, d_q \leq N^{0.5}$のとき、$d_p, d_q$の両方の既知の定数割合の下位ビット(LSBs)があれば、多項式時間で N を因数分解するのに十分であることを示す。当然ながら、d_p, d_qが大きくなればなるほど、より多くの下位ビットが必要となる。例えば、d_p, d_qが$N^{0.13}$のサイズであればその約 1/5 の下位ビット、$N^{0.2}$のサイズならその約 2/3 の下位ビット、d_p, d_qがフルサイズ$N^{0.5}$であればその全てを知る必要がある。この結果の副産物として、入力(N, e, d_p, d_q)に対するヒューリスティックな決定論的多項式時間因数分解アルゴリズムが得られることに注目する。

8.2. Asiacrypt 2021 の発表(2 日目)

・Fault-Injection Attacks against NIST's Post-Quantum Cryptography Round 3 KEM Candidates [Asiacrypt 2021]

Keita Xagawa, Akira Ito, Rei Ueno, Junko Takahashi, Naofumi Homma

NIST PQC ラウンド 3 鍵カプセル化メカニズムの全候補:Classic McEliece、Kyber、NTRU、Saber、BIKE、FrodoKEM、HQC、NTRU Prime、SIKE を、故障利用攻撃(fault injection attack)の観点から調査した。これらすべての KEM 方式は Fujisaki-Okamoto 変換の変種を使用しているため、カプセル化解除時の再暗号化との等価性テスト(equality test)が重要である。

本論文では、等値性判定を省略できる場合の有効な鍵回復攻撃について調査される。その結果、Kyber、NTRU、Saber、FrodoKEM、HQC、NTRU Prime の 2 つの KEM 方式のうちの 1 つ、および SIKE に対する既存の鍵回復攻撃があることがわかった。また、NTRU Prime に含まれるもう 1 つの KEM 方式に対する新しい鍵回復攻撃が提案される。また、BIKE に対して秘密鍵の情報漏えいを引き起こす攻撃が報告される。

オープンソースの pqm4 ライブラリには、Classic McEliece と HQC を除く全ての KEM スキームが

含まれている。本論文では、Kyber, NTRU, Saber, BIKE, SIKE において、カプセル化解除の過程で 1 つの命令スキップ故障(instruction-skipping fault)を与えることで、仮想的に等値性テストがスキップされることが示されている。また、それらに対する攻撃の実験結果も報告される。また、NTRU Prime の実装では選択暗号文攻撃が自由に行えること、Guo, Johansson, and Nilsson (CRYPTO 2020) で報告された FrodoKEM のタイミングサイドチャネルが残っているが、彼らの NIST PQC Round 3 提出課題にはそのようなバグがないことも報告される。

・A formula for disaster: a unified approach to elliptic curve special-point-based attacks [Asiacrypt 2021]

Vladimir Sedlacek, Jesús-Javier Chi-Domínguez, Jan Jancar, Billy Bob Brumley

Refined Power Analysis、Zero-Value Point、Exceptional Procedure 攻撃は、楕円曲線暗号の特定のケースに対するサイドチャネル技術を導入した攻撃である。この 3 つの攻撃は、入力点のある倍数が計算されたかどうかの情報を収集し、静的な ECDH 鍵のビットを適応的に復元する。

本論文では、これらの攻撃を共通のフレームワークで統一し、一般化し、より広い入力のクラスに対して対応する問題が解決される。また、窓付きスカラー倍算法(windowed scalar multiplication method)に対する攻撃のバージョンを導入し、スカラーの一部だけでなく、完全なスカラーを回復させる。最後に、Explicit-Formulas データベースから楕円曲線点加算公式を系統的に解析し、すべての非自明な例外点を分類し、新しい公式でそれらを発見することに成功している。これらの結果は、公式の展開と特殊な点の発見に対する著者らのツールの有用性を示すものであり、将来的には独立した研究対象となる可能性がある。

