CRYPTREC Report 2022

令和 5 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-2000-2022

「暗号技術評価委員会報告」

CRYPTREC Report 2022

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 2022 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 2022 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、多くの国際会議がオンラインで実施されるなか、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。それに加え、今年度は CRYPTREC 暗号リストの改定にあたる年度であることから、CRYPTREC 暗号リストの更新の有無についても確認した。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、2021 年度に決定した執筆方針に基づき、「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を作成した。また、公開鍵暗号の安全性に直結する素因数分解の困難性に関する計算量評価や楕円曲線上の離散対数計算の困難性に関する計算量評価に関する予測図を更新した。次に、b)高機能暗号(Advanced Cryptography)に関するガイドラインを作成するため、暗号技術調査ワーキンググループ(高機能暗号)の設置を継続し、四方順司先生に主査をご担当いただき、委員を 8 名追加した上で 2021 年度に決定した執筆方針に基づき、「CRYPTREC 暗号技術ガイドライン(高機能暗号)」を作成した。次に、c)軽量暗号に関するガイドラインを、2016 年度に公開した「CRYPTREC 暗号技術ガイドライン(軽量暗号)」を更新する形で作成するために、2021 年度に決定した更新方針に基づいて、NIST 軽量暗号プロジェクトのファイナリスト 10 方式に加え、ISO/IEC 29192 シリーズで規格化されている軽量メッセージ認証コードの 1 つである Tsudik's keymode を対象とした安全性評価及び実装性能評価を実施した。また、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た。

2000 年に IT 基本法が制定されたほぼ同時期に発足して以来、23 年間にわたる CRYPTREC 活動は、安全・安心な ICT 社会の実現に貢献してきた。近年のコロナ禍により、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・多様化を推進することが期待されている。その中で暗号技術に対する社会のニーズはかつてないほど大きくなっている。今後も、社会の情勢を踏まえ、健全なサイバー空間の実現・維持につなげるべく、暗号技術の安全性という観点から必要とされる活動を展開していきたい。暗号技術評価委員会の活動は暗号技術やその実装及び運用に携わる研究者及び技術者の献身的な協力により成り立っている。末筆ではあるが、本活動に様々な形でご協力頂いている関係者の皆様に深甚なる謝意を表する次第である。

暗号技術評価委員会　委員長　　高木 剛

本報告書の利用にあたって

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

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

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

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

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

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

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

【問合せ先】　info@cryptrec.go.jp

委員会構成

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

暗号技術調査ワーキンググループ(以下、「調査 WG」という。)は、評価委員会の下に設置され、NICT と IPA が共同で運営する。調査 WG は、評価委員会の指示の下、評価委員会活動に必要な項目について調査・検討活動を担当する作業グループである。評価委員会の委員長は、実施する調査・検討項目に適する主査及びメンバーを選出し、調査・検討活動を指示する。主査は、その調査・検討結果を評価委員会に報告する。2022 年度、評価委員会の指示に基づき実施される調査項目は、「暗号技術調査 WG(耐量子計算機暗号)」及び「暗号技術調査 WG(高機能暗号)」にてそれぞれ検討される。

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

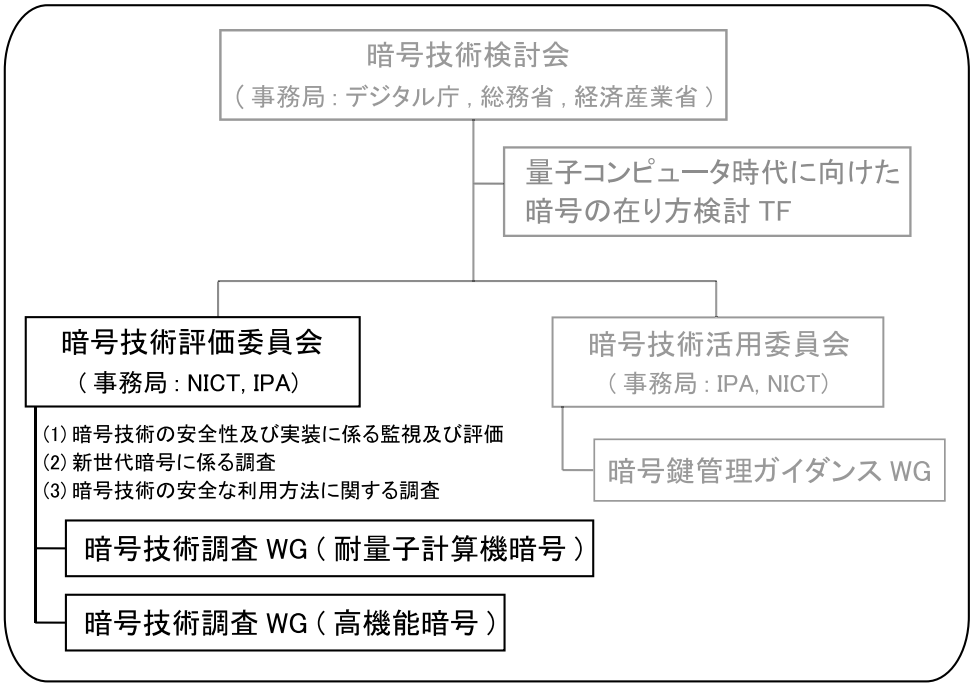

図 0.1：CRYPTREC 体制図

委員名簿*

暗号技術評価委員会

委員長	高木 剛	東京大学 教授
委員	青木 和麻呂	文教大学 准教授
委員	岩田 哲	名古屋大学 准教授
委員	上原 哲太郎	立命館大学 教授
委員	大東 俊博	東海大学 准教授
委員	國廣 昇	筑波大学 教授
委員	四方 順司	横浜国立大学 教授
委員	手塚 悟	慶應義塾大学 教授
委員	花岡 悟一郎	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
委員	山村 明弘	秋田大学 教授

暗号技術調査ワーキンググループ(耐量子計算機暗号)

主査	國廣 昇	筑波大学 教授
委員	青木 和麻呂	文教大学 准教授
委員	伊藤 忠彦	セコム株式会社 主務研究員
委員	草川 恵太	日本電信電話株式会社 主任研究員
委員	下山 武司	国立情報学研究所 特任准教授
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	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

暗号技術調査ワーキンググループ(高機能暗号)

主査	四方 順司	横浜国立大学 教授
委員	岩本 貢	電気通信大学 教授
委員	大原 一真	産業技術総合研究所 主任研究員
委員	金岡 晃	東邦大学 准教授
委員	勝又 秀一	産業技術総合研究所 主任研究員／ PQShield Ltd. Lead Cryptography Researcher

* 2023 年 3 月末時点

委員	川原 祐人	日本電信電話株式会社 主任研究員
委員	国井 裕樹	セコム株式会社 グループリーダー
委員	須賀 祐治	株式会社インターネットイニシアティブ シニアエンジニア
委員	鈴木 幸太郎	豊橋技術科学大学 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	濱田 浩気	日本電信電話株式会社 主任研究員
委員	外園 康智	株式会社野村総合研究所 上級研究員
委員	山田 翔太	産業技術総合研究所 主任研究員
委員	米山 一樹	茨城大学 教授
委員	渡邉 洋平	電気通信大学 助教

オブザーバー

東　 隆夫	内閣官房内閣サイバーセキュリティセンター
宮崎 俊一	内閣官房内閣サイバーセキュリティセンター
高橋 元	内閣官房内閣サイバーセキュリティセンター
高木 浩光	内閣官房内閣サイバーセキュリティセンター
原田 貴志	個人情報保護委員会 事務局
永本 理恵	警察庁 長官官房技術企画課
千葉 亮輔	デジタル庁 デジタル社会共通機能 G
角田 梨翔	デジタル庁 デジタル社会共通機能 G［2022 年 12 月まで］
弓 智宏	デジタル庁 デジタル社会共通機能 G［2022 年 7 月から］
桜田 啓介	デジタル庁 デジタル社会共通機能 G［2022 年 7 月から］
武井 亮	デジタル庁 デジタル社会共通機能 G［2022 年 12 月から］
上田 恭平	総務省 自治行政局 住民制度課［2022 年 6 月まで］
岡 航平	総務省 自治行政局 住民制度課［2022 年 7 月から］
田川 陽子	総務省 自治行政局 住民制度課
平間 將史	総務省 自治行政局 住民制度課
和田 憲拓	総務省 サイバーセキュリティ統括官室［2022 年 7 月まで］
河合 直樹	総務省 サイバーセキュリティ統括官室[2022 年 8 月から］
服部 裕史	総務省 サイバーセキュリティ統括官室
増田 幸司	総務省 サイバーセキュリティ統括官室［2022 年 7 月まで］
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
弓濱 まどか	外務省 大臣官房［2022 年 6 月から］
小林 圭寿	防衛省 整備計画局情報通信課
椛木 隆慎	防衛省 整備計画局情報通信課
松川 陽介	防衛省 整備計画局情報通信課[2023 年 12 月まで］

和平 裕紀　　経済産業省 商務情報政策局
村山 裕紀　　経済産業省 商務情報政策局［2022 年 5 月まで］
澤田 知子　　経済産業省 商務情報政策局［2022 年 6 月から］
伊藤 愼崇　　警察大学校
黒澤 敦　　警察大学校
多賀 文吾　　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、野島 良、篠原 直行、大久保 美也子、黒川 貴司、金森 祥子、吉田 真紀、青野 良範、小川 一人、伊藤 竜馬、高安 敦、横山和弘、笠井 祥、大川 晋司）

独立行政法人情報処理推進機構（瓜生 和久[2022 年 5 月まで]、高柳 大輔[2022 年 6 月から]、神田 雅透、石川 誠、福岡 尊、松﨑 博子、白岩 裕子）

第１章　活動の目的

1.1 電子政府システムの安全性確保

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

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

暗号技術に対する解析・攻撃技術の高度化が日夜進展している状況にあることから、今後も、CRYPTREC によって発信される情報を踏まえて、関係各機関が連携して情報システム及び情報通信ネットワークをより安全なものにしていくための取り組みを実施していくことが非常に重要である。また、過去 23 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

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

奨暗号リストの改訂に関する調査・検討を行うことが重要であるとの認識の下に、暗号技術評価委員会が発展的に改組され、暗号技術検討会の下に「暗号技術監視委員会」が設置された。設置の目的は、電子政府推奨暗号の安全性を把握し、もし電子政府推奨暗号の安全性に問題点を有する疑いが生じた場合には緊急性に応じて必要な対応を行うこと、また、電子政府推奨暗号の監視活動のほかに、暗号理論の最新の研究動向を把握し、電子政府推奨暗号リストの改訂に技術面から支援を行うことである。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年度からは、暗号技術調査ワーキンググループ（耐量子計算機暗号）及び暗号技術調査ワーキンググループ（高機能暗号）の2つのワーキンググループが設置されている。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。なお、2021年度から設置された暗号技術調査ワーキンググループ（耐量子計算機暗号）及び暗号技術調査ワーキンググループ（高機能暗号）の活動の詳細については、第3章を参照のこと。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)」の改定を2023年度に予定している。これについては、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

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)[7]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[8]（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

[7] https://www.cryptrec.go.jp/topics/cryptrec_201212_listpc.html
[8] 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）」[9]（付録 1 を参照）を策定した。

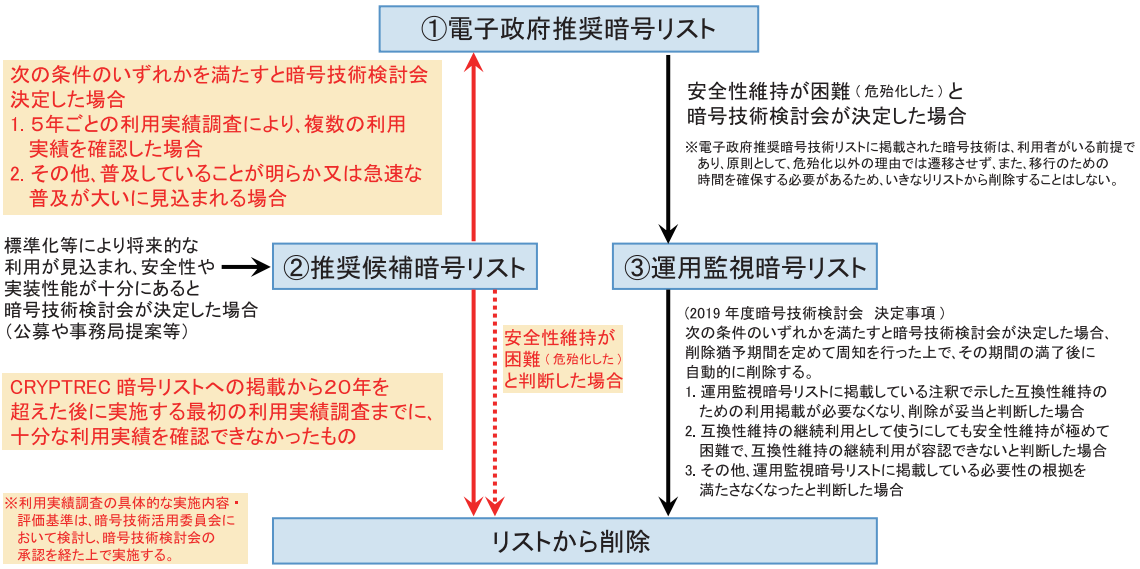

図 1.1：CRYPTREC 暗号リスト移行ルール

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。

③ CRYPTREC 注意喚起レポートの発行：

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

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 2022 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、軽量暗号、及び、高機能暗号に関するガイドラインを作成するため、上記⑤において、

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

を実施することが暗号技術検討会において承認された。

監視に関する基本的な考え方は、CRYPTREC Report 2012 までに記載されていた電子政府推奨暗号リスト[10]掲載の暗号技術に対する考え方[11]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

[10] 2003 年 2 月 20 日に策定されたものを指す。
[11] 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。

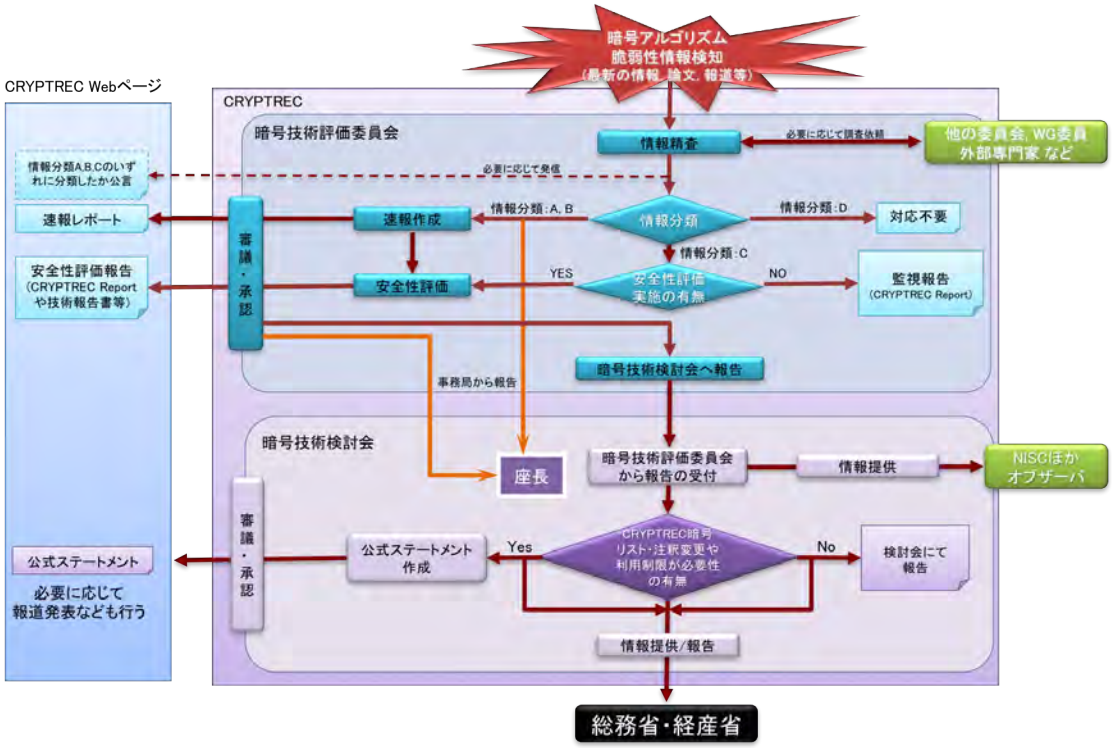

図1.2：暗号アルゴリズムの脆弱性に関する情報発信フロー

[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、2022 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. 共通鍵暗号に関する安全性評価について

2022 年度は、2021 年度に引き続き、共通鍵暗号に関する解読について大きな進展はなかったものの、既存の暗号アルゴリズムへの攻撃について、攻撃に必要な計算量の削減等の進展があった。ここでは主な発表を紹介する。

AES については、ASIACRYPT 2022 にて、MILP モデルを導入することによるブーメラン攻撃の計算量の更新が発表された。特に、AES-192 に対する計算量 2^{124}、データ量 2^{124}、メモリ量 $2^{79.8}$ のブーメラン攻撃が報告されたが、これは 2009 年に報告された既存の裁量な攻撃に対し、計算量を 2^{52} 倍、メモリ量を $2^{72.2}$ 倍に改善するものである。

ChaCha についてはいくつかの解析論文が報告されている。特に、EUROCRYPT 2022 にて、6 ラウンドの ChaCha128 に対する新たな攻撃が報告されたが、これは 2012 年に報告された既存の最良な攻撃に対して、計算量を 1100 万倍以上改善している。

上記のように、2022 年度も AES、ChaCha に対する暗号解析の進展が見られたが、セキュリティマージンはまだ十分にあり、安全性に直ちに影響を与えるものではない。

2.1.2. 公開鍵暗号に関する安全性評価について

公開鍵暗号の一種である RSA については、昨年度に引き続き、部分的に秘密鍵が分かっている場合の新規の素因数分解アルゴリズム（Partial Key Exposure Attack）が、EUROCRYPT 2022、ASIACRYPT 2022 において提案された。

EUROCRYPT 2022 では、CRT-RSA 指数を e、秘密指数を d_p, d_q としたとき、これら d_p, d_q の最上位ビットもしくは最下位ビットを含む 1/3 のビットがわかっている場合の素因数分解が提示された。これにより、e のサイズが $N^{1/12}$ の場合に、最上位ビットもしくは最下位ビットを含む 1/3 がわかっている場合の効率の良い素因数分解を発表した。ASIACRYPT 2022 では、実際のサイドチャネル攻撃のケースも鑑み、秘密指数がブラインディングされているケースに本攻撃が拡張された。本攻撃は部分的であるため、これにより RSA が破られたとは言い難いものの、新しく発見された攻撃手段であるため、今後も動向を注視すべきである。

2.1.3. その他の注視すべき技術動向

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

Round 4 における NIST 4th Standardization Conference において、耐量子計算機暗号形式の候補であった、同種写像を用いた KEM である SIKE はもはや安全ではないということが、SIKE チームから発表された。これは、Castryck と Decru によりクリティカルな攻撃論文が、プレプリントとして発表されたためである。この攻撃によって、同種ベースの暗号形式である SIDH、SIKE、B-SIDH、SIOT は安全ではないことが判明している。その一方、SIDH 署名、CSIDH、SeaSign、CSI-FiSH、OSIDH、SQISign はまだ攻撃が発表されてはいない。これらについては、今後の情勢を注視する必要がある。また、署名形式 Rainbow に対して、ノートパソコン上で攻撃が可能であるという報告が、CRYPTO 2022、PQCrypto 2022 両方で発表された。そして、現在 Round 4 が終わった段階で、耐量子計算機暗号形式の候補は CRYSTALS-KYBER、CRYSTALS-DILITHIUM、FALCON、SPHINCS+ となっている。

2.2. CRYPTREC 暗号リスト改定に関する暗号技術の選定について

2.2.1. 自主取下げに係るメールによる審議と結果

ECDSA、ECDH 及び SC2000 の応募暗号について取り下げの申請があったため、暗号技術評価委員会として表 2.1 の通り対応を行った。

表 2.1：取り下げへの対応

	理由
ECDSA 及び ECDH	取り扱いを応募暗号技術から CRYPTREC が選出した暗号技術に変更し、現状通り、電子政府推奨暗号リストに記載しておくことは妥当であると判断する。仕様書の参照先についても変更無しとする。
SC2000	応募社の判断を尊重し、取り下げを認める。推奨候補暗号リストから当該暗号技術を削除することは妥当であると判断する。

2.2.2. 暗号技術の選定

暗号技術評価委員会では、毎年実施している暗号技術の安全性及び実装に係る監視及び評価[1] に関する活動を通じて、CRYPTREC 暗号リストを維持してきている。第 1 章 1.3

[1] 「CRYPTREC 暗号等の監視」、「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」及び「推奨候補暗号リストへの新規暗号（事務局選出）の追加」の 3 つの活動

節で記した通り、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）を行った。前節の事項以外で、監視活動による変更がないことから、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た。

2.3. 注意喚起レポート

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。

2.4. 推奨候補暗号リストへの新規暗号（事務局選出）の追加

今年度は、推奨候補暗号リストへの新規暗号の追加はなかった。

2.5. 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。

2.6. 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、2020 年度第 2 回暗号技術検討会にて、2016 年度に作成した「CRYPTREC 暗号技術ガイドライン（軽量暗号）」（以下、「2016 年度版ガイドライン」という）を 2023 年度中を目処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その更新方針が承認された。

2.6.1. 軽量暗号に関する技術動向調査

承認された更新方針に従い、今年度は、NIST 軽量暗号プロジェクト（NIST Lightweight Cryptography Project. 以下、「NIST LWC」という）のファイナリスト 10 方式（ASCON, Elephant, GIFT-COFB, Grain-128AEAD, ISAP, PHOTON-Beetle, Romulus, SPARKLE, TinyJAMBU, Xoodyak）を対象とした安全性評価及び実装性能評価を外部評価により実施した。なお、安全性評価に関しては、これら 10 方式に加え、ISO/IEC 標準規格として 29192 シリーズで規格化されている軽量メッセージ認証コードの 1 つである Tsudik's keymode も対象としていた。また、軽量暗号に関わる NIST 公開文書や ISO/IEC などの標準化動向に関わる調査を外部評価により実施した。その外部評価実施内容を報告する。

なお、2023 年 2 月 7 日に、NIST LWC 最終選考結果が発表され ASCON が選ばれた。

実施概要

安全性評価、実装性能評価、標準化動向調査、それぞれについて外部評価により以下

のとおり実施した。

- 安全性評価：NIST LWCファイナリストに選定された10方式とISO/IEC標準規格として承認されたTsudik's keymode の安全性に関する調査及び評価を実施した。
- 実装性能評価：NIST LWCファイナリストに選定された10方式の実装性能（ハードウェア及びソフトウェア）に関する調査及び評価を実施した。
- 標準化動向調査：軽量暗号を取り巻く標準化動向(CAESAR プロジェクト、ISO/IECの軽量暗号関連カテゴリ、NIST LWCなど)の調査を実施した。

2.6.2. 調査結果概要

[安全性評価結果概要]

NIST LWC ファイナリストに選定された 10 方式と ISO/IEC 標準として規格化された Tsudik's keymode の安全性評価について、2022 年 9 月現在における調査結果を表 2.2 の通りまとめた。

表 2.2：安全性評価結果概要

安全性を脅かす攻撃が存在しない方式	特定の場合を除き、 安全性を脅かす方式が存在しない方式
ASCON, Elephant, GIFT-COFB, Grain-128AEAD, ISAP, PHOTON-Beetle, Romulus, SPARKLE, Xoodyak	TinyJAMBU, Tsudik's keymode

TinyJAMBU では、関連鍵設定の場合に現実的な計算量での偽造攻撃が実行可能である。本攻撃が成立するような関連鍵の使用を避けることで TinyJAMBU の安全性を確保できることを確認した。

Tsudik's keymode では、使用するハッシュ関数が伸長攻撃と呼ばれる攻撃を許す場合に偽造攻撃が実行可能となるという既知の脆弱性が存在する。伸長攻撃が実行不可能なハッシュ関数を使用することで Tsudik's keymode の安全性を確保できることを確認した。

[実装性能評価結果概要]

それぞれの方式に関する現時点での実装性能を確認した。

- ハードウェア実装：回路面積とスループット性能に着目して評価した。例えば、Xilinx社のArtix-7上では、TinyJAMBUの回路面積が小さいこと、SPARKLEは比較的面積コストが大きくなることなどを確認した。

