CRYPTREC Report 2025

令和８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-2000-2025

「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、国立研究開発法人情報通信研究機構（NICT）及び独立行政法人情報処理推進機構（IPA）が共同で運営する暗号技術評価委員会の 2025 年度活動報告書である。

2025 年度において本委員会は、暗号技術検討会の承認の下、主として以下の活動を実施した。第一に、CRYPTREC 暗号リストに掲載されている暗号技術の安全性及び実装性能に係る監視、第二に、CRYPTREC 暗号リストへの掲載に向けた耐量子計算機暗号（Post-Quantum Cryptography: PQC）の技術的検討、第三に、新技術等に関する調査及び評価、第四に、暗号技術の安全な利用方法に関する調査である。

第一の活動については、国際会議等で発表される暗号技術の安全性及び実装性能に関する研究成果・技術動向を継続的に監視し、CRYPTREC 暗号リストに掲載されている暗号技術について、その危殆化が進行していないかの評価を実施した。第二の活動については、PQC の CRYPTREC 暗号リストへの掲載を視野に入れ、その安全性及び実装性能を含む技術的観点からの検討を実施した。量子計算機の発展を背景として、PQC への円滑な移行に係る検討は、国内外において重要な課題として位置付けられている。一方で、PQC を CRYPTREC 暗号リストに掲載するための技術的判断に当たっては、安全性・実装性能に関する調査及び評価を踏まえて、その判断に資する根拠を丁寧に整理し、技術的観点から検討することが不可欠である。本委員会では、このような認識の下、必要となる調査及び評価を計画するとともに、PQC の CRYPTREC 暗号リストへの掲載に向けた技術的検討を実施した。第三の活動については、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、「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「耐量子計算機暗号の研究動向調査報告書」の取りまとめに向けた基本方針を策定した。あわせて、耐量子計算機暗号 ML-KEM の安全性・実装性能に関する調査及び評価を外部評価により実施し、技術報告書として CRYPTREC の Web サイト上に公開した。第四の活動については、PQC への移行方針の技術的検討に資するため、PQC への移行に関する技術動向調査を外部評価により実施し、技術報告書として CRYPTREC の Web サイト上に公開した。

本委員会がこのような活動を進める背景には、近年における暗号技術を取り巻く社会的・技術的環境の大きな変化がある。CRYPTREC は、2000 年の IT 基本法制定とほぼ同時期に発足して以来、26 年にわたり、安心・安全な ICT 社会の実現に貢献してきた。2019 年以降のコロナ禍を契機として、非接触・非対面の生活様式を支える ICT の利活用は急速に進展し、今後もさまざまな分野において ICT の高度化・多様化が一層進むことが予想される。こうした状況の中で、暗号技術に対する社会的なニーズはかつてなく高まっている。本委員会としても、今後の社会情勢や技術動向を的確に踏まえつつ、健全なサイバー空間の実現と維持に資するよう、暗号技術の安全性という観点から求められる活動を着実に推進していく所存である。

本委員会の活動は、暗号技術、その実装及び運用に携わる多くの研究者・技術者の協力によって支えられている。末筆ながら、本活動に多大なるご協力を賜っている関係者の皆様に、ここに深甚なる謝意を表する。

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

本報告書は、情報セキュリティに関する基礎的な知識を有する読者を想定している。例えば、電子政府において、デジタル署名やデータ暗号化等の暗号関連システムに関わる業務に従事する方々を主な対象としている。ただし、個別テーマに関する調査報告等を適切に理解するためには、一定程度の暗号技術に関数る知識を有していることが望まれる。

本報告書の構成は以下のとおりである。第 1 章では、暗号技術評価委員会の活動概要について説明する。第 2 章では、暗号技術評価委員会における監視活動について報告する。2025 年度については、従来の監視活動に加え、「耐量子計算機暗号 ML-KEM の安全性・実装性能に関する調査及び評価」及び「耐量子計算機暗号への移行に関する技術動向調査」について、外部有識者による評価を実施しており、その結果を併せて記載している。第 3 章では、暗号技術評価委員会の下で活動する暗号技術調査ワーキンググループ（耐量子計算機暗号）の活動について報告する。

本報告書の内容は、我が国を代表する暗号分野の専門家によって構成される「暗号技術評価委員会」及びその下に設置された「暗号技術調査ワーキンググループ（耐量子計算機暗号）」における審議結果を取りまとめたものである。ただし、暗号技術の性質上、とりわけ安全性に関する事項については、その内容が将来にわたり保証されるものではない。このため、今後も継的に評価及び監視活動を実施していくことが必要である。

本報告書のほか、これまでに発行された CRYPTREC 報告書、ガイドライン、技術報告書、会議資料及び CRYPTREC 暗号リストに掲載された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、NICT 及び IPA）が共同で運営する Web サイト（`https://www.cryptrec.go.jp/`）において参照することができる。

本報告書及び上記 Web サイトから入手した CRYPTREC 活動に関する情報の利用に起因して生じたいかなる不利益や問題についても、本委員会及び CRYPTREC 事務局は一切の責任を負わない。

本報告書に関するご意見及びお問い合わせについては、CRYPTREC 事務局までご連絡いただきたい。

【問い合わせ先】info@cryptrec.go.jp

委員会構成

暗号技術評価委員会は、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、NICT と IPA が共同で運営している（図 1 参照)。暗号技術評価委員会は、CRYPTREC 暗号リスト（付録 A）に掲載されている暗号技術並びに電子政府システム等において利用される暗号技術について、安全性の維持及び信頼性の確保の観点から、その安全性及び実装に係る監視及び評価を行うなど、主として技術的な活動を担い、暗号技術検討会に対して助言を行う。また、暗号技術の安全な利用方法に関する調査や、新たな世代の暗号技術に関する調査も行う。

暗号技術調査ワーキンググループ（WG）は、暗号技術評価委員会の下に設置され、NICT 及び IPA が共同で運営している。暗号技術調査 WG は、暗号技術評価委員会の指示の下、暗号技術評価委員会の活動に必要な事項について調査・検討を行う作業グループである。暗号技術評価委員会の委員長は、実施する調査・検討項目に応じて適切な主査及び委員を選定し、調査・検討を指示する。主査は、その調査・検討結果を暗号技術評価委員会に報告する。2025 年度、暗号技術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)」において検討される。

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

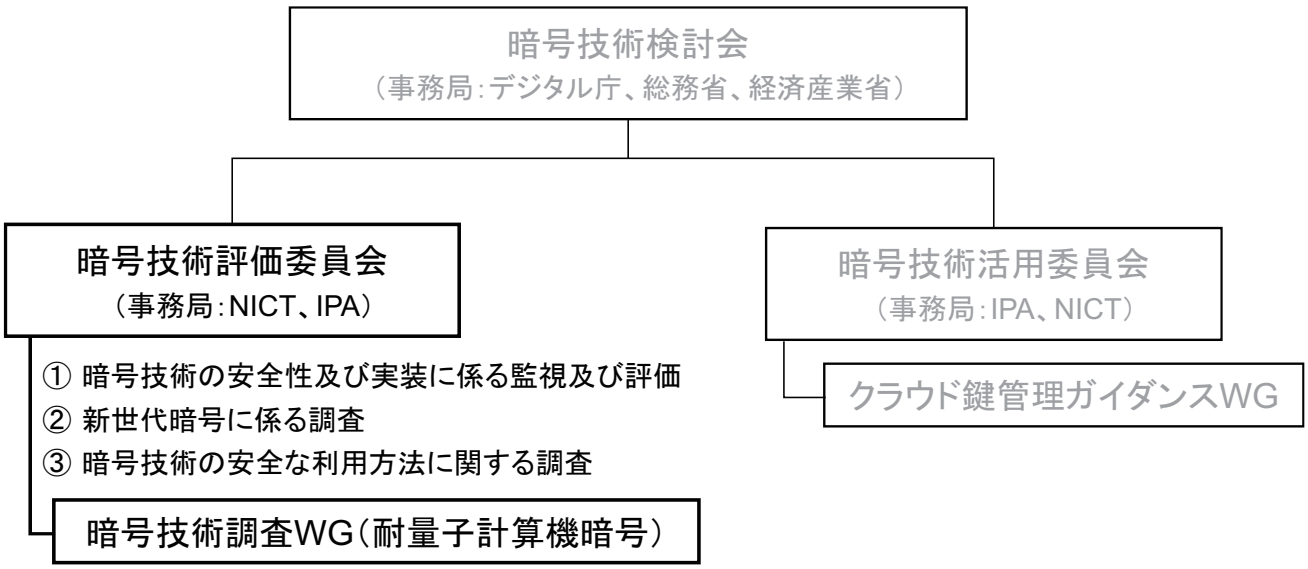

図 1: CRYPTREC 体制図

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	伊藤 忠彦	セコム株式会社 上級研究員
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	千田 浩司	群馬大学 准教授
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	山村 明弘	秋田大学 教授

暗号技術調査 WG（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 上級研究員
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

2025 年度暗号技術評価委員会／暗号技術調査 WG（耐量子計算機暗号）の参加者のみ

加茂 聡	内閣官房 国家サイバー統括室
櫻井 駿	内閣官房 国家サイバー統括室
杉本 貴之	内閣官房 国家サイバー統括室
吉村 康志	内閣官房 国家サイバー統括室
池田 晃輝	デジタル庁 デジタル社会共通機能グループ
北井上 礼樹	デジタル庁 デジタル社会共通機能グループ
山之上 隆広	デジタル庁 デジタル社会共通機能グループ
市川 宙樹	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
岩尾 和樹	総務省 自治行政局 住民制度課
大谷 綾乃	総務省 自治行政局 住民制度課
杉本 恵	総務省 自治行政局 住民制度課
牧村 昇陽	総務省 自治行政局 住民制度課
松尾 淳一	総務省 自治行政局 住民制度課
三橋 郁	総務省 自治行政局 住民制度課
梅城 崇師	総務省 サイバーセキュリティ統括官室
木村 悠生	総務省 サイバーセキュリティ統括官室
竹之内 玲	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
山口 航輝	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 情報通信課
水村 優斗	外務省 大臣官房 情報通信課
石坂 知樹	経済産業省 商務情報政策局 サイバーセキュリティ課
橋本 勝国	経済産業省 商務情報政策局 サイバーセキュリティ課
東 亨佳	経済産業省 商務情報政策局 サイバーセキュリティ課
緑川 美桜	経済産業省 商務情報政策局 サイバーセキュリティ課
吉田 楼蘭	防衛省 大臣官房
石丸 光宏	防衛省 整備計画局 サイバー整備課
椛木 隆慎	防衛省 整備計画局 サイバー整備課
河合 舜	防衛省 整備計画局 サイバー整備課
鈴木 直人	防衛省 整備計画局 サイバー整備課
石山 優貴	警察庁 長官官房 技術企画課
井上 智樹	警察大学校 警察情報通信研究センター
髙橋 知義	警察大学校 警察情報通信研究センター

事務局

NICT	井上 大介、青野 良範、伊藤 琢真、伊藤 竜馬、大久保 美也子、小川 一人、金森 祥子、木村 隼人、黒川 貴司、髙 和真、田村 千代、松井 充、吉田 真紀、笠井 祥、大川 晋司
IPA	高柳 大輔、神田 雅透、鷲見 拓哉、新保 淳、福岡 尊、白岩 裕子、川名 優香、渡邊 由香利

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を確保するためには、ネットワークセキュリティ、通信プロトコルの安全性、機器の物理的安全性、セキュリティポリシーの策定、個人認証システムにおける脆弱性の排除、さらに運用管理上の不備を悪用するソーシャルエンジニアリングへの対応など、幅広い観点から対策を講じる必要がある。その中でも、暗号技術は情報システム及び情報通信ネットワークを支える基盤技術であり、暗号技術の安全性が確立されなければ、十分な情報セキュリティ対策は成り立たない。現在、さまざまな暗号技術が開発され、それらを組み込んだ多くの製品やソフトウェアが市場に提供されている。これらの暗号技術を電子政府システム等で適切に利用するためには、その安全性について適正な評価が行われるとともに、評価に関する情報が容易に入手できることが極めて重要である。

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、同リストに掲載されている暗号技術の安全性及び実装に係る監視及び評価を行っている。また、実導入が進展している暗号技術についても、その安全性及び実装性能を調査し、CRYPTREC 暗号リストへの追加を視野にいれた評価活動を実施している。さらに、暗号技術の安全性に関する重要な指摘があった場合には、必要な注意喚起を行うため、CRYPTREC の Web サイトに注意喚起レポートを掲載してきた。

近年、暗号技術に対する解析・攻撃技術は日々高度化しており、今後も、CRYPTREC が発信する情報を踏まえつつ、関係機関が連携して、情報システム及び情報通信ネットワークの安全性向上に向けた取組みを進めることが極めて重要である。また、26 年にわたり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の収集・分析に支えられており、引き続き、暗号技術に関わる研究者をはじめとする多くの関係者の協力が不可欠である。

1.2　暗号技術評価委員会

電子政府システムで利用可能な暗号技術の評価・選択は、2000 年度から 2002 年度にかけて「暗号技術評価委員会」において実施された。その結果を踏まえ、総務省及び経済産業省により電子政府推奨暗号リストが策定された。一方、電子政府システムの安全性を確保するためには、同リストに掲載された暗号技術の安全性を継続的に把握するとともに、安全性を脅かす事態を的確に予見することが重要な課題となった。

このような認識の下、2003 年度には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。同委員会の目的は、電子政府推奨暗号の安全性を継続的に監視し、その安全性に問題がある疑いが生じ

た場合には、その緊急性に応じて必要な対応を行うとともに、暗号理論に関する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を技術面から支援を行うことにある。そこで、同委員会は、電子政府推奨暗号リスト改訂に向けた検討を進め、2008 年度には「電子政府推奨暗号リストの改訂に関する骨子（案）」及び「電子政府推奨暗号リスト改訂のための暗号技術公募要項（2009 年度）（案）」を策定した。さらに、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へ移行し、委員会名称を「暗号方式委員会」へ変更した。これに先立って実施され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、2010 年度からは応募のあった暗号技術等の安全性評価を開始し、2012 年度には「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）」 を策定した。

2013 年度からは、委員会名称を「暗号方式委員会」から再び「暗号技術評価委員会」に変更し、暗号技術の安全性に係る監視・評価に加え、実装に係る技術（暗号モジュールに対する攻撃及びその対策も含む）の監視・評価を実施することになった。詳細については、1.4 節を参照されたい。

暗号技術評価委員会の下には、暗号技術に関する具体的な検討を行うため、暗号技術調査 WG が設置されている。2013 年度から 2016 年度までは、暗号技術調査 WG（暗号解析評価）及び暗号技術調査 WG（軽量暗号）の 2 つの WG が設置された。2017 年度から 2020 年度までは、暗号技術調査 WG（暗号解析評価）が設置され、2021 年度から 2022 年度までは、暗号技術調査 WG（耐量子計算機暗号）及び暗号技術調査 WG（高機能暗号）の 2 つのワーキンググループが設置された。また、暗号技術調査 WG（耐量子計算機暗号）は、2021 年度から 2022 年度に続き、2023 年度から 2024 年度にかけて再び設置され、2025 年度には 3 回目として設置されている。

これらの活動成果として、暗号技術調査 WG（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）」を策定・公表した。その後、同ガイドラインを改定し、2023 年度には「CRYPTREC 暗号技術ガイドライン（軽量暗号）2023 年度版」 を策定・公表した。暗号技術調査 WG（耐量子計算機暗号）及び暗号技術調査 WG（高機能暗号）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）」を策定・公表した。2023 年度から設置された暗号技術調査 WG（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」を策定・公表した。なお、2025 年度から設置された暗号技術調査 WG（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）2026 年度版」を作成するために、PQC に関する最新動向を調査・把握するとともに、基本的な執筆方針を策定した。詳細については、第 3 章を参照されたい。

1.3 CRYPTREC 暗号リスト

2000 年度から 2002 年度まで実施された CRYPTREC プロジェクトの成果を踏まえ、暗号技術評価委員会において「電子政府推奨暗号リスト（案）」が作成された。同案は、2002 年度に暗号技術検討会に提出され、同検討会における審議並びに総務省及び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。その後、「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」に掲載された暗号技術の利用を推進するものとされた。なお、電子政府推奨暗号リストの技術的根拠については、「CRYPTREC Report 2002 暗号技術評価報告書（平成 14 年度版）[*1]」に詳しく記載されている。

2009 年度には、2008 年度に策定された「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。これを受けて、2010 年度から 2012 年度にか

[*1] https://www.cryptrec.go.jp/report/cryptrec-rp-2000-2002jp.pdf

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おいて評価が行われ、2012 年度には暗号技術検討会において電子政府推奨暗号リストが改定された。最終的には、総務省及び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、「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）」が決定された。選定方法及びその結果については、「CRYPTREC Report 2012（暗号方式委員会報告）[*2]」に記載されている。

2013 年度以降、2021 年度までの間には、CRYPTREC 暗号リストの小改定が行われ、複数の暗号技術が推奨候補暗号リストに追加された。具体的には、暗号技術評価委員会において、2016 年度にハッシュ関数 SHAKE128、2017 年度に認証暗号 ChaCha20-Poly1305、2019 年度に暗号利用モード（秘匿モード）XTS、2021 年度に公開鍵暗号（署名）EdDSA について、安全性評価及び実装性能評価を実施し、十分な安全性及び実装性能を有す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へ追加するよう暗号技術検討会に提案した。

2020 年度には、暗号技術検討会において、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、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）を維持することが決定された。これに合わせて、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む移行ルールが明確化された。

2022 年度には、暗号技術評価委員会においてメール審議（2023 年 1 月 30 日から 2 月 10 日まで）が行われ、CRYPTREC 暗号リスト改定に係る暗号技術については現状維持とすることが決定された。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（2023 年 3 月 9 日から 3 月 23 日まで）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）」を策定した。なお、2023 年度には暗号リストの改定は行われなかったが、一部の項目において注意書きが付された。

2024 年度に開催された暗号技術検討会では、PQC への対応について議論が行われた。その結果、CRYPTREC 暗号リストへの掲載に向けた PQC の技術的検討と、PQC への移行方針の検討を両輪として並行に進めていくべきであるとの認識が共有された。これを受けて、暗号技術評価委員会では、米国 NIST において標準化された PQC 方式である ML-KEM、ML-DSA 及び SLH-DSA について、安全性及び実装性能の評価を先行して実施することが決定された。

2025 年度には、暗号技術評価委員会において、公開鍵暗号（鍵共有）ML-KEM の安全性評価及び実装性能評価が実施され、同方式は十分な安全性及び実装性能を有すると判断し、この結果を暗号技術検討会に報告した。その後、暗号技術検討会において、耐量子計算機暗号（PQC）への対応を踏まえた CRYPTREC 暗号リストの在り方について議論が行われ、以下の 8 点が決定された。

1. 現行の CRYPTREC 暗号リストに PQC 対応のリストを追加すること。
2. 電子政府推奨暗号リストの中に PQC 対応のリストを追加すること。
3. 量子計算機耐性を持つ共通鍵暗号等についてもリスト（表）に追加すること。
4. 電子政府推奨暗号リストを現行暗号リスト（表 1）と PQC リスト（表 2）に区分すること。
5. PQC の各パラメーターセットについて、カテゴリとともにリストに掲載すること。
6. 引き続き議論が必要な課題については「耐量子計算機暗号（PQC）リスト検討タスクフォース（仮称）」を立ち上げ、検討を行うこと。
7. 電子政府推奨暗号リストの説明文や注釈について、必要な修正を行うこと。
8. CRYPTREC 暗号リスト・移行ルールについて、図 1.1 のとおり赤字部分を追加すること。