8.3. Asiacrypt 2021 の発表(3 日目)

・QCB: Efficient Quantum-secure Authenticated Encryption [Asiacrypt 2021]

Ritam Bhaumik, Xavier Bonnetain, André Chailloux, Gaëtan Leurent, María Naya-Plasencia, André Schrottenloher, Yannick Seurin

共通鍵暗号は量子攻撃の影響を軽微にしか受けず、鍵長を 2 倍にすれば安全性が保証されると長い間考えられていた。 しかし、最近の研究により、攻撃者がメッセージの量子重ね合わせで MAC/暗号化オラクルをクエリできる場合、Simon の量子周期発見アルゴリズムを用いることで多数の MAC/認証暗号方式を破ることが可能となる。特に、OCB 認証暗号モードはこの設定で破られるとともに、同じ効率(レート 1、並列化可能)で量子安全なモードは知られていない。

本論文は、これまでの攻撃を一般化し、OCB ライクな方式については量子重ね合わせクエリに対して安全でないことを示すとともに、認証暗号方式の量子安全性について議論する。また、TAE と OCB に着想を得た新しいレート 1 かつ並列化可能なモード QCB を提案し、量子重ね合わせクエリに対する安全性を証明する。

・On the non-tightness of measurement-based reductions for key encapsulation mechanism in the quantum random oracle model [Asiacrypt 2021]

Haodong Jiang, Zhenfeng Zhang, Zhi Ma

弱く安全な(weakly-secure)PKE を IND-CCA 安全な KEM に変える Fujisaki-Okamoto(FO)変換(TCC 2017)の KEM 変種は、NIST ポスト量子暗号標準化プロジェクトの中で広く使われた。標準的な CPA の安全性仮定、すなわち OW-CPA と IND-CPA の下で、量子ランダムオラクルモデル(QROM)におけるこれらの変種の安全性は、例えば Jiang ら(CRYPTO 2018)、および非ブラックボックス帰着(EUROCRYPT 2020)により証明された。非ブラックボックス帰着は、セキュリティロスは線形だが、厳密な可逆実装を持つ特定の可逆敵対者にしか適用することができない。一方、既存のブラックボックス帰着は、任意の実装を持つ任意の敵対者に適用可能だが、安全性の損失が 2 倍となる。

本論文では、FO 変換の KEM バリエーションについて、まずブラックボックス帰着の厳密性の限界を示し、QROM において、基礎となる PKE の標準的な OW-CPA(または IND-CPA)安全性を破ることから、結果の KEM の IND-CCA 安全性を破ることへの測定ベース(measurement-based)の帰着は、必然的に安全性の二次損失を引き起こすことを証明する(「測定ベース」とは、攻撃者からのハッシュクエリーを測定し、測定結果を使用して PKE の基礎を破ろうとするものである)。特に、これらの FO 変換に似た KEM 変種に対するブラックボックス帰着のほとんどはこのタイプであり、我々の結果は、安全性損失の程度という点で、この帰着の厳密性の向上が進んでいないことの説明を示唆する。

さらに、探索問題を決定問題に変換するときに、量子ランダムオラクルを含む暗号システムの安全性を証明するために不可欠な技術として認識されているブラックボックス的な一方向秘匿技術を使う際、2 次的な安全性損失も避けられないことも示される。

・Cryptanalysis of an oblivious PRF from supersingular isogenies [Asiacrypt 2021]

Andrea Basso, Péter Kutas, Simon-Philipp Merz, Christophe Petit, Antonio Sanso

Boneh、Kogan、Woo が Asiacrypt 2020 で提案した SIDH ベースの超特異楕円曲線同種に基づく擬似乱数関数(PRF)について暗号解析を行った。そのために、Boneh らが導入した補助的な仮定に対する攻撃を行い、これが紛失擬似乱数関数(OPRF)そのものに対する攻撃につながることを示す。この攻撃は、敵対者がいくつかの最初の OPRF 評価といくつかのオフライン計算の後、サーバーとそれ以上のやりとりをせずに OPRF を評価することを可能にするので、擬似ランダム性を破る。さらに、概念実証のための実装と、筆者らの攻撃のいくつかのタイミングを提供する。最後に、OPRF パラメータの 1 つの生成を検証し、証明可能なセキュリティを保証するためには、信頼できるサードパーティが必要であることを論じる。

