CRYPTREC Report 2024

令和７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-2000-2024

「暗号技術評価委員会報告」

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 2024 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 2024 年度の活動として、主に、1) 暗号技術の安全性及び実装に係る監視及び評価、2) 新しい暗号技術に係る調査および評価について暗号技術検討会より承認を得て実施した。

1) に関しては、国際会議等で発表される暗号の安全性及び実装に係る技術を監視し、CRYPTREC 暗号リストに掲載されている暗号の危殆化が進んでいないかどうかを判断した。2) に関しては、a) 耐量子計算機暗号 (Post-Quantum Cryptography) に関するガイドラインを作成するため、暗号技術調査ワーキンググループ (耐量子計算機暗号) の設置を継続し、國廣昇先生に主査をご担当いただき、「CRYPTREC 暗号技術ガイドライン (耐量子計算機暗号)」及びその根拠資料となる研究動向調査報告書を執筆した。また、公開鍵暗号の安全性に直結する「素因数分解の困難性に関する計算量評価」や「楕円曲線上の離散対数計算の困難性に関する計算量評価」を示す予測図を更新した。

また、「量子コンピュータが共通鍵暗号の安全性に及ぼす影響の調査及び評価 2024 年度版」を外部評価により実施し、公開した。この外部評価報告書は、2019 年度に公開した「量子コンピュータが共通鍵暗号の安全性に及ぼす影響の調査及び評価」を更新する形で作成した。

2000 年に IT 基本法が制定されたほぼ同時期に CRYPTREC が発足し、以来、25 年間にわたる CRYPTREC 活動は、安心・安全な ICT 社会の実現に貢献してきた。2019 年から始まったコロナ禍以後、非接触・非対面での生活様式を可能とする ICT の利活用が急速に進んできており、今後も様々な分野において ICT の高度化・多様化が予想されている。その中で暗号技術に対する社会のニーズはかつてないほど大きくなっている。今後も、社会の情勢を踏まえ、健全なサイバー空間の実現・維持につなげるべく、暗号技術の安全性という観点から必要とされる活動を展開していきたい。暗号技術評価委員会の活動は暗号技術やその実装及び運用に携わる研究者及び技術者の協力により成り立っている。末筆ではあるが、本活動に様々な形でご協力頂いている関係者の皆様に深甚なる謝意を表する次第である。

暗号技術評価委員会 委員長 高木 剛

本報告書の利用にあたって

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

本報告書の第 1 章は暗号技術評価委員会の活動概要についての説明である。第 2 章は暗号技術評価委員会における監視活動に関する報告である。2024 年度については従来の監視活動に加え「量子コンピュータが共通鍵暗号の安全性に及ぼす影響の調査及び評価」について外部の有識者による外部評価を実施し、その報告を記載している。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）が共同で運営する以下の 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に記載した Web サイトから入手した CRYPTREC 活動に関する情報の利用に起因して生じた不利益や問題について、本委員会及び CRYPTREC 事務局は一切責任をもたない。

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

【問合せ先】 info@cryptrec.go.jp

委員会構成

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

暗号技術調査ワーキンググループ (以下「調査 WG」と表記する) は、評価委員会の下に設置され、NICT と IPA が共同で運営する。調査 WG は、評価委員会の指示の下、評価委員会活動に必要な項目について調査・検討活動を担当する作業グループである。評価委員会の委員長は、実施する調査・検討項目に適する主査及びメンバーを選出し、調査・検討活動を指示する。主査は、その調査・検討結果を評価委員会に報告する。2024 年度、評価委員会の指示に基づき実施される調査項目は、「暗号技術調査 WG(耐量子計算機暗号)」にて検討される。評価委員会と連携して活動する「暗号技術活用委員会」も、評価委員会と同様、暗号技術検討会の下に設置され、NICT と IPA が共同で運営している。

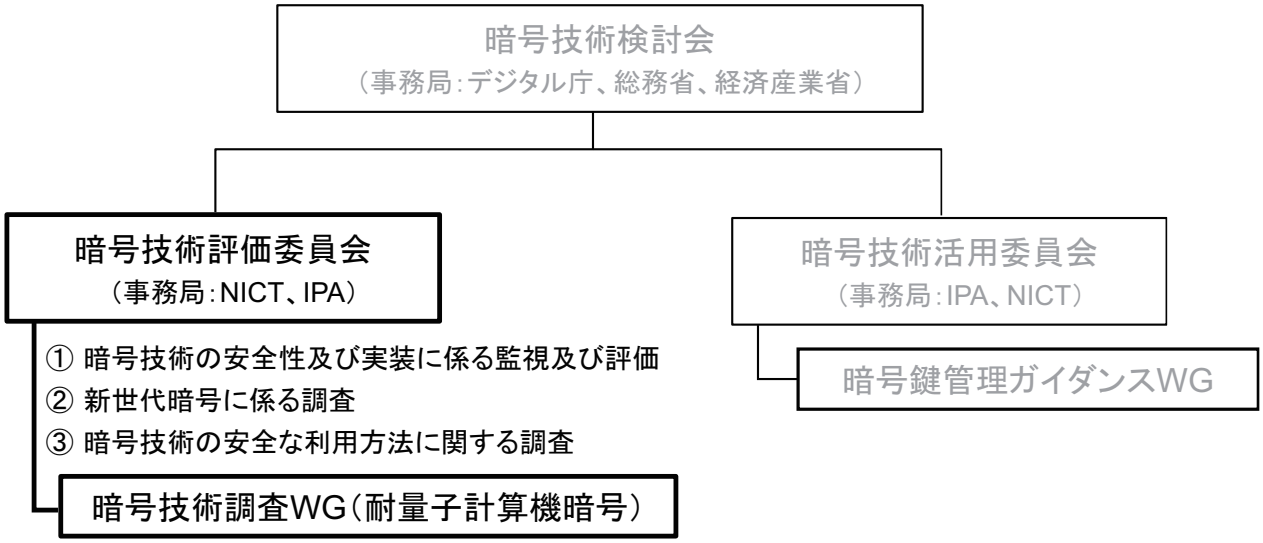

図 1: CRYPTREC 体制図

委員名簿

暗号技術評価委員会

委員長	高木 剛	東京大学 教授
委員	青木 和麻呂	文教大学 准教授
委員	岩田 哲	名古屋大学 教授
委員	上原 哲太郎	立命館大学 教授
委員	大東 俊博	東海大学 教授
委員	國廣 昇	筑波大学 教授
委員	四方 順司	横浜国立大学 教授
委員	手塚 悟	慶應義塾大学 教授
委員	花岡 悟一郎	産業技術総合研究所 首席研究員
委員	藤崎 英一郎	北陸先端科学技術大学院大学 教授
委員	本間 尚文	東北大学 教授
委員	松本 勉	産業技術総合研究所 フェロー／横浜国立大学 上席特別教授
委員	松本 泰	ＮＰＯ日本ネットワークセセキュリティ協会　フェロー
委員	山村 明弘	秋田大学 教授

暗号技術調査ワーキンググループ (耐量子計算機暗号)

主査	國廣 昇	筑波大学 教授
委員	青木 和麻呂	文教大学 准教授
委員	伊藤 忠彦	セコム株式会社 主務研究員
委員	下山 武司	国立情報学研究所 特任准教授
委員	高木 剛	東京大学 教授
委員	高島 克幸	早稲田大学 教授
委員	成定 真太郎	ＫＤＤＩ総合研究所　コアリサーチャー
委員	廣瀬 勝一	福井大学 教授
委員	安田 貴徳	岡山理科大学 教授
委員	安田 雅哉	立教大学 教授

オブザーバー

（2024 年度暗号技術評価委員会／暗号技術調査ワーキンググループ（耐量子計算機暗号）の参加者のみ記載）

高木 浩光	内閣官房内閣サイバーセキュリティセンター
水野 邦俊	内閣官房内閣サイバーセキュリティセンター
松井 裕介	内閣官房内閣サイバーセキュリティセンター
泉 雅巳	内閣官房内閣サイバーセキュリティセンター
北井上 礼樹	デジタル庁 デジタル社会共通機能 G
渡辺 良光	デジタル庁 デジタル社会共通機能 G
山之上 隆広	デジタル庁 デジタル社会共通機能 G
當波 孝明	デジタル庁 デジタル社会共通機能 G
菊池 慶	総務省 自治行政局 住民制度課
井上 裕章	総務省 自治行政局 住民制度課
佐藤 蓮	総務省 自治行政局 住民制度課
宮野 哲史	総務省 サイバーセキュリティ統括官室
内藤 めい	総務省 サイバーセキュリティ統括官室
市川 和秀	総務省 サイバーセキュリティ統括官室
川村 航太	総務省 サイバーセキュリティ統括官室
佐久間 明彦	外務省 大臣官房
水村 優斗	外務省 大臣官房
加藤 優一	経済産業省 商務情報政策局
桶田 雄士	防衛省 整備計画局
井上 智樹	警察大学校
高橋 知義	警察大学校

事務局

国立研究開発法人情報通信研究機構 (井上 大介、青野 良範、伊藤 竜馬、大久保 美也子、小川 一人、金森 祥子、黒川 貴司、篠原 直行、田村 千代、吉田 真紀、笠井 祥、大川 晋司)

独立行政法人情報処理推進機構 (神田 雅透、新保 淳、鷲見 拓哉、福岡 尊、白岩 裕子、川名 優香)

第 1 章

活動の目的

1.1 電子政府システムの安全性確保

電子政府、電子自治体及び重要インフラにおける情報セキュリティ対策は根幹において暗号アルゴリズムの安全性に依存している。情報セキュリティ確保のためにはネットワークセキュリティ、通信プロトコルの安全性、機械装置の物理的な安全性、セキュリティポリシー構築、個人認証システムの脆弱性の排除、運用管理方法の不備を利用するソーシャルエンジニアリングへの対応と幅広く考慮すべき点があるが、暗号技術は情報システム及び情報通信ネットワークにおける基盤技術であり、暗号アルゴリズムの安全性を確立することなしに情報セキュリティ対策は成り立たない。現在、様々な暗号技術が開発され、それを組み込んだ多くの製品・ソフトウェアが市場に提供されているが、暗号技術を電子政府システム等で利用するためには、暗号技術の適正な評価が行われ、その評価情報が容易に入手できることが極めて重要となる。このため CRYPTREC では、「電子政府における調達のために参照すべき暗号のリスト (CRYPTREC 暗号リスト)」 を策定し、リストに記載された暗号アルゴリズムを対象として調査・検討を行っている。それに加えて、実導入が進んでいる暗号技術の安全性及び実装性について調査し、CRYPTREC 暗号リストへの追加を視野にいれた評価活動も行っている。また、暗号技術に関する安全性について重要な指摘があった場合に対応するため、CRYPTREC の Web サイト上に注意喚起レポートを掲載する活動を実施してきた。暗号技術に対する解析・攻撃技術の高度化が日夜進展している状況にあることから、今後も、CRYPTREC によって発信される情報を踏まえて、関係各機関が連携して情報システム及び情報通信ネットワークをより安全なものにするための取り組みを実施することが非常に重要である。また、過去 24 年間に渡って実施してきた暗号技術の安全性及び信頼性確保のための活動は、最新の暗号研究に関する情報収集・分析に基づいており、引き続き、暗号技術に係る研究者等の多くの関係者の協力が必要不可欠である。

1.2 暗号技術評価委員会

電子政府システムにおいて利用可能な暗号アルゴリズムを評価・選択する活動が 2000 年度から 2002 年度まで「暗号技術評価委員会」において実施された。その結論を考慮して電子政府推奨暗号リストが総務省・経済産業省において決定された。そして、電子政府システムの安全性を確保するためには電子政府推奨暗号リストに掲載されている暗号の安全性を常に把握し、安全性を脅かす事態を予見することが重要な課題となった。このため、2003 年度に電子政府推奨暗号の安全性に関する継続的な評価、電子政府推奨暗号リストの改訂に関する調査・検討を行うことが重要であるとの認識の下、暗号技術評価委員会が改組され、暗号技術検討会の下に「暗号技術監視委員会」が設置された。設置の目的は、電子政府推奨暗号の安全性を把握し、もし電子政府推奨暗号の安全性に問題点を有する疑いが生じた場合には緊

急性に応じて必要な対応を行うこと、また、電子政府推奨暗号の監視活動のほかに、暗号理論の最新の研究動向を把握し、電子政府推奨暗号リストの改訂に技術面から支援を行うことである。暗号技術監視委員会では、電子政府推奨暗号リスト改訂のため、2008 年度において、「電子政府推奨暗号リストの改訂に関する骨子（案）」及び「電子政府推奨暗号リスト改訂のための暗号技術公募要項（2009 年度）（案）」を策定した。2009 年度からは、電子政府推奨暗号リスト改訂のための新しい体制に移行し、名称を「暗号方式委員会」と変更した。電子政府推奨暗号リスト改訂のための暗号技術公募 (2009 年度) を受けて、2010 年度からは、応募された暗号技術などの安全性評価を開始し、2012 年度に「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）」 を策定した。2013 年度からは、名称を「暗号方式委員会」から再び「暗号技術評価委員会」と変更し、暗号技術の安全性に係る監視・評価及び実装に係る技術（暗号モジュールに対する攻撃とその対策も含む）の監視・評価を実施することになった。詳しくは、1.4 節を参照のこと。暗号技術評価委員会では、その下に暗号技術調査ワーキンググループを設置し、暗号技術に関する具体的な検討を行っている。2013 年度から 2016 年度までは、暗号技術調査ワーキンググループ（暗号解析評価）及び暗号技術調査ワーキンググループ（軽量暗号）の 2 つのワーキンググループが、2017 年度から 2020 年度までは、暗号技術調査ワーキンググループ（暗号解析評価）が、2021 年度から 2022 年度までは、暗号技術調査ワーキンググループ（耐量子計算機暗号）及び暗号技術調査ワーキンググループ（高機能暗号）の 2 つのワーキンググループが、そして、2023 年度から再度、暗号技術調査ワーキンググループ（耐量子計算機暗号）が設置されている。その間、暗号技術調査ワーキンググループ（軽量暗号）では、2016 年度に「CRYPTREC 暗号技術ガイドライン（軽量暗号）」 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)」 及び「CRYPTREC 暗号技術ガイドライン（高機能暗号）」 を作成し公表している。また、2023 年度から設置された暗号技術調査ワーキンググループ（耐量子計算機暗号）では「CRYPTREC 暗号技術ガイドライン（耐量子計算機暗号）2024 年度版」を作成し公表した。なお、2023 年度から設置された暗号技術調査ワーキンググループ（耐量子計算機暗号）の活動の詳細は第 3 章を参照のこと。これらのガイドラインの他に、2016 年度に策定した「CRYPTREC 暗号技術ガイドライン（軽量暗号）」を改定し、2023 年度に「CRYPTREC 暗号技術ガイドライン（軽量暗号）2023 年度版」 を作成し公表した。

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（意見募集）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が改定された。最終的に、総務省及び経済産業省がパブリックコメント募集（意見募集）を行い、「電子政府におけ

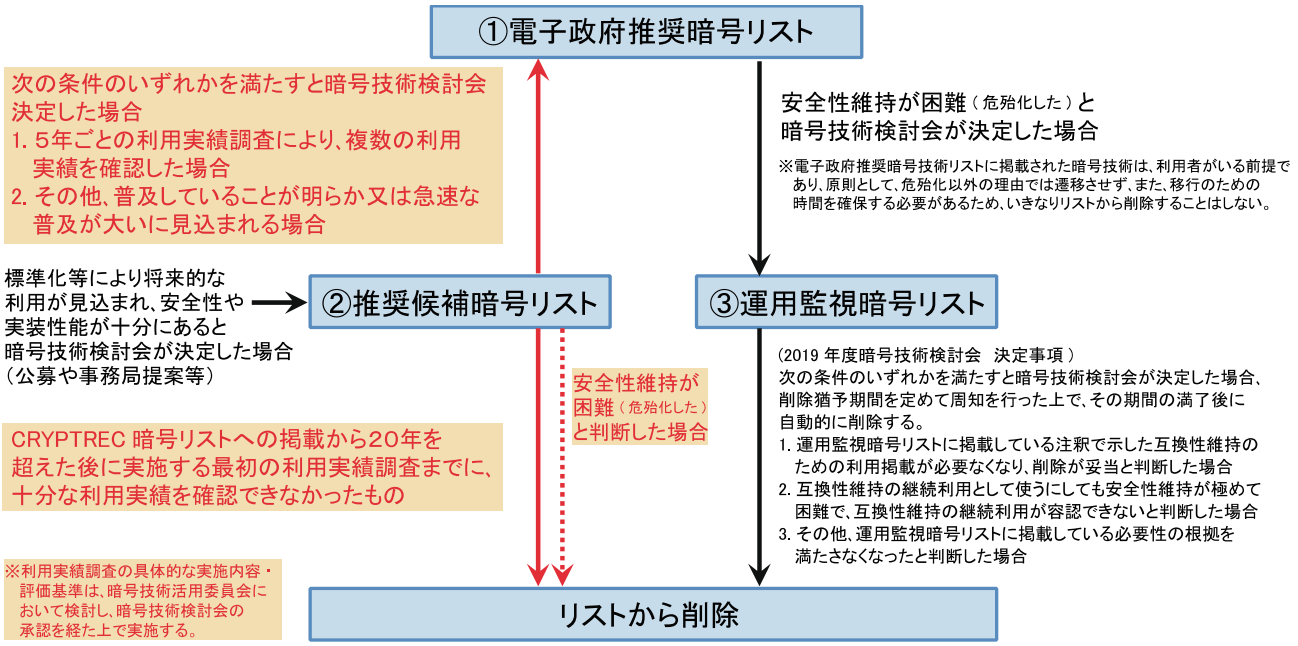

図 1.1: CRYPTREC 暗号リスト移行ルール

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 年度以降、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、2021 年度に公開鍵暗号（署名）EdDSA 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 （図 1.1 を参照)。

2022 年度において、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リスト（CRYPTREC 暗号リスト）」（案）に対するパブリックコメント募集（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）」 (付録 A を参照) を策定した。2023 年度には、暗号リストの改定はないが、一部の項目に対し注意書きが付与された。

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、以下の①～⑤となる。

① CRYPTREC 暗号等の監視：国際会議等で発表される CRYPTREC 暗号リストの安全性及び実装に係る技術（暗号モジュールに対する攻撃とその対策も含む）に関する監視を行い、会議や ML を通して報告する。
② 電子政府推奨暗号リストからの運用監視暗号リストへの降格、並びに、推奨候補暗号リスト及び運用監視暗号リストからの危殆化が進んだ暗号の削除：CRYPTREC 暗号リストの安全性に係る監視活動を継続的に行い、急速に危殆化が進んだ暗号技術やその予兆のある暗号技術の安全性について評価を行う。また、リストからの降格や削除、注釈の改訂が必要か検討を行う。
③ CRYPTREC 注意喚起レポートの発行：CRYPTREC 暗号リストの安全性及び実装に係る技術の監視活動を通じて、国際会議等で発表された攻撃等の概要や想定される影響範囲、対処方法について早期に公開することが望ましいと判断された場合、注意喚起レポートを発行する。
④ 推奨候補暗号リストへの新規暗号（事務局選出）の追加：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。

また、具体的に 2024 年度については、CRYPTREC 暗号リストとは別文書として、耐量子計算機暗号に関するガイドラインを作成するため、および、大規模な量子コンピュータに対する共通鍵暗号系の安全性に関する動向調査を実施するため、⑤において以下の項目を実施することが暗号技術検討会において承認された。

- 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。
- 2019 年度に作成した「量子コンピュータが共通鍵暗号の安全性に及ぼす影響の調査及び評価」の更新のため、外部の有識者による外部評価により 2020 年度以降の技術動向調査を行い、「量子コンピュータが共通鍵暗号の安全性に及ぼす影響の調査及び評価 2024 年度版」を作成する。

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掲載の暗号技術に対する考え方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。

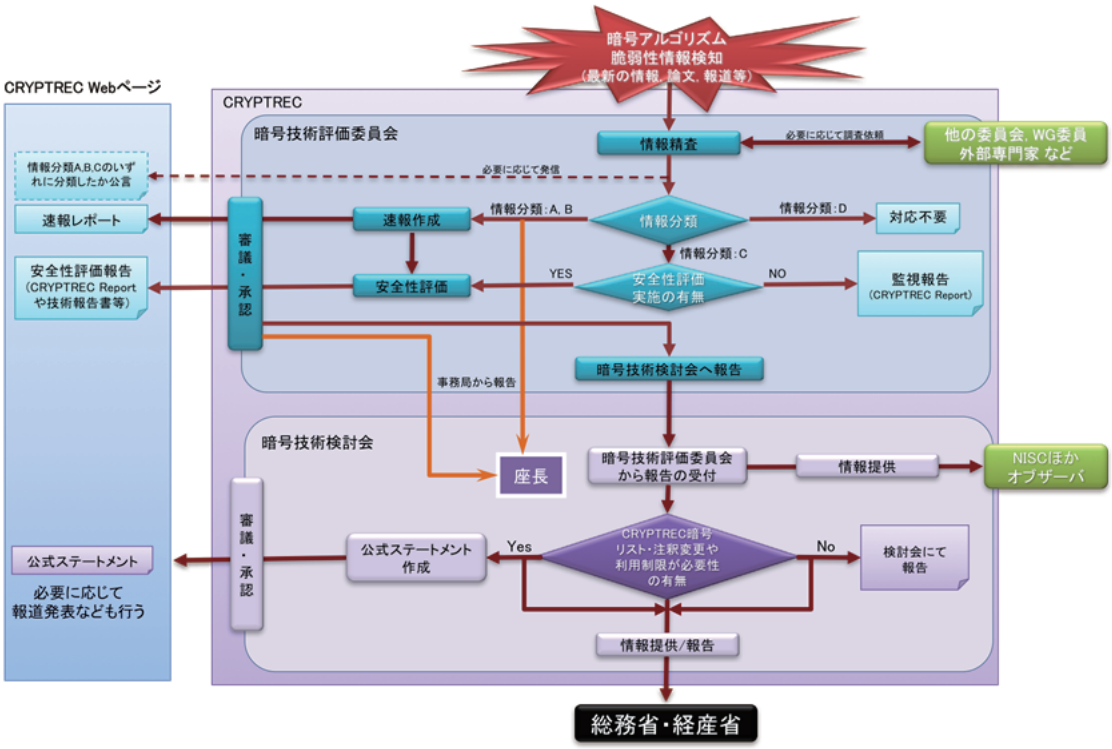

図 1.2: 暗号アルゴリズムの脆弱性に関する情報発信フロー

[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、2024 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 公開鍵暗号に関する安全性評価について

今年度は、CRYPTREC 暗号リストに掲載されている公開鍵暗号の安全性評価について大きな進展はなかった。

2.1.2 共通鍵暗号に関する安全性評価について

今年度は、2023 年度に引き続き、共通鍵暗号の安全性評価について大きな進展はなかったものの、CRYPTREC 暗号リストに掲載されている共通鍵暗号の安全性評価に関して、攻撃に必要な計算量の削減等の進展があった。ここでは学会等で発表された主要論文を紹介する。

ブロック暗号 AES に対する解析論文が FSE 2024、Eurocrypt 2024、Asiacrypt 2024 で報告された。なお、AES-128、AES-192、AES-256 の仕様段数はそれぞれ 10、12、14 ラウンドである。FSE 2024 で報告された解析論文では、13 ラウンド AES-256 に対する関連鍵設定での鍵回復攻撃が時間計算量 2^{250}、データ量 2^{126}、メモリ量 2^{231}、関連鍵数 2 で実行可能であることが示された。これは 2 個の関連鍵で実行可能な既知の攻撃の中で最良の鍵回復攻撃である。Eurocrypt 2024 で報告された解析論文では、6 ラウンド AES に対する既知の攻撃の中で最良の鍵回復攻撃を更新し、$2^{46.4}$ 回の加算計算量で攻撃可能であることを示した。Asiacrypt 2024 では 3 件の解析論文が報告された。1 件目は、AES に対する新しい鍵衝突の概念（Fixed-TPKC[*1]と Free-TPKC[*2]）を提唱し、結果として 2/5/6 ラウンドの AES-128/192/256 に対する Fixed-TPKC と 5/7/9 ラウンドの AES-128/192/256 に対する Free-TPKC を発見し、それぞれ AES-DM に対する衝突攻撃とセミフリースタート衝突攻撃に応用可能であることを示した。2 件目は、6 ラウンド AES に対する既知の攻撃の中で最良の識別攻撃を更新し、計算量を 2^{84} から $2^{76.57}$ まで削減できることを示した。3 件目は、13 ラウンド AES-256 に対する関連鍵設定での鍵回復攻撃が時間計算量 2^{240}、データ量 2^{89}、メモリ量 2^{144}、関連鍵数 2 で実行可能であることが示し、FSE 2024 で報告された結果を改善することに成功した。

ストリーム暗号 ChaCha に対する解析論文が FSE 2024 で報告された。なお、ChaCha の仕様段数は 20 ラウンドで

[*1] Fixed-Target-Plaintext Key Collision
[*2] Free-Target-Plaintext Key Collision

ある。この解析論文では、7 ラウンド ChaCha に対する鍵回復攻撃が時間計算量 $2^{206.8}$、データ量 $2^{110.81}$ で実行可能であることを示し、時間計算量の観点で既存攻撃を改善することに成功した。

ハッシュ関数 SHA2 に対する解析論文が Eurocrypt 2024 と Asiacrypt 2024 で報告された。なお、SHA-224 と SHA-256 の仕様段数は 64 ラウンド、SHA-384 と SHA-512 の仕様段数は 80 ラウンドである。Eurocrypt 2024 で報告された解析論文では、40 ラウンド SHA-224 に対するフリースタート衝突ペア、39 ラウンド SHA-256 に対するセミフリースタート衝突ペア、そして 28 ラウンド SHA-512（SHA-384、SHA-512/224、SHA-512/256 も同様）に対する衝突ペアを現実的な時間内で初めて発見するとともに、31 ラウンド SHA-512 に対する衝突ペアを計算量 $2^{115.6}$ で発見できることを示した。Asiacrypt 2024 で報告された解析論文では、31 ラウンド SHA-256 に対して現実的な計算量（64 スレッドを使用して約 1.2 時間）と無視できるくらい小さいメモリ量（$O(2^{10})$）で衝突メッセージペアを発見した。また、31 ラウンド SHA-512 の衝突攻撃に関して、計算量を $2^{115.6}$ から $2^{94.7}$ へ、メモリ量を $2^{77.3}$ から $2^{35.2}$ へ、それぞれ改善することに成功した。

ハッシュ関数 SHA3 に対する解析論文が Crypto 2024 で報告された。なお、SHA3 の仕様段数は全てのインスタンスにおいて 24 ラウンドである。この解析論文では、SHA3-384 と SHAKE256 に対する衝突攻撃にて攻撃可能ラウンド数を更新し、それぞれ 5 ラウンドと 6 ラウンドまで攻撃が可能であることを示した。また、4 ラウンド SHA3-512 と 5 ラウンド SHA3-224/SHA3-256/SHAKE128 に対して既存の衝突攻撃における計算量を改善した。

ハッシュ関数 RIPEMD-160 に対する解析論文が FSE 2024 で報告された。なお、RIPEMD-160 の仕様段数は 80 ラウンドである。この解析論文では、最大 40 ラウンドの RIPEMD-160 に対して現実的な計算量で衝突メッセージペアを発見できることを示すとともに、最大 43 ラウンドまでのセミフリースタート衝突攻撃が実行可能であることを示した。

上記のとおり、AES、ChaCha、SHA2、SHA3、RIPEMD-160 に対する暗号解析において進展があったものの、セキュリティマージンはまだ十分にあるため、これらの暗号解析がそれぞれの安全性に直ちに影響を及ぼすものではない。

2.1.3 その他注視すべき技術動向

共通鍵暗号については、差分線形攻撃や中間一致攻撃、およびそれらに用いられる共通鍵暗号解読プリミティブがいくつか進展し、認証暗号 Ascon などを含む様々な共通鍵暗号の安全性評価に関する論文が発表されている。

公開鍵暗号・署名においては、NIST 耐量子計算機暗号標準化プロセスにおいて大きな動向があった。2024 年 8 月 13 日、NIST は 3 つの耐量子計算機暗号 CRYSTALS-Kyber、CRYSTALS-Dilithium、SPHINCS$^+$ の標準化を決定し、標準方式の名称を決定した。CRYSTALS-Kyber は ML-KEM（Module-Lattice-Based Key-Encapsulation Mechanism）と名付けられ、NIST FIPS 203 として標準化された。CRYSTALS-Dilithium は ML-DSA（Module-Lattice-Based Digital Signature Algorithm）と名付けられ、NIST FIPS 204 として標準化された。SPHINCS$^+$ は SLH-DSA（StateLess Hash-Based Digital Signature Algorithm）と名付けられ、NIST FIPS 205 として標準化された。その他に格子署名 FALCON も NIST FIPS 206 として標準化予定である。また、2024 年 10 月 24 日、追加の電子署名公募が第 2 ラウンドに移行し、候補数が 14 件まで絞られた。現在の候補は、符号ベースの CROSS、LESS、同種写像ベースの SQIsign、格子ベースの HAWK、MPC-in-the-Head フレームワークによる構成を行った Mirath、MQOM、PERK、RYDE、SDitH、多変数多項式ベースの MAYO、QR-UOV、SNOVA、UOV、共通鍵暗号ベースの FAEST である。

追加の電子署名公募に関連して、今年度も昨年度と同様、耐量子計算機暗号の評価に関する多くの論文が報告された。特に、格子暗号に対するヒューリスティックを用いずに計算量の証明が可能な手法の研究に関する進展、多変数公

開鍵暗号の安全性が 1 本のベクトルを復元することの困難性に依存するという関係の発見、など安全性の根拠となる計算問題に関して理論的な進展があった。

その他、Regev による量子素因数分解アルゴリズムの改良および離散対数問題への拡張が報告された。

2.2 注意喚起レポートについて

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

2.3 仕様書の参照先の変更について

CRYPTREC の Web サイトでは、CRYPTREC 暗号リストに掲載している暗号技術の仕様書の参照先（https://www.cryptrec.go.jp/method.html）を記している。電子政府推奨暗号リストに掲載されている署名 ECDSA とブロック暗号 AES の仕様参照先の変更を確認した。その結果、これらの新旧仕様書においてアルゴリズム部分に変更がないことを確認でき、暗号技術評価委員会での承認を経て仕様参照先の変更を行った。詳細は、表 2.1 のとおり。

表 2.1: 仕様参照先の変更

暗号技術名	旧仕様参照先	新仕様参照先
ECDSA	ANS X9.62-2005(*1) (*1) 仕様書は、一般財団法人 日本規格協会で購入が可能です。	ANS X9.142-2020(*1) (*1) 仕様書は、https://www.x9.org/ で購入が可能です。
AES	NIST FIPS PUB 197 参照先：https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf	NIST FIPS PUB 197 参照先：https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197-upd1.pdf

2.4 学会等情報収集記録

国内外の学術会議で発表された安全性評価技術に関する情報収集を実施した。情報収集対象の国際会議は、表 2.2 に示すとおりである。

以下、2.1 節で紹介した主要論文を中心に、安全性評価技術の最新動向を示す。その他の主要論文については、付録 D を参照されたい。

2.4.1 公開鍵暗号の解読技術

2.1.1 節で述べたとおり、今年度は CRYPTREC 暗号リストに掲載されている公開鍵暗号の安全性評価について大きな進展がなかったため、本節で紹介する論文は無い。その他、付録 D を参照されたい。

表 2.2: 情報収集対象の国際会議

学会名・会議名		開催国・都市	期間
FSE 2024	The 30th Conference on Fast Software Encryption	ベルギー・ルーヴェン	2024 年 3 月 25–29 日
PKC 2024	The 27th International Conference on Practice and Theory in Public Key Cryptography	オーストラリア・シドニー	2024 年 4 月 15–17 日
Eurocrypt 2024	The 43rd International Conference on the Theory and Applications of Cryptographic Techniques	スイス・チューリッヒ	2024 年 5 月 26–30 日
PQCrypto 2024	The 15th International Conference on Post-Quantum Cryptography	イギリス・オックスフォード	2024 年 6 月 12–14 日
Crypto 2024	The 44th Annual International Cryptology Conference	アメリカ・サンタバーバラ	2024 年 8 月 18–22 日
TCC 2024	The 22nd Theory of Cryptography Conference 2024	イタリア・ミラノ	2024 年 12 月 2–6 日
Asiacrypt 2024	The 30th International Conference on the Theory and Application of Cryptology and Information Security	インド・コルカタ	2024 年 12 月 9–13 日

2.4.2 共通鍵暗号の解読技術

Related-Key Differential Analysis of the AES

Christina Boura, Patrick Derbez, Margot Funk

FSE 2024

ブロック暗号 AES に対する解析論文である。AES は差分攻撃などの汎用攻撃手法に対して耐性を持つように設計されているが、この耐性は関連鍵設定では保持されず、時間の経過とともに様々な関連鍵攻撃が提案されてきた。