本決定を踏まえ、ML-KEM が電子政府推奨暗号リストの PQC リスト（表 2）に追加された（付録 A 参照）。

[*2] https://www.cryptrec.go.jp/report/cryptrec-rp-2000-2012.pdf

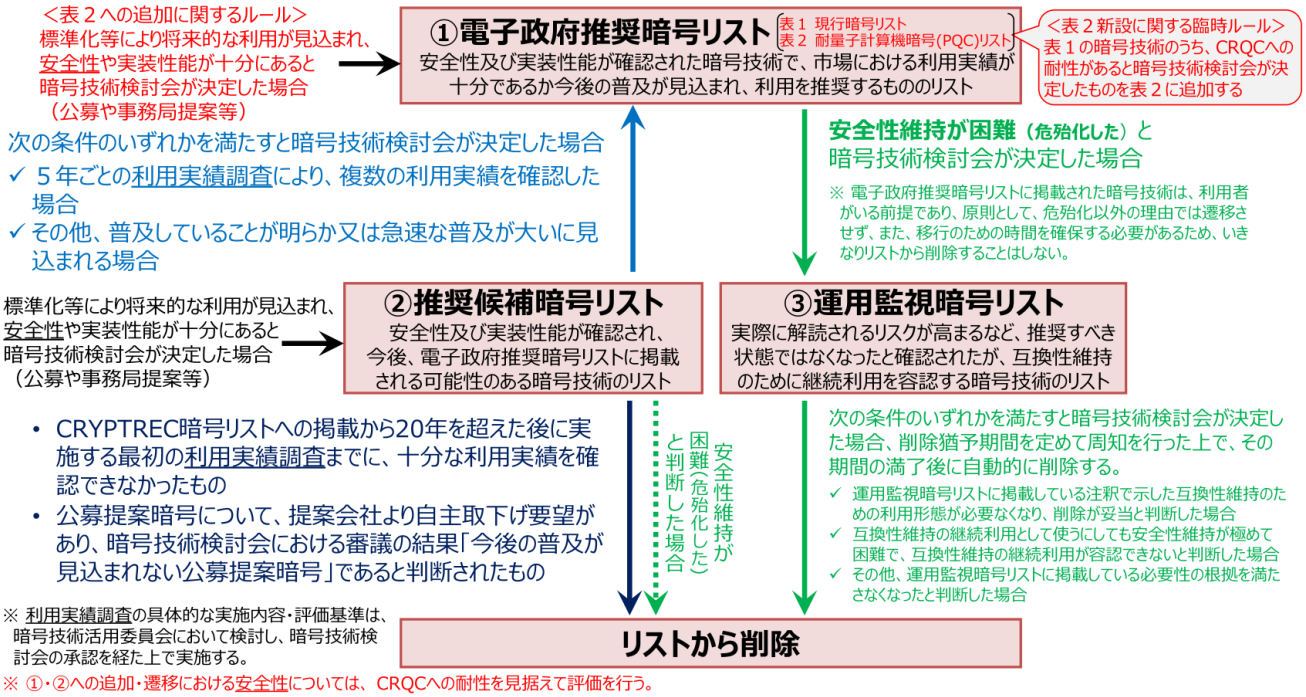

図 1.1: CRYPTREC 暗号リスト移行ルール

1.4 活動の方針

暗号技術評価委員会では、暗号技術の安全性評価を中心とする技術的な検討を行う。具体的には、以下の事項を実施する。

1) 暗号技術の安全性及び実装に係る監視及び評価
2) 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）

1) の内容をさらに細分化すると、以下の①～⑤に整理される。

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、会議やメーリングリストを通して報告する。

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に係る検討
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、⑤「新技術等に関する調査及び評価」に関して、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。

- 第 2 回暗号技術評価委員会以後、NICT の PQC 標準化において、第 4 ラウンドの評価フェーズを経て HQC が選定された。加えて、署名方式についても、NIST における評価フェーズが継続している。こうした状況に加え、2024 年度暗号技術調査 WG（耐量子計算機暗号）の委員から、2025 年度以降も同 WG を継続して設置すべきとの意見が示されていることを踏まえ、引き続き、暗号技術調査 WG（耐量子計算機暗号）を設置し、PQC に関する最新動向の把握を行う。
- PQC をめぐる社会的動向を踏まえ、NIST 標準として公表された FIPS 203、FIPS 204 及び FIPS 205 で規定される暗号技術（ML-KEM、ML-DSA 及び SLH-DSA）について、安全性評価及び実装性能評価に関する活動を開始する。
- 「素因数分解の困難性に関する計算量評価」及び「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、同 WG において検討を行い、必要な更新を実施する。

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に掲載された暗号技術に対する考え方を基本的に踏襲している。すなわち、暗号技術の安全性及び実装に係る監視及び評価は、次の 3 つの段階から構成される。

I) 情報収集
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し、暗号技術に関する情報を収集する。

II) 情報分析
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。

III) 審議及び決定
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。

なお、仕様書参照先の変更を検討する際にも、監視に関するこの基本的な考え方を参考としている。また、暗号技術の脆弱性に関する CRYPTREC からの情報発信については、下記のフロー（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おいて承認されている。

■情報発信フローの概要

（1）暗号技術の脆弱性情報を検知した場合には、まず、CRYPTREC において参照している仕様に対する攻撃が成功したことに関する情報であるか、または、攻撃成功には至っていないものの、攻撃に必要となる計算量の著しい低下につながる結果に関する情報であるかを判断する。その上で、当該情報が以下のいずれに属するかを分類する。

A) 暗号技術の完全な危殆化による緊急対応

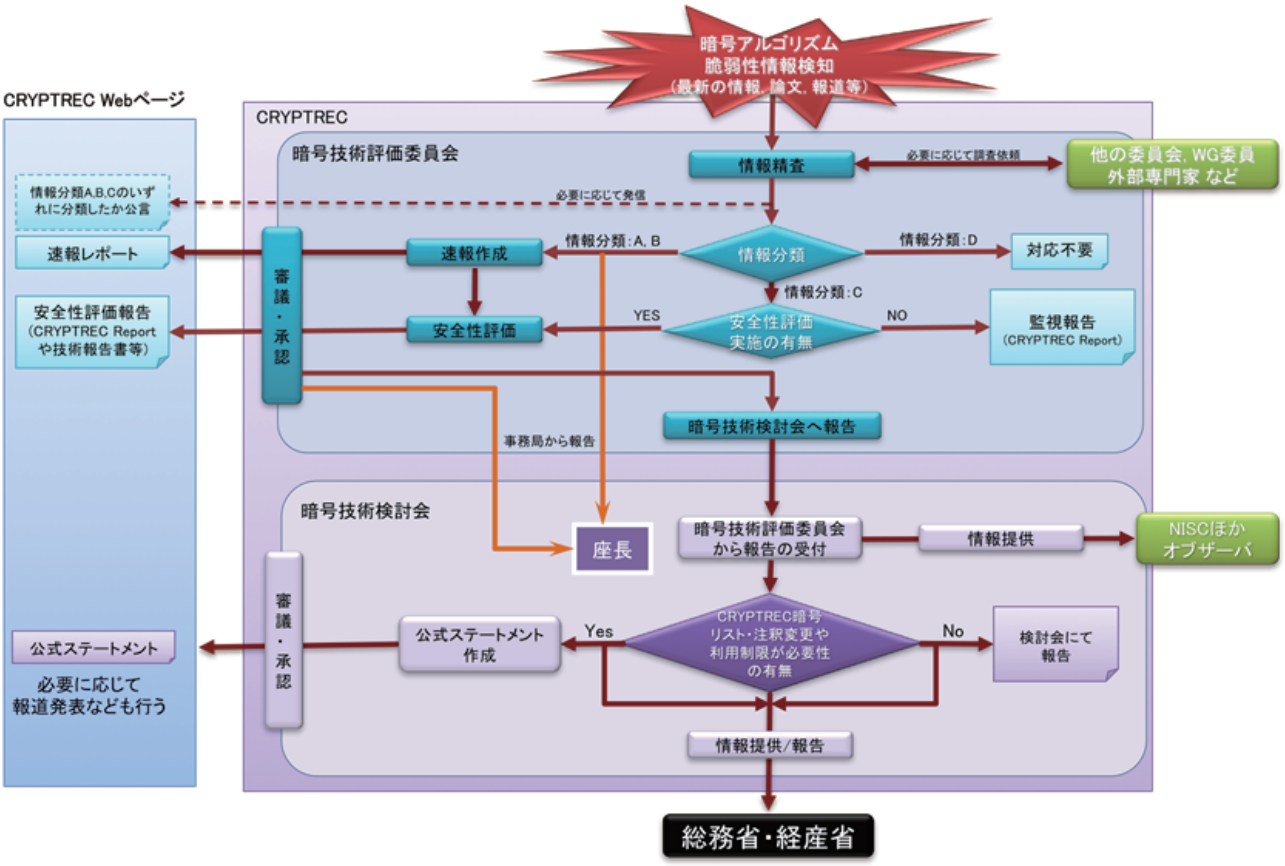

図 1.2: 暗号技術の脆弱性に関する情報発信フロー

B) 正確で信頼性の高い情報を発信による過剰反応の防止

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) または B) に分類される脆弱性情報については、速報を公開するとともに、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または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いて作成するものであり、CRYPTREC 自らが詳細な評価を行ったものではないが、信頼に足る機関または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をいう。

（3）取り扱う暗号技術の範囲は、CRYPTREC 暗号リストに掲載されている暗号技術、及び CRYPTREC 暗号リストには掲載されていないものの、暗号技術評価委員会において影響度が高いと認められた暗号技術とする。

（4）速報及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する。また、これらの脆弱性情報については、暗号技術評価委員会から暗号技術検討会に報告する。

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、2025 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 公開鍵暗号の安全性評価

RSA と ECDH に対する解析論文が Eurocrypt 2025 で報告された。本成果は Coppersmith 法の改良に基づいており、さまざまな暗号方式の安全性評価に影響を与える可能性がある。特に、ECDH 鍵共有では漏洩ビットを利用した共有鍵回復手法の適用可能範囲が拡大され、RSA では秘密指数が小さい場合の秘密鍵復元手法において、格子次元の削減および実行時間の短縮が示された。

RSA に関連する素因数分解問題の解析結果が Crypto 2025 で報告された。本報告では、Takagi 型 RSA 合成数 $N = pq^r, r \geq 1$ の素因数分解問題の困難性が、$\phi(N)$ の素因数から $\prod_i e_i > N^{1/4r}$ を満たす集合 $\{e_i\}$ を求める問題の困難性と等価であることが示された。ここで、ϕ は Euler のトーシェント関数である。さらに、$q \geq N^{\beta}$ の場合には、この範囲を $N^{1/4r}$ から $N^{\beta - r\beta^2}$ へと拡大できることが示された。

ECDSA の亜種に対する故障注入攻撃および実装安全性に関する解析結果が CHES 2025 で報告された。本発表では、ドイツ BSI で標準化されている ECGDSA および ECSDSA について、曲線パラメータや楕円曲線上の点に 1 ビットの故障を注入した場合、署名偽造に繋がる可能性があることが示された。一方で、ECDSA および EdDSA については、本攻撃に対する耐性を有することが確認された。

これらの解析論文に関する詳細については、第 2.4.1 節を参照されたい。

2.1.2 共通鍵暗号の安全性評価

AES に対する解析論文が Crypto 2025、CHES 2025、Asiacrypt 2025 で報告された。Crypto 2025 で報告された解析論文では、Guess-and-Determine リバウンド攻撃に基づく AES-128 の安全性解析結果が報告された。本手法により、2 ラウンド AES-128 の鍵衝突探索に必要な試行回数を 2^{49} から 2^{6} に削減できることを示すとともに、3 ラウンド AES-128 についても 2^{35} 回の試行で鍵衝突可能であることが確認された。CHES 2025 で報告された解析論文では、AES-NI 実装を対象とした Opcode-based Fault Attack が提案された。本手法では、1 組の正誤暗号文を用いることで、AES-128 の鍵候補空間を 2^{32} まで縮小できることが示され、実機実験においても約 1 時間で鍵候補の特定が可能

であることが報告された。Asiacrypt 2025 で報告された解析論文では、AES ベースのハッシュ構成および AES の簡略ラウンド版に対する衝突解析の結果が報告された。具体的には、7 ラウンド AES-MMO/MP に対する 1 ブロック衝突、および 4 ラウンド AES-128-DM に対する 1 ブロック衝突が、計算量 2^{60}、メモリ量 2^{60} で実行可能であることが示された。また、単一既知平文条件下での鍵回復攻撃に関して、AES-128 では 5 ラウンド、AES-192 では 7 ラウンド、AES-256 では 8 ラウンドまでの解析結果が示された。これらの計算量はいずれも 2^{120} であり、メモリ量は AES-128 で 2^{40}、AES-192 および AES-256 で 2^{72} と報告されている。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。

ChaCha に対する解析論文が FSE 2025、Eurocrypt 2025、Asiacrypt 2025 で報告された。FSE 2025 で報告された解析論文では、ChaCha の簡略ラウンド版に対する鍵回復攻撃の改善が報告された。本成果では、既存手法と比較して、7 ラウンド ChaCha に対する計算量およびメモリ量が $(2^{206.8}, 2^{110.81})$ から $(2^{189.7}, 2^{102.63})$ に改善された。また、7.25 ラウンド ChaCha についても、計算量およびメモリ量が $(2^{238.34}, 2^{122.34})$ から $(2^{223.9}, 2^{100.8})$ に改善された。Eurocrypt 2025 で報告された解析論文では、これらの結果を上回る解析結果が報告された。特に、7 ラウンド ChaCha に対して、メモリ量は $2^{102.63}$ から $2^{127.7}$ に増加するものの、計算量を $2^{189.7}$ から $2^{148.2}$ に削減する手法が示された。また、メモリ量の増加を $2^{102.63}$ から $2^{102.9}$ に抑えつつ、計算量を $2^{189.7}$ から $2^{154.2}$ に削減する手法も提案された。さらに、6 ラウンド ChaCha および 7.5 ラウンド ChaCha に対する鍵回復攻撃についても報告されている。6 ラウンド ChaCha については計算量を $2^{71.0}$ から $2^{57.4}$ に、7.5 ラウンド ChaCha については計算量を $2^{255.2}$ から $2^{250.2}$ に、それぞれ改善された。Asiacrypt 2025 で報告された解析論文では、7.5 ラウンド ChaCha に対する鍵回復攻撃の計算量をさらに削減する手法が提案され、結果として計算量が $2^{250.2}$ から $2^{243.6}$ に改善された。なお、ChaCha の仕様段数は 20 ラウンドである。

これらの解析論文に関する詳細については、第 2.4.2 節を参照されたい。

2.1.3 ハッシュ関数の安全性評価

SHA-512 に対する解析論文が Crypto 2025 で報告された。本論文では、新たに発見された局所衝突と 2 ビット条件を考慮した解析により、29 ステップ SHA-512 に対する実用的な衝突攻撃が示された。また、31 ステップ SHA-512 に対する理論的な衝突攻撃が、従来の $2^{97.3}$ から $2^{85.5}$ へと削減された。なお、SHA-512 の仕様段数は 80 ステップである。

SHA-3 および Keccak に対する解析論文が FSE 2025 と Eurocrypt 2025 で報告された。FSE 2025 で報告された解析論文では、3 ラウンド Keccak-256 に対する原像攻撃のための計算量を $2^{73.79}$ から $2^{57.2}$ へ、4 ラウンド Keccak$[r = 640, c = 160]$ に対する原像攻撃のための計算量を $2^{65.4}$ から $2^{60.9}$ へと、それぞれ削減している。Eurocrypt 2025 で報告された解析論文では、5 ラウンド SHA-3 に対する初めての原像攻撃が報告された。攻撃対象として報告された 5 ラウンドインスタンスは、SHA3-224、SHA3-256、SHAKE128、SHAKE256 の 4 種類である。さらに、同論文では、SHA3-224、SHA3-256、SHA3-384、SHAKE128、SHAKE256 の 5 種類の 4 ラウンドインスタンスについても計算量の削減が報告されており、改善幅はそれぞれ $2^{56.5}$、$2^{66.5}$、$2^{96.2}$、$2^{24.5}$、$2^{87.5}$ 倍である。なお、SHA3 の仕様段数は 24 ラウンドである。

RIPEMD-160 に対する解析論文が Asiacrypt 2025 で報告された。本論文では、自動探索モデルとメッセージ修正手法を改良することにより、44 ステップ RIPEMD-160 に対する初めてのセミフリースタート衝突攻撃を、計算量 $2^{76.9}$ で実行可能であることが示された。さらに、41 ステップ、42 ステップ、43 ステップ版に対する計算量の改善も報告されており、それぞれ $2^{49.8}$、$2^{53.9}$、$2^{76.9}$ である。なお、RIPEMD-160 の仕様段数は 80 ステップである。

これらの解析論文に関する詳細については、第 2.4.3 節を参照されたい。

2.2 注意喚起レポートについて

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

2.3 仕様書の参照先の変更について

CRYPTREC の Web サイトでは、CRYPTREC 暗号リストに掲載されている各暗号技術について、仕様書の参照先を公開している（https://www.cryptrec.go.jp/method.html）。今年度は、電子政府推奨暗号リストに掲載されている公開鍵暗号（鍵共有）ECDH について、仕様書の参照先の変更内容を確認した。その結果、新旧仕様書間でアルゴリズム部分に変更がないことを確認した。この結果を踏まえ、暗号技術評価委員会における承認を経て、当該仕様書の参照先を変更した。変更の詳細は、表 2.1 のとおりである。

表 2.1: 仕様参照先の変更

暗号技術名	ECDH
旧仕様書 参照先	SEC 1: Elliptic Curve Cryptography (September 20, 2000 Version 1.0) https://www.secg.org/SEC1-Ver-1.0.pdf または NIST SP 800-56A Revision 2 (May 2013) において、C(2e, 0s, ECC CDH) として規定されたもの https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar2.pdf
新仕様書 参照先	SEC 1: Elliptic Curve Cryptography (September 20, 2000 Version 1.0) https://www.secg.org/SEC1-Ver-1.0.pdf または NIST SP 800-56A Revision 3 (April 2018) において、C(2e, 0s, ECC CDH) として規定されたもの (*4) https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar3.pdf