- ソフトウェア実装：レイテンシ、コードサイズ、RAMサイズなどに着目し評価した。例えば、低リソースプラットフォーム（Arm Cortex-M0）上では、Elephantが最もレイテンシが高く、TinyJAMBU、Xoodyak、ASCON、SPARKLEが低レイテンシであることが分かった。コートサイズは、ASCONが最も大きく、他の候補暗号方式には大きな差は見られなかった。RAMの使用量は、コンパイル時の静的なメモリサイズのレポートから、どのアルゴリズムも約 1kByte程度であった。

［標準化動向調査結果概要］

CAESAR プロジェクト、ISO/IEC の軽量暗号関連カテゴリ、NIST LWC などの状況を調査し、まとめた。調査結果により、軽量暗号をとりまく現状を確認した。例えば、2016年度版ガイドラインに掲載されている SIMON と SPECK については、ISO/IEC の軽量暗号のカテゴリで議論されていたが、結果として軽量暗号としては ISO/IEC 標準規格として承認されず、自動認識・データキャプチャ技術に関する仕様で利用可能な軽量暗号方式として規格化されていることを確認した。

また、評価指標に関して、安全性評価については、提案方式の設計根拠が十分に提示されない場合に第三者による評価が十分に行えないと判断され、評価対象から外されるなどの事例があった。実装性能評価については、従来論文ごとに異なる環境や測定シナリオで示されることが多くあったが、近年は AES-GCM や SHA-256 など広く世界で利用されているアルゴリズムとの比較などにより統一的な測定フレームワークを用いて実施することが一般化されてきていることが分かった。

2.6.3. 外部評価報告書に対する暗号技術評価委員会の見解

実施した外部評価報告書は、今年度に目的としていた調査対象の暗号方式に対して、安全性・実装性能・標準化動向の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。

2.7. 学会等参加状況

国内外の学術会議に参加し、暗号解読技術に関する情報収集を実施した。参加した国際会議は、表2.3に示す通りである。

表 2.3：国際会議への参加状況

学会名・会議名		開催国・都市	期間
EUROCRYPT 2022	The 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques	ノルウェー・トロンハイム (Hybrid Conference)	2022 年 5 月 30 日～6 月 3 日
CRYPTO 2022	The 42nd Annual International Cryptology Conference	アメリカ合衆国・サンタバーバラ (Hybrid Conference)	2022 年 8 月 13 日～8 月 18 日
FDTC 2022	Fault Diagnosis and Tolerance in Cryptography	(Virtual Conference)	2022 年 9 月 16 日
CHES 2022	Cryptographic Hardware and Embedded Systems	ベルギー・ルーヴェン (Hybrid Conference(	2022 年 9 月 18 日～9 月 21 日
PQCrypto 2022	Post-Quantum Cryptography The 13th International Workshop	(Virtual Conference)	2022 年 9 月 28 日～9 月 30 日
TCC 2022	Theory of Cryptography The 20th International Conference	アメリカ合衆国・シカゴ (Hybrid Conference)	2022 年 11 月 7 日～11 月 10 日
NIST 4th Standardization	Fourth PQC Standardization Conference	(Virtual Conference)	2022 年 11 月 29 日～12 月 1 日
ASIACRYPT 2022	The 28th International Conference on the Theory and Application of Cryptology and Information Security	台湾・台北 (Hybrid Conference)	2022 年 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。

2.7.1. 共通鍵暗号の解読技術

・Revisiting Related-Key Boomerang Attacks on AES Using Computer-Aided Tool [ASIACRYPT 2022]

Patrick Derbez, Marie Euler, Pierre-Alain Fouque, Phuong Hoa Nguyen

近年、ブロック暗号のブーメラン識別子やブーメラン攻撃を自動的に探索するために、いくつかの MILP モデルが導入されている。しかし、これらはキースケジュールが線形

である場合にのみ使用可能である。ここでは、AES のような非線形のキースケジュールを有するブロック暗号に対して、新しいモデルを導入する。このモデルはより複雑であり、網羅的な探索には時間がかかりすぎる。しかしながら、ソルバーにいくつかのヒントを追加することで、計算量 2^{124}、データ量 2^{124}、メモリ量 $2^{79.8}$ で AES-192 に対する現在最高の関連鍵ブーメラン攻撃が実行できることを示す。これは、ASIACRYPT 2009 で Biryukov と Hovratovich による攻撃の計算量（それぞれ 2^{176}、2^{123}、2^{152}）よりも優れている。特に、計算量とメモリ量において大きな改善を与えており、これは暗号解読における MILP の威力を示している。

・Synthesizing Quantum Circuits of AES with Lower T-depth and Less Qubits [ASIACRYPT 2022]

Zhenyu Huang, Siwei Sun

量子アルゴリズムによる暗号解読に必要な資源を正確に見積もるためには、量子アルゴリズムを基本的な量子ゲートで構成される量子回路に帰着する必要がある。本研究では、Grover と Simon のアルゴリズムに基づく量子攻撃でよく用いられる反復型共通鍵暗号の量子オラクルを実装する回路について、いくつかの汎用的な合成技術と最適化技術が提案された。まず、ブロック暗号のラウンド関数を in-place に実装するための一般的な構造を提案する。次に、線形および非線形な暗号構成要素の効率的な量子回路を合成するための新しい技術が導入される。これらの技術を AES に適用し、深さ-幅のトレードオフ（depth-width tradeoff）の戦略が系統的に調べられる。その過程で、AES の S-box の古典的回路に関する新しい知見に基づいて、証明可能な最小の T-depth を持つ量子回路が導出されている。その結果、AES の量子回路の実装に必要な T-depth と幅（量子ビット数）が大幅に削減された。著者らの回路と EUROCRYPT 2020 で提案された回路と比較すると、幅を増やさずに T-depth を 60 から 40 に、あるいは幅をわずかに増やして 30 に減らすことに成功している。これらの回路は、Microsoft Q#で実装されており、ソースコードも公開されている。ASIACRYPT 2020 で提案された回路と比較すると、著者ら回路の 1 つは幅が 512 から 371 に減少し、同時に Toffoli-depth が 2016 から 1558 に減少していることが確認されている。また実際、深さを増やす代わりに、幅を 270 に減らすことができる。さらに、深さと幅のトレードオフの全範囲が提供され、AES の量子回路の合成と最適化における新記録も樹立されている。

・Revamped Differential-Linear Cryptanalysis on Reduced Round ChaCha [EUROCRYPT 2022]

Sabyasachi Dey, Hirendra Kumar Garai, Santanu Sarkar, Nitin Kumar Sharma

本論文では、ChaCha における既存の差分線形攻撃に対するいくつかの改良点を提供する。ChaCha は 20 ラウンドを持つストリーム暗号である。CRYPTO 2020 で、Beierle

らは適切なペアが選択された場合、3.5 ラウンド目に差分が発生することを観測している。彼らはこの差分を用いて攻撃の改良を試みたが、適切なペアを得るためには平均で 2^5 回の反復が必要であることを示した。この方法論に関し、リスト化（listing）の助けを借りて、適切なペアを見つけるための技術を提供する。また、Probabilistic Neutral Bits (PNB) 構築の戦略的改善、計算量見積の修正、そして 2 つの入出力ペアを用いた代替的な攻撃方法も提供する。これらの技術を用いて計算量を改善する。具体的には、Beierle らが示した 7 ラウンドの ChaCha256 に対する攻撃の計算量を $2^{230.86}$ から $2^{221.95}$ に減少させた。また、6 ラウンドの ChaCha128 に対する既存の計算量（Shi et al: ICISC 2012）を 1100 万倍以上改善するとともに、6.5 ラウンドの ChaCha128 に対する史上初の攻撃で計算量 $2^{123.04}$ を実現した。

・Rotational Differential-Linear Distinguishers of ARX Ciphers with Arbitrary Output Linear Masks [CRYPTO 2022]

Zhongfeng Niu, Siwei Sun, Yunwen Liu, Chao Li

EUROCRYPT 2021 で提案された回転差分線形攻撃は、差分線形攻撃の差分部分を回転差分に置き換えて一般化したものである。EUROCRYPT 2021 では、Liu らが Morawiecki らの手法（FSE 2013）に基づき、出力線形マスクが単位ベクトルである特殊なケースについて、回転差分線形相関を評価する手法を発表した。この手法により、Friet、Xoodoo、Alzette に対して、出力線形マスクが単位ベクトルである強力な（回転）差分線形識別子がいくつか発見された。しかし、任意の出力マスクに対する回転差分線形相関をどのように計算するかは未解決であった。

本研究では、この未解決問題の一部を解決している。任意の出力線形マスクに対する算術加算の（回転）差分線形相関を計算する効率的なアルゴリズムを提示し、それを基に ARX 暗号の（回転）差分線形相関を評価する手法が導出された。本技術を Alzette、SipHash、Chacha、Speck に適用した結果、決定論的なものを含め、大幅に改善された（回転）差分線形識別子が確認された。本研究の成果は全て実用的であり、実験的に検証され、手法の有効性が確認された。さらに、FSE 2008、FSE 2016、CRYPTO 2020 で採用された ChaCha に対する実験的な識別子を説明することを試みている。予測された相関は実験的な相関に近いものであった。

・Latin Dances Reloaded: Improved Cryptanalysis against Salsa and ChaCha, and the proposal of Forró [ASIACRYPT 2022]

Murilo Coutinho, Iago Passos, Juan Grados, Fábio de Mendonça, Rafael Timóteo, Fábio Borges

本論文では、ARX 暗号、特にストリーム暗号の Salsa/ChaCha ファミリーに対する 4 つの主要な貢献を紹介する。

ChaCha に対する差分線形識別子の改善について提案する。この提案に向けて、アルゴリズムをより単純なサブラウンドの観点から見ることにより、線形近似の導出にアプローチする新しい方法を提案する。このアイデアを使用すると、既存研究で得られた全ての線形近似を 3 つの単純なルールから導き出すことが可能であることを示す。さらに、もう 1 つのルールを追加することで、EUROCRYPT 2021 で Coutinho と Souza が提案した線形近似を改善できることを示す。

Salsa に対する攻撃を改善するため、双方向線形拡張（BLE: Bidirectional Linear Expansions）と呼ばれる技術を提案する。既存研究では、ラウンドに前進する線形拡張のみを検討していたが、BLE では 1 ビットを前進と後退の両方向に拡張することが検討されている。BLE を適用して、7 ラウンドと 8 ラウンドの Salsa に対する最初の差分線形識別子を提案するとともに、8 ラウンドの Salsa に対する PNB を用いた鍵回復攻撃を改善する。

これらの暗号に対する暗号解析の研究から得られた全ての知識を用いて、ラウンドごとの拡散と暗号解析への耐性を向上させるためのいくつかの修正を提案し、新しいストリーム暗号 Forró を完成させた。これにより、安全性を維持したままラウンド数を減らすことができ、多くのプラットフォーム、特に制約のあるデバイスにおいて、より高速な暗号を実現すること可能となる。

さらに著者らは、複数の GPU を備えた高性能環境で使用可能な Salsa、ChaCha、Forró のための新しい暗号解析ツールを開発した。このツールを CryptDances と呼ぶ。CryptDances では、差分相関の計算、ChaCha の新しい線形近似の自動導出、PNB 攻撃の計算量の見積の自動化などが可能になっている。

2.7.2. 公開鍵暗号の解読技術

・Approximate Divisor Multiples - Factoring with Only a Third of the Secret CRT-Exponents [EUROCRYPT 2022]

Alexander May, Julian Nowakowski, Santanu Sarkar

本論文は、CRT-RSA の秘密指数d_p, d_qで、公開指数eが小さい場合の部分鍵公開攻撃について研究している。eが定数である場合、d_p, d_qのうち 1 つのビットの半分を知ることで、Coppersmith の有名な「factoring with a hint」の結果によって RSA 剰余Nを因子分解できることが知られている。この設定をeが定数でない場合に拡張する。

少し意外な結論として、eのサイズが $N^{1/12}$ である RSA が部分鍵公開攻撃に対して最も弱いということが、本論文の攻撃によって示された。これは、最上位ビット（MSB）または最下位ビット（LSB）のいずれかを知っているd_p, d_qの両ビットの 3 分の 1 があれば、多項式時間でNを因数分解できるためである。

$ed_p = 1 + k(p-1)$, $ed_q = 1 + \ell(q-1)$とせよ。技術的には、著者らはNの素因数

分解を二つの新しいアプローチで求めている。第一のステップでは、kとℓを多項式時間で復元する。これは、MSB の場合は完全に初等的に、LSB の場合は Coppersmith の格子に基づく方法を用いて実現される。これにより、求められたkを用いて、kpを法とする一変数多項式の根を計算することで、Nの素因数分解を得ることができる。これは、Howgrave-Graham の approximate divisor アルゴリズムの、Nの未知の約数pの既知の倍数kに対する approximate divisor multiples の場合への拡張と見なすことができる。approximate divisor multiples のポイントは、多項式時間で復元可能な未知数が、倍数kの大きさに対して線形に増加することである。

この部分鍵公開攻撃は、MSB がわかっている場合は厳密である一方、LSB の場合は標準的な Coppersmith タイプのヒューリスティックに依存する。このヒューリスティックを実験的に検証することにより、実際には小さな格子寸法で既に漸近的な境界値に到達することを示すことで、この部分鍵公開攻撃の実用性も示されている。

・A Third is All You Need: Extended Partial Key Exposure Attack on CRT-RSA with Additive Exponent Blinding [ASIACRYPT 2022]

Yuanyuan Zhou, Joop van de Pol, Yu Yu, François-Xavier Standaert

EUROCRYPT 2022 において、May らは CRT-RSA に対する部分鍵公開（PKE）攻撃を提案し、公開指数$e \approx N\^\{1/12\}$ に対する秘密指数 d_p および d_q の最上位ビットら（MSBs）の 1/3、または最下位ビットら（LSBs）の 1/3 どちらかだけを知って、 N を効率よく素因数分解した。実際には、PKE 攻撃はこれらの指数のサイドチャネル漏洩に依存している。CRT-RSA のサイドチャネル耐性実装では、未知のランダムなブラインド係数 r_p ，r_q における加法的なブラインド指数 $d'_p = d_p + r_p(p-1)$, $d'_q = d_q + r_q(q-1)$ を用いているため、PKE 攻撃はより困難なものになることが多い。

以上のことの背景に、本論文は、May らの PKE 攻撃を加法的なブラインド指数の CRT-RSA に拡張している。この場合、ブラインドされた CRT 指数 d_p^π と d_q^π の既知の MSB または LSB のみを使用して秘密鍵全体を復元することができる。$r_p e \in (0, N^{1/4})$ を許容する一方で、著者らが拡張した PKE 攻撃は、$r_p e \approx N^{1/12}$ の時理想的に働く。このケースでは、ブラインドされた CRT 指数 d'_p と d'_q の MSB もしくは LSB の 1/3 から全ての秘密鍵が復元可能である。著者らの拡張した PKE 攻撃は、May らによる以下の 2 ステップのアプローチに準拠している：第一ステップで鍵に依存する定数 k'（$ed'_p = 1 + k'(p-1)$, $ed'_q = 1 + l'(q-1)$ ）を計算し、第二ステップで $k'p$ を法とする一変数多項式の根を計算することでNを素因数分解する。本論文では、この手法を以下のように拡張している。MSB の場合では、第一ステップにおいて、$k'l'$の値を一つ推定した後k'を因数分解により計算する方法と、$k'l'_1, \ldots, k'l'_z$という複数の推定値からk'を GCD により確率的に計算するという、2 つのオプションを提案している。LSB の場合では、第二ステップで現れる差分一変数多項式を構成するアプローチが拡張されている。形式的な分析によって、

本手法における LSB 攻撃は通常の Coppersmith タイプの仮定の下、多項式時間で機能することがわかっている。一方、本手法における MSB 攻撃は、簡約された入力サイズに対し劣指数時間を要する（問題が$e^2 r_p r_q \approx N^{1/6}$のサイズの素因数分解に帰着される）か、新しいヒューリスティックな仮定の下で確率的多項式時間で機能する。最も一般的な鍵サイズ（1024 ビット、2048 ビット、3072 ビット）とブラインド因数のサイズ（32 ビット、64 ビット、128 ビット）の設定の下で、著者らの実験を行い、この Coppersmith タイプの仮定と、彼らの新たなヒューリスティックな仮定の両方が尤もらしい事を確認している。

以上の攻撃は、128 ビットのブラインド指数が存在する場合の CRT-RSA に対して、初めて実験的な有効性が確認された PKE 攻撃であると著者らは主張している。さらに、Montgomery Ladder 指数 CRT 実装を対象としたリアルなサイドチャネル部分鍵漏洩に対して、提案された攻撃の応用実験も行っている。

2.7.3. その他の暗号技術の解読技術

・Breaking Rainbow Takes a Weekend on a Laptop [CRYPTO 2022,PQCrypto 2022]

Ward Beullens

本研究で、NIST のポスト量子暗号標準化プロジェクトで最終選考に残った 3 つの署名方式の 1 つである Rainbow 署名方式に対する新しい鍵回復攻撃が導入された。この新しい攻撃は、NIST に提出されたすべてのパラメータセットに対して既知の攻撃を上回り、SL 1 パラメータに対する鍵回復を実用している。具体的には、第二ラウンドに提出された SL 1 パラメータの Rainbow 公開鍵が与えられた場合、提案された攻撃は標準的なノートパソコンで平均 53 時間（1 週末）の計算時間で対応する秘密鍵を返す。

2.8. 委員会開催記録

2022 年度に暗号技術評価委員会は、表 2.4 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 2.4：暗号技術評価委員会の開催状況

回	開催日	議案
メール審議	2022 年 6 月 1－7 日	暗号技術調査ワーキンググループ（高機能暗号）の活動計画案の審議
第 1 回	2022 年 7 月 26 日	● 暗号技術評価委員会活動計画の具体的な進め方についての審議 ● 暗号技術調査ワーキンググループ（耐量子計算機暗号）の活動計画案の審議 ● 暗号技術調査ワーキンググループ（高機能暗号）の活動計画案の報告 ● 外部評価（軽量暗号に関するガイドライン係る技術動向調査）実施についての審議 ● 監視状況報告
メール審議	2023 年 1 月 30 日－2 月 10 日	● 自主取下げに係るメールによる審議
第 2 回	2023 月 2 月 27 日	● 自主取下げに係る電子メールによる審議内容と結果の報告 ● 暗号技術調査ワーキンググループ（耐量子計算機暗号）の活動内容の報告 ● 暗号技術調査ワーキンググループ（高機能暗号）の活動内容の報告 ● 軽量暗号ガイドラインに係る技術動向調査結果の報告 ● 監視状況報告 ● CRYPTREC Report 2022 作成について ● CRYPTRECシンポジウム開催について

2.9. 暗号技術調査ワーキンググループ開催記録

2022 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 2.5 の通り 2 回開催された。

表 2.5：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	2022 年 9 月 26 日	● 暗号技術評価委員会活動計画及び暗号技術調査ワーキンググループ（耐量子計算機暗号）の活動計画の報告 ● 耐量子計算機暗号の研究動向調査報告書の執筆内容に関する中間報告
第 2 回	2023 年 1 月 30 日	● 耐量子計算機暗号の研究動向調査報告書及びガイドラインの執筆内容に関する報告及び審議 ● 「素因数分解の困難性に関する計算量評価」、「楕円曲線上の離散対数計算の困難性に関する計算量評価」の予測図に関する審議 ● 2022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）活動報告案に関する審議

また、暗号技術調査ワーキンググループ(高機能暗号暗号)は、表 2.6 の通り 3 回開催された。各会合の開催日及び主な議題は以下の通りである。

表 2.6：暗号技術調査ワーキンググループ(高機能暗号暗号)の開催状況

回	開催日	議案
第 1 回	2022 年 6 月 15 日	● 暗号技術評価委員会活動計画及び暗号技術調査ワーキンググループ（高機能暗号）の活動計画の報告 ● 高機能暗号の実用事例に関するヒアリング ● 高機能暗号ガイドラインの執筆に関する作業方針と作業分担についての審議
第 2 回	2022 年 11 月 9 日	● 高機能暗号技術に関する現状調査に関する報告 ● 高機能暗号の実用事例に関するヒアリング ● 高機能暗号ガイドラインの執筆内容に関する中間報告
第 3 回	2023 年 2 月 10 日	● 高機能暗号ガイドラインの執筆内容に関する報告及び審議 ● 2022年度暗号技術調査WG（高機能暗号）活動報告案に関する審議

第３章　暗号技術調査ワーキンググループの活動

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

3.1.　暗号技術調査ワーキンググループ（耐量子計算機暗号）

3.1.1. 活動報告の概要

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

2022 年度第 1 回暗号技術評価委員会において、2021 年度と同様に、PQC WG において下記 2 点について実施することが承認された。

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

これらの成果（3.1.4.～3.1.5.節）は 2022 年度第 2 回暗号技術評価委員会(2023 年 2 月 27 日開催)にて報告され、了承された[1][2]。

3.1.2. 活動スケジュール

【2021 年度のスケジュール】

・2021 年 9 月 7 日 第 1 回 耐量子計算機暗号 WG

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

[1] 耐量子計算機暗号の研究動向調査報告書（CRYPTREC TR-2001-2022）
https://www.cryptrec.go.jp/report/cryptrec-tr-2001-2022.pdf

[2] CRYPTREC 暗号技術ガイドライン（耐量子計算機暗号）（CRYPTREC GL-2004-2022）
https://www.cryptrec.go.jp/report/cryptrec-gl-2004-2022.pdf

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

【2022 年度のスケジュール】
・2022 年 9 月 26 日 第 1 回 耐量子計算機暗号 WG
調査報告書及びガイドラインの執筆に関する中間報告、2022 年度第 2 回 PQC WG までのスケジュールに関する審議
・2023 年 1 月 30 日　第 2 回 耐量子計算機暗号 WG
調査報告書及びガイドラインの執筆に関する最終報告、記載内容の確認、修正案についての議論。公開までのスケジュールに関する審議を行い、調査報告書及びガイドラインの発行日を 2023 年 3 月、Web 公開を 4 月とすることを決定
「素因数分解の困難性に関する計算量評価」、「楕円曲線上の離散対数計算の困難性に関する計算量評価」の予測図に関する説明文の修正に関する審議、予測図に関する審議

3.1.3. 委員構成（敬称略）

主査：國廣 昇　　(筑波大学)
委員：青木 和麻呂　　(文教大学)
委員：伊藤 忠彦　　(セコム株式会社)
委員：草川 恵太　　(日本電信電話株式会社)
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：廣瀬 勝一　　(福井大学)
委員：安田 貴徳　　(岡山理科大学)
委員：安田 雅哉　　(立教大学)

3.1.4. 耐量子計算機暗号に関するガイドラインの作成方針

<u>ガイドライン及び調査報告書の作成</u>

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

ガイドライン及び調査報告書に記載する暗号方式の選定基準及び候補について

主要な耐量子計算機暗号方式（NIST PQC 標準化への提案方式等）を記載するが、対象となる暗号方式は執筆担当委員が選定する。

記載すべき項目及び章立て

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

- iii 章以降：章内部の詳細な構成（A 章の場合）

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

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

「素因数分解の困難性に関する計算量評価」、「楕円曲線上の離散対数計算の困難性に関する計算 量評価」の予測図（以下単に「予測図」という）は公開鍵暗号方式のセキュリティパラメータの選択について検討を行うため、2006 年度に設置された暗号技術調査 WG（公開鍵暗号）において作成された。当時、米国 NIST は「NIST SP 800-57 Part 1 (Revised)(May,2006)」において暗号技術の鍵サイズに関して「80 ビットセキュリティの利用期限を 2010 年まで」と推奨していた。現在では「NIST SP 800-57 Part 1 (Revision 5)(May,2020)」において「112 ビットセキュリティの利用期限を 2030 年まで」と推奨している。これまでの暗号の鍵長の推奨値は、いわゆるムーアの法則(集積回路上のトランジスタ数が 18 ヶ月毎に 2 倍になる)を主な根拠として設定されてきた。ところが、近年、計算機の性能向上は以前と比べて鈍化してきている。

これらの状況を踏まえ、2019 年度第 2 回暗号技術評価委員会において、今後の予測図の取扱いについて対応方針を決定し、この方針は 2020 年度第 1 回暗号技術検討会にて了承された。

説明文の更新について

今後の予測図の取り扱いに係る説明文を読み易さの観点から以下の表のとおり更新した。

【現状】

〈今後の予測図の取扱い〉

(1) 予測図を従来通り、いわゆるムーアの法則を仮定して外挿線を年度末からプラス20年後まで直線で引き、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当面の間更新していく。なお、予測図は各国・国際標準化機関等により示されている主要な暗号技術の安全性基準と比較すると、より現状に則した評価であり、危殆化時期がそれらよりも先に延びるものとなっている。

〈今後の公開鍵暗号のパラメータ選択〉

(2) 公開鍵暗号のパラメータ選択に関する対応方針については、安全性以外にも相互接続性など、運用上の観点もあるため、今後は、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。