本研究では、AES に対する関連鍵設定における識別子の探索と鍵回復攻撃の実行を自動化するためのアルゴリズムとツールを提案する。最初に、AES の全てのバリアントに対する最適な切り詰め差分特性とアクティブ S-box の最小数に関する境界を特定するための 2 つの異なるアプローチを提案する。1 つ目のアプローチは、AES の方程式系に関する線形矛盾をより適切に処理するような MILP 手法であり、非常にシンプルではあるものの以前の自動化手法に匹敵する性能を持つ。2 つ目のアプローチは、動的プログラミングに基づく高速かつ低メモリの手法であり、汎用ソルバーに依存しない。特に、1 つ目のアプローチは AES-128 の関連鍵切り詰め差分特性、2 つ目のアプローチは AES-256 の関連鍵切り詰め差分特性の探索に関する高速化を実現する。最後に、差分中間一致攻撃に基づく鍵回復攻撃の完全な自動化ツールを提供する。このツールを AES-256 に適用したところ、関連鍵設定において、13 ラウンド AES-256 に対する鍵回復攻撃が時間計算量 2^{250}、データ量 2^{126}、メモリ量 2^{231}、関連鍵数 2 で実行できることを示した。関連鍵数が 2 個で実行できる最良の鍵回復攻撃である。

Partial Sums Meet FFT: Improved Attack on 6-Round AES

Orr Dunkelman, Shibam Ghosh, Nathan Keller, Gaetan Leurent, Avichai Marmor, Victor Mollimard
Eurocrypt 2024

ブロック暗号に対する汎用解析手法の提案論文である。FSE 2000 で Ferguson らは部分和（partial sum）手法という新しい解析手法を提案し、6 ラウンド AES に対して 2^{52} 回の S-box 計算で攻撃可能であることを示した。この記録は未だに破られていない。また、CANS 2014 で Todo と Aoki は高速フーリエ変換（FFT）ベース手法を提案し、部分和手法を FFT ベース手法に置き換えることで、6 ラウンド AES に対する攻撃が Ferguson らの攻撃と同等の時間計算量で実行可能であることを示した。FFT ベース手法は部分和手法に匹敵する代替手法として様々なシナリオで使用できるという利点があるものの、互いの利点を活かす方法論についてはこれまでに提案されてこなかった。

本研究では、部分和手法と FFT ベース手法を組み合わせることで、多くの場合で互いの利点を活かせることを示す。基本的な考え方は、部分和手法の一般的な構造を使用するものの、部分和手法で使用される特定の鍵推定ステップにおいて FFT ベース手法に置き換えるということである。また、FFT ベース手法の不利点を解消して攻撃の高速化を実現できるだけでなく、鍵推定するパートと FFT ベース手法を適用するパートを選択できることから、攻撃の柔軟性が高まるという利点がある。

提案手法はブロック暗号 AES、Kuznyechik、MISTY1、CLEFIA に適用された。特に、6 ラウンド AES に対しては最良の攻撃を更新し、$2^{46.4}$ 回の加算計算量で攻撃可能であることを示した。S-box 計算と加算計算を厳密に比較することは困難であるため、実験的に既存研究との比較を行ったところ、圧倒的に提案手法が効率的に実行できることを示した。また、フルラウンドの MISTY1 や 12 ラウンドの CLEFIA に対しても、最良の攻撃を更新できることを示し、汎用攻撃手法としての有効性を示した。

Key Collisions on AES and Its Applications

Kodai Taiyama, Kosei Sakamoto, Ryoma Ito, Kazuma Taka, Takanori Isobe
Asiacrypt 2024

AES に対する鍵衝突攻撃と AES の Davies-Meyer ハッシュモード（AES-DM）に対する衝突攻撃への応用に関する論文である。ブロック暗号に対する鍵衝突とは、2 つの異なる秘密鍵を使用して対象となる平文を暗号化した結果、生成された 2 つの暗号文が衝突するという概念である。既存研究では CIPHERUNICORN-A、MULTI2、SC2000 などに対する鍵衝突攻撃が報告されているが、AES に対する鍵衝突攻撃は報告されていない。また、ブロック暗号に対する鍵衝突攻撃は DM ハッシュモードに対する衝突攻撃へと応用可能であるが、AES-DM に対する（セミフリースタート）衝突攻撃もまた報告されていない。

本研究では、最初に新しいタイプの鍵衝突であるターゲット平文鍵衝突（TPKC: Target-Plaintext Key Collision）を定義する。TPKC は一般的な鍵衝突とよく似ており、2 つの異なる秘密鍵を使用してある特定の平文を暗号化した結果、生成された 2 つの暗号文が衝突するという概念である。TPKC はさらに Fixed-TPKC と Free-TPKC という 2 つの問題に分割され、前者は特定の平文が事前に与えられている条件下で鍵衝突を発見する問題、後者は特定の平文を自由に決められるという条件下で鍵衝突を発見する問題である。なお、Fixed-TPKC と Free-TPKC はそれぞれ DM ハッシュモードの衝突とセミフリースタート衝突に等価な概念となる。次に、これら 2 つの問題を解くための新しい自動解析ツールを開発する。このツールは、AES ライクなハッシュ関数に対する強力な解析手法の 1 つとして知られているリバウンド攻撃をベースとしている。具体的には、リバウンド攻撃を効率的に実行するために、グラフ理論と SAT

ソルバーによる差分特性探索手法を組み合わせ、Fixed-TPKC と Free-TPKC の最適な衝突パターンを探索するツールとなっている。

提案したツールを AES に適用した結果、2/5/6 ラウンドの AES-128/192/256 に対する Fixed-TPKC、5/7/9 ラウンドの AES-128/192/256 に対する Free-TPKC を発見し、それぞれ AES-DM に対する衝突攻撃とセミフリースタート衝突攻撃に応用可能であることを示した。特に、9 ラウンド AES-256-DM に対するセミフリースタート衝突攻撃は理論的に 2^{30} の計算量で実行可能であり、実際の衝突メッセージペアを示すことで提案ツールの有効性を証明した。

The Boomerang Chain Distinguishers: New Record for 6-Round AES

Xueping Yan, Lin Tan, Hong Xu, Wenfeng Qi

Asiacrypt 2024

AES の識別攻撃に関する論文である。2016 年まで、AES の識別攻撃は高々 4 ラウンドが限界であったものの、Eurocrypt 2017 で Grassi らは multiple-of-8 と呼ばれる性質を発見し、この性質を利用することで 5 ラウンド AES の識別攻撃を 2^{32} の計算量で実行できることを示した。その後、Asiacrypt 2019 で Bardeh らは exchange 攻撃を提案し、6 ラウンド AES の識別攻撃を 2^{84} の計算量で実行できることを示した。現状、AES の識別攻撃は Bardeh らの提案手法が最良であると知られている。

これらの既存研究に基づき、本研究では以下の 3 点について考察する。まず、5 ラウンド AES に対する識別攻撃と比較すると、6 ラウンド AES に対する識別攻撃は非常に多くの計算量が必要となるため、このギャップを埋めることが可能であるかという課題に対処する。次に、既存手法では適応的平文暗号文設定における広いデータ空間を有効活用できるという利点があり、この利点を最大限に有効活用した新しい解析手法を提案する。最後に、AES に対する強力な解析手法の 1 つであるブーメラン攻撃に着目し、既存手法では 1 つのブーメラン特性にのみ依存していたが、複数のブーメラン特性を利用して攻撃を改善できないかを検討する。

本研究では 2 種類のブーメラン識別攻撃を提案した。1 つ目は Re-Boomerang 手法と呼ばれ、2 つの関連性の高いブーメラン特性を組み合わせることで識別攻撃を強化するものとなっている。この攻撃は切り詰めブーメラン攻撃と exchange 攻撃を組み合わせることで実現可能である。2 つ目は Re-Boomerang 手法の拡張で Boomerang Chain 手法と呼ばれる。Re-Boomerang 手法では 2 つのブーメラン特性を利用したが、この 2 つのブーメラン特性の間にさらに複数のブーメラン特性を追加することで、攻撃にかかるデータ量の削減を目的としたものとなっている。これらの提案手法を 6 ラウンド AES に適用した結果、計算量を 2^{84} から $2^{76.57}$ まで削減することに成功し、AES の識別攻撃に関して新しい記録を達成した。なお、攻撃成功確率は 60 %である。

Generic Differential Key Recovery Attacks and Beyond

Ling Song, Huimin Liu, Qianqian Yang, Yincen Chen, Lei Hu, Jian Weng

Asiacrypt 2024

ブロック暗号に対する差分攻撃と矩形攻撃（Rectangle Attack）の汎用的攻撃手法の提案論文である。これらの攻撃に関して多くの改善手法が提案されてきた。特に、Crypto 2023 で提案された差分中間一致（差分 MitM）手法がさらなる改善をもたらし、切り詰め差分 MitM 手法への拡張など、さらなる発展が進んでいる。特にこれらの攻撃における鍵推測戦略が異なることに着目する。差分攻撃では最初に差分を満たす可能性がある平文暗号文ペアを生成した後、いくつかの鍵ビットを推測するという戦略を採ることが一般的である。一方で、矩形攻撃では平文暗号文ペアまたは平文暗号文カルテットを生成する前にいくつかの鍵ビットを推測することが可能であり、これにより事前に誤ったペアまた

はカルテットをフィルタリングできることから、効率的な鍵推測が可能となる。

本研究の貢献は以下の 3 点である。1 つ目は、汎用的古典差分攻撃（GCDA: Generic Classical Differential Attack）と呼ばれる新しい攻撃手法の開発である。差分攻撃における鍵推測の順序を改善し、誤った平文暗号文ペアを可能な限り事前にフィルタリングすることで、計算量の削減が可能となった。2 つ目は、一般化差分 MitM 攻撃（GDMA: Generalized Differential MitM Attack）と呼ばれる新しい攻撃手法の開発であり、差分攻撃における最も強力な差分 MitM 手法を改善することに成功した。具体的には、差分 MitM 手法はある特定の鍵推測戦略のみをサポートしているが、任意の鍵推測戦略をサポートするような汎用的手法へと拡張した。3 つ目は、汎用的矩形 MitM 攻撃（GRMA: Generic Rectangle MitM Attack）と呼ばれる新しい攻撃手法の開発であり、差分 MitM 手法を矩形攻撃に組み込みことで新しい矩形攻撃手法を実現した。

3 種類のブロック暗号（AES-256、KATAN-32、SKLINNYe-64-256v2）に適用することで提案手法の有効性を実証した。AES-256 に対しては GCDA と GDMA を適用し、関連鍵設定の下で 12/13 ラウンド AES-256 の計算量を改善した。例えば、13 ラウンド AES-256 に対しては、計算量 2^{240}、データ量 2^{89}、メモリ量 2^{144} で攻撃が実行可能であり、既存の差分 MitM 攻撃の結果を大幅に改善する結果となった。その他、KATAN-32 に対しては GDMA、SKINNYe-64-256v2 に対しては GRMA が適用され、それぞれ既存結果を改善することに成功した。

Boosting Differential-Linear Cryptanalysis of ChaCha7 with MILP

Emanuele Bellini, David Gerault, Juan Grados, Rusydi H. Makarim, Thomas Peyrin

FSE 2024

ストリーム暗号 ChaCha に対する解析論文である。本研究では、ChaCha に対する差分線形攻撃に関し、以下の観点で既存研究を改善した。最初に、差分パートに関し、これまで 1 ビットの入力差分に限定されていたが、2 ビットの入力差分も含めて攻撃に利用可能な差分パスの探索を行った。次に、線形パートに関し、MILP モデリング手法に基づく自動探索ツールを用いてより効果的な線形パスの探索を行った。さらに、差分パートと線形パートを繋ぐ中間ラウンドに関し、CUDA 実装を用いて差分パートの出力差分から線形パートの入力マスクまでの差分線形パスを厳密に評価した。このような手順で発見した差分線形パスを使用することで、7 ラウンド ChaCha に対する鍵回復攻撃が時間計算量 $2^{206.8}$、データ量 $2^{110.81}$ で実行できることを示し、時間計算量の観点で既存攻撃を改善することに成功した。また、識別攻撃に関しても改善できることが示されたものの、攻撃に使用するデータ量が 2^{128} 以上であることが懸念事項であるとの質問があり、既存研究も含めて識別攻撃の有効性については議論の余地がある。

New Records in Collision Attacks on SHA-2

Yingxin Li, Fukang Liu, Gaoli Wang

Eurocrypt 2024

ハッシュ関数 SHA-2 に対する衝突攻撃耐性の解析論文である。SHA-2 に対する衝突攻撃は Asiacrypt 2015 で報告されて以降、ほとんど進展がない。これは SHA-1 と比較して SHA-2 の設計が複雑であり、解析が難しいことが 1 つの要因として考えられる。具体的には、SHA-2 の差分特性を探索するための高度なツールがすでにボトルネックに達しており、より長いラウンドにおける差分特性が見つからないことが、より多くのラウンドにおける衝突が見つけられない原因となっている。

本研究では、SHA-2 の特性探索のために、Eurocrypt 2023 で Liu らが提案した MILP（Mixed Integer Linear Programming）ベースの探索手法を応用する。彼らの MILP ベースの探索手法は符号付差分（signed difference）に

基づいており、その手法は RIPEMD-160 の衝突攻撃耐性評価に適用されたが、SHA-2 の衝突攻撃耐性評価への適用可能性については未解決の問題として残されていた。この問題に対処するため、MILP ベースの手法を SAT/SMT（Boolean Satisfiability/Satisfiability Modulo Theory）ベースの手法へと変換するとともに、特性探索中の矛盾を排除するための新しい戦略について提案された。提案手法を全ての SHA-2 ファミリー（SHA-224、SHA-256、SHA-384、SHA-512、SHA-512/224、SHA-512/256）に適用し、それぞれ既存の衝突攻撃を更新する結果を示した。具体的には、40 ラウンド SHA-224 に対するフリースタート衝突ペア、39 ラウンド SHA-256 に対するセミフリースタート衝突ペア、そして 28 ラウンド SHA-512（SHA-384、SHA-512/224、SHA-512/256 も同様）に対する衝突ペアを現実的な時間内で初めて発見するとともに、31 ラウンド SHA-512 に対する衝突ペアを計算量 $2^{115.6}$ で発見できることを示した。

The First Practical Collision for 31-Step SHA-256

Yingxin Li, Fukang Liu, Gaoli Wang, Xiaoyang Dong, Siwei Sun

Asiacrypt 2024

SHA-256 と SHA-512 の衝突攻撃に関する論文である。Eurocrypt 2013 で Mendel らは SHA-256 の衝突攻撃が 64 ステップ中 31 ステップまで実行可能であることを示した。この攻撃は $2^{65.5}$ の計算量と 2^{34} のメモリ量を必要とする。その後、Eurocrypt 2024 で Li らは Mendel らの 31 ステップ SHA-256 の衝突攻撃を改善した。Li らの攻撃は $2^{49.8}$ の計算量と 2^{48} のメモリ量を必要とする。現状において Li らの攻撃が最良であるものの、依然として 31 ステップ SHA-256 の衝突攻撃はメモリ量の観点で現実的であるとは言えない。また、計算量を T、メモリ量を M、ワードサイズを n（SHA-256 は $n = 32$）とすると、これらの既存攻撃は $T \times M \approx 2^{3n}$ という条件を満たす必要があり、Li らの攻撃は最良のタイムメモリトレードオフを実現している。このため、Li らの手法でメモリ量を削減して、計算量を増加させる場合、現実的な時間内での衝突発見がより困難となる。このような制約事項を取り除き、31 ステップ SHA-256 の衝突攻撃に対して現実的な計算量とメモリ量で実行可能な攻撃手法を開発することが本研究のモチベーションとなる。

本研究では 31 ステップ SHA-256 に対するメモリ効率の高い攻撃手法を新たに開発する。新しい攻撃手法も既存手法と同様に中間一致技術を使用する。既存手法では、内部状態における 3 つのワード（A_{-1}, A_{-2}, A_{-3}）を同時に一致させるという条件があり、この条件が上記の制約事項に影響を及ぼしていた。そこで、提案手法では、1 つのワード A_{-1} のみを一致させるという条件に緩和し、残りの 2 つのワード（A_{-2}, A_{-3}）を on-the-fly で有効性チェックを行うこととした。その結果、最適な場合において $2^{1.5n}$ の計算量を達成しつつ、メモリ量を $2^{0.5n}$ まで削減することに成功した。提案手法を 31 ステップ SHA-256 に適用した結果、現実的な計算量（64 スレッドを使用して約 1.2 時間）と無視できるくらい小さいメモリ量（2^{10} オーダー）で衝突メッセージペアを発見した。同様に、提案手法を 31 ステップ SHA-512 に適用した結果、計算量を $2^{115.6}$ から $2^{94.7}$ へ、メモリ量を $2^{77.3}$ から $2^{35.2}$ へ、それぞれ改善することに成功した。

Probabilistic Linearization: Internal Differential Collisions in up to 6 Rounds of SHA-3

Zhongyi Zhang, Chengan Hou, Meicheng Liu

Crypto 2024

SHA-3 の衝突攻撃に関する論文である。SHA-3 の衝突攻撃に関する研究では主に差分攻撃と内部差分攻撃をベースとした手法が提案されている。前者の手法は FSE 2012 で提案されたターゲット差分アルゴリズム（TDA: Target Difference Algorithm）をベースに、後者は FSE 2013 で提案されたターゲット内部差分アルゴリズム（TIDA: Target Internal Difference Algorithm）をベースに発展してきた。これらのアルゴリズムでは SHA-3 の S-box を線形化し、

線形化された方程式から連立方程式を組み立てた後、この連立方程式を解く、という手順となっている。既存の線形化手法（linearization）では連立方程式を決定論的に組み立てるため、線形方程式の数が多すぎる傾向となり、大きいサイズの capacity を持ち、かつ安全性レベルの高い SHA-3 インスタンス（例えば、ラウンド数の多い SHA3-384、SHA3-512、SHAKE256、など）において TDA/TIDA を適用したとしても、現実的な時間内に連立方程式を解くことが困難となる。

この問題を解決するために、本研究では最大差分密度部分空間（maximum difference density subspace）と呼ばれる新しい概念を導入した確率的線形化手法（probabilistic linearization）を提案するとともに、この提案手法を TIDA に導入してアルゴリズムの一般化を行った。従来手法とは異なり、提案手法では連立方程式を確率論的に組み立てることが可能となり、結果として連立方程式における線形方程式の数を減らすことが可能となる。これは衝突を引き起こすためのデータ量の削減に繋がる。確率論的な手法であるため、連立方程式の解が必ずしも正しい入力差分を示すとは限らない。このため、複数の連立方程式を組み立て、これらの解に正しい入力差分が含まれているかを判定することで攻撃を成功させることが可能となる。

提案手法を全ての SHA-3 インスタンスに適用した。結果として、SHA3-384 と SHAKE256 に対する衝突攻撃では攻撃可能ラウンド数を更新することができ、それぞれ 5 ラウンドと 6 ラウンドまで攻撃が可能であることを示した。また、その他の SHA-3 インスタンスについては既存の計算量を削減することに成功した。具体的には、4 ラウンド SHA3-512 と 5 ラウンド SHA3-224/SHA3-256/SHAKE128 に対して既存の衝突攻撃を改善した。

Automating Collision Attacks on RIPEMD-160

Yingxin Li, Fukang Liu, Gaoli Wang

FSE 2024

ハッシュ関数 RIPEMD-160 に対する解析論文である。RIPEMD-160 の複雑な二重ブランチ構造のため、既存の衝突攻撃では 80 ラウンド中 36 ラウンド、既存のセミフリースタート衝突攻撃では 40 ラウンドまでしか攻撃が有効ではなかった。

本研究では、Eurocrypt 2023 で提案された 36 ラウンド RIPEMD-160 に対する衝突攻撃を改善するため、異なるメッセージ差分を使用して攻撃可能ラウンド数の拡張可能性について検討し、最終的に 40 ラウンドまで拡張可能な 1 つの可能性を特定した。この可能性について詳細に分析するために、SAT/SMT モデリング手法を応用して 40 ラウンド RIPEMD-160 の符号付き差分特性を探索した。結果として、現実的な時間内で衝突を引き起こすようなメッセージ差分を発見し、既存攻撃の大幅な改善を実現した。また、セミフリースタート衝突攻撃に関して、RIPEMD-160 の構造的な特徴を詳細に分析し、解析のボトルネックとなっている部分を解消することで、最大で 43 ラウンドまでのセミフリースタート衝突攻撃が実行可能であることを示した。

2.4.3 その他の解読技術

Improved Provable Reduction of NTRU and Hypercubic Lattices

Henry Bambury, Phong Q. Nguyen

PQCrypto 2024

NTRU 格子および超立方格子（hypercubic lattice）に対するブロックワイズ基底簡約（blockwise reduction）攻撃に関する論文である。NTRU 格子は NTRU および FALCON で、超立方格子は HAWK で、それぞれ用いられている。先行研究として、n 次元超立方格子上の SVP（最短ベクトル問題）に対する、成功確率が証明可能な格子基底簡約

が Ducas（DCC 2023）により与えられている。この論文では n 次元 SVP が $n/2$ 次元の SVP に帰着されていた。同様の帰着が $2n$ 次元 NTRU 格子に対しても可能であると Gama、Howgrave-Graham、Nguyen（Eurocrypt 2006）により予想されていた。

超立方格子と NTRU 格子が持つ特徴的な幾何学的性質は暗号処理の効率化のために用いられる。著者らはこれら格子基底の幾何学的な特徴を利用したブロックワイズ基底簡約アルゴリズムを提案した。特に NTRU について求めるベクトルの復元が証明可能なブロックワイズ基底簡約アルゴリズムを初めて与え、上述の Gama、Howgrave-Graham、Nguyen による予想を解決した。また超立方格子については、先行研究である Ducas の証明可能簡約アルゴリズムの拡張および改良となっている。

この結果を得るために著者らは、超立方格子を含む、$\lambda_1(L)\lambda_1(L^\times) < 1 - 1/\mathrm{poly}(n)$ を満たす格子 L に対するブロックワイズ基底簡約アルゴリズムを与えている。ここで $L^\times$ は L の双対格子である。特に NTRU-HPS では、復号エラーを防ぐためのパラメータ調整により $\lambda_1(L)\lambda_1(L^\times) < 1/2$ を満たす格子が用いられるため、著者らの方式が適用可能である。Ducas のアルゴリズムではブロックサイズ $n/2$ のほぼ正確な SVP オラクルが要求されていたが、本論文では $\sqrt{2}$-近似へと条件が緩和されている。結果として、SVP サブルーチンの計算時間が $2^{\alpha n/2}$ $(\alpha < 1)$ ならば、$\mathbb{Z}^n$-格子同型性判定問題を $2^{\alpha n/2+o(n)}$ で解くことができると著者らは報告した。加えて著者らは、NTRU 格子について、提案攻撃と既存のヒューリスティック攻撃を比較した。本論文で提案された証明可能な攻撃は、$n/2 + \Theta(n/\log n)$ のブロックサイズが必要である一方、ヒューリスティック攻撃はブロックサイズを $4n/9 + \Theta(n/\log n)$ しか必要としない。著者らはこれをヒューリスティック解析と証明可能解析の計算量の間に差が出る興味深い例として報告した。

One Vector to Rule Them All: Key Recovery from One Vector in UOV Schemes

Pierre Pébereau

PQCrypto 2024

耐量子計算機署名方式である MAYO を含む、UOV 型の署名方式に対する攻撃論文である。UOV 型の署名方式では、署名者が線形の連立方程式を解くことで署名可能であるのに対して、署名偽造を行う攻撃者は計算量的に困難な 2 次の連立方程式を解く必要があるというトラップドア構造を用いている。この困難性の差を生むのが oil subspace であり、署名鍵に対応する。

本論文では、oil subspace の中の 1 本のベクトルと検証鍵の情報から、署名鍵を多項式時間で復元するアルゴリズム、およびあるベクトルが oil subspace に含まれるかどうかを判定する多項式時間アルゴリズムが与えられた。また、同様の結果が UOV-like な署名方式である MAYO や VOX に対しても可能であるという結果を著者らは得ている。これらの結果は、UOV 型の署名の安全性が oil subspace の中の 1 本のベクトルを発見することの困難性に依存していることを示しており、サイドチャネル攻撃への対策を強化する必要があることが著者らにより報告された。

検証用コードは `https://github.com/pi-r2/OneVector` で公開されており、UOV の代表的なパラメータに対して数秒から 2.5 分で署名鍵が復元可能であるとしている。

Extending Regev's Factoring Algorithm to Compute Discrete Logarithms

Martin Ekerå, Joel Gärtner

PQCrypto 2024

離散対数問題に対する量子解析論文である。本研究は、Regev[arXiv: 2308.06572] により与えられた素因数分解の量子アルゴリズムに関連がある。著者らは、Regev のアルゴリズムが Shor のアルゴリズムの多次元化であり、Shor

のアルゴリズムが素因数分解問題と離散対数問題をどちらも解くことを観察したうえで、Regev のアルゴリズムを離散対数問題を解くアルゴリズムへと自然に拡張した。

Regev の素因数分解アルゴリズムでは、適当な $(a_1, \ldots, a_d)$ を用いて $\prod a_i^{z_i} \bmod N$ の周期を発見するために、格子基底の中から良いベクトルを探し出す。本研究では同様に、インスタンス $(g, x = g^e)$ からの離散対数の計算のため適当な群の要素 $(g_1, \ldots, g_{d-1})$ を基底として、$x^{z_d} \prod g_i^{z_i} = 1$ を満たす点 $(z_1, \ldots, z_d)$ がなす格子の中から良いベクトルを選びだす。

結論として、巡回群 $\mathbb{F}_p^*$ 上の離散対数問題を Shor のアルゴリズムよりも少ないリソースで解く量子アルゴリズムが構成された。しかし応用上価値の高い楕円曲線上の離散対数問題を解く量子アルゴリズムの構成は未解決として残されている。

2.5 量子コンピュータが共通鍵暗号の安全性に及ぼす影響の調査及び評価

2019 年度、暗号技術調査ワーキンググループ（暗号解析評価）は、「量子コンピュータが共通鍵暗号の安全性に及ぼす影響の調査及び評価」を外部評価により実施し、本報告書（以下、2019 年度外部評価報告書[*3]）を CRYPTREC の技術調査報告書として公開した。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「CRYPTREC 暗号技術ガイドライン（耐量子計算機暗号）[*4]」と「耐量子計算機暗号の研究動向調査報告書[*5]」（以下、PQC ガイドライン等）を策定した。なお、2019 年度外部評価報告書が公開されていることを踏まえ、PQC ガイドライン等では共通鍵暗号の耐量子安全性に関する内容を含めないこととしている。

共通鍵暗号の耐量子安全性に関する技術動向が著しいことを踏まえ、2024 年度は「量子コンピュータが共通鍵暗号の安全性に及ぼす影響の調査及び評価」を外部評価で実施し、本結果を 2019 年度外部評価報告書に反映させる形で更新を行った。

2.5.1 実施概要

量子コンピュータが共通鍵暗号の安全性に及ぼす影響について、公開されている解析手法やその影響範囲などについてまとめ、考察などを行い、2019 年度外部評価報告書に最新の情報を反映させて、報告書（以下、2024 年度外部評価報告書）を作成する。

2.5.2 調査結果の概要

Q2 モデル[*6]での攻撃、Q1 モデル[*7]での攻撃、ハッシュ関数への攻撃に分け、種々の主要な方式（CRYPTREC 電子政府推奨暗号リスト掲載方式および NIST 標準軽量暗号 Ascon）の安全性への影響を確認した。

■Q2 モデルでの攻撃　古典攻撃モデルにおいて安全性が保証されている共通鍵暗号技術（GCM、CBC-MAC、など）に対して多項式時間で実行可能な攻撃が存在するが、Q2 モデルでは攻撃対象が量子回路上に実装されている必要があ

[*3] https://www.cryptrec.go.jp/exreport/cryptrec-ex-2901-2019.pdf
[*4] https://www.cryptrec.go.jp/report/cryptrec-gl-2004-2022.pdf
[*5] https://www.cryptrec.go.jp/report/cryptrec-tr-2001-2022.pdf
[*6] 攻撃者の計算機が量子コンピュータであるとともに、攻撃者に量子オラクル（量子重ね合わせ状態の入出力でクエリ可能なオラクル）が与えらえるモデルのことである。量子クエリ攻撃モデルともいう。
[*7] 攻撃者の計算機が量子コンピュータであるが、その他の設定が基本的に古典的な攻撃モデル（汎用コンピュータへの入出力でクエリ可能なオラクルを使用するモデル）と同じモデルのことである。古典クエリ攻撃モデルともいう。

る。これは非常に特殊な状況であり、現状では既存の共通鍵暗号技術に Q2 モデルでの攻撃の影響が及ぶことは無いと考えられる。特に、CRYPTREC 電子政府推奨暗号リスト掲載方式や NIST 標準軽量暗号 Ascon の安全性を評価する上で Q2 モデルでの攻撃を考慮する必要はない。

■Q1 モデルでの攻撃　Q2 モデルでの攻撃とは異なり、古典攻撃モデルにおいて安全性が保証されている共通鍵暗号技術に対して多項式時間で実行可能な攻撃は存在しない。ただし、古典攻撃モデルにて $2k$ ビット以上の安全性があったとしても、Q1 モデルでの安全性が k ビット以下になる例（例えば、2XOR 構成と呼ばれる構造のブロック暗号）も示されているため、暗号技術ごとに確認が必要である。

Q1 モデルにおいて、ハッシュ関数を除く CRYPTREC 電子政府推奨暗号リスト掲載方式や NIST 標準軽量認証暗号の Ascon-AEAD/Ascon-80pq の安全性に量子計算機が与える影響は、「Grover のアルゴリズム[*8]を用いると k ビット鍵の全数探索が $O(2^{k/2})$ で実行できるため、長期的に保護したいデータには鍵長が 192 ビットや 256 ビットの暗号技術を使用した方が賢明である」と考えられる。これらの暗号技術について、Q1 モデルで安全性が期待できる範囲を表 2.3 でまとめる。

■ハッシュ関数への攻撃　SHA-256、SHA-512、SHA3-256 では、量子計算機が使用可能になると衝突攻撃の攻撃可能段数が古典攻撃モデルと比べて伸びることが知られている。表 2.4 で示すように、安全性マージンは十分に確保されているものの、今後の動向を注視する必要がある。

その他、CRYPTREC 電子政府推奨暗号リスト掲載のハッシュ関数や NIST 標準軽量ハッシュ関数の Ascon-Hash256/Ascon-XOF128 の安全性に量子計算機が及ぼす影響は、汎用量子攻撃（特に、BHT のアルゴリズム[*9]）のみを考慮すれば十分である。これらの暗号技術について、BHT のアルゴリズムを適用するのに必要な計算時間と量子メモリの概算値を表 2.5 でまとめる。

2.5.3　2019 年度外部評価報告書における結論との差異

具体的な方式の実用面での安全性評価について、2019 年度外部評価執筆時からの大きな差異は、ハッシュ関数の衝突攻撃可能段数が古典攻撃モデルの場合に比べて量子攻撃モデルの場合に伸びることが明らかになってきたということである。このような状況の変化に応じ、2019 年度版外部評価報告書の結論を表 2.6 で示すように変更した。その他の結論部分について大きな差異はない。

2.5.4　外部評価報告書に対する暗号技術評価委員会の見解

提出された外部評価報告書[*10]は、2024 年度の調査対象である共通鍵暗号の耐量子安全性に関する技術動向調査として十分な内容を含んでいると考えられることから、本報告書を CRYPTREC の技術調査報告書とすることが承認された。

また、提出された外部評価報告書から、CRYPTREC 電子政府推奨暗号リスト掲載方式と NIST 標準軽量暗号 Ascon の安全性に量子コンピュータが及ぼす影響は汎用量子アルゴリズム（特に、Grover のアルゴリズムと BHT のアルゴリズム）のみを考慮すれば十分であるという結論を得た。本結論をもって、暗号技術評価委員会の見解とした。

[*8] https://dl.acm.org/doi/10.1145/237814.237866
[*9] https://dl.acm.org/doi/10.1145/261342.261346
[*10] https://www.cryptrec.go.jp/exreport/cryptrec-ex-3401-2024.pdf

表 2.3: ハッシュ関数を除く電子政府推奨暗号リスト掲載方式、Ascon-AEAD、そして Ascon-80pq について、Q1 モデルで安全性が期待できる範囲（Grover のアルゴリズム：$\leq 2^{k/2}$）