・Secure and Efficient Software Masking on Superscalar Pipelined Processors [Asiacrypt 2021]

Barbara Gigerl, Robert Primas, Stefan Mangard

電力解析のような物理的なサイドチャネル攻撃は、実世界のアプリケーションにおいて暗号デバ

イスに深刻な脅威となる。そのため、デバイスはマスキングのようなアルゴリズムによる対策を実装している。これまで、マスキングされたソフトウェア実装の設計と検証は、スマートカードに搭載される単純なマイクロプロセッサを中心に行われてきた。しかし、自動車産業をはじめとする多くのアプリケーションでは、より高性能な CPU でサイドチャネル保護された暗号計算を行う必要がある。このような状況において、複雑なアーキテクチャの副作用によるセキュリティの損失、それに伴う性能低下、適切なプロービングモデル(probing model)や検証手法の議論は、まだ大きく未解決の研究課題となっている。

本論文は、これらの疑問に答え、より複雑なプロセッサアーキテクチャをマスキング関連の副作用の文脈で包括的に分析する。まず、9 段のパイプライン、2 つの実行ユニット、ロードストアバッファを備えた RISC-V SweRV コアを分析し、単純なソフトウェアプロービングモデル(software probing model)におけるセキュリティとこのような CPU における実用的なセキュリティの間に大きなギャップがあることを指摘する。具体的には、複雑な CPU アーキテクチャがもたらすアーキテクチャ上の副作用が、マスクされたソフトウェアの保護順位を著しく低下させることを、ハードウェアプロービングモデル(hardware probing model)における形式的な解析と、ゲートレベルタイミングシミュレーション(gate-level timing simulation)による経験的な解析の両面から明らかにした。次に、これらの問題をハードウェアで修正するか、ソフトウェアの制約として残すかの選択肢を議論する。これらのソフトウェア制約に基づき、より複雑な CPU 上でのマスクされたソフトウェアの設計のための一般規則を策定する。最後に、マスキング方式のいくつかの実装戦略を比較し、複雑な CPU のための安全なマスキングソフトウェアの設計が、13%という低いオーバーヘッドで可能であることをケーススタディで示す。

・Divided We Stand, United We Fall: Security Analysis of Some SCA+SIFA Countermeasures Against SCA-Enhanced Fault Template Attacks[Asiacrypt 2021]

Sayandeep Saha, Arnab Bag, Dirmanto Jap, Debdeep Mukhopadhyay, Shivam Bhasin

サイドチャネル攻撃(side-channel attack、SCA)と故障攻撃(fault attack、FA)に対する防御は、2 つのクラスの対策を同時に暗号実装に組み込む必要がある。SCA と FA の対策をストレートに組み合わせた場合、統計的非効率故障解析(Statistical Ineffective Fault Analysis、SIFA)や故障テンプレート攻撃(Fault Template Attack、FTA)などの FA に対して脆弱であることが既に示されている。そのため、SIFA を防止し、SCA を防止するためのマスキングを含む新しいクラスの対策が提案されてきた。これらの対策は、SIFA や SCA に対して個別に安全である一方、SCA と FA を組み合わせた敵が存在する場合にも安全性の主張が成り立つかどうかが重要な問題である。しかし、このような実装では、両方の脅威に対する対策が含まれているため、複合攻撃に対する安全性が望まれている。