【修正案】

＜今後の予測図の取り扱い＞

(1) ~~予測図を従来通り、~~いわゆるムーアの法則を仮定して外挿線を年度末からプラス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。~~なお、予測図は各国・国際標準化機関等により示されている主要な暗号技術の安全性基準と比較すると、より現状に即した評価であり、危殆化時期がそれらよりも先に延びるものとなっている。~~

〈今後の公開鍵暗号のパラメータ選択〉

(2) 公開鍵暗号のパラメータ選択に関する対応方針については、安全性以外にも相互接続性など、運用上の観点もあるため、~~今後は、~~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。

予測図の更新について

素因数分解問題の困難性および楕円曲線上の離散対数問題の困難性に関する計算量評価に大幅な進展はなかったため、TOP500.org における 2022 年 6 月・11 月のベンチマーク結果を追加して予測図の更新を行った(図 3.1、3.2)。

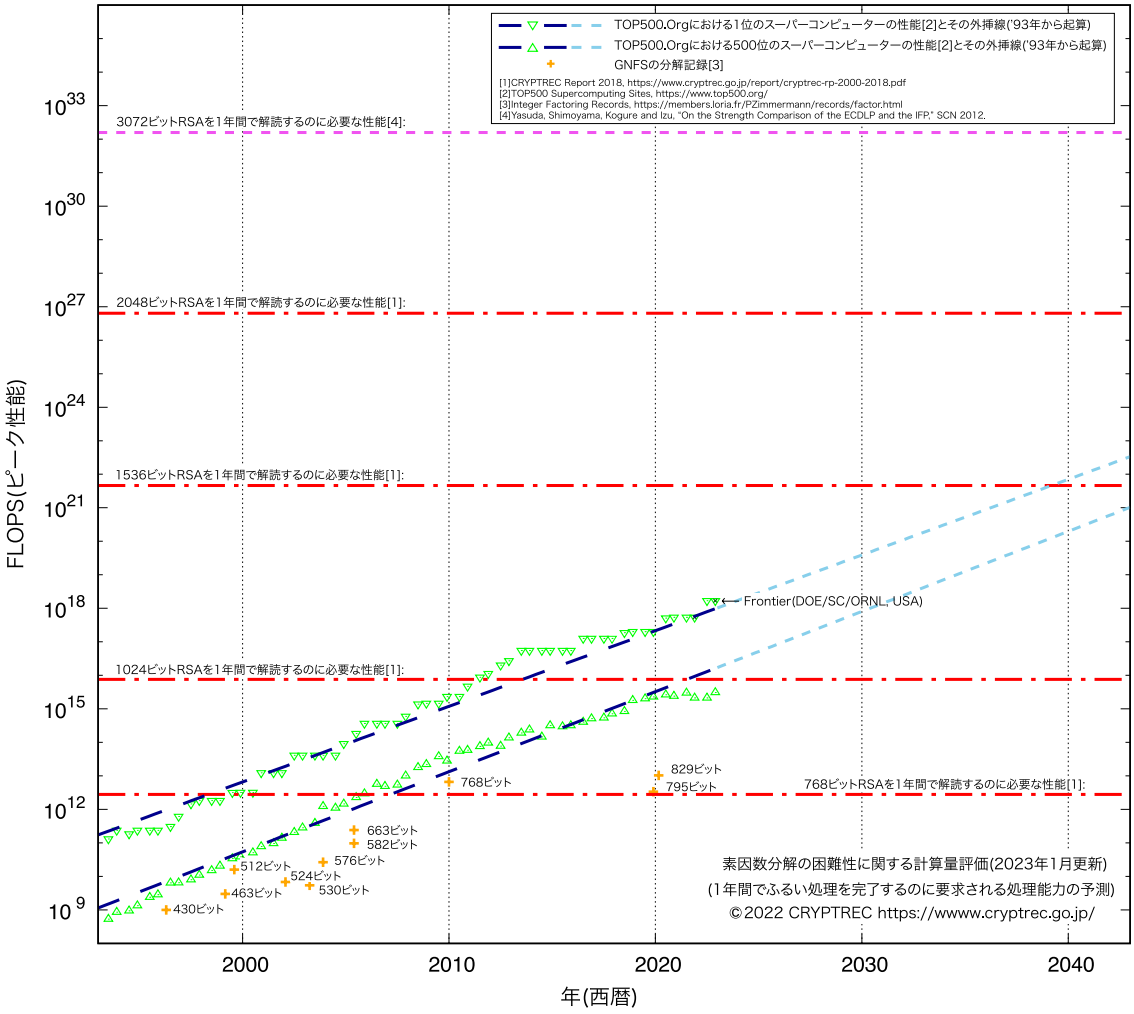

図 3.1：素因数分解の困難性に関する計算量評価(2023 年 1 月更新)

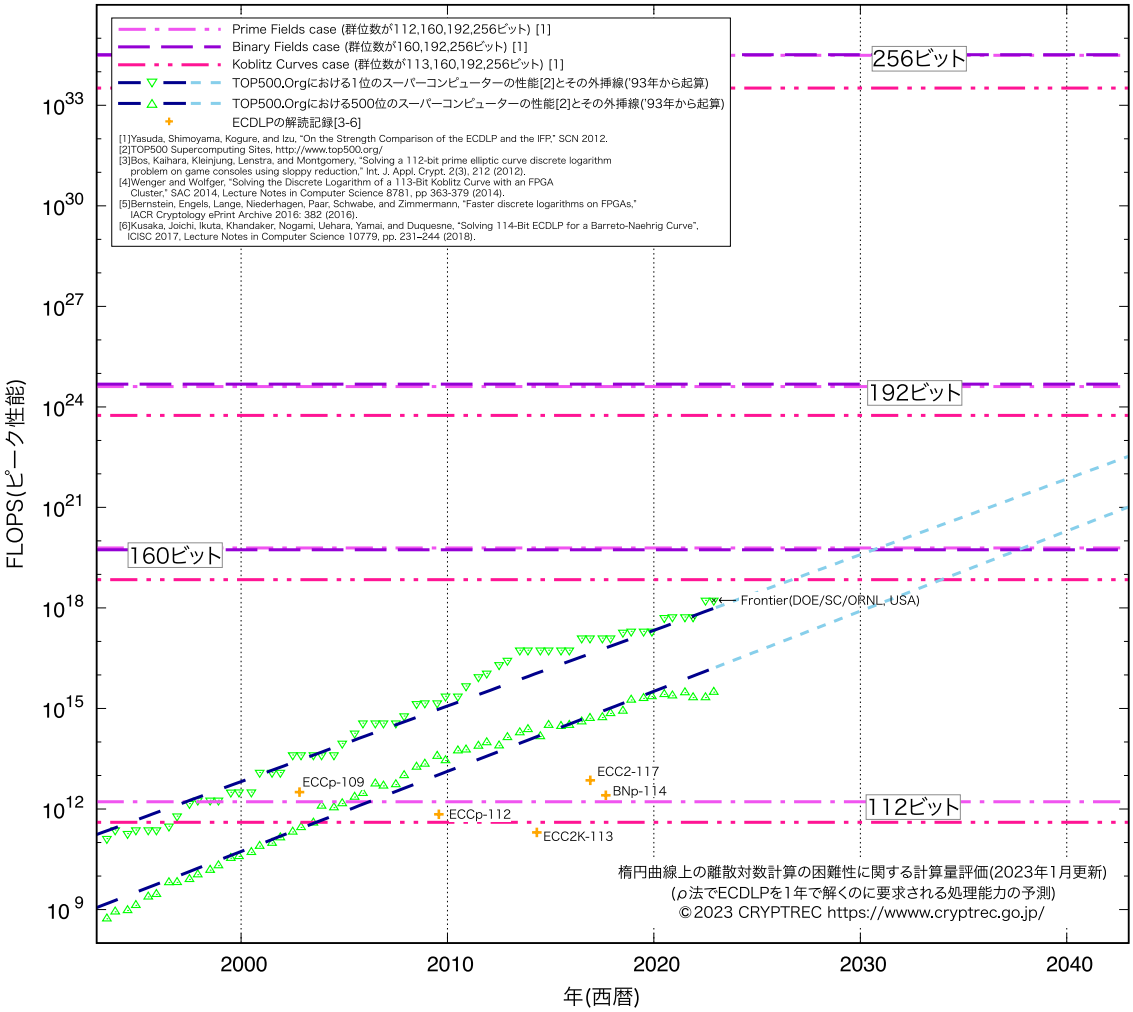

図 3.2：楕円曲線上の離散対数計算の困難性に関する計算量評価(2023 年 1 月更新)

3.2　暗号技術調査ワーキンググループ（高機能暗号）

3.2.1　活動報告の概要

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

そして、2021 年度暗号技術評価委員会において、2021 年度の高機能暗号 WG の活動として下記 4 点について実施する活動計画が承認された。

(1) 2021-2022 年度において高機能暗号ガイドライン[3]を作成すること
(2) 高機能暗号のスコープの明確化
(3) 高機能暗号技術に関する現状調査
(4) 高機能暗号のアプリケーションに関する調査

3.2.2. 活動スケジュール

【2021 年度のスケジュール】

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

【2022 年度のスケジュール】

・2022 年 6 月 15 日　第 1 回高機能暗号 WG
高機能暗号の技術内容に関する執筆分担の議論、アプリケーションについて NEC 様へのヒアリング

・2022 年 11 月 9 日　第 2 回高機能暗号 WG
ガイドライン執筆状況の中間報告および内容確認・議論、アプリケーションについて三菱電機様へのヒアリング

・2023 年 2 月 10 日　第 3 回高機能暗号 WG
高機能暗号ガイドライン内容の最終確認

・第 3 回 WG でのコメント修正版を 2 月 17 日に完成し、WG でのガイドライン完成版とした

[3] CRYPTREC 暗号技術ガイドライン（高機能暗号）（CRYPTREC GL-2005-2022）
https://www.cryptrec.go.jp/report/cryptrec-gl-2005-2022.pdf

3.2.3　委員構成（敬称略）

主査：四方 順司　　(横浜国立大学)
委員：岩本 貢　　(電気通信大学)
委員：大原 一真　　(国立研究開発法人産業技術総合研究所)
委員：勝又 秀一　　(PQShield Ltd. /国立研究開発法人産業技術総合研究所)
委員：金岡 晃　　(東邦大学)
委員：川原 祐人　　(日本電信電話株式会社)
委員：国井 裕樹　　(セコム株式会社)
委員：須賀 祐治　　(株式会社インターネットイニシアティブ)
委員：鈴木 幸太郎　　(豊橋技術科学大学)
委員：花岡 悟一郎　　(国立研究開発法人産業技術総合研究所)
委員：外園 康智　　(野村総合研究所)
委員：山田 翔太　　(国立研究開発法人産業技術総合研究所)
委員：米山 一樹　　(茨城大学)
委員：渡邉 洋平　　(電気通信大学)

3.2.4　高機能暗号のスコープの明確化

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

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

- 守秘
- 認証・署名
- その他

の 3 つに分類した。そして、調査すべき高機能暗号の対象を

- 守秘
  - ID ベース暗号、属性ベース暗号、放送型暗号、しきい値暗号、準同型暗号、プロキシ再暗号化
- 認証・署名
  - ID ベース署名、属性ベース署名、集約署名・MAC・マルチ署名、グループ署名、リング署名、しきい値署名
- その他

- マルチパーティ計算－秘密分散ベース、マルチパーティ計算－Garbled Circuit ベース、ゼロ知識証明、検索可能暗号、Private Information Retrieval、Oblivious RAM

の 18 項目とした。

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

目次案

1. はじめに
2. 高機能暗号技術とその活用法
   - 2.1 高機能暗号とは
   - 2.2 高機能暗号の種類と分類
   - 2.3 高機能暗号はどこに使えるか、その有用性
   - 2.4 高機能暗号の活用例と効果
     - 2.4.1 守秘関連の活用事例
     - 2.4.2 認証・署名関連の活用事例
     - 2.4.3 その他の高機能暗号の活用事例
3. 主な高機能暗号技術のアルゴリズム・プロトコルとその性能
   - 3.1 守秘
     - 3.1.1 ID ベース暗号
     - 3.1.2 属性ベース暗号
     - 3.1.3 放送型暗号
     - 3.1.4 準同型暗号
     - 3.1.5 プロキシ再暗号化
   - 3.2 認証・署名
     - 3.2.1 属性ベース署名
     - 3.2.2 集約署名、MAC、マルチ署名
     - 3.2.3 グループ署名
     - 3.2.4 リング署名
     - 3.2.5 しきい値署名
   - 3.3 その他
     - 3.3.1 マルチパーティ計算～秘密分散ベース～
     - 3.3.2 マルチパーティ計算～Garbled Circuit ベース～
     - 3.3.3 ゼロ知識証明
     - 3.3.4 検索可能暗号
     - 3.3.5 Private Information Retrieval (PIR)
     - 3.3.6 Oblivious RAM (ORAM)
4. おわりに

3.2.5 高機能暗号に関する現状調査

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

第 1 回高機能暗号 WG の中の、高機能暗号のスコープの明確化により定められた、3 分

類 18 項目の暗号技術に対し、“技術”について調査することとした。調査は各委員が分担して行うこととした。調査内容は、第 2 回、第 3 回高機能暗号 WG において報告された。

【2021 年度のスケジュール】

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

【2022 年度のスケジュール】

- 2022 年 6 月 15 日　第 1 回高機能暗号 WG
  高機能暗号技術に関する現状調査（詳細版）について分担を議論
  高機能暗号のアプリケーションに関する現状調査（詳細版）について分担を議論
- 2022 年 11 月 9 日　第 2 回高機能暗号 WG
  現状調査・アプリケーションに関する中間報告
- 2023 年 2 月 10 日　第 3 回高機能暗号 WG
  調査内容をガイドラインに反映

3.2.6　高機能暗号のアプリケーションに関するヒアリング調査

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

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

また、エンドユーザのヒアリングの候補を以下の 4 件に決定した。

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

2021 年度第 3 回 WG（2022 年 2 月 8 日）において、秘密計算の利用事例を NEC 様に、検索可能暗号、属性ベース暗号の利用事例を三菱電機様にヒアリング行うことを決定した。

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

【2021 年度のスケジュール】

- 2021 年 8 月 3 日　第 1 回高機能暗号 WG
  高機能暗号のアプリケーションに関する現状調査について、作業方針・分担を議論
  高機能暗号のアプリケーションについて、エンドユーザのヒアリング先の検討
- 2021 年 12 月 8 日　第 2 回高機能暗号 WG
  高機能暗号のアプリケーションに関する現状調査について中間報告
  ヒアリングに関する中間報告
- 2022 年 2 月 8 日　第 3 回高機能暗号 WG
  ヒアリング先に関する候補者選定
  ヒアリング方法について決定
  高機能暗号ガイドラインの執筆方針に関する議論
- 2022 年 2 月 28 日　NEC 様とのオンライン打ち合わせによりヒアリングを快諾

【2022 年度のスケジュール】

- 2022 年 4 月 13 日　三菱電機とのオンライン打ち合わせによりヒアリングを快諾
- 2022 年 6 月 15 日　NEC 様ヒアリング
  個々のデータのプライバシを強化するために、秘密計算を利用する事例、ゲノム解析、創薬等の報告をいただき、質疑を行った。

・ 2022 年 11 月 9 日 三菱電機様ヒアリング
企業が持つデータベースのデータを共有するにあたり、パブリッククラウドを使用してコストを削減しつつ、不要なデータが他企業に渡る（漏洩する）ことを防ぐために、検索可能暗号や属性ベース暗号を利用する事例、組織内文書管理、委託作業等の報告をいただき、質疑を行った。

3.2.7 高機能暗号ガイドラインの執筆方針

想定する読者：

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

記載する暗号方式の選定基準及び候補：

主要な高機能暗号方式として、対象となる暗号方式は執筆担当委員が選定した。

付録１

CRYPTREC LS-0001-2022

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

電子政府推奨暗号リスト

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

技術分類		暗号技術
公開鍵暗号	署名	DSA
		ECDSA
		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。

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
	128ビットブロック暗号	該当なし
	ストリーム暗号	該当なし
ハッシュ関数		RIPEMD-160
		SHA-1（注8）
暗号利用モード	秘匿モード	該当なし
	認証付き秘匿モード（注16）	該当なし
メッセージ認証コード		CBC-MAC（注11）
認証暗号		該当なし
エンティティ認証		該当なし

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

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

（注11） 安全性の観点から、メッセージ長を固定して利用すべきである。

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

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

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

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] 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 http://www.esat.kuleuven.ac.be/~bosselae/ripemd160.html

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

4. メッセージ認証コード

暗号名	CBC-MAC
関連情報	仕様

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

付録３

軽量暗号の安全性に関する調査及び評価
(Photon-Beetle, Sparkle, Tsudik's keymode)

岩田　哲

名古屋大学大学院工学研究科

2022 年 12 月

原文は、CRYPTREC EX-3201-2022
https://www.cryptrec.go.jp/exreport/cryptrec-ex-3201-2022.pdf
で入手可能。

エグゼクティブサマリ

本報告書では，PHOTON-Beetle，Sparkle，Tsudik's keymode の安全性に関する調査及び評価を報告する．

PHOTON-Beetle． PHOTON-Beetle は暗号学的置換 P_{256} に基づく認証暗号 PHOTON-Beetle-AEAD とハッシュ関数 PHOTON-Beetle-Hash からなる．

- P_{256} は 12 ラウンドの繰り返し構造を有する入出力長 256 ビットの暗号学的置換である．仕様段数である 12 ラウンドの P_{256} に対し，[WGR18, CT-RSA 2018] において，サイズ 2^{184} の zero-sum 分割を用い，時間計算量 2^{183} の識別攻撃が示されている．ただし汎用的攻撃からの利得は小さく，またハッシュ関数などのモードに組み込んだ際の安全性を直ちに脅かすものではない．
- PHOTON-Beetle-AEAD は PHOTON-Beetle-AEAD[128] と PHOTON-Beetle-AEAD[32] からなる．設計者による安全性の主張は次の表の通りである．安全性はビットで表現されている．

モード	安全性モデル	データ計算量	時間計算量
PHOTON-Beetle-AEAD[128]	IND-CPA	121	121
PHOTON-Beetle-AEAD[128]	INT-CTXT	121	121
PHOTON-Beetle-AEAD[32]	IND-CPA	128	128
PHOTON-Beetle-AEAD[32]	INT-CTXT	128	128

  - 表にあるビット安全性の主張を覆す解析結果は知られていない．
  - 表の一部（赤字部分）は理論的根拠がない数字が挙げられている．
- PHOTON-Beetle-Hash は PHOTON-Beetle-Hash[32] が唯一の推奨方式であり，設計者による安全性の主張は次の表の通りである．安全性はビットで表現されている．

モード	安全性モデル	時間計算量
PHOTON-Beetle-Hash[32]	衝突	112（データ計算量 $2^{111.5}$）
PHOTON-Beetle-Hash[32]	原像	128

  - 表にあるビット安全性の主張を覆す解析結果は知られていない．

Sparkle． Sparkle は暗号学的置換の族であり，Schwaemm は Sparkle を暗号学的置換として用いた Sponge 構造に基づく認証暗号であり，Esch は Sparkle を暗号学的置換として用いた Sponge 構造に基づくハッシュ関数である．

- Sparkle には big instances と slim instances があり，Sparkle の big instances の安全性の主張は，入出力長 n ビットに対し，時間計算量とデータ計算量が $2^{n/2}$ を下回る識別攻撃が存在しないことである．slim instances は Sponge 構造に組み込んだ場合の安全性のみを想定し，レート部分に対応する入力のみを制御できる敵に対する識別不可能性を主張している．これらの安全性の主張を覆す解析結果は知られていない．
- Schwaemm は合計 4 通りのパラメータがあり，それぞれの安全性の主張は次の表のとおりである．安全性はビット単位で表現されており，データ制限はバイト単位である．

方式	安全性	データ制限（バイト）
Schwaemm256-128	120	2^{68}
Schwaemm192-192	184	2^{68}
Schwaemm128-128	120	2^{68}
Schwaemm256-256	248	2^{133}

  - 表にあるビット安全性の主張を覆す解析結果は知られていない．
- Esch は Esch256 と Esch384 の 2 通りが定義されており，次の表の安全性が主張されている．安全性はビット単位で表現されており，データ制限はバイト単位である．

方式	衝突	第 2 原像	原像	データ制限（バイト）
Esch256	128	128	128	2^{132}
Esch384	192	192	192	2^{196}

  - 表にあるビット安全性の主張を覆す解析結果は知られていない．

Tsudik's keymode． Tsudik's keymode は軽量ハッシュ関数を構成要素として用いる MAC である．

- ハッシュ関数が length-extension 攻撃を許す場合には Tsudik's keymode に対する偽造攻撃が可能であり，明らかな脆弱性を有している．Merkle-Damgård 変換に基づくハッシュ関数では length-extension 攻撃が可能であり，SHA-256 等を Tsudik's keymode で利用することはできない．
- 一方，ハッシュ関数が（可変長入力の）ランダムオラクルである場合には Tsudik's keymode は理想的に安全な擬似ランダム関数になる．したがって，ランダムオラクルからの強識別不可能性が証明できるようなハッシュ関数を用いれば，Tsudik's keymode の利用に安全性上の問題は見受けられない．

軽量暗号の安全性に関する調査及び評価
(GIFT-COFB, Xoodyak)

三菱電機株式会社
内藤　祐介

2022 年 12 月

原文は、CRYPTREC EX-3202-2022
https://www.cryptrec.go.jp/exreport/cryptrec-ex-3202-2022.pdf
で入手可能。

エグゼクティブサマリー

NIST が主催の Lightweight Cryptography Standardization Process[19] の最終候補である GIFT-COFB [2, 3, 1] と Xoodyak [11, 10] の安全性に関する文献の調査結果をまとめる．

GIFT-COFB の安全性に関する文献調査　GIFT-COFB は，ブロック暗号ベースの認証暗号である．設計者が主張する安全性は，シングルユーザで，秘匿性について，オンライン計算で 64 bit，オフライン計算で 112 bit 以上，偽造不可能性について，オンライン計算で 58 bit，オフライン計算で 112 bit 以上である．GIFT-COFB で用いられているブロック暗号 GIFT-128 と，GIFT-COFB の安全性に関する文献調査の結果は以下の通りある．

GIFT-128 の安全性　GIFT-128 は，鍵サイズとブロックサイズが 128 bit，40 ラウンドのブロック暗号である [5]．これまでの最適な攻撃は，差分攻撃法で，ラウンド数を 27 ラウンドに削減した GIFT-128 を破ることができる [25]．GIFT-128 のラウンド数は 40 ラウンド，攻撃可能なラウンド数は 27 ラウンドと十分にマージンがあるため，GIFT-128 はオフライン計算に関して設計者が主張する 112 bit 以上の安全性を持つと考えられる．

GIFT-COFB の安全性　GIFT-COFB は，利用モードとして文献 [8] の COFB を用いている．COFB の安全性では，ブロック暗号を Pseudo-Random Permutation (PRP) と仮定している．上記の通り，GIFT-128 の安全性は担保されているため，GIFT-COFB の安全性は COFB の安全性に依存する．文献 [8, 4] で，ブロックサイズを n bit，ブロック暗号を PRP 安全と仮定すると，シングルユーザに対して，秘匿性のオンライン計算に対して $n/2$ bit，偽造不可能性のオンライン計算に対して $n/2 - \log_2 n$ bit となることが証明されている．GIFT-COFB は $n = 128$ であり，上記の通り，GIFT-128 はオフライン計算に関して 112 bit 以上の安全性を持つことから，設計者が主張する安全性を持つと考えられる．

Xoodyak の安全性に関する調査　Xoodyak は，置換ベースのアルゴリズムであり，ハッシュ関数と認証暗号の 2 つのアルゴリズムを備える．設計者が主張する安全性は，Collision Resistance，Second Preimage Resistance，Preimage Resistance に関して 128 bit，m-Target Preimage Resistance に関して $\min\{256 - \log_2 m, 128\}$ bit，認証暗号について，シングルユーザで，秘匿性と偽造不可能性について，オンライン計算で 160bit，オフライン計算で 128bit である．Xoodyak で用いられる置換 Xoodoo[12] と Xoodyak の安全性に関する文献調査の結果は以下の通りある．

Xoodoo[12] の安全性　Xoodoo[12] は 384 bit，12 ラウンドの置換である．Xoodoo[12] 単体では，文献 [16] で，オフライン計算量が 2^{33} の Zero-sum Distinguisher が提案されており，Xoodyak の設計者が主張するオフライン計算で 128 bit の安全性はない．ただし，文献 [11] で設計者が述べているように，この攻撃が Xoodyak の安全性に直接影響を及ぼすものではないことに注意されたい．