技術分類	方式名	鍵長 k（ビット）	安全性が期待できる範囲
ブロック暗号	AES Camellia	128 192 256	時間 $\leq 2^{64}$ 時間 $\leq 2^{96}$ 時間 $\leq 2^{128}$
ストリーム暗号	KCipher-2	128	時間 $\leq 2^{64}$
秘匿モード	CBC, CFB CTR, OFB XTS	k	時間 $\leq 2^k$ かつ 古典的に安全性が保証される範囲
認証付き 秘匿モード	CCM, GCM	k	時間 $\leq 2^k$ かつ 古典的に安全性が保証される範囲
メッセージ 認証コード	CMAC, HMAC	k	時間 $\leq 2^k$ かつ 古典的に安全性が保証される範囲
認証暗号	ChaCha20-Poly1305	256	時間 $\leq 2^{128}$ かつ 古典的に安全性が保証される範囲
	Ascon-AEAD128	128	時間 $\leq 2^{64}$ かつ 古典的に安全性が保証される範囲
	Ascon-pq80	160	時間 $\leq 2^{80}$ かつ 古典的に安全性が保証される範囲

2.6 委員会開催記録

表 2.7 のとおり、2024 年度暗号技術評価委員会は 2 回開催された。各会合の開催日および主な議題は以下のとおりである。

2.7 暗号技術調査ワーキンググループ開催記録

表 2.8 のとおり、2024 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 2 回開催された。各会合の開催日および主な議題は以下のとおりである。

表 2.4: 古典・量子攻撃モデルでの SHA2 と SHA3 に対する衝突攻撃の比較

対象	出力長	段数	攻撃可能段数	
			古典	量子
SHA-256	256	64	31	38
SHA-512	512	80	31	39
SHA3-224	224	24	5	6
SHA3-256	256	24	5	6

表 2.5: 電子政府推奨暗号リスト掲載のハッシュ関数、Ascon-Hash256、Ascon-XOF128 に対して BHT のアルゴリズムを適用するのに必要な計算時間と量子メモリの概算値：$\min(2^{c/3}, 2^{h/3})$

方式名	キャパシティ c	出力長 h	計算時間	メモリ
SHA-256	–	256	$2^{85.3}$	$2^{85.3}$
SHA-512/256	–			
SHA3-256	512			
SHA-384	–	384	2^{128}	2^{128}
SHA3-384	768			
SHA-512	–	512	$2^{170.7}$	$2^{170.7}$
SHA3-512	1024			
SHAKE128	256	$\ell \geq 256$	$\min(2^{85.3}, 2^{\ell/3})$	$\min(2^{85.3}, 2^{\ell/3})$
SHAKE256	512	$\ell \geq 256$	$\min(2^{170.7}, 2^{\ell/3})$	$\min(2^{170.7}, 2^{\ell/3})$
Ascon-Hash256	256	256	$2^{85.3}$	$2^{85.3}$
Ascon-XOF128	256	$\ell \geq 0$	$\min(2^{85.3}, 2^{\ell/3})$	$\min(2^{85.3}, 2^{\ell/3})$

表 2.6: ハッシュ関数に関する技術動向の変化

2019 年度外部評価報告書執筆時	現在
古典的に 128 ビット安全性のあるハッシュ関数の安全性に量子攻撃が現実的な脅威を直接及ぼすとは現状考えづらい。	重要な用途に供するハッシュ関数の出力長（スポンジ構造の場合は出力長に加えてキャパシティ長）は BHT のアルゴリズムの計算量 $O(2^{n/3})$ を基準にして 384 ビットや 512 ビットのものを用いた方が無難であると考えられる。

表 2.7: 暗号技術評価委員会の開催状況

回	開催日	議案
第 1 回	2024 年 7 月 9 日	• 暗号技術評価委員会の活動計画に関する報告 • 暗号技術調査ワーキンググループ（耐量子計算機暗号）の活動計画案に関する審議 • 外部評価「量子コンピュータが共通鍵暗号の安全性に及ぼす影響の調査及び評価」の実施に関する審議 • 監視状況報告 • CRYPTREC シンポジウム 2024 開催に関する報告
第 2 回	2025 年 3 月 3 日	• 暗号技術調査ワーキンググループ（耐量子計算機暗号）の活動内容に関する報告 • 耐量子計算機暗号ガイドラインと調査報告書の改定に関する審議 • 外部評価報告書「量子コンピュータが共通鍵暗号の安全性に及ぼす影響の調査及び評価 2024 年度版」の内容に関する報告・審議 • 監視状況報告 • CRYPTREC 暗号リストの仕様参照先の変更に関する報告 • 暗号技術評価委員会の活動報告案に関する審議 • CRYPTREC Report 2024 の目次案に関する審議 • CRYPTREC シンポジウム 2025 開催に関する報告

表 2.8: 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	2024 年 7 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）の活動計画に関する報告 • 予測図の更新に関する報告 • 耐量子計算機暗号の調査活動に関する各委員からの報告 • ガイドライン・調査報告書の追記・改定方針のアップデートに関する報告・審議 • ガイドライン・調査報告書の執筆担当者、担当事務局員、第 2 回ワーキンググループまでのスケジュールに関する審議
第 2 回	2025 年 3 月 3 日	• 2024 年度予測図の更新に関する審議 • ガイドライン・調査報告書の執筆内容に関する各委員からの報告 • 今後の作業スケジュールに関する確認 • 暗号技術調査ワーキンググループ（耐量子計算機暗号）の活動報告案に関する審議

第 3 章

暗号技術調査 WG（耐量子計算機暗号）の活動

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

2020 年度第 2 回暗号技術検討会において、2021 年度から暗号技術評価委員会の活動計画として 2 年をかけて PQC の研究動向を調査し、ガイドラインを作成することが決定された。暗号技術評価委員会は 2021-2022 年度に暗号技術調査ワーキンググループ (耐量子計算機暗号) を設置し、ガイドライン及び調査報告書を作成し、公開した。

その後も、PQC 関連の技術開発、標準化活動が世界的に活発であることから、引き続き、暗号技術調査ワーキンググループ（耐量子計算機暗号）（以下、PQC WG）を設置して下記 2 点の活動を行うことが 2023 年度第 1 回暗号技術評価委員会において承認された。

(1) NIST の PQC 標準化において第 4 ラウンドが進行中であることをはじめ耐量子計算機暗号に関する技術開発、標準化活動が引き続き世界的に活発であることから、動向を 2023 年度から 2 年間かけて調査・把握し、ガイドラインの改定を行う。
(2) 「素因数分解の困難性に関する計算量評価」、「楕円曲線上の離散対数計算の困難性に関する計算量評価」の予測図の更新についても検討し、更新する。

3.2　耐量子計算機暗号ガイドラインの作成

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

年度	回	耐量子計算機暗号ガイドラインの議論・決定・報告
2023 年度	第 1 回 2023/9/13	・追記・改定の方針について議論 ・執筆担当者を議論
	第 2 回 2024/1/19	・追記・改定すべき項目及びその章立ての決定 ・調査の中間報告
2024 年度	第 1 回 2024/7/26	・中間報告、追加及び削除すべき暗号方式があれば議論
	第 2 回 2025/2/3	・内容の確定

3.2.2 2023 年度第 1 回 WG（9/13）での実施内容及び決定事項

- ガイドライン及び調査報告書の作成に関して
  - 2022 年度版ガイドライン、調査報告書をベースに 2024 年度版ガイドライン、調査報告書を作成する。改訂扱いではなく新規の扱いとすることで合意した。
  - 「はじめに」の章は 2022 年度版では同一の内容であったが、2024 年度版では他の章と同様に調査報告書に詳細な記述、ガイドラインは抜粋とする。
  - 「PQC の活用方法」の章は 2022 年度版ではガイドラインのみであったが、2024 年度版からは調査報告書にも含めることで合意。それに合わせて内容を拡充し、ガイドラインには公知の事実のみを載せ、詳細は調査報告書に載せる。
  - 以下に例示したいくつかの暗号方式の扱いに関しては今後の動向を注視し、2023 年度第 2 回以降の WG で改めて議論を行うこととした。
    - NIST 標準化が決まっているが FIPS 文書が発行されていないため詳細が流動的なもの
    - NIST Additional Signatures 候補の中で、格子、符号、多変数、同種写像、ハッシュ関数のカテゴリに含まれるもの
    - MPC-in-the-Head など新たなカテゴリとして分類されているもの
- 記載すべき項目及び章立てと執筆担当者

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

- 調査活動と執筆活動の方針
  - PQC の研究成果が発表される主要な国際会議 Crypto、Eurocrypt、Asiacrypt、PQCrypto を中心に、開発・標準化の動向に関しても 2024 年 9 月 30 日までの情報を可能な限り調査する。その他主要な動向があれば可能な限り取り上げる。
- 2023 年度第 2 回 PQC WG で調査内容の報告
  - 各章の執筆担当者が 2023 年度第 2 回 PQC WG において、その時点までの調査内容を報告する。

3.2.3 2023 年度第 2 回 WG（2024/1/19）での実施内容及び決定事項

- 各章の執筆担当者が 2023 年度第 2 回 PQC WG において、その時点までの調査内容を報告。各章の大まかな更新内容が確認された。
- 調査報告書及びガイドラインの執筆方針について以下の執筆方針が決定された。
  - 1 章についても他の章と同様に、調査報告書は専門的な内容、ガイドラインには調査報告書から技術的に複

雑な内容を省略し抜粋した内容とする。
  - 米国で FIPS 化が決まっている方式に関して、2024 年 9 月 30 日までに正式版が出版された場合には FIPS 版と更新部分を、FIPS 化されない場合には出版時期によって対応が異なるが、Initial draft 版とその更新差分を記述する方針とする。
  - Additional Signatures の候補を各章に記載するかどうかは執筆担当者の判断とする。
  - MPC-in-the-Head、Additional Signatures 提案方式の中でガイドライン中の計算問題の分類に含まれないものについて、大きな動きは認知されていないことから新章とはしない。

3.2.4 2024 年度第 1 回 WG（2024/7/26）での実施内容及び決定事項

- 各章の執筆担当者が 2024 年度第 1 回 PQC WG において、その時点までの調査内容を報告。各章の大まかな更新内容が確認された。
- 調査報告書及びガイドラインの執筆方針について以下の執筆方針が決定された。
  - 「はじめに」の章内にあるセキュリティレベルの表現について修正する。
  - 2024 年 4 月に発表された LWE 問題の量子アルゴリズムに言及する文章を記述。
  - FIPS 化の決まっている方式に関しては 2023 年度第 2 回と同様の方針（その後、2024 年 8 月に正式に FIPS 203,204,205 が発表されたことで調査報告書とガイドラインの記述方針が確定された）。

3.2.5 2024 年度第 2 回 WG（2025/2/3）での実施内容及び決定事項

- 各章の執筆担当者から提出された原稿に基づき、執筆担当者から執筆内容の概要が説明され、相談事項が共有された。また、以下の事項が決定された。
  - 1 章：韓国 KpqC の最終方式 4 件の情報を追記する。ガイドライン内の「現在」を 2024 年 9 月 30 日であると明記する。
  - 5 章：MAYO のパラメータが空欄となっているが公開後に追記する。
  - 全体を見直し、2 月 20 日までに執筆担当者は担当事務局員と合意の取れた原稿を完成させ事務局に提出する。
- 以下の事項は今後の検討事項とし、事務局の案をメーリングリスト上で審議することとした。
  - ガイドライン内で PQC という単語が指す範囲について、他の CRYPTREC 文書の内容との整合性も考慮し、公開鍵暗号のみに限るのではない定義を考える。
  - 句読点の「、。」に関して、数式中の表現との混乱を避けるための方針を決める。
- 評価委員会後にコメントがあった場合の対応について確認された。
- メーリングリストでの審議、および、関連する修正を行った上で、PQC WG 案として、ガイドライン・調査報告書の公開を暗号技術評価委員会および暗号技術検討会に付議することが承認された。
- NIST の状況を鑑みて、2025 年度以降も PQC WG を設置し、ガイドライン／調査報告書の更新を行うことが要望された。

3.2.6　2024 年度メール審議（2025/2/3〜）実施内容及び決定事項

- 第 2 回 WG において決定された「PQC という単語がさす範囲」と「句読点の利用方針」について事務局案を作成し、メール審議を行った。
  - PQC を「古典での実装が可能かつ耐量子性を持つことを技術的に判断可能な暗号技術」とする。また、これまで「耐量子性」と表現していた用語を「耐量子計算機性」に変更することで合意。
  - 句読点は「,」「。」を用いる。ただし数式内などで全角の「,」を用いると不自然になる場合には半角「,」を用いる方針で合意。

3.3　「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

- 「今後の予測図の取り扱い」に基づいて予測図の更新を行った (図 1、2)。素因数分解問題の困難性および楕円曲線上の離散対数問題の困難性に関する計算量評価に大幅な進展はなかったため、2024 年 6 月・11 月のベンチマーク結果を追加した。

＜今後の予測図の取り扱い＞
(1) いわゆるムーアの法則を仮定して外挿線を年度末からプラス 20 年後まで従来どおり直線で引き、評価に大きな変動がないと考えられる限りにおいては、安全サイドに倒した評価※として予測図を当面の間更新していく。
＜今後の公開鍵暗号のパラメータ選択＞
(2) 公開鍵暗号のパラメータ選択に関する対応方針については、安全性以外にも相互接続性など、運用上の観点もあるため、暗号技術評価委員会だけではなく、暗号技術検討会、暗号技術活用委員会や関係各所などを含めて検討する。

※各国・国際標準化機関等により示されている主要な暗号技術の安全性基準と比較すると、より現状に即した評価となっており、危殆化時期は他機関等が規定している暗号技術の利用期限よりも先に延びている。

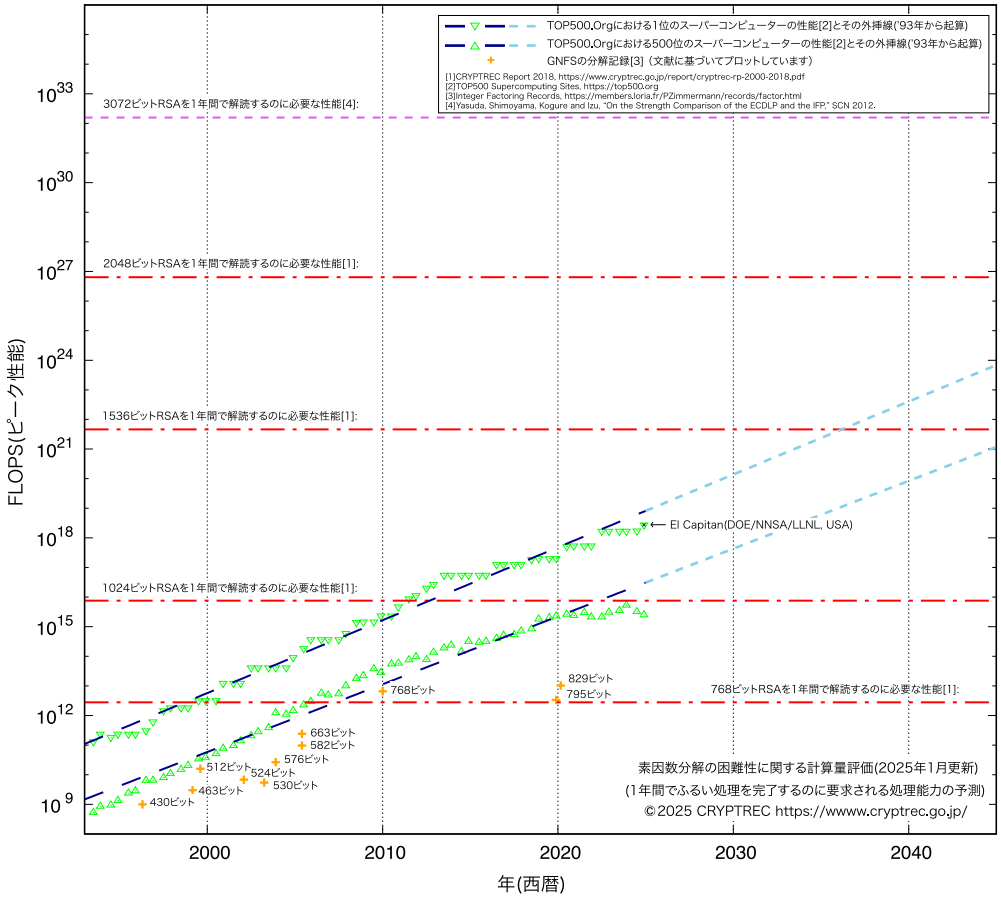

図 3.1: 素因数分解の困難性に関する計算量評価 (2025 年 1 月更新)[*1]

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

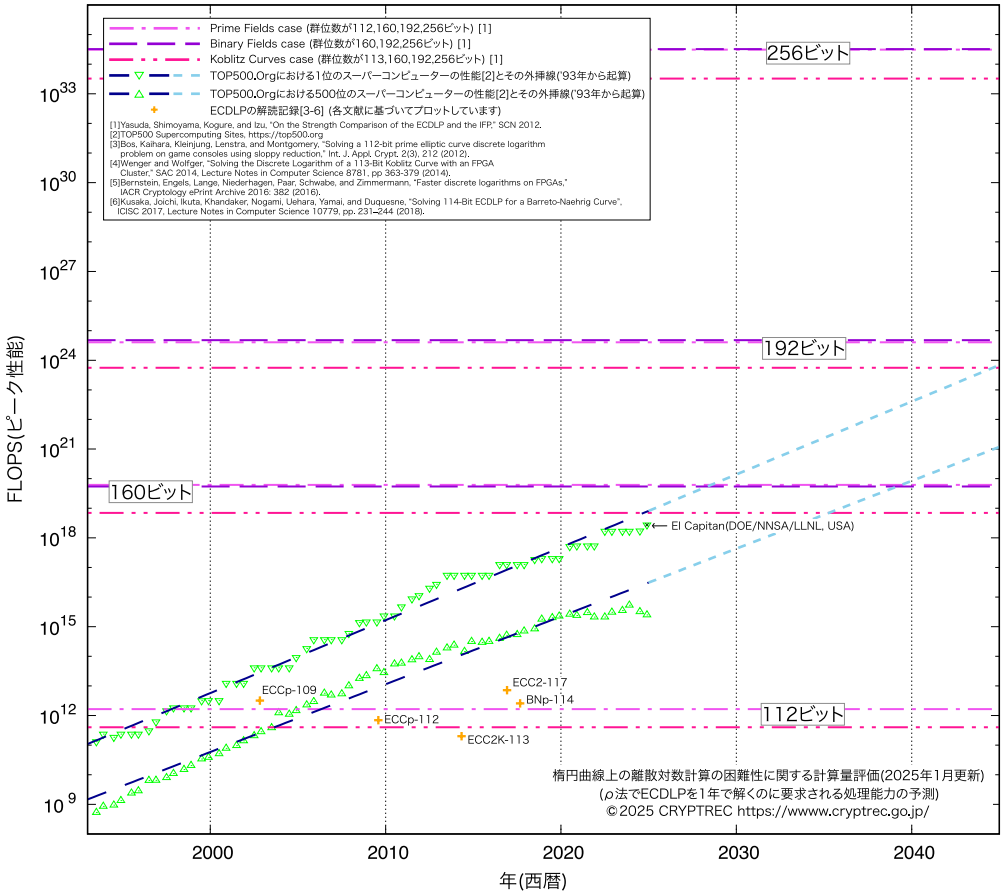

図 3.2: 楕円曲線上の離散対数計算の困難性に関する計算量評価 (2025 年 1 月更新)[*2]

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

付録 A

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）

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

令和5年3月30日
デジタル庁・総務省・経済産業省
（最終更新：令和6年5月16日）

電子政府推奨暗号リスト

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

技術分類		暗号技術
公開鍵暗号	署名	DSA（注18）
		ECDSA
		EdDSA
		RSA-PSS（注1）
		RSASSA-PKCS1-v1_5（注1）
	守秘	RSA-OAEP（注1）
	鍵共有	DH
		ECDH
共通鍵暗号	64ビットブロック暗号（注2）	該当なし
	128ビットブロック暗号	AES
		Camellia
	ストリーム暗号	KCipher-2
ハッシュ関数		SHA-256
		SHA-384
		SHA-512
		SHA-512/256
		SHA3-256
		SHA3-384
		SHA3-512
		SHAKE128（注12）
		SHAKE256（注12）
（次ページに続く）		

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

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

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

技術分類		暗号技術
暗号利用モード	秘匿モード	CBC
		CFB
		CTR
		OFB
		XTS(注17)
	認証付き秘匿モード(注13)	CCM
		GCM(注4)
メッセージ認証コード		CMAC
		HMAC
認証暗号		ChaCha20-Poly1305
エンティティ認証		ISO/IEC 9798-2
		ISO/IEC 9798-3
		ISO/IEC 9798-4

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

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

（注4） 初期化ベクトル長は96ビットを推奨する。

（注12） ハッシュ長は256ビット以上とすること。

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

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

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

推奨候補暗号リスト

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

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

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

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

（注7） 平文サイズは64ビットの倍数に限る。

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

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

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

運用監視暗号リスト

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

技術分類		暗号技術
公開鍵暗号	署名	該当なし
	守秘	RSAES-PKCS1-v1_5（注8）（注9）
	鍵共有	該当なし
共通鍵暗号	64ビットブロック暗号（注15）	3-key Triple DES（注19）
	128ビットブロック暗号	該当なし
	ストリーム暗号	該当なし
ハッシュ関数		RIPEMD-160
		SHA-1（注8）
暗号利用モード	秘匿モード	該当なし
	認証付き秘匿モード（注16）	該当なし
メッセージ認証コード		CBC-MAC（注11）
認証暗号		該当なし
エンティティ認証		該当なし

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

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

（注11） 安全性の観点から、メッセージ長を固定して利用すべきである。

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

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

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

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

更新履歴情報

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

付録 B

CRYPTREC 暗号リスト掲載暗号技術の仕様参照先・問い合わせ先一覧

B.1 電子政府推奨暗号リスト

公開鍵暗号

暗号技術名	DSA (Digital Signature Algorithm)
仕様参照先	NIST Federal Information Processing Standards Publication 186-4 (July 2013), Digital Signature Standard (DSS) https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

暗号技術名	ECDSA (Elliptic Curve Digital Signature Algorithm)
仕様参照先 1	SEC 1: Elliptic Curve Cryptography (September 20, 2000, Version 1.0) https://www.secg.org/SEC1-Ver-1.0.pdf
仕様参照先 2	ANS X9.142-2020, Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA) https://www.x9.org/

暗号技術名	EdDSA (Edwards-Curve Digital Signature Algorithm)
仕様参照先 1	NIST FIPS PUB 186-5, Digital Signature Standard (DSS), February 3, 2023 https://csrc.nist.gov/publications/detail/fips/186/5/final
仕様参照先 2	Edwards-Curve Digital Signature Algorithm (EdDSA) https://www.rfc-editor.org/rfc/rfc8032

暗号技術名	RSA Public-Key Cryptosystem with Probabilistic Signature Scheme (RSA-PSS)
仕様参照先	PKCS #1: RSA Cryptography Standard Version 2.2 https://www.rfc-editor.org/rfc/rfc8017.html

暗号技術名	RSASSA-PKCS1-v1_5
仕様参照先	PKCS #1: RSA Cryptography Standard Version 2.2 https://www.rfc-editor.org/rfc/rfc8017.html

暗号技術名	RSA Public-Key Cryptosystem with Optimal Asymmetric Encryption Padding (RSA-OAEP)
仕様参照先	PKCS #1: RSA Cryptography Standard Version 2.2 https://www.rfc-editor.org/rfc/rfc8017.html

暗号技術名	DH (Diffie-Hellman Scheme)
仕様参照先 1	ANSI X9.42-2003, Public Key Cryptography for The Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography https://x9.org
仕様参照先 2	NIST Special Publication 800-56A Revision 2 (May 2013), Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar2.pdf

暗号技術名	ECDH (Elliptic Curve Diffie-Hellman Scheme)
仕様参照先 1	SEC 1: Elliptic Curve Cryptography (September 20, 2000, Version 1.0) https://www.secg.org/SEC1-Ver-1.0.pdf
仕様参照先 2	NIST Special Publication SP 800-56A Revision 2 (May 2013), Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar2.pdf

共通鍵暗号

暗号技術名	AES
仕様参照先	NIST FIPS PUB 197, Specification for the ADVANCED ENCRYPTION STANDARD (AES), November 26, 2001 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197-upd1.pdf

暗号技術名	Camellia
仕様参照先	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 email: camellia-ml@ntt.com

暗号技術名	KCipher-2
仕様参照先	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 email: kiyomoto@kddi-research.jp

ハッシュ関数

暗号技術名	SHA-256, SHA-384, SHA-512, SHA-512/256
仕様参照先	NIST FIPS PUB 180-4, Secure Hash Standard (SHS), August 2015 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf

暗号技術名	SHA3-256, SHA3-384, SHA3-512, SHAKE128, SHAKE256
仕様参照先	NIST FIPS PUB 202, SHA-3 Standard: Permutation-Based Hash and Extendable- Output Functions, August 2015 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf

暗号利用モード（秘匿モード）

暗号技術名	CBC, CFB, CTR, OFB
仕様参照先	NIST SP 800-38A, Recommendation for Block Cipher Modes of Operation: Methods and Techniques 2001 Edition https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf

暗号技術名	XTS
仕様参照先	NIST SP 800-38E, Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices, January 2010 https://csrc.nist.gov/publications/detail/sp/800-38e/final

暗号利用モード（認証付き秘匿モード）

暗号技術名	CCM
仕様参照先	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) https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38c.pdf

暗号技術名	GCM
仕様参照先	NIST SP 800-38D, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, November 2007 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38d.pdf

メッセージ認証コード

暗号技術名	CMAC
仕様参照先	NIST FIPS SP 800-38B, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, May 2005 (Updated Oct. 2016) https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38b.pdf

暗号技術名	HMAC
仕様参照先	NIST FIPS PUB 198-1, The Keyed-Hash Message Authentication Code (HMAC), July 2008 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.198-1.pdf

認証暗号

暗号技術名	ChaCha20-Poly1305
仕様参照先	ChaCha20 and Poly1305 for IETF Protocols, June 2018 https://www.rfc-editor.org/rfc/rfc8439.html

エンティティ認証

暗号技術名	ISO/IEC 9798-2
仕様参照先	ISO/IEC 9798-2:2008, Information technology – Security techniques – Entity Authentication – Part 2: Mechanisms using symmetric encipherment algorithms, 2008. 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 日本規格協会（https://www.jsa.or.jp/）から入手可能

暗号技術名	ISO/IEC 9798-3
仕様参照先	ISO/IEC 9798-3:1998, Information technology – Security techniques – Entity Authentication – Part 3: Mechanisms using digital signature techniques, 1998. ISO/IEC 9798-3:1998/Amd.1:2010, Information technology – Security techniques – Entity Authentication – Part 3: Mechanisms using digital signature techniques. Amendment 1, 2010 日本規格協会（https://www.jsa.or.jp/）から入手可能

暗号技術名	ISO/IEC 9798-4
仕様参照先	ISO/IEC 9798-4:1999, Information technology – Security techniques – Entity Authentication – Part 4: Mechanisms using a cryptographic check function, 1999. 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 日本規格協会（https://www.jsa.or.jp/）から入手可能

B.2 推奨候補暗号リスト

公開鍵暗号

暗号技術名	PSEC-KEM
仕様参照先	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 email: publickey-ml@ntt.com

共通鍵暗号

暗号技術名	CIPHERUNICORN-E
仕様参照先	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 email: nec-pki@security.jp.nec.com

暗号技術名	Hierocrypt-L1
仕様参照先	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 総合研究所 AI デジタル R&D センター 電子政府推奨暗号 問い合わせ窓口 email: rdc-crypt-info@ml.toshiba.co.jp

暗号技術名	MISTY1
仕様参照先	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 MISTY1 問い合わせ窓口 email: cryptrec_misty1_info@pj.MitsubishiElectric.co.jp

暗号技術名	CIPHERUNICORN-A
仕様参照先	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 email: nec-pki@security.jp.nec.com

暗号技術名	CLEFIA
仕様参照先	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 email: clefia-q@jp.sony.com

暗号技術名	Hierocrypt-3
仕様参照先	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 総合研究所 AI デジタル R&D センター 電子政府推奨暗号 問い合わせ窓口 email: rdc-crypt-info@ml.toshiba.co.jp

暗号技術名	Enocoro-128v2
仕様参照先	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 email: dai.watanabe.td@hitachi.com

暗号技術名	MUGI
仕様参照先	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 インシデントマネジメントセンタ セキュリティスペシャリスト 栗田 博司 email: hiroshi.kurita.wp@hitachi.com

暗号技術名	MULTI-S01
仕様参照先	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 インシデントマネジメントセンタ セキュリティスペシャリスト 栗田 博司 email: hiroshi.kurita.wp@hitachi.com

メッセージ認証コード

暗号技術名	PC-MAC-AES
仕様参照先	https://jpn.nec.com/rd/tg/dss/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 email: k-minematsu@nec.com

B.3 運用監視暗号リスト

公開鍵暗号

暗号技術名	RSAES-PKCS1-v1_5
仕様参照先	PKCS #1: RSA Cryptography Standard Version 2.2 https://www.rfc-editor.org/rfc/rfc8017.html

共通鍵暗号

暗号技術名	Triple DES
仕様参照先	NIST SP 800-67 Revision 2, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, November 2017 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-67r2.pdf

ハッシュ関数

暗号技術名	RIPEMD-160
仕様参照先	The hash function RIPEMD-160 https://homes.esat.kuleuven.be/~bosselae/ripemd160.html

暗号技術名	SHA-1
仕様参照先	NIST FIPS PUB 180-4, Secure Hash Standard (SHS), August 2015 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf

メッセージ認証コード

暗号技術名	CBC-MAC
仕様参照先	ISO/IEC 9797-1:1999, Information technology – Security techniques – Message Authentication Codes(MACs) – Part 1: Mechanisms using a block cipher, 1999 日本規格協会（https://www.jsa.or.jp/）から入手可能

付録 C

量子コンピュータが共通鍵暗号の安全性に及ぼす影響の調査及び評価

2024 年度外部評価報告書「量子コンピュータが共通鍵暗号の安全性に及ぼす影響の調査及び評価 2024 年度版」について、その概要を記載する。なお、本報告書の全文は CRYPTREC の Web ページ（https://www.cryptrec.go.jp/exreport/cryptrec-ex-3401-2024.pdf）から取得可能である。

量子コンピュータが共通鍵暗号の安全性に及ぼす影響の調査及び評価 2024 年度版

NTT 社会情報研究所 / NTT 理論量子情報研究センタ
細山田 光倫

2025 年 1 月

エグゼクティブサマリー

量子コンピュータが共通鍵暗号の安全性に及ぼす影響の調査及び評価を行った．文献調査により，次のことを確認した．

- 量子コンピュータを用いた攻撃のモデル，特にハッシュ関数以外の（秘密鍵を用いる）共通鍵暗号技術への攻撃のモデルには Q1 モデルと Q2 モデルの二種類のモデルが存在する．Q1 モデルにおいては鍵の埋め込まれたオラクルは古典的な攻撃モデルと同じ古典オラクルだが，Q2 モデルにおいては鍵の埋め込まれたオラクルが量子オラクルとなり，攻撃者はオラクルへの量子重ね合わせクエリを行える．Q2 モデルの攻撃を実行するには攻撃対象の暗号技術が（秘密鍵を埋め込んだうえで）量子回路上に実装されている必要がある．
- Q2 モデルにおいては，古典的に安全とされている共通鍵暗号技術（CBC-MAC や GCM など）に多項式時間の攻撃が存在する．多項式時間の攻撃には Simon の量子アルゴリズムが用いられる．
- Q1 モデルにおいては，古典的に安全とされている共通鍵暗号技術に多項式時間の攻撃は現在の所存在しない．しかし従来より認識されていた Grover のアルゴリズムによる鍵全数探索の高速化のみならず，暗号技術の構造に依存した様々な攻撃が存在する．Even-Mansour 暗号および類似の構造を持つ暗号技術に対しては，Q1 モデルであっても Simon のアルゴリズムを活用して古典的攻撃より効率的な攻撃が実行できる．更に，古典的に $2k$ ビット以上の安全性があっても Q1 モデルでの安全性が k ビットを下回る例が示されている．
- 古典的な安全性証明は，ideal permutation model などプリミティブを理想化したモデルでなく反証可能な標準的仮定（ブロック暗号の PRP 安全性など）に依拠するものであれば，Q1 モデルでそのまま通用する．つまり，古典的な安全性証明がついていれば（ブロック暗号などのプリミティブに対する攻撃の影響を考慮する必要はあるが）データ量やクエリ回数などについて安全性が保障される範囲は古典的設定と Q1 モデルで変わらない．Ideal permutation model や ideal cipher model での安全性証明は Q1 モデルでも通用するとは限らず，方式ごとに安全性を再精査する必要がある．
- 既存研究において使用可能と想定されている量子計算のリソースは論文によって異なり，攻撃コストの評価方法も様々である．特にハッシュ関数への汎用攻撃 (衝突探索など) については，使用可能な量子計算のリソースに関する想定や攻撃コストの評価方法に応じて最良の攻撃が異なる．
- 多くのハッシュ関数について，量子計算機が使えるようになれば衝突攻撃の攻撃可能段数が伸びることが示されている．攻撃可能段数が伸びるものには，CRYPTREC の電子政府推奨暗号リストにある SHA-256 と SHA-512 および SHA3-256 が含まれるが，破れているのはそれぞれ 64 段中 38 段，80 段中 39 段，および 24 段中 6 段で，まだ余裕がある．段数削減なしで衝突耐性が破れる心配は今の所無いと考えられるが，今後も研究の進展を注視する必要がある．