本論文では、最近提案された SIFA と SCA を組み合わせた対策の一部が、複合攻撃の対象になることが示される。そのために、故障注入時のサイドチャネル情報を考慮することで FTA 攻撃を強化する。提案する攻撃の成功は、S-Box の非自明な障害伝播特性に起因しており、これは元の

FTA 提案では未解明な点である。また、SIFA で保護された $\chi 5$ S-Box をオープンソースのソフトウェアで実装し、レーザー故障注入とパワー計測を行い、SIFA で保護された $\chi 3$ S-Box をハードウェア実装し、ゲートレベルのパワートレースシミュレーションを行って、提案する攻撃を検証した。最後に、既存の対策を強化するためのいくつかの緩和策について述べる。

8.4. Asiacrypt 2021 の発表（4 日目）

・A Practical Key-Recovery Attack on 805-Round Trivium [Asiacrypt 2021]

Chen-Dong Ye, Tian Tian

キューブ攻撃(cube attack)は Trivium に対する最も重要な暗号解読技術の一つである。キューブ攻撃に基づく鍵回復攻撃は数多く確立されている。しかし、80 ビットの完全な鍵情報を実用的に回復できる攻撃はほとんどない。特に、これまでの実用的な鍵回復攻撃は、FSE 2013 で Fouque と Vannet が提案した 784 ラウンドの Trivium に対するものが最高だった。実用的な鍵回復攻撃を行うには、十分な数の低次の superpoly が必要となる。しかしながら、これは実験的なキューブ攻撃やランダムに選択したキューブを用いた division property に基づくキューブ攻撃では非効率となるため困難な課題となっている。

本論文では、キューブ攻撃における linear superpoly をターゲットとしてキューブの候補を構成するための新しいアルゴリズムが提案されている。実験により、構成したキューブを用いて linear superpoly を見つける成功確が 100%であることが示された。また、805 ラウンドの Trivium において、1000 以上の linear superpoly が得られた。42 個の独立した linear superpoly を用いて 805 ラウンドの Trivium に対して実用的な鍵回復攻撃を行い、攻撃可能ラウンド数を 21 ラウンド増加することができた。攻撃にかかる計算量は $2^{41.40}$ で、GTX-1080 GPU を搭載した PC で数時間以内に実行可能である。

・Algebraic Attacks on Rasta and Dasta Using Low-Degree Equations [Asiacrypt 2021]

Fukang Liu, Santanu Sarkar, Willi Meier, Takanori Isobe

Rasta と Dasta は、それぞれ CRYPTO 2018 と ToSC 2020 で提案された、完全準同型暗号になじむ共通鍵暗号プリミティブである。

本論文では、Rasta と Dasta の設計者が χ 演算の重要な特性を見逃していたことが指摘されている。この性質は、Rasta と Dasta の特殊な構造と相まって、代数的暗号解読の大幅な向上に直結する。特に、Rasta の攻撃的なバージョンであり、ブロックサイズがビット単位のセキュリティレベルよりわずかに大きい full Agrasta の 3 つのうち 2 つのインスタンスを理論的に破ることができることが示されている。さらに、Dasta は、刻々と変化するビット置換と決定論的線形変換からなる線形層を用いるため、Rasta よりも提案攻撃に対して脆弱であることを明らかにした。この暗号解析により、パラメータ$(n, \kappa, r) \in \{(327,80,4), (1877,128,4), (3545,256,5)\}$に対して、Dasta と Rasta の

セキュリティマージンを 1 ラウンドに削減した。ここで、n, κ, r は、それぞれブロックサイズ、セキュリティレベル、ラウンド数を表す。これらのパラメータは、対応する AND depth が合理的な時間で実装でき、同じセキュリティレベルを目標とするものの中で最も小さいものとなっている。

・Automatic Classical and Quantum Rebound Attacks on AES-like Hashing by Exploiting Related-key Differentials [Asiacrypt 2021]