Xoodyak のハッシュ関数の安全性　Xoodyak のハッシュ関数利用モードは，Sponge 構造 [6] である．Sponge 構造は，b bit のランダム置換を用いる場合，b bit のうち r bit が入力メッセージの処理で用いられるレートと呼ばれるパラメータで，残りの c bit $(c = b - r)$ が安全性に寄与するキャパシティと呼ばれるパラメータである．Sponge 構造は，Indifferentiability の意味で，$c/2$ bit の安全性を持つ．Xoodyak のハッシュ関数は，$b = 384, c = 256$ で，Indifferentiability の安全性証明により，Xoodoo[12] をブラックボックスとする攻撃に対しては，Xoodyak は設計者が主張する安全性を持つ．Xoodoo[12] の構造を含めて考えると，Xoodoo[12] 単体での安全性は無いため，Sponge 構造の Indifferentiability の安全性は Xoodyak の安全性に適用できない．一方で，Xoodyak のハッシュ関数に対する攻撃は今のところ存在しないため，Xoodyak のハッシュ関数は設計者が主張する安全性を持つと考えられる．

Xoodyak の認証暗号の安全性　Xoodyak の認証暗号利用モードは，文献 [7, 12] に記載の置換をプリミティブとする Duplex 構造をベースに設計されている．Duplex 構造の安全性は文献 [12] で，ランダム関数との識別不可能性が示されており，Xoodyak の認証暗号の安全性は，Duplex 構造の安全性に依存する．Duplex 構造の安全性の結果に，Xoodyak のパラメータを適用すると，秘匿性に関しては，置換がブラックボックスの場合に，設計者が主張する安全性を持つと考えられる．一方で，偽造不可能性に関しては，文献 [12] の結果を用いると，置換がブラックボックスの場合に，オンライン計算で 64 bit，オフライン計算で 128 bit の安全性となるが，設計者が主張する安全性は，オンライン計算で 160 bit，オフライン計算で 128 bit と異なる．今のところ，設計者が主張する偽造不可能性を破る攻撃は存在しないが，安全性証明と著者の主張に差があることに注意が必要である．また，Xoodoo[12] の構造を含めて考えると，Xoodoo[12] 単体での安全性は無いため，Duplex 構造の安全性は Xoodyak の安全性に適用できない．Xoodoo[12] の構造を含めた Xoodyak の認証暗号に対する攻撃は，ラウンド数を 6 ラウンドに削減した Xoodyak の認証暗号に対する Conditional Cube 攻撃 [24] が最適であり，Xoodoo[12] のラウンド数は 12 ラウンドと十分にマージンがあるため，Xoodyak の認証暗号は設計者が主張する安全性を持つと考えられる．

軽量暗号の安全性に関する調査及び評価
(Ascon, Grain-128AEAD, TinyJambu)

藤堂　洋介 *

2022 年 12 月

1　調査結果・評価結果の概要

昨今の IoT の広がりから、非常に安価な端末でも高い安全性を確保する必要性が高まってきている。これらの需要を受けて、アメリカ国立標準技術研究所 (NIST) は軽量暗号方式の標準化コンペティション (NIST LWC) を 2019 年に開始した。59 方式の Round 1 候補が 2019 年 4 月に発表され、同年 8 月に Round 2 候補として 32 方式まで絞られた。2021 年 3 月に Finalist として 10 方式 (ASCON, Elephant, GIFT-COFB, Grain-128AEAD, ISAP, PHOTON-Beetle, Romulus, SPARKLE, TinyJambu, Xoodyak) が選定された。本報告書は、上記 10 方式のうち、ASCON, Grain-128AEAD, および TinyJambu の安全性に関する既存結果の調査及び評価を与える。

1.1　ASCON

認証暗号 ASCON は 2014 年から 2019 年まで開催された認証暗号のコンペティション『CAESAR Competition』の候補として初めて提案された [DEMSb]。ASCON は CAESAR Competition のユースケース 1『Lightweight applications (resource constrained environments)』の第 1 選択に選定されている。最初の提案から 8 年が経過し、また、CAESAR Competition の Final portfolio にも選定されていることから、第三者の安全性解析による実績は多岐に及んでいる。ASCON は新たにハッシュモードが追加され、NIST が主催する軽量暗号コンペティションの候補にあがっている [DEMSa]。

ASCON は Initialization、Iteration (データ処理部)、Finalization で異なる繰り返し数を持つ暗号学的置換を利用する。Primary recommendation である ASCON-128 は Initialization および Finalization では繰り返し数が 12 である暗号学的置換、Iteration では繰り返し数が 6 である暗号学的置換が利用されている。Initialization をターゲットとした既知の最良な攻撃手法は Cube 攻撃 (高階差分攻撃) による鍵回復攻撃であり 12 段中 7 段まで、Finalization をターゲットとした既知の最良攻撃手法は差分解読法による偽造攻撃であり 12 段中 4 段まで、Iteration をターゲットとした既知の最良攻撃手法は SAT ソルバーを用いた内部状態回復攻撃あり 8 段中 2 段まで、それぞれ攻

* NTT 社会情報研究所

原文は、CRYPTREC EX-3203-2022
https://www.cryptrec.go.jp/exreport/cryptrec-ex-3203-2022.pdf
で入手可能。

撃方法が知られている。

1.2 Grain-128AEADv2

認証暗号 Grain-128AEAD[HJM+a] は NIST LWC で初めて提案された方式ではあるが、2004 年から 2008 年にかけて行われたストリーム暗号のコンペティション eSTREAM 提案 Grain[HJM05, HJM07] の系譜を継ぎ、詳細な暗号構造も 2011 年に Symmetric Key Encryption Workshop (SKEW) で提案された Grain-128a[ÅHJM11] を踏襲している。Grain-128AEAD を対象として攻撃論文の数は少ないが、ほぼ等価な暗号である Grain-128a に対する解析論文は多く出版されている。したがって、Grain-128a に対する第三者の安全性解析の実績も包括して考えた場合、Grain-128AEAD も多くの第三者解析の実績を持っていると判断できる。一方で、Grain-128a の解析が直接的に Grain-128AEAD の安全性に影響を与えるわけではないことに注意されたい。例えば、Grain-128a のストリーム暗号モードは高速相関攻撃により解読可能なことが指摘されているが、同様の攻撃手法は観測できるデータの制限のため Grain-128AEAD では動作しない。また、Grain-128AEAD は NIST LWC の Final Round で、Initialization の仕様変更が行われ、現在は Grain-128AEADv2 となっている [HJM+b]。

1.3 TinyJAMBU

認証暗号 TinyJAMBU[WH19] は CAESAR Competition の第三次候補の一つである JAMBU[WH16] の軽量版として NIST LWC で初めて提案された。JAMBU がブロック暗号 AES およびブロック暗号 Simon を利用したブロック暗号利用モードであったのに対して、TinyJAMBU は、内側のブロック暗号に相当する部分も軽量な鍵付き暗号学的置換を一から設計しており、安全性評価の観点では、JAMBU と TinyJAMBU は大きく異なる。NIST LWC Finalist 10 方式の中でも、軽量実装という基準で優れた性能を有している一方、その非常に軽量な構造のため、多くの安全性上の懸念も指摘されている。例えば、TinyJAMBU はブロック暗号をベースとした認証暗号ではあるが、そのブロック暗号は、ブロック暗号としては安全でないことが指摘されている。また、TinyJAMBU は Finalist Round で P1 の段数を 384 段から 640 段に修正したが [WH21]、オリジナルの 384 段は線形解読法で鍵回復攻撃が可能なことが指摘されている。また、関連鍵攻撃において、192 ビット安全な TinyJAMBU-192 および 256 ビット安全な TinyJAMBU-256 に対して、実用的な計算量で偽造攻撃が可能なことも指摘されている。

軽量暗号の安全性に関する調査及び評価
(Elephant, ISAP, Romulus)

井上明子 (NEC)

2022 年 12 月

原文は、CRYPTREC EX-3204-2022
https://www.cryptrec.go.jp/exreport/cryptrec-ex-3204-2022.pdf
で入手可能。

第1章　エグゼクティブサマリー

現在開催中の NIST Lightweight cryptography プロジェクト (以下, NIST LWC) [1]においてファイナリストとして残っている 10 候補のうち, 3 つの候補 Elephant [21], ISAP [38], Romulus [55] の安全性について調査を行った. 詳細には, Final round[2]に提出されている各候補の仕様に対する安全性評価に関する文献を調査した. その結果として 2022 年 9 月末時点では, 全ての候補に対して提案者らが主張する安全性を損ねるような解析結果は発表されていないことが分かった.

本報告書では, 各候補に対してその仕様 (アルゴリズム) 及び安全性に関する文献の調査結果を記載する. まず 2 章で必要な記法等の準備を行い, 3 章, 4 章, 5 章でそれぞれ Elephant, ISAP, Romulus について述べる. 各候補の章は準備, 仕様, 安全性の 3 節に分かれている. 準備の節ではその候補の章に必要な記法を記載する. 仕様の節では, Final round に提出されている仕様書 [21,38,55] に基づき, 各候補のアルゴリズムを記載する. 但し, 1 つの候補に安全性や効率性等の異なる複数のアルゴリズムが含まれるため, そのうち Primary member として挙げられているアルゴリズムのみを詳述し, 他アルゴリズムは概要を記載する. 安全性の節は以下 4 つの構成になっている.

- **仕様上の安全性**: 各候補の提案者らが主張する主要な安全性とそのレベルを概説する.
- **モードの安全性**: 各候補が用いるモードの証明可能安全性について, 著者らの主張の詳細や安全性評価の調査結果をまとめる.
- **プリミティブの安全性及び関連方式の安全性**: 各候補で用いる暗号プリミティブの攻撃可能段数の調査結果をまとめる. 必要に応じてそのプリミティブを用いた他方式の攻撃可能段数についても述べる.
- **その他**: 上記 2 つ以外の安全性解析結果について述べる. 例として, プリミティブのラウンド数を削減した場合の各候補への安全性評価, サイドチャネル攻撃評価, 量子計算機を用いた場合の安全性評価が挙げられる.

注意事項として, ISAP においては NIST LWC ファイナリストの 1 つ Ascon [41] とアルゴリズムを共有する部分があるため, 該当部分のアルゴリズムや共通する安全性調査の結果は概要のみを記載することとする. 詳細は Ascon の安全性調査レポートを参照されたい.

[1] https://csrc.nist.gov/projects/lightweight-cryptography
[2] https://csrc.nist.gov/Projects/lightweight-cryptography/finalists

軽量暗号の実装性能に関する調査及び評価
（NIST軽量暗号コンペティションファイナリスト）

電気通信大学大学院情報理工学研究科

崎山一男

2022年12月

原文は、CRYPTREC EX-3205-2022
https://www.cryptrec.go.jp/exreport/cryptrec-ex-3205-2022.pdf
で入手可能。

エグゼクティブサマリー

本報告は，米国 NIST (National Institute of Standards and Technology)が推進し，標準化を進めているNIST軽量暗号 (LWC: Lightweight Cryptography)コンペティション [19]でファイナリストに選定された10方式(ASCON, Elephant, GIFT-COFB, Grain128-AEAD, ISAP, Photon-Beetle, Romulus, Sparkle, TinyJambu, Xoodyak) に対する実装性能評価に関する公開情報をまとめ考察を与えたものである．

ハードウェア実装性能の評価報告については，製品の異なるFPGA実装とライブラリの異なるASIC実装がある中で，最も多く使用されたプラットフォームのひとつは，Xilinx社のArtix-7である．図は，Xilinx Artix-7上に実装されたファイナリスト10方式のハードウェアの面積コストとスループット性能をプロットしたものである．細かい設定や測定の条件は考えずに報告された結果のみを用いているため，同じアルゴリズムでも同じ面積コストで異なるスループット性能をプロットしている場合もある．この図から，TinyJambuの回路面積が小さいこと，逆にSPARKLEが比較的面積コストが大きくなることが読み取れる．また，ASCON, Elephant, GIFT-COFB, Romulusのプロットは広く分散しており，軽量実装から高速実装まで，FPGA実装における設計の選択肢が多いアルゴリズムとなっていることがわかる．今後さらに研究が進

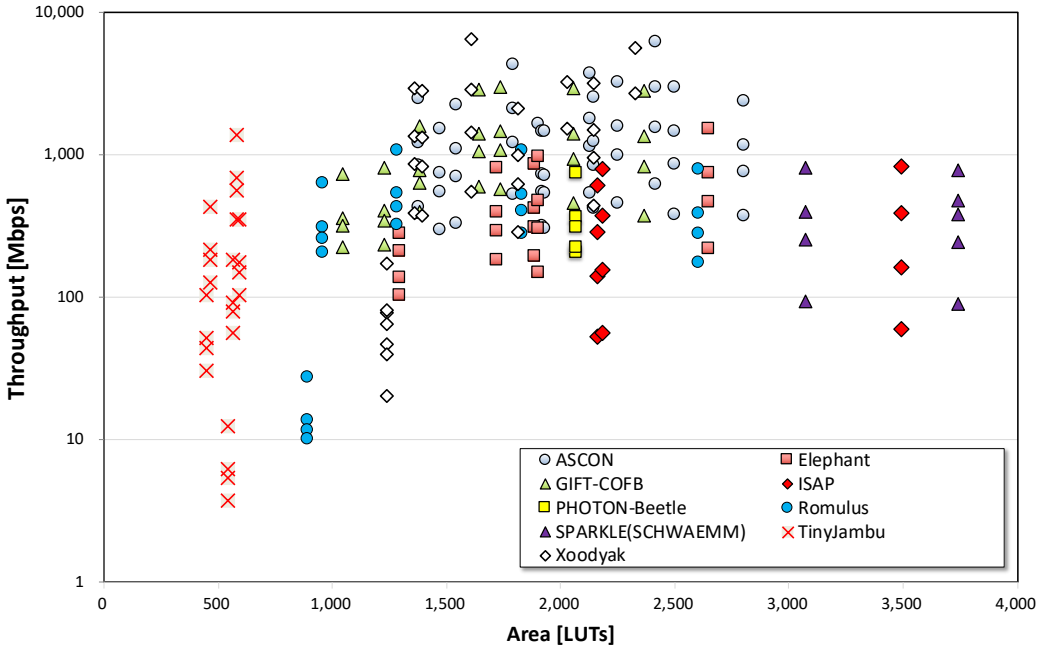

図　NIST 軽量暗号コンペティションファイナリストのXilinx Artix-7上の実装性能．Grain128-AEADは，今回の調査で結果が見つからなかったためプロットはない．

表　NIST軽量暗号コンペティションファイナリストのArm Cortex-M0上の実装性能 [12]

Candidate	Latency [msec]	Code Size [kByte]
ASCON (ascon128v12)	0.633	29.4
Elephant (elephant160v1)	1069	14.4
GIFT-COFB (giftcofb128v1)	6.25	15.1
Grain-128-AEAD (grain128aead)	82.54	15.8
ISAP (isapk128av20)	161.9	14.5
Photon-Beetle (photonbeetleaead128rate128v1)	42.39	15.4
Romulus (romulusn1v12)	17.16	17.0
Sparkle (schwaemm128128v1)	0.76	14.9
TinyJambu (tinyjambu128)	0.394	13.7
Xoodyak (xoodyakv1)	0.599	14.3

み，新たなデータが公開された場合には，他のアルゴリズムにおいても同様の柔軟性が見られる可能性はある．今回，Grain128-AEADについては，Xilinx Artix-7上の公開された実装結果は見つけることができなかった．

軽量暗号のアプリケーションを考えると，低リソースプラットフォーム上での実装性能評価の価値は高い．表は，Arm Cortex-M0上のソフトウェア実装の結果の一部をまとめたものである [12]．括弧内の名称は，各アルゴリズムのプライマリメンバー (primary member)[*1]のリファレンスソフトウェアである．表では，レイテンシとコードサイズをまとめている． RAMの使用量はコンパイル時の静的なメモリサイズのレポートから，どのアルゴリズムも約1kByte程度である．

レイテンシは，平文とADを0バイトから32バイトまで変化させた共通のテストベクトルを用いた際に，暗号化にかかった時間を平均したものである．表から，Elephantが最もレイテンシが高く，TinyJambu，Xoodyak，ASCON, Sparkleが低レイテンシであることがわかる．コードサイズについては，ASCONが最も大きく，他の候補に大きな差はみられなかった．ただし，この結果はほんの一面であり，プラットフォームに適した最適化実装によりより良い結果が得られるものと考える．

このように，公開データを用いて比較の考察を与えることがあるが，厳密な公平性を調べているわけではない．また，実装性能の優劣は公開情報だけでは判断しづらい面があるため，以降はアルゴリズム毎に調査結果をまとめる．

[*1] 提出者が，NISTの要件（鍵128ビット以上，ノンス96ビット以上，タグ64ビット以上）に従ってアルゴリズムのパラメータを設定し，primary memberを一つ決める．

軽量暗号の評価指標、標準化動向に関する調査

(NIST 軽量暗号コンペティションファイナリストなど)

GMO サイバーセキュリティ by イエラエ株式会社

2022 年 12 月

原文は、CRYPTREC EX-3206-2022
https://www.cryptrec.go.jp/exreport/cryptrec-ex-3206-2022.pdf
で入手可能。

エグゼクティブサマリー

本報告書では、過去に実施されていた CAESAR プロジェクトや現在評価が行われている NIST 軽量暗号コンペティション、ISO/IEC 29192 シリーズおよび CRYPTREC 暗号技術ガイドライン（軽量暗号）に対して軽量暗号に関する評価指標および標準化動向について調査・検討を実施した。

その結果として、以下のことが判明した。

- 選定アルゴリズムの側面
  - 各プロジェクト等において選定された軽量暗号アルゴリズムとして共通的なものは存在していない。
    - 各プロジェクトでターゲットとしている軽量暗号に関する技術分類（ブロック暗号、ストリーム暗号、AEAD など）が異なる点も影響しているのではないかと推測される。
  - 軽量暗号に関する各プロジェクトが様々なタイミングで実施されているので、各活動で選定されたアルゴリズム名が改良されるなどが行われている。
    - 懸念事項として、ベースとなる方式を改良した場合、名称が似通っているため同一のアルゴリズムかどうか判定しにくい状況を生み出している。
- 評価指標の側面
  - 安全性
    - 安全性評価を行う際に、アルゴリズムの考案者から設計根拠について十分な情報が出てこない場合は第三者評価が行えないと判断され、評価対象から外されるなどの事例がある
  - 性能
    - 論文等では異なる環境や測定シナリオが統一されておらず、公平な比較が実施しにくい状況となっていることが多いが、統一的な測定フレームワークなどを用いて実施することが一般化された
      - 性能評価を行う際には、AES-GCM や SHA-256 など広く世界で利用されているアルゴリズムが対象になっていた

また、本調査を行い判明したこととしては、軽量暗号を選定しているプロジェクトにおい

て選ばれた軽量暗号アルゴリズムとして共通しているものがないという結果になった。実社会での軽量暗号の利用などを想定するのであれば、ここ数年で標準化されている ISO/IEC と NIST 軽量暗号コンペティションにおいて同一の軽量暗号アルゴリズムが存在すべきであると考えられるが、異なるアルゴリズムとなっている点が興味深い。着眼点を変えると、全ての過去に選定された軽量暗号アルゴリズムは実績があると考えられるが、NIST 軽量暗号コンペティションに投稿されていない点や他プロジェクト等に投稿されたアルゴリズムを改良した方式を提案されているケースも存在している点も興味深いと言える。

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、☆はその他の注視すべき技術動向である。

表 1 具体的な暗号の攻撃に関する発表

公開鍵暗号		頁
★	Approximate Divisor Multiples - Factoring with Only a Third of the Secret CRT-Exponents [EUROCRYPT 2022]	86
★	A Third is All You Need: Extended Partial Key Exposure Attack on CRT-RSA with Additive Exponent Blinding [ASIACRYPT 2022]	117
	How to Backdoor (Classic) McEliece and How to Guard Against Backdoors [PQCrypto 2022]	98
	Improving Bounds on Elliptic Curve Hidden Number Problem for ECDH Key Exchange [ASIACRYPT 2022]	115
	SwiftEC: Shallue--van de Woestijne Indifferentiable Function to Elliptic Curves [ASIACRYPT 2022]	108
ブロック暗号		
★	Revisiting Related-Key Boomerang Attacks on AES Using Computer-Aided Tool [ASIACRYPT 2022]	111
★	Synthesizing Quantum Circuits of AES with Lower T-depth and Less Qubits [ASIACRYPT 2022]	112
	Key Guessing Strategies for Linear Key-Schedule Algorithms in Rectangle Attacks [EUROCRYPT 2022]	83
	A Greater GIFT: Strengthening GIFT against Statistical Cryptanalysis [EUROCRYPT 2022]	85
	Beyond Quadratic Speedups in Quantum Attacks on Symmetric Schemes [EUROCRYPT 2022]	87
	Post-Quantum Security of the Even-Mansour Cipher [EUROCRYPT 2022]	87
	Information-Combining Differential Fault Attacks on DEFAULT [EUROCRYPT 2022]	88
	Superposition Meet-in-the-Middle Attacks: Updates on Fundamental Security of AES-like Ciphers [CRYPTO 2022]	92
	Triangulating Rebound Attack on AES-like Hashing [CRYPTO 2022]	93
	Simplified MITM Modeling for Permutations: New (Quantum) Attacks [CRYPTO 2022]	95
	Simon's Algorithm and Symmetric Crypto: Generalizations and Automatized Applications [CRYPTO 2022]	93
	Quantum Attacks on Lai-Massey Structure [PQCrypto 2022]	102
	Practical Multiple Persistent Faults Analysis [CHES 2022]	104
	Algebraic Meet-in-the-Middle Attack on LowMC [ASIACRYPT 2022]	107
	Mind the TWEAKEY Schedule: Cryptanalysis on SKINNYe-64-256	113

2. EUROCRYPT 2022 の発表

2.1. EUROCRYPT 2022 の発表（2 日目）

・Revamped Differential-Linear Cryptanalysis on Reduced Round ChaCha [EUROCRYPT 2022]

Sabyasachi Dey, Hirendra Kumar Garai, Santanu Sarkar, Nitin Kumar Sharma

本論文では、ChaCha における既存の差分線形攻撃に対するいくつかの改良点を提供する。ChaCha は 20 ラウンドを持つストリーム暗号である。CRYPTO 2020 で、Beierle らは適切なペアが選択された場合、3.5 ラウンド目に差分が発生することを観測している。彼らはこの差分を用いて攻撃の改良を試みたが、適切なペアを得るためには平均で 2^5 回の反復が必要であることを示した。この方法論に関し、リスト化（listing）の助けを借りて、適切なペアを見つけるための技術を提供する。また、Probabilistic Neutral Bits (PNB) 構築の戦略的改善、計算量見積の修正、そして 2 つの入出力ペアを用いた代替的な攻撃方法も提供する。これらの技術を用いて計算量を改善する。具体的には、Beierle らが示した 7 ラウンドの ChaCha256 に対する攻撃の計算量を $2^{230.86}$ から $2^{221.95}$ に減少させた。また、6 ラウンドの ChaCha128 に対する既存の計算量（Shi et al: ICISC 2012）を 1100 万倍以上改善するとともに、6.5 ラウンドの ChaCha128 に対する史上初の攻撃で計算量 $2^{123.04}$ を実現した。

・Key Guessing Strategies for Linear Key-Schedule Algorithms in Rectangle Attacks [EUROCRYPT 2022]

Xiaoyang Dong, Lingyue Qin, Siwei Sun, Xiaoyun Wang

著者らは、線形キースケジュールを有する暗号に対する矩形攻撃（rectangle attack）のための入出力差分の四つ組（quartets）を生成する際、鍵候補を示唆しうる正しい四つ組は、いくつかの非線形な関係を満たす必要があることを見出した。しかし、生成される四つ組の中には、常にこれらの関係を破り、鍵候補を示唆しないものがある。著者らは、過去の矩形攻撃フレームワークからヒントを得て、四つ組を生成する前に特定のキーセルを推測することで、無効な四つ組の数を減少させることができることを見出した。しかし、一度に多くのキーセルを推測すると、早期に中断する手法の利点が失われ、全体の計算量が増す可能性がある。そこで本論文では、より良いトレードオフを得るために、線形キースケジュールを有する暗号に対する新しい矩形攻撃フレームワークを構築し、全体的な計算量を軽減するか、より多くのラウンドを攻撃することを目的としている。