また調査した文献の内容に考察を加えた結果，次のような結論を得た．

- ある関数を計算するための古典計算機向けのプログラムコードがあった場合その関数を量子

回路上に実装することが可能になるため，Q2 モデルにおいて多項式時間の攻撃が可能な暗号技術については，例え難読化処理等を施しても，その関数 (例えば CBC-MAC でメッセージからタグを計算する関数) を実装して秘密鍵を埋め込んだコードを，量子コンピュータを持った攻撃者に手渡すべきではない．しかし，攻撃対象となる暗号技術が量子回路上に実装されているような（あるいは量子回路上に移植可能となるような）非常に特殊な状況でない限り，既存の共通鍵暗号技術，特に CRYPTREC の電子政府推奨暗号リストにある共通鍵暗号技術や最近 NIST 標準として選ばれた Ascon に，Q2 モデルの攻撃の影響が及ぶことは現状では無いと考えられる．

- 従来から指摘されていた通り，Grover のアルゴリズムによって k ビット鍵の全数探索が時間 $O(2^{k/2})$ で実行可能になるため，長期的に保護したいデータには秘密鍵の鍵長が 128 ビットの暗号技術でなく 192 ビットや 256 ビットの暗号技術を使用するのが賢明であると考えられる．またハッシュ関数の衝突攻撃可能段数が古典より伸びることが判明していることも考慮すると，重要な用途に供するハッシュ関数の出力長（スポンジ構造の場合は出力長に加えキャパシティ長）は BHT のアルゴリズムの計算量 $O(2^{n/3})$ を基準にして 384 ビットや 512 ビットのものを用いた方が無難であると考えられる．
- CRYPTREC の電子政府推奨暗号リストの共通鍵暗号技術および Ascon の安全性に量子コンピュータが直接与える影響は，Grover のアルゴリズムや BHT のアルゴリズム以上のものは現状では無いと考えられる．しかし Even-Mansour 暗号への Q1 モデルにおける攻撃のように安全性に現実的な影響を直接及ぼす可能性のある攻撃が今後も発見される可能性があり，また種々のハッシュ関数で古典より攻撃可能段数が伸びているため，研究の動向には今後も注意を払っておく必要がある．

2019 年度版のまとめとの差異

具体的な方式の実用面での安全性評価について，2019 年度版執筆時から今回までの間で一番大きな差異は，ハッシュ関数の衝突攻撃可能段数が古典計算機しか使えない場合に比べて伸びることが明らかになってきたということである．これを踏まえ，2019 年度版ではハッシュ関数について「古典的に 128 ビット安全性のあるハッシュ関数の安全性に量子攻撃が現実的な脅威を直接及ぼすとは現状考えづらい」と結論付けていたものを「重要な用途に供するハッシュ関数の出力長（スポンジ構造の場合は出力長に加えキャパシティ長）は BHT のアルゴリズムの計算量 $O(2^{n/3})$ を基準にして 384 ビットや 512 ビットのものを用いた方が無難であると考えられる」と変更した．まとめの他の部分については，2019 年度とこの 2024 年度版で大きな差異は無い．

付録 D

学会等での主要論文一覧

目次

D.1 暗号技術の安全性評価に関する論文一覧

表 D.1 に暗号技術の安全性評価に関する論文のリストをカテゴリー別に示す。★ は電子政府推奨暗号の安全性に直接関わる技術動向である。

表 D.1: 暗号技術の安全性評価に関する論文一覧

公開鍵暗号	会議名	頁
Key Recovery Attack on the Partial Vandermonde Knapsack Problem	Eurocrypt 2024	64
Cryptanalysis of Rank-2 Module-LIP in Totally Real Number Fields	Eurocrypt 2024	64
Provable Dual Attacks on Learning with Errors	Eurocrypt 2024	65
The Complexity of Algebraic Algorithms for LWE	Eurocrypt 2024	65
Evaluating the Security of CRYSTALS-Dilithium in the Quantum Random Oracle Model	Eurocrypt 2024	66
Reduction from Sparse LPN to LPN, Dual Attack 3.0	Eurocrypt 2024	66
The Hardness of LPN over Any Integer Ring and Field for PCG Applications	Eurocrypt 2024	67
Asymptotics and Improvements of Sieving for Codes	Eurocrypt 2024	67
Practical Attack on All Parameters of the DME Signature Scheme	Eurocrypt 2024	65
The Supersingular Endomorphism Ring and One Endomorphism Problems are Equivalent	Eurocrypt 2024	67
Isogeny Problems with Level Structure	Eurocrypt 2024	68
Algorithms for Matrix Code and Alternating Trilinear Form Equivalences via New Isomorphism Invariants	Eurocrypt 2024	68
The NISQ Complexity of Collision Finding	Eurocrypt 2024	69
A Refined Hardness Estimation of LWE in Two-step Mode	PKC 2024	72
Cryptanalysis of the Peregrine Lattice-Based Signature Scheme	PKC 2024	73
On Algebraic Embedding for Unstructured Lattices	PKC 2024	73
Ring/Module Learning with Errors Under Linear Leakage - Hardness and Applications	PKC 2024	74
Improved Cryptanalysis of HFERP	PKC 2024	74
Breaking Parallel ROS: Implication for Isogeny and Lattice-Based Blind Signatures	PKC 2024	74
A Simpler and More Efficient Reduction of DLog to CDH for Abelian Group Actions	PKC 2024	75
An Algorithm for Efficient Detection of (N, N)-Splittings and Its Application to the Isogeny Problem in Dimension 2	PKC 2024	75
An Improved Practical Key Mismatch Attack Against NTRU	PQCrypto 2024	76
Analyzing Pump and Jump BKZ Algorithm Using Dynamical Systems	PQCrypto 2024	76

	Adaptive Attacks Against FESTA Without Input Validation or Constant-Time Implementation	PQCrypto 2024	77
	The Blockwise Rank Syndrome Learning Problem and Its Applications to Cryptography	PQCrypto 2024	77
	Cryptanalysis of the SNOVA Signature Scheme	PQCrypto 2024	78
	One Vector to Rule Them All: Key Recovery from One Vector in UOV Schemes	PQCrypto 2024	22
	Practical Key-Recovery Attack on MQ-Sign and More	PQCrypto 2024	78
	Practical and Theoretical Cryptanalysis of VOX	PQCrypto 2024	79
	Fault Attack on SQIsign	PQCrypto 2024	79
	A Subexponential Quantum Algorithm for the Semidirect Discrete Logarithm Problem	PQCrypto 2024	79
★	Extending Regev's Factoring Algorithm to Compute Discrete Logarithms	PQCrypto 2024	22
	Improved Provable Reduction of NTRU and Hypercubic Lattices	PQCrypto 2024	21
	Properties of Lattice Isomorphism as a Cryptographic Group Action	PQCrypto 2024	80
	Polynomial XL: A Variant of the XL Algorithm Using Macaulay Matrices over Polynomial Rings	PQCrypto 2024	81
	Solving the Tensor Isomorphism Problem for Special Orbits with Low Rank Points: Cryptanalysis and Repair of an Asiacrypt 2023 Commitment Scheme	Crypto 2024	81
	FuLeakage: Breaking FuLeeca by Learning Attacks	Crypto 2024	81
★	Space-Efficient and Noise-Robust Quantum Factoring	Crypto 2024	82
★	Quantum Complexity for Discrete Logarithms and Related Problems	Crypto 2024	82
	A Systematic Study of Sparse LWE	Crypto 2024	83
	Quantum Lattice Enumeration in Limited Depth	Crypto 2024	83
	Cryptanalysis of Lattice-Based Sequentiality Assumptions and Proofs of Sequential Work	Crypto 2024	84
	Memory-Sample Lower Bounds for LWE	Crypto 2024	84
	Not Just Regular Decoding: Asymptotics and Improvements of Regular Syndrome Decoding Attacks	Crypto 2024	85
	Lossy Cryptography from Code-Based Assumptions	Crypto 2024	85
	CryptAttackTester: high-assurance attack analysis	Crypto 2024	86
	Improved Algorithms for Finding Fixed-Degree Isogenies Between Supersingular Elliptic Curves	Crypto 2024	86
	Radical $\sqrt[N]{\text{élu}}$ Isogeny Formulae	Crypto 2024	86
	Quantum Advantage from One-Way Functions	Crypto 2024	87
	Is ML-Based Cryptanalysis Inherently Limited? Simulating Cryptographic Adversaries via Gradient-Based Methods	Crypto 2024	87
	Sparse Linear Regression and Lattice Problems	TCC 2024	92
	Worst-Case to Average-Case Hardness of LWE: An Alternative Perspective	TCC 2024	93

	Improved Differential Meet-In-The-Middle Cryptanalysis	Eurocrypt 2024	71
	Probabilistic Extensions: A One-Step Framework for Finding Rectangle Attacks and Beyond	Eurocrypt 2024	71
★	Revisiting Differential-Linear Attacks via a Boomerang Perspective with Application to AES, Ascon, CLEFIA, SKINNY, PRESENT, KNOT, TWINE, WARP, LBlock, Simeck and SERPENT	Crypto 2024	88
★	New Approaches for Estimating the Bias of Differential-Linear Distinguishers	Crypto 2024	89
★	Key Collisions on AES and Its Applications	Asiacrypt 2024	17
★	The Boomerang Chain Distinguishers: New Record for 6-Round AES	Asiacrypt 2024	18
★	Generic Differential Key Recovery Attacks and Beyond	Asiacrypt 2024	18
★	It's a Kind of Magic: A Novel Conditional GAN Framework for Efficient Profiling Side-channel Analysis	Asiacrypt 2024	98
★	Quantum Circuits of AES with a Low-depth Linear Layer and a New Structure	Asiacrypt 2024	99

ストリーム暗号		会議名	頁
★	Boosting Differential-Linear Cryptanalysis of ChaCha7 with MILP	FSE 2024	19
	Massive Superpoly Recovery with a Meet-in-the-Middle Framework – Improved Cube Attacks on Trivium and Kreyvium	Eurocrypt 2024	70

ハッシュ関数		会議名	頁
★	Automating Collision Attacks on RIPEMD-160	FSE 2024	21
	Automatic Preimage Attack Framework on Ascon Using a Linearize-and-Guess Approach	FSE 2024	63
	Classical and Quantum Meet-in-the-Middle Nostradamus Attacks on AES-like Hashing	FSE 2024	63
	Improved Meet-in-the-Middle Nostradamus Attacks on AES-like Hashing	FSE 2024	63
★	New Records in Collision Attacks on SHA-2	Eurocrypt 2024	19
	Diving Deep into the Preimage Security of AES-like Hashing	Eurocrypt 2024	72
★	Probabilistic Linearization: Internal Differential Collisions in up to 6 Rounds of SHA-3	Crypto 2024	20
	Generic MitM Attack Frameworks on Sponge Constructions	Crypto 2024	88
	Speeding up Preimage and Key-Recovery Attacks with Highly Biased Differential-Linear Approximations	Crypto 2024	89
★	The First Practical Collision for 31-Step SHA-256	Asiacrypt 2024	20

認証暗号		会議名	頁
	Committing Security of Ascon: Cryptanalysis on Primitive and Proof on Mode	FSE 2024	60
	Practical Related-Key Forgery Attacks on Full-Round TinyJAMBU-192/256	FSE 2024	62

D.2 FSE 2024

Revisiting Yoyo Tricks on AES

Sandip Kumar Mondal, Mostafizar Rahman, Santanu Sarkar, Avishek Adhikari

ブロック暗号 AES に対する解析論文である。本研究では、Asiacrypt 2017 で Ronjom らが報告した AES への Yoyo tricks について詳細に解析する。具体的には、Ronjom らが 5 ラウンド AES と 6 ラウンド AES への Yoyo tricks を使用した識別攻撃（Yoyo 識別攻撃）の成功確率について言及していないことに着目する。最初に、Ronjom らによって報告された 5 ラウンド AES への Yoyo 識別攻撃に必要なデータ量を使用して再現実験を行い、5 ラウンド AES とランダム置換との識別に関する成功確率が著しく低いことを明らかにした。次に、この実験結果に基づき、Yoyo 識別攻撃の成功確率に関する理論値を提供するとともに、この理論値の正確性を論証するための実験を行った。最終的に、5 ラウンド AES と 6 ラウンド AES への Yoyo 識別攻撃を成功させるためには、Ronjom らが報告したデータ量では不十分であることを示すとともに、6 ラウンド AES への Yoyo 識別攻撃をデータ量 2^{128} 未満で実行することが不可能であることを明らかにした。

On Boomerang Attacks on Quadratic Feistel Ciphers: New Results on KATAN and Simon

Xavier Bonnetain, Virginie Lallemand

ブロック暗号 KATAN と Simon に対する解析論文である。本研究では、オリジナルのブーメラン識別子に加え、その派生型である Rotational-XOR (RX) ブーメラン識別子や RX-differential ブーメラン識別子を探索するための新しい理論を確立するとともに、この理論に基づく新しい SMT モデリング手法を提案する。提案手法を KATAN ファミリーと Simon ファミリーに適用することで、既存研究で報告された識別子の有効性を検証し、いくつかの識別子が有効ではないことを明らかにした。さらに、提案手法を KATAN32 と Simon32/64（ブロックサイズが 32 ビットの KATAN と Simon）に適用し、新しい識別子が存在することを示した。具体的には、KATAN32 に対しては最大 151 ラウンドの関連鍵識別子、Simon32/64 に対しては最大 25 ラウンドの関連鍵識別子を発見した。これら新しい識別子は提案手法により有効性が保証されている。

Committing Security of Ascon: Cryptanalysis on Primitive and Proof on Mode

Yusuke Naito, Yu Sasaki, Takeshi Sugawara

認証暗号 Ascon に対するコンテクストコミッティング（context-committing）安全性の解析論文である。認証暗号に対するコンテクストコミッティング安全性は、復号対象の異なるコンテクストである (K, N, A) と (K', N', A') から暗号文・タグのペア (C, T) の衝突発見可能性で評価される。ここで、K は秘密鍵、N はナンス、A は認証データである。

本研究では、Ascon に対するコンテクストコミッティング安全性の解析のために、暗号プリミティブの解析と認証暗号モードの安全性証明に関する結果を示す。最初に、暗号プリミティブの解析として、N と A に差分を挿入した新しい攻撃手法を提案する。この新しい攻撃手法を使用することで、Ascon-128 と Ascon-80pq に対する既存攻撃を 1 ラウンド改善するとともに、3 ラウンド Ascon-128a に対する攻撃に関してもその計算量を 2^{117} から 2^{36} へと改善した。次に、ランダム置換モデルでゼロパディングを備えた Ascon バリアント（ここでは、Ascon-zp という）のコンテクストコミッティング安全性境界が $\min\{\frac{t+z}{2}, \frac{n+t-k-\nu}{2}, \frac{c}{2}\}$ であることを証明した。ここで、鍵長が k ビット、タグ長が t

ビット、パディング長が z ビット、内部状態のサイズが n ビット、ナンス長が ν ビット、キャパシティ長が c ビットである。これは、Ascon-128 と Ascon-128a における安全性境界が $\min\{64+\frac{z}{2}, 96\}$、Ascon-80pq の安全性境界が $\min\{64+\frac{z}{2}, 80\}$ であることを示している。オリジナルの Ascon バリアントでは $z=0$ のため、その安全性境界が 64 ビット（一般的な誕生日攻撃に関する安全性境界）であることを示している。また、平文にゼロパディングを追加することで、Ascon-128 と Ascon-128a では最大 96 ビット、Ascon-80pqd では最大 80 ビットまで安全性を強化できることを示している。

Simplified Modeling of MITM Attacks for Block Ciphers: New (Quantum) Attacks

André Schrottenloher, Marc Stevens

シンプルなキースケジュールを有するブロック暗号への汎用的な中間一致攻撃手法に関する提案論文である。中間一致攻撃はブロック暗号に対する鍵回復攻撃やハッシュ関数に対する原像攻撃への汎用的な解析手法として知られている。また、MILP などの自動探索ツールによって中間一致攻撃を最適化する手法が発展している。MILP を用いた既存の中間一致攻撃では、AES ベースのハッシュ関数に限定した複雑なモデリング手法であったり、シンプルなモデリング手法であっても対象が暗号学的置換（つまり、キースケジュールが適用されない暗号プリミティブ）に限定されていたり、といった限定的な解析手法であった。

本研究では、後者のシンプルなモデリング手法に着目し、シンプルなキースケジュールを有するブロック暗号を対象としたモデリング手法への拡張を試みる。結果として、幅広い暗号プリミティブに対して適用可能なモデリング手法への拡張を実現した。その有効性を検証するために、キースケジュールを簡略化した AES、Saturnin、FUTURE、Haraka-512、PRESENT-80、Fly、PIPO、GIFT-64、などの様々な SPN 型の暗号プリミティブに対して提案手法を適用した。特に、フルラウンドの PIPO-256 と FUTURE に対し、秘密鍵の全数探索よりも効率的に鍵回復攻撃が実行可能であることを示した。

Improved Search for Integral, Impossible-Differential and Zero-Correlation Attacks

Hosein Hadipour, Simon Gerhalter, Sadegh Sadeghi, Maria Eichlseder

積分攻撃、不能差分攻撃、零相関線形攻撃に関し、識別子の特定だけでなく鍵回復の観点から既存の自動探索ツールを改善した論文である。本研究では、Eurocrypt 2023 で Hadipour らによって提案された手法に触発され、以下の観点で既存の自動探索ツールを改善した。最初に、miss-in-the-middle アプローチによる矛盾点の決定をツール使用前に決定しなければならないという制約を取り除いた。次に、セルレベルのモデリング手法からビットレベルのモデリング手法へと拡張した。最後に、鍵回復フェーズのモデリングのために partial-sum 技術を導入した。新たに提案した自動探索ツールの有効性を示すために、Ascon、ForkSKINNY、SKINNY、MANTIS、PRESENT、そして QARMAv2 のような様々な共通鍵暗号プリミティブに適用し、それぞれ既存攻撃の改善に成功した。

Finding Impossible Differentials in ARX Ciphers under Weak Keys

Qing Ling, Tingting Cui, Hongtao Hu, Sijia Gong, Zijun He, Jiali Huang, Xiao Jia

ARX（Addition-Rotation-XOR）型ブロック暗号に対する不能差分を用いた解析論文である。不能差分特性を特定するための自動探索アプローチは数多く提案されてきたが、これらのアプローチはマルコフ暗号と鍵独立性に関する仮定に基づいており、特に軽量 ARX 型暗号ではこの仮定が成立しない場合が散見される。

本研究では、弱鍵設定における ARX 型暗号への不能差分特性探索手法について提案する。ARX 型暗号の構成部品

である算術加算、巡回シフト、XOR の一般的な組み合わせ方法（ローカル構成）について詳細に分析し、弱鍵設定における正確な差分特性を示す。実際の暗号において、ローカル構成上のこれらの差分特性は矛盾する差分伝搬を特定するために使用可能である。このようなアプローチを既存の自動化探索手法と組み合わせることで、弱鍵設定の下での ARX 型暗号に対する不能差分特性を特定するためのフレームワークを提供する。このフレームワークを Speck32/64、LEA、CHAM-64/128 に適用したところ、弱鍵設定の下で最良の不能差分特性を発見した。具体的には、2^{60} 個の弱鍵を有する 8 ラウンド Speck32/64 の不能差分特性、2^{k-1} 個の弱鍵を有する 11 ラウンド LEA の不能差分特性、2^{127} 個の弱鍵を有する 22 ラウンド CHAM-64/128 の不能差分特性である。ここで、k は鍵サイズである。

A Cipher-Agnostic Neural Training Pipeline with Automated Finding of Good Input Differences

Emanuele Bellini, David Gerault, Anna Hambitzer, Matteo Rossi

深層学習ベースの汎用解析手法に関する論文である。Crypto 2019 で Gohr が提案した差分ニューラル解析技術を契機として、現在に至るまで数多くの深層学習ベースの解析手法が提案されてきた。これらの既存研究の大部分は、深層学習に基づいて優れた鍵回復攻撃を実行するために、特定の暗号プリミティブに対する専用のトレーニング手法を適用し、識別子の精度を向上させることに重点が置かれていた。これらの手法は特定の暗号プリミティブに特化されているものであり、他の暗号プリミティブに対して同様の手法を適用することは容易ではない。

本研究では、差分ニューラル解析用の汎用パイプラインを構築することに焦点を当てている。具体的には、この汎用パイプラインは以下の 2 つの特徴を持つ。1 つ目は、最適な差分ニューラル識別子を探索するための入力差分を特定するためのアルゴリズムを持つことである。2 つ目は、暗号プリミティブの構造に依存しないニューラル識別子アーキテクチャである DBitNet を採用していることである。完全に自動化された汎用パイプラインは、特に Speck32 や Simon32 に対して、専用解析手法に匹敵する精度が実現できる。また、他のいくつかの暗号プリミティブ（XTEA、LEA、HIGHT、Simon128、Speck128、PRESENT、KATAN、Gimli）に対する新しい差分ニューラル識別子が存在することを示す。

Practical Related-Key Forgery Attacks on Full-Round TinyJAMBU-192/256

Orr Dunkelman, Shibam Ghosh, Eran Lambooij

認証暗号 TinyJAMBU に対する解析論文である。TinyJAMBU には鍵長の違いによる 3 つのバリアント（TinyJAMBU-128/192/256）が提案されている。本研究では、最初にこれら 3 つのバリアントに対する関連鍵差分特性を分析する。これらの分析結果に基づき、3 つのバリアントに対して鍵回復攻撃が実行可能であることを示す。具体的には、フルラウンドの TinyJAMBU-128/192/256 に対して、それぞれ時間計算量とデータ量が 2^{24}、2^{21}、2^{19} で実行可能である。次に、192 ビットと 256 ビットの鍵長を有する 2 つのバリアント（TinyJAMBU-192/256）を解析対象とし、関連鍵差分攻撃に基づく現実的な時間内で実行可能な偽造攻撃を提案する。結果として、フルラウンドの TinyJAMBU-192 に対する偽造攻撃は 2^{12} 個の関連鍵と 2^{40} の計算量で、フルラウンドの TinyJAMBU-256 に対する偽造攻撃は 2^{10} 個の関連鍵と 2^{32} の計算量で実行可能であることが示された。設計者は関連鍵設定における安全性を主張していないため、本研究結果は設計者の安全性主張を覆すものではない。しかしながら、近年キーコミットメントと呼ばれる認証暗号の性質が注目されており、本研究では TinyJAMBU がこの性質を満たさないことを示している。

Automatic Preimage Attack Framework on Ascon Using a Linearize-and-Guess Approach

Huina Li, Le He, Shiyao Chen, Jian Guo, Weidong Qiu

ハッシュ関数 Ascon-XOF に対する解析論文である。Keccak に対する既存の原像攻撃フレームワークには、線形構造（linear structures）と呼ばれる構造的な特徴を利用する。Keccak と Ascon には構造的な類似性が見られることから、Keccak に対する既存の原像攻撃フレームワークを Ascon-XOF に対する解析用の攻撃フレームワークへと拡張できると考えられる。

本研究では、以下の 2 つの観点から既存の攻撃フレームワークの拡張を行う。1 つ目は、Ascon permutation（Ascon で使用される暗号プリミティブ）の代数的性質に着目した linearize-and-guess アプローチを提案した。このアプローチによって、64 ビットのハッシュ値を出力する 2 ラウンド Ascon-XOF に対して計算量を 2^{39} から $2^{27.56}$ に削減できることを示した。2 つ目は、上記のアプローチを使用して SAT ベースの原像攻撃フレームワークを開発した。このフレームワークにより、最適な構造的特徴を網羅的に探索することが可能となった。結果として、3 ラウンドと 4 ラウンドの Ascon-XOF に対する最良の原像攻撃を示した。

Classical and Quantum Meet-in-the-Middle Nostradamus Attacks on AES-like Hashing

Zhiyu Zhang, Siwei Sun, Caibing Wang, Lei Hu

AES ベースのハッシュ関数に対する解析論文である。Eurocrypt 2006 で Kelsey らが選択ターゲット強制プレフィックス（CTFP: Chosen Target Forced Prefixed）に基づく原像攻撃を提案した。この攻撃では、任意のチャレンジプレフィックス P と攻撃者が事前に準備していたハッシュ値 y に対して、攻撃者が $H(P\|S) = y$ となるようなサフィックス S を生成する。結果として、攻撃者は事前に情報を持っていないプレフィックス P で表される何かしらのイベントを予測したふりをできることから、このような攻撃種別はノストラダムス攻撃としても知られている。その後、Asiacrypt 2022 で量子ノストラダムス攻撃が提案されたものの、一般的な原像攻撃や衝突攻撃ほど研究が盛んではなく、また専用解析手法についても提案されていない。

本研究では、中間一致（MitM）手法に基づくノストラダムス攻撃の専用解析手法について提案する。具体的には、AES ベースのハッシュ関数に対する既存の MitM 原像攻撃に基づき、最適な MitM ノストラダムス攻撃を実行するための新しい MILP モデリング手法を構築し、攻撃におけるオフラインフェーズとオンラインフェーズのトレードオフを実現する。この新しい手法を AES-MMO と Whirlpool に適用し、これら AES ベースのハッシュ関数に対する初めての専用解析ツールとして機能することを論証した。結果として、10 ラウンド中 7 ラウンドの AES-MMO と 10 ラウンド中 6 ラウンドの Whirlpool に対して量子ノストラダムス攻撃が実行可能であることを示した。新しいツールは他の AES ベースのハッシュ関数にも適用可能である。

Improved Meet-in-the-Middle Nostradamus Attacks on AES-like Hashing

Xiaoyang Dong, Jian Guo, Shun Li, Phuong Pham, Tianyu Zhang

AES ベースのハッシュ関数に対する解析論文である。本研究では、前述の Zhang らが示した MitM ノストラダムス攻撃を発展させるために、Asiacrypt 2010 で Guo らが提案したマルチターゲット設定における中間一致攻撃の改良版を自動化ツールに組み込むことを検討する。この改良で攻撃のオンラインフェーズにおける時間計算量の削減が可能となり、古典シナリオと量子シナリオの両方において全体的な時間計算量の削減を可能とする。提案手法を AES-MMO と Whirlpool に適用し、その有効性を示すとともに、前述の Zhang らの結果を改善することに成功した。

D.3 Eurocrypt 2024

Key Recovery Attack on the Partial Vandermonde Knapsack Problem

Dipayan Das, Antoine Joux

低密度の inhomogeneous SIS (Small Integer Solution) 問題の代数的変種である、PV (Partial Vandermonde) ナップザック問題の解析に関する論文である。この問題は、Hoffstein ら (ACNS 2014) および Lu ら (ACISP 2018) による署名方式の構成、Hoffstein ら (Des. Codes Cryptgr. 2015) による公開鍵暗号の構成、Doröz ら (ePrint 2020/520) による多重署名方式の構成など、様々な格子暗号方式の構成に用いられてきた。Boudgoust ら (Crypto 2022) は、PV ナップザック問題の代数的性質を利用した鍵識別攻撃を提案したが、この攻撃は特殊な弱鍵以外では多項式時間で動作しない。

本論文では、PV ナップザック問題に対する別の鍵復元攻撃を提案する。Crypto'22 の攻撃と同様に、この攻撃は格子基底簡約を用いるが、基本となる格子基底アルゴリズムの高速化と次元削減を行った。先行研究とは異なる点として、提案攻撃は PV ナップザック問題を SVP インスタンスではなく uSVP インスタンスに変換する。

提案手法を用いて、既存研究で用いられたパラメータの困難性を再評価した結果、多くのパラメータでは弱鍵が無視できない割合存在することが判明した。例えば、ACISP'18 のパラメータセットの公開鍵には 2^{-19} の確率で弱鍵が含まれ、格子簡約アルゴリズムを用いて中程度のサーバ上で 30 時間で解けることが確認された。同様に ACNS'14 で提案されたパラメータセットも 2^{-19} の割合で弱鍵を含んでおり、それらは 17 時間で解けることが確認された。

Cryptanalysis of Rank-2 Module-LIP in Totally Real Number Fields

Guilhem Mureau, Alice Pellet-Mary, Georges Pliatsok, Alexandre Wallet

格子同型性判定問題 (Lattice Isomorphism Problem: LIP) は 2 つの格子基底 B_1, B_2 が与えられたときに格子が同型であるかどうかを判定する問題である。同型である場合にはある直交行列 O がその証拠 (witness) となり $B_1 = OB_2$ を満たす。近年、LIP をベースとした格子署名がいくつか提案されている。LWE ベース暗号での鍵圧縮を目的とした Ring, Module-LWE の利用と同様に、構造を持つ LIP を安全性の根拠とする方式が多数生まれている。Ducas-Postlethwaite-Pulles-vanWoerden (Asiacrypt 2022, 以下 DPPW22 と表記) により提案された格子署名 Hawk は、NIST PQC Additional Signature 標準化に提出され 2024 年度末現在では第 2 ラウンドまで進んでいる。

著者らは、総実体 K 上のランク 2 の Module 格子上の LIP (Module-LIP) に対する古典多項式時間アルゴリズムを与えている。DPPW22 での Module-LIP は行列を用いた定式化が行われていたが、著者らはそれを R-代数 K_R の直積内の加群 $M_1, M_2 \subset K_R^\ell$ を結ぶのユニタリー変換を探索する問題と再定式化している。ここで、ℓ は問題のランクであり、論文では $\ell = 2$ に対するアルゴリズムを与えている。技術的には加群 M に対する pseudo-basis、pseudo-Gram matrix とその間の同型性の概念を導入し、考え得る変種の中で最も困難であるとした wc-smodLIP$_K^B$ 問題を定義した。これは pseudo-Gram 行列の間の同値関係を与える可逆行列 U を探索する問題であり、整数論的なアルゴリズムを用いていくつかのヒューリスティックの下で多項式時間で可能であることが示される。格子署名 Hawk との関係であるが、本手法が総実体 $Q(\zeta + \zeta^{-1})$ 上で動くアルゴリズムであるのに対し Hawk の安全性がその拡大体 $Q(\zeta)$ 上の LIP であり、総実体でないことから著者らは直接的な攻撃ではないとしているが、今後適用可能な体が拡張される可能性もあると述べている。Proof of concept のコードが `https://gitlab.inria.fr/capsule/code-for-module-lip` に公開されている。

Provable Dual Attacks on Learning with Errors

Amaury Pouly, Yixin Shen

探索版、判定版 LWE 問題はそれぞれ、Z_q 上のエラー付き方程式 $A\boldsymbol{s}+\boldsymbol{e}=\boldsymbol{b}$ に対して $(A,\boldsymbol{b})$ から解 $\boldsymbol{s}$ を求める計算問題，およびランダムに生成されたベクトル $\boldsymbol{r}$ に対して $(A,\boldsymbol{b})$ と $(A,\boldsymbol{r})$ を識別する計算問題として定義される。通常の連立方程式と比較して、エラーベクトル $\boldsymbol{e}$ の存在が問題の困難性を上げている。暗号で用いられるサイズの LWE 問題に対する計算量評価では、主に格子の Primal attack と Dual attack と呼ばれる 2 種類の方式が存在する。Primal attack は問題を q-ary 格子 $L_q(A)$ 上の BDD 問題を通じて探索版 LWE を、dual attack は双対格子 $L_q^{\perp}(A)$ 上の SIS 問題を通じて判定版 LWE を解くものであり、それぞれの攻撃計算量の低い方がパラメータ設定に用いられる。現状の課題として、双方の解析が多くの不正確かつ検証不可能と考えられる仮定に基づいている点があり、実際にいくつかの格子点の分布に関する仮定からは矛盾した結果が得られるという考察がある (Ducas, Pulles, ePrint 2023/302)。著者らは、ヒューリスティックな仮定を取り除いた状態での解析と、その解析が正しいと考えられる問題パラメータの範囲を与えており、その範囲が上記 Ducas らの論文において “contradictory regime” と呼ばれる領域と相補的な関係にあることを突き止めている。著者らは、基本的な dual attack のアルゴリズムの変種 (Modern dual attack) として秘密ベクトル s のいくつかの成分を高確率で復元するアルゴリズムを与えている。これは、$L_q^{\perp}(A)$ の中から Gaussian sampler により短いベクトルのリスト $\{\boldsymbol{w}_i\}$ をサンプリングし、$\sum\cos(2\pi\boldsymbol{w}_i\cdot(\boldsymbol{b}-A\boldsymbol{s}')/q)$ が大きくなる $\boldsymbol{s}'$ を総当たりで探索するものである。総当たりの部分を量子化したアルゴリズムも論文中で考察されている。Kyber512 から 1024 の解析が行われており、Modulus switching を仮定したものとしていないものの双方で、提案アルゴリズムの計算量は仕様書にあるセキュリティレベルを超えると述べられている。