Xiaoyang Dong, Zhiyu Zhang, Siwei Sun, Congming Wei, Xiaoyun Wang, Lei Hu

AES ライクなハッシュ関数(有名な PGV モードやそれらの変種として AES ライクな暗号や置換を加味して作られたハッシュ関数)に対する衝突攻撃は、その基礎となる AES ライクなプリミティブの差分に関する入力ペアを見つける問題に帰着することが可能である。Mendel らによるリバウンド攻撃(rebound attack)は、この目標を達成するための強力なツールであり、その量子版は EUROCRYPT 2020 で Hosoyamada-Sasaki によって初めて検討された。

本研究では、MILP に基づくアプローチにより、基礎となるブロック暗号の関連鍵の差分を考慮したリバウンド攻撃の構成を探索するプロセスを自動化することを目指す。量子設定において、著者らのモデルはリバウンド攻撃にかかる計算量やリソース(例えば、QRAM)を最小化した差分特性の探索を可能とする。本手法を Saturnin-hash、Skinny、Whirlpool に適用し、従来の結果を改善できることを示した。

・Clustering Effect in Simon and Simeck [Asiacrypt 2021]

Gaëtan Leurent, Clara Pernot, André Schrottenloher

Simon と Simeck は、ワード単位のローテーション演算とビット単位の AND 演算のみを用いた単純なラウンド関数を持つ軽量ブロック暗号である。既存研究において、差分解読法や線形解読法には同じ入出力を持つトレイルが多数存在するため、強いクラスタリング効果があると示されている。

本論文では、アクティブビットが w ビットの固定ウィンドウに留まる高確率の差分・線形トレイルのクラスを示すことでこのクラスタリング効果を詳細に分析している。差分特性や線形近似に寄与する優れたトレイルの集合を列挙する代わりに、指定したクラス内に含まれる全てのトレイルを考慮して確率分布を計算する。この結果、既存の結果よりも強力な識別器を構成することができ、この識別器を Simon と Simeck に対する鍵回復攻撃に応用することで、従来の結果と比較して攻撃可能ラウンド数を最大 7 ラウンド向上したことが報告されている。特に、42 ラウンドの Simeck-64 に対しては 2 ラウンドのセキュリティマージンを残す攻撃、45 ラウンドの Simon-96/144 に対してはセキュリティマージンを 16 ラウンドから 9 ラウンドに減らす攻撃が示されている。

・New Attacks on LowMC instances with a Single Plaintext/Ciphertext pair [Asiacrypt 2021]

Subhadeep Banik, Khashayar Barooti, Serge Vaudenay, Hailun Yan

攻撃者が単一の既知平文/暗号文のペアにアクセスできることを仮定した場合、ブロック暗号

LowMC に対する暗号解析は数学的に困難な問題となっている。これは、攻撃者が線形解読法や差分解読法のような共通鍵暗号に対する一般的な暗号解読技術を用いることができないためである。このシナリオは電子署名方式 Picnic の安全性を論じる際に特に関連性が高い。具体的には、LowMC で生成された平文/暗号文のペアが Picnic の公開鍵(検証鍵)となり、対応する LowMC の秘密鍵が Picnic の秘密鍵(署名鍵)となる。Banik らの論文(IACR ToSC 2020)では、LowMC の S-box に対して線形変換技術を使用することにより、LowMC におけるいくつかのインスタンスに対して攻撃を適用している。

本論文では、まず線形変換攻撃(Linearization attack)のより正確な計算量分析が行なわれる。さらに、LowMC に対して 2 段階の中間一致攻撃を行う方法が示されている。第一段階では、マスターキーのキービットのうち一定の割合に相当する鍵候補を削減する。第二段階では、第一段階において削減された鍵候補の集合と残りのキービットの割合を利用してマスターキーの回復を行う。これらの段階を組み合わせた計算量は、Banik らが示した計算量よりも大幅に削減できていることが示されている。

8.5. Asiacrypt 2021 の発表(5 日目)

・Convexity of division property transitions: theory, algorithms and compact models [Asiacrypt 2021]

