CRYPTREC Report 2023

令和 6 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-2000-2023

「暗号技術評価委員会報告」

CRYPTREC Report 2023

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 2023 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 2023 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)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、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を監視し、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を判断した。2)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)の設置を継続し、國廣昇先生に主査をご担当いただき、「CRYPTREC 暗号技術ガイドライン(耐量子計算機暗号)」及びその根拠資料となる研究動向調査報告書の執筆方針を決定した。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」を示す予測図を更新した。また、b)軽量暗号に関する「CRYPTREC 暗号技術ガイドライン(軽量暗号)2023 年度版」を作成し、公開した。ガイドラインは、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した。そして、NIST において標準化された軽量暗号 ASCON を対象とした実装性能評価を外部評価により実施、さらに、軽量暗号に関わる標準化動向に関わる調査を外部評価により実施し、これらの外部評価、および、昨年度までに実施した外部評価等を基に加筆し、作成した。

2000 年に IT 基本法が制定されたほぼ同時期に CRYPTREC が発足し、以来、24 年間にわたる CRYPTREC 活動は、安心・安全な ICT 社会の実現に貢献してきた。2019 年から始まったコロナ禍以後、非接触・非対面での生活様式を可能とする ICT の利活用が急速に進んできており、今後も様々な分野において ICT の高度化・多様化が予想されている。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たない。

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」と表記する)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」と表記する)と独立行政法人情報処理推進機構(以下「IPA」と表記する)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」と表記する)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。2023 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)」にて検討される。

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。

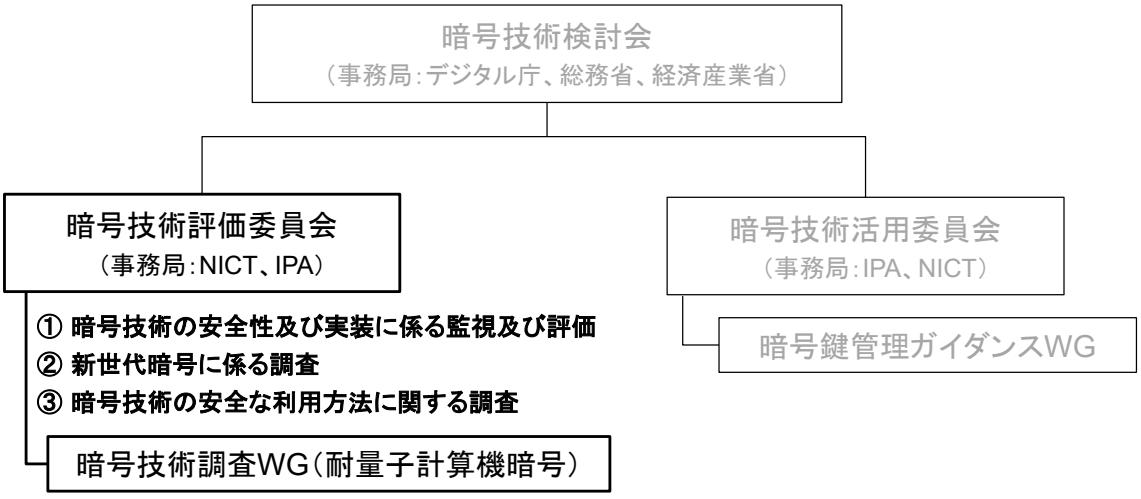

図 0.1：CRYPTREC 体制図

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 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 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	産業技術総合研究所 首席研究員
委員	藤崎 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 IS 研究所 顧問／ ＮＰＯ日本ネットワークセセキュリティ協会　フェロー[*1]
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	下山 武司	国立情報学研究所 特任准教授
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	成定 真太郎	ＫＤＤＩ総合研究所　コアリサーチャー
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 教授

オブザーバー

高木 浩光	内閣官房内閣サイバーセキュリティセンター
宮崎 俊一	内閣官房内閣サイバーセキュリティセンター
水野 邦俊	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[2023 年 12 月まで]
泉 雅巳	内閣官房内閣サイバーセキュリティセンター[2024 年 1 月から]
千葉 亮輔	デジタル庁 デジタル社会共通機能 G
渡辺 良光	デジタル庁 デジタル社会共通機能 G[2023 年 12 月から]
武井 亮	デジタル庁 デジタル社会共通機能 G
稲見 唯睦	デジタル庁 デジタル社会共通機能 G
當波 孝明	デジタル庁 デジタル社会共通機能 G
青島 一路	総務省 自治行政局 住民制度課
河合 直樹	総務省 サイバーセキュリティ統括官室
荒木 友愛	総務省 サイバーセキュリティ統括官室
重信 真也	総務省 サイバーセキュリティ統括官室[2023 年 9 月から]
榎 聡美	総務省 サイバーセキュリティ統括官室
佐久間 明彦	外務省 大臣官房
水村 優斗	外務省 大臣官房
加藤 優一	経済産業省 商務情報政策局[2023 年 7 月から]
塚本 大介	経済産業省 商務情報政策局[2023 年 9 月まで]
味木 耕平	経済産業省 商務情報政策局[2023 年 9 月から]
椛木 隆慎	防衛省 整備計画局
井上 智樹	警察大学校
岡野 孝子	警察大学校

事務局

国立研究開発法人情報通信研究機構（盛合 志帆、篠原 直行、青野 良範、伊藤 竜馬、大久保 美也子、小川 一人、金森 祥子、黒川 貴司、吉田 真紀、笠井 祥、大川 晋司）
独立行政法人情報処理推進機構(神田 雅透、新保 淳、福岡 尊、松﨑 博子、白岩 裕子)

*1：2024年3月に所属変更

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の排除、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考慮すべき点があるが、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するためには、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するための取り組みを実施することが非常に重要である。また、過去 24 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。そして、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な課題となった。

このため、2003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、暗号技

[1] https://www.cryptrec.go.jp/list/cryptrec-ls-0001-2022.pdf
[2] https://www.cryptrec.go.jp/list_2003.html

術評価委員会が改組され、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。暗号技術監視委員会では、電子政府推奨暗号リスト改訂のため、2008年度において、「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。2009年度からは、電子政府推奨暗号リスト改訂のための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]を策定した。

2013年度からは、名称を「暗号方式委員会」から再び「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。詳しくは、1.4節を参照のこと。

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年度までは、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、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、2021年度から2022年度までは、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、そして、2023年度から再度、暗号技術調査ワーキンググループ（耐量子計算機暗号）が設置されている。その間、暗号技術調査ワーキンググループ(軽量暗号)では、2016年度に「CRYPTREC暗号技術ガイドライン(軽量暗号)」[4]を、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）では、2022年度にそれぞれ「CRYPTREC暗号技術ガイドライン(耐量子計算機暗号)」[5]及び「CRYPTREC暗号技術ガイドライン(高機能暗号)」[6]を作成し公表している。また、2023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）の活動の詳細については、第3章を参照のこと。これらのガイドラインの他に、2016年度に策定した「CRYPTREC暗号技術ガイドライン(軽量暗号)」を改定し、2023年度に「CRYPTREC暗号技術ガイドライン(軽量暗号) 2023年度版」[7]を作成し、公表した。この改定の詳細については、第2章を参照のこと。

[3] https://www.cryptrec.go.jp/list/cryptrec-ls-0001-2012r8.pdf
[4] https://www.cryptrec.go.jp/report/cryptrec-gl-2003-2016jp.pdf
[5] https://www.cryptrec.go.jp/report/cryptrec-gl-2004-2022.pdf
[6] https://www.cryptrec.go.jp/report/cryptrec-gl-2005-2022.pdf
[7] https://www.cryptrec.go.jp/report/cryptrec-gl-2006-2023.pdf

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)[8]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。

2013 年度からは、2021 年度までに CRYPTREC 暗号リストの小改定が行われ、いくつかの暗号技術が推奨候補暗号リストに追加された。暗号技術評価委員会では、2016 年度にハッシュ関数 SHAKE128 を、2017 年度に認証暗号 ChaCha20-Poly1305 を、2019 年度に暗号利用モード（秘匿モード）XTS を、安全性評価及び実装性能評価を実施して十分な安全性および実装性能を有していると判断したことから CRYPTREC 暗号リストの推奨候補暗号リストに追加する提案を暗号技術検討会に対して行っている。

2020 年度において、暗号技術検討会では、量子コンピュータ時代に向けた暗号の在り方検討タスクフォースにおける検討を踏まえて、CRYPTREC 暗号リストの 3 リスト構成（電子政府推奨暗号リスト、推奨候補暗号リスト、運用監視暗号リスト）を維持することを決定し、推奨候補暗号リストから暗号技術を削除するルールを含めた、移行ルールが明確化された[9]（図 1.1 を参照）。

2022 年度は、暗号技術評価委員会では、メール審議（期間：2023 年 1 月 30 日～2 月 10 日）を行い、CRYPTREC 暗号リスト改定に係る暗号技術を現状のままとすることに決定し、その後、暗号技術検討会は、「電子政府における調達のために参照すべき暗号の

[8] https://www.cryptrec.go.jp/topics/cryptrec_201212_listpc.html
[9] https://www.cryptrec.go.jp/report/cryptrec-mt-1021-2020.pdf

リスト（CRYPTREC 暗号リスト）」（案）に対するパブリックコメント（期間：2023 年 3 月 9 日～3 月 23 日）を実施し、「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）」[10](付録 1 を参照)を策定した。2023 年度には、暗号リストが更新され、一部の項目に対し注意書きが付与された。

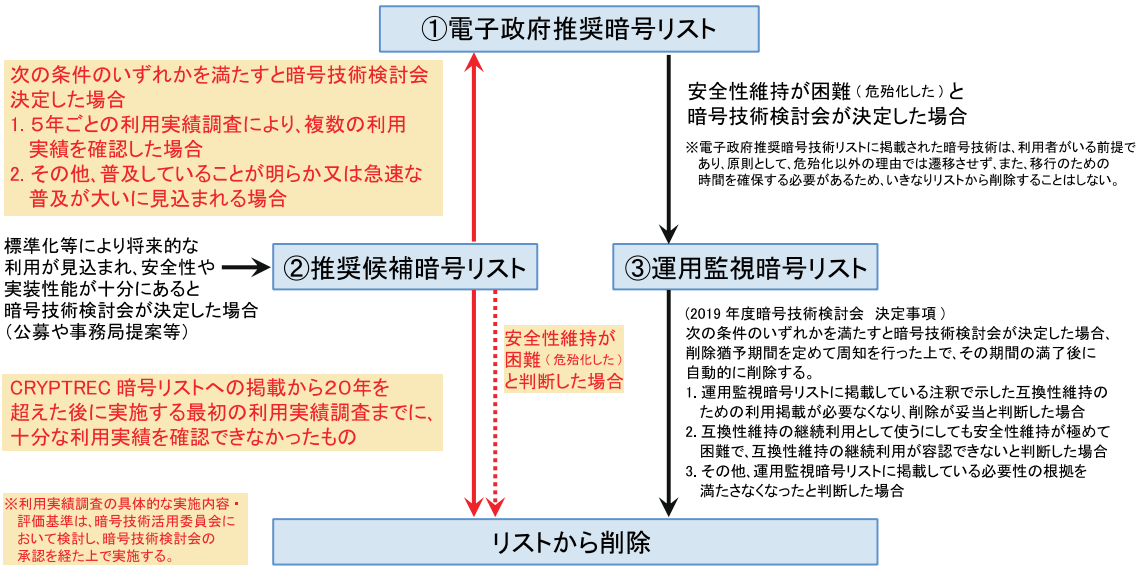

図 1.1：CRYPTREC 暗号リスト移行ルール

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。

[10] https://www.cryptrec.go.jp/list/cryptrec-ls-0001-2022.pdf

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：
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 2023 年度については、CRYPTREC 暗号リストとは別文書として、耐量子計算機暗号、及び、軽量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。
- 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い、2023 年度版「CRYPTREC 暗号技術ガイドライン(軽量暗号)」を作成する。

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[11]掲載の暗号技術に対する考え方[12]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

[11] 2003 年 2 月 20 日に策定されたものを指す。
[12] 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

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 1.2 を参照)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。

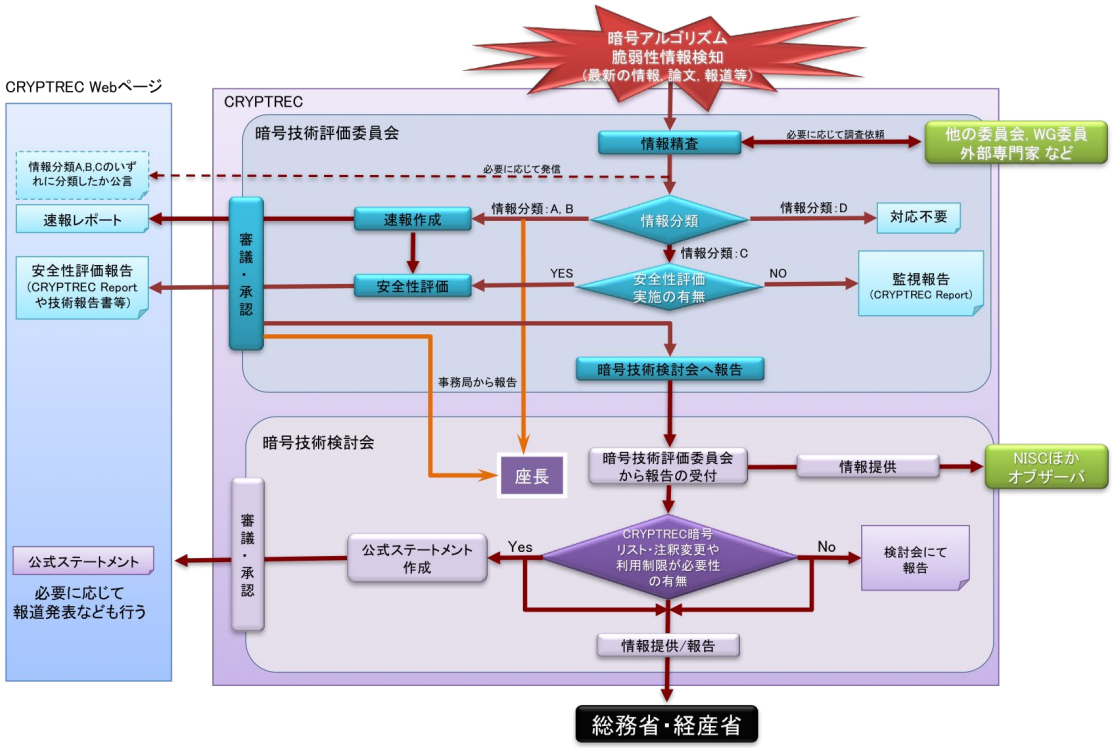

図1.2：暗号アルゴリズムの脆弱性に関する情報発信フロー

[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の周知

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、2023 年度の報告時点で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. Triple DES に関する NIST の情報

米国 NIST は、Triple DES（TDES[1]）の標準化文書である NIST SP 800-67 Rev.2 を 2023 年 12 月 31 日に削除した[2]。そして、米国 NIST のウェブサイトによると、「SP 800-67 Rev.2 の廃止は予定されたものであり、これは TDES が容認されたブロック暗号ではなくなったことを意味する。TDES はすでに暗号化されたデータの復号、キーラッピングの解除、MAC の検証などを目的とする場合に限り許容されるものである。そして、SP 800-67 Rev.2 は歴史的経緯を残しておく目的としてオンライン上で利用可能である。」と明記されている。原文は以下のとおり。

The scheduled withdrawal of SP 800-67 Rev. 2 will signify that TDEA is no longer an approved block cipher. TDEA will continue to be allowed for the decryption, key unwrapping, and verification of MACs of already-protected data, and SP 800-67 Rev.2 will remain available online for historical purposes.

2.1.2. 共通鍵暗号に関する安全性評価について

今年度は、2022 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。

ブロック暗号 AES に対する解析論文が FSE 2023、Eurocrypt 2023、Crypto 2023 で報告された。FSE 2023 の解析論文では、7 ラウンド AES に対する鍵回復攻撃が計算量（データ、時間、メモリ）$2^{110.2}$以下で実行可能であることが示された。Eurocrypt 2023 の解析論文では、切り詰め差分とブーメラン攻撃を組み合わせた新しい攻撃手法が提案され、6 ラウンド AES に対する識別攻撃と鍵回復攻撃がそれぞれ時間計算量2^{87}と2^{61}で実行可能であることが示された。Crypto 2023 の解析論文では、差分攻撃と中間一致攻撃を組み合わせた新しい攻撃手法として差分中間一致攻撃が提案され、12 ラウンド AES-256 に対する関連鍵設定での鍵回復攻撃が時間計算量2^{206}、データ量2^{89}、メモリ量$2^{71.6}$、

[1] 米国では TDEA（Triple DATA Encryption Algorithm）として標準化されている。
[2] https://csrc.nist.gov/news/2023/nist-to-withdraw-sp-800-67-rev-2

2 つの関連鍵で実行可能であることが示された。2 つ（最小）の関連鍵のみ使用できると言う条件の中では、既存研究における攻撃可能ラウンド数を 2 ラウンド更新することに成功した。なお、AES の仕様段数は使用する秘密鍵のサイズによって異なる。AES-128、AES-192、AES-256 の仕様段数はそれぞれ 10、12、14 ラウンドである。

ストリーム暗号 ChaCha に対する解析論文が FSE 2023 と Crypto 2023 で報告された。FSE 2023 の解析論文では、6 ラウンド ChaCha に対する鍵回復攻撃が計算量$2^{99.48}$で実行可能であることが示された。Crypto 2023 の解析論文では、7 ラウンド ChaCha に対する鍵回復攻撃が時間計算量$2^{210.3}$とデータ量$2^{103.3}$で実行可能であることが示された。また、最終ラウンドの XOR と Rotation を行わない 7.5 ラウンド ChaCha に対する鍵回復攻撃が時間計算量$2^{242.4}$とデータ量$2^{125.8}$で実行可能であることが示された。なお、ChaCha の仕様段数は 20 ラウンドである。

ハッシュ関数 RIPEMD-160 に対する解析論文が Eurocrypt 2023 で報告された。この解析論文では、36 ラウンド RIPEMD-160 に対する衝突攻撃が時間計算量$2^{64.5}$で実行可能であることが示された。なお、RIPEMD-160 の仕様段数は 80 ラウンドである。

ハッシュ関数 SHA3 に対する解析論文が FSE 2023 と Eurocrypt 2023 で報告された。FSE 2023 の解析論文では、4 ラウンド SHA3-384 に対する衝突攻撃が時間計算量$2^{59.64}$、メモリ量$2^{45.94}$で実行できることが示された。Eurocrypt 2023 の解析論文では、4 ラウンド SHA3-512 と 5 ラウンド SHAKE256 に対する衝突攻撃がそれぞれ時間計算量2^{237}と2^{185}で実行できることが示された。また、4 ラウンド SHA3-512 に対する原像攻撃が時間計算量$2^{504.58}$で実行できることが示された。なお、SHA3 の仕様段数は全て 24 ラウンドである。

上記のとおり、AES、ChaCha、RIPEMD-160、SHA3 に対する暗号解析において進展が見られたものの、セキュリティマージンはまだ十分にあるため、これらの暗号解析がそれぞれの安全性に直ちに影響を及ぼすものではない。

2.1.3. 公開鍵暗号に関する安全性評価について

今年度は、CRYPTREC 暗号リスト掲載の公開鍵暗号に関する解読について大きな進展はなかった。

2.1.4. その他の注視すべき技術動向

耐量子計算機暗号の解析に関して大きな進展が見られた。特に、2022 年 8 月にプレプリントとして公表された SIKE（NIST PQC 第 4 ラウンド候補）の解読に関する解析論文が Eurocrypt 2023 で報告された。また、この解析手法を一般化・改良した研究成果も複数報告された。その他、小さなパラメータを有する Falcon への解析や、BIKE に対する鍵回復攻撃の検討などの進展が見られた。

実社会へのインパクトのある話題として、クラウドストレージサービス MEGA におけ

る RSA 秘密鍵が漏洩する脆弱性について、Eurocrypt 2023 と PKC 2023 で報告された。なお、これらの解析手法は MEGA に組み込まれた RSA に対してのみ有効であり、RSA が脆弱性を有することを意味するものではない。

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. 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は行わなかった。

2.4. 軽量暗号に関するガイドラインの作成について

2019 年度に設置された量子コンピュータ時代に向けた暗号の在り方検討タスクフォースにて、「CRYPTREC において、軽量暗号は CRYPTREC 暗号リストには組み込まず、別途ガイドラインという形で取り扱う」ことが決定された。2020 年度第 2 回暗号技術検討会にて、2016 年度作成した「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」という）を 2023 年度中に更新することが承認された。2021 年度第 2 回暗号技術評価委員会において、「CRYPTREC 暗号技術ガイドライン（軽量暗号）2023 年度版」（以下、「2023 年度版ガイドライン」という）の作成に向けた更新方針が承認された。NIST 軽量暗号標準化プロジェクト（以下、「NIST LWC」という）では、2023 年 2 月に最終選考結果が発表され、Ascon が選定された。

このような背景の下、今年度は Ascon に焦点を当てた実装性能及び Ascon を選定するに至った選考過程や選考理由に関して、外部有識者による技術動向調査を実施した。また、ガイドラインの更新方針に基づき、CRYPTREC 事務局で 2023 年度版ガイドラインを作成した。この際、2023 年度版ガイドラインの掲載内容の適切性や情報の過不足に関して、外部有識者によるレビューを実施し、レビュー結果を反映させた。

2.4.1. 軽量暗号に関する技術動向調査

NIST LWC の最終選考方式として Ascon が選定されたことを踏まえ、今年度は Ascon に焦点を当てた実装性能評価を外部評価により実施した。また、Ascon を選定するに至った選考過程や選考理由に関して、NIST が公開する文書等を中心とした標準化動向に関する調査を外部評価により実施した。

実施概要

Ascon に関する実装性能評価と標準化動向調査について、以下のとおり実施した。

- 実装性能評価：物理攻撃[3]耐性を持つ実装性能評価も含め、公開されている評価結果を調査し、評価結果についてまとめ、考察などを行い、評価報告書を作成する。
- 標準化動向調査：NIST LWC の公募により、Ascon が選定されるに至った選定指標や評価の観点をまとめるとともに、軽量暗号に関する標準化動向について公開情報を参考としてまとめ、考察などを行い、調査報告書を作成する。