Practical Attack on All Parameters of the DME Signature Scheme

Pierre Briaud, Maxime Bros, Ray Perlner, Daniel Smith-Tone

NIST が最近開始した追加署名の募集に提出された多変数方式 DME に対する攻撃論文である。DME は Double Matrix Exponentiation の略であり、拡大体上の線形写像と非線形写像を交互に組み合わせることで秘密鍵から公開鍵を構成している。公開鍵サイズが他の NIST 署名候補の中でも小さい部類に入るという特徴があるが、サイズ削減のために導入した構造により脆弱性が生まれている。本論文ではこれらの構造を利用して、すべての DME パラメータに対する Gröbner 基底計算アルゴリズムを用いた実時間での代数的攻撃を提案した。

レベル 1 パラメータに対する提案攻撃のコードは `https://github.com/ppbriaud/DMEattack` で公開されており，500ms〜1sec で代理鍵の復元が可能であることが示されている。

The Complexity of Algebraic Algorithms for LWE

Matthias Johann Steiner

LWE 問題に対する代数方程式を通じた解法に関する論文である。Arora と Ge(ICALP, 2011) による線形化解法の提案の後に、Albrecht ら (ACM CCA, 49-2, p.62, 2015, ePrint2014/1018) は Gröbner 基底を用いた解法の計算量を評価した。この計算量評価は入力の代数系が semi-regular であるという仮定と、semi-regular な方程式に対する Hilbert 級数を用いた漸近評価を用いたものであり、精緻なものであるとは言い難かった。この論文では Gröbner 基底の計算量を正確に評価するため、新たに 2 つのアイディアを導入している。1 つ目は方程式系の generic coordinates と呼ばれる性質で、この性質を満たすときには solving degree が Castelnuovo-Monford regularity で押さえられるこ

とが知られている (Caminata and Gorla, WAIFI2020)。LWE 問題から構成された代数方程式系が常にこの性質を満たすことを示すことで、計算時間が変数の個数 n の指数で押さえられる Gröbner 基底計算アルゴリズムの存在を示している。次に、(Semaev and Tenti, J. Algebra, 565, pp. 651-674) の、Gröbner 基底の計算コストが degree of regularity により評価できるという結果を一般化し、LWE 問題を変換した方程式系に適用可能にした。サンプル数が多い場合には方程式系が飽和し計算量が小さくなることが知られているが、degree of regularity からその次数を達成する LWE の最小サンプル数を逆算する手法を提案し、sub-exponential な計算アルゴリズムが存在する範囲を避けることが可能となった。また、NIST 標準方式である Kyber-768 の評価を行い、格子ベース攻撃の方が高速であること、サンプル数が上記範囲に入っていないことを確認している。

Evaluating the Security of CRYSTALS-Dilithium in the Quantum Random Oracle Model

Kelsey A. Jackson, Carl A. Miller, Daochen Wang

NIST 標準化方式である CRYSTALS-Dilithium (ML-DSA, FIPS 204) が安全性の根拠としている計算問題は Module-LWE (MLWE)、Module-SIS (MSIS)、SelfTarget-Module-SIS (SelfTargetMSIS) の 3 種である。前者 2 種は安全性が検討され、古典・量子ともに困難であると考えられている。その一方で、署名の強偽造不可能性を保証する SelfTargetMSIS 問題の理論的な困難性は MSIS 問題との古典的な多項式時間等価性が知られているものの、量子における関係性はこれまで証明されていなかった。この論文では量子ランダムオラクルモデル（QROM）において SelfTargetMSIS が MLWE よりも困難であることを示した。技術的には SelfTargetMSIS の単位行列の部分を一般的な行列とした、Plain-SelfTargetMSIS に変換した後に、Chosen-coordinate binding experiment と collapsing experiment という 2 種類の判定問題を経由して ModuleLWE 問題へと変換している。上述の変換を通じて、SelfTargetMSIS の具体的な量子計算コストが評価可能となった。NIST セキュリティレベル 2,3,5 の量子計算量を基準に q=1 mod 2n の条件のもとで基準を満たすパラメータの再評価を行い、元々の提案方式よりもかなり大きなパラメータが必要となったことを報告している。具体的には公開鍵と署名のサイズが (Kiltz, Lyubashevsky, Schaffner, Eurocrypt 2018) と比較してそれぞれ 2.9 倍、1.3 倍になったと報告されている。

Reduction from Sparse LPN to LPN, Dual Attack 3.0

Kévin Carrier, Thomas Debris-Alazard, Charles Meye-Hilfiger, Jean-Pierre Tillich

符号ベース暗号の安全性評価の多くは ISD（Information set decoding）アルゴリズムによる符号の復号問題の漸近計算量評価により行われてきた。最近提案された RLPN(Reduction to LPN)-decoding アルゴリズム (Carrier, Debris-Alazard, Meyer-Hilfiger, Tillich, Asiacrypt 2022) は線形符号のレート k/n が比較的小さな領域で ISD よりも高速な復号が可能であることが知られている。著者らは符号の復号問題を sparse-LPN 問題へと変換し、さらに plain-LPN 問題へと変換することでより広い領域 ($k/n < 0.42$) においても ISD よりも良い結果を得るアルゴリズムを提案した。著者らはこの手法を LWE 問題に対する dual attack と類似のものと考えており、提案手法の解析技術と格子暗号の解析において提起されていた、サンプリングされたベクトルの独立性のヒューリスティックに関する問題点 (Ducas, Pulles, Crypto 2023) の関係を議論している。技術的には LWE 問題の dual attack と類似している。符号の復号問題を LPN 問題と捉え、双対符号内の低ハミング重みの符号語の探索問題へと変換し、ノイズを求めることで元の符号語を復元している。また、sparse-LPN 問題のインスタンス $(a, a\boldsymbol{s} + e)$ を組み合わせて plain-LPN 問題のインスタンス $(a + a', (a + a')\boldsymbol{s} + e + e')$ に変換することで、ノイズ $e + e'$ が小さくなる替わりに $a + a'$ がスパースとなることで計算量が下がる。この変換には coded-BKW (Guo, Jonansson, Löndahl, Asiacrypt 2014) の技法が用いられ

ている。

The Hardness of LPN over Any Integer Ring and Field for PCG Applications

Hanlin Liu, Xiao Wang, Kang Yang, Yu Yu

LPN 問題を 2 べきの拡大体 F_{2^k} や環 $\mathbb{Z}_N$ へと拡張した計算問題は多くの応用を持つ。その中核にあるのは (Boyle, Couteau, Gilboa, Ishai, ACM CCS 2018) の疑似相関生成器 (pseudorandom correlation generator: PCG) であり、PCG パラダイムと呼ばれる多くのプロトコルが安全性の根拠としている LPN 問題の変種の特徴として以下の点が共通している。

1. F_2 以外の体、環を用いている
2. 特殊なノイズ分布を用いている
3. 10^6 程度の高次元、10^{-5} 程度の低エラーレートの問題である

特に、ノイズ分布として通常はノイズベクトルの各分布を独立にベルヌーイ分布から取る所を、プロトコル設計の必要性から各成分をある範囲の一様分布から取るもの (Exact)、N 次元ベクトルを t 個のスロットに区切り、各スロットにつきノイズを乗せる成分を 1 つのみに制限したもの (Regular) などが用いられ、それぞれ exact-noise LPN、regular-noise LPN と名付けられている。論文ではこれらの特徴を持つ LPN 問題と変種の安全性を再評価し、PCG ライクなプロトコルへの応用を提案している。主要な結果として、exact-noise LPN から regular-noise LPN への帰着で (Feneuil, Joux, Rivain, Crypto 2022) よりも効率の良いものの発見、環 $\mathbb{Z}_{2^\lambda}$ 上の LPN の再評価および 40 ビット程度の計算量の見直し、整数環上の LPN 評価の精密化を主張している。評価アルゴリズムの実装が `http://www.lpnestimator.com/` で公開されている。

Asymptotics and Improvements of Sieving for Codes

Léo Ducas, Andre Esser, Simona Etinski, Elena Kirshanova

格子の最短ベクトルを求めるアルゴリズムである篩 (Sieve) アルゴリズムが符号の Information Set Decoding(ISD) アルゴリズムとの組み合わせにより符号の復号問題に適用可能であるという (Guo, Johansson, Nguyen, ePrint 2023/247) の報告を受け、篩部分のコアを Locality Sensitive Hashing and Filterling (LSH/F) による Near Neighbor Search(NNS) としたアルゴリズムを提案、解析を行っている。結果として、一般的な符号語長 n の線形符号の復号計算量が $2^{0.117n}$ となるアルゴリズムが得られたが、これは近年の ISD である (May, Meurer, Thomae, Asiacrypt 2011) の $2^{0.112n}$ よりも僅かに悪い。NNS を行う際のフィルタリング手法として LSH/F をどのようなものにするかによって漸近計算量が異なるため、random product codes を用いたものだと $2^{0.1001n}$、ハミング距離の場合にしか使えないハッシュ関数を用いたものだと $2^{0.1007n}$ となり、最新の $2^{0.096n}$(Both, May, PQCrypto2018) には及ばないものの、著者らは実装上のオーバーヘッドを考えると最速となる可能性があるとしている。

The Supersingular Endomorphism Ring and One Endomorphism Problems are Equivalent

Aurel Page, Benjamin Wesolowski

同種写像ベースの暗号方式の安全性の根拠となっている計算問題に関する論文である。著者らが取り上げている

- Supersingular Endomorphism Ring 問題: 与えられた超特異楕円曲線に対して、自己準同型環を全て求める計

算問題

- One Endomorphism problem: non-scalar な自己準同型環を 1 つ求める計算問題

著者らは 2 つの問題が、相互に、確率的多項式時間で帰着可能であり、同等であることを示した。その系として以下の暗号学的な応用を示した。

- Endomorphism ring problem の困難性を仮定することで Charles-Goren-Lauter ハッシュ関数が耐衝突性を持つこと、SQIsign identification protocol が一様ランダムな鍵に対して sound であること
- Endomorphism ring problem が超楕円曲線間の任意の同種写像を計算する問題と等価であること（smooth degree の同種写像の場合にのみ結果が知られていた）
- endomorphism ring problem を解く確率的アルゴリズムで、無条件に $O(p^{1/2})$ の計算時間が証明できるものが存在する事（先行研究では一般化リーマン予想を仮定していた）

Isogeny Problems with Level Structure

Luca De Feo, Tako Boris Fouotsa, Lorenz Panny

同種写像ベース暗号の安全性の根拠なっている計算問題の中で、特に 2 つの楕円曲線間の指定された次数を持つ同種写像ϕを求める問題は困難であると考えられてきた。しかしながら、暗号方式の構成のために部分群の情報を付加することで問題が急激に簡単になる現象が発見されており、その性質を用いて鍵共有方式 SIDH は破られている。著者らは同種写像問題の困難性を、同種写像に関する情報の多さによって分類し、どの程度のヒントがあれば問題が多項式時間に落ちるのかを検証している。最も情報が少ないオリジナルの同種写像問題は超楕円曲線 E, E' と次数 d が、SIDH の計算問題ではそれに加え torsion point information$(P, Q, \phi(P), \phi(Q))$ が与えられている。ここで、(P, Q) は $E[N]$ の ordered basis である。Γ を $GL_2(\mathbb{Z}/N\mathbb{Z})$ の部分群とし、基底 (P, Q) に対する Γ-level structure を軌道の集合 $B_E(\Gamma) := \cup_{(P,Q)}\{\gamma \cdot (P, Q) : \gamma \in \Gamma\}$ を定義する。これに対して Γ-SIDH 問題を、(P, Q) に対する $S \in B_E(\Gamma)$ がランダムにとったとき、与えられた $(E, E', d, S, \phi(S))$ から ϕ を復元する問題として定義する。Γ が単位群の場合には SIDH の計算問題となり、多項式時間で計算可能であるが、群が大きくなるほど問題の困難性が増し、$\Gamma = SL_2(\mathbb{Z}/N\mathbb{Z})$ の場合には通常の同種写像問題と同値となる。著者らは、Γ-SIDH 問題が Γ の部分群に対する $(\Gamma \cap SL_2)$-SIDH 問題へと帰着されることを示し、さらに SL_2 の部分群 Γ_0, Γ^* 内での帰着を与え、問題の困難性を整理している。Γ の形と困難性、対応する暗号方式を表として与えている。

Algorithms for Matrix Code and Alternating Trilinear Form Equivalences via New Isomorphism Invariants

Anand Kumar Narayanan, Youming Qiao, Gang Tang

耐量子計算機署名の候補の中で、線形写像の同型性判定問題の困難性に基づくものがいくつか提案されている。この論文で対象としているのは NIST PQC 追加署名方式に提案された MEDS が用いる Matrix Code Equivalence(MCE) 問題と ALTEQ が用いる Alternating Trilinear Form Equivalence (ATFE) 問題である。MCE 問題は 2 つの行列 $C, D \in F_q^{m \times n}$ に対してそれらを結びつける可逆正方行列 A, B で $D = ACB$ を満たすものを探索する計算問題であり、ATFE 問題は 2 つの 3 重線型交代写像 $\phi, \psi : F_q^n \times F_q^n \times F_q^n \to F_q^n$ が与えられたときに任意の u, v, w に対して $\phi(Au, Av, Aw) = \psi(u, v, w)$ を満たす可逆正方行列 A を探索する問題計算である。これらの計算問題の困難性は互いに多項式時間等価であることが示されている。(Grochow, Qiao, Tang, J. Groups, Complexty, Cryptology,

14(2022))。著者らはこれら 2 つの問題に対するヒューリスティックアルゴリズムを提案しその計算量評価を与えている。技術的には先行研究における群作用の不変量を用いて判定を行うという枠組みを踏襲している。MCE 問題の解析では新たな不変量である corank-1 associated invariant を用いた誕生日パラドックスによる衝突発見アルゴリズムで、Gröbner 基底計算を避けることで効率を上げている。ATFE の解析においても isomorphism invariant を用いて同様の衝突発見アルゴリズムを用いている。著者らはまた、MEDS の提案パラメータに対する安全性評価を行い、MEDS のカテゴリー I,III,V がそれぞれビットセキュリティ 102.59、152.55、186.57 であるという結果を得ている。

The NISQ Complexity of Collision Finding

Yassine Hamoudi, Qipeng Liu, Makrand Sinha

値域の大きさが N であるハッシュ関数の値を返すオラクルへのアクセスのみが与えられた状態で、関数の衝突を発見する古典アルゴリズムのクエリ回数が $\Theta(N^{1/2})$ であり、これが最良となることはよく知られた結果である。量子アルゴリズムと量子クエリを許した場合には回数を $\Theta(N^{1/3})$ まで下げることができる (Brassard, Høyer, Tapp, LATIN1998 および Aaronson, Shi, J. ACM, 51-4, pp.595-605, 2004) が、これは理想的な量子デバイスを仮定した場合の理論的な結果であった。著者らは問題設定を Noisy-intermediate Scale Quantum (NISQ) デバイスへと拡張した以下の想定でのクエリ回数について議論している。

1. 古典・量子クエリの両方が可能であり、クエリ結果に従い適応的なハイブリッドアルゴリズムが実行可能。ただし量子クエリの回数は制限されている
2. 量子クエリが実行可能だが、オラクルの戻り値には dephasing, depolarizing のノイズが含まれている
3. 古典・量子のハイブリッドアルゴリズムだが、量子回路の深さには上限が定められている。

著者らはこれらの設定において衝突発見の成功確率の上界とそれを達成する具体的なアルゴリズムを与えている。例えば、1. のモデルでは、c 回の古典クエリと q 回の量子クエリを許した場合の最良成功確率は $\Theta((c^2+cq^2+q^3)/N)$ であると主張している。著者らは (Zhandry, CRYPTO2019) の compressed oracle を拡張した、hybrid compressed oracle と呼ばれる情報理論的な下界証明フレームワークを導入し、成功確率の解析を行い、さらに応用として写像の preimage search のクエリ回数に関する下界を証明している。

Improving Key Recovery Linear Attacks with Walsh Spectrum Puncturing

Antonio Flórez-Gutiérrez, Yosuke Todo

線形解読法に基づく鍵回復攻撃の効率化手法に関する論文である。線形解読法に基づく鍵回復攻撃では、平文、暗号文、秘密鍵の値から線形近似値を決定する関数を類似した写像に置き換えること（鍵回復写像近似：key recovery map approximation）で、データ量の増加を犠牲にして時間計算量またはメモリ量を改善することが可能となる。

本研究では、新しいタイプの鍵回復写像近似を提案する。これは Walsh spectrum puncturing と呼ばれ、Walsh spectrum の非ゼロ係数を削除することで鍵回復攻撃の効率化を目指すものである。この新しい技術を用いることにより、従来手法と比べデータ量の増加を最小限に抑えつつ、時間計算量とメモリ量を大幅に改善することが可能となった。実際に、ブロック暗号の Serpent、GIFT-128、DES、Noekeon に適用し、既存攻撃を改善できることを示した。

Massive Superpoly Recovery with a Meet-in-the-middle Framework – Improved Cube Attacks on Trivium and Kreyvium

Jiahui He, Kai Hu, Meiqin Wang, Hao Lei

Trivium、Kreyvium、Grain-128AEAD のようなストリーム暗号ベースの共通鍵暗号に対する解析論文である。ストリーム暗号に対する強力な解析手法の 1 つにキューブ攻撃がある。キューブ攻撃では、平文・初期化ベクトルの部分集合（cube）に対する出力ビットの係数（superpoly）を復元することで、秘密鍵ビットの情報を抽出することを目的とする。キューブ攻撃に対して有効な解析手法として division property や単項式予測（MP: Monomial Prediction）などの技術が提案されているが、superpoly の復元には莫大なコストがかかるという問題点がある。Asiacrypt 2022 では MP の簡略版としてコア単項式予測（CMP: Core MP）と呼ばれる技術が提案され、効率は向上するものの、精度が犠牲になっているという問題点がある。

本研究では、コア単項式トレイルの代数的意味を明らかにすることで、CMP に関する新たな知見を提供する。具体的には、superpoly を復元するためには、コア単項式トレイルを全て抽出することで十分であることを証明する。これは CMP のみに基づくアプローチであり、CMP が MP と同等の精度を達成できることを実証するものである。さらに、多くの既存研究で導入されており分割統治戦略からアイデアを得て、CMP ベースのアプローチを組み込んだ中間一致攻撃フレームワークを設計し、さらなる高速化を実現した。

Trivium、Kreivium、Grain-128AEAD に対してこのフレームワークを適用し、その有効性を検証した。結果として、最大 851 ラウンドの Trivium と最大 899 ラウンドの Kreyvium に対して superpoly 復元攻撃を実行できることを示した。また、192 ラウンドの Grain-128AEAD に対しては既存の superpoly 復元攻撃よりも 5 倍高速化できることを示した。

A Generic Algorithm for Efficient Key Recovery in Differential Attacks and its Associated Tool

Christina Boura, Nicolas David, Patrick Derbez, Rachelle Heim Boissier, María Naya-Plasencia

ビット置換と線形キースケジュールを持つ SPN 型ブロック暗号に対する解析論文である。差分攻撃はブロック暗号に対する古典的かつ強力な攻撃であり、これまでに様々な解析手法が提案されてきたものの、鍵回復フェーズは依然として煩雑かつエラーが生じやすい手順となっている。

本研究では、識別子が与えられた場合に効率的な鍵推測戦略を出力できる新しいアルゴリズムと関連ツールを提案する。新しいアルゴリズムはグラフ理論に基づいている。ノードはアクティブ S-box を、平文側のエッジは r ラウンドの S-box から $r+1$ ラウンドの S-box への依存関係（暗号文側は逆）を表し、各ノードに対して基本的な戦略を設定することで、暗号全体の最適な鍵推測戦略を生成するアプローチを取っている。

RECTANGLE、PRESENT-80、SPEEDY-7-192、GIFT-64 の 4 つの SPN 型ブロック暗号に対して新しいツールを適用し、それぞれ既存の鍵回復攻撃を改善できることを示した。具体的には、RECTANGLE-128 に対して従来の最良の差分攻撃を 1 ラウンド拡張、PRESENT-80 に対して従来の最良の差分攻撃を 2 ラウンド拡張、SPEEDY に対して既存の鍵回復ステップを改良、そして RECTANGLE-80 および GIFT に対してより効率的な鍵回復戦略を提案した。また、新しいツールは数秒以内に評価結果を出力可能となっている。

Improved Differential Meet-In-The-Middle Cryptanalysis

Zahra Ahmadian, Akram Khalesi, Dounia M'foukh, Hossein Moghimi, María Naya-Plasencia

ブロック暗号に対する汎用解析手法の提案論文である。本研究では、Crypto 2023 で Boura らによって提案された差分中間一致攻撃（MITM）の適用範囲を切り詰め差分に拡張し、さらにこのようなタイプの攻撃を改善するための 3 つの新しいアイデアを紹介する。1 つ目は、オリジナルの差分 MITM よりも長い構造的特性を利用できるようにしたことである。ラウンド鍵の加算が内部状態の一部にしか影響を及ぼさない場合、並列分割（parallel partitioning）技術を応用して 1 ラウンド長い特性を利用できる可能性を見出した。2 つ目は、鍵回復段階を確率論的に改善する方法を提案したことである。鍵候補の一部を確率的に選択し、候補数を減らしながら探索を進めることで攻撃全体の効率を向上させる。3 つ目は、不能差分攻撃で導入されたステートテスト（state-test）技術を組み合わせることである。中間状態において特定の条件を満たさない場合、その鍵候補を排除することで攻撃の範囲を絞り込むことを可能にした。また、切り詰め差分中間一致攻撃の探索を自動化するための MILP ツールを開発した。このツールでは新しい 3 つのアイデアを組み込んでいる。このツールをブロック暗号 CRAFT、SKINNY-64-192、SKINNY-128-384 に適用し、それぞれ最良の攻撃を更新した。

Probabilistic Extensions: A One-Step Framework for Finding Rectangle Attacks and Beyond

Ling Song, Qianqian Yang, Yinchen Chen, Lei Hu, Jian Weng

ブロック暗号に対する汎用解析手法の提案論文である。一般的に、差分攻撃（やそのバリアント）では、効率的な識別子を探索し、確率 1 で前方及び後方にいくつかのラウンドを拡張し、この拡張部分に含まれる秘密鍵を復元するというプロセスが行われる。

本研究では、識別子部分と拡張部分を統合されたエンティティとして扱い、全体的な計算量を削減する、もしくはより多くのラウンド数を持つ暗号に対して攻撃を行うことを目的として、差分攻撃と Rectangle 攻撃を効率化させるためのフレームワークを提案する。このフレームワークでは主に 3 つのアイデアを組み込んでいる。1 つ目は、拡張部分において確率的な差分伝搬を許容することである。これにより、従来よりも多くのラウンド数をカバーする可能性が高まる一方、拡張部分の差分伝搬を考慮した解析が必要となり、解析の複雑性が増すこととなる。2 つ目は、この問題を解決するために、分割束ね（Split-and-Bunch）技術を導入する。従来手法では一度に推測しなければならない鍵ビット数が多く、これが計算量増加の要因であった。新しい技術を導入することで、鍵ビットを小さなグループに分割して推測することが可能となり、これらの推測結果を統合することで計算量の増加を抑制することが可能となった。3 つ目は、全体的な鍵回復戦略を柔軟に選択できるようにしたことである。

新しいフレームワークをいくつかのブロック暗号（Deoxys-BC-384、SKINNY-128-256、ForkSkinny-128-256、CRAFT）に適用し、その効果を検証した。結果として、Deoxys-BC-384 に対して最大 15 ラウンドまで攻撃できることを示した。これは、Deoxys-BC-384 のセキュリティマージンが 1 ラウンドしか残されていないことを示す結果となった。また、CRAFT に対して最大 23 ラウンドまで攻撃できることを示した。これは最良の攻撃を 2 ラウンド更新する結果となった。

Diving Deep into the Preimage Security of AES-like Hashing

Shiyao Chen, Jian Guo, Eik List, Danping Shi, Tianyu Zhang

AES ライクのハッシュ関数に対する解析論文であり、Aoki と Sasaki による中間一致（MitM）攻撃の初期研究に基づき、これらのハッシュ関数に対する原像攻撃や衝突攻撃の自動化を発展させるものである。Eurocrypt 2021 で Bao らは MitM 攻撃の自動化モデルを導入することで、従来の手動解析よりも広範囲な探索空間を取り扱うことを可能にした。その後、推測決定（guess-and-determine）、双方向伝搬（bidirectional propagation）、重ね合わせ内部状態（states in superposition）のような技術が導入されてきたが、初期内部状態が単一の独立した内部状態に限定されること、S-box の入力がバイト全体を推測しないと伝搬されないこと、のような制約があった。

本研究では、これらの制約を排除するための新しい技術を導入する。特に、S-box 線形化手法（S-box linearization）と分散初期構造（distributed initial structures）という新しい技術の導入により、探索空間をさらに拡大することができ、Whirlpool や Streebog のような AES ライクハッシュ関数の構造における自由度を削減した。また、既存のモデリング手法を改良し、軽量な MILP ベースの探索モデルを提示することで、対象のハッシュ関数に対する原像攻撃を改善した。具体的には、10 ラウンド AES-192 ハッシュ関数モード、10 ラウンド Rijndael-192/256 ハッシュ関数モード、7.75 ラウンド Whirlpool に対する初の原像攻撃を達成し、5 ラウンドと 6 ラウンドの Whirlpool、7.5 ラウンドと 8.5 ラウンドの Streebog に対する原像攻撃の計算量削減を達成した。また、6 ラウンドと 6.5 ラウンドの Whirlpool に対する衝突攻撃も改善した。

D.4 PKC 2024

A Refined Hardness Estimation of LWE in Two-step Mode

Wenwen Xia, Leizhang Wang, Geng Wang, Dawu Gu, Baocang Wang

標準方式を含め、多くの格子暗号は LWE 問題の困難性をその安全性の根拠としている。実際のパラメータ設定ではデファクトスタンダードとして、Core-SVP モデルと呼ばれる限られたフレームワークでの攻撃手法による計算量評価が用いられている。これは LWE 問題の Primal(Dual) attack として BDD 問題 (SIS 問題) を通じて uniqueSVP 問題へと変換し、SVP サブルーチンを用いた BKZ アルゴリズムを仮定し、格子基底簡約により短いベクトルが見つかる時点での BKZ のブロックサイズ β に対応する β 次元の最短ベクトルの計算量を基準とするものである。格子暗号のパラメータ設定に用いられる lattice-estimator（Albrecht et al, Asiacrypt 2017）や leaky-LWE-estimator（Dachman-Soled et al, Crypto 2020）等ではこのモデルが用いられている。

一方で、著者らが two-step mode と呼ぶ、BKZ アルゴリズムを用いてある程度基底簡約を行った後に、基底全体の探索を行うフレームワークが知られていた。この論文では、最新の結果を踏まえて two-step mode での LWE 問題の再評価を行っている。主な結果として uniqueSVP 問題を解く場合、BKZ のみで解くよりも two-step mode で解く方が高速であるという経験則の厳密な証明、最新の結果を反映した計算量の上界と下界を計算する lwe-estimator の作成と実験、標準方式 Kyber および Dilithium の再評価がある。leaky-LWE-Estimator と比較すると 2.1 から 3.4 ビット、インデックスとブロックサイズの戦略を改良することで 2.2 から 4.6 ビット程度の計算量の改善が行われた。また、保守的な設定を用いた計算量評価（conservative estimations）では先行研究よりも 4.17 から 8.11 ビット上昇しており、計算量評価の精度が上がっていると主張されている。

実験用のコードは `https://github.com/Summwer/lwe-estimatorwith-pnjbkz.git` で公開されている。

Cryptanalysis of the Peregrine Lattice-Based Signature Scheme

Xiuhan Lin, Moeto Suzuki, Shiduo Zhang, Thomas Espitau, Yang Yu, Mehdi Tibouchi, Masayuki Abe

NIST PQC 標準方式である格子ベース署名方式 FALCON の欠点として、署名生成における格子上の離散ガウス分布からのサンプリングに浮動小数点演算が用いられていることによる実装上の困難と結果の不安定性があった。課題解決のため、サンプリング方法を変更すると効率とセキュリティに影響が出るため、良いサンプリング手法の研究が続けられていた。この論文で対象としている Peregrine 署名方式は FALCON のサンプリング部分を中心二項分布（centered binomial distribution）としたもので、韓国の PQC 標準化コンペティション（KpqC）の第 1 ラウンド候補であった。サンプリング方法を変更したことにより、署名から秘密鍵の情報が漏れないという安全性証明が消えていることに着目した著者らは Peregrine に対する実時間で高確率の秘密鍵復元が可能な攻撃を提案した。公開されている Reference implementation と Peregrine の仕様書に書かれているアルゴリズムとの間には差異があることが指摘されているものの、Peregrine-512 に対して前者では 25,000 個の署名から、後者では 1100 万個の署名から数時間で復元が可能であることを確認している。技術的には (Nguyen, Regev, Eurocrypt 2006) の GGH 暗号、NTRU 署名への統計情報を用いた学習アルゴリズムを適用したものであり、Peregrine の署名に用いられるエラー分布中心二項分布であることから高次元ひし形の組み合わせでとなるという事実を用いている。検証用のコードは `https://github.com/lxhcrypto/Peregrine_attack` で公開されている。

On Algebraic Embedding for Unstructured Lattices

Madalina Bolboceanu, Zvika Brakerski, Devika Sharma

多くの格子暗号は効率化のために Ring-,Module-のような構造を持つ格子 (structured lattice) 上の問題を安全性の根拠としているが、それらの問題の困難性と構造を持たない格子 (unstructured lattice) 上の格子問題との関係性は大きな未解決問題である。一方で、整数上の unstructured lattice は数体上の何らかの order の ideal lattice としてみなせることが知られているが、そのような性質が新たなアルゴリズムや安全性評価につながるかどうかは未知であった。この論文では、Ring-LWE 問題の一般化である Order-LWE 問題 (Bolboceanu, Brakerski, Perlman, Sharma, Asiacrypt 2019) に関する困難性の研究を行った。ここで Order は整数環 O_K の部分環の意味での整環 (order) であり、次元 n の格子となる。著者らはまず、Order-LWE の Primal と Dual 版問題に対して整環のイデアル上の Discrete Gaussian Sampling 問題への量子帰着を証明し、同イデアル上の SIVP への量子帰着を与えることで Order-LWE の困難性を証明している。同様の技法を用いることで、Ring-LWE 問題の困難性を証明している。これは先行研究 (Lyubashevsky, Peikert, Regev, Eurocrypt 2010) での Ring-LWE の困難性の帰着先が O_K の全てのイデアルのなす格子上の近似 SVP であったのに対し、帰着先に全てのイデアルを含む必要はないという新規性を持っている。次に、著者らは任意の数体に対してある整環が存在して Order-LWE 問題が通常の LWE 問題と同様の困難性をもつことを示した。これらは構造を持つ格子問題が一般的には難しいことを示唆するが、条件を満たす整環は著者らが skewed と呼ぶ、基底の 1 つの成分が他のものよりも非常に短いという性質を持つため、暗号への応用には向かないとしている。

Ring/Module Learning with Errors Under Linear Leakage – Hardness and Applications

Zhedong Wang, Qiqi Lai, Feng-Hao Liu

格子暗号の実用において、サイズの削減と効率化のために Ring/Module 等の構造の入った格子の計算問題が多く用いられ、問題の困難性の検証が続けられている。近年では、暗号方式内の秘密ベクトルの一部分を公開することで効率化を行う提案がいくつか行われている。例えば、(Lyubashevsky, Nguyen, Seiler, PKC 2021) のゼロ知識証明においてワンタイムコミットメント内のランダムネスのうち 1 ビットを公開することで 30% 程度 proof size を削減するといったアイディアがある。著者らは、いくつかの暗号方式に関わる Module-LWE (MLWE) 問題の変種を Module-LWE with linear secret leakage(MLWE-LS) として定式化し、その困難性について議論した。より具体的には、環 $R_q = \mathbb{Z}_q[X]/(X^d + 1)$ に対して定義される n 次元 m サンプルの Module-LWE 問題のインスタンス $(A, As + e)$ に加え、攻撃者の指定した $z_1, \ldots, z_k \in R_q^{m+n}$ と $c_1, \cdots, c_k \in R_q$ に対して秘密元 s から計算された値 $\sum_{i=1}^{k} \langle \phi(z_i), \phi(c_i) \rangle$ が与えられる。ただし、$\phi(\cdot)$ は R_q^{ℓ} の元を多項式として表現し $Z_q^{\ell d}$ に埋め込む写像であり、上記 Lyubashevsky らのゼロ知識証明について議論するための調整である。このとき、探索版、判定版問題はそれぞれ s を探索する問題、$(A, As + e)$ と $(A, rand)$ の識別を行う問題として定式化される。著者らは判定版 MLWE-LS 問題の困難性が探索版 MLWE 問題の問題と多項式倍の差を除いて等しいことを証明し、Lyubashevsky らのゼロ知識証明のパラメータをアップデートした。