Aleksei Udovenko

積分暗号は共通鍵暗号プリミティブを攻撃するための強力なツールであり、division property は積分識別器(integral distinguisher)を見つけるための最先端のフレームワークである。

本研究では、従来のビットベース division property に対する新たな理論的・実用的な知見が述べられる。特に、division property の monotonicity/convexity という性質とこの性質におけるグラフ指標との関連に焦点が当てて解析されている。著者らの解析結果は、伝搬特性のコンパクトな表現につながり、軽量ブロック暗号の 16 ビット Super-Sbox や 32 ビットランダム S-box のような、より大きな S-box の CNF/MILP モデリングを可能にするものである。これは、Derbez と Fouque (ToSC 2020)が提起した、16 ビット Super-Sbox の SAT/SMT/MILP モデリングの可能性に疑問を呈する課題を解決するものである。これまでのアプローチでは実現不可能であった、8 ラウンド LED の Super-Sboxes を CNF 式によるモデル化も行われている。

・Massive Superpoly Recovery with Nested Monomial Predictions [Asiacrypt 2021]

Kai Hu, Siwei Sun, Yosuke Todo, Meiqin Wang, Qingju Wang

キューブ攻撃において、対象となるキューブの superpoly に関する代数構造または部分情報を正確に決定することは、攻撃を実行する上で重要なステップとなっている。現在、superpoly を正確に回復するには、division property に基づくアプローチが最も強力な手段となっている。しかし、ラウンド数の増加に伴い、対象となる出力ビットの代数的標準形(algebraic normal form、

ANF)が複雑になるため、superpoly を回復する既存手法にはボトルネックが存在する。実際に、Trivium、Grain-128AEAD、Kreyvium に対する既存手法では、攻撃可能ラウンド数がそれぞれ 842、190、892 までに止まっている。

本論文では、単項式予測法(monomial prediction technique、ASIACRYPT 2020、division property の代替)に基づき、大規模な superpoly に関する ANF を正確に回復する新しいフレームワークが提案される。この新しいフレームワークを Trivium, Grain, Kreyvium に適用することで、845 ラウンドの Trivium、191 ラウンドの Grain-128AEAD、894 ラウンドの Kreyvium における superpoly を回復することが可能となった。さらに、メビウス変換の助けを借り、スパース構造を利用することで全てのキービットを含む superpoly に対する新しい鍵回復技術を提示し、対象となる暗号方式に対して最良の鍵回復攻撃ができるようになった。

・Quantum Linearization Attacks [Asiacrypt 2021]

Xavier Bonnetain, Gaëtan Leurent, María Naya-Plasencia, André Schrottenloher

最近の研究では、量子重ね合わせクエリモデルを仮定した状況において、量子周期探索を用いると Even-Mansour 構成のようなブロック暗号、MAC、認証暗号などの多くの暗号方式を破ることができると報告されている。これまでに解読された暗号方式は全て強い代数的構造を有しており、単一の入力ブロックに関する周期関数を構成することが可能となっている。この周期を発見することで、秘密鍵の回復や暗号利用モードの機密性・真正性の保持を破ることができる。

本論文では、量子重ね合わせクエリモデルを仮定した状況において、MAC を対象に Simon のアルゴリズムを用いた新しい攻撃手法「量子線形変換攻撃」(Quantum linearization attack)が提案されている。さらに、他の量子アルゴリズム(Deutsch、Bernstein-Vazirani、Shor の 3 種類)を用いた本攻撃のバリエーションも紹介される。これらのアルゴリズムが共通鍵暗号に対する量子暗号解読や鍵回復攻撃に利用されたのは、著者らの知る限り今回が初めてである。これらの攻撃は、LightMAC、PMAC などの並列化可能な MAC や、(古典的な)誕生日攻撃に対する安全性を保証している方式(LightMAC+、PMAC+)、tweakable ブロック暗号を用いたもの(ZMAC)など、多くの変種を破ることができる。より一般的には、並列化可能かつ量子安全な擬似ランダム関数(PRF)の構成が困難な課題であることを示している。