調査結果概要

実装性能評価

Ascon の実装面における特徴、物理攻撃対策を施した Ascon の実装性能、Ascon に対する物理攻撃耐性評価について確認した。

- 実装面における特徴:実装コストと処理性能のトレードオフの観点で高い柔軟性を有する。例えば、コンパクトな S-box を同時に処理することで実装コストを犠牲にして高い処理性能を得ることができる一方、異なる時間に S-box を再利用することで処理性能を犠牲にして実装コストを下げることができる。
- 実装性能：代表的な物理攻撃対策技術として、Threshold Implementation[4]とその発展的技術である Domain Oriented Masking[5]があり、これらの物理攻撃対策を施した Ascon の実装評価に関して、2 件の文献を参考に調査結果をまとめるとともに、考察を行った。
- 物理攻撃耐性評価:代表的な物理攻撃耐性評価技術として、相関電力解析[6]、Test Vector Leakage Assessment[7]、テンプレート攻撃[8]、などがあり、これらの評価技術を用いた Ascon の物理攻撃耐性評価に関して、6 件の文献を参考に調査結果をまとめるとともに、考察を行った。

標準化動向調査

NIST LWC の最終ラウンドにおける評価基準と選定プロセス、Ascon が選定されるに至った選定指標と評価の観点、Ascon の標準化動向について確認した。

- 評価基準と選定プロセス：NIST が公開するステータスレポート NISTIR 8454[9]を

[3] サイドチャネル攻撃等を含めた物理的な攻撃という意味で、本資料では物理攻撃という用語を使用する。
[4] 秘密分散法に基づくマスキング手法
[5] d次プロービングモデルに対して耐性のあるマスキング手法
[6] 電力のサイドチャネル情報を効率よく解析する手法
[7] サイドチャネルからの漏洩評価における統計的手法
[8] 事前に攻撃対象モジュールの特性を評価したテンプレートを準備し、このテンプレートを使用してパラメータを操作できない攻撃対象モジュールの秘密鍵を推定する手法
[9] https://csrc.nist.gov/pubs/ir/8454/final

参考に、評価基準と選定プロセスの対応関係を表 2.1 のとおりまとめた。

- 選定指標と評価の観点：同様に、選定指標と評価の観点について表 2.2 のとおりまとめた。
- 標準化動向：IETF[10]、W3C[11]、ISO/IEC[12]、ITU-T[13]、Global Platform の 5 団体を対象とし、Ascon の標準化動向についてまとめた。結果として、2023 年 9 月現在、IETF でのみ、インターネットドラフトやワーキンググループで Ascon が取り上げられていることが確認できた。

表 2.1：NIST LWC 最終ラウンドにおける評価基準と選定プロセス

評価基準	選定プロセス
暗号学的安全性	第三者による安全性評価、耐量子安全性
制約のある環境下におけるソフトウェア及びハードウェアでの実装性能	ベンチマーク
サイドチャネル攻撃	ベンチマーク
知的財産	知的財産に関する声明
その他	バリエーション、設計の微調整

表 2.2：Ascon が選定されるに至った選定指標や評価の観点

選定指標	評価
機能	● 認証暗号モードとハッシュモードに加え、XOF[14]機能を含む。 ● 暗号学的置換ベースの設計により、追加機能の実装コストが少ない。
成熟度	● CAESAR コンペティションのユースケース１（軽量アプリケーション） ● 最終ラウンドにおける設計の微調整なし
安全性	● 第三者による安全性評価が最も多いファイナリスト ● 他ファイナリストよりも先行的に安全性評価が行われているにも関わらず依然として高い安全性を維持
実装性能	● ソフトウェアとハードウェアの両面で非常に優れた性能を発揮 ● 実装コストと処理性能の様々なトレードオフをサポートする柔軟性 ● 物理攻撃対策にかかる追加コストが低い。

外部評価報告書に対する暗号技術評価委員会の見解

提出された外部評価報告書は、今年度の調査対象である Ascon の実装性能及び標準化動向に関する技術動向調査として十分な内容を含んでいると考えられることから、本報告書を CRYPTREC の技術調査報告書とすることが了承された。

[10] Internet Engineering Task Force
[11] World Wide Web Consortium
[12] International Organization for Standardization/International Electrotechnical Commission
[13] International Telecommunication Union Telecommunication Standardization Sector
[14] eXtendable Output Function：可変長出力関数

2.4.2. 2023 年度版ガイドラインの作成

2021 年度から 2023 年度にかけて実施した軽量暗号に関する技術動向調査（安全性評価、実装性能評価、標準化動向調査）に基づき、CRYPTREC 事務局にて 2023 年度版ガイドラインを執筆・編集した。また、2023 年度版ガイドラインの作成に当たり、ドラフト版の内容に関して外部有識者によるレビューを実施した。

実施概要

2023 年度版ガイドラインの作成について、以下のとおり実施した。

- ガイドライン（ドラフト版）の作成：ガイドラインの更新方針及び 2021 年度から 2023 年度にかけて実施した軽量暗号に関する技術動向調査に基づき、CRYPTREC 事務局にて 2016 年度版ガイドラインの更新を行う。完成したものを 2023 年度版ガイドライン（ドラフト版）とする。
- 2 名の外部有識者によるレビュー：CRYPTREC 事務局が作成した 2023 年度版ガイドライン（ドラフト版）について、2 名の外部有識者がその更新内容の妥当性等を評価し、レビュー報告書を作成する。また、第 2 回暗号技術評価委員会にてレビュー結果を報告する。
- ガイドライン（案）の作成：レビュー結果の基づき、CRYPTREC 事務局にて 2023 年度版ガイドライン（ドラフト版）の更新を行う。更新内容について外部有識者に了承を得たものを 2023 年度版ガイドライン（案）とする。
- ガイドライン公開に関する審議：第 2 回暗号技術評価委員会にて、2023 年度版ガイドライン（案）が CRYPTREC 暗号技術ガイドラインとして公開するにふさわしいかを審議する。

2023 年度版ガイドラインの概要

2023 年度版ガイドラインの目次とその概要は表 2.3 のとおり。

2023 年度版ガイドライン（案）に対する暗号技術評価委員会の見解

作成した 2023 年度版ガイドライン（案）は、軽量暗号に関する最新動向を踏まえて 2016 年度版ガイドラインを更新したものであり、暗号技術ガイドラインとして十分な内容を含んでいると考えられる。また、外部有識者によるレビュー結果で更新内容の妥当性が評価されている。以上から、2023 年度版ガイドライン（案）を CRYPTREC 暗号技術ガイドラインとすることが了承された。

表 2.3：2023 年度版ガイドラインの目次とその概要

章		章タイトル	概要
第 1 章		はじめに	導入、謝辞
第 2 章		軽量暗号とその活用法	
	2.1	軽量暗号とは	定義、代表的な軽量暗号
	2.2	軽量暗号の標準化動向	● CAESAR コンペティション ● NIST LWC ● 他標準化団体における ASCON の検討状況
	2.3	軽量暗号はどこに使えるのか	家電、スマートテレビ、スマート農業、医療、自動車、等での活用例
	2.4	どんな軽量暗号、パラメータを選べばいいか	一般的方針、鍵長・ブロック長の選択、利用シナリオ、等
	2.5	軽量暗号活用例と効果	家電、スマートテレビ、スマート農業、医療、自動車、等での効果
第 3 章		軽量暗号の実装性能	
	3.1	ブロック暗号の実装性能	12 種類の軽量ブロック暗号に対するハードウェア・ソフトウェア実装評価
	3.2	認証暗号の実装性能	10 種類の軽量認証暗号に対するソフトウェア実装評価
	3.3	ASCON の実装性能	● ハードウェア実装性能 ● ソフトウェア実装性能 ● 物理攻撃耐性評価
第 4 章		代表的な軽量暗号	
	4.1	ブロック暗号	各技術分野の各方式に関する仕様等[15]の調査結果
	4.2	ストリーム暗号	
	4.3	ハッシュ関数	
	4.4	メッセージ認証コード	
	4.5	認証暗号	
付録 A		ASCON の物理攻撃耐性	
	A.1	サイドチャネル攻撃対策	● Threshold Implementation ● Domain Oriented Masking
	A.2	サイドチャネル解析・漏洩評価	● 相関電力解析 ● 故障利用攻撃 ● Test Vector Leakage Assessment ● テンプレート攻撃
付録 B		CAESAR final portfolio: AEGIS, COLM	AEGIS、COLM に関する仕様等の調査結果
付録 C		NIST LWC ファイナリスト（ASCON を除く）	ASCON を除く NIST LWC ファイナリスト 9 方式に関する仕様等の調査結果

2.5. 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

[15] 設計者、発表年、仕様参照先、特徴、安全性解析状況、主な実装性能評価、標準化状況、等

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
FSE 2023	The 29th International Conference on Fast Software Encryption	中国・北京 日本・神戸 (Hybrid)	3 月 20 日 ～ 3 月 24 日
Eurocrypt 2023	The 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques	フランス・リヨン (Hybrid)	4 月 23 日 ～ 4 月 27 日
PKC 2023	The 26th International Conference on Practice and Theory in Public Key Cryptography	米国・アトランタ (Hybrid)	5 月 7 日 ～ 5 月 10 日
PQCrypto 2023	The 14th International Conference on Post-Quantum Cryptography	米国・カレッジパーク	8 月 16 日 ～ 8 月 18 日
Crypto 2023	The 43rd Annual International Cryptology Conference	米国・サンタバーバラ	8 月 19 日 ～ 8 月 24 日
FDTC 2023	The 20th Workshop on Fault Diagnosis and Tolerance in Cryptography	チェコ・プラハ (Hybrid)	9 月 10 日
CHES 2023	The 25th Annual Conference on Cryptographic Hardware and Embedded Systems	チェコ・プラハ	9 月 10 日 ～ 9 月 14 日
TCC 2023	Theory of Cryptography 20th International Conference	台湾・台北	11 月 29 日 ～ 12 月 2 日
Asiacrypt 2023	The 29th Annual International Conference on the Theory and Application of Cryptology and Information Security	中国・広州	12 月 5 日 ～ 12 月 9 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４を参照のこと。

2.5.1. 共通鍵暗号の解読技術

Cryptanalysis of Reduced Round ChaCha – New Attack & Deeper Analysis [FSE 2023]

Sabyasachi Dey, Hirendra kumar Garai, Subhamoy Maitra

ストリーム暗号 ChaCha に対する解析論文である。最初に、分割統治法を使用して秘密鍵ビットを効率的に分割する方法を検討する。この分割方法は複数の入出力差分を使

用することで実現でき、結果として、6 ラウンド ChaCha を計算量$2^{99.48}$で攻撃可能であることが示された。これは既存攻撃よりも2^{40}倍高速である。次に、計算量評価の見積もり方法を分析する。ChaCha に対する既存の計算量評価は一般的に理論的な見積もりが与えられているが、Eurocrypt 2022 で Dey らはこの理論的な見積もり方法にいくつかの問題点があることを指摘した。そこで、32 ビットの秘密鍵を有する ChaCha のトイモデルを対象とし、計算量見積もりの正しさを検証した。この検証結果に基づき、6 ラウンド ChaCha に対する計算量を見積もった。最後に、成功確率の見積もり方法を考察する。PNB ベースの既存攻撃では成功確率が約 50%と見積もられていた。本研究では成功確率の正確な範囲、つまり成功確率の上界と下界の理論値を示すとともに、トイモデルでこの理論値の正しさを検証した。この理論値を使用して既存攻撃（FSE 2008 で報告された Aumasson らの攻撃と 2006 年に Discret. Appl. Math.で報告された Maitra の攻撃）の成功確率を再見積もりし、Aumasson らの攻撃の成功確率の範囲が 79.9%～84.2%、Maitra の攻撃の成功確率の範囲が 99.7%～99.8%であることを示した。

New Key Recovery Attack on Reduced-Round AES [FSE 2023]

Navid Ghaedi Bardeh, Vincent Rijmen

ブロック暗号 AES に対する解析論文である。Asiacrypt 2017 で Ronjom らはゼロ差分特性（zero-difference property）と呼ばれる 4 ラウンド AES の新しい性質を報告した。本研究では、このゼロ差分特性に対して新しい洞察を提供することで、ゼロ差分特性の一般化を目指しており、この目的を達成することで、ゼロ差分特性のより単純な定式化と解釈を提供することが可能となる。

ゼロ差分特性の一般化のために、本研究では Daeman と Rijmen によって報告された関連差分（related differences と related differentials）の概念を使用し、SPN 型共通鍵暗号のためのゼロ差分特性を再定義する。最も注目すべき点は、SPN 型共通鍵暗号におけるゼロ差分特性に関連差分が埋め込まれていることである。最大 4 ラウンドの関連差分をゼロ差分特性に埋め込むことで、ゼロ差分特性を最大 8 ラウンドまで拡張できるようになる。本研究では、4 ラウンドの関連差分をゼロ差分特性に埋め込むことで得られる 7 ラウンド AES の新しい関連差分特性を提供する。この新しい関連差分特性を利用することで、7 ラウンド AES に対する鍵回復攻撃を計算量（データ、時間、メモリ）$2^{110.2}$以下で実行可能となる。

Finding Collisions against 4-round SHA-3-384 in Practical Time [FSE 2023]

Senyang Huang, Orna Agmon Ben-Yehuda, Orr Dunkelman, Alexander Maximov

ハッシュ関数 SHA3-384 に対する解析論文である。SHA3 に対する最も強力な衝突攻撃は、2020 年に Journal of Cryptology で Guo らが報告した線形化手法に基づくものである。しかしながら、この手法は SHA3-224 や SHA3-256 のような入力サイズ（レートサ

イズ）が大きいバリアントに対して有効であるものの、SHA3-384 や SHA3-512 のような入力サイズの小さいバリアントに対して適用できないという問題があった。

本研究では、以下に示す新しい 3 つのアイデアを提案することで、既存研究における課題を克服する。1 つ目は、提案攻撃では 1 ブロック分のメッセージではなく 2 ブロック分のメッセージを使用することである。これにより、衝突を発見するための制約が緩和され、柔軟性のある解析が可能となる。2 つ目は、既存の線形化手法を適用する代わりに SAT (Boolean satisfiability problem) 手法を使用することである。具体的には、要求される差分条件を満たすようなメッセージの値を SAT 手法で探索する。これにより、メッセージの値からより広い範囲の入力差分へと接続することが可能となり、差分特性を選択する際の柔軟性の向上に繋がる。3 つ目は、Keccak の非線形層における非ランダム性を検知するための 2 つの新しいツールと deduce-and-sieve アルゴリズムを開発したことである。このアルゴリズムを使用することで、SAT ソルバーを直接呼び出す場合と比べ、UNSAT となるケースのほとんどを効率的に検出することが可能となる。結果として、4 ラウンド SHA3-384 に対する衝突攻撃が時間計算量$2^{59.64}$、メモリ量$2^{45.94}$で実行できることを示した。

Truncated Boomerang Attacks and Application to AES-based Ciphers [Eurocrypt 2023]

Augustin Bariant, Gaëtan Leurent

AES ベースのブロック暗号（AES、Kiasu-BC、Deoxys-BC、TNT-AES）に対する解析論文である。AES ベースのブロック暗号に対する効果的な解析手法の 1 つにブーメラン攻撃がある。この攻撃は 1 つの長い差分を使用する代わりに 2 つの短い差分を組み合わせて解析する手法である。実際に、Kiasu-BC や Deoxyx-BC に対する最良の攻撃はブーメラン攻撃によって達成されている。

本研究では切り詰め差分（truncated differential）を用いたブーメラン攻撃に関する一般的なフレームワークを提供する。また、このフレームワークを使用することで、AES ベースのブロック暗号に対する既存のブーメラン攻撃を大幅に改善できることを示す。一般的なブーメラン攻撃では、最初に効果的なブーメラン識別子を探索したのち、鍵回復フェーズについて検討する。一方、提案するフレームワークでは、鍵回復フェーズも考慮してブーメラン識別子を探索する。このために、平文側と暗号文側の 1 ラウンド分の差分伝搬を注意深く解析する必要がある。結果として、6 ラウンド AES に対する識別攻撃と鍵回復攻撃がそれぞれ時間計算量2^{87}と2^{61}で実行可能であることを示した。その他、提案するフレームワークを Kiasu-BC、Deoxyx-BC、TNT-AES に適用することで、それぞれ既存攻撃を改善できることを示した。

Analysis of RIPEMD-160: New Collision Attacks and Finding Characteristics

with MILP [Eurocrypt 2023]

Fukang Liu, Gaoli Wang, Santanu Sarkar, Ravi Anand, Willi Meier, Yingxin Li, Takanori Isobe

ハッシュ関数 RIPEMD-160 に対する解析論文である。MD-SHA ハッシュ関数族（MD4、MD5、SHA0、SHA1）の多くが解読されているにも関わらず、RIPEMD-160 は今もなお高い安全性を確保しており、ISO/IEC 標準として採用されている。実際に、仕様段数が 80 ラウンドである RIPEMD-160 への最良の攻撃は、35 ラウンドの原像攻撃と 34 ラウンドの衝突攻撃である。

本研究では 4 つの主要な貢献がある。1 つ目は、メッセージ差分を選択する新しい戦略を提案したことである。2 つ目は、差分特性の性質を注意深く抽出することで、RIPEMD-160 における両方のブランチで同時にかつ効率的にメッセージ修正（message modification）を実行するための方法論を提案したことである。3 つ目は、RIPEMD-160 の差分特性を効率的に探索するために、符号付き差分（singed differential）特性探索のための MILP（Mixed Integer Linear Programming）手法を初めて提案したことである。4 つ目は、符号付き差分特性の探索における矛盾した結果を自動的に検出するための新しい方法を提案したことである。これらの提案手法に基づき、36 ラウンド RIPEMD-160 に対する衝突攻撃が時間計算量$2^{64.5}$で実行可能であることを明らかにした。

Collision Attacks on Round-Reduced SHA-3 Using Conditional Internal Differentials [Eurocrypt 2023]

Zhongyi Zhang, Chengan Hou, Meicheng Liu

ハッシュ関数族の SHA3（SHA3-224/256/384/512、SHAKE128/256）に対する解析論文である。SHA3 の中でも SHA3-512 は衝突攻撃に対して最も強い耐性を示しており、4 ラウンド SHA3-512 に対する衝突攻撃が時間計算量2^{263}（誕生日攻撃よりも2^6倍高速）で実行可能であることが知られている。また、SHAKE256 に対する衝突攻撃についてはまだ報告されていない。

本研究は 2010 年に Peyrin が報告した条件付き内部差分攻撃（conditional internal differential attack）と FSE 2013 で Dinur らが報告したターゲット内部差分アルゴリズム（TIDA: target internal difference algorithm）に触発され、SHA3 解析のために一般化された内部差分を改善するとともに、6 つの SHA3 バリアントに対する理論的な解析結果を示す。主要な貢献は 3 つある。1 つ目は、誕生日攻撃のバリアントを提案したことである。2 つ目は、差分遷移条件や差分条件表という新しい概念を抽象化し、既存の条件付き内部差分攻撃を改良したことである。3 つ目は、既存の TIDA を改良したことである。これらの提案手法に基づき、SHA3 に対する新しい衝突攻撃を開発し、結果として最大 5 ラウンドまでの衝突攻撃が実行可能であることを示した。特に、4 ラウンド SHA3-512 と 5 ラウンド SHAKE256 に対する衝突攻撃がそれぞれ時間計算量2^{237}と

2^{185}で実行できることを示した。

Meet-in-the-Middle Preimage Attacks on Sponge-based Hashing [Eurocrypt 2023]

Lingyue Qin, Jialiang Hua, Xiaoyang Dong, Hailun Yan, Xiaoyun Wang

スポンジベースのハッシュ関数（SHA3-512、Xoodyak-XOF、Ascon-XOF）に対する解析論文である。Markle-Damgard 構成のハッシュ関数に対して、中間一致技術を用いた原像攻撃に関する研究成果が数多く報告されている。一方、スポンジベースのハッシュ関数（特に、Keccak/SHA3）に対して、線形化技術を用いた原像攻撃が主流となっており、中間一致技術を用いた原像攻撃に関するフレームワークが確立されていない。

本研究では、スポンジベースのハッシュ関数に対して適用可能な中間一致技術に基づく原像攻撃の汎用フレームワークを提供する。この新しいフレームワークはビットレベルの MILP ベース自動探索手法に基づいている。従来研究におけるバイトレベルのモデリング手法とは異なり、ビットレベルのモデリング手法ではモデルが大規模となり、現実的な時間内に解を得ることが困難になる。そこで、対象となるハッシュ関数の構造を詳細に分析し、それぞれの構造に適したモデリング手法を適用することで、MILP モデルの削減を目指した。

提案手法を SHA3-512、Xoodyak-XOF、Ascon-XOF に適用した。4 ラウンド SHA3-512 に対する原像攻撃が時間計算量$2^{504.58}$とメモリ量2^{108}で実行できることを示した。3 ラウンド Xoodyak-XOF に対する原像攻撃が時間計算量$2^{125.06}$とメモリ量2^{97}で実行できることを示した。また、4 ラウンド Ascon-XOF に対する像攻撃が時間計算量$2^{124.67}$とメモリ量2^{54}で実行できることを示した。

Differential Meet-In-The-Middle Cryptanalysis [Crypto 2023]

Christina Boura, Nicolas David, Patrick Derbez, Gregor Leander, María Naya-Plasencia

ブロック暗号の SKINNY-128-384 と AES-256 に対する解析論文である。本研究では、差分攻撃と中間一致攻撃を組み合わせた新しい攻撃手法である差分中間一致攻撃を提案する。具体的には、差分攻撃の概念を使用し、解析対象の暗号化関数における中間ラウンドをカバーしながら、その外部ラウンドに対して中間一致攻撃を実行するものである。従来の Demirci-Selçuk 中間一致攻撃も同様のアプローチを採用しているが、特に鍵回復フェーズにおいて提案手法の方が効率的に実行できることを示している。

提案手法を単一鍵設定における SKINNY-128-384 と関連鍵設定における AES-256 に適用した。結果として、25 ラウンド SKINNY-128-384 に対する鍵回復攻撃が時間計算量$2^{372.5}$、データ量$2^{122.3}$、メモリ量$2^{188.3}$で実行できることを示した。また、12 ラウンド AES-256 に対する関連鍵設定での鍵回復攻撃が時間計算量2^{206}、データ量2^{89}、メモリ量$2^{71.6}$、2 つの関連鍵で実行できることを示した。

Moving a Step of ChaCha in Syncopated Rhythm [Crypto 2023]

Shichang Wang, Meicheng Liu, Shiqi Hou, Dongdai Lin

ストリーム暗号 ChaCha に対する解析論文である。既存研究によると、ChaCha に対する最良の鍵回復攻撃は 20 ラウンド中 7 ラウンドまで有効であることが示されている。本研究では、7 ラウンド ChaCha に対する既存の鍵回復攻撃を改善するとともに、最終ラウンドの XOR と Rotation を行わない 7.5 ラウンド ChaCha に対する有効な鍵回復攻撃を初めて示す。