このトレードオフモデルでは、全体の計算量に影響を与える多くのパラメータが存在しており、特に四つ組を生成する前に推測するキーセルの数と位置の選択が重要となる。

最適なパラメータを特定するため、SKINNY を例として一貫した自動ツールを構築する。このツールには、鍵回復フェーズに最適な矩形識別子、四つ組生成前に推測するキーセルの数と位置、網羅的な探索ステップに影響を与えるキーカウンタのサイズ、などが含まれている。この自動化ツールを用いて、関連鍵設定で 32 ラウンドの SKINNY-128-384 に対する鍵回復攻撃が実行できることを確認し、既存の最良な攻撃を 2 ラウンド拡張した。また、SKINNY における他のバージョンについても、従来よりも 1 ラウンド多く達成した。さらに、これまでの矩形識別子を用いて、ラウンド数を削減した ForkSkinny、Deoxys-BC-384、GIFT-64 に対してより良い攻撃を行っている。最後に、著者らの矩形攻撃フレームワークを関連鍵設定から単一鍵設定に変換し、10 ラウンドの Serpent に対する新しい単一鍵矩形攻撃が実行できることを示す。

・A Correlation Attack on Full SNOW-V and SNOW-Vi [EUROCRYPT 2022]

Zhen Shi, Chenhui Jin, Jiyan Zhang, Ting Cui, Lin Ding, Yu Jin

本論文では、合成関数の近似技術に基づき、線形フィードバックシフトレジスタ（LFSR: Linear Feedback Shift Register）のバイナリストリームと SNOW-V および SNOW-Vi のキーストリーム間の相関を探索する方法を提案する。連続する 3 クロックで有限状態機械（FSM: Finite State Machine）に入力される LFSR の 4 つのタップ間の線形関係を利用して、SAT/SMT 手法に基づく自動探索モデルを提案し、高い相関を持つ一連の線形近似トレイルを探し出す。中間マスクを全て網羅することで、相関が $-2^{-47.76}$ のバイナリ線形近似を見つけることができる。このような近似を使用して、SNOW-V に対する相関攻撃を提案し、期待される時間計算量が $2^{246.53}$、メモリ計算量が $2^{238.77}$, 同じ鍵と初期ベクトル(IV)で生成されたキーストリームのデータ量が $2^{237.5}$ となった。SNOW-Vi については、同じ相関を持つバイナリ線形近似を提供し、SNOW-V と同じ計算量で相関攻撃を実行する。著者らの知る限り、これはフルラウンドの SNOW-V と SNOW-Vi に対する最初の攻撃であり、この攻撃は計算量に関して秘密鍵の全数探索よりも優れている。その結果、鍵と IV の単一ペアのキーストリームの最大長が 2^{64} 未満であるという設計上の制約を無視すれば、SNOW-V と SNOW-Vi のいずれも 256 ビットのセキュリティレベルを保証できないことが示された。

・Refined Cryptanalysis of the GPRS Ciphers GEA-1 and GEA-2 [EUROCRYPT 2022]

Itai Dinur, Dor Amzaleg

EUROCRYPT 2021 で、Beierle らは General Packet Radio Service (GPRS) 暗号 GEA-1 と GEA-2 に対する初めての解析結果を公に発表した。彼らは、GEA-1 は 64 ビットのセッション鍵を使用しているにも関わらず、65 ビットのキーストリームを知るだけで、計算量 2^{40} でセッション鍵を復元できることを示した。なお、この攻撃には

44GiB のメモリが必要となる。この攻撃は、暗号の初期化処理における脆弱性を悪用したもので、設計者が意図的に隠して安全性を低下させたと推測される。

GEA-2 ではそのような脆弱性は見つかっていないが、Beierle らはこの暗号に対して約 2^{45} の計算量となる攻撃を発表している。主な実用上の障害は、GPRS フレームを完全に暗号化するために使用される 12800 ビットのキーストリームを知る必要があることである。この攻撃のバリエーションは、連続するキーストリームビットが少ない場合や、（連続する長いブロックがない）利用可能なキーストリームが断片化されている場合にも適用可能であるが、よりコストはかかる。

本論文では、GEA-1 と GEA-2 に対するこれまでの解析を改善し、補完するものである。GEA-1 について、計算量は 2^{40} のままであるものの、メモリ量を 44 GiB から約 4MiB までのおよそ $2^{13} = 8192$ 倍に削減可能な攻撃手法を考案した。実装では、最新のラップトップで GEA-1 のセッションキーを平均 2.5 時間で復元できる。

GEA-2 について、Beierle らの解析を補完する 2 つの攻撃が説明される。最初の攻撃は、攻撃者が利用できる連続したキーストリームビット数ℓと計算量の間の線形トレードオフを得ることができる。これにより、従来の攻撃を（おおよそ）$\ell \leq 7000$ の範囲で改善する。具体的には、$\ell = 1100$の場合、従来の攻撃はブルートフォースの計算量 2^{64} より高速ではないものの、本攻撃の計算量は約 2^{54} を達成した。利用可能なキーストリームが断片化されている場合、第二の攻撃は、計算量のコスト増加なしに、既存攻撃のメモリ量を 32 GiB から 64 MiB に 512 倍減少させることができる。

本攻撃は、ストリーム暗号の解析技術と他の文脈で用いられるアルゴリズム技術（例えば k-XOR 問題の解決など）の新しい組み合わせに基づくものである。

・A Greater GIFT: Strengthening GIFT against Statistical Cryptanalysis [EUROCRYPT 2022]

Ling Sun, Bart Preneel, Wei Wang, Meiqin Wang

GIFT-64 は PRESENT より軽量な 128 ビット鍵による 64 ビットブロック暗号である。本論文では、差分攻撃と線形攻撃に対する GIFT-64 の詳細な分析を行う。著者らの研究は、最適な差分特性と線形特性の自動探索手法を注意深い手動分析で補完している。このハイブリッドアプローチにより、新たな知見が得られる。差分攻撃の設定では、ラウンドごとに 2 つのアクティブな S-box を持つ差分特性の存在を理論的に説明し、これらの特性のいくつかの新しい性質を導出する。さらに、GIFT-64 の 7 ラウンド以上をカバーする全ての最適な差分特性は、ラウンドごとに 2 つの S-box をアクティブにしなければならないことを証明する。全ての最適な特性は手作業で構成することができる。差分攻撃の設定における作業と並行して、線形攻撃の設定においても同様の分析を行う。しかし、差分攻撃の設定での明確な見解とは異なり、GIFT-64 の最適な線形特性は、少なくとも 1 ラウンドが 1 つの S-box のみをアクティブにするものでなければな

らない。さらに、自動探索手法の助けを借りて、線形攻撃に対して同等の安全性を維持しながら、差分攻撃に対してより優れた耐性を持つ 24 種類の GIFT-64 の亜種を見出した。これらの亜種は統計的暗号解析に対して GIFT-64 を強化されたため、ラウンド数を 28 から 26 に減らすことができると著者らは主張した。この観測により、GIFT-64 よりもエネルギー消費量の少ない暗号を作ることが可能になった。GIFT-64 の場合と同様に、ラウンド数を削減した亜種についても、ほとんどのアプリケーションに関係がないため、関連鍵の安全性を主張することはない。

2.2. EUROCRYPT 2022 の発表（3 日目）

・Approximate Divisor Multiples - Factoring with Only a Third of the Secret CRT-Exponents [EUROCRYPT 2022]

Alexander May, Julian Nowakowski, Santanu Sarkar

本論文は、CRT-RSA の秘密指数d_p, d_qで、公開指数eが小さい場合に秘密鍵の一部分が漏洩した場合の攻撃について研究している。eが定数である場合、d_p, d_q両方のビット表現の連続した半分を知ることで、Coppersmith の有名な「factoring with a hint」の結果によって RSA 剰余Nを素因数分解可能であることが知られている。この設定をeが定数でない場合に拡張する。

本論文の少し意外な結論として、eのサイズが $N^{1/12}$ である RSA が部分鍵公開攻撃に対して最も弱いということが示されている。この状況では、d_p, d_q両方の最上位ビット（MSB）または最下位ビット（LSB）の 3 分の 1 を知ることができれば多項式時間でNを因数分解できるためである。

著者らはNの素因数分解を二段階のアプローチで求めている。$ed_p = 1 + k(p-1)$, $ed_q = 1 + \ell(q-1)$とする。第一ステップでは、kとℓを多項式時間で復元する。これは、MSB が知られている場合には初等的な方法を用いて、LSB の場合は Coppersmith の格子に基づく方法を用いて計算される。後半のステップでは求められたkを用いて、kpを法とする一変数多項式の根を計算することで、Nの素因数分解を得ることができる。これは、Howgrave-Graham の approximate divisor アルゴリズムの、Nの未知の約数pの既知の倍数kに対する approximate divisor multiples の場合への拡張と見なすことができる。

この部分秘密鍵公開攻撃は、MSB が既知の場合は攻撃の成功が理論的に証明可能な一方、LSB の場合は標準的な Coppersmith タイプのヒューリスティックに依存する。このヒューリスティックを実験的に検証することにより、攻撃の実効性も示されている。攻撃が有効な範囲の計算はNの大きさを無限大とした漸近的なものであるが、実際に小さな格子次元での実験により、漸近的な境界値に到達することが示される。

・Beyond Quadratic Speedups in Quantum Attacks on Symmetric Schemes [EUROCRYPT 2022]

Xavier Bonnetain, André Schrottenloher, Ferdinand Sibleyras

本論文では、古典的なクエリのみを用いたブロック暗号に対する初の量子鍵回復攻撃を行い、最良の古典攻撃と比較して 2 次以上の計算量短縮を達成したことを報告する。

本研究の対象は、EUROCRYPT 2012 にて Gaži と Tessaro によって提案された 2XOR-Cascade 構成である。これは、2n ビットの鍵を持つ n ビットブロック暗号から 5n/2 ビットの安全性を持つ n ビットブロック暗号を提供する鍵長拡張技術であり、イデアルモデルにおける安全性証明がなされている。また、著者らは ASIACRYPT 2019 にて Bonnetain らが提案した offline-Simon アルゴリズムを拡張することで、対象とする構成を量子時間$\tilde{O}(2^n)$で攻撃できることを示し、最高の古典攻撃より 2.5 倍の量子速度向上を達成する。

これらの研究結果は、共通鍵暗号のポスト量子安全性に重要な影響を与える。一般に、共通鍵暗号のポスト量子安全性については、鍵のサイズを 2 倍にすることで十分であると考えられている。これは、Grover の量子探索アルゴリズムやその派生アルゴリズムが、最大でも 2 次関数的な高速化にしか到達できないためである。しかし、この 2XOR-Cascade 構造に対する攻撃は、特定の対称的な構造を利用することで、この限界を克服できることを示すものである。具体的には、2XOR-Cascade 構造はその基礎となるブロック暗号と同程度のセキュリティレベルしか提供できないため、ブロック暗号への量子攻撃者に対して安全性を向上させるための手段としては頼りにできないと言える。

・Post-Quantum Security of the Even-Mansour Cipher [EUROCRYPT 2022]

Gorjan Alagic, Chen Bai, Jonathan Katz, Christian Majenz

Even-Mansour 暗号は、公開されたランダム置換$P: \{0,1\}^n \to \{0,1\}^n$から、(鍵付きの)擬似ランダム置換$E$を構成するための単純な方法である。これは古典的な攻撃に対して安全であり、その最適な攻撃ではEへのq_E回のクエリとPへのq_P回のクエリを必要とし、$q_P q_E \approx 2^n$ のオーダーで実行可能となる。しかし、攻撃者にEとPの両方に対する量子アクセスが与えられた場合、この暗号は安全ではなく、$q_P = q_E = O(n)$回のクエリを用いた攻撃が知られている。

しかし、現実世界における設定では、量子攻撃者は、Pに対しては量子アクセス権を保持することができる一方で、信頼できるパーティーにより実装された鍵付き置換Eについては、古典的なアクセスしかできない。この設定では、$q_P^2 q_E \approx 2^n$の攻撃が知られており、純粋な古典的ケースと比較して安全性が低下することが示されているが、この自然な「ポスト量子」設定においても Even-Mansour 暗号の安全性がまだ証明できるかという疑問も残されている。

本論文では、この未解決の問題を解決し、このポスト量子設定における攻撃には

$q_P^2 q_E + q_P q_E^2 \approx 2^n$ が必要であることを示す。著者らの結果は Even-Mansour 暗号において 2 つの鍵を使用した場合と単一の鍵を使用した場合の両方に適用される。その過程で、量子クエリの下界に関する先行研究の結果を一般化し、その方面からも興味深い結果が得られている。

・Information-Combining Differential Fault Attacks on DEFAULT [EUROCRYPT 2022]

Marcel Nageler, Christoph Dobraunig, Maria Eichlseder

差分故障解析（DFA: Differential Fault Analysis）は、共通鍵暗号の実装に対する非常に強力な攻撃である。ほとんどの対策は実装レベルで適用される。ASIACRYPT 2021 にて Baksi らは、線形構造を持つ S-box を使用することで、DFA に対する暗号レベルの耐性を内在させることを目的とした設計戦略を提案した。彼らは、彼らのインスタンスであるブロック暗号 DEFAULT において、DFA 攻撃者は 128 鍵ビットのうち最大 64 ビットしか学習できないため、残りのブルートフォース攻撃の計算量 2^{64} は現実的ではないと主張した。

本論文では、DFA 攻撃者がラウンド間の情報を組み合わせて完全な鍵を復元できることを示し、その安全性の主張を無効化する。具体的には、このような暗号は、線形方程式を用いた正規化手法で効率的に表現できる大きな等価鍵のクラスを持つことを観察する。これを DEFAULT の強力なキースケジュールの特異性と組み合わせ、100 回以下の誤った計算と無視できる計算量で鍵回復に成功している。さらに、独立したラウンド鍵を持つ理想化された DEFAULT でさえ、正規化された鍵に基づく情報結合攻撃（Information-Combining Attacks）に対して脆弱であることを示す。

・A Novel Completeness Test for Leakage Models and its Application to Side Channel Attacks and Responsibly Engineered Simulators [EUROCRYPT 2022]

Si Gao, Elisabeth Oswald

今日のサイドチャネル攻撃の標的となるものは、命令が並列に処理され、32 ビットのデータワード上で動作するような複雑なデバイスであることが多い。その結果、これらの現代的なデバイスで漏洩の発生に関係する状態（state）は規模が大きいだけでなく、ユーザーが気づいていない可能性のある様々なマイクロアーキテクチャ要因により予測することが困難となる。一方、ワーストケース攻撃やシミュレーターに基づく安全性評価は、基礎となる状態に明示的に依存している。つまり、潜在的に不完全である状態は、簡単に誤った結論に繋がる可能性がある。

本論文では、想定される状態の「完全性」に対する新しい概念とともに、「崩壊モデル」に基づく効率的な統計的検定を提案する。この新しい検定は、グレーボックス設定において、複数の 32 ビット変数を含む状態を回復するために使用することができる。

さらに、この新しい検定がサイドチャネル攻撃分析に役立つことを説明し、既存の実装に対する新しい攻撃ベクトルを明らかにする。また、統計的検定を適用することで、最新の漏洩シミュレータでさえ、それぞれのターゲットデバイスの利用可能な漏洩をすべて捕捉していないことを示す。

・Towards Micro-Architectural Leakage Simulators: Reverse Engineering Micro-Architectural Leakage Features is Practical [EUROCRYPT 2022]

Si Gao, Elisabeth Oswald, Dan Page

リークシミュレータは、サイドチャネルリークを考慮したソフトウェアのテストを簡単かつ迅速に行えるという魅力的な機能を備えている。そのため、リークモデルの品質は非常に重要であり、これにはマイクロアーキテクチャのリークを忠実に含めることが含まれる。

マイクロアーキテクチャのリークは、ARM Cortex M シリーズのようなローからミッドレンジの商用プロセッサでも現実的なものである。マイクロアーキテクチャの要素が公に知られていない場合、どのようにそれを記述すればよいのだろうか？という問に、グレーボックス設定で対応することは、当初は実行不可能と思われていた。

本論文では、最新のリークモデリング技術を用いて、商用プロセッサのマイクロアーキテクチャのリークの重要な要素をリバースエンジニアリングすることが可能であることを初めて実証した。このアプローチでは、まず、パイプラインの各ステージのマイクロアーキテクチャのリークを復元し、グリッチを発生させることが知られている要素のリークを復元する。リバースエンジニアリングされたリーク機能を用いて、一般的なリークシミュレータ ELMO の拡張版を構築する。

・Private Circuits with Quasilinear Randomness [EUROCRYPT 2022]

Vipul Goyal, Yuval Ishai, Yifan Song

関数fのためのt-private 回路とは、入力xのランダムな符号化を出力$f(x)$の符号化に対応付けるランダム化ブール回路Cであり、回路C内の任意のt本を探ってもxについて何も明らかにならないものである。t-private 回路は、サイドチャネル攻撃から組込み機器を保護するために使用することができる。このようなデバイスで新しいランダム性を生成するコストが高いことに動機づけられ、いくつかの研究がt-private 回路のランダム性計算量を最小化する問題を研究してきた。Coron ら（EUROCRYPT 2020）による最もよく知られた上限は、sを回路のサイズとした時の、$O(t^2 c \log s)$-ビットである。本研究は、この上限を入力エンコーダで使用されるランダムネスを含めて$O(t \log s)$に改善した。さらに、t-private 回路のステートフルな亜種に対してもこれを拡張する。この構成は、fの回路から無視できる故障確率でt-private 回路Cを生成する効率的なランダム化アルゴリズムが存在するという意味で、semi-explicit なものである。

・Quantum Algorithms for Variants of Average-Case Lattice Problems via Filtering [EUROCRYPT 2022]

Yilei Chen, Qipeng Liu, Mark Zhandry

この論文では、LWE、SIS 問題のような耐量子暗号の根拠であると信じられている問題の変種が、量子多項式時間で解けてしまうことを示す。具体的な問題としては以下の 3 つ。

・$c > 0$とする。SIS(Short Integer Solutions)問題の変種で法qがnの多項式程度、変数mが$\Omega((q-c)^3 n^{c+1} q \cdot \log\ q\ )$という非常に大きな値を持ち、さらに解$\boldsymbol{x}$の$\ell_\infty$ノルムが$(q-c)/2$以下であるとするもの。

・LWE(Learning with errors)問題の量子版変種ともいえる$S|LWE\rangle$問題で、量子状態のサンプル（$f(e_i)|a_i \cdot \boldsymbol{u} + e_i \bmod q\rangle$の重ね合わせ）から$\boldsymbol{u}$を復元する問題。またその構成版で、LWE サンプルの重ね合わせ状態を生成する問題である$C|LWE\rangle$問題。

・適当なパラメータのもとでの EDCP(Extrapolated dihedral coset problem)

オリジナルの SIS、EDCP、LWE の最悪計算量は格子問題と同等であることが知られているが、この論文で取り上げられている変種の持つパラメータでは既存の格子問題への還元は示されていない。ただし、これらの問題に対してはこれまで古典・量子のどちらのアルゴリズムも知られていなかったことに注意。EDCP に対するアルゴリズムは Ivanyos ら（2018）の結果をわずかに拡張したものである。

技術的には SIS と EDCP からそれぞれ$C|LWE\rangle$問題、$S|LWE\rangle$問題への量子帰着が与えられたことと、$S|LWE\rangle$問題の量子アルゴリズムを与えた点が着目される。後半は$C|LWE\rangle$問題のインスタンスのような LWE サンプルの量子的重ね合わせが与えられたときに、フィルタリングと呼ばれる技術を用いることで秘密ベクトルが復元できる手法である。

・Orientations and the Supersingular Endomorphism Ring Problem [EUROCRYPT 2022]

Benjamin Wesolowski

この論文では、同種写像に関する二種類の問題とその関係について取り扱う。一つ目は超特異楕円曲線の自己準同型環の計算、二つ目は oriented supersingular curve 上の類群の作用の逆転である。一般化されたリーマン予想が成り立つという仮定の下で互いに多項式時間還元可能であるという関係を持つことが示された。

この結果から、本質的には等しい２つの問題のクラスが明らかになった。最初のクラスは oriented curve の自己準同型環の計算問題に対応し、(CSIDH のような)広いクラスの暗号学的計算問題がこのクラスに還元、もしくはこのクラスの問題から還元される。

また、このクラスの問題には準指数時間で動作するヒューリスティックな量子アルゴリズムが存在することが知られている、二つ目のクラスは orientable curve の自己準同型環の計算に対応する。すべての同種写像ベースの暗号の安全性は本質的にはこの問題に、もしくはこの問題から還元される。知られている最良のアルゴリズムでも指数時間を必要とする。

この論文で新たに提案する問題の還元手法は、既知のものを一般化したのみではなく結果の強化をも含んでいる。一例として、$\mathbb{F}_p$上で定義された曲線上の CSIDH の安全性はこれまで自己準同型環問題への準指数時間での還元が知られていたが、この論文では多項式時間での還元を与えており、そのような還元がおそらくありそうにないということを示す議論に対して反論を与えている。

2.3. EUROCRYPT 2022 の発表（4 日目）

・Anonymity of NIST PQC Round 3 KEMs [EUROCRYPT 2022]

Keita Xagawa

この論文では、NIST PQC 標準化の第 3 ラウンドに提出された KEM の全て

Classic McEliece、Kyber、NTRU、Saber、BIKE、FrodoKEM、HQC、NTRU Prime (Streamlined NTRU Prime and NTRU LPRime)、SIKE

を対象に方式の匿名性を調査している。これは、Grubbs, Maram, Paterson (EUROCRYPT 2022）の、NIST PQC 標準化の第 3 ラウンド方式の匿名性と頑健性を調査すべきであるという提案にこたえるものである。これらの結果は KEM のベースとなる公開鍵暗号方式の strongly disjoint-simulatable 性，KEM の強疑似ランダム性，smoothness/sparseness を主な技術として用いている。

得られた主な結果を以下に列挙する。

・NTRU は量子ランダムオラクルモデル(QROM)の下で、ベースとなる決定的 PKE が strongly disjoint-simulatable の性質を持てば匿名性をもつ。NTRU は QROM のもとで衝突困難性をもつ。NTRU を KEM とし、適切な DEM と組み合わせたハイブリッド PKE は匿名性と頑健性(robustness)をもつ。(BIKE、FrodoKEM、NTRU LPRime、SIKE に関しても同様の結果が確認されたが、HQC-128/256 については匿名性を持たないことが確認された)

・Classic McEliece はベースの PKE が strongly disjoint-simulatable であれば、それを KEM として適切な DEM と組み合わせたハイブリッド方式が QROM の下で匿名性を持つ。

・Grubbs, Maram, Paterson（EUROCRYPT 2022）は、Kyber と Saber の提案書内にある QROM の下での IND-CCA 安全性証明に瑕疵があることを指摘した。本論文では、Streamlined NTRU Prime にも QROM の下での IND-CCA 安全性証明に技術的

な問題があることを示している。

3. CRYPTO 2022 の発表

3.1. CRYPTO 2022 の発表（1 日目）

・Rotational Differential-Linear Distinguishers of ARX Ciphers with Arbitrary Output Linear Masks [CRYPTO 2022]

Zhongfeng Niu, Siwei Sun, Yunwen Liu, Chao Li

EUROCRYPT 2021 で提案された回転差分線形攻撃は、差分線形攻撃の差分部分を回転差分に置き換えて一般化したものである。EUROCRYPT 2021 では、Liu らが Morawiecki らの手法（FSE 2013）に基づき、出力線形マスクが単位ベクトルである特殊なケースについて、回転差分線形相関を評価する手法を発表した。この手法により、Friet、Xoodoo、Alzette に対して、出力線形マスクが単位ベクトルである強力な（回転）差分線形識別子がいくつか発見された。しかし、任意の出力マスクに対する回転差分線形相関をどのように計算するかは未解決であった。

本研究では、この未解決問題の一部を解決している。任意の出力線形マスクに対する算術加算の（回転）差分線形相関を計算する効率的なアルゴリズムを提示し、それを基に ARX 暗号の（回転）差分線形相関を評価する手法が導出された。本技術を Alzette、SipHash、Chacha、Speck に適用した結果、決定論的なものを含め、大幅に改善された（回転）差分線形識別子が確認された。本研究の成果は全て実用的であり、実験的に検証され、手法の有効性が確認された。さらに、FSE 2008、FSE 2016、CRYPTO 2020 で採用された ChaCha に対する実験的な識別子を説明することを試みている。予測された相関は実験的な相関に近いものであった。

・Superposition Meet-in-the-Middle Attacks: Updates on Fundamental Security of AES-like Ciphers [CRYPTO 2022]