・Generic Framework for Key-Guessing Improvements [Asiacrypt 2021]

Marek Broll, Federico Canale, Antonio Florez-Gutierrez, Gregor Leander, Maria Naya-Plasencia

本論文では、ブロック暗号に対する鍵回復攻撃において重要な秘密鍵の推測手順を改善するための汎用的な手法を提案している。この手法は、S-box に関する新しい特性を定義し、これらの特性を決定木の特殊ケースとして表現することにより達成されるものであり、様々な攻撃手法に対するきめ細やかな推測戦略を見つけるために重要な概念となる。 このような決定木を効率的に見つけるアルゴリズムを提案・実装し、このアルゴリズムを用いて NOKEON、GIFT、RECTANGLE に対する

いくつかの応用例を提供する。

・NTRU Fatigue: How Stretched is Overstretched? [Asiacrypt 2021]

Wessel van Woerden, Léo Ducas

最近まで、NTRU 格子の格子簡約攻撃は、同じパラメータを持つ(ring)-LWE 格子の場合と同様の挙動を示すと考えられていた。しかし、いくつかの研究(Albrecht-Bai-Ducas 2016, Kirchner-Fouque 2017)は、大きなモジュラス q、いわゆる NTRU の overstretched 領域に対して大きなギャップがあることを示した。NTRU スキームは NIST PQC コンペティションの最終選考に残ったため、疲労点(fatigue point)がどこにあるのか、つまり、どの q で overstretched 領域が始まるのかを正確に理解することは、漸近的かつ具体的に重要である。

本論文では、Kirchner と Fouque の解析を漸近的に改善し、3 元 NTRU の疲労点を$q \leq n^{2.783+o(1)}$ から $q = n^{2.484+o(1)}$ まで絞り込み、最後にこの現象の背景を説明する新しい解析が提案される。この解析をさらに具体的に推し進め、疲労点を約 $q = 0.004 \cdot n^{2.484}$ に設定したとき、オーバーストレッチ領域における困難性の正確に予測することができるようになった。これらの予測は、広範な実験によって裏付けられている。

・Faster Dual Lattice Attacks for Solving LWE -- with applications to CRYSTALS [Asiacrypt 2021]

Qian Guo, Thomas Johansson

LWE 問題に基づく暗号システムには、LWE 問題を解くための汎用アルゴリズムのコストに関連するセキュリティレベルが割り当てられている。これには少なくとも、いわゆる格子攻撃と双対格子攻撃が含まれる。

本論文では、Bleichenbacher の研究に遡ることができるアイデアを用いて、双対格子攻撃の改良を提示する。提案手法では、格子簡約アルゴリズムにおける 2 つの最新技術、すなわち、「次元の自由化」と「1 回のふるい分けで多くの短いベクトルを生成する技術」を利用するが、この 2 つのトリックの非互換性が、双対格子攻撃が興味深くはない主な理由と考えられていた。そのため著者らの新しい削減戦略は、重要な暗号パラメータセットに対して、単純な格子攻撃よりも効率的な双対アプローチを可能にしている。

さらに、提案攻撃を NIST のポスト量子暗号プロジェクトの最終候補である CRYSTALS-Kyber と CRYSTALS-Dilithium に適用し、コア SVP モデルにおいて古典的および量子的に新しい低い計算量を与えることを示した。最も重要なことは、提案されたセキュリティパラメータについて、洗練された格子簡約戦略を用いた著者らの新しい双対攻撃が、古典的なゲートカウントメトリック(gate-count metric)、すなわち古典的 Random Access Machine(RAM)モデルにおける最先端の格子攻撃を大幅に改善したことである。具体的には、外挿モデルによる Kyber1024 では、改善係数が 15 ビットになる(Albrecht et al.at Eurocrypt 2019)。また、Kyber768 は、その主張するセキュリティレベル以下の古典的なゲート計算量で解くことができることを示す。さらに、Homomorphic