ChaCha に対するほぼ全ての既存研究では、PNB（Probabilistic Neutral Bits）の概念に基づいた差分線形攻撃が使用されている。PNB の概念を使用すると、秘密鍵ビットを 2 つの集合、すなわち重要な鍵ビット（non-PNB）の集合と非重要な鍵ビット（PNB）の集合に分割できる。本研究では、既存の PNB の概念をさらに洗練させるため、シンコペーション（syncopation）と呼ばれる新しい概念を導入した。この新しい概念を使用し、non-PNB に対して新たな制約条件を追加することで、相関性の高い（条件付き）PNB の集合を識別できるようになる。適切な（条件付き）PNB を特定することで、鍵回復攻撃の改善に貢献できることが知られているため、この新しい概念は理に適っている。

結果として、7 ラウンド ChaCha に対する鍵回復攻撃が時間計算量$2^{210.3}$とデータ量$2^{103.3}$で実行できることを示した。また、最終ラウンドの XOR と Rotation を行わない 7.5 ラウンド ChaCha に対する鍵回復攻撃が時間計算量$2^{242.4}$とデータ量$2^{125.8}$で実行できることを示した。

2.5.2. 公開鍵暗号の解読技術

2.1.2 節で述べたとおり、今年度は CRYPTREC 暗号リスト掲載の公開鍵暗号に関する解読について大きな進展はなかったため、本節で紹介する論文は無い。その他、付録４を参照のこと。

2.5.3. その他の解読技術

An Efficient Key Recovery Attack on SIDH [Eurocrypt 2023]

Wouter Castryck, Thomas Decru

本論文で、超特異同種 Diffie-Hellman プロトコル（SIDH）に対する効率的な鍵回復攻撃が発表された。この攻撃は Kani の reducibility criterion に基づいており、アリスとボブがプロトコル中に交換するねじれ点の像に強く依存している。開始曲線の自己準同型環の知識を前提とすれば、システムパラメータに依存する少数の整数の因数分解を除き、ヒューリスティックな多項式時間でこの攻撃は行われる。また、この攻撃はパーティの一方が 2-同種を使用し、開始曲線が非常に小さな次数のスカラー倍ではない

自己準同型を備えている場合、高速かつ簡単に実装可能である。これは NIST 耐量子暗号標準化の第 4 ラウンド候補となった SIDH のインスタンスである SIKE のケースに当てはまる。実際に、著者らはセキュリティレベル 1 を目指す SIKEp434 をシングルコアのプロセッサにより 10 分程度で解読する Magma での攻撃の実装を行った。

Caveat Implementor! Key Recovery Attacks on MEGA [Eurocrypt 2023]

Martin R. Albrecht, Miro Haller, Lenka Mareková, Kenneth G. Paterson

MEGA は大規模なクラウドストレージおよび通信プラットフォームであり、保存データのエンドツーエンドの暗号化を提供することを目的としている。Backendal らによる最近の解析論文（IEEE S&P 2023）では、MEGA のサービスプロバイダが実行可能な実用的な攻撃を提示され、MEGA 開発者が示していた安全性主張が無効化されるという結果となった。これに対し、MEGA 開発者は MEGA ユーザの RSA 秘密鍵に対して、既存攻撃を防ぐための軽量な健全性チェック機能を追加した。

本研究では、この新しい健全性チェック機能を分析し、ターゲットユーザの RSA 秘密鍵を復元するために、健全性チェック機能をいかにして悪用するかを示すとともに、結果として既存攻撃よりもわずかに高い計算量で RSA 秘密鍵を復元できることを示す。具体的には、MEGA システムにおけるターゲットユーザのマスター鍵に関し、ECB 暗号化オラクルの存在を特定する。このオラクルは、攻撃者に対して、ターゲットユーザの RSA 秘密鍵を選択したデータで部分的に上書きする機能を提供する。さらに、2 つの異なる攻撃手法を提供する。これらの攻撃では、ユーザ認証中における健全性チェックとその後の暗号化処理で発生する異なるエラー条件を悪用する。結果として、Backendal らの RSA 鍵回復攻撃を実行するためには 512 回のログイン試行数が必要であったものの、提案手法では 2 回のログイン試行数で十分であることが示された。

The Hidden Number Problem with Small Unknown Multipliers: Cryptanalyzing MEGA in Six Queries and Other Applications [PKC 2023]

Nadia Heninger, Keegan Ryan

Backendal らはクラウドストレージプロバイダの MEGA に悪用可能ないくつかの脆弱性を特定した。彼らは、悪意のあるサーバーが 512 回のログイン試行後にクライアントの RSA 秘密鍵を回復することができる RSA 鍵回復攻撃を実証した。

本論文では、MEGA プロトコルの脆弱性によって明らかになった追加情報を利用し、RSA 秘密鍵を復元するために必要なクライアントのログイン試行数がわずか 6 回である攻撃を示す。この最適化された攻撃は、いくつかの暗号解析技術を組み合わせたものである。特に、未知の小さな乗数を持つ Hidden Number Problem の亜種を定式化し、その解を与える。この問題に対する格子構成が、May と Ritzenhofen の因数分解問題に対する改善された結果を与えるために使用できることも示される。

2.6. 委員会開催記録

2023 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	2023 年 7 月 3 日	● 暗号技術評価委員会活動計画の具体的な進め方に関する報告 ● 暗号技術調査ワーキンググループ（耐量子計算機暗号）の活動計画案に関する審議 ● 軽量暗号ガイドラインの更新にあたり、NIST で標準化された ASCON に関する外部評価を行うことに関する審議 ● 軽量暗号ガイドラインの更新にあたり、外部有識者によるトータルのレビューを行うことに関する審議 ● 軽量暗号ガイドラインの更新について、公開までのスケジュールに関する報告 ● 監視状況報告 ● CRYPTREC シンポジウム 2023 開催に関する報告
第 2 回	2024 月 2 月 27 日	● 暗号技術調査ワーキンググループ（耐量子計算機暗号）の活動内容に関する報告 ● 軽量暗号に関する技術動向調査結果に関する、外部評価による技術動向調査結果に関する報告・審議 ● 軽量暗号ガイドラインの外部有識者によるレビュー結果に関する報告 ● 軽量暗号ガイドラインの更新に関する報告・審議 ● 監視状況報告 ● CRYPTREC Report 2023 作成について ● CRYPTRECシンポジウム2024開催について

2.7. 暗号技術調査ワーキンググループ開催記録

2023 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	2023 年 9 月 13 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）の活動計画に関する報告 ● 耐量子計算機暗号調査報告書・ガイドライン改定の方針に関する審議 ● 次回ワーキンググループ開催までのスケジュールに関する審議
第 2 回	2024 年 1 月 19 日	● 2023年度予測図の更新に関する審議 ● 次回ワーキンググループ開催までのスケジュールに関する審議 ● ガイドライン・調査報告書の章立てと内容に関する審議 ● 各委員の調査活動に関する報告 ● 耐量子計算機暗号調査報告書・ガイドライン改定の方針に関する審議 ● 暗号技術調査ワーキンググループ（耐量子計算機暗号）の活動報告案に関する審議

第 3 章 暗号技術調査 WG（耐量子計算機暗号）の活動

3.1 2023 年度暗号技術調査 WG（耐量子計算機暗号）活動経緯と活動内容の概要

2020 年度第 2 回暗号技術検討会において、2021 年度から暗号技術評価委員会の活動計画として 2 年をかけて PQC の研究動向を調査し、ガイドラインを作成することが決定された。暗号技術評価委員会は 2021-2022 年度に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、ガイドライン及び調査報告書を作成、公開した。

その後も、PQC 関連の技術開発、標準化活動が世界的に活発であることから、引き続き、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、PQC WG）を設置して下記 2 点の活動を行うことが 2023 年度第 1 回暗号技術評価委員会において承認された。

(1) NIST の PQC 標準化において第 4 ラウンドが進行中であることをはじめ耐量子計算機暗号に関する技術開発、標準化活動が引き続き世界的に活発であることから、動向を 2023 年度から 2 年間かけて調査・把握し、ガイドラインの改定を行う。

(2) 「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検討し、更新する。

3.2 WG委員の構成（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：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：成定 真太郎　　（KDDI 総合研究所）
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）

3.3　耐量子計算機暗号ガイドラインの作成

3.3.1 スケジュール（2023 年度第 1 回暗号技術評価委員会で承認）

年度	回	耐量子計算機暗号ガイドラインの議論・決定・報告
2023 年度	第 1 回 2023/9/13	✓　追記・改定の方針について議論 ✓　執筆担当者を議論
	第 2 回 2024/1/19	✓　追記・改定すべき項目及びその章立ての決定 ✓　調査の中間報告
2024 年度	第 1 回 (8 月頃を想定)	✓　中間報告、追加及び削除すべき暗号方式があれば議論
	第 2 回 (2 月頃を想定)	✓　内容の確定

3.3.2 第 1 回WG（2023/9/13）での実施内容及び決定事項

- ガイドライン及び調査報告書の作成
  - 2022 年度版ガイドライン、調査報告書をベースに 2024 年度版ガイドライン、調査報告書を作成する。改訂扱いではなく新規の扱いとすることで合意した。
  - 「PQC の活用方法」の章は 2022 年度版ではガイドラインのみであったが、2024 年度版からは調査報告書にも含めることで合意。それに合わせて内容を拡充し、ガイドラインには公知の事実のみを載せ、詳細は調査報告書に載せる。
  - 以下に例示したいくつかの暗号方式の扱いに関しては今後の動向を注視し、2023 年度第 2 回以降の WG で改めて議論を行うこととした。
    - ✧ NIST 標準化が決まっているが FIPS 文書が発行されていないため詳細が流動的なもの
    - ✧ NIST Additional Signatures 候補の中で、格子、符号、多変数、同種写像、ハッシュ関数のカテゴリに含まれるもの
    - ✧ MPC-in-the-Head など新たなカテゴリとして分類されているもの

- 調査活動と執筆活動の方針
  - PQC の研究成果が発表される主要な国際会議 Crypto、Eurocrypt、Asiacrypt、PQCrypto を中心に、開発・標準化の動向に関しても 2024 年 9 月 30 日までの情報を可能な限り調査する。その他主要な動向があれば可能な限り取り上げる。

- 2023 年度第 2 回 PQC WG での調査内容の報告
  各章の執筆担当者が 2023 年度第 2 回 PQC WG において、その時点までの調査内容を報告する。

- 記載すべき項目及び章立てと執筆担当者

	執筆担当者
i. はじめに	事務局（青野）
ii. PQC の活用方法	伊藤委員
iii. 格子に基づく暗号技術	下山委員、安田（雅）委員
iv. 符号に基づく暗号技術	成定委員
v. 多変数多項式に基づく暗号技術	安田（貴）委員
vi. 同種写像に基づく暗号技術	高島委員
vii. ハッシュ関数に基づく署名技術	廣瀬委員

3.3.3 第 2 回WG（2024/1/19）での実施内容及び決定事項

- 各章の執筆担当者が 2023 年度第 2 回 PQC WG において、その時点までの調査内容を報告。各章の大まかな更新内容が確認された。
- 調査報告書及びガイドラインの執筆方針について以下の執筆方針が決定された。
  - 1 章についても他の章と同様に、調査報告書は専門的な内容、ガイドラインには調査報告書から技術的に複雑な内容を省略し抜粋した内容とする。
  - 米国で FIPS 化が決まっている方式に関して、2024 年 9 月 30 日までに正式版が出版された場合には FIPS 版と更新部分を、FIPS 化されない場合には出版時期によって対応が異なるが、Initial draft 版とその更新差分を記述する方針とする。
  - Additional Signatures の候補を各章に記載するかどうかは執筆担当者の判断とする。
  - MPC-in-the-Head、Additional Signatures 提案方式の中でガイドライン中の計算問題の分類に含まれないものについて、大きな動きは認知されていないことから新章とはしない。

3.4 「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

3.4.1 予測図における分解記録のプロットについて

第 1 回 WG におけるご意見に従い、分解記録のプロットについては、図の中の該当する参考文献のところに、「文献に基づいてプロットしています」と追記した。

3.4.2 2023 年度予測図の更新

- 「今後の予測図の取り扱い」に基づいて予測図の更新を行った(図 1、2)。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、2023 年 6 月・11 月のベンチマーク結果を追加した。

- 図 1 と図 2 において TOP500.Org のアドレスに https と http の表記揺れがあるため、https に統一することで合意した。

＜今後の予測図の取り扱い＞

(1) いわゆるムーアの法則を仮定して外挿線を年度末からプラス20年後まで従来どおり直線で引き、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※として予測図を当面の間更新していく。

〈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。

※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、より現状に即した評価となっており、危殆化時期は他機関等が規定している暗号技術の利用期限よりも先に延びている。

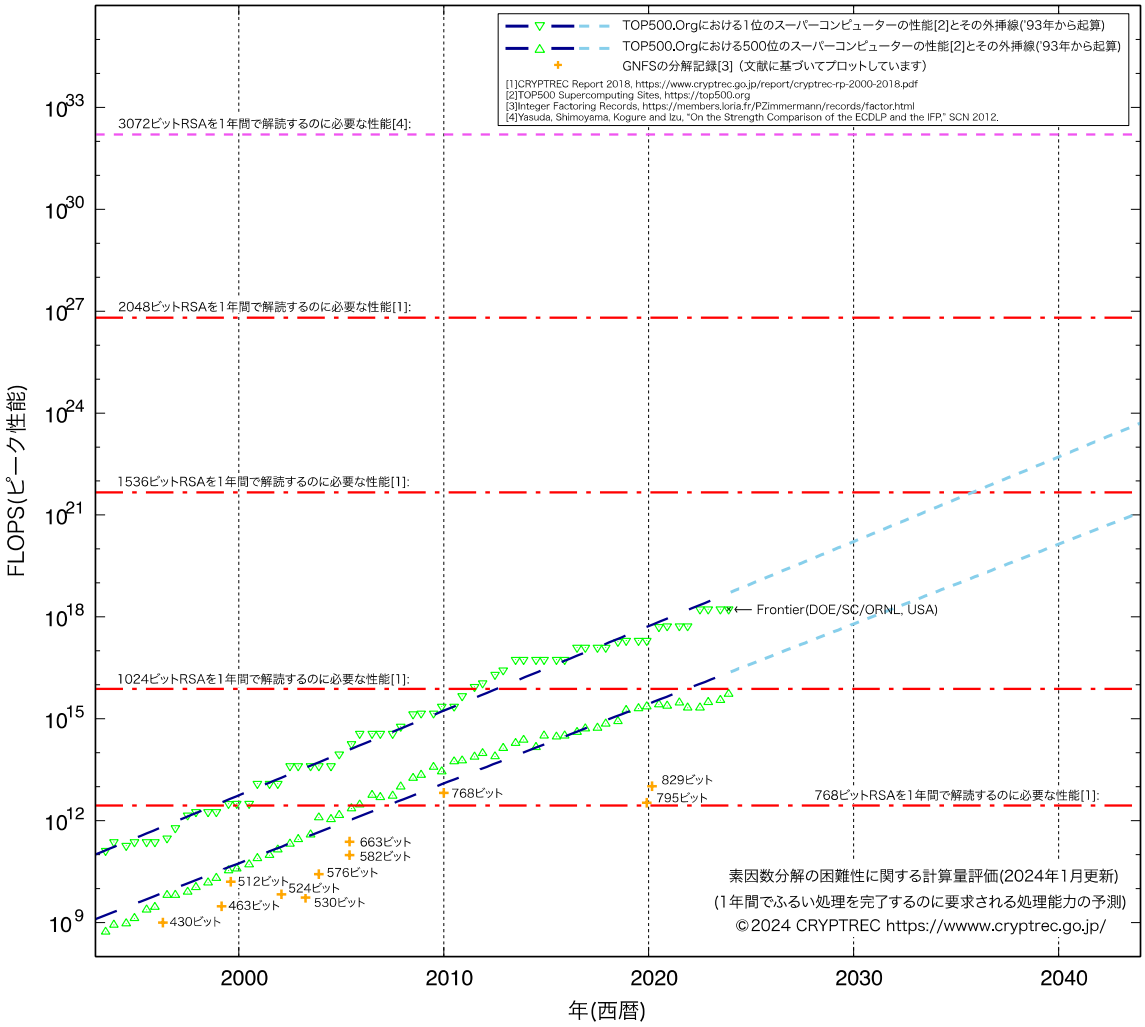

図 1：素因数分解の困難性に関する計算量評価（2024 年 1 月更新）[1]

[1] 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。

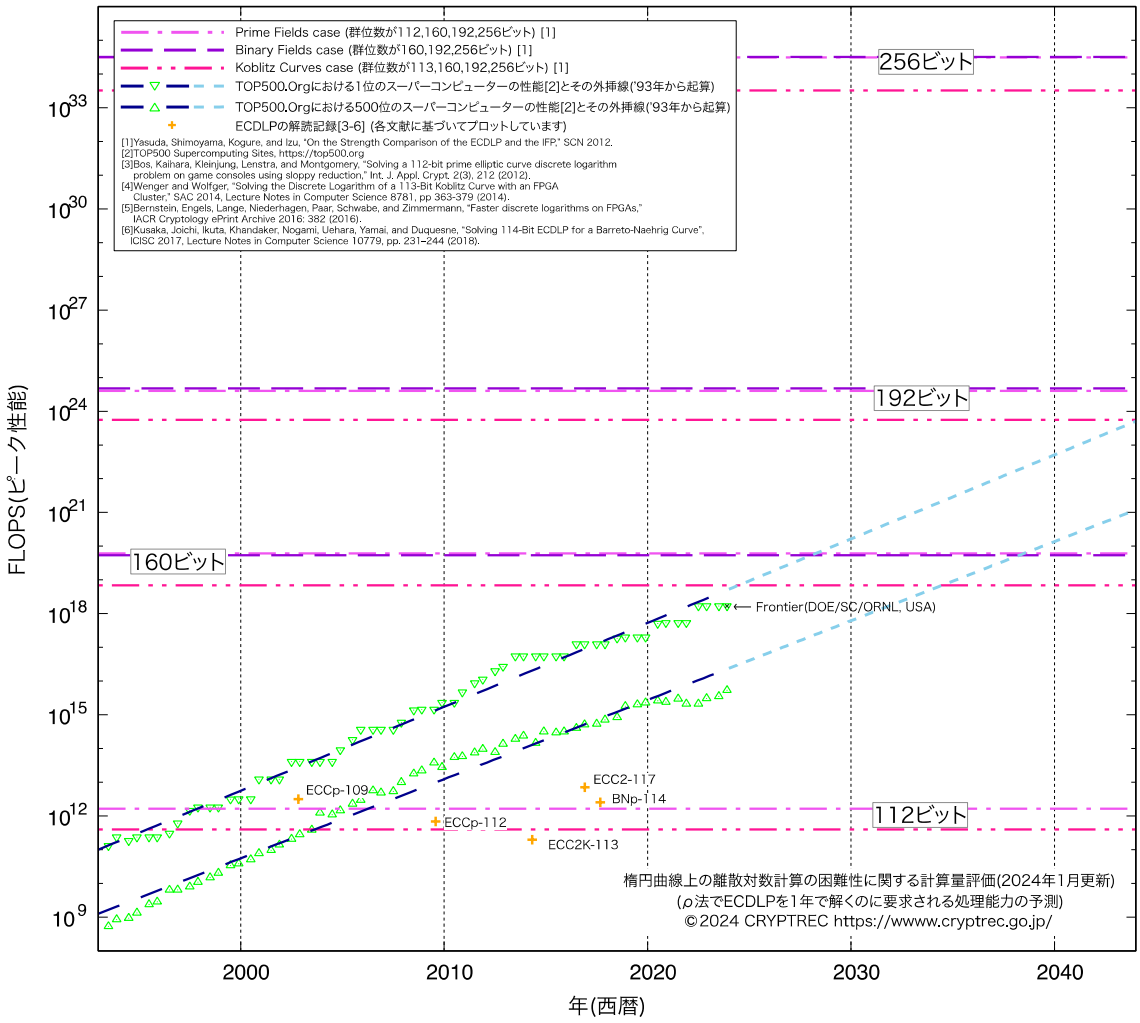

図 2：楕円曲線上の離散対数計算の困難性に関する計算量評価(2024 年 1 月更新)[2]

以上

[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。

付録1

CRYPTREC LS-0001-2022R1

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）

令和5年3月30日
デジタル庁・総務省・経済産業省
（最終更新：令和6年5月16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(注18)
		ECDSA
		EdDSA
		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
		SHA-512/256
		SHA3-256
		SHA3-384
		SHA3-512
		SHAKE128(注12)
		SHAKE256(注12)
（次ページに続く）		

[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

技術分類		暗号技術
暗号利用モード	秘匿モード	CBC
		CFB
		CTR
		OFB
		XTS(注17)
	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		ChaCha20-Poly1305
エンティティ認証		ISO/IEC 9798-2
		ISO/IEC 9798-3
		ISO/IEC 9798-4

（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12） ハッシュ長は256ビット以上とすること。

（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。

（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。

（注18） FIPS PUB 186-5では廃止されているが、本リスト掲載時から安全性・利用実績の状況に大きな変化がないため、掲載を継続する。

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	該当なし
	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
	ストリーム暗号	Enocoro-128v2
		MUGI
		MULTI-S01（注7）
ハッシュ関数		該当なし
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14）	該当なし
メッセージ認証コード		PC-MAC-AES
認証暗号		該当なし
エンティティ認証		該当なし

（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。

[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（注19）
	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。

（注19） SP 800-67 Revision 2では廃止されているが、本リスト掲載時から安全性・利用実績の状況に大きな変化がないため、掲載を継続する。

[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

更新履歴情報

更新日付	更新箇所	更新前の記述	更新後の記述
令和６年 5月16日	（注18）	[新規追加]	FIPS PUB 186-5では廃止されているが、本リスト掲載時から安全性・利用実績の状況に大きな変化がないため、掲載を継続する。
	（注19）	[新規追加]	SP 800-67 Revision 2では廃止されているが、本リスト掲載時から安全性・利用実績の状況に大きな変化がないため、掲載を継続する。

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	仕様
・ SEC 1: Elliptic Curve Cryptography (September 20, 2000, Version 1.0) https://www.secg.org/SEC1-Ver-1.0.pdf	
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) ・ 参照 URL https://www.x9.org/	

暗号名	EdDSA (Edwards-Curve Digital Signature Algorithm)
関連情報 1	仕様 *
・ NIST FIPS PUB 186-5, Digital Signature Standard (DSS), February 3, 2023 ・ 参照 URL https://csrc.nist.gov/publications/detail/fips/186/5/final	
関連情報 2	仕様*
・ Edwards-Curve Digital Signature Algorithm (EdDSA) ・ 参照 URL https://www.rfc-editor.org/rfc/rfc8032	

* [事務局注]［事務局注］暗号技術評価委員会におけるメール審議(2023 年 7 月 24～31 日)により、EdDSA の仕様の参照先は、NIST FIPS PUB 186-5 及び IETF RFC 8032 の 2 つを併記することになった。

暗号名	RSA Public-Key Cryptosystem with Probabilistic Signature Scheme (RSA-PSS)
関連情報	仕様 ・ PKCS #1: RSA Cryptography Standard Version 2.2 ・ 参照 URL https://www.rfc-editor.org/rfc/rfc8017.html