Zhenzhen Bao, Jian Guo, Danping Shi, Yi Tu

中間一致攻撃アプローチは最も強力な共通鍵暗号解読技術の一つとして良く知られており、ハッシュ関数である MD4、MD5、Tiger、HAVAL、Haraka-512 v2 のフルラウンド構成に対する原像攻撃や、フルラウンドのブロック暗号 KTANTAN の鍵回復への応用で実証されている。攻撃が成功するには、プリミティブを 2 つの独立したチャンクに分離し、内部状態の各アクティブセルが 1 つのチャンクのみを表現するために使用される、もしくはそうでない場合に内部状態の各アクティブセルは混合されると使用不可能とみなされる。本論文では、そのようなセルの一部が線形的に混合され、独立した

セルと同様に有用であることが観察されている。これは、重ね合わせ状態の導入とそれに付随する一連の技術の導入につながり、Bao ら（EUROCRYPT 2021）と Dong ら（CRYPTO 2021）が提案した MILP ベースの探索フレームワークに組み込まれ、AES ライクのハッシュ関数やブロック暗号に幅広く応用できることが分かる。

・Triangulating Rebound Attack on AES-like Hashing [CRYPTO 2022]

Xiaoyang Dong, Jian Guo, Shun Li, Phuong Pham

リバウンド攻撃は FSE 2009 で Mendel らによって導入され、内部状態からの自由度を利用して、差分パスの重い中間ラウンドをフリーに実現することができる。インバウンドフェーズは Lamberger ら（ASIACRYPT 2009）と Gilbert と Peyrin（FSE 2010）が提案した Super-Sbox 技術により、2 ラウンドに拡張できることが知られている。また、Sasaki ら（ASIACRYPT 2010）は非フルアクティブな Super-Sbox と呼ばれる技術を導入し、攻撃に必要となるメモリ使用量をさらに削減した。

本論文では、新たにスーパーインバウンド技術を導入することで、これらの既存研究をさらに発展させる。この新しい技術では、内部状態と秘密鍵の自由度を最大限に活用することで、複数の 1 ラウンドまたは（非フルアクティブな）2 ラウンドの Super-Sbox インバウンドフェーズを接続する。この技術を応用して、いくつかの AES ライクなハッシュ関数で古典的または量子的な衝突を発見し、AES-128 と Skinny ハッシュモード、Saturnin-hash、Grostl-512 などをターゲットとして攻撃可能ラウンド数を 1～5 ラウンド向上させた。本攻撃の正しさを実証するため、古典的な設定において推定計算量 2^{24} の 6 ラウンド AES-128-MMO/MP に対する semi-free-start 衝突攻撃を実装し、標準的な PC で瞬時に衝突ペアを見つけることができた。

3.2. CRYPTO 2022 の発表（2 日目）

・Simon's Algorithm and Symmetric Crypto: Generalizations and Automatized Applications [CRYPTO 2022]

Federico Canale, Gregor Leander, Lukas Stennes

本論文では、Simon のアルゴリズムを適用して共通鍵暗号プリミティブを破る方法について理解を深める。一方で、新しい攻撃の探索を自動化する。このアプローチを用いると、5 ラウンド MISTY L-FK や 5 ラウンド Feistel-FK（内部置換付き）などの構成に対する初めての効率的な鍵回復攻撃を Simon のアルゴリズムで自動的に見つけることができる。また、Simon のアルゴリズムの一般化として、非標準的な Hadamard 行列を用いた研究を行い、周期以外の性質を持つ量子共通鍵暗号解読ツールの拡張を目指す。主な結果としては、いずれの一般化もそれを達成できないことであり、量子計算機で非標準的な Hadamard 行列を利用して共通鍵暗号プリミティブを破るには、根本

的に新しい攻撃が必要であると結論付けている。

・On the Impossibility of Key Agreements from Quantum Random Oracles [CRYPTO 2022]

Per Austrin, Hao Chung, Kai-Min Chung, Shiuan Fu, Yao-Ting Lin, Mohammad Mahmoody

ASIACRYPT 2020(先行版は ePrint 2018/1066)において細山田と山川が取り上げた以下の問題についての考察である：A、B はそれぞれローカルには量子的な計算能力を持つが、間の通信は古典的であるものとする。このとき、量子ランダムオラクルのみを用いて盗聴者に情報を漏らさない形での鍵共有を行うことができるか？

この論文は、上記の問題に初めて進展を与えた。具体的には、以下の 2 点を証明している。

・A、B の片方が古典、もう片方が量子の計算能力を持ち、合計d回のランダムオラクルへのアクセスを行った後に確率 1 で鍵共有を成功させる方式を仮定すると、盗聴者が$O(d^2)$回の古典的なランダムオラクルへのアクセスを行うことで共有鍵を復元する方法が存在する。

・A,B の両方がランダムオラクルへの量子的なアクセスが可能である場合には、盗聴者がpoly(d)回の古典的なランダムオラクルへのアクセスを行うことで共有鍵を復元する方法が存在する。ただしこのとき、2 値変数$\{\pm 1\}^N$上の全次数dの実多変数多項式に関するある「自然な」仮定を必要とする。これは、多項式fの変数x_iに関する influence と呼ばれる量を導入し、多項式f, gの全てのx_iに関する influence が$1/poly(d)$以下であるならば、その積$f(x) \cdot g(x)$を 0 とするような$x \in \{\pm 1\}^N$が存在するというものである。論文内では influence が指数関数的小さい場合の証明を与えており、その結果として盗聴者が$2^{O(md)}$回のランダムオラクルへの古典アクセスを行うことで共有鍵を復元する攻撃を与えている。ここで、mはランダムオラクルの出力長を示す。

以上のどちらの証明においても、盗聴者は古典である。次のステップとしては量子ランダムオラクルのもとでプロトコルが imperfect completeness を持つ場合においても同様の攻撃が可能であるかどうかを検証する問題が挙げられるが、この不可能性を示唆するひとつの結果を著者らは得ている。Aaronson-Ambainis により 2009 年に提出された「シミュレーション予想」が偽であるならば、量子ランダムオラクルモデルの下で古典的な盗聴者によっては鍵の復元が不可能なプロトコルが存在する。

・Some Easy Instances of Ideal-SVP and Implications to the Partial Vandermonde Knapsack Problem [CRYPTO 2022]

Katharina Boudgoust, Erell Gachon, Alice Pellet-Mary

Pan ら（EUROCRYPT'21）と Porter ら（ePrint 2021/600, arXiv:2105.03219）のイデアル格子問題､モジュール格子問題に対する subfield attacks の考え方を一般化し、最短ベクトル問題が容易となるようなイデアル格子を与えるためのシンプルな条件を与える。簡単に言えば、イデアルを固定する自己同型写像が多いほど、最短ベクトルの計算が容易となる。同様の観察はガロア体の素イデアルに対しては知られていたが、著者らは任意の数体の任意のイデアル（その素分解が分岐しない場合）に対して結果を一般化した。

暗号への応用として、patrial Vandermonde knapsack 問題(partial Fourier recovery problem という名でも知られる)の一部のインスタンスが多項式時間で解けることを示し、攻撃の実装と実験を行った。また、ランダムなインスタンスに対しても無視できない確率で格子次元が半分になることを示している。

・Breaking Rainbow Takes a Weekend on a Laptop [CRYPTO 2022, PQCrypto 2022]

Ward Beullens

この論文は NIST PQC 標準化の第 3 ラウンドにおける署名方式の Finalilsts に残った 3 つの署名方式のうちの一つである、多変数多項式署名 Rainbow の鍵回復攻撃を取り扱っている。Rainbow 仕様書では EIP 問題の HighRank 攻撃の計算量から NIST PQC 標準化の Call for Proposal にて指定されている計算困難性をみたすパラメータを求めていた。署名の効率化のために導入された UOV の繰り返し構造に含まれる、秘密鍵のなす部分空間の性質を用いることで指数時間ではあるものの大幅に計算時間を短縮した。具体的には第 2 ラウンド仕様書の SL1 パラメータの場合、標準的なノート PC により 3 時間半程度で成功率 1/15 の攻撃が動作することを確認しており、攻撃時間の期待値は 53 時間程度であると予想される。ただし、この論文で提案されている攻撃手法のみを用いた場合 SL3,SL5 のパラメータに対する攻撃時間は逆に増えてしまうが、Beullens の別の論文(Eurocrypt2021)で提案されている MinRank 攻撃との組み合わせにより合計の攻撃時間が 20 ビット程度下がるとしている。

3.3. CRYPTO 2022 の発表（3 日目）

・Simplified MITM Modeling for Permutations: New (Quantum) Attacks [CRYPTO 2022]

André Schrottenloher, Marc Stevens

中間一致攻撃とは､内部状態が 2 つの独立した経路(前方と後方)に沿って計算され、その後に照合されるという一般的なパラダイムである。近年では、EUROCRYPT 2021 で Bao らが提案した MILP モデルに代表されるように、既存攻撃を改良するために汎用ソルバーに詳細な攻撃モデルを解かせるといった手法が用いられるのが一般的とな

りつつある。

本論文では、汎用ソルバーへの入力として大幅に削減された攻撃表現と、任意の解に対して詳細な攻撃の存在と計算量を証明する理論分析を組み合わせた、よりシンプルなMILP モデリングを研究している。このモデリング手法により、広範なクラスの暗号学的置換に対する古典的攻撃と量子的攻撃の両方を発見することができる。最初に、SPONGENT ハッシュ関数の暗号学的置換を用いた PRESENT ライクな構成に対し、識別子の中間一致攻撃ステップを最大 3 ラウンド改善した。次に、AES ライクな設計に対し、提案モデルは Bao らのモデルよりもはるかに単純であるにもかかわらず、既存の最良な結果を再現することができる。唯一の制限は、キースケジュールから自由度を使用しないことである。さらに、このモデルは Feistel ネットワークのような、より多くの置換をターゲットとしても拡張できることを示す。そして、Simpira v2 や Sparkle の縮小版に対する新しい推測決定攻撃を行った。最後に、提案モデルを用いて、古典的な攻撃と同じラウンド数で、新しい量子的な原像および擬似原像攻撃（例：Haraka v2, Simpira v2, ...）を見つけることができることを示している。

・Improving Support-Minors Rank Attacks: Applications to GeMSS and Rainbow [CRYPTO 2022]

Pierre Briaud, Javier Verbel, Daniel Smith--Tone, Ray Perlner, Daniel Cabarcas, John Baena

多変数公開鍵暗号に対する Support-Minors(SM)法と呼ばれる新たな攻撃が近年発見された。特に、NIST PQC 標準化の第 3 ラウンド候補である GeMSS に対する Tao らの攻撃(CRYPTO2021)と、Rainbow に対する Beullens(EURPCRYPT2021)の攻撃により注目を集めている。

この論文では、SM 法におけるグレブナー基底の計算と解析について研究を行い、オリジナルの GeMSS および Øygarden(PQCrypto2021)による修正版に対する攻撃計算量を著しく下げ、単なるパラメータ修正では対処不可能であるという結論を得た。具体的な数値として、GeMSS128 のパラメータセットに対する推定攻撃計算量は 2^{72} であり、Øygarden の修正を施すことで署名生成の時間がオリジナルの GeMSS よりも 2^{14} 倍程度増えてしまうため現実的な運用が不可能であると考えられる。

アルゴリズム解析のもう一つの貢献として、SM 法を大規模に実装した場合，XL 法のメモリアクセスコストが問題となるが Block-Wiedemann アルゴリズムをサブルーチンとして用いることでコストが削減できることを示した。

Bernstein が NTRU Prime 仕様書(NIST PQC 標準化ラウンド 3 提出版)において示したメモリアクセスモデルの下で、Rectangular MinRank 攻撃を用いると Rainbow 仕様書内で提案されているすべてのパラメータに対して解読計算量を下げることができた。これは、Rainbow 開発チームが求めた攻撃計算量の下界と矛盾する結果であった

（https://troll.iis.sinica.edu.tw/by-publ/recent/response-ward.pdf）。

・Accelerating the Delfs-Galbraith Algorithm with Fast Subfield Root Detection [CRYPTO 2022]

Maria Corte-Real Santos, Craig Costello, Jia Shi

この論文では、超特異楕円曲線$E/\mathbb{F}_{p^2}$から部分体上の楕円曲線$E'/\mathbb{F}_p$への同種写像を求める新しいアルゴリズムを与えている。これは、一般的な超特異曲線同種写像問題に対する Delfs-Galbraith アルゴリズムのボトルネックとなるステップであった。高速化技術のコアとなるのは、計算コストの高い求根アルゴリズムを回避して多項式$f \in L[X]$が部分体$K \subset L$に根を持つかどうかを高速に判定する新たな手法である。特に、$f = \Phi_{\ell,p}(X, j) \in \mathbb{F}_{p^2}[X]$、つまり$f$が超特異 j 不変量で評価された$\ell$-th モジュラー多項式であるときに超特異楕円曲線と部分体上の楕円曲線を結ぶℓ-isogeny が存在するかどうかを効率的に判定する方法である。オリジナルの Delfs-Galbraith ウォークとの併用により多くのℓ-isogeny の近傍を調べることで、超特異楕円曲線のより多くの部分を同じ時間で探索することが可能となる。改良後のアルゴリズムの漸近計算量は $\tilde{O}(p^{1/2})$ であり、元の Delfs-Galbraith アルゴリズムと変わらないが、理論解析と実験の双方で部分体の探索時間が大幅に削減されたことを確認している。

以上の結果は同種写像ベース暗号に関する基本的な問題である一般的な超楕円曲線同種写像問題の計算困難性を新たな観点から見直すものである。

・Partial Key Exposure Attacks on BIKE, Rainbow and NTRU [CRYPTO 2022]

Andre Esser, Alexander May, Javier Verbel, Weiqiang Wen

部分鍵漏洩攻撃(Partial key exposure attack)のモデルでは、サイドチャネル攻撃などにより秘密鍵の一部のビット（情報消失モデル）や部分的に誤りを含んだビット（情報誤りモデル）が得られたと仮定して秘密鍵の完全復元を目指す。本論文の著者らは、耐量子計算機暗号のほとんどは漏洩した鍵の部分情報からの完全復元に耐性を持つという通説があるとしている。そして、実際に符号ベース暗号 BIKE、多変数公開鍵暗号 Rainbow、格子暗号 NTRU に対する部分鍵漏洩攻撃を構成することで、この通説に疑問を投げかけるものである。論文内で提案されている攻撃は、各暗号方式の秘密鍵が持つ冗長性、つまり鍵が格納されるメモリ内でのビット長と、鍵自体の持つエントロピーに大きな差があることを利用している。この性質を用いることで、鍵の僅かな部分情報から残りの部分を多項式時間で復元可能である。

実際の攻撃では多項式事件に拘る必要は無いため、より大きな消失率や誤り率の部分鍵からの復元が可能である。論文の見積もりによれば BIKE の場合、秘密鍵のビット半分から、または 1/4 がエラーのある場合でも2^{60}程度の攻撃計算量で復元可能である。この結果から、提案されている多くの耐量子計算機暗号では漏洩した部分鍵の情報に多

くのエラーが含まれていても鍵の完全な回復が可能であることを示している。

4. PQCrypto 2022 の発表

4.1. PQCrypto 2022 の発表（1 日目）

・How to Backdoor (Classic) McEliece and How to Guard Against Backdoors [PQCrypto 2022]

Tobias Hemmert, Alexander May, Johannes Mittmann, Carl Richard Theodor Schneider

本論文では、符号ベース暗号の一種である McEliece 暗号にバックドアを仕掛けることが可能であることを示す研究である。バックドア化された公開鍵は通常の公開鍵と区別がつかないが、秘密鍵を抽出する効率的なアルゴリズムが存在する。標準的な McEliece 暗号の鍵生成では、短い乱数シード δ を疑似乱数生成器（PRG）により拡張して秘密鍵とする。本論文のバックドアは、δ を暗号化した状態で公開鍵内に埋め込み、攻撃者はその情報を取り出すことで秘密鍵を再生成可能である。このとき、δ の暗号化自体にも McEliece 暗号を利用することが可能であるため、バックドアのセキュリティ自体も耐量子とすることができる。本論文の方法を用いることで、現在 NIST PQC 標準化の第 4 ラウンド候補となっている Classic McEliece 暗号へのバックドアの埋め込みも可能であり、悪意のある実装が広まる可能性がある。

Classic McEliece 暗号の提案書に規定されているように δ が秘密鍵の一部分として保存されるのであれば、疑わしい公開鍵と δ から再生成した公開鍵を比較することでこのようなバックドアの検出が可能である。以上により、McEliece 暗号の実装時には秘密鍵の一部として δ を格納し、バックドア対策の一環として δ を用いたチェックを行う機構を組み込む必要性を著者らは主張している。

・Efficiently Masking Polynomial Inversion at Arbitrary Order [PQCrypto 2022]

Markus Krausz, Georg Land, Jan Richter-Brockmann, Tim Güneysu

組込み機器に実装された暗号に対するサイドチャネル攻撃は大きな脅威であるにも関わらず、耐量子計算機暗号に関して安全な実装は見出されていない。本論文では、耐量子計算機暗号の主要な要素である多項式の逆元計算の効率的なマスク方法を提案している。技術的には多項式の情報を秘密分散の考え方でいくつかのシェアに分割し、シェア上において演算を行うことで多項式計算のマスクをおこなう。シェアの個数が$d+1$であるとき、マスキングの次数はdであるという。特に，$d=1$の場合を first-order masking と呼ぶ。このとき、加法的マスクと乗法的マスクを行うためのシェアの構成が

必要となるが、相互変換を行う効率的な方法、多項式の反転に対応するマスク演算を提案している。

Cortex-M4 上で格子暗号 Streamlined NTRU Prime と符号ベース暗号 BIKE の鍵生成に対応する多項式の逆元計算のマスクなし、ありの場合の実装と性能比較を行っている。first-order masking での実装において、マスキング無しの場合と比較して NTRU では 35%の、BIKE では 11%のオーバーヘッドにとどまった。また、Schneider らの提案した Test Vector Leakage Assessment(TVLA)評価法による first-order masking の安全性も検証されている。

・A Power Side-Channel Attack on the Reed-Muller Reed-Solomon Version of the HQC Cryptosystem [PQCrypto 2022]

Thomas Schamberger, Lukas Holzbaur, Julian Renner, Antonia Wachter-Zeh, Georg Sigl

この論文では、耐量子計算機暗号の一種である符号ベース暗号 HQC(Hamming Quasi-Cyclic)が取り上げられている。NIST PQC 標準化に提案された方式の第 2 ラウンドまでは復号に繰り返し BCH 復号器を用いていたが、第 3 ラウンド以降は公開鍵サイズの削減のため、Reed-Muller 符号と Reed-Solomon 符号を組み合わせたものへと変更となっており、それに合わせて解析も改良する必要がある。このタイプの復号器は藤崎-岡本変換後の平文チェックに用いられるため、草川ら(ASIACRYPT2021)、上野ら(TCHES2021)のサイドチャネル攻撃が脅威となると考えられていた。しかし、論文の著者らは HQC の Reed-Muller 復号器が最尤推定を用いたものであるため、復号距離の限界が設定されていないことから、上記の電力解析攻撃がうまく動かない可能性を指摘している。

この論文では、HQC の提案パラメータセットに対して秘密鍵の復元が可能な新たな攻撃を提案し、それが高確率で成功することを理論的にも実験的にも確認している。同様のテーマを扱った Guo ら(TCHES2022)の先行研究と比較して、必要な攻撃クエリ数は 1/12 であり、復号処理時間を知るためのタイミングオラクルの呼び出し回数が減ることでその不確実さを減らすことができる。また、著者らは ARM Cortex-M4 上での Reed-Solomon 復号器の実装と電力解析の実験を行い、漏洩した部分秘密鍵から Information Set Decoding アルゴリズムを用いて攻撃を行う場合の計算量評価を行っている。

・A New Key Recovery Side-Channel Attack on HQC with Chosen Ciphertext [PQCrypto 2022]

Guillaume Goy, Antoine Loiseau, Philippe Gaborit

この論文では、耐量子計算機暗号の一種である符号ベース暗号 HQC(Hamming

Quasi-Cyclic)が取り上げられている。NIST PQC 標準化に提案された方式が取り上げられている。符号ベース暗号の KEM のデカプセル化における復号処理ステップはサイドチャネル攻撃に対する脆弱性を持つことが知られており、そのフレームワークの中で HQC に対する攻撃、具体的には選択暗号文を用いた鍵回復攻撃が提案されている。攻撃の前提として、攻撃者が物理的にアクセス可能なデバイス上において、静的に割り当てられた秘密鍵が再利用されている状況を想定する。また、HQC の提案書にあるように、デカプセル化時の処理の効率化のため、Reed-Muller 符号の復号ステップにおいて高速 Hadamard 変換を用いた実装をターゲットとする。Hadamard 変換はその形から、入力の僅かな変化が出力の大きな変化を引き起こす diffusion property を持つため、サイドチャネル攻撃のターゲットとして利用しやすい。本論文では、処理中のデバイスからの電磁放射を計測し、線形分類器により Reed-Muller 符号の復号パターンを区別している。選択暗号文によるクエリを繰り返し情報を集めることで、秘密鍵の復元が可能となる。ARM Cortex M4 プロセッサと近接場マイクロプローブ ICR HH100-6 を用いた実験によれば、2 万回以下の実験で秘密鍵を全て復元することが可能である。また、攻撃への対策として、Hadamard 変換の線形性を利用しその入力cをランダムな$c_2, \ldots, c_n$を用いて$c = c_1 + c_2 + \cdots + c_n$を満たすように分解してから変換を行うという手法を提案している。

4.2. PQCrypto 2022 の発表（2 日目）

・A New Fault Attack on UOV Multivariate Signature Scheme [PQCrypto 2022]

Hiroki Furue, Yutaro Kiyomura, Tatsuya Nagasawa, Tsuyoshi Takagi

本論文では、耐量子計算機暗号の一種である unbalanced oil and vinegar 型の多変数多項式署名の故障利用攻撃について取り上げている。署名の秘密鍵を構成する中心写像F（多変数二次関数）と線形写像Tはメモリの固定された領域に保存されているが、署名生成時にFまたはTの係数のうちどれかひとつがランダムに変化するような故障注入が可能であるという状況のもとに攻撃方法を提案している。具体的には、ランダムに選んだ平文に対してTを変化させた秘密鍵を用いて署名を生成し、連立方程式として解くことで線形写像Tの部分情報を復元、続いてFを変化させた秘密鍵を用いて署名を生成してFの部分情報を復元する。

復元した部分情報から、元の問題をよりサイズの秘密鍵復元問題へと変換することが可能であり、既存の秘密鍵復元アルゴリズムにより完全に鍵を復元することができる。100 ビットセキュリティを持つパラメータに対する攻撃実験の結果、80-90%の確率で 5 個の変数を、70%の確率で 10 個の変数を復元することが可能であり、前者の場合には 10 ビット程度安全性が下がることになる。

・Improvement of Algebraic Attacks for Superdetermined MinRank [PQCrypto 2022]

Magali Bardet, Manon Bertin

この論文では、暗号学的な応用の観点から MinRank(MR)問題を取り上げている。Verbel ら(PQCrypto 2019)は多変数連立方程式の解が大量に存在する問題のクラスに対して、Overdetermined system(過剰決定系)よりも解が多いという意味を込めて Superdetermined system という用語を与えた。そして、双線形 Kipnis-Shamir (KS) modeling をベースに、Superdetermined な MinRank 問題を解く新しい方法を提案した。その後、Barder ら(ASIACRYPT 2020)はカーネル変数の Plücker 座標(KS modeling におけるカーネル行列の maximal minor)を考えることにより、新たな Support Minors modeling を導入した。

この論文では、任意のインスタンスに対して KS modeling と SM modeling の間のリンクについて代数的な説明を完全に与える。そして、superdetermined な MinRank インスタンスは SM modeling の簡単なインスタンスとみなすことができることを示す。特に、次数落ちが生じる次数(the “first degree fall”)と変数の数をできるだけ少なくして計算を進めることが、必ずしも最良の戦略ではないことを示す。また、一般的なランダムインスタンスに対する計算量評価も与える。

以上の結果を、NIST PQC 標準化の第 1 ラウンドに提出された符号ベース暗号 DAGS に適用し、Barelli と Couveur(ASIACRYPT 2018)により提案され、その後 Bardet ら(CBC2019)により改良された代数攻撃が、superdetermined な MinRank インスタンスであることを確認した。このインスタンスは一般的なものではないが、適切な解析を行うことで解くための最適なパラメータ（shortened positions の個数）を選択することが可能な実例となっている。

・Breaking Category Five SPHINCS+ with SHA-256 [PQCrypto 2022, Best Paper Award]