(*4) 使用するメッセージ認証コードは HMAC または AES-CMAC に限る。

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 E 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
FDTC 2024	Fault Diagnosis and Tolerance in Cryptography	カナダ・ハリファックス	2024 年 9 月 4 日
CHES 2024	Conference on Cryptographic Hardware and Embedded Systems	カナダ・ハリファックス	2024 年 9 月 4–7 日
FSE 2025	Fast Software Encryption Conference	イタリア・ローマ	2025 年 3 月 17–21 日
PQCrypto 2025	International Conference on Post-Quantum Cryptography	台湾・台北	2025 年 4 月 8–10 日
Eurocrypt 2025	International Conference on the Theory and Applications of Cryptographic Techniques	スペイン・マドリッド	2025 年 5 月 4–8 日
PKC 2025	International Conference on Practice and Theory in Public Key Cryptography	ノルウェー・レーロース	2025 年 5 月 12–15 日
Crypto 2025	Annual International Cryptology Conference	アメリカ・サンタバーバラ	2025 年 8 月 17–21 日
FDTC 2025	Fault Diagnosis and Tolerance in Cryptography	マレーシア・クアラルンプール	2025 年 9 月 14 日
CHES 2025	Conference on Cryptographic Hardware and Embedded Systems	マレーシア・クアラルンプール	2025 年 9 月 14–18 日
TCC 2025	Theory of Cryptography Conference	デンマーク・オーフス	2025 年 12 月 1–5 日
Asiacrypt 2025	International Conference on the Theory and Application of Cryptology and Information Security	オーストラリア・メルボルン	2025 年 12 月 8–12 日

2.4.1 公開鍵暗号の安全性評価技術

Solving Multivariate Coppersmith Problems with Known Moduli

Keegan Ryan

Eurocrypt 2025

RSA 暗号解析や楕円曲線 Diffie-Hellman（ECDH）鍵共有の解析で用いられる、Coppersmith 法の改良に関する論文である。

本論文で取り上げられている Coppersmith 法は 90 年代より、代数的な構造を持つ暗号方式の公開情報と秘密情報が満たす関係を多変数方程式 $f_k(x_1, x_2, \ldots) \equiv 0 \pmod{N},\ j = 1, \ldots, k$ として記述し、x_i の範囲が制限される場合に多項式時間で秘密情報の復元を行うヒューリスティックアルゴリズムを与えるフレームワークである。代表的な応用として、RSA 暗号において秘密鍵の上位ビットが 0 であるなど極端なパラメータでの運用が行われる場合、部分情報

の漏洩がある場合の鍵復元攻撃、楕円曲線、同種写像ベースの鍵共有方式における部分情報からの鍵復元攻撃などが知られている。

一般的な方針として、次数 k を固定した後に与えられた方程式の積、線形結合などからシフト多項式と呼ばれる $f_j \equiv 0 \pmod N$ for $j = 1, \ldots, J \Rightarrow g \equiv 0 \pmod{N^k}$ を満たす多項式 g の集合とそれを基底とする格子を考え、格子基底簡約等を用いてシフト多項式の線形結合の中から係数の小さい多項式 g を選ぶ。変数の絶対値が小さい範囲においては $g \equiv 0 \pmod{N^k} \rightleftarrows g \equiv 0$ が成り立ち、$\mathbb{Z}$ 上の方程式を数値解法などの手法で解くことで元の方程式の解の候補を絞る。このとき、多項式 g の集合の選択により構成される格子の体積と次元が変化し、発見されるベクトルのノルムの理論的な上限が変化する。解の範囲を広げるため、できるかぎりノルムの上限を小さくするシフト多項式を選ぶ必要がある。この選択は方程式の形に合わせたヒューリスティックな職人芸であり、長年自動化の研究が続けられてきたものの最適な集合を得ることは難しく、同じ方程式に対する微小な改良が重ねられてきた。

実際の Coppersmith 法の計算においては、シフト多項式を選択する際の次数 k が大きくなるにつれて格子の次元が増大し、格子基底簡約を実時間で計算することが困難になるため、k を無限大とした漸近的な攻撃可能上界の他に有限の k に対する効率の良いシフト多項式の選択が課題となる。本論文では、グレブナー基底計算アルゴリズムを用いることで、最適なシフト多項式の集合を自動的に選択する手法を提案する。構成される格子の中に有用な短いベクトルが含まれることが証明可能であるものの、この集合は大きく実際の計算では効率が悪い。次に、多項式の中の係数に対応する有向グラフに対する最大重み閉包を持つ頂点集合の計算アルゴリズムを用いて多項式集合の次元削減を行い最適化する。この多項式集合はシンボリックな数式処理により事前計算可能であり、ノルム上界の評価の他、計算時間が多項式で押さえられることも示される。

著者は提案手法を 13 件の暗号解読に関わる多変数方程式の問題に適用し、多項式時間で求解が可能な範囲を調査した。これらの問題には RSA 暗号や ECDH 鍵共有の解読に関わるものが含まれる。詳細な報告は Appendix としてまとまっている。特に ECDH および RSA 暗号解読については、多項式時間で解読可能な範囲に関して以下の改善が得られたと報告された。なお、特に注意書きの無い場合には k を無限大とした漸近的な範囲の上界であり、実験で用いられた小さな k での解読範囲とは異なることに注意。

1. “Elliptic Curve Hidden Number Problem”：ECDH 鍵交換において、最上位ビットを返すオラクル（部分情報の漏洩に関する安全性の議論に用いられる）を用いて、共有秘密鍵を復元する攻撃。多項式時間で攻撃可能な秘密鍵の最大値を X とすると、サンプル数 3 の場合先行研究では漸近的に $\log_p X < 0.2083$ であったものが $\log_p X < 0.3090$ に拡張されている。
2. “Stereotyped RSA”：$e = 3$ の教科書的 RSA において、パディング等の要素により平文の上位ビットの約 2/3 が攻撃者に明らかになっている状況での平文復元攻撃を扱う。平文の下位ビットを未知数 x として扱う。多項式時間で攻撃可能な下位ビットの範囲の漸近的な値 $X \approx N^{1/3}$ は先行研究と同等であるものの、有限の k に対して用いられる格子の次元と計算時間を削減している。
3. “RSA factoring with high bits known”：RSA 秘密鍵を構成する素数 p の上位ビットが漏洩している条件の下で、N の素因数分解を復元する設定を扱う。p の下位ビットを未知数 x とおいたときの多項式時間での素因数分解が可能な範囲の漸近値は先行研究と同様であるが、有限の k に対しては構成される格子の次元と計算時間を削減している。
4. “RSA with Small Private Exponent”：教科書的な RSA の秘密指数 d が小さい場合に、公開鍵 (N, e) から d を復元する攻撃を扱う。多項式時間で攻撃可能範囲は δ をパラメータとして $d < N^\delta$ の形で表現される。先行研究における漸近的な攻撃可能範囲 $\delta = 1 - 1/\sqrt{2} \approx 0.2928$ に近い $\delta = 0.2925$ を達成するため、シフト多項式の次数を $k = 9$ として格子を構成する。先行研究では 746 次元の格子が必要だったものを 42 次元まで削減し、

1000 ビット RSA の解読実験において格子基底簡約の実行時間を 5418 秒から 13 秒に短縮した。

5. “CRT-RSA with Small Exponents”：CRT-RSA の秘密指数 d_p, d_q が小さい場合に、公開鍵 (N, e) から秘密指数 d_p, d_q を復元する攻撃を取り扱う。多項式時間での攻撃可能範囲は δ をパラメータとして $d_p < N^{\delta}$ の形で表現される。先行研究における漸近的な攻撃可能範囲 $\delta = 1/2 - 1/\sqrt{7} \approx 0.1220$ に対して、本研究のアルゴリズムが与える漸近値は 0.0486 とかなり小さい。$k = 8$ に対する構成では先行研究の格子次元が 177 であったのに対して 89 に削減している。
6. “Partial Key Exposure attacks on CRT-RSA”：CRT-RSA における秘密指数 d_p, d_q それぞれの下位ビットが漏洩している場合の全体の復元を扱う。先行研究と同等の格子の構成と解読性能が得られている。

以上にまとめた以外にも、RSA 写像を用いた疑似乱数生成器に対する格子の次元削減、$N = p^r q$ 型の合成数を用いた multi-power RSA に対する先行研究との比較、同種写像ベースの鍵交換方式 CSIDH の解析、“Modular Inversion Hidden Number Problem” の計算可能範囲の拡張などが報告されている。提案手法は先行研究と同様にいくつかのヒューリスティックに基づくが、記述・実装・実行が容易であることを特徴としており、Coppersmith 法を多変数多項式系に適用する際の複雑さを低減する可能性があると報告している。

New Results on the ϕ-Hiding Assumption and Factoring Related RSA Moduli

Jun Xu, Jun Song, Lei Hu

Crypto 2025

素因数分解問題に関する論文である。ϕ-hiding assumption とは、合成数 N に対して、オイラー関数の値 $\phi(N)$ の素因数 e の発見が困難であるという仮定であり、2000 年代から PIR、Lossy trapdoor 等の構成に用いられてきた。この仮定の困難性に関しては、[Blömer-May, Eurocrypt 2005] が 1 変数の Coppersmith 法を用いることで $e > N^{1/4}$ を満たす $\phi(N)$ の因子を発見する問題と N の素因数分解との等価性を示しており、以降 N の形と e の範囲に関して計算量的等価性の探究が続けられてきた。

本論文では、Takagi's RSA 型の合成数 $N = pq^r, r \geq 1$ に対して、$e > N^{1/4r}$ を満たす $\phi(N)$ の素因数を発見する計算問題の困難性が N の素因数分解と等価であることを示し、次に $q > N^{\beta}$ であることが知られている場合には e の範囲が $e > N^{\beta - r\beta^2}$ へと拡張可能なことを証明している。応用として、素数 $e > N^{1/4r}$ が与えられたときに $\phi(N)$ が e で割り切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る。続けて、著者らは e が $O(\mathrm{loglog}N)$ 個の因子の集合 $\{e_i\}$ からなる合成数である場合にも動作するようにアルゴリズムを拡張している。特に重要な帰結として、$N = pq$ 型の合成数に対して従来は $e > N^{1/4}$ を満たす素数を発見することで N の素因数分解を可能としていたが、$\phi(N)$ の小さな素因数を集めることで積が $N^{1/4}$ よりも大きくなれば、積の情報から素因数分解へと繋がることになる。

最後の結果は [Kakvi et al., Asiacrypt 2012] らにより議論された、関数 $\mathrm{RSA}_{N,e}(x) := x^e \mod N$ が置換写像であるかどうかの検査に関する懸念事項を現実のものとして明らかにしている。$\mathrm{RSA}_{N,e}$ 関数の核はオイラーの定理から $\gcd(e, \phi(N))$ 個存在するため、この値が大きいと写像の重複度が上がり安全性に影響する。Kakvi らの論文では、$e_i < N^{1/4}$ を満たす $\phi(N)$ の素因数 e_i が存在すれば写像が少なくとも e_i-to-1 写像であり、セキュリティ上の不安があるという指摘のみであったが、本論文ではこれを実際に素因数分解が可能であるという実際の計算にまで推し進めている。

著者らはこの解析をさらに応用し、Semi-Smooth RSA subgroup moduli（SS-moduli）と呼ばれる特別な合成数の素因数分解の解析などに応用した。SS-moduli は [Groth, TCC 2005] による署名構成に用いられた特殊な形をした p, q による合成数 $N = pq$ であり、[Naccache-Stern, CCS 1998] や [Yamakawa-Yamada-Hanaoka-Kunihiro, Crypto

2016] らにより大きな合成数 $e|\phi(N)$ の発見と素因数分解問題の関係の探求が進められてきた。

1 変数の Coppersmith 法を用いた解析では範囲が $e > N^{1/2}$ となるが厳密な証明が与えられており、2 変数の Coppersmith 法を用いることで範囲が $e > N^{1/4}$ へと拡張できることが知られていたものの解析にヒューリスティックが含まれており厳密な証明ではなかった。本論文では、$e > N^{1/4}$ に対して厳密な証明が与えられるアルゴリズムが示されている。

アルゴリズムの検証コードは `https://github.com/TearsJin/659A70AF5035D498` にて公開されている。

Fault Attacks on ECC Signature Verification

Kevin Schneider, Lukas Auer, Alexander Wagner

CHES 2025

ECDSA の変種である Elliptic Curve German Digital Signature Algorithm（ECGDSA）および Elliptic Curve Schnorr Digital Signature Algorithm（ECSDSA）に対する故障攻撃に関する論文である。ECGDSA はドイツ情報セキュリティ庁（BSI）にて標準化されたもの、ECSDSA は BSI のガイドライン BSI TR-03111 で策定されたものを解析の対象としている。

楕円曲線を用いた署名方式へのサイドチャネル攻撃は従来、署名生成時の秘密鍵や一時乱数の漏洩を狙うものが主であった。一方で、本論文は署名検証処理への故障注入攻撃を扱っている。特に、セキュアブートやファームウェアのアップデートの文脈で、攻撃者が不正な文書（ファームウェアのイメージファイル）と署名を自由に操作可能な状況において、署名検証実行中のハードウェアへの故障注入による署名の誤受理を目的とした攻撃について考察する。

署名方式 ECGDSA への攻撃では短 Weierstrass 標準形で表現された楕円曲線 $E : y^2 = x^3 + ax + b$ 上の公開鍵点 $P = (x, y)$ への 1 ビット故障注入を行い、別の点 $P = (x', y')$ とする。これは元の曲線上の点ではないが、a は共通している別の $E' : y^2 = x^3 + ax + b'$ 上の点と考えることができる。ECGDSA の実装が高速化のため Weierstrass 曲線の不完全加算公式を用いている場合、公式に b が現れないことから上記 b から b' への変化は検出されず、曲線 E' 上の演算として処理される。このとき、新たな曲線 E' の位数が smooth であれば P' に関する ECDLP を効率的に計算可能であり、そこから任意の文書に対する偽造署名を作る攻撃が可能となる。

ECSDSA への攻撃でも同様に、暗号パラメータである楕円曲線群の生成元 G に対して故障注入を行うことで別の曲線上の演算として処理をさせ、偽造署名が生成可能であることが示される。ただしこの攻撃は署名検証アルゴリズムで計算される点 Q の x 座標のみが文書と結合されてハッシュ関数に入力される形でのチェックが行われるという ECSDSA の仕様を利用するものであり、他の Schnorr 型署名で採用されているような、x, y 座標が両方ともハッシュ関数の入力となる仕様では攻撃が成り立たないと報告されている。

上記 2 つの攻撃はいずれも、故障注入後の P' もしくは G' を用いた署名検証演算が別の smooth な楕円曲線上の演算として解釈できるという性質を用いていた。しかしながら ECDSA と EdDSA ではそのような解釈ができずに、1 ビットの反転が演算が進むにつれてランダムなエラーとして伝播し、群の構造そのものが消失すると報告されている。

論文では続けて、ECDSA と EdDSA を対象として、セキュアブートローダーに組み込まれている署名検証ルーチンに対する故障注入攻撃の実証実験を行っている。オープンソースのセキュアブートローダー MCUboot に組み込まれている Mbed TLS v3.5.2（ECDSA）および wolfBoot に組み込まれている wolfSSL v5.7.0（EdDSA、Ed25519）の署名検証ルーチンをターゲットとしている。実験ではデバッガを用いて命令スキップ、分岐スキップ、big integer 構造体の limb 数の破壊、演算結果を 0 や入力値に置き換える故障などを注入するシミュレーションを行い、実際に無効な署名が受理されるかどうかを検証した。

攻撃の詳細と必要なリソースは論文 Table 3 にまとめられている。楕円曲線の性質を用いず、最終判定の結果が

reject であるものを valid に書き換える攻撃の他に楕円曲線の性質を用いた 4 種類（ECDSA と EdDSA の合計 8 種類）の攻撃実験が行われている。これらのうち、ECDSA の u_1, u_2 の計算に関する 2 種類の攻撃、および EdDSA の点加算に対する攻撃は理論上は可能であるが実装上の対応を見つけることが出来なかったため可能性に留まるが、残りの 5 種類は成功している。

本体の署名生成が保護されていたとしても検証ルーチンが未保護であれば故障注入によりセキュアブートを回避可能であると論文は報告している。

2.4.2 共通鍵暗号の安全性評価技術

Differential-Linear Cryptanalysis of Reduced Round ChaCha

Zhichao Xu, Hong Xu, Lin Tan, Wenfeng Qi

FSE 2025

軽量ストリーム暗号 ChaCha に対する安全性評価について報告したものである。Salsa20 に対する暗号解析と同様に、2008 年に Aumasson らによって提案された Probabilistic Neutral Bits（PNB）手法に基づく暗号解析を基盤としている。本研究の目的は、ラウンド関数を簡略化した ChaCha に対する差分線形攻撃の効率を向上させることである。以下の 2 点が課題として挙げられている。1 つ目は、攻撃に用いる差分線形識別子の精度向上である。既存の 4 ラウンド識別子に対する相関値を高めることで、攻撃成功確率の向上が期待される。2 つ目は、鍵回復攻撃の効率化である。PNB 手法におけるバックワード相関（backward correlation）の精度を改善することで、必要な計算量の削減を図る。

これらの課題に取り組むことで、7 ラウンドおよび 7.25 ラウンド ChaCha に対する鍵回復攻撃の性能を向上させることに成功した。具体的には、differential-linear hull effect を考慮することで、FSE 2023 で報告された識別子の相関値を $2^{-34.15}$ から $2^{-32.2}$ へと向上させた。また、PNB 評価に置いて、PNB に割り当てる値を $1000\ldots000$ に変更するとともに、使用する閾値を 1 つから 2 つに拡張することで、より精密なバックワード相関値の取得を実現した。結果として、7 ラウンド ChaCha のバックワード相関値は $2^{-14.18}$ から $2^{-11.855}$ へと改善され、PNB の数も 160 から 169 へと増加したことで、鍵回復に要する計算量は $2^{189.7}$ にまで削減された。一方、7.25 ラウンド ChaCha においてもバックワード相関値が $2^{-6.85}$ から $2^{-11.25}$ に向上し、その結果として鍵回復の計算量が $2^{223.9}$ にまで改善された。さらに、7.25 ラウンド ChaCha と $7.5^{\oplus}$ ラウンド ChaCha が本質的に等価であることを示した。両者の違いは、最終ラウンドにおいて 4 つの算術加算が追加されているかどうかに限られる。加算は可換演算であるため、順序を変更しても暗号強度に影響を及ぼさない。この性質を活用することで、$7.5^{\oplus}$ ラウンド ChaCha に対する攻撃も、7.25 ラウンド ChaCha に対する攻撃と同等の計算量・メモリ量で実行可能であることを明らかにした。

Improved Cryptanalysis of ChaCha: Beating PNBs with Bit Puncturing

Antonio Flórez-Gutiérrez, Yosuke Todo

Eurocrypt 2025

軽量ストリーム暗号 ChaCha に対する安全性評価について報告したものである。ChaCha に対する安全性評価においては、2008 年に Aumasson らによって提案された Probabilistic Neutral Bits（PNBs）の概念に基づく鍵回復攻撃が主流であり、これまでの多くの研究でこの手法が採用されてきた。しかしながら、従来の PNBs を用いた攻撃は、ChaCha のような ARX（Addition-Rotation-XOR）構造の複雑さに対しては一定の効果を示す一方で、実験的手法に依存しており理論的な裏付けに欠けている。また、7 ラウンド以上の ChaCha に対する実用的な攻撃手法はこれまで十分に確立されていないという課題がある。

本研究では、PNBs に代わる理論的手法に基づいた鍵回復攻撃手法を開発し、より多くのラウンドを有する ChaCha に対して効率的な攻撃を可能にすることを目的とする。この目的のために、Eurocrypt 2024 で提案された Walsh Spectrum Puncturing（特に、Bit Puncturing）と呼ばれる技術を ChaCha に対する安全性評価に応用する。この手法は、ある関数の Walsh スペクトラムに注目し、一部のスペクトラム成分を無視（Puncture）することで、相関値の高い近似関数を構築するものである。また、Walsh スペクトラムは高次元となるため、一般的にその全体を計算することは困難である。この問題を解決するために、トレイル列挙（trail enumeration）と呼ばれる技術を導入することで、一部のスペクトラム成分を現実的な計算時間で近似的に求めることを可能とした。