暗号名	RSASSA-PKCS1-v1_5
関連情報	仕様 ・ PKCS #1: RSA Cryptography Standard Version 2.2 ・ 参照 URL https://www.rfc-editor.org/rfc/rfc8017.html

暗号名	RSA Public-Key Cryptosystem with Optimal Asymmetric Encryption Padding (RSA-OAEP)
関連情報	仕様 ・ PKCS #1: RSA Cryptography Standard Version 2.2 ・ 参照 URL https://www.rfc-editor.org/rfc/rfc8017.html

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 ・ 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	仕様
・ SEC 1: Elliptic Curve Cryptography (September 20, 2000, Version 1.0) ・ 参照 URL https://www.secg.org/SEC1-Ver-1.0.pdf	
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@ntt.co.jp	

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:049-278-7500, 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, 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	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

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://csrc.nist.gov/publications/detail/sp/800-38e/final

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. 認証暗号

暗号名	ChaCha20-Poly1305
関連情報	仕様
	・ ChaCha20 and Poly1305 for IETF Protocols, June 2018 ・ 参照 URL https://www.rfc-editor.org/rfc/rfc8439.html

8. 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。

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。	

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@ntt.com

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　CIPHERUNICORN-E 問い合わせ窓口 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	〒100-8310 東京都千代田区丸の内 2-7-3 (東京ビル) 三菱電機株式会社 IT ソリューション事業センター 技術グループ MISTY1 問合せ窓口 E-MAIL：cryptrec_misty1_info@pj.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 CIPHERUNICORN-A 問い合わせ窓口 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	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	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	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. メッセージ認証コード

暗号名	PC-MAC-AES
関連情報	公開ホームページ
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　セキュアシステムプラットフォーム研究所　主席研究員 峯松 一彦 TEL：080-8823-8882 E-MAIL: k-minematsu@nec.com

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://www.rfc-editor.org/rfc/rfc8017.html

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
	・ The hash function RIPEMD-160 ・ 参照 URL https://homes.esat.kuleuven.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

軽量暗号の安全性に関する調査及び評価

「CRYPTREC 暗号技術ガイドライン（軽量暗号）2023 年度版」を作成にあたり実施した外部評価についてその概要を記載する。

目次

付録３－１

軽量暗号 Ascon の実装性能に関する調査及び評価

電気通信大学 大学院情報理工学研究科

崎山 一男

2023 年 9 月

原文は、CRYPTREC EX-3301-2023
https://www.cryptrec.go.jp/exreport/cryptrec-ex-3301-2023.pdf
で入手可能。

エグゼクティブサマリー

米国 National Institute of Standards and Technology (NIST) は，軽量暗号 (LWC: Lightweight Cryptography) コンペティション [34] で Ascon を選定した．本報告は，公開されている Ascon-128 の認証暗号モードにおける暗号化及び復号処理を行う実装研究を中心に論文を調査し，物理攻撃への耐性を持つハードウェア及びソフトウェア実装の性能評価結果をまとめ，考察を与えたものである．理論的安全性については，藤堂の文献 [48] を参照されたい．

Ascon は，認証暗号モードとハッシュモードに対応する軽量な暗号アルゴリズムであり，実装コストと処理パフォーマンスのトレードオフの点で高い柔軟性がある．つまり，ハードウェア実装でもソフトウェア実装でも，暗号機能を効率的に実現することができるため，様々なユースケースでの利用が期待される．高い柔軟性の理由は，以下のとおりである．

- 同じラウンド処理の繰り返しで実現できる
- ラウンド処理が並列実装にも対応できる
- 同じ 5 ビットの S-box が繰り返し使われている

5 ビットのコンパクトな S-box を同時に処理することで，実装コストの増加に見合う処理パフォーマンスを得ることができる．一方で，異なる時間に S-box を再利用して処理することで，処理パフォーマンスを犠牲にして実装コストを下げることができる．つまり，ハードウェア実装においては，インタフェースや求める性能に合わせてアーキテクチャを柔軟に変更することができ，ソフトウェア実装においては CPU のワードサイズに合わせたプログラミングが可能となる．また，複数のラウンド処理をまとめて計算することで，処理パフォーマンスのさらなる向上が実現できる．

Ascon が特に優れている理由のひとつは，ほとんど全ての処理を同じラウンド処理の繰り返して実現できる点にある．暗号化処理と復号処理の違いは，ラウンド処理における入出力データのインタフェース部分のみである．この極めて規則的な処理構造のおかげで，各モードの切り替えに対するオーバーヘッドは極めて小さくてすむ．AES 暗号にも，似たような実装上の性質はあるものの，暗号処理自体のデータパスが同じである Ascon は，実装における柔軟性がさらに高いと言える．

コンペティションで，AES 暗号が選定されたのは，1997 年 9 月であり，サイドチャネル攻撃の危険性を Kocher が最初に指摘したのが 1995 年 12 月である．そのため，AES 暗号に対してアルゴリズムレベルでの物理攻撃対策が十分に考慮できる状況ではなかった [24]．乱数によるマスキングや WDDL といった，サイドチャネル攻撃対策の研究が盛んになったのは 2000 年前後である [9, 43] ．つまり，Kocher によるサイドチャネル攻撃の論文や AES 暗号の選定により物理攻撃対策への研究者の意識が高まり，暗号アルゴリズムを新規に設計する場合においては，物理攻撃対策を含めた実装性は考慮すべきひとつの要素となった．Ascon はその最初の暗号アルゴ

リズムと言える．

その後，Nikova らによって Threshold Implementation (TI) が提案されたのが，2006 年である [32, 33]．現在 TI は，ハードウェア実装とソフトウエア実装の両方で多くの研究報告がなされており，現在も改良が進んでいる．Domain Oriented Masking (DOM) [20, 19] といった，TI よりもさらに効率的な実装を目指した対策技術が提案されるなど，暗号研究者内での理解は急速に進んだ．Ascon が最初に提案されたのは，2014 年の認証暗号のコンペティション CAESAR competition [4] である．Ascon を最初に提案したころは，最新の物理攻撃対策技術の成熟期にあった．実際に，Ascon-128 が物理攻撃対策との親和性が高い実装構造となっていることは興味深い事実である．

物理攻撃耐性を評価する手法にも大きな変化があった．サイドチャネル攻撃の発見直後は，鍵復元攻撃の成否や，少ない波形数での攻撃成功を目指すケーススタディが比較的多かった．非プロファイリング型の攻撃では選択関数やリーケージモデルの研究が，プロファイリング型の攻撃の場合ではテンプレートの作成方法に関する研究が研究の中心であった．これらは，攻撃者の能力に関するものである．適切な攻撃者が実装されていない場合には鍵が復元できないため，脆弱性は見つけることができない．さらに，実験における計算量の限界により攻撃を実装できない場合にも，脆弱性はないものとされてきた．つまり，攻撃が失敗したときには，暗号実装の安全性を判断することはできない．

現在では，Test Vector Leakage Assessment (TVLA) [18] による統計的に安全性を評価する手法が主流となっている．TVLA は，鍵が実際に導出できるかどうかを試すのではなく，サイドチャネルリークによる攻撃の可能性を判断するものである．未知の攻撃手法を含め，厳密に安全性評価が行えるようになった．現在の暗号アルゴリズムの実装研究では，TI といった乱数を用いたマスキング対策で物理攻撃を実装し，その安全性評価には TVLA を用いることが主流となっている．マスキング対策における実装上の問題は，冗長化した回路やプログラムのサイズによる実装コストと，マスキングに必要となる乱数コストである．実装コストを抑えるための研究成果は多く存在しているが，暗号アルゴリズム毎に最適な冗長化や乱数コストを狙う研究と，汎用的なコスト削減に向けた設計手法の確立を目指すものとに分かれる．

本報告では，最初に Ascon に適用する物理攻撃対策技術とその安全性評価手法に関する調査を行う．次に，実際のハードウェア実装及びソフトウェア実装における物理攻撃対策に関するケーススタディを 8 件を取り上げ，それらの内容をまとめた上で考察を与える．Ascon-128 の実装性能は非常に高く，特に物理攻撃対策については暗号研究者がこれまでに培った最新の技術を搭載しやすい構造である．一方で，今後 Ascon が，IoT デバイスとして様々なプラットフォームに実装されることを想定すると，対策を含めた暗号アルゴリズム実装について，その生産性の向上が重要となる．したがって，マスキング設計ツールやその安全性検証ツールを Ascon に適用した論文の調査を含め，今後の暗号実装研究の新たな方向性についても言及する．

付録３－２

軽量暗号 Ascon などに関わる標準化動向調査

GMO サイバーセキュリティ by イエラエ株式会社

2023 年 9 月

原文は、CRYPTREC EX-3302-2023
https://www.cryptrec.go.jp/exreport/cryptrec-ex-3302-2023.pdf
で入手可能。

エグゼクティブサマリー

本報告書では、NIST 軽量暗号コンペティションで 2023 年 2 月 7 日に選定された Ascon について標準化動向の調査を行った。Ascon の選定に関連する情報については、文献 [1]に詳しく記載されているため、この文献を中心に調査を行った。

Final Round では、最終候補として 10 のアルゴリズムが選択され、以下に示すような選考プロセスにおいて評価が行われた。

- 選考プロセスでのポイント
  - 様々な評価基準（安全性、ソフトウェアおよびハードウェアの性能、設計の成熟度、第三者による安全性評価の量、知的財産権の有無など）に異なる重み付けを割り当てて実施
  - 異なるセキュリティ要件、異なる機能性、異なる複雑性を持った攻撃などを踏まえた評価の実施
  - 限られたリソースにおける安全性評価および性能評価の実施

最終候補となったアルゴリズムの中から NIST が Ascon を選定したポイントについて整理を行うと以下の項目が挙げられる。

- 安全性
  - 高いセキュリティーマージン
  - 多数の第三者による安全性評価の数
- 設計/実装
  - 設計の微調整を行わないという設計の成熟度
  - 軽量暗号コンペティションである CAESAR プロジェクトにおいて軽量暗号の最終的なポートフォリオに選択されている実績
  - 漏えいに対するモードレベルでの保護メカニズムを有すること
  - 実装と設計の柔軟性
  - サイドチャネル攻撃に対する対策を行うための追加コストが低いこと
- 機能性
  - ハッシュに加えて XOF や MAC などの追加機能を有すること
- 性能
  - ソフトウェアおよびハードウェア環境において、現行の NIST 標準である AES-GCM や SHA-2 を上回る性能を有すること

また、NIST 以外の標準化団体における検討については、2023 年 9 月現在では大きな動きは見られなかったが、2023 年後半に予定されている NIST が発行する標準仕様の公開を受けて、本格的に様々な団体での検討が行われるものと考える。また、標準化された暗号技術が利用できる環境としてソフトウェアやハードウェア実装が公開されることが重要であるが、CAESAR プロジェクト等の実績などから実装がいくつか公開されているケースが見受けられた。これは Ascon の設計が成熟しており、NIST 軽量暗号コンペティションにおいて設計の微修正が行われていないことが背景にあると考える。

付録４

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である。

表 1 具体的な暗号の攻撃に関する発表

2. FSE 2023 の発表

Vectorial Decoding Algorithm for Fast Correlation Attack and Its Applications to Stream Cipher Grain-128a

Zhaocun Zhou, Dengguo Feng, Bin Zhang

LFSR (Linear Feedback Shift Register) ベースのストリーム暗号に対する解析論文である。Meier と Staffelbach によって提唱された高速相関攻撃は、LFSR ベースのストリーム暗号に対する重要な解析手法である。この攻撃は、LFSR の内部状態とキーストリームの相関関係を利用し、デコードアルゴリズムを通じて LFSR の初期内部状態の復元することを目的としている。

本研究では、高速相関攻撃を実行するための従来手法であるバイナリアプローチを一般化したベクトル形式の反復デコードアルゴリズム (Vectorial Decoding Algorithm) を提案する。バイナリアプローチではバイナリ形式の線形近似しか攻撃に利用できなかったものの、一般化したベクトル形式のアプローチでは多次元線形近似 (Multidimensional linear approximations) を攻撃に応用することが可能になるとともに、パリティチェックの質の観点でも優位性がある。また、反復デコードアルゴリズムを改良するための 2 つの新しい基準を提案し、高速相関攻撃の新しい暗号学的特性を示すことで、その効率性と計算量の見積もりを容易にすることが可能となった。

提案手法を LFSR ベースのストリーム暗号である Grain-128a に適用し、仮説に基づき、その安全性バウンドに関する興味深い結果を導き出した。結果として、行列環上の LFSR、そして Grain-128a のようなバイアスのある多次元線形近似を持つ非線形関数に対する潜在的な脆弱性の存在を明らかにした。

New Cryptanalysis of ZUC-256 Initialization Using Modular Differences

Fukang Liu, Willi Meier, Santanu Sarkar, Gaoli Wang, Ryoma Ito, Takanori Isobe

ストリーム暗号 ZUC-256 に対する解析論文である。ZUC-256 は 5G アプリケーション用に設計されたストリーム暗号であり、AES-256、SNOW-V とともに、Security Algorithms Group of Experts (SAGE) による 5G 移動通信における標準化アルゴリズムの評価対象となっている。ZUC-256 のラウンド関数における注目すべき特徴は、多くの演算が異なる体上で定義されているため、解析が非常に困難となることである。

本研究では、モジュラー差分(modular difference)、符号付き差分(signed difference)、XOR 差分 (XOR difference) に着目し、異なる体上で定義された演算間の相互作用を注意深く制御するための新しい技術を開発する。一見すると、この技術は MD-SHA ハッシュ関数を解析するために Wang らが開発した従来手法と非常によく似ているが、ZUC-256 は MD-SHA ハッシュ関数と比べてラウンド関数がはるかに複雑であるため、提案した新しい技術は ZUC-256 の解析に大きく貢献するものとなる。

結果として、複雑な入力差分を使用することにより、33 ラウンド中 31 ラウンドの ZUC-256、そして 33 ラウンド中 30 ラウンドの ZUC-256-v2 に対し、識別攻撃が有効となることが示された。また、関連鍵設定において、15 ラウンド ZUC-256、そして 14 ラウンド ZUC-256-v2 に対して、16 ビットの部分鍵を効率的に復元する方法も示された。

Cryptanalysis of Reduced Round ChaCha – New Attack & Deeper Analysis

Sabyasachi Dey, Hirendra kumar Garai, Subhamoy Maitra

ストリーム暗号 ChaCha に対する解析論文である。最初に、分割統治法を使用して秘密鍵ビットを効率的に分割する方法を検討する。この分割方法は複数の入出力差分を使用することで実現でき、結果として、6 ラウンド ChaCha を計算量$2^{99.48}$で攻撃可能であることが示された。これは既存攻撃よりも2^{40}倍高速である。次に、計算量評価の見積もり方法を分析する。ChaCha に対する既存の計算量評価は一般的に理論的な見積もりが与えられているが、Eurocrypt 2022 で Dey らはこの理論的な見積もり方法にいくつかの問題点があることを指摘した。そこで、32 ビットの秘密鍵を有する ChaCha のトイモデルを対象とし、計算量見積もりの正しさを検証した。この検証結果に基づき、6 ラウンド ChaCha に対する計算量を見積もった。最後に、成功確率の見積もり方法を考察する。PNB ベースの既存攻撃では成功確率が約 50%と見積もられていた。本研究では成功確率の正確な範囲、つまり成功確率の上界と下界の理論値を示すとともに、トイモデルでこの理論値の正しさを検証した。この理論値を使用して既存攻撃（FSE 2008 で報告された Aumasson らの攻撃と 2006 年に Discret. Appl. Math.で報告された Maitra の攻撃）の成功確率を再見積もりし、Aumasson らの攻撃の成功確率の範囲が 79.9%～84.2%、Maitra の攻撃の成功確率の範囲が 99.7%～99.8%であることを示した。

SAT-aided Automatic Search of Boomerang Distinguishers for ARX Ciphers

Dachao Wang, Baocang Wang, Siwei Sun

ARX（Addition-Rotation-XOR）暗号に対する解析論文である。ARX 暗号における算術加算のドメインサイズは、一般的に 16 ビットや 32 ビットのように大きいため、算術加算用のブーメラン接続表（BCT: Boomerang Connectivity Table）を効率的に構築することは困難な課題として残されていた。

本研究ではこのような課題に対処するため、BCT を構築するための動的プログラミングアルゴリズムを紹介する。このアルゴリズムでは、算術加算における桁上がりと桁下がりに関する単純かつ興味深い特性に着目している。このアルゴリズムを使用することで、BCT 構築の実行時間を$8^{2(n-1)}$から$4^{2(n-1)}$回に短縮できるようになった。ここで、nは算術加算のドメインサイズである。

このアルゴリズムを使用して、ARX 暗号全体の最適なブーメラン特性を探索するための 2 つの自動化フレームワークを提案する。これらのフレームワークでは、SAT(Boolean

Satisfiability Problem）モデルによって構築され、ARX ベースのブロック暗号 Speck に適用された。結果として、10 ラウンド Speck32/64 と 12 ラウンド Speck48/72 に対し、それぞれ確率$2^{-29.15}$と$2^{-44.15}$のブーメラン特性が存在することを示した。

Automatic Search of Rectangle Attacks on Feistel Ciphers: Application to WARP

Virginie Lallemand, Marine Minier, Loïc Rouquette

ブロック暗号 WARP に対するブーメラン攻撃を用いた解析論文である。ブーメラン攻撃は 1 つの長い差分を使用する代わりに 2 つの短い差分を組み合わせて解析する手法である。当初、これらの 2 つの差分は自由に選択できると考えられていたが、Murphy によって相互依存性が指摘され、単純な組み合わせで攻撃することができないことが明らかとなった。近年、このような問題を解決するための自動化ツールが提案されている。

本研究では、最初に FSE 2022 で Delaune らが提案した自動化ツールを WARP のような Feistel 暗号に適用することを検討する。元のツールは SKINNY のような SPN 暗号を対象としたものであるからである。結果として、元のツールを単純に WARP に適用するだけでは、20 ラウンドを超える識別子の発見には至らなかった。そこで、同じ入出力差分を有する様々な解を数え上げる手法を適用し、これまでの最良の結果を 2 ラウンド更新する 23 ラウンド WARP へのブーメラン識別子を発見した。さらに、鍵回復フェーズを追加することで、26 ラウンド WARP に対する鍵回復攻撃が時間計算量$2^{115.9}$、データ量$2^{120.6}$で実行できることを示した。

Throwing Boomerangs into Feistel Structures: Application to CLEFIA, WARP, LBlock, LBlock-s and TWINE

Hosein Hadipour, Marcel Nageler, Maria Eichlseder

Feistel 型ブロック暗号に対するブーメラン攻撃を用いた解析論文である。ブーメラン識別子を探索するための自動化ツールに関する既存研究の大部分は、SPN 型ブロック暗号を対象としたものであった。また、FSE 2020 で Boukerrou らが Feistel 型ブロック暗号へのブーメラン接続表の構築を定式化する理論的フレームワークを提供したが、自動化ツールについては提供されていない。

本研究では、FSE 2022 で Hadipour らが提案したブーメラン識別子を探索する手法を拡張するとともに、Feistel 型ブロック暗号に対するブーメラン識別子を探索するための自動化ツールを提供する。この自動化ツールを使用し、一般化 Feistel 構造ベースのブロック暗号（WARP、CLEFIA、TWINE、LBlock、LBlock-s）に対するブーメラン識別子の探索を行った。結果として、20 ラウンドと 21 ラウンドの WARP に対する既存のブーメラン識別子を改善するとともに、2 ラウンド拡張した 23 ラウンド WARP のブーメラン識別子を発見した。また、CLEFIA に対するブーメラン識別子も 1 ラウンド拡張することができ、この識別子を使用して 11 ラウンド CLEFIA に対する鍵回復攻撃が時間計算量

$2^{116.1}$、データ量$2^{103.13}$、メモリ量$2^{113.6}$で実行できることを示した。その他、TWINE、LBlock、LBlock-s に対する既存のブーメラン識別子も改善した。

Finding Collisions against 4-round SHA-3-384 in Practical Time

Senyang Huang, Orna Agmon Ben-Yehuda, Orr Dunkelman, Alexander Maximov

ハッシュ関数 SHA3-384 に対する解析論文である。SHA3 に対する最も強力な衝突攻撃は、2020 年に Journal of Cryptology で Guo らが報告した線形化手法に基づくものである。しかしながら、この手法は SHA3-224 や SHA3-256 のような入力サイズ（レートサイズ）が大きいバリアントに対して有効であるものの、SHA3-384 や SHA3-512 のような入力サイズの小さいバリアントに対して適用できないという問題があった。
本研究では、以下に示す新しい 3 つのアイデアを提案することで、既存研究における課題を克服する。1 つ目は、提案攻撃では 1 ブロック分のメッセージではなく 2 ブロック分のメッセージを使用することである。これにより、衝突を発見するための制約が緩和され、柔軟性のある解析が可能となる。2 つ目は、既存の線形化手法を適用する代わりに SAT（Boolean satisfiability problem）手法を使用することである。具体的には、要求される差分条件を満たすようなメッセージの値を SAT 手法で探索する。これにより、メッセージの値からより広い範囲の入力差分へと接続することが可能となり、差分特性を選択する際の柔軟性の向上に繋がる。3 つ目は、Keccak の非線形層における非ランダム性を検知するための 2 つの新しいツールと deduce-and-sieve アルゴリズムを開発したことである。このアルゴリズムを使用することで、SAT ソルバーを直接呼び出す場合と比べ、UNSAT となるケースのほとんどを効率的に検出することが可能となる。結果として、4 ラウンド SHA3-384 に対する衝突攻撃が時間計算量$2^{59.64}$、メモリ量$2^{45.94}$で実行できることを示した。

Finding Collisions for Round-Reduced Romulus-H

Marcel Nageler, Felix Pallua, Maria Eichlseder

ハッシュ関数 Romulus-H に対する解析論文である。Romulus-H は Hirose が提案したダブルブロック長（Hirose-DBL: double block length）構造を採用しており、内部のブロック暗号として SKINNY を採用している。Hirose-DBL 構造のハッシュ関数は暗号プリミティブが理想的である場合に安全性が証明されているものの、SKINNY を暗号プリミティブとして採用した場合に安全性が保証されるかは明らかとされていない。また、Romulus-H に対する既存研究では原像攻撃とフリースタート（free-start）衝突攻撃にのみ焦点が当てられていた。

本研究では、Hirose-DBL 構造のハッシュ関数に対する衝突攻撃耐性を評価するための新しいフレームワークを提案する。このフレームワークを構築するために、統合差分特性（joint differential characteristics）を考慮する。Hirose-DBL 構造は 2 回の