Encryption Standard のドラフト版(https://homomorphicencryption.org 参照)の提案されたパラメータに提案攻撃が適用された。結果、例えば 192 ビットの安全性を目指すパラメータセットを、古典的な RAM モデルで $2^{187.0}$ 回の操作で解くことが可能となった。これらのパラメータは、よく知られた Fully Homomorphic Encryption ライブラリで展開されている。

・Lattice sieving via quantum random walks [Asiacrypt 2021]

Johanna Loyer, André Chailloux

格子暗号は、ポスト量子暗号の有力な提案の一つである。最短ベクトル問題(Shortest Vector Problem、SVP)は格子暗号の暗号解析において最も重要な問題であり、多くの格子暗号はその困難性に基づく安全性を主張している。SVP に対する最良の量子アルゴリズムは Laarhoven [Laa16 PhD]によるもので、(ヒューリスティックに)時間 $2^{0.2653d + o(d)}$ で実行される(d は格子の次元)。

本論文では、Laarhoven の結果を改良し、(ヒューリスティックに)時間 $2^{0.2570\,d + o(d)}$ で実行されるアルゴリズムが提示される。また、本アルゴリズムの量子メモリと量子ランダムアクセスメモリの量を定量化し、時間とメモリの間のトレードオフを提示する。

・A Systematic Approach and Analysis of Key Mismatch Attacks on Lattice-Based NIST Candidate KEMs [Asiacrypt 2021]

Yue Qin, Chi Cheng, Xiaohan Zhang, Yanbin Pan, Lei Hu, Jintai Ding

格子ベースの KEM に対する鍵不一致攻撃の研究は、現在進行中の NIST のポスト量子暗号の標準化における暗号評価の重要な部分である。このような攻撃は数多く存在しているが、しかしこれらの KEM の鍵不一致攻撃に対する耐性を評価する統一的な手法はまだない。効率性の重要な指標は、そのような攻撃を成功させるために必要なクエリ数である。

本論文では、そのような攻撃に必要な最小平均クエリ数の下界を求める体系的アプローチの提案、開発を行った。基本的な考え方は、クエリの下限を求める問題を最適なバイナリ復元木(binary recovery tree、BRT)を見つけることに変換することである。この BRT において、下限の計算は、本質的には特定のシャノンエントロピーの計算となる。またこの最適 BRT のアプローチにより、いくつかの格子ベースの NIST 候補 KEM において、必要なクエリの数に関して、理論的な下限と実際の攻撃で観測された下限の間に大きなギャップがある理由を説明できる。さらにこれら既存攻撃に対する汎用的な改善方法が提案され、実験により確認された。提案された手法は、CCA 安全な NIST 候補 KEM に対するサイドチャネル攻撃を改善するために直接利用することができる。

CRYPTREC Report 2021
(暗号技術評価委員会報告 CRYPTREC RP-2000-2021)

発行日　2022 年 6 月 30 日　第 1 版
発行者
・〒184-8795
東京都小金井市貫井北町四丁目 2 番 1 号
国立研究開発法人情報通信研究機構
（サイバーセキュリティ研究所 セキュリティ基盤研究室）
NATIONAL INSTITUTE OF
INFORMATION AND COMMUNICATIONS TECHNOLOGY
4-2-1 NUKUI-KITAMACHI,KOGANEI
TOKYO,184-8795 JAPAN

・〒113-6591
東京都文京区本駒込二丁目 28 番 8 号
独立行政法人情報処理推進機構
（技術本部 セキュリティセンター 暗号グループ）
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN
2-28-8 HONKOMAGOME,BUNKYO-KU
TOKYO,113-6591 JAPAN