提案手法を 6 ラウンド、7 ラウンド、7.5 ラウンドの ChaCha に適用し、いずれの場合においても既存の攻撃手法を大きく上回る結果が得られた。特に、7 ラウンド ChaCha に対しては、攻撃に必要な時間計算量を既存手法よりも 2^{40} 以上削減し、結果として $2^{148.2}$ の時間計算量で鍵回復攻撃が可能であることを示した。また、7.5 ラウンド ChaCha に対する従来の攻撃手法では、秘密鍵に対する全数探索よりもわずかに効率が良い程度であったが、提案手法により $2^{250.2}$ の時間計算量で鍵回復攻撃が可能であることを確認した。なお、ChaCha のラウンド数は 20 であるため、提案手法が ChaCha の安全性に影響を及ぼすことはない。

Guess-and-Determine Rebound: Applications to Key Collisions on AES

Lingyue Qin, Wenquan Bi, Xiaoyang Dong

Crypto 2025

ブロック暗号 AES に対するリバウンド攻撃を用いた安全性評価に関する研究である。リバウンド攻撃にはいくつかの技術的課題が残されており、本研究では次の 2 点に着目する。第一に、Crypto 2022 で Dong らが提案した triangulating リバウンド攻撃を、AES のように高度に結合した非線形層を有する暗号に適用する場合。方程式間の依存性が高く、個々の変数を独立に解くことが困難となる。その結果、効率的な triangulation が成立せず、最終的に全数探索に近い計算量を要してしまう。第二に、鍵衝突攻撃では、データ処理部のみならずキースケジュール部にも差分を導入する必要がある。しかし、従来のリバウンド攻撃は単一鍵差分を前提としており、関連鍵差分を扱うことができなかった。そのため、データ処理部とキースケジュール部の間で差分トレイルに矛盾が生じやすいという問題があった。

これらの課題を解決するために、本研究では Guess-and-Determine リバウンド攻撃を提案した。この手法は、従来の triangulation に代わり、方程式系の一部を推定（guess）し、整合する変数を逐次的に決定（determine）することで解析を進めるものである。非線形方程式群をガウス消去法などの線形代数的手法と組み合わせて処理することにより、インバウンド領域を柔軟に拡張できる構造を実現した。さらに、リバウンド攻撃を関連鍵差分に対応させるための条件を導入することで、データ処理部とキースケジュール部との間で差分の不整合が生じず、確率計算も重複なく取り扱うことが可能となった。

提案手法により、従来では理論的な攻撃に留まっていた AES に対する鍵衝突攻撃を、現実的な時間内で実行可能なレベルまで効率化することに成功した。具体的には、2 ラウンド AES-128 に対して、従来必要とされていた 2^{49} 回の試行を 2^{6} 回まで削減し、実際に数秒以内で衝突を発見できることを確認した。また、これまで不可能と考えられていた 3 ラウンド AES-128 に対しても、2^{35} 回の試行という、実用的な計算量で攻撃を実現した。さらに、5 ラウンド AES-192 と 6 ラウンド AES-256 に対しても、理論上の計算量を 2^{61} から 2^{21} まで削減し、数分以内で衝突例を生成することに成功している。

Triangulating Meet-in-the-Middle Attack

Boxin Zhao, Qingliang Hou, Lingyue Qin, Xiaoyang Dong

Crypto 2025

NIST PQC 標準化プロジェクトにおける追加署名方式の第 2 ラウンド候補である FAEST では、AES の秘密鍵を署名鍵として用い、その秘密鍵によって生成された平文 – 暗号文ペアが検証鍵として設定される。具体的には、AES-128 を使用する場合には 1 組の平文暗号文ペアが、AES-192 または AES-256 を使用する場合には 2 組の平文暗号文ペアが検証鍵となる。つまり、FAEST の安全性は、1 組または 2 組の平文暗号文ペアが与えられた状況において、対応する AES 秘密鍵の復元困難性に帰着される。

本研究ではそのような状況を想定し、中間一致（MitM: Meet-in-the-Middle）攻撃手法を用いて AES の安全性を評価する。MitM 攻撃における現状の課題は、非線形制約を持つニュートラルワードを効率的に処理する点にある。既存研究は理論的に有効な手法を示したものの、解空間を事前に計算してテーブルに格納しておく必要があり、攻撃を実験的に実行するには膨大なメモリ（例：2^{80} 程度）が必要であるため、実際の鍵回復実験は困難であった。また、非線形方程式系の一部を効率的に解く Triangulation Algorithm（TA）は、「ある変数がただ 1 つの方程式にしか現れない」という条件が満たされなくなると処理を停止してしまうという構造的制約を抱えていた。

これらの課題を克服するために、本研究では以下の 2 つのアプローチを提案する。第一に、LaMacchia らおよび Bender らが提案した構造化ガウス消去法の着想を取り入れ、従来の TA を拡張した。これにより、従来の TA が停止するような状況でも処理を継続できるようになり、より複雑な非線形方程式系の効率的な解法が可能となった。第二に、拡張した TA を MitM 攻撃に組み込む新手法「Triangulating MitM 攻撃」を提案する。本手法により、解空間を事前にテーブル化して保持する必要がなくなり、攻撃に要するメモリ量を大幅に削減できる。

提案手法の有効性を検証するため、AES-128 に対して単一の既知平文暗号文ペアによる鍵回復攻撃を実施した。既存手法が最大 2^{96} 程度のメモリを要したのに対し、提案手法は 4 ラウンド AES-128 に対して最大 2^{24} まで、5 ラウンド AES-128 に対して最大 2^{40} までメモリ量を削減することに成功した。さらに、AES-192 および AES-256 に対しては、2 組の既知平文暗号文ペアを用いる初の鍵回復攻撃を提示し、それぞれ最大で 6 ラウンドおよび 7 ラウンドまでの攻撃が可能であることを示した。なお、部分的な鍵回復実験を実際に実施し、理論的な分析結果と一致することを確認している。

Practical Opcode-based Fault Attack on AES-NI

Xue Gong, Xin Zhang, Qianmei Wu, Fan Zhang, Junge Xu, Qingni Shen, Zhi Zhang

CHES 2025

AES New Instructions (AES-NI) に対するサイドチャネル攻撃の観点からの安全性評価に関する研究である。AES-NI は、AES の暗号化および復号処理を高速化するために Intel により導入されたハードウェア命令セットであり、多くの暗号アプリケーションにおいて性能向上に寄与している。また、AES-NI は一部のサイドチャネル攻撃を効果的に軽減すると考えられている一方で、能動的な故障注入、特に悪意のあるビット反転に対する耐性については十分に明らかではなかった。

本研究では、AES-NI のオペコードが解析され、1 ビットのみが異なる 6 組の命令ペアが特定された。これにより、特定のビット反転が生じた場合に、AES-NI 実装が故障注入型の解析に対して影響を受けうることを示している。この性質は、ECB モードおよび CBC モードにおける AES 鍵の復元に繋がる可能性がある。さらに本研究では、最終ラ

ウンド鍵の候補空間を削減する手法として、Opcode-based Fault Analysis (OFA) という新しい手法が提案された。OFA では、正しい暗号文と故障を含む暗号文の 1 組を使用し、ガウス消去法により最終ラウンド鍵の探索空間を縮小する。特に、AES-128 に対しては、鍵候補空間を 2^{32} まで削減できることが示された。また、AES-192 および AES-256 に対しては、Enhanced Opcode-based Fault Analysis（EOFA）が提案され、全数探索と比較して鍵候補空間をそれぞれ 2^{160}、2^{192} まで削減できることが示されている。最後に、著者らは提案手法の実現可能性を検証するため、物理環境における実験を行っている。具体的には、Rowhammer を用いて対象オペコードにビット反転を誘発し、OFA および EOFA を AES 実装に適用した。その結果、AES-ECB-128、AES-ECB-192、および AES-CBC-128 に対する実験において、1.03 時間から 1.36 時間程度で鍵候補を特定できることが確認された。

Scrutinizing the Security of AES-based Hashing and One-way Functions

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

Asiacrypt 2025

ブロック暗号 AES に対する中間一致（MitM: Meet-in-the-Middle）攻撃を用いた安全性評価に関する研究である。AES に対する MitM 衝突攻撃において、ニュートラルワード生成に伴う非線形制約処理が計算量上のボトルネックとなっており、特に AES-MMO/MP に対しては、計算量的に有効な衝突攻撃の構成が困難なため、10 年以上に渡って攻撃可能段数が更新されていない状況が続いていた。本研究では、この問題の原因が、MitM 攻撃において固定定数や部分一致条件が前後両チャンクに分散し、S-box に起因する非線形制約が多数ラウンドに広がる点にあることに着目した。これにより、ニュートラルワード生成のたびに大規模な非線形制約問題を解く必要が生じ、衝突攻撃に必要な計算量が膨大になるという課題があった。

これらの課題を解決するために、本研究では Single-Color Initial Structure (SCIS) と呼ばれる MitM 攻撃のための新しい手法を提案した。SCIS 手法では、制約を一方のチャンク（青チャンク）に集中的に配置し、もう一方のチャンクに高い自由度を持たせる。これにより、非線形制約は青チャンク内の少数ラウンドに局所化され、構造が固定された小規模な非線形方程式系として扱えるようになる。このような方程式系に対し、代数的 MitM、guess-and-determine、三角化アルゴリズムなどの既存技術を用いて高速に解くことが可能となり、重い非線形制約処理を一度に集約しつつ、多数のニュートラルワードを効率的に列挙できるようになった。

提案手法により、7 ラウンド AES-MMO/MP に対する 1 ブロック衝突攻撃ならびに 4 ラウンド AES-128-DM に対する 1 ブロック衝突攻撃を古典モデルで初めて実現し、従来の限界を突破した。これらの攻撃における計算量およびメモリ量はいずれも 2^{60} である。また、ゼロ知識証明やマルチパーティ計算の文脈において重要となる単一既知平文条件下での鍵回復攻撃に関し、AES-128 では 5 ラウンド（計算量 2^{120}、メモリ量 2^{40}）、AES-192 では 7 ラウンド（計算量 2^{120}、メモリ量 2^{72}）、AES-256 では 8 ラウンド（計算量 2^{120}、メモリ量 2^{72}）までの新たな結果を示した。さらに、Rijndael-192 や Rijndael-256 に対しても同様に、衝突攻撃や鍵回復攻撃に関する包括的な安全性評価を行なった。

Divide-and-Conquer Trail Enumeration Puncturing: Application to Salsa and ChaCha

Antonio Flórez-Gutiérrez, Yosuke Todo

Asiacrypt 2025

ストリーム暗号 Salsa および ChaCha に対する鍵回復攻撃の効率化に関する研究である。これらの暗号に対する従来の鍵回復攻撃の多くは差分線形解析に基づいており、鍵回復写像を高相関な近似関数に置き換えることで計算量の削減を実現していた。最新の研究では、Walsh スペクトラムに基づくビット・パンクチャリングおよびトレイル列挙パン

クチャリングと呼ばれる手法が提案され、従来の Probabilistic Neutral Bits に基づく手法と比べ、実験的ではなく理論的に鍵回復写像の構築が可能となった。しかし、この最新手法にもいくつかの課題が残されている。第一に、実際の攻撃でトレイル列挙を行う場合には計算量削減のための簡略化が不可避であり、不要な鍵推測を含む非効率な攻撃手順を導入せざるを得ない点である。第二に、この種の攻撃はオフライン計算量によって制限されることが多く、Walsh スペクトル構成などの解析段階における計算量が支配的になることで、攻撃が現実的な計算量の範囲を超えてしまう点である。第三に、最新手法では、相関が少数の支配的トレイルによって決定されるという仮定を前提にしているが、膨大なオフライン計算量のために、その仮定の妥当性を実際に検証することが不可能な点である。

これらの問題を解決するために、本研究では分割統治型トレイル列挙パンクチャリングを提案した。その中核となるのは、鍵回復写像の Walsh スペクトルや入力構造を一度に扱うのではなく、複数の小さな成分に分解し、それぞれの成分を独立に近似・評価した上で統合する点にある。具体的には、二種類の分解手法を組み合わせて反復的に適用する。第一の手法はスペクトル線形分解であり、鍵回復写像の Walsh スペクトルが中間マスクに関して線形結合として表現できる性質を利用し、スペクトルを複数の小さな擬似ブール関数の線形結合として分解する。第二の手法は入力領域分離分解であり、鍵回復写像が複数の出力ビットの XOR として表現される点に着目し、それぞれを入力領域の小さな独立関数として近似する。さらに、最終鍵加算を出力側に畳み込む最終鍵加算簡約手法を導入することで、トレイル探索およびパンクチャリングの対象となる入力次元を大幅に削減し、擬似ブール関数を明示的に構成・保存することなく評価可能とした。

提案手法により、Salsa および ChaCha に対する鍵回復攻撃の段数および計算量を大幅に改善した。具体的には、128 ビット鍵を使用する Salsa に対して初めて 8 ラウンドまでの鍵回復攻撃を実現し、計算量 $2^{125.8}$ とデータ量 $2^{110.3}$ で攻撃が可能であることを示した。これは Aumasson らによる 2008 年の研究以降、初めて段数を更新する結果である。また、7 ラウンドおよび 8.5 ラウンドの Salsa、ならびに 7.5 ラウンドの ChaCha に対しても、従来手法と比較して計算量を削減した鍵回復攻撃を実現した。特に、7.5 ラウンドの ChaCha に関しては、計算量を $2^{250.2}$ から $2^{243.6}$ まで削減することに成功した。なお、Salsa と ChaCha の仕様ラウンド数は 20 であるため、提案手法がこれらの暗号の安全性に及ぼすことはない。

Quantum Circuit Synthesis for AES with Low DW-cost

Haoyu Liao, Qingbin Luo

Asiacrypt 2025

AES の量子計算量に関する論文である。共通鍵暗号に対する量子攻撃の計算量を計るデファクトスタンダードとして、Grover アルゴリズムを用いた既知平文攻撃による鍵復元の困難性が用いられる。このフレームワークは近年、NIST PQC 標準化においてセキュリティレベルを指定する解読計算量の基準として用いられており、共通鍵暗号の以外の分野でも注目度の高いトピックである。

本論文では、先行研究 [Jaques et al., Eurocrypt 2020] と比較して、オラクルとして呼ばれる AES-128.192,256 の演算回路で DW-cost がそれぞれ 65280, 87552, 112896 のものを提案し、先行研究と比較して 45% 程度の削減となっている。DW-cost は量子回路の規模を深さと幅の積で測ったものである。なお、比較対象である Jaques らの回路計算量評価は NIST PQC 追加署名方式の Call for Proposals において引用されているため、本論文の結果が PQC の安全性の基準に反映されるかどうかは今後注目すべき点であると考えられる。

技術的には Grover アルゴリズムから呼ばれる AES 計算回路の中で、S-box の計算を行う量子回路の最適化による回路規模の削減を行っている。AES S-box の計算は $GF(2^8)$ 上の演算により定義されるが、量子回路の構成においては回路を可逆とするための逆元計算のコストが大きく、その部分を可能な限り削ることで攻撃計算量の削減が見込まれ

ていた。本論文では、古典での効率的な実装に用いられた Rijmen による composite field arithmetic を用いることで $GF(2^4)$ 上の計算に分割し、さらにその計算における中間状態を S-box 入力の uncompute に用いることで回路規模を削減している。その他鍵スケジューリング回路においても各ラウンド後に用いられる副鍵のみを in-place で生成することで回路規模の削減を行い、さらに DW-cost が最小となるような Toffoli ゲートの配置などの改良を積み重ねて今回の結果を得ている。

2.4.3 ハッシュ関数の安全性評価技術

Practical Preimage Attacks on 3-Round Keccak-256 and 4-Round Keccak[$r = 640, c = 160$]

Xiaoen Lin, Le He, Hongbo Yu

FSE 2025

軽量ハッシュ関数 Keccak の安全性、特に原像攻撃耐性に関する評価結果について報告したものである。近年の Keccak に対する原像攻撃では、線形構造（linear structures）や代数的手法（algebraic attacks）が広く活用されている。本研究では既存手法を改良し、3 ラウンド Keccak-256 および 4 ラウンド Keccak[$r = 640, c = 160$] に対する原像攻撃の効率化を図る。

まず、3 ラウンド Keccak-256 に対して、自由度を拡張しつつ、充足されていない制約に対応するための 3 段階の解析モデルを導入する。さらに、異なる変数の値を推測することで解決時間が大きく異なることを示し、推測の効率向上を実現する。これらの手法により、推測時間は 2^{52} に短縮され、各推測に必要な計算コストはおよそ 3 ラウンド Keccak 呼び出し $2^{5.2}$ 回分に抑えられる。結果として、原像発見に要する全体の計算量は約 $2^{52} \times 2^{5.2} = 2^{57.2}$ に削減される。次に、Crunchy Contest のインスタンスである 4 ラウンド Keccak[$r = 640, c = 160$] に対する原像攻撃では、自由度を節約し、より良い線形化を行うためのいくつかのテクニックを使用する。これらのテクニックに基づいて MILP モデルを構築し、$2^{60.9}$ のより良い計算量を伴う原像攻撃を導出する。3 ラウンド Keccak-256 と 4 ラウンド Keccak[$r = 640, c = 160$] の結果は、実際の例で検証済である。

Preimage Attacks on up to 5 Rounds of SHA-3 Using Internal Differentials

Zhongyi Zhang, Chengan Hou, Meicheng Liu

Eurocrypt 2025

ハッシュ関数 SHA-3（Keccak）の安全性、特に原像攻撃耐性に関する評価結果について報告したものである。従来の SHA-3 に対する原像攻撃は、主に線形構造（linear structure）、代数的手法（algebraic method）、中間一致（MitM: Meet-in-the-Middle）手法といった技術に基づいており、ブルートフォース探索の高速化技術を除くと、攻撃可能ラウンド数は最大 4 ラウンドの範囲に留まっていた。また、内部差分（internal differentials）と呼ばれる技術を活用した衝突攻撃では、SHA-3 に対して最大 6 ラウンドまで適用可能であることが知られているものの、内部差分を原像攻撃に応用した研究はこれまでに報告されていない。

本研究では、内部差分を原像攻撃に応用するための新しいフレームワークである、搾取 MitM 攻撃（squeeze MitM attack）を提案する。この手法は、Dinur らが 2013 年に提案した搾取攻撃（squeeze attack）と従来の MitM 攻撃を組み合わせたものであり、内部差分の技術も組み込まれている。また、SHA-3 のラウンド関数における逆演算を詳細に分析し、Dinur らのターゲット内部差分アルゴリズム（TIDA: Target Internal Differential Algorithm）を順方向処理だけでなく逆方向処理にも適用できる形で拡張するとともに、逆方向処理における S-box の線形化技術も開発した。さらに、攻撃にかかる計算量を最適化するための概念として、値差分分布表（VDDT: Value-Difference Distribution