ブロック暗号呼び出しがあるが、統合差分特性を考慮することで、これら 2 回の呼び出しにおける差分特性の関係性を詳細に分析できるようになる。統合差分特性を特定するために、MILP モデルと CP モデルに基づく二段階の探索プロセスを構築する。さらに、特定した統合差分特性に基づく衝突を探索するための効率的な CP モデルも構築する。これらのモデルを使用して Romulus-H を解析した結果、10 ラウンドの現実的な衝突を発見するとともに、14 ラウンドの現実的なセミフリースタート（semi-free-start）衝突を発見した。なお、仕様段数は 40 ラウンドである。

Towards Tight Differential Bounds of Ascon

Rusydi H. Makarim Raghvendra Rohi

認証暗号 Ascon に対する解析論文である。Ascon は CAESAR コンペティションから数多くの安全性評価に耐えてきた経緯があるにも関わらず、差分確率の厳密な境界が近年まで明らかにされていない状況であった。FSE 2022 で Erlacher らは 4 ラウンドと 6 ラウンドの Ascon に対して、差分と線形のアクティブ S-box 数に関する（厳密ではない）下界証明を行なった。しかしながら、依然として 4〜6 ラウンドにおけるアクティブ S-box の最小数に関しては明らかにされていない。

本研究では、SMT（Satisfiability Modulo Theory）と MILP（Mixed Integer Linear Programming）をベースとした自動化ツールを効率的に組み合わせ、上記のような下界証明に関する問題の解決を目指す。最初に、SMT 手法を使用して、3 ラウンドの差分トレイルに関するパターンを詳細に分析する。次に、MILP 手法を使用して、これら 3 ラウンドの差分トレイルに関するパターンを拡張することで、4 ラウンドと 5 ラウンドのアクティブ S-box 数の上界をそれぞれ 44 個から 43 個と 78 個から 72 個に改善する。最後に、同様のアプローチを線形解析に応用することで、4 ラウンドと 5 ラウンドの線形トレイルに関する結果も改善した。

Improved Differential and Linear Trail Bounds for ASCON

Solane El Hirch Silvia Mella Alireza Mehrdad Joan Daemen

認証暗号 Ascon に対する解析論文である。上記の解析論文と同様、Ascon に対する差分確率と線形確率の厳密な境界を証明することが重要となっている。この目的のために SAT や MILP などの汎用ソルバーを使用した解析手法や専用ツールを使用した解析手法が数多く提案されているものの、汎用ソルバーは専用ツールと比較して機能面で劣るため、汎用ソルバーを使用して得られた結果に限界があると考えられる。

本研究では、Ascon に対する差分トレイルと線形トレイルを探索するための専用ツールを提案する。この専用ツールは、FSE 2017 で Mella らが提案した Keccak に対する専用ツールを応用したものであり、ツリーベースのアプローチに基づいている。Ascon に対する専用ツールとするために、Ascon の線形層と非線形層の構造的特徴を注意深く抽

出し、専用ツールとして反映させている。結果として、専用ツールを使用することで、3 ラウンドの線形トレイルに関する境界がタイトであることを証明するとともに、他のラウンドにおける差分トレイルと線形トレイルに関する上界も改善した。特に、差分トレイルと線形トレイルの両方に関し、6 ラウンドの上界が2^{-128}以下、12 ラウンドの上界が2^{-256}であることを初めて証明した。

Integral Cryptanalysis of WARP based on Monomial Prediction

Hosein Hadipour, Maria Eichlseder

ブロック暗号 WARP に対する積分（integral）攻撃を用いた解析論文である。WARP に対する既存の積分攻撃を用いた解析は開発者によってのみ実行されており、識別攻撃は最大で 20 ラウンド、鍵回復攻撃はさらに 1 ラウンドのみ追加可能であると示されている。また、開発者による解析はニブル単位のモデルに基づくものである。

本研究では、積分攻撃を用いた解析をビット単位のモデルに基づいて実行するために、Asiacrypt 2020 で Hu らが示した単項予測（monomial prediction）技術を使用する。具体的には、単行予測表（monomial prediction table）という概念を提案するとともに、この概念を最適化問題（MILP、SAT、CP）に帰着させた上で、積分攻撃をビット単位で解析するための自動化ツールを提供した。結果として、積分識別子が最大 24 ラウンドまで構築できることを示すとともに、32 ラウンド WARP に対する鍵回復攻撃が時間計算量2^{127}、時間計算量2^{127}、時間計算量2^{108}で実行できることを示した。これは既存の識別攻撃を 3 ラウンド、既存の鍵回復攻撃を 8 ラウンド更新する結果となっている。

Practical Cube Attack against Nonce-Misused Ascon

Jules Baudrin, Anne Canteaut, Léo Perrin

認証暗号 Ascon に対する解析論文である。Ascon ではラウンド関数の次数が低いことため、キューブ（cube）攻撃や高階差分（higher-order differential）攻撃に関連する攻撃手法が有効に機能する可能性を秘めている。実際に、Ascon に対するキューブ攻撃を用いた解析論文は数多く報告されている。

本研究においてもキューブ攻撃を用いた既存の解析論文に続き、上記の直感が正しいという新しい証拠を提供する。Ascon の内部状態における代数正規系(algebraic normal form）の最高次数に焦点を当てることで、6 ラウンド Ascon（暗号化フェーズにおける最大ラウンド）に対する内部状態復元攻撃を時間計算量2^{40}以下という現実的な計算量で実行できることを示す。ただし、これはナンス誤用（nonce-misuse）設定で有効な攻撃であるため、開発者の主張する安全性要件を侵害するものではないことに注意が必要である。また、提案攻撃で鍵回復攻撃や偽造攻撃が成立するものではない。

New Low-Memory Algebraic Attacks on LowMC in the Picnic Setting

Fukang Liu, Willi Meier, Santanu Sarkar, Takanori Isobe

耐量子署名方式 Picnic で使用されるブロック暗号 LowMC の解析論文である。Picnic の安全性は、1 つの平文・暗号文ペアから LowMC の秘密鍵が復元困難であることに帰着されている。Asiacrypt 2021 で Dinur は Picnic3 で使用される LowMC（各ラウンドにて全ての S-box 層が導入されているバージョン）に対する最良の鍵回復攻撃を報告した。また、Asiacrypt 2021 で Banik らは Picnic2 で使用される LowMC（各ラウンドにて 10 個の S-box 層が導入されているバージョン）に対する中間一致手法に基づく鍵回復攻撃を報告した。特に、前者の攻撃ではメモリ消費量が莫大であるという課題がある。

本研究では、これらの既存研究に対し、特にメモリ消費量の観点で改善する。これは Bouillaguet らによって提案されたクロスブレッド（crossbred）アルゴリズムのシンプルバージョンを使用することで達成できる。結果として、時間計算量とデータ量のトレードオフの観点で、Dinur の鍵回復攻撃よりも優れた結果を示した。同様に、Banik らの中間一致手法に基づく鍵回復攻撃も改善できることを示した。提案手法における最大の特徴はそのシンプルさであり、基本的な線形代数の知識で容易に実装できる。

New Key Recovery Attack on Reduced-Round AES

Navid Ghaedi Bardeh, Vincent Rijmen

ブロック暗号 AES に対する解析論文である。Asiacrypt 2017 で Ronjom らはゼロ差分特性（zero-difference property）と呼ばれる 4 ラウンド AES の新しい性質を報告した。本研究では、このゼロ差分特性に対して新しい洞察を提供することで、ゼロ差分特性の一般化を目指しており、この目的を達成することで、ゼロ差分特性のより単純な定式化と解釈を提供することが可能となる。

ゼロ差分特性の一般化のために、本研究では Daeman と Rijmen によって報告された関連差分（related differences と related differentials）の概念を使用し、SPN 型共通鍵暗号のためのゼロ差分特性を再定義する。最も注目すべき点は、SPN 型共通鍵暗号におけるゼロ差分特性に関連差分が埋め込まれていることである。最大 4 ラウンドの関連差分をゼロ差分特性に埋め込むことで、ゼロ差分特性を最大 8 ラウンドまで拡張できるようになる。本研究では、4 ラウンドの関連差分をゼロ差分特性に埋め込むことで得られる 7 ラウンド AES の新しい関連差分特性を提供する。この新しい関連差分特性を利用することで、7 ラウンド AES に対する鍵回復攻撃を計算量（データ、時間、メモリ）$2^{110.2}$以下で実行可能となる。

Cryptanalysis of Rocca and Feasibility of Its Security Claim

Yosuke Todo, Akinori Hosoyamada, Akiko Inoue, Ryoma Ito, Tetsu Iwata, Kazuhiko Minematsu, Ferdinand Sibleyras

認証暗号 Rocca に対する解析論文である。Rocca は FSE 2022 で提案されており、Rocca

開発者は鍵回復攻撃と識別攻撃に対して256ビット安全性、偽造攻撃に対して128ビット安全性が保証すると主張していた。この安全性主張の注目すべき点は、認証暗号の一般的な安全性要件である秘匿性（privacy）と改ざん検知（authenticity）に関してギャップがあるということである。つまり、鍵回復攻撃における安全性主張により、復号オラクルを通じて攻撃者に複数の偽造結果を取得させることを許容していることを意味する。

本研究では、最初にフルスペックのRoccaに対する鍵回復攻撃を示す。この攻撃では暗号化オラクルと復号オラクルを使用し、時間計算量2^{128}、データ量2^{128}、成功確率 1で実行可能である。つまり、この攻撃ではRoccaの鍵回復攻撃に関する256ビット安全性を破るものである。次に、Roccaに対する鍵回復攻撃を様々な安全性モデルの下での攻撃に拡張し、Roccaの安全性主張が保証されるような対策案を検討する。最後に、証明可能安全性の観点から、Roccaの安全性主張（つまり、秘匿性と改ざん検知に関してギャップがあるという主張）を達成することが可能かについての理論的な問題について考察する。考察結果として、否定的な結果と肯定的な結果の両方を提示する。具体的には、オンライン認証暗号と呼ばれるクラスに属する認証暗号については否定的な結果が生じ、Encode-then-Encipher アプローチを採用する認証暗号については肯定的な結果が得られた。

Practical Attacks on the Full-round FRIET

Senpeng Wang, Dengguo Feng, Bin Hu, Jie Guan, Tairong Shi

認証暗号FRIETに対する解析論文である。FRIETはEurocrypt 2020で提案され、故障利用攻撃に耐性のある方式であることが特徴である。認証暗号モードはFRIET-AEと呼ばれ、その内部置換としてFRIET-PCとFRIET-Pが提案されている。

本研究では、FRIET-PC のラウンド関数における差分伝搬と線形マスク伝搬に着目する。FRIET-PCはAND-Rotation-XOR構造を採用しており、唯一の非線形演算はビット単位のAND演算のみである。AND演算の差分確率と線形相関を固定することで、任意のラウンドにおけるFRIET-PCに対して確率が1となる差分識別子と相関の絶対値が1となる線形識別子を構築できることを発見した。FRIET-PCを組み込んだFRIET-AEに対してこの性質を悪用することにより、攻撃者は有効かつ任意のタグ・暗号文ペアを容易に作成することが可能となる。これは開発者が主張する機密性と完全性の要件を破ることとなる。

Revisiting the Extension of Matsui's Algorithm 1 to Linear Hulls: Application to TinyJAMBU

Muzhou Li, Nicky Mouha, Ling Sun, Meiqin Wang

認証暗号TinyJAMBUに対する解析論文である。Eurocrypt 1993でMatsuiが線形攻撃

を初めて提案し、その解析論文にて 2 つのアルゴリズム（アルゴリズム 1 とアルゴリズム 2）を紹介した。本研究ではアルゴリズム 1 に着目する。アルゴリズム 1 を実行する上での問題点は、線形ハル（linear hull）効果が強い場合、つまり同じ内部状態ビットを含む強力な線形トレイルが複数ある場合、アルゴリズム 1 で鍵ビットを復元することが不可能であることである。この問題を解決するために、Rock らはアルゴリズム 1 で使用するための線形ハル効果を拡張したものの、彼らの評価モデルでは依然としてデータ量とエラー確率の関係性を正確に評価できないという問題点があった。

本研究では、Rock らの評価モデルを改善し、より正確な評価を行うための統計モデルを提案する。具体的には、最尤推定ベースの評価モデルと閾値ベースのモデルを採用している。これらの評価モデルを使用した解析手法を TinyJAMBU に適用し、鍵ビットの推定にかかるエラー確率の評価を行った。結果として、閾値ベースと最尤推定ベースの評価モデルにおけるエラー確率がそれぞれ 2.19%と 1.90%であるのに対し、Rock らの評価モデルにおけるエラー確率が 93.75%であり、既存手法よりも非常に高い精度を達成したと言える。なお、最尤推定ベースの評価モデルではエラー確率が最も低いものの、計算効率は閾値ベースの評価モデルの方が高い。

3. Eurocrypt 2023 の発表

Truncated Boomerang Attacks and Application to AES-based Ciphers

Augustin Bariant, Gaëtan Leurent

AES ベースのブロック暗号（AES、Kiasu-BC、Deoxys-BC、TNT-AES）に対する解析論文である。AES ベースのブロック暗号に対する効果的な解析手法の 1 つにブーメラン攻撃がある。この攻撃は 1 つの長い差分を使用する代わりに 2 つの短い差分を組み合わせて解析する手法である。実際に、Kiasu-BC や Deoxyx-BC に対する最良の攻撃はブーメラン攻撃によって達成されている。

本研究では切り詰め差分（truncated differential）を用いたブーメラン攻撃に関する一般的なフレームワークを提供する。また、このフレームワークを使用することで、AES ベースのブロック暗号に対する既存のブーメラン攻撃を大幅に改善できることを示す。一般的なブーメラン攻撃では、最初に効果的なブーメラン識別子を探索したのち、鍵回復フェーズについて検討する。一方、提案するフレームワークでは、鍵回復フェーズも考慮してブーメラン識別子を探索する。このために、平文側と暗号文側の 1 ラウンド分の差分伝搬を注意深く解析する必要がある。結果として、6 ラウンド AES に対する識別攻撃と鍵回復攻撃がそれぞれ時間計算量2^{87}と2^{61}で実行可能であることを示した。その他、提案するフレームワークを Kiasu-BC、Deoxyx-BC、TNT-AES に適用することで、それぞれ既存攻撃を改善できることを示した。

Better Steady than Speedy: Full Break of SPEEDY-7-192

Christina Boura, Nicolas David, Rachelle Heim Boissier, Maria Naya-Plasencia

ブロック暗号 Speedy に対する解析論文である。共通鍵暗号解析における最も強力な手法に差分攻撃があるが、1990 年に Biham と Shamir が初めて提案した以降、基本的な解析手法に関する改良だけでなく、いくつかの専用的な解析手法も提案されてきた。これらの既存研究の大部分は、鍵回復攻撃フェーズの改善に関するものであるが、新しい共通鍵暗号プリミティブを設計する際に実施される差分攻撃を使用した安全性評価では、最適な識別子の探索に限定されていることが多く、この識別子からヒューリスティックな手法を用いて鍵回復攻撃の実行可能ラウンド数を見積もることが多い。

本研究では、差分攻撃を使用した鍵回復フェーズにおける多くのステップを最適化する方法を示し、ブロック暗号 Speedy に適用してその効果を論証する。最初に、いくつかの制約条件下で成立する最適な差分トレイルと、この差分トレイルに関連する多重差分（multiple differentials）を探索するための手法を提示する。それから、鍵推測パートにおける計算量を最適化する手法を示し、これらの手法を Speedy に適用する。結果として、Speedy ファミリーの 1 つである Speedy-7-192（時間計算量とデータ量に関して 192 ビット安全性を有する 7 ラウンド Speedy）に対し、時間計算量$2^{187.84}$、データ量$2^{87.28}$、メモリ量2^{42}で鍵回復攻撃を実行できることを示した。これは Speedy-7-192 の安全性要件を破る攻撃である。他のバリアントである Speedy-5-192 と Speedy-6-192 に対しても同様に攻撃が可能であり、これらのバリアントに対してはわずかに安全性要件を破るには至らなかったものの、既存の最良の攻撃を達成している。

Exploiting Non-Full Key Additions: Full-Fledged Automatic Demirci-Selçuk Meet-in-the-Middle Cryptanalysis of SKINNY

Danping Shi, Siwei Sun, Ling Song, Lei Hu, Qianqian Yang

ブロック暗号 SKINNY に対する解析論文である。Demirci-Selçuk 中間一致 (DS-MITM) 攻撃は差分攻撃の高度なバリアントとして知られているが、その高度さゆえに AES を除くほとんどの共通鍵暗号プリミティブに対して最適な DS-MITM 攻撃を実行することが困難となっている。また、既存の自動化ツールは DS-MITM 攻撃の最も基本的な特徴しか捉えることができず、この攻撃を強化するために開発な重要な技術、例えば差分列挙（differential enumeration)、鍵依存篩法（key-dependent sieve)、鍵ブリッジ（key bridging）などの重要な技術については、依然として手作業に頼らざるを得ない。

本研究では、DS-MITM 攻撃を強化するための既知の重要な技術を統合した本格的な自動化フレームワークを開発する。この自動化フレームワークでは、識別子の探索に留まらず、鍵回復攻撃を直接的に評価することが可能となる。さらに、攻撃に有効となる線形関係を生成するために、部分鍵の加算を効率的に利用できる新しい技術を提供する。

このような自動化フレームワークを SKINNY ファミリーに適用し、多くのバリアントにて既存結果を大幅に改善したことを示した。

Finding the Impossible: Automated Search for Full Impossible-Differential, Zero-Correlation, and Integral Attacks

Hosein Hadipour, Sadegh Sadeghi, Maria Eichlseder

ブロック暗号に対する自動化評価ツールの提案論文である。ブロック暗号に対する汎用的な攻撃手法として、不能差分（ID: Impossible Differential）攻撃、零相関線形（ZC: Zero-Correlation Linear）攻撃、積分（Integral）攻撃があり、これらの攻撃に対するブロック暗号の安全性を評価することは非常に重要であるものの、これらの評価を厳密かつ網羅的に実行することは困難な作業でもある。これは、ヒューリスティックな方法で解決することが困難であること、既存の自動化ツールでは多くの変数と制約事項が必要であるため現実的な時間内で解を得ることが困難であること、などの要因が考えられる。また、既存の自動化ツールでは識別子の探索に限定されており、鍵回復フェーズも含めた統合的な自動化ツールへの拡張は依然として困難な課題である。

本研究では、制約プログラミング（CP: Constraint Programming）に基づく新しい自動化ツールを提案する。このツールでは、ID 識別子、ZC 識別子、積分識別子の探索に留まらず、これらの識別子から鍵回復フェーズに拡張するための統合的な解析が可能となる。このツールを使用してブロック暗号 SKINNY ファミリー、CRAFT、Deoxys-BC を評価し、この有効性を検証した。結果として、SKINNY ファミリーの全てのバリアントに関し、既存の ID 攻撃、ZC 攻撃、積分攻撃を全て大幅に更新できることを示した。CRAFT と Deoxys-BC に対しても同様である。提案ツールは汎用的であり、他のブロック暗号に対しても同様に適用可能である。

Caveat Implementor! Key Recovery Attacks on MEGA

Martin R. Albrecht, Miro Haller, Lenka Mareková, Kenneth G. Paterson

MEGA は大規模なクラウドストレージおよび通信プラットフォームであり、保存データのエンドツーエンドの暗号化を提供することを目的としている。Backendal らによる最近の解析論文（IEEE S&P 2023）では、MEGA のサービスプロバイダが実行可能な実用的な攻撃を提示され、MEGA 開発者が示していた安全性主張が無効化されるという結果となった。これに対し、MEGA 開発者は MEGA ユーザの RSA 秘密鍵に対して、既存攻撃を防ぐための軽量な健全性チェック機能を追加した。

本研究では、この新しい健全性チェック機能を分析し、ターゲットユーザの RSA 秘密鍵を復元するために、健全性チェック機能をいかにして悪用するかを示すとともに、結果として既存攻撃よりもわずかに高い計算量で RSA 秘密鍵を復元できることを示す。具体的には、MEGA システムにおけるターゲットユーザーのマスター鍵に関し、ECB 暗号化

オラクルの存在を特定する。このオラクルは、攻撃者に対して、ターゲットユーザの RSA 秘密鍵を選択したデータで部分的に上書きする機能を提供する。さらに、2 つの異なる攻撃手法を提供する。これらの攻撃では、ユーザ認証中における健全性チェックとその後の暗号化処理で発生する異なるエラー条件を悪用する。結果として、Backendal らの RSA 鍵回復攻撃を実行するためには 512 回のログイン試行数が必要であったものの、提案手法では 2 回のログイン試行数で十分であることが示された。

Meet-in-the-Middle Preimage Attacks on Sponge-based Hashing

Lingyue Qin, Jialiang Hua, Xiaoyang Dong, Hailun Yan, Xiaoyun Wang

スポンジベースのハッシュ関数（SHA3-512、Xoodyak-XOF、Ascon-XOF）に対する解析論文である。Markle-Damgard 構成のハッシュ関数に対して、中間一致技術を用いた原像攻撃に関する研究成果が数多く報告されている。一方、スポンジベースのハッシュ関数（特に、Keccak/SHA3）に対して、線形化技術を用いた原像攻撃が主流となっており、中間一致技術を用いた原像攻撃に関するフレームワークが確立されていない。

本研究では、スポンジベースのハッシュ関数に対して適用可能な中間一致技術に基づく原像攻撃の汎用フレームワークを提供する。この新しいフレームワークはビットレベルの MILP ベース自動探索手法に基づいている。従来研究におけるバイトレベルのモデリング手法とは異なり、ビットレベルのモデリング手法ではモデルが大規模となり、現実的な時間内に解を得ることが困難になる。そこで、対象となるハッシュ関数の構造を詳細に分析し、それぞれの構造に適したモデリング手法を適用することで、MILP モデルの削減を目指した。

提案手法を SHA3-512、Xoodyak-XOF、Ascon-XOF に適用した。4 ラウンド SHA3-512 に対する原像攻撃が時間計算量$2^{504.58}$とメモリ量2^{108}で実行できることを示した。3 ラウンド Xoodyak-XOF に対する原像攻撃が時間計算量$2^{125.06}$とメモリ量2^{97}で実行できることを示した。また、4 ラウンド Ascon-XOF に対する像攻撃が時間計算量$2^{124.67}$とメモリ量2^{54}で実行できることを示した。

Analysis of RIPEMD-160: New Collision Attacks and Finding Characteristics with MILP

Fukang Liu, Gaoli Wang, Santanu Sarkar, Ravi Anand, Willi Meier, Yingxin Li, Takanori Isobe

ハッシュ関数 RIPEMD-160 に対する解析論文である。MD-SHA ハッシュ関数族（MD4、MD5、SHA0、SHA1）の多くが解読されているにも関わらず、RIPEMD-160 は今もなお高い安全性を確保しており、ISO/IEC 標準として採用されている。実際に、仕様段数が 80 ラウンドである RIPEMD-160 への最良の攻撃は、35 ラウンドの原像攻撃と 34 ラウンドの衝突攻撃である。