Improved Cryptanalysis of HFERP

Max Cartor, Ryann Cartor, Hiroki Furue, Daniel Smith-Tone

(Patarin, Eurocrypt 1996) の HFE 公開鍵暗号方式は秘密鍵となる体 K 上の中心写像 f をアフィン変換 $S, T : F_q^n \to F_q^n$、および $K \leftrightarrow F_q^n$ の相互変換を行う同型写像で挟んだものを公開鍵写像 P としており、MinRank 攻撃は中心写像を行列としてみたときのランクの低さを利用して P から S, T, f の復元計算が可能であるため、改良方式では f をなるべく高いランクとする方向で研究が進められてきた。HFERP (Ikematsu et al., PQCrypto 2018) は Q-rank と呼ばれる量を基準に提案された方式である。著者らは HFERP への MinRank 攻撃が、多変数署名方式 Rainbow に対する (Beullens, Crypto 2022) による Simple Attack と同様の考え方により改良可能であることを発見した。技術的には、HFERP の中心写像が HFE 方式の中心写像の連結であることからまず秘密鍵と等価な写像を復元し、個別の HFE に対して鍵復元攻撃を行うことで全体の鍵を復元している。この攻撃から著者らは HFE の改良において Degree of the hidden HFE component が重要であるとしている。上記 MinRank 攻撃と support minors modeling を組み合わせることで、HFERP の提案論文で 80,128 ビットセキュリティとされていたパラメータが 57 から 69 ビット程度に低下した。著者らは、他の多変数公開鍵暗号方式に対しても同様の攻撃が可能であるとしている。攻撃アルゴリズムの検証用コードは `https://github.com/maxcartor/HFERP-Cryptanalysis` で公開されている。

Breaking Parallel ROS: Implication for Isogeny and Lattice-Based Blind Signatures

Shuichi Katsumata, Yi-Fu Lai, Michael Reichle

ブラインド署名の安全性に関する論文である。ブラインド署名はその匿名性から、署名の偽造に関する安全性をどう定義するのかに関して議論があった。本論文では、ℓ-同時偽造不可能性（ℓ-concurrent unforgeability）という安全性が導入された（ここで ℓ は 2 以上の自然数)。これは ℓ 回の署名セッションが終了した後に攻撃者が $\ell + 1$ 個以上の正当な署名を生成できないという安全性の定式化であり、既存の署名方式がそれを満たすかどうかを著者らは議論した。

この種の安全性の議論は、Schnorr（ICICS 2001）により導入された ROS_ℓ 問題（Random inhomogeneities in an Overdetermined Solvable system of linear equations）と、ROS_ℓ 問題が解ければ Schnorr 署名の ℓ-concurrent unforgeability が破られるという事実に端を発する。セキュリティパラメータ λ に対して、$\ell = \mathrm{polylog}(\lambda)$ では ROS_ℓ 問題が解けることが Wagner（Crypto 2002）により示されていたが、ℓ-同時偽造不可能性についてはそもそも $\ell = \mathrm{poly}(\lambda)$ に対する多項式時間攻撃が Benhamouda ら（Eurocrypt 2021) で知られていた。

本論文では、元々の問題の変種として parallel $ROS_{(\ell,\omega,C)}$ 問題とその多項式時間攻撃を提案し、近年提案された parallel repetition 型のブラインド署名に対しても同様の攻撃が可能であることが示された。具体的には、同種写像ベースの CSI-Otter、格子ベースの Blaze+、BlindOR がターゲットとなっており、それぞれに対応する parallel $ROS_{(\ell,\omega,C)}$ 問題の具体的な形と解析が与えられている。

A Simpler and More Efficient Reduction of DLog to CDH for Abelian Group Actions

Steven D. Galbraith, Yi-Fu Lai, Hart Montgomery

可換群 G の集合 X への群作用を用いた暗号プリミティブに関する論文である。特に本論文は、効率的群作用（Efficient Group Action: EGA）と呼ばれる、任意の $g \in G, x \in X$ に対して $gx \in X$ が効率的に計算可能であるという仮定の下、離散対数問題および計算量的 Diffie-Hellman 問題の類似物である以下の二つの問題（Galbraith et al., Math Crypto. 2021）に対する取り組みである：

- GA-DLog: (x, gx) から g を計算せよ。
- GA-CDH: (x, ax, bx) から $(ab)x$ を計算せよ。

これらの計算問題の困難性について、上述の Galbraith らの研究では GA-Dlog から GA-CDH への量子帰着が、GA-CDH オラクルが perfect correctness を持つという条件の下で可能であることが示された。その後、Montgomery と Zhandry (J. Crypto, 2024) により、信頼性の低い GA-CDH オラクルを信頼性の高いオラクルに変換する手法が提案され、上記帰着問題は一定の解決を見たものの、帰着効率はオラクルの信頼率 ε に対して $1/\epsilon^{21}$ という非効率なものであった。

本論文で著者らは、Montgomery と Zhandry の帰着手法中で用いられる確率の評価アルゴリズムを単純化し、最終的な効率を $1/\epsilon^4$ まで向上させた。

An Algorithm for Efficient Detection of (N, N)-Splittings and Its Application to the Isogeny Problem in Dimension 2

Maria Corte-Real Santos, Craig Costello, Sam Frengley

2 次元超特殊（superspecial）同種写像問題に関する論文である。これは、正標数 p の基礎体 K 上の種数 2 の超特殊曲線 C, C' について、超特殊アーベル曲面であるヤコビ多様体間の同種 $\phi : \mathrm{Jac}(C) \to \mathrm{Jac}(C')$ を計算する問題であり、種数 2 の同種写像ベース 2022 年の SIKE 攻撃に関連するトピックといえる。

2 次元超特殊同種写像問題を解く既知のアルゴリズムで最も良いものは、Costello-Smith (PQCrypto 2020) による 2 ステップアルゴリズムである。第 1 ステップでは $\mathrm{Jac}(C), \mathrm{Jac}(C')$ のそれぞれから（疑似）ランダムウォークを行い、超特異楕円曲線の積で表現される $E_1 \times E_2$ と $E_1' \times E_2'$ へのパスを発見する。第 2 ステップでは、E_1 と E_1'、E_2 と E_2' 間のパスを Delfs-Galbraith アルゴリズム (Des. Codes. Crypyo. 2016) により発見して合成することで、目的の同種写像を得る。このアルゴリズムは同種写像ベースの暗号解析に用いられたことから、この分野の基本的なアルゴリズム

として知られている。

一方、種数 2 の曲線 C のヤコビ多様体 Jac(C) が分裂している (split) とは、二つの楕円曲線 E_1, E_2 の直積の上への分離的 K-同種写像 $\phi : \mathrm{Jac}(C) \to E_1 \times E_2$ が存在することをいう。この同種 ϕ をより詳細に研究するため、著者らは Bruin-Doerksen に従い、最適 (N, N)-分裂（optimal (N, N)-splitting）という性質を研究した。ここで上記の同種 ϕ が最適 (N, N)-分裂であるとは、ϕ の次数が平方数 N^2（ここで N は p と互いに素）であり、ϕ の核が Jac(C) に定まる N-Weil ペアリングに関して極大等方部分群かつ $(\mathbb{Z}/N)^2$ と同型、すなわち (N, N)-同種写像であり、かつ、ϕ に射影及びヤコビ埋め込みを合成することで得られる被覆 $C \to E_1$ が非自明な不分岐被覆を経由しない、すなわち最適である、ことと定義される。

本論文では、与えられた種数 2 の超特殊曲線について、Jac(C) が最適 (N, N)-分裂であるかどうかを判定する高速なアルゴリズムが与えられた。これを用いることで上記疑似ランダムウォークの速度が飛躍的に上がり、p が 100-1000 ビットの場合に 25-160 倍の高速化を達成している。

D.5 PQCrypto 2024

An Improved Practical Key Mismatch Attack Against NTRU

Zhen Liu, Vishakha, Jintai Ding, Chi Cheng, Yanbin Pan

NTRU に対する鍵不一致攻撃に関する論文である。NTRU の復号は、一変数多項式である秘密鍵 f と暗号文 c に対して積 $a = c * f \mod q$ を計算することで行われる。ここで、NTRU の公開パラメータの一部である $q \ll p$ なる互いに素な正整数 p, q と素数 N について、剰余環を $\mathcal{R}_p := F_p[x]/(x^N - 1)$, $\mathcal{R}_q := F_q[x]/(x^N - 1)$ とした際、$a = c * f \mod q$ は剰余環 $\mathcal{R}_q$ で一致することを意味する。実際の復号は、$\mathcal{R}_p$ において f の逆元となる多項式 f_p を利用して、$a = c * f \mod p$ で行われる。この復号が成功するためには a の係数が $[-q/2, q/2)$ の範囲に収まる必要があるが、NTRU ではパラメータを調整することでこれを実現している。

ここで、正整数 n を用いて操作された暗号文 $c_i = c + n * p * x^i$ を同じ鍵で復号すると、$c_i * f = a + n * p * x^i * f \mod q$ が成り立つが、もし $a + n * p * x^i * f$ の係数が $[-q/2, q/2)$ にある場合、同様の手法で平文が復号される。係数がこの範囲を超える（オーバーフロー）する位置から秘密鍵 f の情報を復元するというアプローチが、Hoffstein ら (2000) が提案した鍵不一致攻撃の基本的な手法であるが、係数が $[-q/2, q/2)$ の範囲からはみ出る箇所が 1 か所でしか起きないという強い仮定があった。

本論文では、その仮定を取り除いた攻撃が提案された。また、NTRU に対する鍵不一致攻撃には Qin ら (Asiacrypt 2021) によりクエリ回数の下限が知られているが、この攻撃のクエリ回数はほぼその下界を満たしている。実験では、NIST 耐量子標準化プロジェクトに提案された NTRUEncrypt と NTRU-HPS への攻撃を行い、実際に提案パラメータでの鍵回復を成功させている。

Analyzing Pump and Jump BKZ Algorithm Using Dynamical Systems

Leizhang Wang

格子暗号の解析に関する論文である。格子暗号解析では、BKZ アルゴリズムをはじめとする格子基底簡約アルゴリズムによる前処理を行った後の基底に対して格子点探索アルゴリズムを用いて秘密情報に対応する格子点を見つけるという 2 段階の攻撃がデファクトスタンダードとなっている。そのため、格子基底簡約アルゴリズムの計算時間と出力される基底のクオリティの関係を調査することは重要な課題として認識されている。ヒューリスティックに高速な基底簡

約アルゴリズムとして、BKZ (Schnorr-Euchner, FCT1991) の利用が仮定されるが、近年ではブロックを処理するサブルーチンとして、Schnorr-Euchner が用いたような ENUM アルゴリズムではなく、篩アルゴリズムを用いることが一般的となっており、それに合わせて BKZ のブロック処理の戦略および解析手法も更新されている。この論文では、ブロック処理の戦略として Pump and jump を用いた BKZ アルゴリズムの解析を dynamical systems (Hanrot ら、Crypto 2011) により解析した結果を与えている。Pump は篩アルゴリズムの性質を使った BKZ の改良手法である。篩アルゴリズムはその性質から入力された格子基底の中で短いベクトルを指数個出力する。それらのベクトルを Babai の最近平面アルゴリズム等で、より小さいインデックス側に広げたブロック中での短いベクトルの生成に利用する。Jump はブロック処理のインデックスを、ブロックを $i = 1$ から順番に処理していくのではなく、いくつかスキップして行く戦略で、ヒューリスティックに速いことが知られている。著者らは BKZ のブロックサイズ β と Jump の幅 J，ツアー数 T に対して出力される $\boldsymbol{b}_1$ の上界を与えている。

Adaptive Attacks Against FESTA Without Input Validation or Constant-Time Implementation

Tomoki Moriya, Hiroshi Onuki, Maozhi Xu, Guoqing Zhou

同種写像ベースの公開鍵暗号である FESTA に対する適応的攻撃についての論文である。FESTA とは、Castryck-Decru による SIDH 攻撃（Eurocrypt 2023）において用いられた Kani の定理を活用した、トラップドア関数およびそれを用いた公開鍵暗号方式である。FESTA は CIST（Computational Isogeny with Scaled-Torsion）問題を安全性の根拠としている。

本論文では、秘密鍵を公開鍵及び入出力から割り出す攻撃を提案している。この攻撃において想定しているシナリオは以下のようなものである。攻撃者 Bob はまず、秘密鍵を持っている人物 Alice に誤った処理で作成した暗号文を提示する。この暗号文は正しい処理で作られたものと同じ型を持っている。Alice はこの暗号文を復号するが、ここで仮に「復号処理が実行できたかできなったか」の情報が Bob に渡った場合、Bob は Alice の秘密鍵を割り出すことができることが本論文で報告された。

FESTA の暗号化処理において、Bob の入力の一部である 2×2 変換行列 B は、公開パラメータとして設定されている可換部分群 $\mathcal{M}_b \subset GL_2(\mathbb{Z}/2^b\mathbb{Z})$ に属していることが想定されている。しかしながら著者らは、B が $\mathcal{M}_b$ に属していない場合に復号プロトコルがどのように振舞うかを観察することで、上述の適応的攻撃を導いた。

したがって、変換行列 B が指定された可換部分群 $\mathcal{M}_b$ に属するかをチェックする工程はスキップできないと指摘された。さらにこの攻撃シナリオの場合、Alice は復号の過程において、「復号に失敗する」という例外 1 と、「復号に成功したが B が $\mathcal{M}_b$ に属さなかった」という例外 2 のどちらかを得る。この例外出力結果はもちろんのこと、この例外が出力される時間が異なる場合、サイドチャネル攻撃が可能であることが指摘された。以上の観点から、FESTA は注意深く実装されるべきであると報告された。

The Blockwise Rank Syndrome Learning Problem and Its Applications to Cryptography

Nicolas Aragon, Pierre Briaud, Victor Dyseryn, Philippe Gaborit, Adrien Vinçotte

耐量子計算機署名方式の候補である、ROLLO および RQC に関する攻撃論文である。これらは Rank-based cryptography とよばれる符号ベース暗号の一種に属し、特定の階数（rank）を持つ符号語を発見する問題の困難性を安全性の根拠とする。より詳細には、ROLLO は LRPC 方式に、RQC は RQC 方式に属する。これらの方式は、Rank Support Learning 問題に基礎を置く多重シンドローム（multi-syndrome）アプローチにより効率化されていたが、著

者らは Asiacrypt 2023 において Song らにより導入されたブロックワイズエラー（blockwise error）アプローチにより、検証鍵および署名長の長さをさらに大きく削減できることを指摘したうえで、この二つのアプローチを組み合わせた新たなアプローチを提案した。これは著者らが導入した Blockwise Rank Syndrome Learning 問題に基礎を置く。この新たなアプローチにより一般的な RQC 方式および LRPC 方式における検証鍵と署名の長さを大きく改善した。

加えて本論文では、上述の Song らによって導入された l-RD 問題について新たな攻撃を導入し、ROLLO-I に対する攻撃を実施した。結果、128/192/256 ビットセキュリティの方式に対して、主張されていた安全性は 145/225/281 ビットセキュリティであったが、著者らの攻撃によりこれが 116/166/224 ビットセキュリティに低下した。

Cryptanalysis of the SNOVA Signature Scheme

Peigen Li, Jintai Ding

耐量子計算機署名方式である SNOVA に対する攻撃論文である。SNOVA は多変数方程式の求解困難性に基づいた署名であり、NIST 耐量子計算機電子署名の第 2 ラウンド候補である。特に、構造付きの UOV 型の署名としてその署名サイズの小ささと処理性能が注目されているものの、行列を変数として並べた写像を用いる非可換環的な構成をしており、その安全性は詳しく解析されていなかった。SNOVA の開発者らによれば、パラメータ (v, o, q, l) の SNOVA は、パラメータ (l^2v, l^2o, q) を持つ $\mathbb{F}_q$ 上の UOV として捉えることが可能であり、その性質を用いてパラメータが設定されていた。

本論文では、提案パラメータを持つ SNOVA の攻撃計算量は開発者が主張するよりも低いことが報告された。著者らは、SNOVA の構成を注意深く取り扱うことで、同じパラメータの SNOVA がパラメータ (lv, lo, q) を持つ l^2o 本の式を持つ UOV として捉えられることを明らかにし、攻撃の解析を行った。なお、この攻撃を適用した後でも攻撃計算量は引き続き指数的であり、パラメータの修正により安全性は確保されるとして NIST 追加署名の第 2 ラウンドに残っている。

また同様の手法により署名方式 NOVA の偽造攻撃に必要となる計算量も低くなることが判明している。

Practical Key-Recovery Attack on MQ-Sign and More

Thomas Aulbach, Simona Samardjiska, Monika Trimoska

署名方式 MQ-Sign に対する攻撃についての論文である。MQ-Sign は UOV 型の署名方式で、Shim らにより KpqC に提出されたアルゴリズムであり、鍵長を削減するために中心写像にスパースな構造を入れている。具体的には、中心写像を $F = F_V + F_{OV} + F_{LC}$ と vineger-vineger 変数の項、oil-vineger 変数の項、それ以外の線形・定数項に分割して表現したときに、F_V, F_{OV} をランダム多項式に基づくものとするか、スパースなものとするかにより 4 種の選択があり、F_V に関する選択を 1 文字目の S/R で、F_{OV} に関する選択を 2 文字目の S/R で表現し、それぞれ MQ-Sign-SS, -RS, -SR, -RR と名付けている。

本論文では、F_{OV} がスパース構造を持つ MQ-Sign-SS および MQ-Sign-RS に対する鍵復元攻撃を EIP 問題として定式化し、そのスパース性から行列のランクが著しく落ちる事を利用して多項式時間での鍵復元攻撃を行っている。

さらに本論文では、MQ-Sign-SR に対する高速な偽造攻撃を提案している。こちらは F_V のスパース性を利用することで変数の数を削減しており、グレブナー基底計算を用いた解析によればレベル I, III, V のパラメータの攻撃計算量はそれぞれ 2^{111}, 2^{170}, 2^{228} となり、128, 192, 256 ビットセキュリティを持たないことが確認された。

多項式時間攻撃のスクリプトは `https://github.com/mtrimoska/MQ-Sign-attack` で公開されており、最も高いセキュリティレベル V のものでも 7 秒で署名鍵の復元が可能であるとしている。

Practical and Theoretical Cryptanalysis of VOX

Hao Guo, Yi Jin, Yuansheng Pan, Xiaoou He, Boru Gong, Jintai Ding

耐量子計算機署名方式である VOX についての攻撃論文である。VOX は UOV 系の署名方式であり、NIST PQC 標準化プロジェクトの追加署名に提出されている。2023 年に Furue, Ikematsu による rectangular MinRank 攻撃が発見され、その後開発者によるパラメータのアップデートがあった。

本論文では、更新されたパラメータをもつ方式に対する MinRank 攻撃再評価を行い、現実的な時間内で署名鍵の復元が可能であることが示された。VOX の特徴は中心写像 F の構成を少量のランダムな二次多項式と剰余環の構造を持つ多項式を混ぜて構成することで鍵サイズの削減と効率化を図っており、その特徴が MinRank 攻撃により効率的に抽出可能であることが改めて確認された形となる。

攻撃スクリプトは `https://github.com/tuovsig/analysis` で公開されており、古典的な Kipnis-Shamir 攻撃とグレブナー基底計算を組み合わせたものでも 2 秒程度で鍵復元が可能であるとしている。理論的な計算量評価も行っており、開発者らの想定とは逆に、レベル 1, 3, 5 のパラメータがそれぞれ 112, 69, 48 ビットセキュリティであると計算している。

Fault Attack on SQIsign

JeongHwan Lee, Donghoe Heo, Hyeonhak Kim, GyuSang Kim, Suhri Kim, Heeseok Kim, Seokhie Hong

耐量子計算機署名方式である SQISign に対するサイドチャネル攻撃論文である。SQISign は同種写像ベースのシグマプロトコルを Fiat-Shamir 変換により署名方式としたものである。

本論文では、署名生成関数の中のコミットメントフェーズにおいて、イデアル I_{com} と同種写像 ϕ_{com} の計算ルーチンに対する故障注入攻撃が提案された。特に、計算ルーチンの実行を制御することで平文に対する偽の署名を生成する手法と、署名の情報から分割統治法による秘密鍵の復元攻撃手法が提案された。I_{com} の計算ルーチンへの攻撃はリファレンス実装における copy 関数への故障注入であり、これにより結果がランダムな値となる。対策として、イデアルのノルムをチェックする機構を組み込むことが有効であるとしている。ϕ_{com} の計算ルーチンへの攻撃は for ループの実行を途中で打ち切るものであり、対策としてループ回数のカウンタチェックが有効であるとしている。

さらにこれらの脆弱性を利用して、2 種類の攻撃シナリオの下で具体的攻撃が検討された。deterministic SQISign に対しては、鍵を固定した署名生成オラクルへのアクセスが可能であり、署名生成の実行中に 1 回だけ故障注入が可能なシナリオが想定され、randomized SQISign は対しては、署名生成オラクルが用いる鍵が毎回異なるものであっても良いが、攻撃者が 2 回故障注入できるシナリオが想定されている。

A Subexponential Quantum Algorithm for the Semidirect Discrete Logarithm Problem

Christopher Battarbee, Delaram Kahrobaei, Ludovic Perret, Siamak F. Shahandashti

半直積離散対数問題（Semidirect Discrete Logarithm Problem、以下 SDLP）に関する量子解読論文である。SDLP とは、有限群（もしくは有限半群）G の元 g と、自己準同型 $\phi : G \to G$ が与えられたとき、$s_{g,\phi}(x) := \phi^{x-1}(g)\phi^{x-2}(g)\cdots\phi(g)g$ から x を復元する計算問題である。これは通常の有限アーベル群に対する離散対数問題を半直積 $G \rtimes \mathrm{End}(G)$ へと一般化したものであり、耐量子性を持つ暗号プリミティブとして期待されている。

本論文では、半群の加算族 $\{G_p\}_p$ が “簡単（easy）” であるという技術的な仮定の下、準指数時間および準指数量子

クエリ数で SDLP を解くアルゴリズムが報告された。ここで $\{G_p\}_p$ が簡単であるとは、群の位数が p の多項式オーダーかつ、群演算と自己準同型写像の評価が $O((\log p)^2)$ 時間で完了するものとして定義される。

この解読に向けたアプローチとして、著者らは SDLP の群作用離散対数問題（Group Action Discrete Logarithm Problem、以下 GADLP）への量子帰着を研究した。本論文で使用される GADLP インスタンスは巡回群作用についてのものである。著者らはまず、関数 $s_{g,\phi} : \mathbb{Z}_{\geq 0} \to G$ を観察し、有限個の正整数 n を除き $s_{g,\phi}(n) = s_{g,\phi}(n+r)$ が満たされる数 r のことを周期（period）と呼び、$s_{g,\phi}(n) = s_{g,\phi}(n+r)$ が満たされる最小の n を指数（index）と呼んだ。このように関数 $s_{g,\phi}$ は G における長さ r のサイクルを与えるが、このサイクルに自由かつ推移的な巡回群作用を明示的に与えることで、指数 n の計算と GADLP に問題を帰着した。より具体的には、簡単な半群の加算族 $\{G_p\}_p$ に対して、一回の GADLP クエリで機能する、時間計算量 $O((\log p)^4)$、正解確率 $\Omega(1)$ で SDLP を解くアルゴリズムを与えた。これにより簡単な半群の加算族に対する SDLP は、指数 n の計算と、GADLP の量子アルゴリズムを与えることに帰着される。前者に関しては具体的な量子アルゴリズムを、後者については Kuperberg もしくは Regev により与えられた GADLP のアーベル群隠れシフト問題（abelian hidden shift problem）への帰着を利用することで、上述の結果を導出している。

Properties of Lattice Isomorphism as a Cryptographic Group Action

Benjamin Bencina, Alessandro Budroni, Jesús-Javier Chi-Domínguez, Mukul Kulkarni

格子同型問題（Lattice Isomorphism Problem、LIP）に関する論文である。格子同型問題とは、NIST 耐量子計算機署名方式の候補である HAWK などの安全性の根拠となっている数学的プリミティブである。

格子同型問題は 2 つの格子 L_1 と L_2 の間が同型かどうかを判定する、もしくは同型を与える直交変換を計算せよという問題である。格子に付随する二次形式に本問題を換言すれば、二次形式が整数係数可逆線型変換（すなわち $\mathrm{GL}_n(\mathbb{Z})$ の元）で移りあうかを判定する、もしくはその変換を計算せよという問題となる。これは二次形式の為す空間への $\mathrm{GL}_n(\mathbb{Z})$-作用の群作用暗号（group action cryptography）に他ならないが、本論文ではこの観点を LIGA（Lattice Isomorphisms as a Group Action）と整理して研究が行われている。二次形式への群作用が推移的かつ忠実（faithful）となる $\mathrm{GL}_n^{\pm}(\mathbb{Z}) := \mathrm{GL}_n(\mathbb{Z})/\simeq_{\pm}$ を考慮する。ここで二つの行列 A, B が $A \simeq_{\pm} B$ であるとは $A \in \{B, -B\}$ を指し、これは同値関係となる。この設定の下、二次形式 Q の $U \in \mathrm{GL}_n^{\pm}(\mathbb{Z})$ の作用は $U \star Q := U^T Q U$ で与えられる。この下で本論文では、群作用暗号におけるプリミティブである以下の問題を考慮している。

- 一方向性（One-wayness）：$U \in \mathrm{GL}_n^{\pm}(\mathbb{Z})$ と二次形式 Q があたえられたとき、$(Q, U \star Q)$ から U を求めよ。
- Weak-unpredictability：$U \in \mathrm{GL}_n^{\pm}(\mathbb{Z})$ と多項式個の二次形式 Q_i および P が与えられたとき、$(Q_i, U \star Q_i)$ から $U \star P$ を求めよ。
- Weak-pseudorandomness：$U \in \mathrm{GL}_n^{\pm}(\mathbb{Z})$ と多項式個の二次形式 Q_i および R_i が与えられたとき $(Q_i, U \star Q_i)$ と (Q_i, R_i) を識別せよ。

本論文では、LIGA の下では Weak-unpredictability と Weak-pseudorandomness は成り立たないことが示された。そのうえで著者らは、LIP は PRF や更新可能暗号には使用すべきではないと結論づけた。また weak unpredictability を破るための別系統の手法として、サンプル数（群作用の列の長さ ℓ）と計算時間のトレードオフを与えるアルゴリズムも提案されている。さらに著者らは今後暗号に使える可能性のある計算問題として、二次形式同士を結び付ける Transpose Quadratic Form Problem および Inverse Quadratic Form Problem を提案している。これらの問題は search-LIP 問題に帰着されるため、困難であると期待される。

Polynomial XL: A Variant of the XL Algorithm Using Macaulay Matrices over Polynomial Rings

Hiroki Furue, Momonari Kudo

MQ 問題に対する解析論文である。MQ 問題は n 変数 m 方程式の連立 2 次方程式の求解問題であり、多変数公開鍵暗号の安全性の根拠となっている。この連立 2 次方程式の求解問題を解くアルゴリズムの一つとして、XL アルゴリズムが知られている。

本論文では、前処理として k 変数の値を仮置きすることで計算量を下げる変種である h-XL の改良として polynomial XL を提案し、アルゴリズムの解析と $n = m$ の場合の計算量の上界を与えている。XL アルゴリズムの大まかな流れは元の方程式にある単項式を Macaulay 行列により線形化し、消去法によりグレブナー基底を計算、最後に各変数の値を順番に求めていくというものである。 提案アルゴリズムでは、固定されていない $n - k$ 変数の方程式から多項式環 $F_q[x_1, \ldots, x_k]$ 上の Macaulay 行列を生成し、計算処理を進めることで k 変数の総当たりを回避し高速化している。著者らは計算量解析の実例として、$n = m = 20, 40, 60, 80$ に対する MQ 問題の解析時間について、h-XL, h-WXL, Crossbred 等の他のアルゴリズムと著者らの方式を比較し、優位であることを示した。

D.6 Crypto 2024

Solving the Tensor Isomorphism Problem for Special Orbits with Low Rank Points: Cryptanalysis and Repair of an Asiacrypt 2023 Commitment Scheme

Valerie Gilchrist, Laurane Marco, Christophe Petit, Gang Tang

テンソル同型問題（Tensor Isomorphism Problem、以下 TIP）と、D'Alconzo ら（Asiacrypt 2023）によるコミットメントスキームの解析に関する論文である。TIP は 3-テンソル（すなわち立方行列）間の同型写像を求める計算問題であり、NIST PQC 標準化プロジェクトの追加署名候補 MEDS の安全性の根拠となっている。

本論文では、特別な 3-テンソルに対する TIP を解く多項式時間アルゴリズムが提案された。この問題は D'Alconzo らによるコミットメントスキームの安全性の根拠となっていたので、本論文のタイトルにあるコミットメントスキームが安全でないことが報告された。

TIP は 3 つの一般線型群の直積からの群作用に関する問題として記述される。著者らは、当該コミットメントスキームで用いられる 3-テンソルの軌跡が低いランクのテンソルを持つこと、さらにその点については非自明な固定化部分群を導けることが、本攻撃において本質的な観察であると報告した。著者らは方式の修正として、ランダムテンソルを用いた新たな方式を提案している。

FuLeakage: Breaking FuLeeca by Learning Attacks

Felicitas Hörmann, Wessel P. J. van Woerden

耐量子計算機署名方式である FuLeeca についての解析論文である。FuLeeca は NIST PQC 標準化プロジェクトの追加署名に提出された Hash-and-Sign フレームワークの符号ベース署名である。構成が格子署名 FALCON に似ていることから、FALCON の変種の解析で用いられた複数署名からの秘密鍵復元手法の適用可能性が本論文で検討された。

技術的には符号ベースの記述がなされている FuLeeca を格子ベースの記述に変換する事で FALCON を中心とする GPV フレームワークの格子署名に対する鍵復元アルゴリズムを適用している。攻撃者の持つ署名数が少ない場合には

鍵復元に用いられる格子の部分格子が抽出され、それに合わせて攻撃計算量が下がる。多い場合には学習アルゴリズムを用いて鍵復元を行う。顕著な結果として、最も高いセキュリティパラメータの場合でも 175,000 個の署名から 1 時間で復元可能な格子攻撃が実証されている。また、元々の方式で用いられていた準巡回符号の構造を用いることで、Cramer ら（Eurocrypt 2016）の量子多項式時間での short generator 復元攻撃が適用可能であるという 2023 年 7 月の pqc-forum での指摘が正しいことが確認された。

Space-Efficient and Noise-Robust Quantum Factoring

Seyoon Ragavan, Vinod Vaikuntanathan

量子アルゴリズムを用いた素因数分解に関する論文である。本論文は、2023 年に Regev(arXiv: 2308.06572) により発表された量子素因数分解アルゴリズムを、量子メモリ効率およびノイズ耐性の二点で改善した。

第一の結果として著者らは、素因数分解問題を解く $O(n\log n)$ 量子ビット、$O(n^{3/2}\log n)$ 量子ゲートの量子回路を提案した。Regev のアルゴリズムは $O(n^{3/2})$ 量子ビット、$O(n^{3/2}\log n)$ 量子ゲートであるため、量子ビット数が削減されている。Regev のアルゴリズムは Shor のアルゴリズム（$O(n)$ 量子ビット、$O(n^2\log n)$ 量子ゲート）の一般化として得られた経緯を加味すると、著者らの結果は量子ビット・量子ゲートのトレードオフを改良したと言える。この結果を得るために著者らは、Kaliski(arXiv: 1711.02491) のフィボナッチ数列を用いた指数計算回路を適用し、in-place での剰余乗算を可能とした。さらにいくつかの量子ビット数・量子ゲート数のトレードオフも提案しており、乗算の方法によっては $(10.32 + o(1))n$ 量子ビット、$O(n^{5/2}\log n)$ ゲート数のものも構成可能であると報告された。

第二の結果として、著者らは後処理アルゴリズムを改良した。元々 Shor のアルゴリズムはノイズに弱いことが指摘されており、Regev アルゴリズムもその性質を引き継いでいた。この論文では、回路実行中にエラーがあった場合、その出力がランダムな d 次元の点となると仮定することでフィルタリング手法を提案し、良いサンプルのみを用いて後処理を行う事で成功率を上げている。結果として回路中の 1 論理ゲート当たりのノイズが $\tilde{O}(1/n^{1.5})$ であれば十分な確率で素因数分解が可能であると報告された。