Table）を導入した。

提案手法は、SHA-3 の各インスタンスに適用され、5 種類の 4 ラウンドインスタンス（SHA3-224、SHA3-256、SHA3-384、SHAKE128、SHAKE256）に対して計算量の大幅な削減に成功するとともに、4 種類の 5 ラウンドインスタンス（SHA3-224、SHA3-256、SHAKE128、SHAKE256）に対して初めての原像攻撃を実現した。また、Keccak のトイバージョンを用いて、4 ラウンド原像攻撃に対する実験的検証も行っている。さらに、提案手法は、NIST 耐量子計算機暗号の標準化プロセスを通じて標準化された ML-DSA や SLH-DSA で用いられる SHAKE128 と SHAKE256（具体的には、SHAKE128$(M, 256)$ と SHAKE256$(M, 512)$）にも適用可能となっている。なお、SHA-3 の全インスタンスにおけるラウンド数は 24 であるため、提案手法が SHA-3 の安全性に影響を及ぼすことはない。

New Collision Attacks on Round-Reduced SHA-512

Yingxin Li, Fukang Liu, Gaoli Wang, Haifeng Qian, Keting Jia, Xiangyu Kong
Crypto 2025

ハッシュ関数 SHA-512 の衝突攻撃耐性評価に関する論文である。SHA-512 の衝突攻撃耐性評価における現状の課題は、28 ステップを超える実用的な衝突攻撃がこれまでに提案されていない点、そして 31 ステップに対する理論的な衝突攻撃の計算量が $2^{97.3}$ と膨大であり、現実的に実行が困難であるという点にある。特に、既存の差分特性探索手法では「2 ビット条件（2-bit conditions）」と呼ばれる性質を十分に扱えず、これが攻撃成功確率の大幅な低下を招くという制約が存在していた。

本研究では、これらの課題を克服するために、2 つの新たなアプローチを提案する。最初のアプローチとして、SHA-512 の構造特性に基づく新しい局所衝突（local collision）を構築した。具体的には、メッセージワード $W_9, W_{10}, W_{14}, W_{17}, W_{19}$ に差分を注入することで、従来よりも広範囲のステップ間で衝突を誘発できるようにした。この新たな局所衝突の構築により、より長いステップ数に対して実用的な攻撃を構築することが可能となる。次に、SHA-512 の主要構成要素であるブール関数（XOR、IF、MAJ）における差分伝搬特性を精密にモデル化するために、2 ビット条件を考慮した新しい解析モデルを導入した。このモデルを用いることで、SAT/SMT ソルバーによる差分特性探索の精度を大幅に向上させ、不要または矛盾する条件を効果的に削減することが可能となる。

提案した局所衝突を適用することで、29 ステップ SHA-512 に対する初の実用的な衝突攻撃を達成した。さらに、2 ビット条件を統合した改良モデルにより、31 ステップ SHA-512 に対する理論的な衝突攻撃を効率化し、計算量を従来の $2^{97.3}$ から $2^{85.5}$ へと大幅に削減することに成功した。なお、SHA-512 のステップ数は 80 であるため、提案手法が SHA-512 の安全性に影響を及ぼすことはない。

Improved Semi-Free-Start Collision Attacks on RIPEMD-160

Zhuolong Zhang, Muzhou Li, Haoyang Wang, Shiqi Hou, Wei Wang, Meiqin Wang
Asiacrypt 2025

ハッシュ関数 RIPEMD-160 に対するセミフリースタート（SFS: Semi-free-start）衝突攻撃の高度化を目的とした安全性評価に関する研究である。最新の研究では、SAT/SMT に基づく自動探索モデルとメッセージ修正技術の導入により、最大 43 ステップまでの簡略化された RIPEMD-160 に対する SFS 衝突攻撃が実現された。しかし、既存の自動探索手法では、主としてハミング重みに基づくヒューリスティックな目的関数が用いられており、回転演算に起因する差分の派生や、非線形関数によって生じるビット制約条件といった確率低下要因が十分に考慮されていなかった。このため、特に RIPEMD-160 のステップ関数における右分岐側の差分確率が著しく低下してしまい、結果として 44 ス

テップ版への拡張が困難であった。さらに、従来のメッセージ修正技術では、メッセージや内部状態の調整によって直接制御できない未制御条件が一様に扱われ、成立確率や検証コストの異なる条件を区別した検証順序が最適化されていなかった。その結果、理論的な差分確率と比べて実際の攻撃計算量が大きく見積もられてしまうという課題が残されていた。

本研究では、これらの課題を解決するために、2 つの観点から既存手法を改良した。第一に、自動探索モデルの目的関数を再設計した。単純なハミング重みに加え、回転演算に起因する差分の派生や非線形関数に起因するビット条件制約を明示的に考慮することで、攻撃成功に寄与する主要な確率成分を統合的に評価する包括的目的関数を導入した。第二に、RIPEMD-160 専用のメッセージ修正手法を提案した。未制御条件が成立確率や検証コストの異なる複数の条件から構成されている点に着目し、これらを独立な部分集合に分割した上で最適な検証順序を自動的に決定することにより、SFS 衝突攻撃の効率性を向上させた。

提案手法により、44 ステップに簡略化した RIPEMD-160 に対する初の SFS 衝突攻撃を実現した。本攻撃の計算量は $2^{76.9}$ 回の 44 ステップ圧縮関数演算であり、必要なメモリ量は無視できる程度である。また、既存の 41〜43 ステップ版に対する SFS 衝突攻撃についても大幅な高速化を達成し、それぞれの計算量は $2^{49.8}$ 回、$2^{53.9}$ 回、$2^{76.9}$ 回の圧縮関数演算である。なお、RIPEMD-160 の仕様ステップ数は 80 であるため、提案手法が RIPEMD-160 の安全性に影響を及ぼすことはない。

2.5 耐量子計算機暗号への対応方針について

2022 年 7 月 5 日、米国国立標準技術研究所（NIST）から PQC の標準化方式として、公開鍵暗号 1 方式と電子署名 3 方式が発表された。これら 4 方式のうち、格子に基づく公開鍵暗号方式 ML-KEM は FIPS 203 として、格子に基づく署名方式 ML-DSA は FIPS 204 として、ハッシュ関数に基づく署名方式 SLH-DSA は FIPS 205 として、それぞれ 2024 年 8 月 13 日に標準化された。

2024 年度暗号技術検討会において、PQC への対応について議論が行われ、CRYPTREC 暗号リストへの掲載に向けた PQC の技術的検討と、PQC への移行方針の検討を両輪として並行に進めていくべきであるとの合意が得られた[*1]。これに伴い、ML-KEM、ML-DSA、SLH-DSA の安全性・実装性能の評価を先行して実施することで合意された。

このような背景を踏まえ、暗号技術評価委員会では、CRYPTREC 暗号リストへの掲載に向けた PQC の技術的評価と、PQC への移行に向けた技術的課題の検討を進める。

2.5.1 CRYPTREC 暗号リストへの掲載に向けた PQC の技術的評価

ML-KEM、ML-DSA、SLH-DSA の安全性・実装性能の評価を外部評価により実施する。この際、CRYPTREC 暗号リストへの掲載に向け、以下に示す基本方針、安全性・実装性能に関する調査・評価の内容、スケジュールに基づき、外部評価を進めることとする。

■基本方針　過去の事例に従い、安全性評価に関する外部評価を 2 件、実装性能評価に関する外部評価を 1 件とする。

■安全性に関する調査・評価の内容　以下の内容を含めるものとする。

- 安全性証明
- 方式に特化した安全性評価

[*1] https://www.cryptrec.go.jp/report/cryptrec-mt-1011-2024.pdf（資料 5）

- 暗号強度に関する考察（ベースとなる計算問題、鍵長やパラメータごとの安全性レベル、など）
- その他（Module 構造の有無に応じた計算量評価、など）

■実装性能に関する調査・評価の内容　以下の内容を含めるものとする。

- ソフトウェア・ハードウェアにおける実装性能評価
- ソフトウェア・ハードウェアのサイドチャネル攻撃耐性評価
- 暗号強度に関する考察（ベースとなる計算問題、鍵長やパラメータごとの安全性レベル、など）
- 現在の CRYPTREC 暗号リストに含まれる同技術分類の方式との性能比較に関する考察（例えば、KEM の場合は ECDH、署名の場合は EdDSA）

■スケジュール　表 2.3 のとおり。

表 2.3: ML-KEM、ML-DSA、SLH-DSA の外部評価スケジュール

対象	実施項目	評価完了年月	審議完了年月
ML-KEM (FIPS 203)	安全性評価 ×2、実装性能評価 ×1	2026 年 1 月	2026 年 3 月
ML-DSA (FIPS 204)	安全性評価 ×2、実装性能評価 ×1	2026 年 7 月	2026 年 9 月
SLH-DSA (FIPS 205)	安全性評価 ×2、実装性能評価 ×1	2026 年 9 月	2026 年 11 月

2.5.2　PQC への移行に向けた技術的課題の検討

PQC への移行に向けた技術的課題の検討に資するため、PQC 移行の技術動向に関する調査を外部評価により実施する。この際、以下に示す調査・評価の内容、スケジュールに基づき、外部評価を進めることとする。

■調査・評価の内容　以下の内容を含めるものとする。

- 2024 年度末に CRYPTREC のウェブサイトで公開した暗号技術ガイドライン（耐量子計算機暗号）2024 年度版では、PQC の導入における課題、PQC 導入へのアプローチ、PQC の活用に向けて、などが簡潔に整理されている。これらの内容のうち、技術的な部分のみを抽出し、深く掘り下げて体系的に整理する。
- 2020 年度にハイブリッドモードに関する技術動向調査を外部評価により実施し、本報告書を CRYPTREC のウェブサイトに公開した。本報告書の公開から約 5 年が経過していることを踏まえ、ハイブリッドモードに関する技術動向を再整理した上で、その内容を更新する。

■スケジュール　2025 年度に外部評価 1 件を完了させる。

2.6　耐量子計算機暗号 ML-KEM の安全性・実装性能に関する調査及び評価

第 2.5.1 節で示した基本方針、安全性・実装性能に関する調査・評価の内容およびスケジュールに基づき、2025 年度は、外部評価により「耐量子計算機暗号 ML-KEM の安全性・実装性能に関する調査及び評価」を実施した。外部評価報告書のエグゼクティブサマリーは、付録 C を参照されたい。

2.6.1 実施概要

耐量子計算機暗号 ML-KEM の安全性・実装性能について、公開されている解析手法や評価結果の有無を調査し、存在する場合はその影響範囲などについてまとめるなど、安全性と実装性能を評価した上で報告書を作成する。

2.6.2 ML-KEM の安全性に関する調査結果の概要

■安全性証明 古典ランダムオラクルモデルにおいて、使用される 2 つのハッシュ関数がランダムオラクルと仮定した場合、タイトな IND-CCA2 安全性を持つことが確認された。また、量子ランダムオラクルモデルにおいて、IND-CCA2 安全性はノンタイトであり漸近的な保証を与えるにとどまるものの、耐量子性の観点で十分に高い信頼性を有する結果とみなされることが確認された。

■Module-LWE 問題に対する計算量見積 BKZ シミュレーション[*2]と dimension-for-free 技術に基づき、primal 攻撃の計算量（攻撃に必要なゲートコストとメモリ量）を見積もった[*3]。その結果、攻撃に必要なゲートコストは、ML-KEM の全てのパラメータセットにおいて NIST 安全性水準を上回っており、十分な安全性を有することが確認された。詳細は、表 2.4 のとおり。

表 2.4: BKZ シミュレーションと dimension-for-free 技術に基づく primal 攻撃の計算量見積

	ML-KEM-512	ML-KEM-768	ML-KEM-1024
NIST 安全性レベル	レベル 1 （AES-128 相当）	レベル 3 （AES-192 相当）	レベル 5 （AES-256 相当）
要求されるゲートコスト（ビット）	143	207	272
攻撃に必要なゲートコスト（ビット）	151.5	215.1	287.3
攻撃に必要なメモリ量（ビット）	93.8	138.5	189.7

さらに、幾何級数仮定（GSA）と MATZOV 計算量モデルに基づき、primal 攻撃、dual 攻撃および hybrid 攻撃の計算量を見積った。その結果、攻撃に必要なゲートコストは、ML-KEM の全てのパラメータセットにおいて NIST 安全性レベルの水準を下回っていることが確認された。詳細は、表 2.5 のとおり。しかし、この見積では、計算量に影響しうる重要な性質[*4]が考慮されておらず、計算量見積が過小評価されている可能性がある。これらの性質を考慮した場合には、攻撃者に最も有利な状況を仮定しても、NIST 安全性水準を上回ることが確認された。

■Module 構造を考慮した攻撃 Module 構造を考慮した攻撃は、現時点において、Module 構造を考慮しない攻撃を上回るものではないということが確認された。

■暗号強度に関する考察 具体的な計算量見積に基づく評価の結果、古典計算および量子計算の双方について攻撃者側に極めて有利な仮定を置いた場合であっても、NIST 安全性レベルに対して十分な安全性マージンを有している。また、調査対象とした全ての攻撃クラスにおいて、現時点で現実的な脅威とみなせる脆弱性は発見されていない。これら

[*2] BKZ は Block-Korkine-Zolotarev の略であり、格子基底簡約を行う BKZ アルゴリズムのシミュレーターを指す。

[*3] 既存研究において、dual 攻撃が primal 攻撃と比較して計算コストがかかると予想されているため、ここでは Primal 攻撃の計算量見積のみ提供されている。

[*4] 例えば、篩処理の Progressive 化による格子基底の理想的な挙動からのずれ、BDGL 型篩処理で発生するオーバーヘッド等がある。

表 2.5: 幾何級数仮定（GSA）と MATZOV 計算量モデルに基づく計算量見積

	ML-KEM-512	ML-KEM-768	ML-KEM-1024
NIST 安全性レベル	レベル 1 （AES-128 相当）	レベル 3 （AES-192 相当）	レベル 5 （AES-256 相当）
要求されるゲートコスト（ビット）	143	207	272
primal 攻撃に必要なゲートコスト（ビット）	140.2	201.0	270.7
dual 攻撃に必要なゲートコスト（ビット）	149.9	214.3	288.5
hybrid 攻撃に必要なゲートコスト（ビット）	139.7	196.4	262.3

を踏まえると、最新の技術動向を考慮しても、ML-KEM は十分な安全性を有すると評価できる。

2.6.3 ML-KEM の実装性能に関する調査結果の概要

■サイドチャネル攻撃耐性 秘密鍵の復元につながるサイドチャネル攻撃の可能性が確認された。これに対する対策として、マスキングおよびハイディングの適用が推奨される。

■ハードウェア実装性能 回路面積の最適化実装 [XL21]、計算時間の最適化実装 [DMG23] およびサイドチャネル攻撃対策が施された実装 [Kam+22] について紹介された。詳細は、表 2.6 のとおり。

表 2.6: ML-KEM の FPGA 実装性能比較。なお、[Kam+22] では、マスキング対策とハイディング対策の両方を施した実装評価結果を示している。

参考文献	パラメータ	計算時間 (μs)			回路面積		FPGA
		KeyGen	Encap	Decap	LUT (×1000)	FF (×1000)	
[XL21]	512	23.4	31.5	41.4	7.4	4.6	Artix-7
	768	39.2	49.2	62.4	7.4	4.6	
	1024	58.3	70.3	86.4	7.4	4.6	
[DMG23]	512	10.0	14.7	20.5	9.5	8.5	Artix-7
	768	12.0	17.0	22.2	10.5	9.8	
	1024	16.2	21.7	26.4	11.6	11.1	
[Kam+22]	512	–	88.1	137.7	163.6	–	Virtex-7

■ソフトウェア実装性能 OpenSSL 3.6.0 を使用して測定した結果、ML-KEM は ECDH と同等以上の性能を発揮することが確認された。詳細は、表 2.7 のとおり。

また、ML-KEM と ECDH の帯域幅（具体的には、鍵長と暗号文長）を比較した結果、最大で 25 倍の差が生じていることが確認された。詳細は、表 2.8 のとおり。なお、帯域幅の増加は対処可能であり、インターネット上での ML-KEM の使用を妨げるものではないことが実証された。

■実装性能に関する考察 ML-KEM の計算時間は従来方式と比べて高速である一方、鍵長や暗号文長が増加するため、メモリ制約があるデバイス等においては実装上の課題が生じる可能性があるが、それ以外の用途においては問題な

表 2.7: ECDH と ML-KEM における計算時間の比較（ミリ秒）。† は古典安全性レベルを表しており、耐量子安全性は考慮していない。

	鍵交換アルゴリズム	安全性レベル	KeyGen	Encap	Decap
古典	EC X25519	$1^{\dagger}$	0.027	0.058	0.029
	EC P-256	$1^{\dagger}$	0.008	0.058	0.047
	EC P-384	$3^{\dagger}$	0.088	0.327	0.229
	EC P-521	$5^{\dagger}$	0.098	0.341	0.226
量子	ML-KEM-512	1	0.020	0.014	0.023
	ML-KEM-768	3	0.031	0.020	0.032
	ML-KEM-1024	5	0.047	0.028	0.043
ハイブリッド	X25519 + ML-KEM-768	$1^{\dagger} + 3$	0.061	0.076	0.060
	P-256 + ML-KEM-768	$1^{\dagger} + 3$	0.044	0.076	0.076
	P-384 + ML-KEM-1024	$3^{\dagger} + 5$	0.143	0.344	0.256

表 2.8: ECDH と ML-KEM における帯域幅（鍵長と暗号文長）の比較（バイト）。† は古典安全性レベルを表しており、耐量子安全性は考慮していない。

	鍵交換アルゴリズム	安全性レベル	カプセル化鍵	暗号文
古典	EC X25519	$1^{\dagger}$	32	32
	EC P-256	$1^{\dagger}$	65	65
	EC P-384	$3^{\dagger}$	97	97
	EC P-521	$5^{\dagger}$	123	123
量子	ML-KEM-512	1	800	768
	ML-KEM-768	3	1184	1088
	ML-KEM-1024	5	1568	1568
ハイブリッド	X25519 + ML-KEM-768	$1^{\dagger} + 3$	1216	1120
	P-256 + ML-KEM-768	$1^{\dagger} + 3$	1249	1153
	P-384 + ML-KEM-1024	$3^{\dagger} + 5$	1665	1617

く利用できる。サイドチャネル攻撃に対して厳密に保護されていることを前提として、政府および重要インフラシステムへの広範な展開にも適していると考えられる。

2.6.4 外部評価報告書に対する暗号技術評価委員会の見解

ML-KEM の安全性・実装性能に関する暗号技術評価委員会の見解は次のとおり。

- ML-KEM は、全てのパラメータセット（ML-KEM-512/768/1024）において、米国 NIST が規定する安全性レベル 1/3/5 を満たしている。
- ML-KEM は、従来方式と比較して高速である一方、鍵長および暗号文長が増加するが、メモリ制約が厳しいデバイスを除き、実用上問題なく利用できる。

- ML-KEM は、サイドチャネル攻撃対策が不十分な場合に脆弱性が生じる可能性があるものの、適切な対策の実装を前提とすれば、電子政府システムを含む多様なシステムへの広範な展開が可能である。

提出された外部評価報告書[*5][*6]は、2025 年度の調査対象である耐量子計算機暗号 ML-KEM の安全性・実装性能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。

2.7 耐量子計算機暗号への移行に関する技術動向調査

第 2.5.2 節で示した調査・評価の内容およびスケジュールに基づき、2025 年度は、外部評価により「耐量子計算機暗号への移行に関する技術動向調査」を実施した。外部評価報告書のエグゼクティブサマリーは、付録 D を参照されたい。