本研究では 4 つの主要な貢献がある。1 つ目は、メッセージ差分を選択する新しい戦略を提案したことである。2 つ目は、差分特性の性質を注意深く抽出することで、RIPEMD-160 における両方のブランチで同時にかつ効率的にメッセージ修正（message modification）を実行するための方法論を提案したことである。3 つ目は、RIPEMD-160 の差分特性を効率的に探索するために、符号付き差分（singed differential）特性探索のための MILP（Mixed Integer Linear Programming）手法を初めて提案したことである。4 つ目は、符号付き差分特性の探索における矛盾した結果を自動的に検出するための新しい方法を提案したことである。これらの提案手法に基づき、36 ラウンド RIPEMD-160 に対する衝突攻撃が時間計算量$2^{64.5}$で実行可能であることを明らかにした。

Collision Attacks on Round-Reduced SHA-3 Using Conditional Internal Differentials

Zhongyi Zhang, Chengan Hou, Meicheng Liu

ハッシュ関数族の SHA3（SHA3-224/256/384/512、SHAKE128/256）に対する解析論文である。SHA3 の中でも SHA3-512 は衝突攻撃に対して最も強い耐性を示しており、4 ラウンド SHA3-512 に対する衝突攻撃が時間計算量2^{263}（誕生日攻撃よりも2^6倍高速）で実行可能であることが知られている。また、SHAKE256 に対する衝突攻撃についてはまだ報告されていない。

本研究は 2010 年に Peyrin が報告した条件付き内部差分攻撃（conditional internal differential attack）と FSE 2013 で Dinur らが報告したターゲット内部差分アルゴリズム（TIDA: target internal difference algorithm）に触発され、SHA3 解析のために一般化された内部差分を改善するとともに、6 つの SHA3 バリアントに対する理論的な解析結果を示す。主要な貢献は 3 つある。1 つ目は、誕生日攻撃のバリアントを提案したことである。2 つ目は、差分遷移条件や差分条件表という新しい概念を抽象化し、既存の条件付き内部差分攻撃を改良したことである。3 つ目は、既存の TIDA を改良したことである。これらの提案手法に基づき、SHA3 に対する新しい衝突攻撃を開発し、結果として最大 5 ラウンドまでの衝突攻撃が実行可能であることを示した。特に、4 ラウンド SHA3-512 と 5 ラウンド SHAKE256 に対する衝突攻撃がそれぞれ時間計算量2^{237}と2^{185}で実行できることを示した。

An Efficient Key Recovery Attack on SIDH

Wouter Castryck, Thomas Decru

本論文で、超特異同種 Diffie-Hellman プロトコル（SIDH）に対する効率的な鍵回復攻撃が発表された。この攻撃は Kani の reducibility criterion に基づいており、アリスとボブがプロトコル中に交換するねじれ点の像に強く依存している。開始曲線の自己準同型環の知識を前提とすれば、システムパラメータに依存する少数の整数の因数分解

を除き、ヒューリスティックな多項式時間でこの攻撃は行われる。また、この攻撃はパーティの一方が 2-同種を使用し、開始曲線が非常に小さな次数のスカラー倍ではない自己準同型を備えている場合、高速かつ簡単に実装可能である。これは NIST 耐量子暗号標準化の第 4 ラウンド候補となった SIDH のインスタンスである SIKE のケースに当てはまる。実際に、著者らはセキュリティレベル 1 を目指す SIKEp434 をシングルコアのプロセッサにより 10 分程度で解読する Magma での攻撃の実装を行った。

A Direct Key Recovery Attack on SIDH

Luciano Maino, Chloe Martindale, Lorenz Panny, Giacomo Pope, Benjamin Wesolowski

本論文は、SIDH への攻撃論文である。任意の開始曲線の場合、提案されている攻撃は劣指数計算量で実行可能である。開始曲線の自己準同型環が既知の場合、著者らの攻撃は、一般化リーマン予想を仮定した上で、多項式時間の複雑さを持つ。本攻撃は、Séta や B-SIDH など、秘密にしている同種の元での点の像を公開する同種ベース暗号システムにも適用できる。一方で、CSIDH、CSI-FiSh、SQISign には適用されないことも明記されている。

Breaking SIDH in Polynomial Time

Damien Robert

本論文は、SIDH (Supersingular isogeny Diffie-Hellman)問題に対して秘密鍵復元を行う Castryck-Decru(CD)攻撃の改良である。CD 攻撃は Eurocrypt 2023 で正式に発表されたが、2022 年の ePrint 版発表時点から SIDH に基づく鍵交換方式 SIKE への影響が知られ、NIST 耐量子計算機暗号プロジェクト等に影響を与えていた。しかし一方で、CD 攻撃は始点曲線E_0が特殊極値曲線に制限されていたことから、パラメータの改良による別の鍵交換方式を提案可能な余地があった。この論文では、CD 攻撃およびフォロワーによる改良を高次元のアーベル多様体の視点から統合して扱うことで、任意の始点曲線に対する SIDH への多項式時間攻撃を提案している。特に、提案した 8 次元攻撃法は任意の SIDH に対して攻撃時間が多項式であることが証明されているが、実用的には一つ下の 4 次元攻撃法が、ヒューリスティックな議論を含むもののより高速な多項式時間での攻撃を可能としている。本論文の発表を受け、Castryck-Decru 論文の ePrint 版は更新され、Robert 論文に対して”He also crushed the hope for secure higher-dimensional variants of SIDH”とのコメントを付けている。

Generic Attack on Duplex-Based AEAD Modes using Random Function Statistics

Henri Gilbert, Rachelle Heim Boissier, Louiza Khati, Yann Rotella

Duplex ベースの認証暗号に対する解析論文である。十分に長い鍵長を有する Duplex

ベースの認証暗号モードは、cをキャパシティとすると、バースデーバウンドである$2^{c/2}$ビット安全であることが証明されている。しかしながら、このバウンドがタイトであることは知られておらず、実際に最も有名な汎用攻撃手法にかかる計算量が$2^c/\alpha$であると言われている。ここで、αは小さな安全性損失因子（security loss factor）である。

本研究では、duplex ベースの認証暗号モードに対する汎用攻撃手法について説明する。提案攻撃は無視できるくらい少ないメモリ量と暗号化クエリを使用せず、時間計算量$O(2^{3c/4})$で実行可能である。また、無視できるくらい少ない追加計算量にて、秘密鍵を復元可能であることも示す。このような汎用攻撃手法を用いて Xuudyak を評価したところ、Xoodyak 開発者が示す安全性主張を破れることを示した。

Context Discovery and Commitment Attacks: How to Break CCM, EAX, SIV, and More

Sanketh Menda, Julia Len, Paul Grubbs, Thomas Ristenpart

様々な認証暗号モードに対する解析論文である。近年、コンテキストコミットメントの観点から安全性を評価する重要性について注目が集まっている。これは、認証暗号方式に対し、攻撃者が選択した 2 つの異なるコンテキスト（つまり、秘密鍵、関連データ、ナンス、平文、その他）から攻撃者が選択した暗号文を正常に復号できるかを評価することである。コンテキストコミットメントに関する多くの未解決問題が残っており、特に CCM、EAX、SIV などの重要な暗号利用モードに関するコミットメント安全性についても、ほとんど明らかにされていない。

本研究では、これらの未解決問題の解決を目指す。最初に、コンテキストのどの部分が攻撃者によって制御されうるのかという観点から、コンテキストコミットメント安全性をより詳細に定義するのに役立つ新しいフレームワークを導入する。次に、コンテキスト検出可能性（context discoverability）と呼ばれる新しい安全性概念を定式化する。これは、ハッシュ関数の安全性要件の 1 つである原像耐性に類似しているとみなせる。さらに、無制限のコンテキストコミットメント安全性（攻撃者が 2 つのコンテキストを全て制御可能な安全性）がコンテキスト検出可能性に関する安全性に帰着されることを示す。また、CCM、EAX、SIV、GCM、OCB3 を含む幅広い認証暗号方式に対する新しいコンテキスト検出攻撃を示す。

最後に、SIV モードに対する制限付きコンテキストコミットメント安全性に関する解析も行われ、一般化誕生日問題に対する Wagner の k-tree アルゴリズムを使用し、計算量$O(2^{n/3})$で実行可能な新しい攻撃手法も提示する。

Disorientation Faults in CSIDH

Gustavo Banegas, Juliane Krämer, Tanja Lange, Michael Meyer, Lorenz Panny, Krijn Reijnders, Jana Sotáková, Monika Trimoska

本論文では、CSIDH の族に対する新しいクラスの故障注入攻撃について研究されてい

る。この攻撃は、いくつかの同種ステップにおいて、その方向を効果的に反転させるものであり、群作用の評価中に行われるLegendre記号またはElligator計算に関連する特定のサブルーチンに障害を与えることで行われている。これらのサブルーチンは、ほぼすべての既知のCSIDH実装に存在するものである。そして、故障を持つサンプルのセットを後処理することで、秘密鍵に対する制約が推測できる。詳細は実装に依存するが、多くの場合、わずかな数の故障注入の成功と、わずかな計算資源で、完全な秘密鍵を回復できることが示されている。また、オリジナルのCSIDHのPoC実証ソフトウェアと、CTIDHの一定時間実装を攻撃するための完全な詳細も提供されている。また、この攻撃に対する一連の簡単な対策も提示され、その安全性についても議論されている。

On the Hardness of the Finite Field Isomorphism Problem

Dipayan Das, Antoine Joux

有限体同型問題（FFI）は、平均計算量を安全性の根拠とする格子問題（LWE、SIS、NTRU）などの代替えとしてPKC'18で導入された。同論文ではその応用として、FFI問題を用いた完全準同型暗号方式も構築している。

本論文では、FFI問題の決定亜種が、標数$q = \Omega(\beta n^2)$において多項式時間で解けることを証明する（ここでq, β, nはFFI問題のパラメータ）。このFFI識別器の結果を用いて、完全準同型暗号のセマンティックな安全性に対する多項式時間攻撃も提案されている。また、いくつかのFFI問題の亜種を、これまで知られていなかったq-ary格子問題として記述する方法を示す。その結果、これまで難解であったいくつかのパラメータに対する探索問題を、簡単な格子簡約アプローチで解くことができるようになった。

A New Algebraic Approach to the Regular Syndrome Decoding Problem and Implications for PCG Constructions

Pierre Briaud, Morten Øygarden

約20年前にAugotらによって導入された正則シンドローム復号化（RSD）問題は、特定の誤差分布を持つシンドローム復号問題の変種である。

この問題では、誤差ベクトルは等しい大きさのブロックに分割され、それぞれが1つのノイズ座標を含んでいる。最近、MPCやZKのアプリケーションで使用されているため、この仮定への関心が高まっている。この文脈では「規則的なノイズを含むLPN」と呼ばれるこの仮定により、通常のLPNと比較してより優れた効率が達成されている。これまでの暗号解読の研究において、この問題の特殊性を利用した攻撃方法は示されていない。

本論文では、RSDに対する最初の代数的攻撃が提示される。基礎となる多項式システムの入念な理論解析に基づき、規則的なノイズ分布を利用することができる具体的な攻撃が提案される。特に、他のアルゴリズムを凌駕するような具体的なパラメータの例が

いくつか挙げられている。

4. PKC 2023 の発表

Post-Quantum Anonymity of Kyber

Varun Maram, Keita Xagawa

Kyber は、NIST の PQC 標準化プロセスで採用された鍵カプセル化メカニズム（KEM）であり、公開鍵暗号化（PKE）と key establishment の文脈で採用された唯一の方式でもある。NIST PQC の文脈における KEM とそれに関連する PKE 方式の主な安全性目標は、IND-CCA セキュリティであった。しかし、いくつかの重要な現代アプリケーションは、その基礎となる KEM/PKE スキームの匿名性を要求している（Bellare et al.） そのようなアプリケーションの例としては、匿名認証システム、暗号通貨、ブロードキャスト暗号化方式、認証された鍵交換、オークションプロトコルがある。よって、このような「IND-CCA を超える」アプリケーションに NIST の新しい PQC 標準が互換性を持つかを分析することは重要である。

Grubbs ら（EUROCRYPT 2022）と草川（EUROCRYPT 2022）は、ほとんどの NIST PQC 第 3 ラウンド候補 KEM の匿名性を研究してきた。しかし技術的な障壁のため、Kyber の匿名性を示すことができていなかった。

本論文ではこの障壁を克服し、Grubbs ら（EUROCRYPT 2022）と草川（EUROCRYPT 2022）が提起した未解決の問題を解決し、Kyber とそこから派生した（ハイブリッド）PKE スキームの匿名性を、ポスト量子設定において確立している。また、具体的評価付きの Kyber の IND-CCA 安全性証明を得るためのアプローチも提供される。これは、Kyber のポスト量子 IND-CCA 安全性の主張に関する前述の研究によって特定された別の問題を、証明可能安全性の観点から解決している。またこの結果は、NIST PQC 第 3 ラウンドのファイナリストである Saber にも同様の方法で適用されている。

A Key-Recovery Attack against Mitaka in the t-Probing Model

Thomas Prest

Mitaka は、Eurocrypt 2022 で提案された格子ベースの署名である。Mitaka の主な特徴は、高次で効率的にマスクできることで、サイドチャネル攻撃が懸念されるシナリオで耐性があるという点である。特に Mitaka は、t-probing モデルにおける安全性の証明が主張されてきた。

本論文では、Mitaka の安全性証明の欠陥を明らかにし、その後、t-probing モデルにおいて安全でないことを示す。4 以上の任意の共有数dについて、1 回の実行で$t < d$個の変数を probing することで、攻撃者は約 2^21 回の実行で効率的に秘密鍵を復元でき

る。さらに、攻撃者がd/tに線形な実行回数でアクセスできる限り、$t = 3$という定数値で十分であることも示される。

The Hidden Number Problem with Small Unknown Multipliers: Cryptanalyzing MEGA in Six Queries and Other Applications

Nadia Heninger, Keegan Ryan

Backendal らはクラウドストレージプロバイダの MEGA に悪用可能ないくつかの脆弱性を特定した。彼らは、悪意のあるサーバーが 512 回のログイン試行後にクライアントの RSA 秘密鍵を回復することができる RSA 鍵回復攻撃を実証した。

本論文では、MEGA プロトコルの脆弱性によって明らかになった追加情報を利用し、RSA 秘密鍵を復元するために必要なクライアントのログイン試行数がわずか 6 回である攻撃を示す。この最適化された攻撃は、いくつかの暗号解析技術を組み合わせたものである。特に、未知の小さな乗数を持つ Hidden Number Problem の亜種を定式化し、その解を与える。この問題に対する格子構成が、May と Ritzenhofen の因数分解問題に対する改善された結果を与えるために使用できることも示される。

Hull Attacks on the Lattice Isomorphism Problem

Léo Ducas, Shane Gibbons

格子同型問題(LIP)は、2 つの格子の間の同型性を求める問題であり、暗号の基礎として提案されている。この問題は、符号の等価性問題の格子変形であり、符号の hull という概念は壊滅的な攻撃につながる可能性がある。

本研究では、格子設定での hull、すなわち s-hull の適応における暗号解読的役割を研究する。まず、s-hull が算術識別器の作成に役立たないことが示される。これは、s-hull の genus が、sと元の genus から効率的に予測することができる、すなわち余分な情報を持たないためである。

しかしながらその一方で、本論文では、hull は幾何学的な攻撃には利用可能であることが示される。これはある特定の格子では、hull の最小距離は元々の格子よりも比較的小さいことが原因となっている。これによる攻撃にかかる計算量は指数的なままだが、その指数に含まれる定数が半分になる。この 2 つ目の結果は、Ducas & van Woerden が提案した LIP の一般的な困難性予想に対する反例となっている。

以上の結果は、暗号のための LIP インスタンス化においては、hull の幾何に十分な配慮する必要があることを示唆する。また、unimodular 格子は、その自己双対性から、攻撃者に元の格子しか残さないため、興味のあるオプションとなることも指摘されている。特筆すべきこととして、これは提案されているインスタンス化、すなわちトリビアル格子$\mathbb{Z}^n$と Barnes-Wall 格子がすでにそのケースに当てはまっていることも指摘されている。

5. PQCrypto 2023 の発表

New NTRU Records with Improved Lattice Bases

Elena Kirshanova, Alexander May, Julian Nowakowski

NTRU に関する解析論文である。NTRU は 1998 年に生まれた格子ベース暗号の出発点である。NTRU の亜種である NTRU-HPS、NTRU-HRSS は NIST 耐量子暗号コンペティションのラウンド 3 のファイナリストであり、また CRYSTALS-KYBER や FALCON なども NTRU の影響を受けている。Coppersmith と Shamir は、格子基底の簡約を介して NTRU を攻撃することを提案し、その Coppersmith-Shamir 格子の亜種は、Security Innovations, Inc. による$n = 173$次元までの NTRU チャレンジを解読することに成功している。

本論文は、現代の NTRU バージョンを攻撃するツールを提供している。この攻撃ツールは、適切な格子の基底の設定と、G6K ライブラリの格子篩アルゴリズムを用いた現代の BKZ をチューニングすることで為される。この新しい格子基底を用いて、 NTRU - HPS に対して$n \in [101,171]$、HTRU-HRSS に対して$n \in [101,211]$の場合にn次元の暗号解析を実施している。特に既存手法では 172 日を必要とするのに対し、本方式では 83 日以内で HPS - 171 インスタンスへの攻撃を実現している。

Do Not Bound to a Single Position: Near-Optimal Multi-positional Mismatch Attacks Against Kyber and Saber

Qian Guo, Erik Mårtensson

耐量子暗号 Kyber と Saber についての暗号解析論文である。格子ベース KEM では、一時的な鍵の偶発的な再利用が、その安全性を損ないうることが知られている。この鍵ペアを再利用する攻撃として、鍵不一致攻撃が知られている。

本論文では、NIST 耐量子暗号コンペティションにおける第 3 ラウンドの候補である Kyber と Saber に対する鍵不一致攻撃を提案している。著者らの方式は秘密鍵を回復するために必要なオラクルへのアクセス数を削減しており、これはサイドチャネル解析においても重要だと指摘している。

Faulting Winternitz One-Time Signatures to Forge LMS, XMSS, or SPHINCS+ Signatures

Alexander Wagner, Vera Wesselkamp, Felix Oberhansl, Marc Schink, Emanuele Strieder

耐量子署名形式である SPHINCS+に対する故障注入攻撃に関する論文である。ハッシ

ュベースの署名は耐量子署名形式として有力視されており、LMS、XMSS、SPHINCS+などが知られている。Winternitz ワンタイム署名 (WOTS) は、これらすべてで使用される基本的なビルディングブロックの 1 つである。

本論文では、任意の平文に対する署名を偽造する攻撃を可能とする WOTS に標的とする故障注入攻撃を提案している。この故障注入攻撃は、WOTS 内のチェックサム計算を役に立たなくすることで、偽造攻撃を実現している。また本攻撃の実用性の推定や、署名生成または検証を実行する露出デバイスに備えるべき適切な対策も示している。

Breaking and Protecting the Crystal: Side-Channel Analysis of Dilithium in Hardware

Hauke Steffen, Georg Land, Lucie Kogelheide & Tim Güneysu

耐量子署名形式 CRYSTALS-Dilithium に関するサイドチャネル攻撃論文である。CRYSTALS-Dilithium は NIST 耐量子暗号標準であり、ソフトウェア実装に対してはサイドチャネル攻撃による分析が行われてきた。

本論文では、ハードウェア実装に対する分析を実施し、脆弱性のある操作の解析と、Beckwith らによる最近のハードウェア実装に対する単純電力解析 (Simple Power Analysis, SPA) と相関電力解析 (Correlation Power Analysis, CPA) を行っている。SPA 攻撃は 700,000 のトレースのプロファイルを必要とし、プロファイリングが完了次第、1101 個のトレースの係数ペアを特定できる。CPA 攻撃は 66,000 のトレースに対して秘密係数を復元する。本論文はこれらの攻撃に対する具体的な対策も提示している。

Classical and Quantum 3 and 4-Sieves to Solve SVP with Low Memory

André Chailloux, Johanna Loyer

格子ベース暗号の安全性において重要である最短ベクトル問題 (SVP) に関する論文である。d次元 SVP について既知の最速攻撃は、格子篩 (lattice sieving) により行われ、定数t, mに対して時間計算量 $2^{td+o(d)}$かつメモリ計算量$2^{md+o(d)}$で行われる。
格子篩における簡約ベクトルの探索は、与えられた制約を満たすk個のベクトルの配置問題に帰着される。

本論文は、このk-格子篩アルゴリズムのためのフレームワークを提示する。このフレームワークでは、入力となるベクトルのリストをフィルタリングし、総和が零ベクトルとなるk個の符号語を中心とするリストを得た後、フィルタされたリストにおけるシンプルな配置問題を解くことで為される。結果として、$k = 3$の時の時間計算量の改善と、$k = 4$の時の新しいトレードオフを与えている。

Fast Enumeration Algorithm for Multivariate Polynomials over General Finite Fields

Hiroki Furue, Tsuyoshi Takagi

多変数多項式の出力を列挙するアルゴリズムに関する論文である。多変数多項式の出力の列挙は、多変数公開鍵暗号に対する代数的攻撃において重要な問題である。

一般に、有限体$\mathbb{F}_q$上のn変数d次多項式に対する出力列挙アルゴリズムは、$O(\binom{n}{k}q^n)$回の操作が必要である。Bouillaguet らは、CHES 2010 にて、$q=2$の場合の計算量$O(d\cdot 2^n)$である高速列挙アルゴリズムを提案した。このアルゴリズムは Gray 符号の順序に従って与えられた多項式の入力をカバーしている。

本論文では、qが一般の場合にこの結果を拡張し、計算量$O(d\cdot q^n)$である高速列挙アルゴリズムを提案している。提案されたアルゴリズムは、すべての入力をカバーするために Gray コードの代わりに辞書式順序を用いており、特に$q=2$の場合でも Bouillaguet らによるアルゴリズムとは異なる。

Breaking the Quadratic Barrier: Quantum Cryptanalysis of Milenage, Telecommunications' Cryptographic Backbone

Vincent Quentin Ulitzsch, Jean-Pierre Seifert

携帯電話ネットワークに対する量子暗号解析の論文である。現在の携帯電話ネットワークの暗号化に用いられている Milenage アルゴリズムは、7 つの秘密鍵アルゴリズムを中心に、認証と鍵同意が行われている。このアルゴリズムはまだ量子暗号解析の対象になっていなかったが、その一方で近年、量子計算機を用いた対称鍵暗号への攻撃の二次以上の高速化が進んでいる。

本論文では、Milenage アルゴリズムに対する量子解析を実施し、攻撃の二次以上高速化した。特に、異なる量子攻撃モデルによって識別可能な指数的高速化を含む、すべての Milenage アルゴリズムに対する量子攻撃シナリオが提供され、Milenage の量子攻撃に対する構造的弱点を指摘している。