Quantum Complexity for Discrete Logarithms and Related Problems

Minki Hhan, Takashi Yamakawa, Aaram Yun

離散対数問題に対する量子解析に関する論文である。本論文では generic group model、つまり群の構造やエンコーディングのような付加情報を用いずに、量子アルゴリズムおよび量子・古典ハイブリッドアルゴリズムの計算量について研究が行われている。

群 G の位数を $|G|$ とするとき、Shor 型のアルゴリズムで離散対数問題を解く量子計算量は $O(\log|G|)$ と記述できる。本論文では、離散対数問題を解く量子回路の深さは少なくとも $\Omega(\log|G|)$ であることが示された。これは Shor のアルゴリズムが漸近的に最適な量子アルゴリズムであることを意味する。また、離散対数問題を解く量子・古典のハイブリッドアルゴリズムで（量子・古典に関わらず）Q 回の群要素操作を行うアルゴリズムは、深さ $\Omega(\log\log|G| - \log\log Q)$ の量子回路で表現される群操作を $\Omega(\log|G|/\log Q)$ 回必要とすることが示された。さらに量子回路以外の要素として、t 個の群要素を保存する量子メモリと r 個の群要素を保存する quantum random access classical memory (QRACM) を利用可能な場合、量子・古典ハイブリッドアルゴリズムは $\Omega(\sqrt{|G|})$ 回の群操作クエリかもしくは $\Omega(\log|G|/\log(tr))$ 回のクエリを必要とする。後者の下界は古典クエリに対する下界でもある。ここで、QRACM は古典データ x_i を保存しつつも、量子的なアクセスにより操作 $|i\rangle \otimes |0\rangle \to |i\rangle \otimes |x_i\rangle$ を可能なデバイスとされる。

本論文ではこれらの結果を応用し、multiple DLP（$g^{x_1}, \ldots, g^{x_m}$ から $x_1, \ldots, x_m$ を計算する問題）を個別に解くよ

りも同時に解く方が効率的となるアルゴリズムを示し、パスワード認証鍵共有 (PAKE) の文脈で提唱されている性質 quantum annoying property (Eaton, PQCrypto2021) が strong form では成り立たないことを報告した。この性質は、もしも方式が破られるならば PAKE のパスワードの推測ごとに 1 回の離散対数問題を解かなければならないとされるもので、方式の安全性を議論するために導入された。

A Systematic Study of Sparse LWE

Aayush Jain, Huijia Lin, Sagnik Saha

sparceLWE 問題に関する論文である。sparceLWE 問題は、LWE 問題と sparseLPN 問題の性質を引き継いだ計算問題として、本論文で導入された。著者らは計算困難性と暗号応用について研究している。n, m, σ, p をそれぞれ LWE 問題の次元、サンプル数、ノイズパラメータ、法とする。自然数 k に対して k-sparse LWE 問題 (k-sLWE) を、$(A, sA + e \bmod p)$ と (A, u) を識別する問題とする。ここで u はランダムなベクトル、A の各行は k 個の非ゼロ要素しか持たないものとし、それ以外は通常の LWE 問題と同様とする。

本論文では、k-sLWE 問題の基本的な性質として、LWE 格子 $L = \{xA + p\mathbb{Z}^m : x \in \mathbb{Z}^{1\times m}\}$ の最小距離と密度が通常の LWE 問題とどの程度離れているかが検証され、サンプル数 m が十分に大きい場合には通常の LWE と同様の挙動を示すことが示されている。また、$m = O(n^2 \log n \log p)$ と設定すると Gentry らの格子署名 (STOC, 2008) で用いられているようなトラップドア行列でスパースなものがサンプリング可能であることが示されている。これらにより、鍵サイズの小さい暗号方式が構成可能である。

さらに著者らは安全性の検討も行っている。sparceLWE 問題は、$k = O(\log n)$ であればスパース性から総当たりが可能である。また sparseLPN に対して有効であった攻撃は、エラーベクトルが疎でないことから単純な適用は難しいと著者らは考察したが、$Ax = 0$ を満たすスパースなベクトルを見つけることで攻撃の成功率を上げることが可能だと示唆した。著者らは現実的に考えられる攻撃として、A が疎であることから、特定の $L = \Theta(n)$ 変数のみが非ゼロであるようなサンプルのみを集めることで次元を下げる Dense-Minor 攻撃を検討した。著者らは n' 次元の k-sLWE の Dense-Minor 攻撃が、n 次元 m サンプルの LWE 問題となるような (n', k) を逆算するスクリプトを、lattice-estimator をベースに構成している。

最後に応用として、k-sLWE ベースの準同型暗号が効率的に構成可能であることを示した。

Quantum Lattice Enumeration in Limited Depth

Nina Bindel, Xavier Bonnetain, Marcel Tiepelt, Fernando Virdia

SVP（最短ベクトル問題）の計算量評価についての論文である。SVP を解く代表的なアルゴリズムには列挙法（ENUM）と篩法（sieve）があり、それぞれの古典・量子計算量が評価されている。

格子次元 n に対して、列挙法の時間計算量が $2^{cn\log n}$, $c \approx 0.2$ であるのに対して、篩法の時間計算量が $2^{O(0.292n)}$ であることが知られており、篩法の方が漸近的に高速である。理論的な評価だけではなく SVP challenge のような解読コンテストの結果から、実際の計算も高速であることが知られている。

一方で、量子計算量の解析では Aono ら（Asiacrypt 2018）の量子木探索を用いることで列挙法の時間計算量の指数部分が半分となる $2^{0.5cn\log n}$ 量子回路計算量のアルゴリズムが知られている反面、篩法の量子計算量は $2^{O(0.265n)}$ であるため、次元によっては逆転する可能性が示唆されていた。

本論文では、古典/量子ハイブリッドの列挙アルゴリズムを用いて、CRYSTALS-Kyber に対する詳細な計算量評価を行っている。このハイブリッドアルゴリズムでは、列挙法で用いる列挙木の根に近い部分を古典で、残りの部分を量

子で行う事を仮定している。古典と量子を切り分ける深さは NIST PQC 標準化プロジェクトで求められる量子回路の最大深さの制限をもとにしている。本計算量評価は、量子誤り訂正によるオーバーヘッドも加味している。ただし、量子木探索を行う部分木の大きさはインスタンスごとに異なり、実際の計算量が multiplicative Jensen's gap と呼ばれる量 (論文内 Def. 1) に依存する。この gap をどの程度に想定すると Kyber-512/768/1024 の各パラメータの計算量が NIST で求められる AES の（深さを制限した）解読計算量よりも小さくなるのかという議論と、その gap 値が現実的にどの程度ありえそうかが Table 5 にまとめられている。どの設定でも Kyber-1024 では AES の解読計算量よりも大きくなると考えられるが、Kyber-512/768 では設定によっては小さくなるため、より細かい検証が必要と考えられる。

Cryptanalysis of Lattice-Based Sequentiality Assumptions and Proofs of Sequential Work

Chris Peikert, Yi Tang

格子ベースの Proof of sequential work (PoSW) の解析に関する論文である。PoSW とは、関数 f を固定したときに入力 x_0 に対する $x_i = f^i(x_0)$ を大きな i に対して $x_1, x_2, \ldots$ と順番に計算したことを証明する手法である。f の構成を工夫することで、$x_1, \ldots, x_n$ から x_{2n} を計算するようなスキップを行う事が別の計算困難な問題を解くことよりも難しく、順番に計算することが最良に近いということが適当な仮定の下で示される。

現在までに耐量子性を持つ PoSW の候補はハッシュ関数に基づくものと、Lai and Malavolta (Crypto 2023) により提案された格子ベースのものが知られている。本論文の対象は後者の格子ベース PoSW である。Lai and Malavolta の関数の構成はランダム行列 A に対して $f_A(x) = -AG^{(-1)}(x) \mod q$ とするものである。パラメータは ℓ を q のビット長、$m = ln$ とする。関数 f_A の入力は $\boldsymbol{x} \in \mathbb{Z}_q^n$、$G^{(-1)}$ は $\boldsymbol{x}$ の各成分を 2 進数で展開して $\mathbb{Z}_2^m$ の元とする関数とする。G はベクトル $g = (1, 2, 2^2, \ldots, 2^{\ell-1})$ を並べたガジェット行列として表現できる。入力ベクトル $\boldsymbol{x}_0$ に対して、$\boldsymbol{x}_{i+1} = f_A(\boldsymbol{x}_i),\ i = 1, \cdots, T$ を順番に計算すると、関係式 $\boldsymbol{x}_{i+1}G = A\boldsymbol{x}_i$ により、G, A を対角線上に並べた行列 A_T に対する SIS 問題のひとつの解が $(\boldsymbol{x}_1\ \boldsymbol{x}_2\ \boldsymbol{x}_T)$ であることがわかり、これを PoSW として用いることができる。

本論文ではベースとなる A, G に対して $AR = G$ を満たす成分の小さい行列 R をサンプリングする手法 (Micciancio-Regev, Eurocrypt2012) を構成部品として、関係式を k 倍の大きさの拡大行列に拡張する手法を構成している。この拡張手法は並列に実行可能であり、並列度に制限が無いとすると $O(\log_k T)$ ステップで PoSW となるベクトルの計算が可能であり、Lai and Malavolta の構成が sequential work の証明とはならないことが示される。また、同様の高速な関数の計算手法が任意の ℓ_p-ノルムに対して成り立つことが示されており、単純な回避策が無いことも示唆されている。

Memory-Sample Lower Bounds for LWE

Mingqi Lu, Junzhao Yang

LWE 問題の計算量の下界に関する論文である。n, σ, q をそれぞれ LWE 問題の次元、ノイズパラメータ、法とする。また，オイラー関数 $\phi(q)$ に対して $k = \Omega(n\log(\frac{1}{1-\phi(q)/q}))$ とする。本論文では、LWE 問題を解く任意のアルゴリズムは、$\Omega(k^2/\log(q/\sigma))$ ビットのメモリか、もしくは $2^{\Omega(k)}$ 個のサンプルを必要とすることが証明されている。

また、著者らは LWR 問題の解析も行っている。n, p, q をそれぞれ LWR 問題の次元、rounding parameter、法とする。このとき、LWR 問題を解く任意のアルゴリズムは、$\Omega(k^2/\log(q/p))$ ビットのメモリか、もしくは $2^{\Omega(k)}$ 個のサンプルを必要とすることが証明されている。

q が素数であるときには $k = \Omega(n\log q)$ であり情報理論的なメモリの上界と一致するため、証明されたメモリの下界がタイトであることがわかる。技術的には Garg ら（APPROX/RANDOM 2021）における LPN 問題のメモリ-サンプル下界証明のフレームワークと、Garg-Raz-Tal (STOC 2018) の学習問題に対する時間-空間計算量の下界証明フ

レームワークを用いており、近年の計算量理論の成果が暗号に応用された形となる。

Not Just Regular Decoding: Asymptotics and Improvements of Regular Syndrome Decoding Attacks

Andre Esser, Paolo Santini

シンドローム復号問題（Syndrome Decoding Problem、SDP）および正則シンドローム復号問題（Regular Syndrome Decoding Problem、RSDP）に関する解析論文である。

線形符号のパリティ検査行列 H とシンドローム $\boldsymbol{s}$ が与えられたときに、通常の SDP は $H\boldsymbol{e} = \boldsymbol{s}$ を満たすハミング重み w 以下のエラーベクトル $\boldsymbol{e}$ を発見することを目的とする。一方 RDSP は、暗号で用いられる特徴を捉えた条件付けとして、エラーベクトルを $e = (\boldsymbol{e}_1, \ldots, \boldsymbol{e}_{n/b})$ と b 次元ごとに区切ったときに、各 $\boldsymbol{e}_i \in \mathbb{F}_2^b$ のハミング重みが w 以下であることを保証するものである。重みが極端に大きい場合には、多項式時間アルゴリズムが存在する。

本論文では、Both と May (PQCrypto 2018) による Information Set Decoding 型の解析アルゴリズムを用いた SDP と RSDP との計算量比較が行われている。k/n が 0.49 よりも小さい領域においては RSD の方が計算量が小さいことが示される。続いて本論文では、新たな RSDP 向けのアルゴリズムの提案が行われ、先行研究となる Briaud and Øygarden (Eurocrypt 2023) と Carozza, Couteau, and Joux (Eurocrypt 2023) のアルゴリズムとの比較が行われ、僅かではあるが計算量が減っていることが確認された。

応用として Liu ら (Eurocrypt 2024) の疑似相関生成器 (PCG)、Hazay ら (Crypto 2018) のマルチパーティ計算、Boyle ら（ACM CCS 2019）の OT の再解析を行い、最大で 30 ビット程度攻撃計算量を改良している。

Lossy Cryptography from Code-Based Assumptions

Quang Dao, Aayush Jain

Dense-Sparse LPN 問題の解析を含む論文である。公開鍵暗号方式や署名方式を構成可能なプリミティブとして、トラップドア関数が古くから研究されている。Peikert と Waters（STOC2008）により、Lossy トラップドア関数が導入され、DDH 問題および格子問題に基づく構成とその応用としての CCA 安全な公開鍵暗号が構成されている。Lossy トラップドア関数はサンプリングされた関数 $f(0,t)$ がトラップドア t を用いることで逆元計算が効率的に可能であるという通常のトラップドア関数の条件の他に、Lossy（非可逆）な関数 $f(1,t)$ が効率的にサンプリング可能であるがその値域が定義域に比べて指数関数的に小さく、かつ $f(0,t)$ と $f(1,t)$ が識別困難であるという条件が付けられている。

本論文では、符号の Dense-Sparse LPN 問題を提案している。これは、ランダムな（細長い）密行列 T と疎行列 M、秘密ベクトル $\boldsymbol{s}$ と疎なエラーベクトル $\boldsymbol{e}$ に対して $(TM, \boldsymbol{s}TM + \boldsymbol{e})$ とランダムベクトル $\boldsymbol{u}$ を用いた $(TM, \boldsymbol{u})$ が識別困難であるという仮定で、通常の LPN 問題のランダム行列 A の部分を TM で置き換えたものである。この問題の計算困難性を仮定することで、耐衝突性を持つ暗号学的ハッシュ関数の構成、$f(0,t)$ と $f(1,t)$ が識別困難な Lossy トラップドア関数の構成が行われている。また、既知の LPN 問題に対する攻撃のサーベイとそれらを用いた Dense-Sparse LPN 問題の評価が行われており、適切なパラメータを取ることで攻撃時間が次数 n の指数となると主張されている。

興味深い点として、Dense-Sparse LPN 問題の計算量が計算量クラス $\mathsf{BPP}^{\mathsf{SZK}}$ に含まれる、つまり SZK の能力を持つオラクルの存在により多項式時間で求解可能であるという特徴を持ち、これは既知の暗号の構成に用いられている LWE 問題のような学習問題を含んだクラスである。

CryptAttackTester: high-assurance attack analysis

Daniel J. Bernstein, Tung Chou

符号ベース暗号の攻撃計算量解析に関する論文である。暗号解析における攻撃計算量の意味は厳密には研究ごとに異なっており、その違いが攻撃の改良の主張、パラメータ設定において数ビットから数十ビットの範囲で無視できない違いを生んでいる。特に、素因数分解問題と最短ベクトル問題のように、背景が異なる計算問題同士の比較は困難であった。本論文では、攻撃計算量を評価する要素として、回路計算のコスト、メモリアクセスのコスト等を正確に評価し、成功確率を含めた場合の議論を行うフレームワークおよび評価を行うソフトウェアを提供している。

応用として、AES-128 の計算量評価、および符号の復号問題を解く Information Set Decoding(ISD) アルゴリズムの計算量評価と McEliece 暗号の評価を行い、同様の手法により NIST PQC 標準化プロジェクト第 4 ラウンド候補である Classic McEliece 暗号の評価にを与えている。オンライン上の符号ベース暗号解読コンテストである `decodingchallenge.org` において、2023 年時点で解読されている最も大きなパラメータである $n = 1284$ の計算量（number of bit operations）は $2^{70.9}$ 程度であると評価される一方で、128 ビットセキュリティを持つとされる $n = 3488$ のパラメータは $2^{150.59}$ であると評価している。

Improved Algorithms for Finding Fixed-Degree Isogenies Between Supersingular Elliptic Curves

Benjamin Bencina, Péter Kutas, Simon-Philipp Merz, Christophe Petit, Miha Stopar, Charlotte Weitkämper

同種写像問題に関する論文である。同種写像問題とは、与えられた $\mathbb{F}_{p^2}$ 上の 2 つの同種な超特異楕円曲線 E_1, E_2 に対し、同種写像を計算する問題である。同種写像として次数 d が指定されているケースもあり、その場合の計算困難性も期待されている。

本論文では、次数 d が正の実数 ϵ で $d \approx p^{1/2+\epsilon}$ となるケースで、この問題の解析を古典アルゴリズムおよび量子アルゴリズム双方で行った。古典アルゴリズムについては、$1/2 < \epsilon < 3/4$ の場合に、従来知られていた中間一致アルゴリズムを、メモリ計算量および時間計算量双方で改善した。量子アルゴリズムにおいては、$0 < \epsilon < 5/2$ の場合に、時間計算量を改善した。

著者らは問題を解く戦略は Deuring 対応に基づいている。すなわち、E_1, E_2 の自己準同型環である虚 2 次整環 O_1, O_2 に対する接続イデアル（connecting ideal）を計算し、同種写像の集合 $\mathrm{Hom}(E_1, E_2)$ のノルム形式 (norm form) を計算するアプローチをとる。このノルム形式を用いて次数 d を表現し、最終的に同種写像計算に必要な表現に引き戻す。

著者らは応用として Basso ら (ACNS 2024) の SIDH 型署名の再評価を行っており、128 ビットセキュリティとされているパラメータの計算量が約 2^{109} であると報告した。検証用のコードは `https://github.com/isogeny-finding/improved-isogeny-finding` で公開されている。

Radical $\sqrt[N]{\text{élu}}$ Isogeny Formulae

Thomas Decru

N-根基同種写像 (radical N-isogeny) を計算するアルゴリズムに関する論文である。近年、CSIDH において N-根基同種写像の計算を用いることで高速化する研究が行われており（Castryck ら、Asiacrypt 2022)、CSIDH-512 に適

用すると既存の研究よりも 35% 程度高速化が可能である。

本論文では、奇素数 N について、N-根基同種写像を計算する $O(N)$ 計算量の公式が与えられた。一方で、公式の正しさは完全には証明されておらず、数学的な予想（Conjecture 1）を仮定しているが、証明に向けたいくつかのアイデアも与えられている。

Quantum Advantage from One-Way Functions

Tomoyuki Morimae, Takashi Yamakawa

量子優位性と暗号に関する論文である。量子計算機が真に古典計算機よりも高速であるかどうかを議論するための計算量理論的な枠組みが数多く提案されているが、先行研究では標準的でないかまたは強すぎる仮定に基づいていた。量子優位性を示すフレームワークはサンプリング、探索問題、対話証明系を用いたものの 3 種に分類され、本論文では対話証明系の強さを根拠に議論を行っている。技術的には inefficient-verifier proofs of quantumness (IV-PoQ) と呼ばれる対話証明系を定義し、これを statistically-hiding かつ computationally-binding な性質を持つビットコミットメントから構成する。このようなビットコミットメントが古典的な一方向性関数 (OWF) から構成されることは知れているため、OWF の存在から IV-PoQ の存在が導かれることになる。一方で、IV-PoQ の検証者が古典、証明者が量子であることを用いて対話系の存在が量子優位性を導くため、対偶を取ることで量子優位性が無いならば OWF が存在せず、したがって古典的な暗号は安全ではないという結果を示している。

Is ML-Based Cryptanalysis Inherently Limited? Simulating Cryptographic Adversaries via Gradient-Based Methods

Avital Shafran, Eran Malach, Thomas Ristenpart, Gil Segev, Stefano Tessaro

機械学習を用いた暗号の解析に関する論文である。機械学習を用いた暗号解読に関する研究は長年散発的に発表されており、近年の機械学習理論の進展により新たな攻撃が生まれているものの、既存の解読に特化したアルゴリズムとの定量的な性能比較は行われていない。機械学習の文脈から観ると、暗号への攻撃はいくつかの（平文-暗号文のような）ペアをサンプリングし、全てのペアに対する損失関数の平均が最小となるように勾配法などで最適化を行う手法とみることができる。一方で、既存の攻撃は個々のサンプルを直接処理していると考えられる。

本論文では、前者と後者をそれぞれ gradient-based、sample-based と名付け、両攻撃を含んだ攻撃フレームワークを定式化した。直感的には gradient-based の手法は損失関数の平均値を取るため既存の sample-based な攻撃よりも弱いと考えられる。本論文ではこの直感に反する結果として、任意の sample-based の攻撃は gradient-based な手法によりほぼ効率を落とさずにシミュレーション可能であること、gradient-based な手法を多少弱めても同様の結果が得られることを示している。このシミュレーションは並列化可能であり、sample-based な手法の中で並列化が難しい箇所がある場合、並列度を上げることで攻撃の実時間が短縮できる可能性があることを示唆している。

関連する話題として、近年 Wegner ら (NeuralIPS2022) による LWE（Learning with Errors）問題の機械学習を用いた解析の研究が進んでいる。Wagner らの後続研究では BKZ アルゴリズムによる前処理の効果が検討されており、本論文のフレームワークは Wagner らのフレームワークを前処理部分も含めて包含していると述べている。

Generic MitM Attack Frameworks on Sponge Constructions

Xiaoyang Dong, Boxin Zhao, Lingyue Qin, Qingliang Hou, Shun Zhang, Xiaoyun Wan

スポンジ構造型ハッシュ関数に対する中間一致（MitM: Meet-in-the-Middle）攻撃手法を用いた原像攻撃と衝突攻撃に関する論文である。MitM 攻撃手法は Merkle-Damgard 構造型ハッシュ関数に対して幅広く適用されてきた実績があるものの、スポンジ構造型ハッシュ関数に対する適用例はあまり多くない。また、Merkle-Damgard 構造型ハッシュ関数に対する MitM 攻撃手法をスポンジ構造型ハッシュ関数に対して直接的な応用が難しいという問題があった。

本研究ではこのような問題を解決し、スポンジ構造型ハッシュ関数に適用可能な MitM 原像攻撃と MitM 衝突攻撃のための汎用的な攻撃フレームワークを提案した。本フレームワークは NIST LWC 標準暗号の Ascon-Hash、NIST PQC 標準暗号の SPHINCS$^+$-Haraka、ISO/IEC 標準暗号の PHOTON と SPONGENT、などの様々なスポンジ構造型ハッシュ関数に適用され、攻撃フレームワークとしての有効性が示された。具体的には次のとおりである。Ascon-Hash に対し、原像攻撃は 12 ラウンド中 5 ラウンドまで、衝突攻撃は 4 ラウンドまで実行可能であることが示された。なお、原像攻撃は初めての成果であり、衝突攻撃は従来手法による 2 ラウンドの攻撃を改善した。また、SPHINCS$^+$-Haraka に対し、5 ラウンド中 4 ラウンドまでの原像攻撃が示された。これは従来手法による 3.5 ラウンドの攻撃を改善した。PHOTON と SPONGENT、その他のスポンジ構造型ハッシュ関数に関しても同様、初めての成果を示す、もしくは従来手法の改善に成功している。

Revisiting Differential-Linear Attacks via a Boomerang Perspective with Application to AES, Ascon, CLEFIA, SKINNY, PRESENT, KNOT, TWINE, WARP, LBlock, Simeck and SERPENT

Hosein Hadipour, Patrick Derbez, Maria Eichlseder

共通鍵暗号プリミティブの差分線形識別子を効率的に探索するための汎用的かつ自動化されたツールの開発に関する論文である。従来の差分線形攻撃では、対象となるプリミティブ E を差分攻撃パート E_u と線形攻撃パート E_l の 2 つのパートに分割し、これらのパートが完全に独立であるという仮定の下で計算量が評価されてきた。しかしながら、実際にはこれらのパートには依存関係があるため、従来の計算量評価が正確ではないという問題があった。この問題を解決するための代表的な手法として sandwich フレームワークがある。このフレームワークでは、対象となるプリミティブを 2 つのパートだけでなく、これらの依存関係を考慮するための中間パート E_m を導入する。つまり、プリミティブを $E = E_l \circ E_m \circ E_u$ と分割して解析することにより、計算量をより正確に評価できるようになった。差分線形攻撃と類似した攻撃手法であるブーメラン攻撃では、この中間パート E_m を詳細に分析するためのブーメラン接続表（BCT: Boomerang Connectivity Table）フレームワークが提案され、このフレームワークを拡張するような様々な応用手法もまた提案されてきた。一方で、差分線形攻撃においても BCT フレームワークと同様に差分線形接続表（DLCT: Differential-Linear Connectivity Table）フレームワークが提案されているが、BCT フレームワークのような拡張手法が提案されていないという課題がある。特に、複数ラウンドをカバーする中間パート E_m を許容するような手法が未解決な課題として残されている。また、差分線形識別子を自動的に探索するツールが提案されているものの、ARX 暗号のための専用ツールであり、ブロックサイズが小さいバリアントにしか適用できないという汎用性の面で課題がある。

本研究ではこれらの課題を解決する。具体的には、BCT フレームワークの拡張手法を参考に、複数ラウンドをカバーする中間パート E_m を許容するような新しい接続表を定義し、DLCT フレームワークを拡張した。また、この拡

張した DLCT フレームワークを使用し、制約プログラミング（CP）と混合整数線形計画法（MILP）に基づく差分線形識別子探索のための汎用的な自動化ツールを開発した。提案ツールが様々なプリミティブに適用可能であることを示すために、AES、Ascon、CLEFIA を含む 11 種類のプリミティブに適用され、それぞれ既存の差分線形識別子を改善できることが示された。

Speeding up Preimage and Key-Recovery Attacks with Highly Biased Differential-Linear Approximations

Zhongfeng Niu, Kai Hu, Siwei Sun, Zhiyu Zhang, Meiqin Wang

スポンジ構造型ハッシュ関数に対する原像攻撃とスポンジ構造型認証暗号に対する鍵回復攻撃の高速化手法に関する論文である。代表的なスポンジ構造型ハッシュ関数・認証暗号として Ascon と Sparkle がある。これらの暗号学的置換に対して差分線形（DL: Differential-linear）識別が最も有効な解析手法の 1 つであると知られているが、これらの識別攻撃が原像攻撃や鍵回復攻撃のようなより現実的な攻撃へと拡張された研究はない。特に、Sparkle のハッシュ関数/XOF バリアントである Esch/XOEsch に対する原像攻撃はまだ報告されておらず、Sparkle の認証暗号バリアントである Schwaemm に対する鍵回復攻撃は設計者らによる評価しか報告されていない。

本研究では、最初に原像攻撃を高速化させるための高バイアスな DL 識別子に基づく新しい解析フレームワークを提案する。基本的なアイデアは次のとおりである。関数 F の像（image）O が与えられ、x と $x \oplus \delta$ がそれに対応する原像かをチェックする。$y = F(x)$ を計算した結果、$y = O$ の場合は原像 x が得られるため攻撃成功となる。一方、$y \neq O$ の場合は DL 近似を応用して確率的に $F(x \oplus \delta)$ の計算をスキップさせる。このスキップできる計算量だけ高速化が可能となり、これには複数個の高バイアスな DL 識別子が必要となる。同様のアイデアを使用し、鍵回復攻撃を高速化させるための解析フレームワークも提案された。後者のフレームワークでは、高バイアスな関連鍵差分線形識別子を使用して単一鍵設定での鍵回復攻撃を実現している。つまり、単一鍵設定での安全性を主張するためには、関連鍵設定での解析も考慮する必要があることを意味する。

これらのフレームワークはスポンジ構造型ハッシュ関数（Ascon-Hash）と XOF（XOEsch、Ascon-XOF）に対する原像攻撃とスポンジ構造型認証暗号（Schwaemm）に対する鍵回復攻撃に適用された。Ascon-Hash に対しては 12 ラウンド中 4 ラウンドまで原像攻撃に成功するが、これは設計者の主張する安全性レベルを超えた結果であることに注意が必要である。XOEsch に対しては 7 ラウンド中 2.5 ラウンドまで、Ascon-XOF に対しては 12 ラウンド中 4 ラウンドまで原像攻撃に成功した。また、Schwaemm に対しては 7 ラウンド中 4.5 ラウンドまで鍵回復攻撃に成功した。

New Approaches for Estimating the Bias of Differential-Linear Distinguishers

Ting Peng, Wentao Zhang, Jingsui Weng, Tianyou Ding

共通鍵暗号プリミティブの差分線形（DL: Differential-Linear）バイアスを厳密に評価するための汎用的な手法に関する論文である。前述のとおり、DL 解析では対象となるプリミティブ E を $E = E_l \circ E_m \circ E_u$ と分割して解析する手法である。ここで、E_u は差分パート、E_m は中間パート、E_l は線形パートである。2017 年に Blondeau らは「DL 解析は、理論的な意味において、多次元線形攻撃もしくは切り詰め差分攻撃のいずれかとして考えることができる」と主張し、これらの変換方法について議論した。しかし、このアイデアはその後の進展がなく、理論的な意味での主張に留まっている。

本研究では、DL バイアスと切り詰め差分確率における関連性を形式的に表現する新しい公式を提示し、Blondeau らの理論を拡張させる。この拡張のために、切り詰め差分分布表（TDT: Truncated Differential Distribution Table）

を提案する。TDT は単一の S-box に関する切り詰め差分分布、もしくは複数ラウンドの切り詰め差分分布を表現するものである。TDT を利用することで、切り詰め差分確率の評価を大幅に加速化することが可能となる。新しい公式と TDT に基づき、DL バイアスを厳密に見積もるための 2 つの新しいアプローチを提案する。1 つは中間パート E_m が複数ラウンドである際の DL バイアスを計算するためのものであり、もう 1 つは中間パート E_m が 1 ラウンドのみである際のバイアスを計算するためのものである。対象となるプリミティブの解析困難性に合わせてアプローチを使い分けることとなる。

これらのアプローチを 5 つの共通鍵暗号プリミティブ（Ascon、Serpent、KNOT、AES、CLEFIA）に適用した。Ascon に対しては、既存研究において 4/5 ラウンド DL 識別子の理論値と実験値に大きな乖離があったという問題に対処する。提案アプローチを適用することで理論値の改善に成功し、理論値と実験値がほぼ一致することを示した。また、新しい 6 ラウンド DL 識別子を発見し、既存の DL 識別子の中で最良の結果を達成した。AES に対しては、3 ラウンド DL 識別子をある条件の下で網羅的に探索し、その結果をベースとして 4/5 ラウンド DL 識別子へと拡張した。AES の 5 ラウンド DL 識別子は初めての結果である。その他、Serpent、KNOT、CLEFIA に対しても同様の結果が得られた。

D.7 CHES 2024

Exploiting Small-Norm Polynomial Multiplication with Physical Attacks Application to CRYSTALS-Dilithium

Olivier Bronchain, Melissa Azouaoui, Mohamed ElGhamrawy, Joost Renes, Tobias Schneider

格子ベース署名方式 CRYSTALS-Dilithium の故障攻撃に関する論文である。CRYPSTALS-Dilithium は多項式環 $\mathbb{Z}_q[X]/(X^{256}+1)$ 上の Module-LWE 問題を安全性の根拠とした Fiat-Shamir with abort 型構成の署名である。署名は環上の $z = y + s * c \mod q$ の計算により生成されるが、z のノルムが基準値を超える場合には別の乱数を用いて再計算を行う。本論文では、サイドチャネル情報として $x = c * s$ と y のハミング重みに関する情報が漏洩した場合の鍵復元攻撃、および故障注入攻撃として y のビットを反転させた場合の鍵復元攻撃を提案している。攻撃に必要なサンプル数の見積もりおよび実際の攻撃実験をおこなっており、サイドチャネルの SNR 比にもよるがいずれも現実的な想定で CRYSTALS-Dilithium の仕様書にあるレベル 2,3,5 のパラメータに対しても鍵復元が可能であるとしている。

Defeating Low-Cost Countermeasures against Side-Channel Attacks in Lattice-based Encryption A Case Study on Crystals-Kyber

Prasanna Ravi, Thales Paiva, Dirmanto Jap, Jan-Pieter D'Anvers, Shivam Bhasin

格子ベース KEM CRYSTALS-Kyber のサイドチャネル攻撃に関する論文である。既存のサイドチャネル対策の中で著者らが低コストで実行可能な検出技術に基づく方法と呼んだ一群の対策手法について取り上げている。この手法は一般的には悪意のある入力を検出しそれらをブロックするものであるが、代表的な方法として暗号文の整合性チェックとデカプセル化時のエラーチェックが取り上げられ、それらを無効化する一般的な攻撃手法が提案されている。

暗号文の整合性チェックに関する考察として、先行研究の多くが、攻撃時に低エントロピーの暗号文がオラクルに入力されるという仮定を置き、その対策としてエントロピーのチェック機構を実装しているという共通点を指摘している。この対策への攻撃として、既存のサイドチャネル攻撃の中で用いる暗号文の中でエントロピーが低いものを除外することで、ほぼオーバーヘッド無しに攻撃を成功させることが可能であるとしている。

鍵デカプセル化時のエラー検出に関する考察として、先行研究では鍵デカプセルエラーの検出時には秘密鍵のリフレッシュが行われ、複数の悪意のある暗号文の復元テストが不可能となる対策があるという共通点を指摘している。この場合でも、正規の暗号文のみを用いた攻撃が可能であることが示される。技術的には復号関数のサイドチャネル情報から連立不等式を構成し、Pessl と Peokop（TCHES 2021）の信頼度伝搬法に基づくアルゴリズムにより秘密鍵を復元しているが、先行研究と比較して必要な不等式の数が半分になっている。

以上の結果を CRYSTALS-Kyber の実装へと適用し、10 万回程度の測定で Kyber-768 の秘密鍵の復元が可能であることを確認している。

Carry Your Fault: A Fault Propagation Attack on Side-Channel Protected LWE-based KEM

Suparna Kundu, Siddhartha Chowdhury, Sayandeep Saha, Angshuman Karmakar, Debdeep Mukhopadhyay, Ingrid Verbauwhede

多項式環上の LWE ベース KEM に対する故障注入攻撃に関する論文である。KEM のデカプセル化ルーチン内でパッシブなサイドチャネル攻撃への対策として多項式環の演算をマスキングするために導入された、Arithmetic to Boolean (A2B) 機構と呼ばれる箇所を攻撃の対象としている。Delvaux (TCHES 2022) による先行研究では、マスキングのために導入された乱数がサイドチャネル情報のバラエティを増やしてしまい、攻撃の成功確率上昇につながることが示唆されていた。これは、セキュリティを強化するための対策がかえって脆弱性を生む状況の発見である。

本論文ではさらに、A2B 機構における演算の変更自体が問題であると指摘している。多項式環の加算回路の A2B 機構に対して複数ビットを反転させる故障注入攻撃と、その結果として復号エラーが起きたかどうかの情報から秘密鍵を復元する攻撃を提案している。技術的にはビットの反転が演算回路の中でどのように伝搬するのかを Delvaux の信頼度伝搬法による攻撃をベースに解析している。また、著者らは標準的に用いられている単純な手法では対策は困難であるとしている。

実験として、格子ベース KEM CRYSTALS-Kyber のデカプセル化モジュールに対する攻撃のデモンストレーションを行い 185 万回の故障注入から鍵復元が可能であるとしている。また、同様の脆弱性が格子暗号 SABER の実装にも存在する可能性が高いと指摘している。

Elisabeth Krahmer, Peter Pessl, Georg Land, Tim Güneysu

Correction Fault Attacks on Randomized CRYSTALS-Dilithium.