2.7.1 実施概要

PQC への移行に関する技術動向を調査し、公開情報を基にまとめ、考察などを行い、報告書を作成する。

2.7.2 調査結果の概要

■PQC 移行時・導入時における課題　PQC への移行時および導入時に直面する技術的課題について、用途別（署名用途、守秘用途、鍵共有用途）に整理された。

■PQC 導入へのアプローチ　PQC 導入に伴う全体プロセス、移行計画策定の検討事項、用途別の導入アプローチ、並びに段階的な移行モデルであるハイブリッド構成の位置付けについて整理された。特に、ハイブリッド構成は、既存システムとの連続性を確保しつつ、新たな暗号方式を段階的に導入するための現実的な構成例として位置付けられていると整理された。

■ハイブリッド構成に関する解説　ハイブリッド構成は単一の技術要素ではなく、複数のレイヤーにまたがる設計課題を内包していることが確認された。この認識に基づき、ハイブリッド構成を目的（後方互換性の確保および安全性の維持）と運用主体（アルゴリズム、プロトコル、システム）の各レイヤーから体系的に整理された。

■ハイブリッド構成の安全性に関する解説　標準化文書に記載された内容を基に、ハイブリッド構成における安全性について整理された。特に、安全性が成立するための条件と、それらの条件が実際の運用においてどのような構成要素に依存して具体化されるのかという点に着目された。

■ハイブリッド構成の実装・運用に関する解説　PQC およびハイブリッド構成の実装に関する主要な OSS の整備状況と、実運用環境における実装・移行事例が整理された。特に、国際会議 PQC Conference で報告された以下の事例について紹介された。

1. 実運用を想定した PQC 移行および性能評価の事例
2. Web PKI における段階的 PQC 導入の事例

[*5] https://www.cryptrec.go.jp/exreport/cryptrec-ex-3501-2025.pdf
[*6] https://www.cryptrec.go.jp/exreport/cryptrec-ex-3502-2025.pdf

3. PKI 階層設計におけるハイブリッド構成の活用事例
4. S/MIME 電子メールにおけるハイブリッド構成の実装事例

■PQC 移行に関わる標準化動向の調査　PQC 移行期におけるハイブリッド構成の方式の取り扱いに着目し、国際的な標準化団体および関連組織における検討状況が整理された。調査対象組織の一覧は、表 2.9 のとおり。

表 2.9: 調査対象組織の一覧

No.	組織名	URL
1	NIST	https:www.nist.gov/
2	IETF	https://www.ietf.org/
3	ITU	https://www.itu.int/
4	ETSI	https://www.etsi.org/
5	IEEE	https://www.ieee.org/
6	ISO	https://www.iso.org/
7	ASC X9	https://x9.org/
8	NSA	https://www.nsa.gov/
9	CSA	https://cloudsecurityalliance.org/
10	PQCRYPTO	https://pqcrypto.eu.org/
11	PQCC	https://pqcc.org/

■調査結果に関する考察　2020 年度外部評価報告書「ハイブリッドモードの技術動向調査」の公開時点[*7]では、ハイブリッド構成は概念レベルにとどまり、標準化活動も議論が始まったばかりの段階であった。一方、2025 年以降は主要な標準化機関において本格的な標準化活動が進展しており、その動きが活発化していることが確認された。特に、2026 年 1 月時点では、ハイブリッド構成は主要な標準化機関において技術仕様として確立されており、TLS、X.509、VPN などの各種プロトコルや PKI 基盤に関しても、具体的な実装指針が整備されていることが確認された。これらの具体的な整備により、ハイブリッド構成は単なる概念段階を超えて、既存プロトコル・証明書・運用基盤の中で「移行期に採用可能な実装構成」として体系的に確立されたと評価できる。

2.7.3　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[*8]は、2025 年度の調査対象である耐量子計算機暗号への移行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。

2.8　委員会開催記録

表 2.10 のとおり、2025 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。

[*7] 2020 年度の報告書では、ハイブリッド構成のことをハイブリッドモードと称していた。
[*8] https://www.cryptrec.go.jp/exreport/cryptrec-ex-3503-2025.pdf

表 2.10: 暗号技術評価委員会の開催状況

回	開催日	議案
第 1 回	2025 年 7 月 1 日	• 暗号技術調査 WG（耐量子計算機暗号）の活動計画案に関する審議 • 耐量子計算機暗号への対応方針と 2025 年度外部評価に関する審議 • CRYPTREC 暗号リストにおける仕様書参照先の変更に関する審議 • 監視状況報告 • CRYPTREC シンポジウム 2025 開催に関する周知
第 2 回	2026 年 3 月 3 日	• 暗号技術調査 WG（耐量子計算機暗号）の活動内容に関する報告 • CRYPTREC 暗号リストにおける仕様書参照先の変更に関するメール審議結果の報告 • 外部評価スケジュールの変更と ML-DSA 外部評価の実施に関するメール審議結果の報告 • 外部評価スケジュールの再変更と SLH-DSA 外部評価の実施に関する審議 • 耐量子計算機暗号 ML-KEM の安全性・実装性能に関する調査及び評価の内容に関する報告・審議 • 耐量子計算機暗号への移行に関する技術動向調査の内容に関する報告・審議 • 監視状況報告 • 2025 年度暗号技術評価委員会の活動報告案に関する審議 • 2026 年度暗号技術評価委員会の活動計画案に関する審議 • CRYPTREC Report 2025 の目次案に関する審議 • CRYPTREC シンポジウム 2026 開催に関する周知

第 3 章

暗号技術調査 WG（耐量子計算機暗号）の活動

3.1　2025 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

以下、本節において暗号技術調査ワーキンググループ (耐量子計算機暗号) を PQC WG と表記する。

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。この決定に従い、暗号技術評価委員会は 2021-2022 年度に PQC WG を設置し、ガイドライン及び調査報告書を作成、公開した。

その後、2023 年度第 1 回暗号技術評価委員会において、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、PQC WG を設置して以下の 2 点の活動を行った。NIST PQC 標準化プロジェクトにおいて選定の第 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および標準化活動が引き続き世界的に活発であることを踏まえ、動向を 2023 年度から 2 年間かけて調査・把握し、ガイドライン及び調査報告書を作成、公開した。「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検討し、更新した。

2025 年度暗号技術評価委員会準備委員会において、PQC 関連の技術開発および標準化の活発な活動が世界的に継続していることを踏まえ、引き続き PQC WG を設置し以下の 2 点の活動を行うことが承認された。

(1) 2025 年 6 月の時点で、NIST の PQC 標準化において 3 件の標準化文書（FIPS 203〜205）が公開され、今後も 2 件の標準化（FALCON、HQC)、および追加署名の選定プロジェクトが継続していること、また標準方式が世界各国で推奨暗号とされ、PQC への移行が進められていることを踏まえ、動向を 2025 年度から 2 年間かけて調査・把握し、ガイドライン及び調査報告書を作成する。

(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」の予測図の更新を行う。500 位に位置するスーパーコンピュータのプロットがさまざまな要因によって鈍化傾向を示していることから、500 位のプロットについて見直す。なお、後者については、2025 年度第 1 回暗号技術評価委員会において、500 位のプロットの削除に関して PQC WG で検討することが決定された。

3.2 耐量子計算機暗号ガイドラインの作成

上記活動 (1) の 2025 年度の活動内容および 2026 年度の計画について記述する。

3.2.1 スケジュール（2025 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
2025 年度	第 1 回 2025/8/4	・追記・改定の方針について議論 ・執筆担当者を議論・決定
	第 2 回 2026/1/22	・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
2026 年度	第 1 回	・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	・内容の確定

3.2.2 記載すべき項目及び章立てと執筆担当者

	執筆担当者
1. はじめに	事務局（青野、伊藤（琢））
2. PQC の活用方法	伊藤委員
3. 格子に基づく暗号技術	下山委員、安田（雅）委員
4. 符号に基づく暗号技術	成定委員
5. 多変数多項式に基づく暗号技術	安田（貴）委員
6. 同種写像に基づく暗号技術	高島委員
7. ハッシュ関数に基づく署名技術	廣瀬委員
8. 総括（追加される場合）	國廣主査、事務局

※國廣主査、青木委員、高木委員はガイドライン及び調査報告書の全体的な構成及び内容等について担当する。

3.2.3 作業工程表

ガイドライン及び調査報告書の調査・執筆活動は以下の工程表に従い行う。

作業分類	時期（目安）	作業の内容	作業担当者
執筆準備	2025 年度第 1 回 WG	執筆方針・調査内容の確定、執筆担当者の決定	
動向調査	2025 年度第 2 回 WG	調査内容の中間報告	執筆担当の各委員
	2026 年度第 1 回 WG	調査内容の中間報告	執筆担当の各委員
	～2026 年 9 月末	執筆内容の文献把握	執筆担当の各委員
原稿執筆	～2026 年 11 月	各章の執筆作業	執筆担当の各委員
		執筆担当委員 ⇒ 担当事務局員に原稿を送付	執筆担当の各委員
	2026 年 12 月	担当事務局員による原稿の添削	担当事務局員
	2027 年 1 月	執筆担当委員、担当事務局員間で合意の取れた原稿の完成	執筆担当の各委員、担当事務局員
		合意の取れた原稿を事務局に送付	執筆担当の各委員
		原稿のマージ作業、マージした原稿の ML 上での共有	事務局
		原稿内容のチェック	事務局
	2026 年度第 2 回 WG	調査内容の中間報告	執筆担当の各委員
	2027 年 1 月～2 月 （評価委員会の 1 週間前まで）	原稿内容の確認・修正	WG 全員
暗号技術評価委員会の確認	2027 年 2 月頃	評価委員会提出版の完成（WG 終了後できるだけ早く）	WG 全員
		暗号技術評価委員会コメント対応	基本的には事務局内での対応
暗号技術検討会の確認	2027 年 3 月頃	暗号技術検討会提出版の完成	事務局
		暗号技術検討会コメント対応	事務局
公開		公開版の完成	事務局
		公開	事務局

※暗号技術評価委員会への提出版が完成した時点で、暗号技術評価委員会および暗号技術検討会のメンバーに同時に共有しコメントを募る。

3.2.4　2025 年度第 1 回 WG（8/4）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以下の方針で合意した
  - 過去のガイドライン及び調査報告書をベースに 2026 年度版ガイドライン及び調査報告書を作成する。基本的な方針は 2024 年度版と同様とし、2026 年度版も過去版の改訂扱いではなく新規の扱いとする。
  - ガイドライン及び報告書の暗号方式の解説を行う節のタイトル「代表的な暗号方式」「主要な暗号方式」が内容を反映していないため、事務局が新たなタイトル案を提示する。
  - ガイドライン及び報告書の総括を行う章を新たに追加する可能性を今後検討する。
  - 暗号技術評価委員会で行っている FIPS203,204,205 の外部評価の結果とガイドライン及び調査報告書の内容に矛盾が起きないように執筆する。
- 調査活動と執筆活動の方針に関して以下で合意した。
  - 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 2026 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。
  - 各章の執筆担当者が 2025 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。

3.2.5　2025 年度第 2 回 WG（2026/1/22）での実施内容及び決定事項

- 各章の執筆担当者が 2025 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。
  - 暗号方式の解説を行う節タイトルに関して、*.2 節を「代表的な暗号方式」から「暗号方式の基本設計」へ、*.3 節を「主要な暗号方式」から「実用的な暗号方式」へと変更する。ただし各章の暗号技術名と合わせたときに自然なものとなるよう執筆担当者は適宜調整する。

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

第 3.1 節 (2) に記載の 2025 年度の活動内容に関しては、以下のとおり、「今後の予測図の取り扱い」の方針に基づいて予測図の更新を行った（図 3.1 および 3.2)。また、500 位に位置するスーパーコンピュータのプロットが近年さまざまな要因によって鈍化傾向を示している状況を踏まえ、500 位のプロットの削除について検討した。

> ＜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。

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、2025 年 6 月・11 月のベンチマーク結果を追加した。その他の修正箇所は以下のとおりである。

- 500 位のプロットの削除について検討した結果、500 位のプロットは 2024 年度までとし、それに対応する外挿線は削除した。
- 暗号強度要件（アルゴリズム及び鍵長）に関する設定基準における基本設定方針に沿ったパラメータ（利用可・移行完遂期間、2022 年 3 月策定以降）を黄色部分で示した。
- セキュリティ強度が 112 ビットセキュリティ相当の Binary Fields 及び Koblitz Curves （群位数 233 ビット）を追記した（図 3.2)。

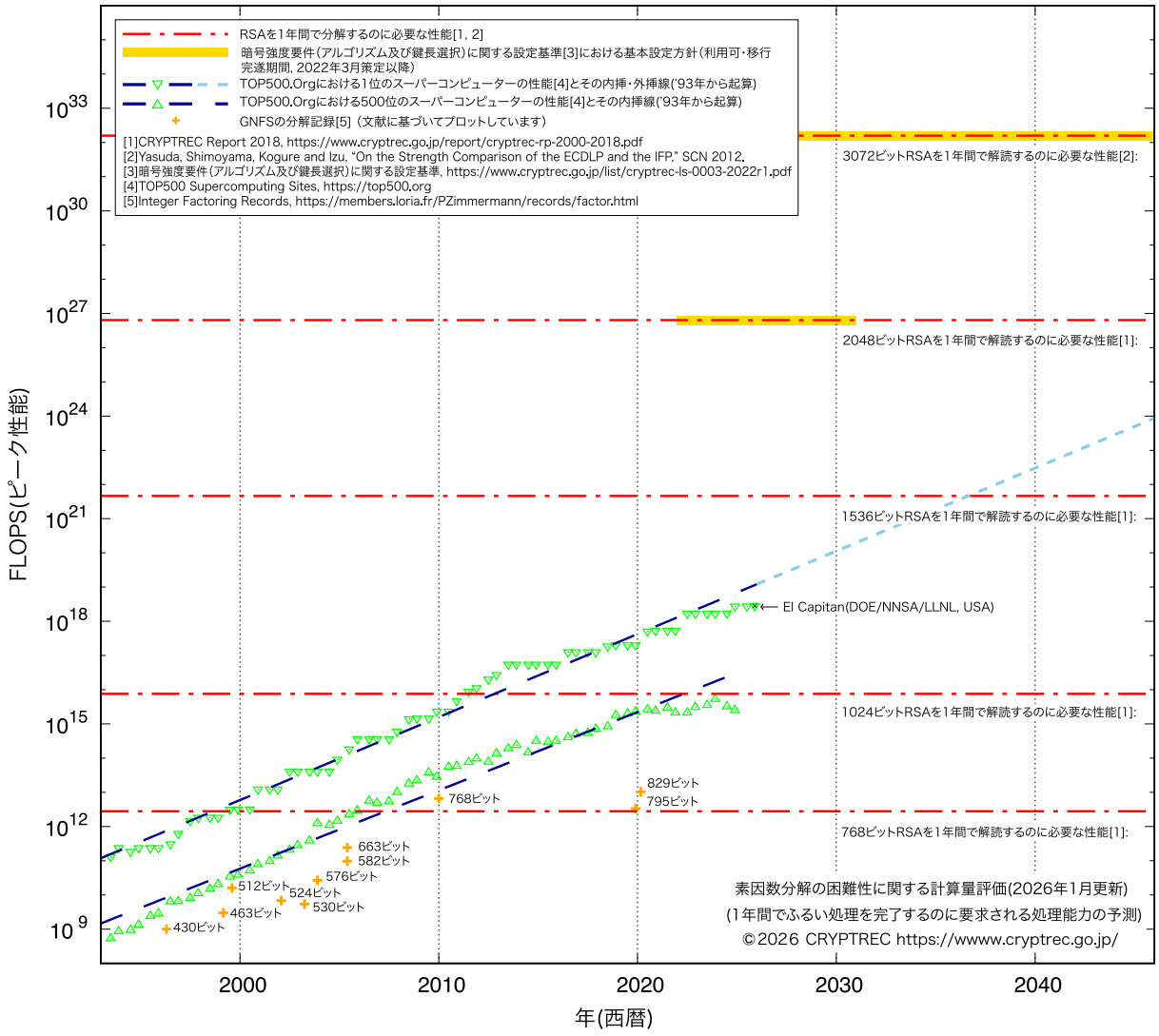

図 3.1: 素因数分解の困難性に関する計算量評価 (2026 年 1 月更新)[*1]

[*1] スーパーコンピュータ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。

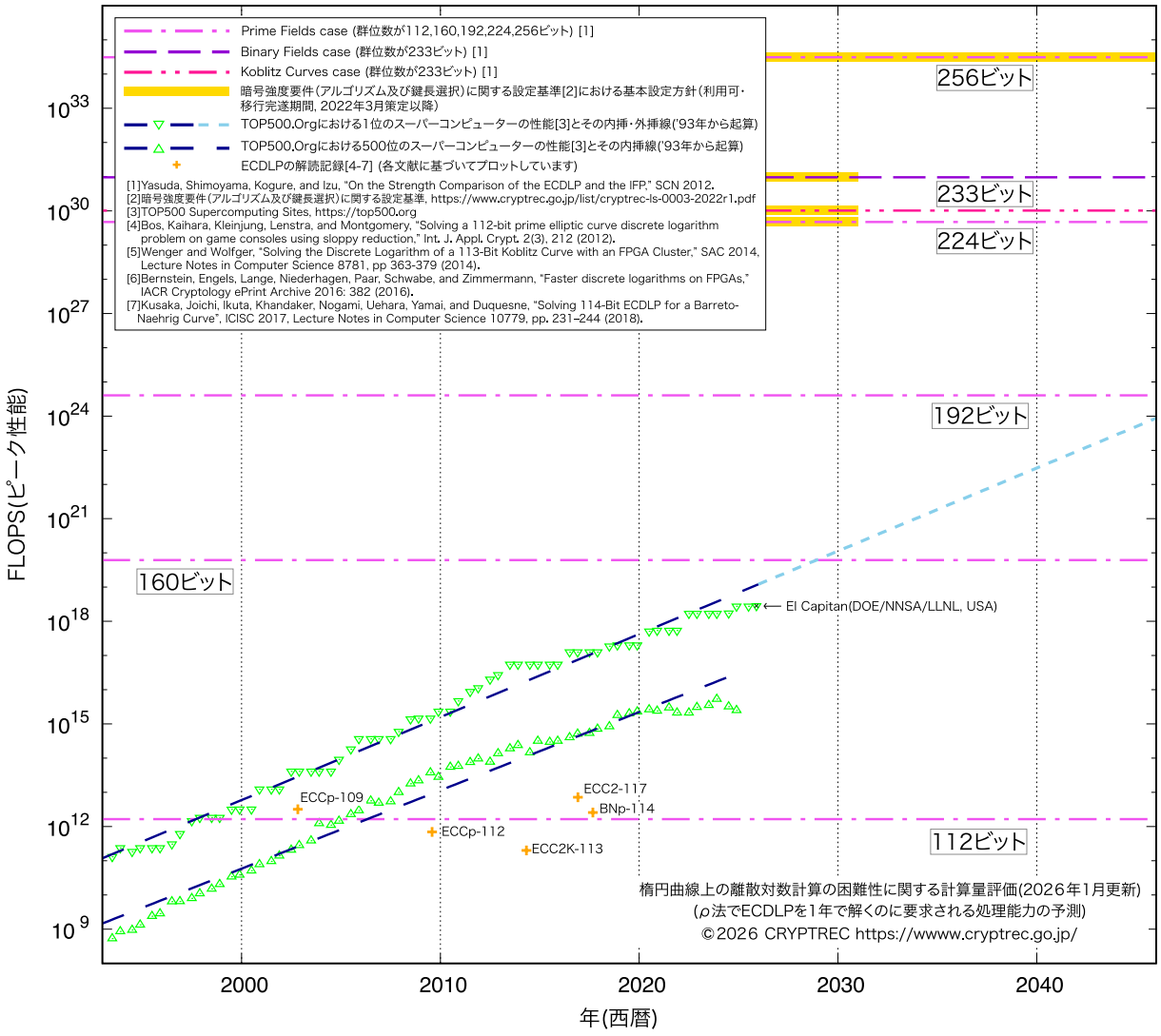

図 3.2: 楕円曲線上の離散対数計算の困難性に関する計算量評価 (2026 年 1 月更新)[*2]