Time and Query Complexity Tradeoffs for the Dihedral Coset Problem

Maxime Remaud, André Schrottenloher, Jean-Pierre Tillich

$\mathbb{Z}_N$における二面体群コセット問題（DCP）は、LWE が帰着できる問題であるため、耐量子暗号における安全性において重要である。Ettinger - Høyer アルゴリズムは線形回のクエリで DCP を解くことが知られているが、時間計算量は指数回数必要である。最初の時間効率の高いアルゴリズムは Kuperberg によって導入された。これらのアルゴリズムは、劣指数時間計算量と$\tilde{O}(2^{\sqrt{c\log N}})$回のクエリで実行される。ここで$c$はある定数である。この Kuperberg 流のふるい分けアルゴリズムは、量子及び古典における時間、メモリ、クエリの間のトレードオフを示している。これらのトレードオフは、クエリコストを抑えたい攻撃者にとってクエリ回数を削減することを可能にする。

それを踏まえ本論文は、Ettinger - Høyer アルゴリズムと Kuperberg アルゴリズムを

補間する方法を示している。この手法によって、線形クエリ-指数時間の攻撃と、劣指数クエリ-劣指数時間の攻撃を滑らかに補間することが可能となり、従って、クエリコストを考慮した攻撃のファインチューニングを可能としている。

6. Crypto 2023 の発表

Differential Meet-In-The-Middle Cryptanalysis

Christina Boura, Nicolas David, Patrick Derbez, Gregor Leander, María Naya-Plasencia

ブロック暗号の SKINNY-128-384 と AES-256 に対する解析論文である。本研究では、差分攻撃と中間一致攻撃を組み合わせた新しい攻撃手法である差分中間一致攻撃を提案する。具体的には、差分攻撃の概念を使用し、解析対象の暗号化関数における中間ラウンドをカバーしながら、その外部ラウンドに対して中間一致攻撃を実行するものである。従来の Demirci-Selçuk 中間一致攻撃も同様のアプローチを採用しているが、特に鍵回復フェーズにおいて提案手法の方が効率的に実行できることを示している。

提案手法を単一鍵設定における SKINNY-128-384 と関連鍵設定における AES-256 に適用した。結果として、25 ラウンド SKINNY-128-384 に対する鍵回復攻撃が時間計算量$2^{372.5}$、データ量$2^{122.3}$、メモリ量$2^{188.3}$で実行できることを示した。また、12 ラウンド AES-256 に対する関連鍵設定での鍵回復攻撃が時間計算量2^{206}、データ量2^{89}、メモリ量$2^{71.6}$、2 つの関連鍵で実行できることを示した。

Moving a Step of ChaCha in Syncopated Rhythm

Shichang Wang, Meicheng Liu, Shiqi Hou, Dongdai Lin

ストリーム暗号 ChaCha に対する解析論文である。既存研究によると、ChaCha に対する最良の鍵回復攻撃は 20 ラウンド中 7 ラウンドまで有効であることが示されている。本研究では、7 ラウンド ChaCha に対する既存の鍵回復攻撃を改善するとともに、最終ラウンドの XOR と Rotation を行わない 7.5 ラウンド ChaCha に対する有効な鍵回復攻撃を初めて示す。

ChaCha に対するほぼ全ての既存研究では、PNB (Probabilistic Neutral Bits) の概念に基づいた差分線形攻撃が使用されている。PNB の概念を使用すると、秘密鍵ビットを 2 つの集合、すなわち重要な鍵ビット (non-PNB) の集合と非重要な鍵ビット (PNB) の集合に分割できる。本研究では、既存の PNB の概念をさらに洗練させるため、シンコペーション (syncopation) と呼ばれる新しい概念を導入した。この新しい概念を使用し、non-PNB に対して新たな制約条件を追加することで、相関性の高い (条件付き) PNB の集合を識別できるようになる。適切な (条件付き) PNB を特定することで、鍵回復攻

撃の改善に貢献できることが知られているため、この新しい概念は理に適っている。結果として、7 ラウンド ChaCha に対する鍵回復攻撃が時間計算量$2^{210.3}$とデータ量$2^{103.3}$で実行できることを示した。また、最終ラウンドの XOR と Rotation を行わない 7.5 ラウンド ChaCha に対する鍵回復攻撃が時間計算量$2^{242.4}$とデータ量$2^{125.8}$で実行できることを示した。

7. FDTC 2023 の発表

Fault Attacks on a Cloud-Assisted ECDSA White-Box Based on the Residue Number System

Christophe Giraud and Agathe Houzelot

White-Box Cryptography は、攻撃者が暗号実装に対して完全にコントロールできる場合において、暗号のソフトウェア実装を保護することを目的とする。2000 年代初頭から、ブロック暗号の White-Box 実装はコミュニティの興味を大いに惹いてきた。しかし、産業界からの需要があったにも関わらず非対称暗号についてはあまり研究されて来なかった。実に、Zhou らが 2020 年に、ECDSA の実装を保護するための最初の非対称暗号の設計を発表したのが唯一のものである。この発表は非対称暗号の white-box に挑む上で偉大な一歩であった。

本論文では、このスキームのセキュリティに関して研究し、故障利用攻撃でプライベート鍵を復元する効率的な方法を提示する。さらに、対応する ECDSA のプライベート鍵を得るためだけに必要な 2 つの故障注入を要する 2 つの攻撃の詳細を述べる。最後に、この両方の攻撃を防ぐための、white-box のサイズやスキームの性能に影響しない対策も提案する。

8. CHES 2023 の発表

Efficient Persistent Fault Analysis with Small Number of Chosen Plaintexts

Fan Zhang, Run Huang, Tianxiang Feng, Xue Gong, Yulong Tao, Kui Ren, Xinjie Zhao and Shize Guo

2018 年に、Zhang らが最初に紹介した Persistent Fault Analysis (PFA)は、ブロック暗号の鍵を復元するために誤った Sbox によって暗号化された暗号文の統計的特徴を使用する。しかし、ほとんどの PFA の変種において、フォールトに関する事前の情報(場所と値)が必要で、複数のフォールトがあるシナリオにおいては関連した解析がさらに困難になる。このような事前要求を回避し、複数のフォールトの下での解析の効率を改善するため、著者は Chosen-Plaintext based Persistent Fault Analysis (CPPFA)と

いう手法を提案している。CPPFA は選択平文を導入することで PFA を容易にし、AES-128 の鍵探索空間を極めて小さく縮小することができる。以前の最新の研究は 1509 個または 1448 個の暗号文を、それぞれ 8 個または 16 個のフォールトの下で必要とするのに対し、著者の提案は 256 個の選択平文に対応する暗号文のみを必要とする。特に、CPPFA はすべてのフォールトの場所、値、量が不明であるような複数フォールトのシナリオでも適用可能で、CPPFA の最悪の時間計算量は AES-128 に対して$O(2^{8+n_f})$で、ここでn_fはフォールトの数を表す。実験結果は、$n_f > 4$のときに、256 組の平文暗号文のペアで AES-128 の鍵を復元できることを示している。LED-64 に対しては、わずか 16 組の平文暗号文のペアで残りの鍵探索空間を 2^{10} まで絞り込むことができる。

JitSCA: Jitter-based Side-Channel Analysis in Picoscale Resolution

Kai Schoos, Sergej Meschkov, Mehdi B. Tahoori and Dennis R. E. Gnad

セーフティとセキュリティの両方が必要な環境において、絶縁された通信チャネルが必要とされることが多い。直流的に絶縁された通信チャネル(Galvanic isolation)は、通常、それを通した物理的なサイドチャネル攻撃に対しても効果があると期待されている。しかしながら、本論文では意図せず通信シグナルの極小のジッタの形でサイドチャネル情報が漏洩し得ることを示している。time-to-digital converter (TDC)を使用した FPGA ベースのレシーバを使用して、最悪のケースで 54±45ps 以内のシグナルジッタを観測する。TDC は典型的なオシロスコープの測定より高い時間分解能を持ち、多くの他のシステムでそのような測定が可能である。送信機に暗号アクセラレータを動作させ、受信機側に FPGA を接続して、TDC を使用して信号のジッタを測定する。著者は送信機で動いている AES アクセラレータの鍵の復元を実行することで、信号のジッタに十分なサイドチャネル漏洩があることを示している。さらに、この漏洩を TDC を使って測定した消費電力によるサイドチャネルと比較し、タイミングジッタのみで十分なサイドチャネル情報を含んでいることも示している。具体的には、前者のオンチップの電力解析による鍵の復元に 27,000 波形を必要とするのと比較して、後者の本論文によるクロスデバイスのジッタベースの攻撃でも、セットアップによるが 47,000 波形で鍵の復元が実行できた。直流的絶縁を実施してもこの結果に大きな変化はなく、よく調整されたジッタタイミング情報は非常に強力な攻撃になり得ることを示している。要約すると、著者は安全と考えられている多くのシステムにおいても情報が漏洩する新しいサイドチャネルベクターを提案している。通信チャネルはシグナルジッタとして知られる小さなタイミング変動を通して意図せず情報を漏洩させ得る。これは極めて多数の装置に影響し、考慮を要することになる。

Improved Attacks on (EC)DSA with Nonce Leakage by Lattice Sieving with Predicate

Luyao Xu, Zhengyi Dai, Baofeng Wu and Dongdai Lin

Lattice Reduction algorithmは、公開鍵暗号に対する最も強力で万能な手法のひとつであると認められている。本論文では、主に、あるサイドチャネル攻撃を通したnonceの漏洩がある(EC)DSAに対するLattice攻撃に集中する。LLLやBKZのようなlattice reduction algorithmに依存する以前の研究では最終的には”lattice barrier”に到達する。”lattice barrier”とは、少ないnonceしか既知でない場合にlattice algorithmが実行不可能になることである。最近では、Albrecht と Heningerが”predicate”で補強したlattice algorithmを紹介し、lattice barrierを突破した(Eurocrypt 2021)。

本論文では先行研究を発展させ、最初に、大きいデータベースの中のlattice vectorを標的とする探索を目的とするより効率的なpredicate algorithmを提案する。そして、predicate algorithmと篩を、”dimension for free”、”progressive sieving”の手法と組み合わせてこの攻撃のパフォーマンスをさらに改良する。さらに、最適なKannan embedding factorをどのように選ぶかについての理論的な解析を与える。

その結果、このアルゴリズムは、最先端の攻撃の現状の記録である、3ビットのnonce漏洩がある256ビットの曲線、2ビットのnonce漏洩がある160ビットの曲線に対する攻撃を、計算時間、サンプル数、成功率の意味で凌駕した。以前には非現実的と考えられていた3ビットのnonce漏洩がある384ビットの曲線と2ビットのnonce漏洩がある160ビットの曲線に対してもlattice recordを更新した。最後に、1ビットのnonce漏洩のあるECDSAへの最初のlattice攻撃を提示する。それは、1ビットのnonce漏洩がある112ビットの曲線への攻撃を現実的な時間で成功させることを可能とする。

Carry-based Differential Power Analysis (CDPA) and its Application to Attacking HMAC-SHA-2

Yaacov Belenky, Ira Dushar, Valery Teper, Vadim Bugaenko, Oleg Karavaev, Leonid Azriel and Yury Kreimer

本論文では、Carry-based Differential Power Analysis (CDPA)と呼ぶ、算術加算を利用する攻撃手法を提案する。この手法をHMAC-SHA-2の攻撃に適用する。この手法の完全な数学的解析を記述し、ある仮定と十分な量の電力波形があればいかなる鍵も復元できることを示す。本論文の実験部分では、ソフトウェアシミュレーションとFPGAボードの両方において、消費電力測定を用いて攻撃が成功することを示す。FPGA ボードにおいてわずか30,000波形の測定で、HMAC-SHA-2の署名の偽造に必要な秘密情報を3%のケースで復元でき、275,000波形での攻撃では成功率が100%に達する。これは、HMAC-SHA-2の実装は、それが純粋なハードウェア実装であっても、サイドチャネル攻撃に対して脆弱であることを意味する。著者の知る限り、これはHMAC-SHA-2の純粋なハードウェア実装に対する本格的な攻撃として初めて公表されるものであり、プロファイルス

テージを必要としない攻撃である。

9. TCC 2023 の発表

Rigorous Foundations for Dual Attacks in Coding Theory

Charles Meyer-Hilfiger, Jean-Pierre Tillich

コードベース暗号に対する dual 攻撃についての論文である。一般の線形符号の復号化やコードベース暗号のパラメータ選択において、情報集合復号（information set decoding, ISD）のテクニックは過去 60 年にわたり支配的であったが、近年、特定のパラメータについては、ISD のテクニックよりも、dual 攻撃の方が高性能であることがわかった。しかし、dual 攻撃の計算量解析はいくつかの仮定に依存しており、その仮定は実験的にも確認されているとは言い難い状況であった。この dual 攻撃は、格子ベース暗号における dual 攻撃のコードベース暗号への類似として見ることができる。格子ベース暗号においても dual 攻撃は有力であることが指摘されており、ある種の確率変数の独立性が成立するかどうかについても同様にわかっていない。

本論文は、コードベース暗号における dual 攻撃において使用される基本的な量について、シンプルな代替表現を与えることで研究を行う。この代替表現は、上述の確率変数の独立性に依存せず研究することができる。この研究によって、Asiacrypt 2022 で導入された dual 攻撃の問題点が明らかとなっている。実際、この dual 攻撃で選択されたパラメータについて、独立性仮定に依存した解析では予想できない誤った候補を生成してしまうことを指摘している。さらにこの dual 攻撃の修正アルゴリズムの提案と、計算量の評価なども行っている。

10. Asiacrypt 2023 の発表

Correlation Cube Attack Revisited: Improved Cube Search and Superpoly Recovery Techniques

Jianhua Wang, Lu Qin, Baofeng Wu

本研究ではある特別なキューブのインデックス集合（ISoC: Index Set of Cube）に関連する superpoly の低次数因子を効率的に抽出することでキューブ攻撃を発展させる。これは EUROCRYPT 2018 で提案された相関キューブ攻撃の特殊ケースと考えられるが、提案するフレームワークの下で、鍵変数に関するより有益な等式を鍵回復フェーズで取得できるという利点がある。提案攻撃を実行するためには、以下に示す 2 つの問題を解決する必要がある。1 つ目の問題は superpoly の代数標準形を効果的に復元すると

ともに、その低次数因子を抽出することである。2 つ目の問題は大量かつ良い性質を有する ISoC を効率的に探索することである。

これらの問題を解決するために、2 つの新しい技術を提案する。1 つ目の提案技術は変数置換技術である。これは鍵変数の複雑な表現を新しい変数に置換するとともに、中間ラウンドにおける内部状態の痕跡を排除するために使用される。新しい変数の導入によって superpoly をよりコンパクトに表現でき、結果として因数分解が容易になる。また、superpoly 復元の計算量を改善できるため、特殊な ISoC を効果的に識別できるようになる。2 つ目の提案技術はベクトル数値マッピング技術である。これは superpoly の次数評価における数値マッピング技術 (CRYPTO 2019) の効率性と単項予測技術 (ASIACRYPT 2020) の精度との間のトレードオフを模索した結果として得られた技術である。これらの技術を組み込むことで、高速枝刈り技術を MILP でモデル化できるようになり、代数次数が一定のしきい値を満たすような良い性質の ISoC をフィルタリングすることができる。また、自動化された MILP ソルバーのおかげで、探索空間全体にわたって適切なキューブを包括的に探索することが現実的に可能となった。

提案手法をストリーム暗号 Trivium に適用した結果、2020 年に Kesarwani らによって提示された 3 つのキューブに対する superpoly を復元できたが、Kesarwani らが主張するように、842 ラウンドまでのゼロサム特性が存在しないことを明らかにした。また、既存の最良かつ現実的な鍵回復攻撃は$2^{53.17}$の計算量で実行可能な 820 ラウンド Trivium に対するものであったが、本研究では 820、825、830 ラウンド Trivium に対して、それぞれ$2^{79.8}$、$2^{79.7}$、$2^{79.4}$個の秘密鍵を2^{60}の計算量で復元した。

Differential-Linear Approximation Semi-Unconstrained Searching and Partition Tree: Application to LEA and Speck

Yi Chen, Zhenzhen Bao, Hongbo Yu

差分線形攻撃は ARX (Addition-Rotation-XOR) 暗号に対する最も効果的な攻撃手法の 1 つである。しかしながら、次のような 2 つの技術的な問題により、この攻撃の効果を高めること、そしてこの攻撃をより多くのアプリケーションに対して適用することが困難であることが課題となっている。1 つ目の問題は、より良い差分線形近似を探索するための効果的な手法が存在しないことである。これは、既存手法を使用するとより良い差分線形近似の探索に多くの制約事項が必要となる、もしくは探索のための手法が非効率であることに起因する。2 つ目の問題は、差分線形攻撃のためのパーティション化技術には鍵回復攻撃の時間計算量を削減する可能性を秘めているが、ARX 暗号に対してパーティションを構築するための汎用的なツールが存在しないことである。

本研究はこれら 2 つの問題の解決を目指す。最初に、新たに考案した探索アルゴリズムに基づき、既知の差分線形近似からより良い差分線形近似を生成するための新しいアイデアを提案する。次に、ARX 暗号に対してパーティションを構築するために、パーテ

ィションツリーと呼ばれる汎用的なツールを提供する。これらの新しい技術に基づき、本研究では 2 つの ISO/IEC 標準暗号である LEA と Speck に対して、既存攻撃よりも優れた攻撃が実行可能であることを示す。

LEA に対して初めて 17 ラウンドの識別子が構成できることを示した。これは既存の最良な識別子よりも 1 ラウンド長い結果となる。また、17 ラウンドの LEA-128、18 ラウンドの LEA-192、18 ラウンドの LEA-256 に対する初めての鍵回復攻撃も示した。これらの攻撃は既存の最良な鍵回復攻撃を 3〜4 ラウンド更新するものである。最後に、Speck48 と Speck64 に対して既存研究よりも優れた識別子が構成可能であることを発見した。さらに、Speck96 と Speck128 に対して初めての識別子を発見した。具体的には、11 ラウンドの Speck48、13 ラウンドの Speck64、15 ラウンドの Speck96、そして 18 ラウンドの Speck128 に対する識別子である。

Quantum Speed-Up for Multidimensional (Zero Correlation) Linear Distinguishers

Akinori Hosoyamada

線形攻撃は共通鍵暗号解析の分野において最も重要な技術の 1 つである。Kaplan らは線形攻撃のための量子技術を用いた平方的高速化手法について提案した。しかしながら、彼らの提案手法は一般的な 1 次元の線形識別子を構成することを目的とした場合にのみ適用できることが知られている。古典的な攻撃において、攻撃にかかる計算量を削減するためにしばしば多次元線形近似が解析されることを踏まえると、Kaplan らの技術を多次元線形解析のために拡張可能かについて検討することは興味深いものと考えられる。

本研究では多次元（ゼロ相関）線形識別子と積分識別子を構成するための量子技術を用いた高速化手法について示す。1) Simon アルゴリズムのサブルーチンとフーリエ変換後の線形相関との間に深い関連性があることに着目する。Simon アルゴリズムはアダマール変換と対象となる関数へのオラクルクエリで構成されるサブルーチンを繰り返し実行するが、このサブルーチンを微修正することで、線形相関の二乗に比例する確率で線形マスクのペアを出力できることを発見した。このサブルーチンを相関抽出アルゴリズム（CEA）と呼ぶ。2) CEA と量子振幅増幅（QAA）技術を組み合わせて多次元線形識別子の構成が高速化可能であることを示す。例えば、メッセージサイズがnビット、ラウンド数をrとすると、Beyne による FEA-1 と FEA-2 への多次元線形識別攻撃にかかる計算量をそれぞれ$\mathcal{O}\left(2^{(r/4-3/4)n}\right)$から$\mathcal{O}\left(2^{(r/8-1/4)n}\right)$と$\mathcal{O}\left(2^{(r/6-3/4)n}\right)$から$\mathcal{O}\left(2^{(r/12-1/4)n}\right)$へ改善できる。3) CEA が多次元ゼロ相関線形識別の構成も高速化可能であることを示す。ラウンド関数が全単射でブロックサイズがnビットである 5 ラウンドのバランス型 Feistel 構造とタイプ I/II 一般化 Feistel 構造に対して、提案手法を用いると計算量$\mathcal{O}\left(2^{n/2}\right)$で量子識別子を構成することができる。4) 積分識別子の構成に関する高速化手法を示す。この高速化手法は積分特性とゼロ相関線形特性の深い関連性に依るものであ

る。特に、単一の量子クエリによって、4 ビットセルの SPN 暗号における積分特性が 2.5 ラウンドの AES における積分特性と等価であることを明らかにした。5) CEA におけるアダマール変換を汎用的な量子フーリエ変換に置き換えることで、提案手法は任意の有限アーベル群に対する汎用的な線形識別子の構成へと拡張できる。具体的には、Bayne による FF3-1 構造への識別攻撃を高速化できることを示した。

Exact Security Analysis of ASCON

Bishwajit Chakraborty, Chandranan Dhar, Mridul Nandi

ASCON は NIST が主催する軽量暗号標準化プロセスの最終選考方式であり、Duplex 構造の認証暗号方式に加えて Sponge 構造のハッシュ関数を提供する。ASCON の認証暗号方式には ASCON-128 と ASCON-128a と呼ばれる 2 つのバリエーションがあり、過去には軽量な認証暗号アプリケーションとして CAESAR コンペティションの最終選考方式の 1 つに選出された。

この論文では、ランダム置換モデルにおける ASCON 認証暗号方式の安全性を厳密かつ網羅的に評価した結果を示す。ASCON（と Duplex 構造を持つ一般的な認証暗号方式）の偽造不可能性に関する既存の安全性は、Dをデータ計算量、Tを時間計算量、cをスポンジ構造のキャパシティとすると、$DT/2^c$で表すことができる。ここで、κを鍵サイズ、τをタグサイズ、bを基礎となる暗号学的置換のブロックサイズ（ASCON の場合は 320 ビット）とする。本研究では、Tの上界を2^κと2^cのうちの最小値、Dの上界を2^τと2^cのうちの最小値、DTの上界を2^bと限定した場合において、ASCON が AE 安全性（理想的な認証暗号との識別不可能性）を達成できることを示した。

軽量暗号標準化プロセスにおける NIST が提示した要求($D \leq 2^{53}$、$T \leq 2^{112}$、$\kappa \geq 128$、$\tau \geq 64$)を考慮すると、キャパシティサイズが$c = 136$、タグサイズが$\tau = 64$において、ASCON の AE 安全性が保証されることを明らかにした。このパラメータ選択は 184 ビットという高いレートを実現できることから、ランダム置換モデルにおける ASCON の AE 安全性を損なうことなく、ASCON の効率性をさらに高めることができることを意味する。

Revisiting Higher-Order Differential-Linear Attacks from an Algebraic Perspective