格子ベース署名 CRYSTALS-Dilithium への故障注入攻撃に関する論文である。実装時の安全性のため、署名生成時に deterministic mode と randomized mode の 2 種類が選べるようにしてある。後者は hedged mode とも呼ばれ、より安全性が高いとされており、標準化方式の中ではデフォルトのモードである。本論文では、両方のモードの実装に対する故障注入攻撃による鍵復元攻撃について検討し、後者のモードでも安全ではないことを指摘している。本論文で仮定される攻撃手法は先行研究のフレームワークを引き継いだものであり、署名生成ルーチンの実装に対して故障注入を行うことで生成した複数の不正な署名が、署名検証ルーチンで受理されるかどうかの情報から格子基底簡約により秘密鍵を復元するという順序で行われる。故障注入は命令スキップと公開鍵行列 A の内容の操作により行われる。

本論文では Dilithium-2 に対して、命令スキップ攻撃では 1024 個の不正な署名から、A の操作をによる攻撃では 512 個の不正な署名を用いて鍵復元が可能であるとしている。先行研究による故障注入攻撃への対策を乗り越えて攻撃する手法も示されており、故障のシミュレーション、および ARM ベースのマイクロコントローラに対するクロック

グリッチを行い、攻撃の正しさを検証している。攻撃の検証コードは `https://github.com/Chair-for-Security-Engineering/dilithium-faults` で公開されている。

Hints from Hertz: Dynamic Frequency Scaling Side-Channel Analysis of Number Theoretic Transform in Lattice-Based KEMs

Tianrun Yu, Chi Cheng, Zilong Yang, Yingchen Wang, Yanbin Pan, Jian Weng

格子ベース暗号 CRYSTALS-Kyber、NTRU に対するサイドチャネル攻撃に関する論文である。Ring-,Module-のような構造を持つ格子ベース暗号では高速化のため数論変換（NTT）が用いられることが多い。暗号の処理においては NTT 処理が最も時間がかかるため攻撃の対象となりやすい。

本論文では、近年の CPU に消費電力削減のための処理内容に合わせた電圧や動作周波数の調節機構が備わっている点に注目する。NTT 処理中の CPU 周波数と消費電力の情報から入力のハミング重みに関する情報を抽出し、秘密鍵の部分情報を抽出する攻撃を提案している。実証実験として、Intel Core-i7 9600K を用いた 20 万回分の計測データを平均することで情報が抽出可能であり、CRYSTALS-Kyber、NTRU の復号ルーチンに対して解析を行う事で攻撃計算量の指数部分が 30 から 40% 程度削減されることを示している。

D.8 TCC 2024

Sparse Linear Regression and Lattice Problems

Aparna Gupte, Neekon Vafa, Vinod Vaikuntanathan

格子暗号の安全性に関わる、スパース線形回帰（Sparse Linear Regression、以下 SLR）に関する論文である。基底追跡、LASSO、Dantzig セレクタといった ℓ_1-緩和法により、デザイン行列が特別な場合、SLR を解くことができる。しかし一般のデザイン行列に対するアルゴリズムは知られていない。また現状知られている効率的なアルゴリズムについても、平均計算量は知られていない。

本研究では、格子に対する BDD（Bounded Distance Decoding、有界距離復号）問題に関する最悪計算量を仮定した上で、SLR の平均計算量を与えている。この SLR 問題と BDD 問題の関係性において、SLR 問題のデザイン行列の制限固有値（restricted eigenvalue）条件は、BDD 問題のインスタンスを定義する格子の基底に関する条件数に対応している。この帰着により、BDD 問題の困難性を仮定した上で、デザイン行列の分布において、SLR 問題が困難な領域が与えられた。

加えて本論文では、デザイン行列が通常のガウシアンで生成されているケースを考察している。この方式で生成されるデザイン行列が識別可能な領域にある場合、LASSO により SLR 問題を解くことができるが、本論文では、この行列が識別不能な領域にある場合、例え多くのスパース解を持っていたとしても、解を求めることが困難であることを示している。この困難性は、連続的 LWE（Continuous Learning With Errors）に関する最悪計算量仮定に基づいている。これは近年、最短ベクトル問題（Shortest Vector Problem）の最悪計算量仮定と等価であることが示されており、この意味で、格子暗号の困難性と SLR 問題を関連付けている。

Worst-Case to Average-Case Hardness of LWE: An Alternative Perspective

Alexandra Veliche, Divesh Aggarwal, Leong Jin Ming

格子暗号の安全性に関する、LWE（Learning With Errors）問題の困難性に関する論文である。先行研究である Regev（STOC 2005）、Peikert（STOC 2009）、Brakerski-Peikert-Langlois-Regev-Stehle（STOC 2013）によって、GapSVP および BDD 問題の最悪計算量に関する困難性から、LWE 問題の平均計算量に関する困難性が導かれていた。GapSVP 問題は格子基底と実数 $\alpha < \beta$ が与えられたときに最短ベクトルの長さが α より小さいか、β より大きいかを判定する計算問題であり、α と β の間にある場合にはどちらを返しても良いものとする。BDD 問題は格子基底とベクトル $\boldsymbol{v}$, 実数 r が与えられたときに $\boldsymbol{v}$ から距離 r 以内にある格子点を探索する問題である。これらの問題から帰着される LWE 問題の平均計算量に関する困難性の評価が最良であるかは不明であった。

本論文では、計算量の代替えとして、PPT（確率的多項式時間、Probabilistic Polynomial Time）アルゴリズムにより達成できる最大の成功確率を基に、LWE 問題の困難性が研究された。この観点から、LWE の困難性と BDD の困難性の関係性がより明らかにされている。特に、BDD 問題を解く PPT アルゴリズムについてのとある困難性予想を仮定した上で、LWE 問題を解く PPT アルゴリズムの攻撃精度の上からの評価を改良した。さらに LWE 問題について、決定論的 PPT 攻撃の攻撃精度の最高値と、計算論的 PPT 攻撃のそれの関係性も与えられた。この方式は実用的な安全性解析のフレームワークに応用しうる。

D.9 Asiacrypt 2024

Rare Structures in Tensor Graphs – Bermuda Triangles for Cryptosystems Based on the Tensor Isomorphism Problem

Lars Ran, Simona Samardjiska

NIST 耐量子計算機署名方式の候補である MEDS と ALTEQ の安全性に関連する、3-TI（3-Tensor Isomorphism）問題に関する解読論文である。3-TI 問題とは、有限体 $\mathbb{F}_q$ 上で与えられた、座標変換で移りあう二つの 3-テンソル（立方行列のこと）に対して、その座標変換を具体的に求める問題である。MEDS の安全性は、3-TI 問題と同値な問題である MCE（Matrix Code Equivalence、行列符号同値）問題に依拠している。ALTEQ の安全性は、3-TI 問題の特別な場合である ATFE（Alternting Trilinear Form Equivalence、交代三線型形式同値）問題に依拠している。先行研究として、MCE 問題に対しては Narayanan らによるグラフ理論的アルゴリズムが、ATFE 問題に対しては Ran らによる代数的アルゴリズムが知られており、MEDS と ALTEQ の安全性をわずかに低減させることが報告されていた。

本論文では、3-TI 問題を解く新手法が報告された。著者らは、署名鍵である座標変換を復元するために、“triangles” という新たな不変量を導入した。“triangles” とは、3-テンソルのグラフにおける長さ 3 の周期のことを指しており、確率約 $1/q$ という非常に稀な確率で存在する。このアプローチはグラフベースのアルゴリズムで典型的だが、しかし通常の組合せ論的手法とは異なり、不変量を非線形方程式系としてモデル化しそれを解くという、純粋な代数的手法を用いて行われる。この非線形方程式系の求解には、tri-graded な多項式環に適応した Gröbner 基底法を用いている。

著者らは、この新たな不変量である “triangles” を探し出すアルゴリズムを提案し、その計算量の下限と上限を評価した。そして、“triangles” が存在する場合に機能する、MEDS と ALTEQ 双方への新たな暗号解析を与えている。特に（“triangles” が存在する）ALTEQ について、実用的な攻撃が提案された。この攻撃は全てのセキュリティレベルに対して少なくとも 60 ビットの改善を与え、特にレベル I のパラメータに対してわずか 1501 秒で署名鍵を復元する

ことが報告された。

Don't Use It Twice! Solving Relaxed Linear Equivalence Problems

Alessandro Budroni, Jesús-Javier Chi-Domínguez, Giuseppe D'Alconzo, Antonio J. Di Scala, Mukul Kulkarni

NIST 耐量子計算機署名方式の候補である LESS 署名方式、MEDS 署名方式の安全性に関連する、LCE（Linear Code Equivalence）問題に関する解読論文である。LCE 問題とは、二つの (n, k)-線型符号に対して与えられる生成行列 G, G' について、$G' = SGQ$ となる k 次正則行列 S と n 次単項行列 Q を計算せよ、という問題であり、LESS 署名方式の安全性の根拠となっている。線型符号が行列の為す線形空間の部分空間である場合、LCE 問題は MCE（Matrix Code Equivalence）問題と等価である。この意味で本論文は、MCE 問題を安全性の根拠とする MEDS 署名方式とも関連している。

本論文は、この LCE 問題と MCE 問題に関して、秘密を回復するために必要なサンプル数について研究している。先行研究として、$G'_i = SG_iQ$ なる対 (G_i, G'_i) が $i = 1, \ldots, t$ について与えられているとき、サンプル数 t が $t = kn$ であれば、(S, Q) が復元できることが知られていた。このサンプル数 t を減らすのが本論文の目標である。加えて本論文では、組織形式 LCE 問題（LCE Systematic Form Version）も視野に入れることで、$G'_i = S_iG_iQ$ のようなケースに Q を復元する方式についても提案している。ここで組織形式 LCE 問題とは、G, G' が組織符号の生成行列であるとき、G' が GQ の組織符号となる単項行列 Q を計算する問題である。

結果として、サンプル数 t が $t = \lfloor \frac{n^2}{k(n-k)} \rfloor + 1$、さらに $k = n/2$ であるときは $t = 2$ であれば、多項式時間計算量および多項式メモリ計算量で LCE 問題を解くアルゴリズムが提案された。著者らはサンプル G'_i のパリティ検査行列を H'_i としたとき、$(G_i \otimes H'_i) \cdot vec(Q) = 0$ が満たされることに着目した。ここで $vec(Q)$ は Q の行ごとに成分を並べた列ベクトルである。サンプル数が $t = 2$ の場合、著者らは Saeed のアイデアに着想を得て上記の線型方程式を解くことで、署名鍵を導いている。結果として、LCE 問題に依拠する LESS 署名形式および MEDS 署名形式において、署名鍵の再使用は避けるべきと結論された。

Attacking ECDSA with Nonce Leakage by Lattice Sieving: Bridging the Gap with Fourier Analysis-based Attacks

Yiming Gao, Jinghui Wang, Honggang Hu, Binang He

ECDSA および Diffie-Hellman 鍵共有に対するサイドチャネル攻撃に関する論文である。特に本論文では、サイドチャネル攻撃のアプローチとして、HNP（Hidden Number Problem）について考察する。HNP を解くための 2 つの主要なアプローチとして、格子ベース攻撃とフーリエ解析ベース攻撃が知られている。十分に長いナンス（Nonce）部分列が漏洩している場合、格子ベース攻撃はより効率的であり、少ないサンプル数で攻撃可能である。しかし、例えばナンスのわずかな部分（例えば 1 ビット）のみが漏洩している場合には、従来手法による攻撃は困難であった。またフーリエ変換ベースの攻撃手法と比較して、入力の誤りについてのロバスト性が失われていた。

本論文では、これら 2 つのアプローチ間のアルゴリズム的なトレードオフを導入している。Albrecht と Heninger が Eurocrypt 2021 で提案した格子を修正するために、著者らはパラメータ x を導入した新たな格子を提案した。漏洩したビット数を l として、簡約された格子次元は約 $\log_2 x/l$ に比例して減少する。著者らはさらに、誤り入力を伴う HNP も著者らの格子ベース手法で解けるよう、アルゴリズムを拡張した。結果として、ECDSA に対する既存の最先端の格子ベースの攻撃が改良された。特に 1 ビット漏洩に対する以前の最良の格子ベース攻撃は 112 ビット以下の曲

線上でのみ行われていたが、これを 160 ビット以下の曲線に改良した。

ZKFault: Fault Attack Analysis on Zero-knowledge-based Post-quantum Digital Signature Schemes

Puja Mondal, Supriya Adhikary, Suparna Kundu, Angshuman Karmakar

NIST 耐量子計算機署名方式の候補である LESS 署名方式、CROSS 署名方式、MEDS 署名形式についての故障注入攻撃についての論文である。これらの符号ベース署名方式は、秘密鍵の知識についての対話型ゼロ知識署名を Fiat-Shamir 変換することで、署名方式を得ている。LESS、CROSS、MEDS では、署名長を圧縮するために、参照木（Reference Tree）と著者らが呼んでいる木構造を利用している。例えば LESS 署名方式では、署名者と検証者の間で単項行列生成器を共有し、Goldreich-Goldwasser-Micali 構成を活用することで、チャレンジに対するレスポンス（すなわち署名）を、シード値と参照木のノードを指定することで圧縮する。

本論文では、この参照木に対する故障注入攻撃を研究している。著者らは、この参照木にビットフリップを発生させることで、秘密鍵が漏洩することを指摘した。この故障注入攻撃は、参照木を用いて署名長を圧縮している上述の 3 つの方式に通用する。特に LESS 方式及び CROSS 方式について参照木の構造が研究され、全ての秘密鍵が漏洩するような単一故障注入攻撃が提案された。また著者らは、こういった故障注入攻撃を防ぐ方法と、その方法が署名長にどのような影響を与えるかを議論している。

Reducing the Number of Qubits in Quantum Information Set Decoding

Clémence Chevignard, Pierre-Alain Fouque, André Schrottenloher

シンドローム復号問題に関する量子解析論文である。本論文では、Bernstein が PQCrypto 2010 で提案したシンドローム復号問題の量子求解アルゴリズムである ISD（Information Set Decoding）の量子メモリコストの最適化を取り組んでいる。

Bernstein の ISD は、Prange の ISD に Grover の量子探索を組み合わせることで得られており、符号の長さが n であるとき、各反復処理で $O(n)$ 次元の線型系を解くことができる。耐量子計算機暗号では、n として 10^3 から 10^5 の値が採用されている。このアルゴリズムにおいては、ガウスの消去法が、行列を記憶するのに $O(n^2)$ のメモリを必要とするため、量子メモリ計算量のボトルネックとなっていた。

著者らはこの量子メモリを削減するため、Wiedemann によるスパース行列の逆行列アルゴリズムを活用した。このアルゴリズムでは、ベクトルへの行列作用のみを考慮すれば良いため、メモリの削減が実現される。結果として、$O(n)$ 量子メモリ、$O(n^3)$ 個の Toffoli ゲートを用いた深さ $O(n^2\log n)$ の ISD 量子回路が提案された。例えば最小の Classic McEliece については、以前の研究では 50 万量子メモリが必要だったが、著者らのアルゴリズムはこれを 18098 量子メモリまで削減した。

これらの方式はメモリについては最適化されているが、Toffoli ゲート数についてはそうではない。このトレードオフとして、$O(n\log^2 n)$ 量子ビットの下で、Toffoli ゲートの数を $O(n^2\log^2 n)$ に削減した方式も本論文で提案された。

Cryptanalysis of Rank-2 Module-LIP with Symplectic Automorphisms

Hengyi Luo, Kaijie Jiang, Yanbin Pan, Anyu Wang

格子同型問題（Lattice Isomorphism Problem）についての解読論文である。格子同型問題とは、NIST 耐量子計算機署名形式の候補である HAWK などの安全性の根拠となっている数学的プリミティブである。

Eurocrypt 2024 において、Mureau らは、数体 K 上の加群格子に対する格子同型問題（module-LIP）を定義し、$\mathbb{K}$ が総実体のとき、$\mathbb{K}^2$ の階数 2 部分加群の LIP 問題を解くヒューリスティックな古典アルゴリズムを提案した。このアルゴリズムはほとんどの部分加群とほとんどの総実体に対し、数論的な仮定の下で機能していた。

本論文ではこのアルゴリズムが改良され、決定論的な古典多項式時間アルゴリズムでの解法が与えられた。このアルゴリズムは全ての階数 2 部分加群と全ての総実体に機能し、数論的仮定も必要ないと報告された。

この結果を得るためのテクニックとして著者らは、（擬）シンプレクティック自己同型という新たな加群の同型を導入した上で、CM 体上の module-LIP を解くことが、ある特定のシンプレクティック自己同型を見つけることに帰着できることを示した。さらに弱（擬）シンプレクティック自己同型を効率的に計算するアルゴリズムを与えた。体が総実体である場合、これはその望ましい特定のシンプレクティック自己同型となっているため、著者らの主張した結果が従う。加えて本論文では、弱シンプレクティック自己同型は、HAWK の偽造耐性の証明で用いられた omSVP 仮定を無効にすることが報告された。ただし本論文は、HAWK に対する直接的な攻撃を与えるものではない。

On the Spinor Genus and the Distinguishing Lattice Isomorphism Problem

Cong Ling, Jingbo Liu, Andrew Mendelsohn

格子同型問題（Lattice Isomorphism Problem、LIP）についての解読論文である。LIP とは、NIST 耐量子計算機署名形式の候補である HAWK などの安全性の根拠となっている数学的プリミティブであり、二つの与えられた整格子が整数環上で同型かを判断する問題である。これらが任意の素数 p についての p 進整数環上及び実数体上でも同型であるとき、二つの整格子は「同じ種数を持つ」と呼ばれる。同じ種数を持たないのであれば同型ではないことから、種数は LIP を解く上で重要な概念である一方、同じ種数を持っている場合、同型であるかを判別することは依然として困難である。

著者らはこの問題に取り組むため、種数の概念をより細分化したスピノール種数（spinor genus）を研究した。二つの整格子が「同じスピノール種数を持つ」とは、ある固有直交変換 γ と、任意の素数 p に対し p 進整数環上のスピノールノルム 1 のある局所変換 δ_p が存在して、$\gamma \cdot \delta_p$ で p 進整数環上の格子の同型が与えられることを言う。

本論文では、同じ種数を持つ二つの格子が同じスピノール種数を持つかどうかを判定する方法が、特別な場合に与えられた。特に、同じ種数を持つ二つの階数 2 の非等方（anisotropic）な整二次形式について、同じスピノール種数を持つかどうかを量子多項式時間で判定するための必要条件が与えられた。これは特別な場合の新たな LIP の解法を与えるが、HAWK では類数が 1 より大きい数体上の階数 2 のエルミート整二次形式が用いられていることから、本論文は直接的に HAWK を攻撃するものではないことも報告された。

Extending Class Group Action Attacks via Sesquilinear Pairings

Joseph Macula, Katherine E. Stange

楕円曲線への類群の群作用に関する暗号学的計算問題の解析に関する論文である。適当な整環（order）を固定する。イデアル類群 $\mathrm{Cl}(\mathcal{O})$ の虚数乗法（CM）を持つ楕円曲線の集合への作用を用いた Diffie-Hellman 型の鍵共有方式がいくつか提案されており、それらの安全性は DDH-CGA(Decisional Diffie-Hellman for Class Group Action) 問題として整理されている。判定問題の困難性は体と楕円曲線の構造に依存する。

本論文では、oriented な楕円曲線に対する群作用を用いた計算問題を取り上げる。CSIDH, OSIDH のような多くの先行研究がこの問題を用いた鍵共有方式となっている。Castryck ら (J. Cryptology 35, 4 および Res. Num. Th. 8, 4) により、体の類数が偶数である場合には DDH 問題を多項式時間で計算するアルゴリズムが得られており、以降も効

率的に解けてしまう DDH-CGA の特徴づけが行われてきた。近年、Castryck et al. (Crypto 2023) はペアリングを用いてある種の隠れ同種写像問題を SIDH の計算問題に還元することで解くアプローチを発表した。この計算が効率的に行われるためには同種写像の次数が既知かつ代数体の判別式 $\Delta_{\mathcal{O}}$ が素数の高いべき乗で割り切れるという条件が必要である。

この論文では、Stange(arXiv: 2405.14167) により導入された楕円曲線間の半双線型ペアリングを用いて種々の暗号学的成果を得ている。

- Castryck et al. (Crypto 2023) の攻撃を拡張し、拡大体上での計算を行わない形にすることで多項式時間で可能な判別式の範囲を拡張した。特に、Castryck らにより攻撃に必要な torsion point の個数を減らした変種である SIDH_1 問題から SIDH への帰着
- 公開鍵暗号方式 FESTA を構成するトラップドア関数の鍵復元問題 (Computational isogeny with scaled-torsion: CIST) を同種写像の向き (orientation) を発見する計算問題へと帰着
- ペアリングと向きの情報を用いることで、同種写像による点の像 $\phi(P)$ に関する情報を部分的に復元する効率的なアルゴリズムの構成。それを用いた全数探索により、類群作用を用いた暗号方式を破るアルゴリズムが得られる。
- 同種写像が未知の状況において、与えられた点がある torsion point の像であるかどうかを判定する DDH 型の計算問題を用いて暗号方式を構成することの困難さ
- 2 つの独立な向きから同種写像を復元する計算問題に対して、既知の KLPT アルゴリズムとは異なる SIDH 問題を経由したアプローチでのアルゴリズムを与えた

Evasive LWE Assumptions: Definitions, Classes, and Counterexamples

Chris Brzuska, Akin Ünal, Ivy K. Y. Woo

Elasive LWE 問題の解析に関する論文である。この計算問題は Wee(Eucorypt 2022) により提案された LWE 問題の変種であり、2 種の試行 Pre と Post により定義される。適当なランダム行列 B と秘密ベクトル s、および指定された分布からサンプリングした行列 P に対して、

- $(B, P, sB + e, sP + e'', \mathsf{aux})$ を $(B, P, \$, \$, \mathsf{aux})$ と識別する試行を Pre
- $(B, P, sB + e, B^{-1}(P), \mathsf{aux})$ と $(B, P, \$, B^{-1}(P), \mathsf{aux})$ を識別する試行を Post

とする。このとき，任意の多項式時間攻撃者に対してその成功率は多項式倍の差しかないことを主張するのが Elasive LWE 仮定である。ここで，$B^{-1}(P)$ は格子型トラップドアの Preimage、つまり $BS = P \mod q$ を満たす行列 S で、各列のノルムが小さいものを表す。e, e'' は適当な分布から取られたエラーベクトルとする．$はランダム要素，aux は Preimage のサンプリングに用いられた乱数列（coin tosses）をあらわす。この仮定は Preimage $B^{-1}(P)$ の情報がほぼ $sP + e''$ の構成にしか使えず、攻撃者のアドバンテージにならないということを示している。

Wee はこの仮定を暗号文ポリシー属性ベース暗号（Ciphertext-Policy Attribute-Based Encryption: CP-ABE）の構成に用いたが、その後類似の仮定を用いて様々な暗号方式の構成が行われている。本論文では Witness encryption(Tsabary, Crypto2022)、Witness encryption および null-IO(Vaikuntanathan et al., Asiacrypt 2022)、属性ベース暗号（Agrawal et al., Crypto2023）の構成に用いられた変種を取り上げる。これらの構成の中で用いられる変種は Preimage のサンプリング中に用いられた乱数の情報が aux に完全に含まれないという共通点があり、private-coin 型と名付けられている。

private coin 型の場合 Post 側では復元可能ではあるが、pre 側では復元が困難な構成、つまり仮定を破る反例が与えられる。具体的な反例（Counterexample 1）として両方の試行に P と aux が含まれず、Pre 側が $(B, sB+e, sP+e'')$ を $(B, \$, \$)$ と識別する試行 Post 側が $(B, sB+e, B^{-1}(P))$ と $(B, \$, B^{-1}(P))$ を識別する試行であるとする。このときに Pre 側では識別不可能であっても、Post 側では $B^{-1}(P)$ の中から P に関する、識別に役立つ情報を引き出すことができて識別可能となる。同様の反例は試行に B が与えられない場合や、Preimage Sampler に B が入る場合などでも可能であり、これらの反例を用いて、上に挙げた先行研究での仮定が成り立たないことが示される。

本論文ではさらに、仮定の修正案として Private-coin Binding、Private-coin Hinding と呼ばれる変種を提案しており、この仮定を用いることで Vaikuntanathan et al. の構成および Agrawal et al. の構成が修正できること、また Tsabary の構成も修正可能であると見込まれることが主張されている。

On the Semidirect Discrete Logarithm Problem in Finite Groups

Christopher Battarbee, Giacomo Borin, Julian Brough, Ryann Cartor, Tobias Hemmert, Nadia Heninger, David Jao, Delaram Kahrobaei, Laura Maddison, Edoardo Persichetti, Angela Robinson, Daniel Smith-Tone, Rainer Steinwandt

有限群の半直積群上の離散対数問題（Semidirect Discrete Logarithm Problem: SDLP）に関する量子アルゴリズムを与える論文である。非可換群上の SDLP は、有限群 G とその自己同型群 $Aut(G)$ の半直積から半群を構成して定義される。これまでに効率的な一般的な G に対する量子アルゴリズムが知られていなかったことから、耐量子計算機暗号プリミティブを構成する候補としていくつかの構成に用いられてきた。本論文では非可換群上の SDLP をほとんどすべての群に対して量子多項式時間で解くアルゴリズムを与え結論として既存の非可換群上の SDLP を安全性の根拠に用いた暗号方式は耐量子計算機暗号としては実用的ではないと結論付けている。

技術的には、Imran and Ivanyos (Des. Codes. Crypt., 2024) の可解群上の SDLP に対する量子多項式時間アルゴリズムの手法を大幅に拡張したものである。本論文では、G が可解群でない場合の SDLP に対して、いくつかの有限単純群上の SDLP への量子帰着が与えられている。知られる通り、有限単純群はいくつかのグループに分類されるが、単純群が巡回群であった場合には、通常の DLP として Shor のアルゴリズムにより量子多項式時間で解くことができる。交代群の場合には SDLP を行列 T, ベクトル u, v が与えられたときに $T^x u = v$ を満たす整数 x を計算する matrix power problem へと変換し、量子多項式時間で解くアルゴリズムが与えられる。Lie 群上のの SDLP も Shor のアルゴリズムをサブルーチンとして呼ぶことで解かれ、そのほかの散在単純群上の SDLP に関しては群の位数の制限から現実的な時間内に解かれてしまう。

It's a Kind of Magic: A Novel Conditional GAN Framework for Efficient Profiling Side-channel Analysis

Sengim Karayalcin, Marina Krcek, Lichao Wu, Stjepan Picek, Guilherme Perin

AES-128 に対するサイドチャネル攻撃についての論文である。プロファイル型サイドチャネル攻撃では、攻撃対象のデバイスの完全なコピーであるプロファイルデバイス（profiling device）に、マスク（乱数）も込めてアクセスできることを仮定する。しかし著者らは、安全な製品のデバッグモードやテストモードには強力な保護を適用するため、現実的にプロファイルデバイスを取得することは困難であると指摘する。

本研究では、攻撃者がプロファイルデバイスにはアクセスできないが、全く異なるデバイスにアクセスできる場合の鍵回復攻撃を検討している。具体的な手順は以下のようである。攻撃者はまず、攻撃するデバイスとは全く別のデバイ

ス（参照デバイスと呼ぶ）に攻撃アルゴリズムを実装する。参照デバイスは実際に攻撃するデバイスとは異なるものの、攻撃者にとってホワイトボックスであり、すべての内部状態とマスクにアクセスできると仮定される。次に、実際に攻撃するデバイスのデータを用いた、新しい CGAN (Conditional Generative Adversarial Network、条件付き敵対的生成ネットワーク) フレームワークを導入する。この CGAN フレームワークにおいて、生成器は、ホワイトボックス設定で得られる特徴量を模倣する。この模倣された内部的特徴量を入力としてサイドチャネル攻撃を行うことが、著者らの提案した手法である。

著者らは実験を行い、本手法がブラックボックスなサイドチャネル攻撃の有効性を向上させ、最悪ケースにおける安全性評価の結果と一致するか、または潜在的に上回るケースがあることを報告した。以上の結論を下に、著者らのフレームワークはプロファイルデバイスにアクセスする必要はなく、従ってより現実的な攻撃であると報告された。

Quantum Circuits of AES with a Low-depth Linear Layer and a New Structure

Haotian Shi, Xiutao Feng

AES-128 についての量子解析に関する論文である。量子解読アルゴリズムの中には、AES-128 の量子回路実装を必要とするものもある。この攻撃のコストを適切に評価するために、AES-128 の最適な量子実装が求められている。

本論文では、AES-128 の新たな量子回路が提案された。著者らは、Rijndael (AES) MixColumns 行列を表す CNOT 回路を、幅 32 深さ 16 から、幅 32 深さ 10 に削減した。さらにパイプライン構造を圧縮した。パイプライン構造とは、Grover と Simon のアルゴリズムに基づく量子攻撃で反復して用いられる量子オラクルの実装であるが、従来のパイプライン構造はラウンド数に応じて幅が大きくなってしまう。本論文では、ラウンド数に応じて幅が増加しない圧縮パイプライン構造を提案した。これはアンシラ量子ビットが少ない場合に効果的である。これにより、AES-128 の量子回路の T-深さ（行あたりの T ゲートの数）を 60 から 33 に削減した。さらに入力レジスタを変更しない Sbox 回路を提案することで、鍵スケジュールにおいて鍵を保存するために割り当てられていたアンシラ量子ビットを削減した。

結果として、AES-128 の量子回路実装として、幅と Toffoli 深さ（行あたりの Toffoli ゲートの数）の積 TofD-W のコストが 130720 にまで削減された。これは現状知られている中で最良である。

CRYPTREC Report 2024
(暗号技術評価委員会報告　CRYPTREC RP-2000-2024)

発行日：2025 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 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