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

3.4 暗号技術調査 WG 開催記録

表 3.1 のとおり、2025 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 3.1: 暗号技術調査 WG（耐量子計算機暗号）の開催状況

回	開催日	議案
第 1 回	2025 年 8 月 4 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 • ガイドライン・調査報告書の執筆方針に関する審議 • ガイドライン・調査報告書の執筆担当者、執筆スケジュールに関する審議 • 2025 年度予測図の更新に関する審議
第 2 回	2026 年 1 月 22 日	• 政府機関等における PQC 利用に関する関係府省庁連絡会議の報告 • 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 • ガイドライン・調査報告書の執筆方針に関する審議 • 2025 年度予測図の更新に関する審議 • 今後の作業スケジュールに関する確認

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８年３月30日）

電子政府推奨暗号リスト

暗号技術検討会[1]及び関連委員会（以下「CRYPTREC」という。）により安全性（セキュリティ）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」[3]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。

＜表１　現行暗号リスト＞

技術分類		暗号技術
公開鍵暗号	署名	DSA（注１）
		ECDSA
		EdDSA
		RSA-PSS
		RSASSA-PKCS1-v1_5
	守秘	RSA-OAEP
	鍵共有	DH
		ECDH（注２）
共通鍵暗号	64ビットブロック暗号（注3）	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４）
		SHAKE256（注４）

（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。

3 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 なお、当該設定基準の見直しの検討を行う予定であり、当面の間、表２（耐量子計算機暗号（PQC）リスト）の公開鍵暗号は、当該設定基準を適用しない。

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５）
	認証付き秘匿モード（注６）	CCM
		GCM（注７）
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）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２）使用するMACはHMAC又はCMACに限る。

（注３）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）ハッシュ長は256ビット以上とすること。

（注５）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６）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７）初期化ベクトル長は96ビットを推奨する。

＜表２　耐量子計算機暗号（PQC）リスト＞

現行暗号の解読に利用可能な水準の量子計算機（CRQC: Cryptographically Relevant Quantum Computer）への耐性を有することが確認された暗号技術のリスト[4]。

技術分類		暗号技術	
		名称	パラメーターセット（注８）
公開鍵暗号	署名	―	―
	鍵共有	ML-KEM	ML-KEM-768 (Category 3) ML-KEM-1024 (Category 5)
共通鍵暗号		AES	AES-192 (Category 3) AES-256 (Category 5)
ハッシュ関数		SHA2	SHA-384 (Category 4) SHA-512
		SHA3	SHA3-384 (Category 4) SHA3-512

（注８）セキュリティのカテゴリを合わせて記載する。各カテゴリはNISTの“Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process”に従い、次のように、カテゴリ名の右に記載の鍵探索又は衝突探索と同程度以上の計算資源が攻撃に必要であることを意味する。

・Category 1　128ビット鍵を持つブロック暗号に対する鍵探索
・Category 2　256ビットのハッシュ関数に対する衝突探索
・Category 3　192ビット鍵を持つブロック暗号に対する鍵探索
・Category 4　384ビットのハッシュ関数に対する衝突探索
・Category 5　256ビット鍵を持つブロック暗号に対する鍵探索

https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf （令和８年３月25日現在）

4 暗号技術の耐量子計算機暗号（PQC）リストへの追加について検討中である。
https://www.cryptrec.go.jp/report/cryptrec-mt-1501-2026.pdf

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[5]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９）
共通鍵暗号	64ビットブロック暗号（注10）	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11）
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12）	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９）KEM（Key Encapsulating Mechanism）－ DEM（Data Encapsulating Mechanism）構成における利用を前提とする。

（注10）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11）平文サイズは64ビットの倍数に限る。

（注12）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。

5 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[7]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[8]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」[9]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13)
	鍵共有	該当なし
共通鍵暗号	64ビットブロック暗号 (注14)	3-key Triple DES (注15)
	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
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17)
認証暗号		該当なし
エンティティ認証		該当なし

（注13）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14）CRYPTREC暗号リストにおいて、64ビットブロック暗号により、同一の鍵を用いて暗号化する場合、2^{20}ブロックまで、同一の鍵を用いてCMACでメッセージ認証コードを生成する場合、2^{21}ブロックまでとする。

（注15）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。

（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17）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。

7 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。
8 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
9 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	［新規追加］	（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。
	注	［新規追加］	（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。
令和８年３月30日	電子政府推奨暗号リスト（本文）	暗号技術検討会及び関連委員会（以下、「CRYPTREC」という。）により安全性及び実装性能が確認された暗号技術について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリスト。	暗号技術検討会及び関連委員会（以下「CRYPTREC」という。）により安全性（セキュリティ）及び実装性能が確認された暗号技術について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリスト。
	電子政府推奨暗号リスト（表）	［表の件名付与］	＜表１　現行暗号リスト＞
	電子政府推奨暗号リスト（表）	［表の新設］	＜表２　耐量子計算機暗号（PQC）リスト＞ 現行暗号の解読に利用可能な水準の量子計算機（CRQC: Cryptographically Relevant Quantum Computer）への耐性を有することが確認された暗号技術のリスト。
	電子政府推奨暗号リスト（耐量子計算機暗号（PQC）リスト）	［技術分類の追加］	技術分類：公開鍵暗号－署名 名称／パラメーターセット：－ 技術分類：公開鍵暗号－鍵共有 名称：ML-KEM パラメーターセット： ML-KEM-768（Category 3） ML-KEM-1024（Category 5）
	電子政府推奨暗号リスト（耐量子計算機暗号（PQC）リスト）	［技術分類の追加］	技術分類：共通鍵暗号 名称：AES パラメーターセット： AES-192（Category 3） AES-256（Category 5）
	電子政府推奨暗号リスト（耐量子計算機暗号（PQC）リスト）	［技術分類の追加］	技術分類：ハッシュ関数 名称：SHA2 パラメーターセット： SHA-384（Category 4） SHA-512 名称：SHA3 パラメーターセット： SHA3-384（Category 4） SHA3-512
	脚注	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	３　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 なお、当該設定基準の見直しの検討を行う予定であり、当面の間、表２（耐量子計算機暗号（PQC）リスト）の公開鍵暗号は、当該設定基準を適用しない。
	脚注	［新規追加］	４　暗号技術の耐量子計算機暗号（PQC）リストへの追加について検討中である。 https://www.cryptrec.go.jp/report/cryptrec-mt-1501-2026.pdf
	脚注	脚注３、４、７、８	脚注５、７、８、９
	注	（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）	［削除］

	注	（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）	［削除］
	注	［新規追加］	（注２）使用するMACはHMACまたはCMACに限る。
	注	［新規追加］	（注８）セキュリティのカテゴリを合わせて記載する。各カテゴリはNISTの“Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process”に従い、次のように、カテゴリ名の右に記載の鍵探索又は衝突探索と同程度以上の計算資源が攻撃に必要であることを意味する。 ・Category 1 128ビット鍵を持つブロック暗号に対する鍵探索 ・Category 2 256ビットのハッシュ関数に対する衝突探索 ・Category 3 192ビット鍵を持つブロック暗号に対する鍵探索 ・Category 4 384ビットのハッシュ関数に対する衝突探索 ・Category 5 256ビット鍵を持つブロック暗号に対する鍵探索 https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf （令和８年３月25日現在）
	注	注18、２、12、17、13、４、５～７、14、９、15、19、11	注１、３、４、５、６、７、９～11、12、13、14、15、17

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 ＜表 1 現行暗号リスト＞

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 Federal Information Processing Standards Publication 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 3 (April 2018), Recommendation for Pair Wise Key Establishment Schemes Using Discrete Logarithm Cryptography https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar3.pdf ただし使用するメッセージ認証コードは HMAC または AES-CMAC に限る.

共通鍵暗号

暗号技術名	AES
仕様参照先	NIST Federal Information Processing Standards Publication 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 NTT 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 セキュリティ部門 情報セキュリティグループ 福島 和英 TEL: 070-3508-2305, FAX: 049-278-7510 email: ka-fukushima@kddi.com

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 Federal Information Processing Standards Publication 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 Federal Information Processing Standards Publication 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 Federal Information Processing Standards Publication 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://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://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://jsa.or.jp/）から入手可能

B.2 電子政府推奨暗号リスト ＜表 2 耐量子計算機暗号（PQC）リスト＞

公開鍵暗号

暗号技術名	ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism)
仕様参照先	NIST Federal Information Processing Standards Publication 203 (August 2024), Module-Lattice-Based Key-Encapsulation Mechanism Standard https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.pdf

共通鍵暗号

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

ハッシュ関数

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

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

B.3 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 NTT 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	和文：https://www.mitsubishielectric.co.jp/corporate/randd/misty_j.pdf 英文：https://www.mitsubishielectric.com/rd/misty_e_b.pdf
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 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	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 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

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.4 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	3-key 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 Federal Information Processing Standards Publication 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（）から入手可能

付録 C

耐量子計算機暗号 ML-KEM の安全性・実装性能に関する調査及び評価

2025 年度外部評価報告書「耐量子計算機暗号 ML-KEM の安全性に関する調査及び評価」および「CRYPTREC: ML-KEM Evaluation Report」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-3501-2025.pdf, https://www.cryptrec.go.jp/exreport/cryptrec-ex-3502-2025.pdf）から取得可能である。

耐量子計算機暗号 ML-KEM の
安全性に関する調査及び評価

安田 雅哉
（立教大学理学部）

2026 年 1 月

第 1 章

調査結果・評価結果の概要（エグゼクティブサマリー）

FIPS 標準化された ML-KEM [64] は，加群格子上の LWE である Module-LWE 問題に基づく KEM で，通常（構造化なし）の LWE 問題に基づく方式に比べて効率的である．

■ML-KEM の構成概要　ML-KEM の基礎環は $R = \mathbb{Z}[X]/(X^n+1)$ $(n = 256)$ で，素数 $q = 3329$ を法とする剰余環 $R_q = R/qR$ を用いる．また，安全性レベルに応じて，3 種類の階数 $k \in \{2, 3, 4\}$ を選択する．ML-KEM では，秘密鍵 $\boldsymbol{s} = (s_1, \ldots, s_k) \in R_q^k$ とノイズ $\boldsymbol{e} = (e_1, \ldots, e_k) \in R_q^k$ の成分多項式 $s_i, e_i \in R_q$ のすべての $\mathbb{Z}_q$ 係数は，中心二項分布 CBD_η $(\eta \in \{2, 3\})$ からサンプルされる．本章では，すべてのベクトルは列ベクトルとする．このとき，すべての成分が R_q 上一様ランダムに選ばれた行列 $\boldsymbol{A} \in R_q^{k \times k}$ に対して，組 $(\boldsymbol{A}, \boldsymbol{t})$ を ML-KEM の公開鍵とする．ただし，$\boldsymbol{t} = \boldsymbol{A}\boldsymbol{s} + \boldsymbol{e} \in R_q^k$ とする．また，各係数が $\{0, 1\}$ に属する平文 $m \in R_q$ に対し，すべての $\mathbb{Z}_q$ 係数を CBD_η からサンプルした $\boldsymbol{y}, \boldsymbol{e}_1 \in R_q^k$ と $e_2 \in R_q$ を選び，公開鍵 $(\boldsymbol{A}, \boldsymbol{t})$ を用いて，

$$c = (\boldsymbol{u}, v) = \left(\boldsymbol{A}^\top \boldsymbol{y} + \boldsymbol{e}_1, \boldsymbol{t}^\top \boldsymbol{y} + e_2 + \left\lceil \frac{q}{2} \right\rfloor \cdot m\right) \in R_q^k \times R_q \tag{1.1}$$

を m の暗号文とする．さらに，暗号文に対して，$v - \boldsymbol{s}^\top \boldsymbol{u} \in R_q$ の各 $\mathbb{Z}_q$ 係数をノイズ補正することで復号できる．このように構成した公開鍵暗号方式を，藤崎-岡本変換により KEM（ML-KEM）に変換する．ML-KEM では，R_q における乗算を高速化するために，数論変換が多用される．

■ML-KEM の証明可能安全性　ML-KEM の秘密鍵 $\boldsymbol{s} \in R_q^k$ に対して，R_q^k 上で一様にサンプルされた $\boldsymbol{a} \in R_q^k$ と $t = \boldsymbol{a}^\top \boldsymbol{s} + e \in R_q$ の組 $(\boldsymbol{a}, t) \in R_q^k \times R_q$ を Module-LWE サンプルという．ただし，$e \in R_q$ の各 $\mathbb{Z}_q$ 係数は CBD_η からサンプルされる．Module-LWE サンプルの分布が $R_q^k \times R_q$ 上の一様ランダム分布と識別困難な Module-LWE 仮定の下で，ML-KEM の基盤である公開鍵暗号方式は IND-CPA 安全である．したがって，藤崎-岡本変換で得られる ML-KEM は IND-CCA 安全である．その安全性証明は，ランダムオラクルモデル（ROM）においてはタイトである一方，量子ランダムオラクルモデル（QROM）においてはノンタイトである（文献 [13, §4] を参照）．しかし，いくつかの自然な仮定の下では，QROM においてもタイトな安全性帰着がある．

表 1.1　ML-KEM における 3 種類のパラメータとゲートコストによる攻撃計算量の見積もり

ML-KEM パラメータ（k：階数パラメータ）	512（$k=2$）	768（$k=3$）	1024（$k=4$）
攻撃可能な BKZ の最小ブロックサイズ β	413	637	894
攻撃に必要なゲートコスト（ビット）	151.5	215.1	287.3
NIST 標準化の安全性レベル [63]	レベル 1	レベル 3	レベル 5
要求される古典ゲート数（ビット）	143	207	272

■ML-KEM の安全性を支える Module-LWE 問題に対する攻撃計算量　現時点で，ML-KEM の安全性を支える Module-LWE 問題に対する最良の攻撃法は，$\mathbb{Z}_q$ 上の LWE 問題に帰着した上で，BKZ 基底簡約などの $\mathbb{Z}$ 格子上のアルゴリズムを適用するものである．暗号文 (1.1) の形から，攻撃に利用できる Module-LWE サンプル数は最大 $k+1$ 個であり，ML-KEM に対しては primal 攻撃と dual 攻撃が有効となる．表 1.1 に，ML-KEM パラメータと，それらに対する攻撃計算量の見積もりをまとめる．具体的には，ML-KEM パラメータに対し primal 攻撃と BKZ 基底簡約の組み合わせが有効で，攻撃者に有利な観点で，BKZ の progressive 化とシミュレーション [29]，dimension-for-free [32] など最新技術の効果を考慮する．また，BKZ の内部 SVP オラクルで呼び出す篩アルゴリズムの最内部にある繰り返し関数に対して，文献 [6] の解析に基づくゲートコストを表 1.1 に示す（詳細は文献 [13, Table 4] を参照）．表 1.1 から，各 ML-KEM パラメータに対して，攻撃に必要なゲートコストは耐量子計算機暗号の NIST 標準化 [63] の安全性レベル 1, 3, 5 で要求される古典ゲート数を上回り，十分な安全性を持つと考えられる．

篩アルゴリズムの解析の精密化・改良による影響　篩アルゴリズムの多角的な解析の精密化と，将来予想されるアルゴリズム的改良を考慮すると，表 1.1 内のゲートコスト評価は $-16 \sim 14$ 程度変動する可能性がある [13, §5.3, Summary]．最悪の場合，NIST 標準化で要求される古典ゲート数を下回る可能性があるが，これはあくまで攻撃者に最も有利な条件下での評価に過ぎない．実際には，文献 [56, §4.1.1] で指摘されているように，篩アルゴリズムのメモリアクセスのコストを現実的に反映した条件下では，NIST 標準化で要求される古典ゲート数は維持されると考えられる．（文献 [79] によるメモリアクセスのコスト削減は実用的なもので，[13] の予想の範囲内と考えられる．）

最新の dual-sieve 攻撃による影響　文献 [23] で新しい dual-sieve 攻撃が提案され，NIST 標準化で要求される古典ゲート数を下回ると主張している．しかし，その解析は理想的な理論モデルに基づき，オーバーヘッドが隠れている．また，LWE チャレンジで検証されている primal 攻撃に比べ，dual 攻撃の実用性の解析は進んでおらず，文献 [35] の指摘のように，dual 攻撃の成功確率は実際よりかなり高く見積もられている．したがって，文献 [23] の攻撃計算量は実際よりかなり小さく見積もられている可能性が高く，表 1.1 内のゲートコスト評価には影響しないと考えられる．

代数構造を利用した格子アルゴリズムの影響　加群格子上の BKZ 基底簡約は，$\mathbb{Z}$ 格子上のアルゴリズムと同程度の品質の基底を出力するか不明で，実用的な動作のための実装基盤も現時点では整備されていない．また，イデアル格子上の SVP に対する量子アルゴリズムは，Module-LWE への適用には障壁があり，文献 [56, Appendix C] の指摘のように，ML-KEM に対する実用的な攻撃に繋がる可能性は低い．以上から，現時点で，代数構造を利用したアルゴリズムは，代数構造を利用しないアルゴリズムよりも影響が大きいとは言えない．

参考文献

[1] Martin R Albrecht. On dual lattice attacks against small-secret LWE and parameter choices in HElib and SEAL. In *Advances in Cryptology–EUROCRYPT 2017*, volume 10211 of *Lecture Notes in Computer Science*, pages 103–129. Springer, 2017.

[2] Martin R. Albrecht, Benjamin R. Curtis, Amit Deo, Alex Davidson, Rachel Player, Eamonn W. Postlethwaite, Fernando Virdia, and Thomas Wunderer. Estimate all the {LWE, NTRU} schemes! In Dario Catalano and Roberto De Prisco, editors, *Security and Cryptography for Networks - 11th International Conference, SCN 2018, Amalfi, Italy, September 5-7, 2018, Proceedings*, volume 11035 of *Lecture Notes in Computer Science*, pages 351–367. Springer, 2018. `https://estimate-all-the-lwe-ntru-schemes.github.io/docs/`.

[3] Martin R. Albrecht and Amit Deo. Large modulus Ring-LWE $\geq$ Module-LWE. In Tsuyoshi Takagi and Thomas Peyrin, editors, *Advances in Cryptology - ASIACRYPT 2017 - 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part I*, volume 10624 of *Lecture Notes in Computer Science*, pages 267–296. Springer, 2017.