Kai Hu, Thomas Peyrin, Quan Quan Tan, Trevor Yap Hong Eng

本研究では、高階差分（HD）攻撃と高階差分線形（HDL）攻撃を代数的側面から見直すとともに、HD/HDL 識別子を検出するための 2 つの新しいツールを提供する。1 つ目のツールは Higher-order Algebraic Transitional Form（HATF）と呼ばれものであり、確率的 HD/HDL 近似を検出するために使用される。dを対象となる関数の代数次数とすると、一般的に HATF は計算量が$\mathcal{O}\left(2^{\ell+d2^\ell}\right)$となる$\ell$階 HDL 近似のバイアスを見積もるこ

とができる。もし対象となる関数が 2 次関数であるならば、計算量をさらに$\mathcal{O}(2^{3.8\ell})$にまで削減可能できるため、ASCON や Xoodyak のようにラウンド関数を 2 次関数で表現可能な暗号方式に対する HDL 攻撃に HATF が有効となる。また、2 つ目のツールは Differential Supporting Function（DSF）と呼ばれるものであり、暗号学的置換への入力に対して適切な線形近似を見つける便利な方法を提供することで、決定的 HD 識別子を容易に探索することを可能にする。

HATF を使用することで、ラウンドを削減した ASCON と Xoodyak の初期化フェーズにおける多くの HDL 近似を発見した。例えば、5 ラウンド ASCON に対しては 8 階 HDL 近似まで得ることができ、既存の最良な差分線形（DL）近似を使用した場合と比較して、識別攻撃の計算量を2^{16}から2^{12}まで削減した。また、単一鍵設定において、これまで 6 ラウンド ASCON と 5 ラウンド Xoodyak に対する DL 識別子は存在しなかったが、HATF を使用することで HDL 識別子が存在することを示した。HATF は DL 攻撃（つまり、1 階 HDL 攻撃）に対しても十分に機能し、ASCON や Xoodyak における既存の DL 近似を理論的観点から説明できるようになった。

DSF を使用することで、8 ラウンド ASCON-p（ASCON で使用される暗号学的置換）に対する新しい識別攻撃が実行可能であり、既存の最良な攻撃と比較して計算量を2^{130}から2^{48}まで削減した。また、フルラウンド ASCON-pに対するゼロサム識別攻撃も実行可能であり、既存の最良な攻撃と比較して計算量を2^{130}から2^{55}まで削減した。

More Insight on Deep Learning-aided Cryptanalysis

Zhenzhen Bao, Jinyu Lu, Yiran Yao, Liu Zhang

CRYPTO 2019 において、Gohr は洗練されたニューラルネットワークを使用することで差分分布表（DDT）ベースの識別子よりも優れた暗号学的識別攻撃を実行できることを示した。これは差分ニューラル識別子（ND）が純粋な暗号文差分以外の追加情報を使用している可能性について提言するものである。しかしながら、この可能性に関する明示的な理論はまだ明らかとなっていない。

本研究では DDT と併用可能な明示的なルールを提供する。nをワードサイズとすると、この明示的なルールは法2^nの下での算術加算を通じて得られる XOR 差分伝搬の正しいペアにおけるビット値間の強い相関性に基づいており、純粋な DDT ベースの識別子と比べて差分ニューラル識別子の効果を高めることが期待できる。興味深いことに、これらのルールはマルチビット制約に関する先行研究（ASIACRYPT 2012、 CRYPTO 2013）や固定鍵差分確率の最新研究（CRYPTO 2022）と密接に関連している。対照的に、これらのルールの組み合わせでは ND のパフォーマンスは向上しないことが明らかになった。これはこれらのルールもしくはこれらのルールと同等の形式が ND によってすでに利用されているということを示唆するものであり、暗号解析分野におけるニューラルネットワークの威力が浮き彫りになったと考えられる。

さらに、本研究では、差分ニューラル識別子の精度と攻撃可能ラウンド数を向上させるためには、差分伝搬を制御することが不可欠であることを明らかにする。通常、秘密鍵に対して差分を埋め込むと、ブロック暗号のデータ処理部における内部状態の差分を打ち消すことができ、結果としてより強力な差分伝搬を得ることが可能となる。ただし、従来の攻撃とは異なり、差分ニューラル攻撃は出力差分を指定しないため、単一の差分伝搬に限定されないという特徴がある。つまり、鍵差分が差分ニューラル攻撃にとって有益かどうかが不明確であると言える。また、これに伴って、Speck が関連鍵設定での差分ニューラル攻撃に対してどの程度の耐性があるかも不明確であると言える。本研究では、14 ラウンド Speck32/64 に対する鍵回復攻撃を実行することにより、関連鍵設定での差分ニューラル攻撃が単一鍵設定の場合よりも強力であることを確認した。

Quantum Attacks on Hash Constructions with Low Quantum Random Access Memory

Xiaoyang Dong, Shun Li, Phuong Pham, Guoyan Zhang

ASIACRYPT 2022 において、Benedikt、Fischlin、Huppert は繰り返しハッシュ関数への量子ハーディング攻撃を初めて提案した。この攻撃は指数関数的な量子ランダムアクセスメモリ量（qRAM: quantum Random Access Memory)、具体的にはnをハッシュ関数の出力長とすると、$2^{0.43n}$の量子アクセス可能な古典メモリ（QRACM: Quantum Random Accessible Clasical Memory）が必要となる。大規模な qRAM の必要性は現実的ではなく、Benedikt らは少ない qRAM（low-qRAM）で実行可能な量子ハーディング攻撃の検討を今後の課題としている。本研究ではこの課題に対する回答を提示する。

1 つ目の貢献は、ASIACRYPT 2017 で提案された Chailloux らの衝突探索アルゴリズムに基づき、繰り返しハッシュ関数への新しい量子ハーディング攻撃アルゴリズムを提案したことである。提案する攻撃は Benedikt らの攻撃と比べて$2^{0.43n}$から$2^{0.46n}$とわずかに計算量が高くなるものの、qRAM を全く必要としないこと(no-qRAM)が特徴的である。

2 つ目の貢献は、hash XOR combiner、hash concatenation combiner、Hash-Twice、そして Zipper hash に対する様々な low-qRAM または no-qRAM な量子攻撃を提示したことである。hash XOR combiner に対する攻撃では、CRYPTO 2022 で提案された Schrottenloher と Stevens の量子中間一致攻撃、2007 年に SIAM J. Comput.で提案された Ambainis の element distinctness アルゴリズム、そして SAC 2020 で提案された Jaques と Schrottenloher の衝突探索アルゴリズムに基づくものであり、これらの技術を発展させて 3 種類の異なる low-qRAM 量子原像攻撃を提案し、既存攻撃を改善できることを示した。hash concatenation combiner に対する攻撃では、新しい no-qRAM 量子衝突攻撃と no-qRAM 量子ハーディング攻撃を提案し、それぞれ既存攻撃を改善できることを示した。また、その他の重要な hash combiner である Hash-Twice と Zipper hash に対し、初めてとなる量子ハーディング攻撃を示した。

Algebraic Attacks on Round-Reduced Rain and Full AIM-III

Kaiyi Zhang, Qingju Wang, Yu Yu, Chun Guo, Hongrui Cui

Picnic は MPC-in-the-Head パラダイムに従って設計された共通鍵暗号プリミティブに基づく署名アルゴリズムであり、NIST PQC における第 3 ラウンドの追加候補となっている。より安全で効率的な署名方式を設計するために、AES に基づく伝統的な一方向性関数を利用する、または LowMC、Rain、AIM のような低計算量の一方向性関数を利用することが最近の主流となっている。なお、LowMC、Rain、AIM はそれぞれ署名アルゴリズムの Picnic、Rainier、AIMer で使用される共通鍵暗号プリミティブである。Rainier と AIMer は MPC-in-the-Head に基づく署名方式の中でも最も効率的であると言われており、これらは耐量子デジタル署名アルゴリズムの有望な候補となっている。一方で、これらの署名アルゴリズムとその基礎となる共通鍵暗号プリミティブに対して安全性評価が十分ではない。

本研究では Rain と AIM に対する代数攻撃耐性の評価結果について示す。最初に、1 ラウンドに簡略化した Rain に対して、2^nの計算量で攻撃が実行できることを示す。なお、nはセキュリティパラメータであり、$n \in \{128, 192, 256\}$である。次に、2 ラウンドに簡略化した Rain に対して、それぞれ$2^{120.3}$、$2^{180.4}$、$2^{243.1}$の計算量で攻撃が実行できることを示す。さらに、192 ビット安全性を有する AIM バリエーションの AIM-III に対して、フルスペックにも関わらず$2^{186.5}$の計算量で攻撃が実行できることを示す。これらの攻撃は体上の冪函数の代数的構造に関する性質を利用したものである。最後に、提案する代数攻撃に対して AIM の安全性を保証するための対策案について提供する。

Exploiting the Symmetry of $\mathbb{Z}^n$: Randomization and the Automorphism Problem

Kaijie Jiang, Anyu Wang, Hengyi Luo, Guoxiao Liu, Yang Yu, Xiaoyun Wang

格子暗号の多くは、SVP や CVP 等の格子点探索問題の困難性を安全性の根拠としている。その一方で、他の計算問題を根拠とした暗号の開発も進められている。格子同型問題（LIP: Lattice Isomorphism Problem）は 2 つの格子L_1, L_2が与えられたときにそれらが直交変換により写像されるかどうかを問う問題である。インスタンスは 2 つの基底行列B_1, B_2の形で与えられ、$OB_1 = B_2$を満たす直行行列、つまり$O^T O = I$を満たすある行列Oを求めることになる。この問題の困難性を用いた公開鍵暗号（Bennett et al.、ePrint 2021/1548)、署名(Ducas et al.、 Asiacrypt2022)などの基本的な暗号プリミティブがここ数年で提案されている。特に、$L_2 = \mathbb{Z}^n$（整数格子）に固定した LIP は$\mathbb{Z}$LIP と呼ばれ、この形の問題が過去の格子暗号の解析において暗に用いられてきた歴史がある。

$\mathbb{Z}^n$を直交変換により回転させた格子は著しい対称性を持ち、特に格子の自己同型群 Aut(L)は符号付き置換群と同型であることが知られる。この性質を用いることで$\mathbb{Z}$LIP に関連する計算問題の困難性を調査したことがこの論文の主結果である。上に述べた

LIP、 ℤLIP 以外で扱われている計算問題と困難性に関する結果を以下にまとめる。

- ℤSVP、γ- ℤSVP：$\mathbb{Z}^n$と同型であることが知られている格子Lに対して、最短ベクトルを求める問題、およびそのγ近似を求める問題。γ=O(1)の場合には困難性はℤSVP と等しい。ℤSVP≧ℤLIP。
- SCVP、 ℤSCVP：自身とその双対格子が等しい格子をユニモジュラ―格子と呼び、ユニモジュラ―格子内のベクトル$w \in L$が任意の$v \in L$に対して$\langle w, v\rangle \equiv \langle v, v\rangle \bmod 2$を満たすときに特性ベクトル(characteristic vector)であると呼ばれる。SCVP は与えられたユニモジュラ―格子の中で最短の特性ベクトルを求める問題であり、ℤSCVP は格子の種類を$\mathbb{Z}^n$と同型なものに制限したものである。ℤSCVP≧ℤLIP。
- LAP、 ℤLAP：格子基底 B が与えられたときに、その格子の自己同型群 Aut(L)の中で非自明なものを求める問題。ℤLAP は格子の種類を$\mathbb{Z}^n$と同型なものに制限している。ℤLAP≡ℤLIP、LAP≡LIP
- HSP:隠れ部分群問題。群Gとそれを定義域とする関数fが、ある部分群 H に対して$f(g_1) = f(g_2) \Leftrightarrow g_1 H = g_2 H$を満たすとき、$f$を計算するオラクルへのアクセスから$H$の生成元を求める問題。$G = GL_n(\mathbb{Z})$かつ$H = Stab(B^T B) \leq G$の場合にℤLIP からの帰着が存在する。

技術的には randomized reduction framework と呼ばれる、離散ガウス分布を用いた格子のランダム基底生成を利用したランダム帰着である。上に述べた帰着以外にも、n次元のℤLIP から$(n/2)$次元の SVP、ℤLIP およびℤSVP から O(1)-uSVP への帰着が知られている。

Non-Interactive Commitment from Non-Transitive Group Actions

Giuseppe D'Alconzo, Andrea Flamini, Andrea Gangemi

群作用に関する困難性仮定は耐量子計算機暗号に良く用いられる。実際、CSIDH では、楕円曲線上の同種写像に基づいた仮定から、プリミティブを構成している。さらに、テンソルや、符号問題に基づいたプリミティブもある。

本論文では、群作用に基づいたビットコミットメント法を提案する。提案法は、非推移的な群作用に基づいて構成され、Decisional Group Action Inversion 問題を安全性の根拠とし、標準モデルで安全性が証明できる。

既存のビットコミットメント法は、コミットメントのフェーズで、送信者と受信者の間で通信を行う interactive な手法であったが、本提案方式は non-interactive な方式である。さらに、送信者が honest である場合は、2 つのコミットメントがあった場合に、同じ入力値から作られたコミットメントかどうかを、入力値を示すことなく示すことができる、という特徴 (Linkable Commitment) も有する。そして、このようなコミットメントが持つべき安全性を新規に定義した。

Concrete Analysis of Quantum Lattice Enumeration

Shi Bai, Maya-Iggy van Hoof, Floyd B. Johnson, Tanja Lange, Tran Ngo

格子の SVP、 CVP を解く基本的なアルゴリズムである格子点列挙(Lattice Enumeration)アルゴリズムは深さ優先の木探索アルゴリズムとして実装されることが多く、その量子版アルゴリズムを考えることは安全性評価にとって重要である。深さn、大きさTの木を探索する量子アルゴリズムは(Montanaro、 ToC2018)および(Ambains-Kokainis、 STOC2017)による量子 Tree Backtrack を用いた$O(\sqrt{T} * poly(n))$時間のものが知られており、いくつかの先行研究において格子探索への応用が言及されていた。初期の具体的な計算量の見積もりとして(Aono-Nguyen-Shen、 Asiacrypt18)による枝刈りのフレームワークと組み合わせた場合の漸近的な計算量の解析が存在する。論文の主な結果として、上記 Montanaro、 Ambains-Kokainis らのアルゴリズムを組み合わせた量子木探索の詳細な回路と計算量評価を与えている。類似研究として量子回路の深さを制限した場合の古典-量子ハイブリッドアルゴリズムによる格子点探索の計算量を扱った(Bindel et al.、 ePrint 2023/1423)が存在する。

量子回路の設計は”Clifford+T”と呼ばれる標準的な手法を用いている。これは量子万能回路が Clifford gates と呼ばれる量子ゲートのセット（H、S、CNOT が代表元として取られることが多い）と、非 Clifford ゲートである$T = \sqrt{S}$を用いて構成可能であることから、以上の 4 種のゲートを用いて回路を構成するモデルである。また、Tゲートの低誤り実装が他の Clifford gates と比べて困難であることから T ゲートの個数、深さを用いて量子計算量の見積もりがなされることが多い。なお、論文内の実際の設計では非 Clifford ゲートとして Toffoli ゲートも用いており、リソースの見積もりの段階で 1Toffoli=4T (Selinger、 Phys. Rev. A87 042302)の変換を行っている。

著者らはまず回路の T ゲートの個数と深さを、木のサイズ$\mathcal{T}$、格子次元 n、ノードから伸びる子の数の最大値 d、浮動小数点の精度 p、入力格子中の成分の最大値 B を含む複雑な式により評価し、次に先行研究および論文内の計算機実験によるヒューリスティックな評価を代入することで漸近計算量$\sqrt{\mathcal{T}n}$からのオーバーヘッドを正確に見積っている。深さとサイズのオーバーヘッドはそれぞれ$128cn^3 \log n$と$10752n^6$としている。ここで、c は$\log \mathcal{T} \approx c \cdot n \log n$となる支配的項であり、既存の研究では 0.125 程度と見積もられているが著者らは懐疑的である。

Solving the Hidden Number Problem for CSIDH and CSURF via Automated Coppersmith

Jonas Meers, Julian Nowakowski

HNP(Hidden Number Problem)は$\mathbb{Z}_p$において複数の整数の組$\left(t_i, \mathrm{MSB_k}(\alpha \cdot t_i \bmod p)\right)$が与えられたときに整数$\alpha$を復元する問題である。ここで、$\mathrm{MSB_k}$は入力の上位$k$ビットを返す関数であり$k$の大きさにより問題の困難性が異なる。Diffilie-Hellman 鍵共有にお

いて、g^{ab}の上位$k \geq \sqrt{\log p}$ビットから HNP を経由して残りのビットを復元する古典的な結果(Boneh-Venkatesan、 CRYPTO1996)をベースとして、ECDSA、SGX、DSA、qDSA などの様々な状況において Computational Diffie-Hellman 問題の部分解導出の困難性や、暗号方式のサイドチャネル攻撃への耐性を議論するために気論が拡張されている。これらは$\mathrm{MSB_k}(\alpha \cdot t_i \bmod p)$関数の$\alpha \cdot t_i$の部分を対象となる Diffie-Hellman 鍵共有の群に合わせて適切な多項式関数$f(\alpha, t_i)$とし、$\mathrm{MSB_k}(\cdot)$の値からαを復元する問題は mod Nにおける多変数連立方程式の小さい解を求める問題へと変換される。方程式の求解は Coppersmith 法と呼ばれるヒューリスティックな多項式時間アルゴリズムを用いて解かれる。

この論文では同種写像暗号の一種である CSIDH と CSURF で用いる楕円曲線群に合わせ HNP の変種である CI(Commutative Isogeny)- HNP を定義し、Coppersmith 法を用いた場合に多項式時間で解けるパラメータの範囲について議論している。主な結果として、CSIDH、CSURF に対してそれぞれ共有鍵となる曲線$E_{AB} = CDH(E_A, E_B)$を表現するそのモンゴメリ係数(M_0, M_1)の上位kビットを与えるオラクルにアクセス可能な場合に、それぞれ$k \geq 13/24$、 31/41 であれば多項式時間での完全復元が可能であることを示した。

技術的には CSIDH、CSURF に対する CI-HNP に対応する方程式はそれぞれ 3 変数 3 制約式の 2 次方程式と、2 変数 1 制約式の 3 次方程式であり、Coppersmith 法における多項式格子の構成における自動化手法の提案と sage による計算機実験を行い、ソースコードを公開している。

Memory-Efficient Attacks on Small LWE Keys

Andre Esser, Rahul Girme, Arindam Mukherjee, Santanu Sarkar

LWE 問題は NIST 標準化方式の CRYSTALS-Kyber、 Dilithium をはじめとする多くの代表的な格子暗号の安全性の根拠として用いられている。近年ではオリジナルの LWE 暗号(Regev、 STOC2005)のようにエラー分布に離散ガウス分布を用いることは少なく、実装上の都合から$\{-t, \ldots, t\}^m$のような制限された区間上の確率分布を用いることが多い。この論文では、この種の LWE を small max norm LWE 問題として定式化し、nested collision search と呼ばれる新たな組み合わせ論的アルゴリズムを提案している。これは、先行研究で用いられてきた meet-in-the-middle 系列のアルゴリズムよりも少ない多項式サイズでのメモリで動作するが、衝突探索を並列化することで時間空間計算量トレードオフを考えることも可能である。

論文が対象としているのは Ternary LWE と呼ばれる、$\boldsymbol{s}, \boldsymbol{e}$の成分がともに{-1,0,1}からサンプリングされたときに$(A, \boldsymbol{b} = A\boldsymbol{s} + \boldsymbol{e})$から$\boldsymbol{s}$を復元する問題である。

原理は以下のようになる。Odlyzko ハッシュ関数の変種で、一部の成分を取り出した関数$f_1(\boldsymbol{x}) = h(A\boldsymbol{x}), f_2(\boldsymbol{y}) = h(\boldsymbol{b} - A\boldsymbol{y})$ をランダムにサンプリングしたベクトル$\boldsymbol{x}, \boldsymbol{y}$に対して計算を行い、衝突$f_1(\boldsymbol{x}) = f_2(\boldsymbol{y})$かつ$\boldsymbol{x} + \boldsymbol{y}$が Ternary になっている時点で$\boldsymbol{x} + \boldsymbol{y}$が問

題の解となっている確率が高いという事実を利用する。ここで、ハッシュ関数の衝突検索には通常 meet-in-the-middle 法のように大量のメモリ空間を必要とするが、ρ法を用いることにより多項式空間で動作するものが得られる。上記分割は$\boldsymbol{x}+\boldsymbol{y}$の 2 つのみであったが、4 分割およびそれ以上による nested collision search を用いることも可能である。この場合には最初のレイヤーで$\boldsymbol{x}=\boldsymbol{x_1}+\boldsymbol{x_2},\ \boldsymbol{y}=\boldsymbol{y_1}+\boldsymbol{y_2}$の再分割を行い、それぞれの部分空間で発見した衝突の情報をもとに上のレイヤーで結合を行う。合計 3 回のρ法の呼び出しが必要となるが、指数関数的な計算時間の改良が可能である。

同様のアイデアは s、e を{-2,…,+2}や{-3,…,+3}からサンプリングしている CRYSTAL-Dilithium の解析にも適用可能であり、多項式空間アルゴリズムの計算量が$2^{1.742n}$から$2^{1.282n}$へと大幅に改善した。

Too Many Hints - When LLL Breaks LWE

Alexander May, Julian Nowakowski

格子暗号へのサイドチャネル攻撃の文脈から、LWE 問題において秘密ベクトル s およびエラーベクトル e の部分情報を知ることでどの程度問題が簡単になるのかを調査することは暗号学的に興味深い課題である。この論文では、$\langle \boldsymbol{v},\boldsymbol{s}\rangle=\ell$を満たす組$(\boldsymbol{v},\ell)$を perfect hint、$\langle \boldsymbol{v},\boldsymbol{s}\rangle=\ell \bmod m$を満たす組$(\boldsymbol{v},\ell,m)$を modular hint と呼び、これらの値がどの程度集まれば元の LWE 問題の困難性が著しく下がるのかが議論されている。特に、CRYSTALS-Kyber の 512 次元パラメータにおいて 449 個の modular hint があれば LLL アルゴリズムのみで鍵復元が可能である事、200 個程度の perfect hints があれば LLL もしくは BKZ-20 程度の弱い基底簡約アルゴリズムのみで鍵復元が可能であることが実験的に示されている。

技術的には Perfect hint、 Modular hint の列から LWE の次元削減を行い、また Perfect hint を用いて格子の体積を上げることで疎な格子を構成する。両者とも格子点探索の計算量を下げる方向に格子を変換する手法である。

CRYPTREC Report 2023
(暗号技術評価委員会報告 CRYPTREC RP-2000-2023)

発行日　2024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
（セキュリティセンター セキュリティ技術評価部 暗号グループ）
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN
2-28-8 HONKOMAGOME,BUNKYO-KU
TOKYO,113-6591 JAPAN