Ray Perlner, John Kelsey, David Cooper

NIST PQC 標準化の Selected Algorithms 2022 で選ばれた署名方式 3 件のうちの 1 つである SPHINCS+に対する攻撃である。署名の EUF-CMA 安全性はハッシュ関数のいくつかの性質を満たすと仮定して証明されるが、その中のひとつであり、第二原像攻撃を緩和した DM-SPR(distinct-function multi-target second-preimage resistance)という性質を SHA-256 が持たないことが指摘されていた（Sydney Antonov, 2022/04/21）。これが実際の署名の偽造につながるかどうかは未知であった。この論文の攻撃では $WOTS^{+}$公開鍵からワンタイムキーを生成、ハイパーツリーを改変することで任意のメッセージに対して有効な署名を作り出すことが可能となる。偽造に必要な計算時間は仕様書に書かれていたものよりも 40 ビット程度低くなる。

4.3. PQCrypto 2022 の発表（3 日目）

・Quantum Attacks on Lai-Massey Structure [PQCrypto 2022]

Shuping Mao, Tingting Guo, Peng Wang, Lei Hu

Aaram Yun らは、Lai-Massey 構造が Feistel 構造と同等の安全性を有すると考えた。しかし、Luo らは、3 ラウンドの Lai-Massey 構造が、Feistel 構造とは異なる Simon アルゴリズムの量子攻撃に耐性があることを示した。本研究では、典型的な Lai-Massey 構造に対する量子攻撃を行う。その結果、3 ラウンドの Lai-Massey 構造に対する量子 CPA 識別子と、Feistel 構造と同じ 4 ラウンドの Lai-Massey 構造に対する量子 CCA 識別子が存在することが示された。Lai-Massey 構造に対する攻撃を quasi-Feistel 構造に対する攻撃へと拡張する。quasi-Feistel 構造の結合（combiner）が線形である場合、3 ラウンドの balanced quasi-Feistel 構造に対する量子 CPA 識別子と、4 ラウンドの balanced quasi-Feistel 構造に対する量子 CCA 識別子が存在することを示す。

・Attack on SHealS and HealS: the Secdond Wave of GPST [PQCrypto 2022]

Steven D. Galbraith, Yi-Fu Lai

この論文では、Fouotsa と Petit(ASIACRYPT 2021)による同種写像ベースの公開鍵暗号 SHealS、HealS、および鍵交換方式 HealSIDH への攻撃を行っている。問題の背景として、static-static な暗号プロトコル、つまり、両者が鍵を変更することなく静的に保持しながら安全にプリミティブを実行可能であるようなものの構成を取り上げている。CSIDH を用いた同種写像ベースの暗号ではこれが可能であったが、その後 Kuperberg により準指数時間での攻撃が発見された。SIDH はより強固な基盤ではあるが、同種写像ベースの強力な計算量的仮定から効率的なプロトコルを構成することは引き続き取り組むべき問題となっている。

Galbraith らによる adaptive GPST 攻撃の存在が、SIDH 系の方式が static-static な性質を持つことを困難にしている。この攻撃では、ボブが悪意を持つ場合にはハンドシェイクの情報から相手のアリスの秘密鍵を抜き出すことが可能である（当然、逆にアリスがボブの秘密鍵を抜き出すことも可能となる）。対策としてはゼロ知識証明の埋め込みや k-SIDH 法の利用が知られているが、複数の同種写像の計算を並列に行うことが必要とされ、実用的ではない。

Fouotsa と Petit(ASIACRYPT 2021)はこの問題の解決として、同種写像間の可換図式を応用した新しい鍵検証機構をもつ SIDH の変種を与えている。この方式は、素数長を 2 倍にした SIKE よりも少ない同種写像計算で、他の既知の解決策よりもはるかに効率的である。さらに、適応的な攻撃者に対して安全な static-static な鍵交換と公開鍵暗号が得られることが主張されている。

この論文では、Fouotsa と Petit のプロトコルに対して適応的な攻撃を構成することで、彼らの主張に反論する。この攻撃を可能とする背景には、Fouotsa と Petit が SHealS、HealS、HealSIDH の構成に用いた鍵検証機構の脆弱性の発見がある。この攻撃は GPST 攻撃の微調整であり、クエリー数の観点からいえば SIDH に対する GPST 攻撃と同じである。つまり、Fouotsa と Petit のプロトコルは追加の鍵検証機構により効率が下がったのみで、安全性の向上を与えていないという結論を与えている。

5. FDTC 2022 の発表

・FA-LLLing for RSA: Lattice-based Fault Attacks against RSA Encryption and Signature [FDTC 2022]

Guillaume Barbu

Cao et al. (CT-RSA 2022)により提案された、故障注入攻撃により得られた情報から Hidden Number Problem のインスタンスを生成し、格子基底簡約により解くことで秘密情報を復元する新たな攻撃を取り扱う。この論文では、Cao らの方針に従い、RSA 暗号と RSA-CRT 署名に対する新たな故障注入攻撃を提案している。具体的には、暗号化処理中のm^eの繰り返し二乗法による計算の最終段階においてハードウェアの誤動作を引き起こし、連続した下位$l = 32,64,128$ビットをランダムに反転させる。実験では 2 個の暗号文から平文が、2 個の署名からNの素因数分解が導出可能な事が示されている。

6. CHES 2022 の発表

6.1. CHES 2022 の発表（1 日目）

・Guessing Bits: Improved Lattice Attacks on (EC)DSA with Nonce Leakage [CHES 2022]

Chao Sun, Thomas Espitau, Mehdi Tibouchi and Masayuki Abe

この論文では、(EC)DSA および Schnorr ライクな署名スキームへのサイドチャネル攻撃を取り扱う。nonce は署名生成時に用いられる使い捨ての乱数であるが、ECDSA などではその一部分が漏洩すると格子基底簡約を用いた攻撃により秘密鍵が復元されることが 20 年前から知られていた(Howgrave-Graham and Smart, DCC 2001)。サイドチャネル攻撃により nonce の部分情報を得ることが可能であるためこの攻撃の実現可能性に関する議論が、格子基底簡約の性能の進展と新たな解析手法の適用を中心に続けられていた。

著者らは既知の格子攻撃に現れる BDD(Bounded Distance Decoding)問題の計算の一部分を総当たりにより処理することで、複数個のより簡単な BDD 問題のインスタンスへと変換する。変換後の問題は復号距離の上限は同じであるが、格子体積が大きいため元のインスタンスよりもはるかに簡単なものとなる。また、このときに現れる格子は同一のものでターゲットベクトルのみが異なるため、実際の攻撃においては格子基底を事前に簡約しておき、nonce に合わせてターゲットベクトルを変更することでさらなる効率化が可能である。結果として、現在知られている攻撃可能な範囲（位数 160 ビットの ECDSA における 2 ビット漏洩、位数 256 ビットの ECDSA における 3 ビット漏洩）と同等の性能かそれ以上の性能を持つことが確認された。
TPM-FAIL データセットを用いた実験では、攻撃に必要な署名数を 40,000(Jancar et al., CHES 2020)から 800 に削減している。

6.2. CHES 2022 の発表（2 日目）

・Practical Multiple Persistent Faults Analysis [CHES 2022]

Hadi Soleimany, Nasour Bagheri, Hosein Hadipour, PrasannaRavi, Shivam Bhasin and Sara Mansouri

本論文では、multiple persistent faults analysis に着目する。これは、様々なシナリオにおいてこの解析手法を適用した場合に既存研究では多くのギャップが存在することが明らかとなっているため、このギャップを埋める必要性があると考えたからである。主な貢献は次の 2 つである。最初に、著者らは、multiple persistent faults 設定において適用可能な persistent fault を適用するための新しい技術を提案する。この設定では、生き残った秘密鍵とそのために必要なデータ量を減らすことに焦点を当てる。まず、AES に対する persistent fault analysis を実行するために 8 個の faults と 16 個の faults が存在することを考える。この時、生き残った秘密鍵の候補数をわずか 2^9 に減らすために、既存の最良な攻撃ではそれぞれ 2008 個と 1643 個の暗号文を必要とするのに対し、提案手法ではそれぞれ 1509 個と 1448 個の暗号文があれば良いことを示している。なお、計算量はいずれも 2^{50} である。次に、暗号文単独モデルにおいて秘密鍵を回復する一般化されたフレームワークを開発している。この方法は persistent fault analysis と鍵回復プロセスの両方の実行に対して大いに柔軟で、必要な暗号文の量と計算量の間の一般的なトレードオフを提供している。Sbox において 16 個の persistent faults を有する AES を破るために、提案手法は現実的な計算量の範囲内で、必要な暗号文の量を 477 個まで減らせることを示している。この手法の正確さを確認するために、2 つの有名なブロック暗号である AES と LED への electromagnetic fault injection で数回のシミュレーションと、ARM Cortex-M4 マイクロコントローラでの実験検証を行った。なお、AES と LED は実際に fault の種類と fault の数の分布を検証するのに

適したブロック暗号として知られている。

7. TCC 2022 の発表

・Post-Quantum Insecurity from LWE [TCC 2022]

Alex Lombardi, Ethan Mook, Willy Quach, Daniel Wichs

本論文では、多くの基本的な暗号プリミティブについて learning-with-errors (LWE) 仮定の下で古典的な安全性が証明されたとしても、耐量子の安全性は保障されないことを示す。つまり、LWE 自体の耐量子性は広く信じられているが、それ自身の安全性以外のものは何も保証されない。耐量子安全な仮定を用いたとしても、そこから構成される暗号方式の内部では量子的な安全性が破られる可能性があることを示している。

具体的には、人工的な構成ではあるものの疑似ランダム関数、CPA-安全な共通鍵暗号、MAC、署名、CCA-安全な公開鍵暗号で、LWE 仮定のもとで古典的に安全であることがブラックボックス帰着により示されるが、量子的な攻撃に対しては安全ではないものを構成した。これらの構成はすべてステートレス、非対話的なものであるが、安全性の定義には対話的なゲームベースの証明で、攻撃者が方式へのクエリを可能なものを考えている。量子多項式時間攻撃者は古典的なクエリを数回行うのみで方式を破ることが可能である。技術的には、対話型証明を安全性証明のゲームに注意深く埋め込むことで主張を示している。

先行研究においてはステートフルな方式、対話型プロトコルに対して同様の研究がおこなわれており、ブラックボックス安全性証明をもつ、ステートレスもしくは非対話型の暗号方式については、方式に対する量子攻撃が仮定に対する量子攻撃に帰着されるはずであると考えられてきたが、本論文はそれが間違いであることを示している。

本論文の別の結果として、古典的な送信者と受信者の間での 3 ラウンドの "quantum disclosure of secrets（QDS）"プロトコルに関するものがある。受信者が量子的であった場合、3 ラウンド目には受信者は秘密メッセージを知ることができるが、古典の場合には LWE 仮定のもとでそれを知ることができない。

・The Parallel Reversible Pebbling Game: Analyzing the Post-Quantum Security of iMHFs [TCC 2022]

Jeremiah Blocki, Blake Holman, Seunghoon Lee

この論文では、古典的な（並列）石移動ゲーム（以下、pebbling ゲーム）を取り扱う。ひとつの応用として性的なデータ依存グラフ(DDG)を持つ関数fの評価に必要なリソース（空間、時空間、累積空間）の分析がある。暗号分野で特に興味深いのは、有向非巡

回グラフ（DAG）Gと暗号学的ハッシュ関数Hによって定義される data-independent memory-hard 関数(iMHF)$f_{G,H}$の解析である。グラフGの pebbling 計算量は、$f_{G,H}$を複数回評価する場合のコストや、関数$f_{G,H}$の定義域Xが固定された場合の総当たりの原像攻撃の総コストを特徴づける。定義域の濃度を$|X| = m$とすると、古典的な攻撃者は原像を計算するために関数$f_{G,H}$を、少なくともm回評価する必要がある一方で、Grover のアルゴリズムを実行する量子攻撃者は関数$f_{G,H}$を計算する量子回路$C_{G,H}$への、$O(\sqrt{m})$回のブラックボックスアクセスのみで済む。そのため、量子攻撃のコストを分析するためには、量子回路$C_{G,H}$の時間-空間計算量（回路の幅×深さに等しい）を調べることが重要となる。

論文音議論ではまず、古典的な計算ではグラフGに対する効率的な pebbling 戦略は$f_{G,H}$を妥当な計算コストで評価するアルゴリズムに対応するが、量子の場合には妥当な計算コストを持つ量子回路には対応しないことを指摘する。その上で新たに、量子力学における No-deleting 定理に対応する制限を課した、並列可逆（reversible）pebbling ゲームを導入する。新たなゲームの可逆時間-空間計算量を代表的なグラフのクラス（line graph、Argon2i-A、Argon2i-B、DRSample）に対して解析し、以下の結果を得ている。

(1) サイズNの line graph の可逆時間-空間計算量が最大 $O(N^{1+2/\sqrt{\log N}})$ である
(2) 任意の (e,d)-簡約可能な DAG に対して、可逆時間-空間計算量が $O(Ne + dN2^d)$ であることを示した。特に、Argon2i-A と Argon2i-B の可逆時空間計算量はそれぞれ最大 $O(N^2 \log\log N/\sqrt{\log N})$、$O(\frac{N^2}{(\log N)^{1/3}})$である。
(3) DRSample に対しては、可逆時間-空間計算量が最大$O(N^2 \log\log N/\log N)$であることを示した。

最後に、Alwen and Blocki の depth-reducible グラフに対する（非可逆）pebbling 攻撃を拡張し、可逆 pebbling の累積 pebbling コストについて研究している。

8. ASIACRYPT 2022 の発表

8.1. ASIACRYPT 2022 の発表（1 日目）

・Latin Dances Reloaded: Improved Cryptanalysis against Salsa and ChaCha, and the proposal of Forró [ASIACRYPT 2022]

Murilo Coutinho, Iago Passos, Juan Grados, Fábio de Mendonça, Rafael Timóteo, Fábio Borges

本論文では、ARX 暗号、特にストリーム暗号の Salsa/ChaCha ファミリーに対する

4 つの主要な貢献を紹介する。

ChaCha に対する差分線形識別子の改善について提案する。この提案に向けて、アルゴリズムをより単純なサブラウンドの観点から見ることにより、線形近似の導出にアプローチする新しい方法を提案する。このアイデアを使用すると、既存研究で得られた全ての線形近似を 3 つの単純なルールから導き出すことが可能であることを示す。さらに、もう 1 つのルールを追加することで、EUROCRYPT 2021 で Coutinho と Souza が提案した線形近似を改善できることを示す。

Salsa に対する攻撃を改善するため、双方向線形拡張（BLE: Bidirectional Linear Expansions）と呼ばれる技術を提案する。既存研究では、ラウンドに前進する線形拡張のみを検討していたが、BLE では 1 ビットを前進と後退の両方向に拡張することが検討されている。BLE を適用して、7 ラウンドと 8 ラウンドの Salsa に対する最初の差分線形識別子を提案するとともに、8 ラウンドの Salsa に対する PNB を用いた鍵回復攻撃を改善する。

これらの暗号に対する暗号解析の研究から得られた全ての知識を用いて、ラウンドごとの拡散と暗号解析への耐性を向上させるためのいくつかの修正を提案し、新しいストリーム暗号 Forró を完成させた。これにより、安全性を維持したままラウンド数を減らすことができ、多くのプラットフォーム、特に制約のあるデバイスにおいて、より高速な暗号を実現すること可能となる。

さらに著者らは、複数の GPU を備えた高性能環境で使用可能な Salsa、ChaCha、Forró のための新しい暗号解析ツールを開発した。このツールを CryptDances と呼ぶ。CryptDances では、差分相関の計算、ChaCha の新しい線形近似の自動導出、PNB 攻撃の計算量の見積の自動化などが可能になっている。

・Algebraic Meet-in-the-Middle Attack on LowMC [ASIACRYPT 2022]

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

本論文では、部分的な非線形層の特徴を利用し、LowMC の安全性を解析するために代数的な中間一致攻撃（MITM）という新しい手法を提案している。これにより、単純な差分列挙攻撃のメモリ計算量を最先端技術よりも削減することが可能となる。さらに、LowMC の差分トレイルから完全な秘密鍵を取得する効率的な代数的手法が CRYPTO 2021 で提案されているが、その計算量は秘密鍵のサイズに対して依然として指数関数的であった。本研究では、トレイル内に十分な数のアクティブ S-box が存在する場合、これを定数時間にまで短縮する方法を示している。上記の新技法により、CRYPTO 2021 で発表された LowMC および LowMC-M に対する攻撃はさらに改善され、一部の LowMC インスタンスを初めて破ることができた。

・Enhancing Differential-Neural Cryptanalysis [ASIACRYPT 2022]

Zhenzhen Bao, Jian Guo, Meicheng Liu, Li Ma, Yi Tu

CRYPTO 2019 で Gohr は、十分に訓練されたニューラルネットワークが、従来の差分識別子よりも優れた暗号解読の識別タスクを実行できることを示した。さらに、型破りな鍵推測戦略を適用することで、最新のブロック暗号 Speck32/64 に対する 11 ラウンドの鍵回復攻撃を行い、公表されている最先端の結果を改善した。このことから、次のような疑問が浮かぶ：機械学習（ML）は従来手法に対してどの程度の優位性があるのか、また、現代暗号の暗号解読においてその優位性は一般的に存在するのか？

本論文では、最初の疑問に対する答えとして、12 ラウンド以上の Speck32/64 に対して、ML を用いた鍵回復攻撃を考案した。その結果、改良型 12 ラウンド攻撃と、初の実用的な 13 ラウンド攻撃を達成した。この成果において本質的な点は、ML ベースの攻撃における古典的な要素、すなわちニュートラルビットを強化することにある。2 番目の質問に対しては、ラウンドを削減した Simon32/64 に対する様々なニューラルネットワーク識別子を生成し、純粋な差分ベースの識別子との比較を行った。

・SwiftEC: Shallue--van de Woestijne Indifferentiable Function to Elliptic Curves [ASIACRYPT 2022]

Jorge Chávez-Saab, Francisco Rodríuez-Henríquez, Mehdi Tibouchi

本論文では、任意の値を楕円曲線上の点にハッシュ化する方法について取り上げる。ANTS-VII の Shallue と van de Woestijne 以降多くの提案がなされてきたが、ハッシュ関数の望ましい性質として、

・有限体上の任意の楕円曲線上に適用可能

・基礎体上のランダムオラクルとの合成において、楕円曲線上のランダムオラクルと indifferentiable である

という 2 点を持っているものはこれまで存在しなかった。

Brier らの基礎研究(CRYPTO 2011)以来様々なアプローチが提案されている。Shallue-van de Woestijne (SW)写像$f: \mathbb{F}_q \to E(\mathbb{F}_q)$と 2 つのランダムオラクルを用いたものがあったが、コスト面で不利であった。最近、Koshelev (DCC 2022)は indifferentiable なハッシュ関数でスカラー倍算の回数が 1 回で済むものを提案したが、特殊なクラスの楕円曲線にしか適用できなかった。

本研究はこの未解決問題を取り扱い、広範囲の楕円曲線に対し 1 回のスカラー倍算で indifferentiable なハッシュ関数を構成することに成功している。技術的には、SW 写像を 1 パラメータ族$(f_u)_{u\in\mathbb{F}_q}$に拡張し、独立なランダムオラクルH, H'を用いた$F: m \mapsto f_{H'(m)}(H(m))$が、ランダムオラクルと区別不可能であること示している。また、任意の楕円曲線の点を一様に近いランダム文字列として表現する Tibouchi (FC 2014)の

Elligator Squared 技術は、本論文のアプローチを用いて改良することが可能である。

・Full Quantum Equivalence of Group Action DLog and CDH, and More [ASIACRYPT 2022]

Hart Montgomery, Mark Zhandry

暗号学的群作用は、標準的に暗号に用いられる群の条件を緩和し、その構造を簡素化することで Shor のアルゴリズムのような群構造を利用する量子アルゴリズムへの耐性を獲得したものである。楕円曲線上の同種写像から構成されるものが最も有名であり、多くの応用を持つ。

本論文では、群作用上の離散対数問題(DLog)と Computational Diffie-Hellman(CDH)問題の困難性について取り扱う。主結果として、アーベル群上の作用に関して CDH と DLog は量子的に等価であることを証明している。2018 年の Galbraith らの結果では、CDH を成功率 1 で解くアルゴリズムによる離散対数問題の解法を示すことで量子的な等価性を示しているが、実用的には成功率が 1 よりも小さい、non-negligible な成功率の場合に興味があり、この論文はその問題に答えていることになる。

・Cryptographic Primitives with Hinting Property [ASIACRYPT 2022]

Navid Alamati, Sikhar Patranabis

Hinting PRG は、PRG のシードに関する循環安全性（circular security）の「決定論的」な形式を持つ PRG の（潜在的に）より強い亜種である（Koppula and Waters, CRYPTO 2019）。ヒンティング PRG は、多くの暗号アプリケーション、特に CCA 安全な公開鍵暗号とトラップドア関数を可能にする。本論文では、Hinting 性質を持つ暗号プリミティブを研究し、以下の結果を得ている。

・Hinting PRG の設計において、巡回群や同種ベースの群作用に対するある種の決定論的仮定から、より概念的に単純な新規のアプローチを提示することで、既存のアプローチと比較してより単純な安全性証明を可能にした。

・Hinting 性質を弱 PRF に自然に拡張した Hinting 弱 PRF を導入し、任意の Hinting 弱 PRF から循環もしくは KDM 安全な共通鍵暗号を実現する方法を示す。Hinting PRG を構築するための単純なアプローチは、同じ決定論的仮定の集合から Hinting 弱 PRF を実現するために拡張できることを実証する。

・Hinting 性質の強化版である機能的 Hinting 性質を提案し、秘密のシードや鍵の関数に関するヒントが存在する場合でも安全性を保証する。本論文では、平易な Hinting PRG および Hinting 弱 PRF を実現するための簡単な技術を基に、特定の関数（族）に対する機能的な Hinting PRG および Hinting 弱 PRF を実現する方法を示す。また、ある種の代数的特性を持つ帰納的 Hinting 弱 PRF が、ブラックボックス方式で KDM 安全な公開鍵暗号を実現する上で適用可能であることを実証する。

・最後に、ランダムオラクルだけが与えられたこれらのプリミティブの単純な実現を使って、Hinting 弱 PRF（および Hinting PRG）を公開鍵暗号からブラックボックス的に分離できることを示す。

・A New Isogeny Representation and Applications to Cryptography [ASIACRYPT 2022]

Antonin Leroux

本論文は新たな同種写像の表現について議論している。この表現は、同種写像の評価方法と、同種な超特異楕円曲線（具体的には、超特異楕円曲線E_1, E_2とその間の次数Dの巡回同種写像の３つ組の集合）からなる言語の所属判定により定義される。この同種写像の評価と所属判定は、署名の構築や暗号鍵の検証など、いくつかの基本的な暗号学的応用があることが知られている。本論文の前半では、同種写像についての既知の結果を言語と証明の枠組みで再解釈し、同種な超特異楕円曲線の所属判定問題が NP 問題に属することを Deuring 対応から自然に導く。

論文の主な結果として、（大きな）素数次数を対象として、新たに部分整環の表現を構成した。同種写像の codomain に対応する自己準同型環の部分整環を適切に取り、その中から滑らかなノルムをもつものを見つけ出すところが構成方法における主要な部分である。

提案した新たな表現手法により、同種写像ベース暗号の安全性の根拠となる新たな計算問題、SubOrder to Ideal Problem (SOIP)が定義される。

ひとつの応用として、部分整環の表現をベースとした新しい非対話型鍵交換(Non-Interactive Key Exchange, NIKE)である pSIDH を提案している。また、部分整環の表現を用いた計算を効率的に行うため、いくつかのヒューリスティックなアルゴリズムを提案している。

・Group Action Key Encapsulation and Non-Interactive Key Exchange in the QROM [ASIACRYPT 2022]

Julien Duman, Dominik Hartmann, Eike Kiltz, Sabrina Kunzweiler, Jonas Lehmann, Doreen Riepel

同種写像暗号 CSIDH(Commutative Supersigular Isogeny Diffie-Hellman)を抽象化した暗号学的群作用は耐量子計算機暗号の文脈から注目を集めている。この論文では、過去に提案された群作用ハッシュ ElGamal KEM(GA-HEG KEM)と群作用ハッシュ Diffie-Hellman 非対話型鍵交換(GA-HDH NIKE)の 2 つの暗号方式の安全性について再検討を行う。後者は特に Post-Quantum WireGuard (IEEE S&P 2021) や OPTLS (ACM CCS 2020) などでの実利用が検討されている。

これらの 2 つのプロトコルは、量子ランダムオラクルモデル(QROM)の下で active security は群作用強 CDH 問題（Group Action Strong CDH）の変種で、DDH オラク

ルへの任意の量子アクセスを仮定する問題の困難性に依存することが示された。さらに、古典での強 CDH 仮定（DDH オラクルにアクセス可能な攻撃者が CDH を解けないという仮定）により、QROM の下での安全性が示されるようなプロトコルの変種を提案している。最初の変種は key confirmation を必要とするため、KEM にしか使えない。第二の変種は Cash ら(EUROCRYPT '08)の手法に基づいており、かなり効率がわるいが QROM の下で CDH 仮定から actively secure な同種写像ベースの非対話型鍵交換が初めて構成できたことになる。

・Horizontal Racewalking Using Radical Isogenies [ASIACRYPT 2022]

Wouter Castryck, Thomas Decru, Marc Houben, Frederik Vercauteren

この論文では、Castryck ら(ASIACRYPT2020)が取り上げた、有限体上の楕円曲線の間の、固定された小次数の long chain の計算における radical isogeny の利用に関する 3 つの未解決問題について考察を行っている。

まず、与えられた次数Nの radical isogeny formula を求めるための補間手法を示すことで、大きな関数体上での多項式の因数分解を回避する。この方法により、$N \leqq 13$の範囲でしか求められていなかった radical isogeny formula を$N \leqq 37$の範囲まで拡張した。次に、既知の手法とアドホックな操作の組み合わせにより、N≤19 に対して公式の最適化バージョンを導き出し、2020 年に得られた計算方法よりも 2 倍以上高速化した。第三に、$p \equiv 7 \pmod 8$の場合の$\mathbb{F}_p$上の、曲面に沿った超特異楕円曲線間のウォーク（$\mathbb{F}_p$上の自己準同型環が$\mathbb{Z}[\frac{1+\sqrt{-p}}{2}]$となる超特異楕円曲線の間の同種写像）において、radical isogeny を正しく選択する問題を解決した。これはNが偶数の場合非自明であり、$N = 4$の場合ですら PKC2022 で Onuki と Moriya によって初めて解決されている。著者らは、Nが偶数の場合の予想を建て、$N \leq 14$に対してそれを証明している。これらの手法により、次のように CSIDH の実質的な高速化が得られた：16-isogeny 用いて、512 ビットの素体上での 2-isogeny の long chain の計算が 3 倍高速に、radical isogeny を用いた CSIDH の実装が 12%程度高速化された。

8.2. ASIACRYPT 2022 の発表（2 日目）

・Revisiting Related-Key Boomerang Attacks on AES Using Computer-Aided Tool [ASIACRYPT 2022]

Patrick Derbez, Marie Euler, Pierre-Alain Fouque, Phuong Hoa Nguyen

近年、ブロック暗号のブーメラン識別子やブーメラン攻撃を自動的に探索するために、いくつかの MILP モデルが導入されている。しかし、これらはキースケジュールが線形である場合にのみ使用可能である。ここでは、AES のような非線形のキースケジュー

ルを有するブロック暗号に対して、新しいモデルを導入する。このモデルはより複雑であり、網羅的な探索には時間がかかりすぎる。しかしながら、ソルバーにいくつかのヒントを追加することで、計算量 2^{124}、データ量 2^{124}、メモリ量 $2^{79.8}$ で AES-192 に対する現在最高の関連鍵ブーメラン攻撃が実行できることを示す。これは、ASIACRYPT 2009 で Biryukov と Hovratovich による攻撃の計算量（それぞれ 2^{176}、2^{123}、2^{152}）よりも優れている。特に、計算量とメモリ量において大きな改善を与えており、これは暗号解読における MILP の威力を示している。

・Synthesizing Quantum Circuits of AES with Lower T-depth and Less Qubits [ASIACRYPT 2022]

Zhenyu Huang, Siwei Sun

量子アルゴリズムによる暗号解読に必要な資源を正確に見積もるためには、量子アルゴリズムを基本的な量子ゲートで構成される量子回路に帰着する必要がある。本研究では、Grover と Simon のアルゴリズムに基づく量子攻撃でよく用いられる反復型共通鍵暗号の量子オラクルを実装する回路について、いくつかの汎用的な合成技術と最適化技術が提案された。まず、ブロック暗号のラウンド関数を in-place に実装するための一般的な構造を提案する。次に、線形および非線形な暗号構成要素の効率的な量子回路を合成するための新しい技術が導入される。これらの技術を AES に適用し、深さ-幅のトレードオフ（depth-width tradeoff）の戦略が系統的に調べられる。その過程で、AES の S-box の古典的回路に関する新しい知見に基づいて、証明可能な最小の T-depth を持つ量子回路が導出されている。その結果、AES の量子回路の実装に必要な T-depth と幅（量子ビット数）が大幅に削減された。著者らの回路と EUROCRYPT 2020 で提案された回路と比較すると、幅を増やさずに T-depth を 60 から 40 に、あるいは幅をわずかに増やして 30 に減らすことに成功している。これらの回路は、Microsoft Q#で実装されており、ソースコードも公開されている。ASIACRYPT 2020 で提案された回路と比較すると、著者ら回路の 1 つは幅が 512 から 371 に減少し、同時に Toffoli-depth が 2016 から 1558 に減少していることが確認されている。また実際、深さを増やす代わりに、幅を 270 に減らすことができる。さらに、深さと幅のトレードオフの全範囲が提供され、AES の量子回路の合成と最適化における新記録も樹立されている。

・Exploring SAT for Cryptanalysis: (Quantum) Collision Attacks against 6-Round SHA-3 [ASIACRYPT 2022]

Jian Guo, Guozhen Liu, Ling Song, Yi Tu

本研究では、古典的および量子的な設定における SHA-3 ハッシュ族のインスタンスに対する衝突攻撃に焦点を当てる。JoC 2020 で Guo らが提案した SHA3-256 および他の変種に対する 5 ラウンドの衝突攻撃以来、他に本質的な進展は発表されていない。

徹底的な調査により、このような SHA-3 への衝突攻撃をより多くのラウンドに拡張することの課題は、差分トレイル探索の非効率性にあることが突き止められた。

この障害を克服するために、本論文の著者らは、SAT ベースの自動探索ツールキットを開発した。このツールは衝突攻撃の複数の中間ステップで使用され、その過程で遭遇する差分トレイル探索やその他の最適化問題において高い効率性を示しているとされる。その結果、6 ラウンド SHAKE128 に対する古典衝突攻撃、量子衝突攻撃、SHA3-224 と SHA3-256 に対する 6 ラウンド量子衝突攻撃が発表された。時間計算量はそれぞれ、$2^{123.5}$、$2^{67.25}/\sqrt{S}$、$2^{97.75}/\sqrt{S}$、$2^{104.25}/\sqrt{S}$である（Sは量子コンピュータのハードウェアリソースを表す）。6 ラウンドの SHA3-224 と SHA3-256 に古典衝突攻撃が適用されないことは、量子衝突攻撃のカバー率が高いことを示していて、CRYPTO 2021 で Hosoyamada と Sasaki が観測した SHA-2 に対するものと一致すると、著者らは指摘している。

・Mind the TWEAKEY Schedule: Cryptanalysis on SKINNYe-64-256 [ASIACRYPT 2022]

Lingyue Qin, Xiaoyang Dong, Anyu Wang, Jialiang Hua, Xiaoyun Wang

近年、特定の用途に合わせた共通鍵暗号の設計が話題となっている。EUROCRYPT 2020 で、Naito、Sasaki、Sugawara は、認証付き暗号 PFB_Plus の要件を満たすために、閾値実装フレンドリー暗号 SKINNYe-64-256 を考案した。やがて Peyrin が、SKINNYe-64-256 は新しい tweakey スケジュールにより安全性の期待を失う可能性があると指摘した。SKINNYe-64-256 の安全性の問題はまだ不明だが、Naito らは対応策として、SKINNYe-64-256 v2 を導入することを決定した。

本論文では、SKINNYe-64-256 の新しい tweakey スケジュールについて形式的な暗号解析を行い、tweakey スケジュールにおける予想外の差分キャンセレーション（differential cancellation）を発見している。例えば、連続する 30 ラウンドのうち、キャンセレーションが起こる回数は最大 8 回であり、予想される 3 回のキャンセレーションより大幅に多いことを発見した。この性質は、線形代数による tweakey の更新関数（LFSR）の解析によって導き出される。さらに、矩形攻撃、MITM 攻撃、不可能差分攻撃（impossible differential attack）について新たな発見をし、対応する自動化ツールに著者らの発見による新たな制約を適応させた。最終的に、SKINNYe-64-256 に対する 41 ラウンドの関連 tweakey 矩形攻撃が発見された。残っているセキュリティマージンは 3 ラウンドのみである。STK (Siperposition TweaKey) は任意のサイズの tweakey を受け付ける一方、SKINNY と SKINNYe-64-256 v2 は最大 4n の tweakey サイズまでしかサポートしていない。本論文では、SKINNY-64 のために、サポートする tweakey のサイズをさらに拡張する新しい tweakey スケジュールを紹介し、これが STK と SKINNY のセキュリティ要件を継承していることをフォーマルに証明する。

・Optimizing Rectangle Attacks: A Unified and Generic Framework for Key Recovery [ASIACRYPT 2022]

Ling Song, Nana Zhang, Qianqian Yang, Danping Shi, Jiahao Zhao, Lei Hu, Jian Weng

矩形攻撃はブロック暗号に対して非常に強力な暗号解読法である。矩形識別子が与えられると、鍵回復攻撃を可能な限り効率的に行うことが期待できる。文献上では、矩形鍵回復攻撃のアルゴリズムは 4 種類存在している。しかし、これらの性能はケースバイケースである。また、攻撃方法が最適化されていないアプリケーションも数多く存在する。本論文では、矩形鍵回復攻撃について深く考察し、あらゆる攻撃パラメータに対応可能な統一的かつ汎用的な鍵回復アルゴリズムが提案される。特に、従来の 4 つの矩形鍵回復アルゴリズムをカバーするだけでなく、これまで見落とされていた 5 種類の新しい攻撃も明らかにする。また、新しい鍵回復アルゴリズムとともに、最適な攻撃パラメータを自動的に見つけるフレームワークを提案し、新しいアルゴリズムを用いて矩形攻撃の計算量を最小にする。新しい鍵回復アルゴリズムの効率性を実証するため、既存の識別子に基づく Serpent、CRAFT、SKINNY、Deoxys-BC-256 に適用し、一連の改良型矩形攻撃が得られた。

・Nostradamus Goes Quantum [ASIACRYPT 2022]

Barbara Jiabao Benedikt, Marc Fischlin, Moritz Huppert

EUROCRYPT 2006 で Kelsey と Kohno によって導入されたノストラダムス攻撃（nostradamus attack）では、攻撃者は反復型ハッシュ関数Hのハッシュ値yをコミットする必要がある。また、後に与えられたプレフィックスPに対して、攻撃者は$H(P||S) = y$となる適切なサフィックス表現 S を見つけなければならなかった。さらに、Kelsey と Kohno は、Hの圧縮関数（出力と状態がnビット）の$2^{2n/3}$回の評価によるハーディング攻撃（herding attack）を示し、この攻撃を計算量の観点で原像攻撃と衝突探索の間にある攻撃であると位置付けた。本論文は、量子攻撃者に対するノストラダムス攻撃の安全性を調査し、ノストラダムス問題に対して量子ハーディング攻撃アルゴリズムを提案した。これは$n^{1/3}\ 2^{3n/7}$回の圧縮関数への評価を行うものであり、古典ケースにおける評価を大幅に改善している。また、量子ハーディング攻撃は$2^{3n/7}$回の評価では実行できないことを証明し、著者らのアルゴリズムが（本質的に）最適であることを示す。また、ランダムな圧縮関数に対する一般的なノストラダムス攻撃について、およそ$2^{\frac{3n}{7}-s}$回の評価についても議論されている（ここでsは敵対的に選択したサフィックスSの最大ブロック長である）。

8.3. ASIACRYPT 2022 の発表（3 日目）

・Improving Bounds on Elliptic Curve Hidden Number Problem for ECDH Key Exchange [ASIACRYPT 2022]

Jun Xu, Santanu Sarkar, Huaxiong Wang, Lei Hu

Hidden Number Problem(HNP)の楕円曲線上のアナロジーである EC-HNP は Asiacrypt 2001 で Boneh らによって導入された。PKC 2017 において Shani によりその Diffie-Hellman バージョンが与えられ、楕円曲線上の Diffie-Hellman 鍵交換のビットセキュリティが議論されたが、この議論はサイドチャネル攻撃が行われる状況の解析にも利用できる。

本論文では、EC-HNP の Diffie-Hellman バージョンの解析に現れる多変数剰余方程式を解くための Coppersmith 法の解析を見直した。その結果、任意の正の整数d、十分に大きな素数p、および$\mathbb{F}_p$上の楕円曲線において、ECDH 鍵のx座標の LSB または MSB の$1/(d+1)$を出力するオラクルが存在すれば、鍵の残りの全ビットを$\log_2 p$の多項式時間で計算するヒューリスティックなアルゴリズムを構成した。$d>1$であれば、この結果は既存の結果として知られている必要 LSB(MSB)量である$5/6$（厳密な評価）と 1/2（ヒューリスティックな評価）の両方を著しく下回る。Coppersmith 法で仮定されているヒューリスティックがあるため、固定された楕円曲線上での ECDH ビット安全性は得られていないが、NIST 曲線に対して Coppersmith 法の格子が小さいもののいくつかを用いて実験したところ、ヒューリスティックの有効性が確認された。

・Log-$\mathcal{S}$-unit Lattices Using Explicit Stickelberger Generators to Solve Approx Ideal-SVP [ASIACRYPT 2022]

Olivier Bernard, Andrea Lesavourey, Tuong-Huy Nguyen, Adeline Roux-Langlois

本論文は任意の数体に適用可能な、イデアル格子の近似最短ベクトル問題を解くアルゴリズムの改良を与えている。このアルゴリズムは元々、2019 年に Pelle-Mary, Hanrot, Stehlé により提案されたことから PHS アルゴリズムと呼ばれ、その後 2020 年に Bernard と Roux-Langlois が任意の数体上で動作するように改良したものが Twisted-PHS アルゴリズムと呼ばれる。

これまでの素数導手の円分体上での実験では、変換後の log-$\mathcal{S}$-unit 格子の計算に準指数時間が必要なことから、拡大次数が高々70 程度のものまでしか実験できていなかった。この論文では、最近の Bernard と Kučera による Stickelberger ideal に関する結果から、Twisted-PHA アルゴリズムで有用なフルランクの log-$\mathcal{S}$-unit 部分格子を構築するための生成器を構成している。その結果、数値実験をほとんどの導手mに対して拡大次数 210 までの円分体に拡張した。

Twisted-PHS アルゴリズムが Cramer、Ducas、Wesolowski による CDW アルゴリ

ズムの性能を上回る場合があり、漸近的な volumetric lower bound を超える場合があることを実験的に示している。さらに、類数のプラス部分が $h_m^+ \leq O(\sqrt{m})$ であるという、ほとんどの円分体に対して成り立つ状況を想定すると、明示的な Stickelberger generator を用いることで CDW アルゴリズムの中のほとんどの量子ステップを回避することが可能である。

・A Non-heuristic Approach to Time-space Tradeoffs and Optimizations for BKW [ASIACRYPT 2022]

Hanlin Liu, Yu Yu

Blum ら(JACM2003)による BKZ アルゴリズムは、LPN 問題の準指数時間アルゴリズムとして知られており、ノイズの大きさμと時間・空間計算量は詳細に解析されている。この論文では、Wagner(CRYPTO2002)の一般化誕生日パラドックスアルゴリズムをc分木構造に適用することで、BKW アルゴリズムの変種を提案した。

結果として、Esser ら(CRYPTO2018)の LPN 問題、LWE 問題に対する時間-空間トレードオフの解析からヒューリスティックな議論を取り除いた。このアルゴリズムは Grover の量子探索、Dinur らの Dissection テクニックと組み合わせることも可能である。

また、新たに時間-空間トレードオフをかんがえることで既存の結果よりも必要なサンプル数の少ないアルゴリズムを導き出している。

・On Module Unique-SVP and NTRU [ASIACRYPT 2022]

Joël Felderhoff, Alice Pellet-Mary, Damien Stehlé

NTRU 問題は、非常に短い非ゼロベクトルを含むことが保証されている格子に対して、それを見つける計算問題のインスタンスとみなすことができる。さらに、対象となる格子は適当な数体の整数環上での階数 2 のモジュラー構造を持つ。

この計算問題を module unique 最短ベクトル問題、略して mod-uSVP と呼ぶことにする。本論文では、NTRU 問題が mod-uSVP の単なる特殊なケースではなく、計算困難性の観点からは典型的なインスタンスの集合であるという証拠を、以下の２つの還元によって示す。

まず、mod-uSVP の最悪計算量を NTRU の最悪計算量に還元する。技術的にはイデアル格子の短いベクトルを発見する id-SVP オラクルを用いて、Pellet-Mary と Stehlé (ASIACRYPT2021)による id-SVP の最悪計算量から NTRU の最悪計算量への還元を用いる。ここで NTRU と mod-uSVP が最悪時には等しい計算量を持つことが示される。

次に、mod-uSVP がランダム自己帰着性を持つことを示す。具体的にはある確率分布 D を用意し、ここから出力される mod-uSVP のインスタンスを解くことで mod-uSVP

の最悪インスタンスを解くことができることを示す。これと第一の結果を組み合わせることで、mod-uSVP の最悪計算量が NTRU の平均計算量と関連付けられる。

8.4. ASIACRYPT 2022 の発表（4 日目）

・A Third is All You Need: Extended Partial Key Exposure Attack on CRT-RSA with Additive Exponent Blinding [ASIACRYPT 2022]

Yuanyuan Zhou, Joop van de Pol, Yu Yu, François-Xavier Standaert

EUROCRYPT 2022 において、May らは CRT-RSA に対する部分鍵漏洩(Partial Key Exposure: PKE)攻撃を提案し、公開指数eのサイズが$N^{1/12}$の場合、秘密指数d_pおよびd_qの両方の最上位ビット（MSBs）の 1/3、または最下位ビット（LSBs）の 1/3 を知ると、Nを素因数分解可能であることを示した。PKE 攻撃の実効性はこれらの指数のサイドチャネルからの漏洩に依存しているが、よくあるサイドチャネル耐性実装では、未知のランダムなブラインド係数r_p,r_qを用いたブラインド指数$d_p' = d_p + r_p(p-1)$, $d_q' = d_q + r_q(q-1)$を暗号化に用いているため、PKE 攻撃はより困難なものになると考えられる。

以上の背景のもと、本論文は May らの PKE 攻撃をブラインド指数の CRT-RSA に拡張した。May らの攻撃とほぼ同様の二段階攻撃を用いて$r_p e \in (0, N^{1/4})$の場合に攻撃が可能である．特に，$r_p e \approx N^{1/12}$の場合にはブラインド指数d_p', d_q'の MSB または LSB の 3 分の 1 の情報からNを素因数分解可能である．

本手法における LSB 攻撃は通常の Coppersmith タイプの仮定の下、多項式時間で機能することが示された。一方， MSB 攻撃の計算時間は$e^2 r_p r_q$に比例するためNの準指数時間ではあるが、新たにヒューリスティックな仮定を導入することで確率的多項式時間であることが示せる。一般的な鍵サイズ（1024 ビット、2048 ビット、3072 ビット）とブラインド因数のサイズ（32 ビット、64 ビット、128 ビット）に対して計算機実験を行い、Coppersmith タイプの仮定と新たなヒューリスティックの両方がなりたつことを確認している。

以上の攻撃は、128 ビットのブラインド指数が存在する場合の CRT-RSA に対して初めて実験的な有効性が確認された PKE 攻撃であると著者らは主張している。さらに、Montgomery Ladder 指数 CRT 実装を対象としたサイドチャネル部分秘密鍵漏洩に対し、提案攻撃の実験を行っている。

・Optimising Linear Key Recovery Attacks with Affine Walsh Transform Pruning [ASIACRYPT 2022]

Antonio Flórez-Gutiérrez

線形解読法は、ブロック暗号に対する鍵回復攻撃の主要な系統の 1 つである。いくつ

かの論文では、高速 Walsh 変換を使用することで、その計算量を低減できる可能性に注目している。これらの先行研究は、鍵回復ラウンドの構造を無視して、任意のブール関数として扱っていた。本論文では、Walsh 変換のための新しいアフィン枝刈り技術を使用して、これらの関数の Walsh スペクトルのゼロを利用することによって、これらのアルゴリズムの計算量とメモリ量を最適化した。これらの新しい最適化戦略は、DES に対する改良された攻撃と 29 ラウンドの PRESENT-128 に対する最初の既知の攻撃という 2 つの応用例で紹介される。

・Stretching Cube Attacks: Improved Methods to Recover Massive Superpolies [ASIACRYPT 2022]

Jiahui He, Kai Hu, Meiqin Wang, Bart Preneel

キューブ攻撃は、共通鍵暗号の代数的性質を利用して、特殊な多項式である superpoly を復元し、その後に秘密鍵を復元するものである。対応するブール関数の ANF（algebraic normal form）が利用できない場合、division property に基づくアプローチにより、巧妙な方法で正確な superpoly を復元することができる。しかし、superpoly を復元するための計算コストは、暗号のラウンド数が増加するにつれて法外に大きくなる。例えば、ASIACRYPT 2021 で提案された NMP（nested monomial prediction）は、 Trivium の 845 ラウンドまでの解析に留まっている。この NMP 技術のボトルネック、すなわち単項トレイルの数が多すぎて解けないモデルを緩和するために、著者らは superpoly に寄与する特定の中間ラウンドのいわゆる valuable term に焦点を当てている。2 つの新しい技術、すなわち、NBDP（Non-zero Bit-based Division Property）と CMP（Core Monomial Prediction）を導入し、MP の MILP モデルと比較して、より単純な MILP モデルを実現することが可能となる。CMP 技法は、valuable term を回復する計算量の点で、monomial prediction よりも大幅な改善をもたらすことが示されている。分割統治法とこれら 2 つの新しい技術を組み合わせることで、より効果的に valuable term を捕らえ、superpoly に何も貢献しない中間項に対する計算リソースの浪費を避けることが可能となる。 その結果、以前の攻撃の計算コストを大幅に削減することができ、846、847、848 ラウンドの Trivium、192 ラウンドの Grain、895 ラウンドの Kreyvium、776 ラウンドの Acorn における superpoly の ANF を実用時間で復元できた。さらに、Möbius 変換の内部的な性質を調べることで、鍵の全ビットを含む superpoly を用いた鍵回復方法を示し、対象となる暗号に対して最適な鍵回復攻撃を実行できるようになった。

・On the Field-Based Division Property: Applications to MiMC, Feistel MiMC and GMiMC [ASIACRYPT 2022]

Jiamin Cui, Kai Hu, Puwen Wei, Meiqin Wang

近年、MPC や ZKP などの高度な暗号プロトコルが実用化され、Arithmetization-Oriented (AO) 暗号と呼ばれる有限体上の共通鍵暗号が開発されている。このようなAO暗号は、代数的攻撃、特に高階差分攻撃に対して脆弱であることが指摘されている。そのため、代数次数の増大を注意深く評価することに意義がある。しかし、AO暗号の次数推定は、一般的に正確な方法がないため、暗号解析者の課題となっている。

本論文では、代数次数の上界を求めるための最先端のフレームワークである division property を、バイナリ体から$\mathbb{F}_{2^n}$をスコープにいれた範囲に拡張する。これは、AO 暗号の代数的次数を検出する汎用的な手法であり、Feistel 暗号にも適用可能である。この一般化された division property における著者らのアイデアは、ブロック暗号の多項式表現においてある特定の単項式を含んでいるかどうかを評価することにある。演算の特徴を深く調べることで、体演算ベースの単項式の伝搬規則が紹介される。これは SMT のビットベクトル理論を用いて効率的にモデル化できる。そして、代数次数と単項式の指数との関係から、次数推定のための新しい検索ツールを構築することができる。

著者らは、この新しい枠組みを Feistel MiMC、GMiMC、MiMC などのいくつかの重要な AO 暗号に適用した。Feistel MiMC については、代数次数の増大が本来の指数関数的な限界よりも大幅に遅くなることが示された。また、CRYPTO 2020 で提案された Feistel MiMC の 83 ラウンド識別子よりもはるかに優れた、124 ラウンドまでの秘密鍵高階差分識別子が初めて提示された。また、データ量 2^{251} のフルラウンドゼロサム識別子も提示される。本手法は、より多くの分岐を持つ一般的な Feistel 構造に対してさらに拡張でき、GMiMC の実用的なインスタンスに対して、最大 50 ラウンドの高階差分識別子を示すことが可能である。SP-network における MiMC については、本結果は Bouvier によって証明された正確な代数次数と対応する。著者らはさらに、異なる指数をもつ MiMC のような方式に対する高階差分攻撃に対する安全性を保証するために、MiMC 仕様のラウンド数は十分ではないことを指摘した。

CRYPTREC Report 2022
(暗号技術評価委員会報告 CRYPTREC RP-2000-2022)

発行日　2023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