[4] Martin R Albrecht and Léo Ducas. Lattice attacks on NTRU and LWE: A history of refinements. In *Computational Cryptography: Algorithmic Aspects of Cryptology*, volume 469 of *London Mathematical Society Lecture Note Series*, pages 15–40. Cambridge University Press, 2021.

[5] Martin R. Albrecht, Léo Ducas, Gottfried Herold, Elena Kirshanova, Eamonn W. Postlethwaite, and Marc Stevens. The general sieve kernel and new records in lattice reduction. In Yuval Ishai and Vincent Rijmen, editors, *Advances in Cryptology - EUROCRYPT 2019 - 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19-23, 2019, Proceedings, Part II*, volume 11477 of *Lecture Notes in Computer Science*, pages 717–746. Springer, 2019.

[6] Martin R Albrecht, Vlad Gheorghiu, Eamonn W Postlethwaite, and John M Schanck. Estimating quantum speedups for lattice sieves. In *Advances in Cryptology–ASIACRYPT 2020*, volume 12492 of *Lecture Notes in Computer Science*, pages 583–613. Springer, 2020.

[7] Martin R. Albrecht, Florian Göpfert, Fernando Virdia, and Thomas Wunderer. Revisiting the expected cost of solving uSVP and applications to LWE. In Tsuyoshi Takagi and Thomas Peyrin, editors, *Advances in Cryptology - ASIACRYPT 2017 - 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part I*, volume 10624 of *Lecture Notes in Computer Science*, pages 297–322. Springer, 2017.

[8] Martin R Albrecht, Rachel Player, and Sam Scott. On the concrete hardness of learning with errors. *Journal of Mathematical Cryptology*, 9(3):169–203, 2015.

[9] Martin R Albrecht and Yixin Shen. Quantum augmented dual attack. *arXiv preprint arXiv:2205.13983*, 2022. `https://arxiv.org/pdf/2205.13983`.

[10] Erdem Alkim, Léo Ducas, Thomas Pöppelmann, and Peter Schwabe. Post-quantum key exchange - A new hope. In Thorsten Holz and Stefan Savage, editors, *25th USENIX Security Symposium, USENIX Security 16, Austin, TX, USA, August 10-12, 2016*, pages 327–343. USENIX Association, 2016.

[11] Yoshinori Aono, Yuntao Wang, Takuya Hayashi, and Tsuyoshi Takagi. Improved progressive BKZ algorithms and their precise cost estimation by sharp simulator. In *Advances in Cryptology–EUROCRYPT 2016*, volume 9665 of *Lecture Notes in Computer Science*, pages 789–819. Springer, 2016.

[12] Sanjeev Arora and Rong Ge. New algorithms for learning in presence of errors. In *International Colloquium on Automata, Languages, and Programming (ICALP 2011)*, volume 6755 of *Lecture Notes in Computer Science*, pages 403–415. Springer, 2011.

[13] Roberto Avanzi, Joppe Bos, Léo Ducas, Eike Kiltz, Tancréde Lepoint, Vadim Lyubashevsky, John M. Schanck, Peter Schwabe, Gregor Seiler, and Damien Stehlé. CRYSTALS-Kyber – algorithm specifications and supporting documentation (version 3.02). `https://pq-crystals.org/kyber/data/kyber-specification-round3-20210804.pdf`, 2021.

[14] Shi Bai and Steven D. Galbraith. Lattice decoding attacks on binary LWE. In Willy Susilo and Yi Mu, editors, *Information Security and Privacy - 19th Australasian Conference, ACISP 2014, Wollongong, NSW, Australia, July 7-9, 2014. Proceedings*, volume 8544 of *Lecture Notes in Computer Science*, pages 322–337. Springer, 2014.

[15] Anja Becker, Léo Ducas, Nicolas Gama, and Thijs Laarhoven. New directions in nearest neighbor searching with applications to lattice sieving. In *Proceedings of the twenty-seventh annual ACM-SIAM Symposium on Discrete Algorithms (SODA 2016)*, pages 10–24. SIAM, 2016.

[16] Buchmann Johannes Bernstein, Daniel J and Erik Dahmen. *Post-quantum cryptography*. Springer, 2009.

[17] Lei Bi, Xianhui Lu, Junjie Luo, and Kunpeng Wang. Hybrid dual and meet-LWE attack.

In *Information Security and Privacy (ACISP 2022)*, volume 13494 of *Lecture Notes in Computer Science*, pages 168–188. Springer, 2022.

[18] Jean-François Biasse and Fang Song. Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields. In *ACM-SIAM Symposium on Discrete Algorithms (SODA 2016)*, pages 893–902. SIAM, 2016.

[19] Nina Bindel, Johannes Buchmann, Florian Göpfert, and Markus Schmidt. Estimation of the hardness of the learning with errors problem with a restricted number of samples. *Journal of Mathematical Cryptology*, 13(1):47–67, 2019.

[20] Katharina Boudgoust, Corentin Jeudy, Adeline Roux-Langlois, and Weiqiang Wen. On the hardness of module learning with errors with short distributions. *Journal of Cryptology*, 36(1):1–70, 2023.

[21] Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan. (Leveled) fully homomorphic encryption without bootstrapping. *ACM Transactions on Computation Theory (TOCT)*, 6(3):1–36, 2014.

[22] Peter Campbell, Michael Groves, and Dan Shepherd. Soliloquy: A cautionary tale. ETSI 2nd quantum-safe crypto workshop, 2014, 2014. `https://docbox.etsi.org/workshop/2014/201410_CRYPTO/S07_Systems_and_Attacks/S07_Groves_Annex.pdf`.

[23] Kevin Carrier, Charles Meyer-Hilfiger, Yixin Shen, and Jean-Pierre Tillich. Assessing the impact of a variant of MATZOV's dual attack on Kyber. In *Advances in Cryptology–CRYPTO 2025*, volume 16000 of *Lecture Notes in Computer Science*, pages 444–476. Springer, 2025.

[24] Kevin Carrier, Yixin Shen, and Jean-Pierre Tillich. Faster dual lattice attacks by using coding theory. 2024. `https://hal.science/hal-04519755/document`.

[25] Yuanmi Chen. *Réduction de réseau et sécurité concrete du chiffrement completement homomorphe*. PhD thesis, Paris 7, 2013.

[26] Yuanmi Chen and Phong Q. Nguyen. BKZ 2.0: Better lattice security estimates. In Dong Hoon Lee and Xiaoyun Wang, editors, *Advances in Cryptology - ASIACRYPT 2011 - 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011. Proceedings*, volume 7073 of *Lecture Notes in Computer Science*, pages 1–20. Springer, 2011.

[27] Ronald Cramer, Léo Ducas, Chris Peikert, and Oded Regev. Recovering short generators of principal ideals in cyclotomic rings. In *Advances in Cryptology–EUROCRYPT 2016*, volume 9666 of *Lecture Notes in Computer Science*, pages 559–585. Springer, 2016.

[28] Ronald Cramer, Léo Ducas, and Benjamin Wesolowski. Short stickelberger class relations and application to ideal-svp. In *Advances in Cryptology–EUROCRYPT 2017*, volume 10210 of *Lecture Notes in Computer Science*, pages 324–348. Springer, 2017.

[29] Dana Dachman-Soled, Léo Ducas, Huijing Gong, and Mélissa Rossi. LWE with side information: Attacks and concrete security estimation. In *Advances in Cryptology–CRYPTO 2020*, volume 12171 of *Lecture Notes in Computer Science*, pages 329–358. Springer, 2020.

[30] TU Darmstadt and UC San Diego. LWE challenge. `https://www.latticechallenge.org/lwe_challenge/challenge.php`. 2025-12-31 閲覧.

[31] Gabrielle De Micheli and Daniele Micciancio. A fully classical LLL algorithm for modules. *Cryptology ePrint Archive, Paper 2022/1356*, 2022. `https://eprint.iacr.org/2022/1356.pdf`.

[32] Léo Ducas. Shortest vector from lattice sieving: a few dimensions for free. In *Advanves in Cryptology–EUROCRYPT 2018*, volume 10820 of *Lecture Notes in Computer Science*, pages 125–145. Springer, 2018.

[33] Léo Ducas. Estimating the hidden overheads in the BDGL lattice sieving algorithm. In *Post-Quantum Cryptography (PQCrypto 2022)*, volume 13512 of *Lecture Notes in Computer Science*, pages 480–497. Springer, 2022.

[34] Léo Ducas, Lynn Engelberts, and Paola de Perthuis. Predicting module-lattice reduction. In *Advances in Cryptology–ASIACRYPT 2025*, volume 16247 of *Lecture Notes in Computer Science*, pages 133–166. Springer, 2025.

[35] Léo Ducas and Ludo N Pulles. Does the dual-sieve attack on learning with errors even work? In *Advances in Cryptology–EUROCYPT 2023*, volume 14083 of *Lecture Notes in Computer Science*, pages 37–69. Springer, 2023.

[36] Jan-Pieter D' anvers and Senne Batsleer. Multitarget decryption failure attacks and their application to Saber and Kyber. In *Public-Key Cryptography (PKC 2022)*, volume 13177 of *Lecture Notes in Computer Science*, pages 3–33. Springer, 2022.

[37] Kirsten Eisenträger, Sean Hallgren, Alexei Kitaev, and Fang Song. A quantum algorithm for computing the unit group of an arbitrary degree number field. In *ACM Symposium on Theory of computing (STOC 2014)*, pages 293–302, 2014.

[38] Nicolas Gama and Phong Q Nguyen. Predicting lattice reduction. In *Advances in Cryptology–EUROCRYPT 2008*, volume 4965 of *Lecture Notes in Computer Science*, pages 31–51. Springer, 2008.

[39] Timo Glaser and Alexander May. How to enumerate LWE keys as narrow as in Kyber/Dilithium. In *Cryptology and Network Security (CANS 2023)*, volume 14342 of *Lecture Notes in Computer Science*, pages 75–100. Springer, 2023.

[40] Qian Guo and Thomas Johansson. Faster dual lattice attacks for solving LWE with applications to CRYSTALS. In *Advances in Cryptology–ASIACRYPT 2021*, volume 13093 of *Lecture Notes in Computer Science*, pages 33–62. Springer, 2021.

[41] Minki Hhan, Jiseung Kim, Changmin Lee, and Yongha Son. Let's meet ternary keys on Babai's plane: A hybrid of lattice-reduction and meet-LWE. *Cryptology ePrint Archive,*

Paper 2022/1473, 2022. https://eprint.iacr.org/2022/1473.

[42] Dennis Hofheinz, Kathrin Hövelmanns, and Eike Kiltz. A modular analysis of the Fujisaki-Okamoto transformation. In Yael Kalai and Leonid Reyzin, editors, *Theory of Cryptography - 15th International Conference, TCC 2017, Baltimore, MD, USA, November 12-15, 2017, Proceedings, Part I*, volume 10677 of *Lecture Notes in Computer Science*, pages 341–371. Springer, 2017.

[43] Nick Howgrave-Graham. A hybrid lattice-reduction and meet-in-the-middle attack against NTRU. In *Advances in Cryptology–CRYPTO 2007*, volume 4622 of *Lecture Notes in Computer Science*, pages 150–169. Springer, 2007.

[44] Internet Engineering Task Force (IETF). Post-quantum cryptography for engineers, February 2024. https://datatracker.ietf.org/doc/html/draft-ietf-pquip-pqc-engineers-03.

[45] Ravi Kannan. Improved algorithms for integer programming and related lattice problems. In David S. Johnson, Ronald Fagin, Michael L. Fredman, David Harel, Richard M. Karp, Nancy A. Lynch, Christos H. Papadimitriou, Ronald L. Rivest, Walter L. Ruzzo, and Joel I. Seiferas, editors, *Proceedings of the 15th Annual ACM Symposium on Theory of Computing, 25-27 April, 1983, Boston, Massachusetts, USA*, pages 193–206. ACM, 1983.

[46] Jiseung Kim, Changmin Lee, and Yongha Son. Worst-case analysis of lattice enumeration algorithm over modules. *Cryptology ePrint Archive, Paper 2025/480*, 2025. https://eprint.iacr.org/2025/480.pdf.

[47] Paul Kirchner and Pierre-Alain Fouque. An improved BKW algorithm for LWE with applications to cryptography and lattices. In *Advances in Cryptology–CRYPTO 2015*, volume 9215 of *Lecture Notes in Computer Science*, pages 43–62. Springer, 2015.

[48] Thijs Laarhoven. Search problems in cryptography: from fingerprinting to lattice sieving. *PhD thesis, Eindhoven University of Technology*, 2016. https://pure.tue.nl/ws/files/14673128/20160216_Laarhoven.pdf.

[49] Thijs Laarhoven and Artur Mariano. Progressive lattice sieving. In *Post-Quantum Cryptography (PQCrypto 2018)*, volume 10786 of *Lecture Notes in Computer Science*, pages 292–311. Springer, 2018.

[50] Thijs Laarhoven, Michele Mosca, and Joop Van De Pol. Finding shortest lattice vectors faster using quantum search. *Designs, Codes and Cryptography*, 77(2):375–400, 2015.

[51] Adeline Langlois and Damien Stehlé. Worst-case to average-case reductions for module lattices. *Des. Codes Cryptogr.*, 75(3):565–599, 2015.

[52] Changmin Lee, Alice Pellet-Mary, Damien Stehlé, and Alexandre Wallet. An LLL algorithm for module lattices. In *Advances in Cryptology–ASIACRYPT 2019*, volume 11922 of *Lecture Notes in Computer Science*, pages 59–90. Springer, 2019.

[53] A. K. Lenstra, H. W. Lenstra, and Lovász L. Factoring polynomials with rational coeffi-

cients. *Mathematische Annalen*, 261(4):515–534, 12 1982.

[54] Cathy Yuanchen Li, Jana Sotáková, Emily Wenger, Mohamed Malhou, Evrard Garcelon, François Charton, and Kristin Lauter. SalsaPicante: A machine learning attack on LWE with binary secrets. In *ACM SIGSAC Conference on Computer and Communications Security (ACM CCS 2023)*, pages 2606–2620, 2023.

[55] Richard Lindner and Chris Peikert. Better key sizes (and attacks) for LWE-based encryption. In Aggelos Kiayias, editor, *Topics in Cryptology - CT-RSA 2011 - The Cryptographers' Track at the RSA Conference 2011, San Francisco, CA, USA, February 14-18, 2011. Proceedings*, volume 6558 of *Lecture Notes in Computer Science*, pages 319–339. Springer, 2011.

[56] National lnstitute of Standards and Technology (NIST). NIST IR 8413-upd1: Status report on the third round of the NIST post-quantum cryptography standardization process. 2022. `https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8413-upd1.pdf`.

[57] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On ideal lattices and learning with errors over rings. In Henri Gilbert, editor, *Advances in Cryptology - EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Monaco / French Riviera, May 30 - June 3, 2010. Proceedings*, volume 6110 of *Lecture Notes in Computer Science*, pages 1–23. Springer, 2010.

[58] Artur Mariano, Thijs Laarhoven, and Christian Bischof. A parallel variant of LDSieve for the SVP on lattices. In *2017 25th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP)*, pages 23–30. IEEE, 2017.

[59] MATZOV. Report on the security of LWE: Improved dual lattice attack, 2022. `https://zenodo.org/records/6412487`.

[60] Alexander May. How to meet ternary LWE keys. In *Advances in Cryptology–CRYPTO 2021*, volume 12826 of *Lecture Notes in Computer Science*, pages 701–731. Springer, 2021.

[61] Tamalika Mukherjee and Noah Stephens-Davidowitz. Lattice reduction for modules, or how to reduce ModuleSVP to ModuleSVP. In *Advances in Cryptology–CRYPTO 2020*, volume 12171 of *Lecture Notes in Computer Science*, pages 213–242. Springer, 2020.

[62] National Institute of Standards and Technology (NIST). FIPS 202: SHA-3 standard: Permutation-based hash and extendable-output functions. `https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf`, August 2015.

[63] National Institute of Standards and Technology (NIST). Submission requirements and evaluation criteria for the post-quantum cryptography standardization process, 2016. `https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf`.

[64] National Institute of Standards and Technology (NIST). FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard. `https://nvlpubs.nist.gov/nistpubs/FIPS/`

NIST.FIPS.203.pdf, August 13, 2024.

[65] Eamonn W. Postlethwaite and Fernando Virdia. On the success probability of solving unique SVP via BKZ. In Juan A. Garay, editor, *Public-Key Cryptography - PKC 2021 - 24th IACR International Conference on Practice and Theory of Public Key Cryptography, Virtual Event, May 10-13, 2021, Proceedings, Part I*, volume 12710 of *Lecture Notes in Computer Science*, pages 68–98. Springer, 2021.

[66] Gokulnath Rajendran, Prasanna Ravi, Jan-Pieter D'anvers, Shivam Bhasin, and Anupam Chattopadhyay. Pushing the limits of generic side-channel attacks on LWE-based KEMs-parallel PC oracle attacks on Kyber KEM and beyond. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2023(2):418–446, 2023.

[67] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In Harold N. Gabow and Ronald Fagin, editors, *Proceedings of the 37th Annual ACM Symposium on Theory of Computing, Baltimore, MD, USA, May 22-24, 2005*, pages 84–93. ACM, 2005.

[68] Oded Regev. The learning with errors problem (invited survey). In *Proceedings of the 25th Annual IEEE Conference on Computational Complexity, CCC 2010, Cambridge, Massachusetts, USA, June 9-12, 2010*, pages 191–204. IEEE Computer Society, 2010.

[69] Tsunekazu Saito, Keita Xagawa, and Takashi Yamakawa. Tightly-secure key-encapsulation mechanism in the quantum random oracle model. In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part III*, volume 10822 of *Lecture Notes in Computer Science*, pages 520–551. Springer, 2018.

[70] Claus Peter Schnorr. Lattice reduction by random sampling and birthday methods. In *Symposium on Theoretical Aspects of Computer Science (STACS 2003)*, volume 2607 of *Lecture Notes in Computer Science*, pages 145–156. Springer, 2003.

[71] Claus-Peter Schnorr and M. Euchner. Lattice basis reduction: Improved practical algorithms and solving subset sum problems. *Math. Program.*, 66:181–199, 1994.

[72] Samuel Stevens, Emily Wenger, Cathy Li, Niklas Nolte, Eshika Saxena, François Charton, and Kristin Lauter. Salsa Fresca: Angular embeddings and pre-training for ML attacks on learning with errors. *arXiv preprint arXiv:2402.01082*, 2024. https://arxiv.org/pdf/2402.01082.

[73] Yutaro Tanaka, Rei Ueno, Keita Xagawa, Akira Ito, Junko Takahashi, and Naofumi Homma. Multiple-valued plaintext-checking side-channel attacks on post-quantum KEMs. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2023(3):473–503, 2023.

[74] Emily Wenger, Mingjie Chen, Francois Charton, and Kristin E Lauter. SALSA: Attack-

ing lattice cryptography with transformers. *Advances in Neural Information Processing Systems (NeurIPS 2022)*, 35:34981–34994, 2022.

[75] Emily Wenger, Eshika Saxena, Mohamed Malhou, Ellie Thieu, and Kristin Lauter. Benchmarking attacks on learning with errors. In *IEEE Symposium on Security and Privacy (SP)*, pages 279–297. IEEE, 2025.

[76] Han Wu and Guangwu Xu. Enhancing the dual attack against MLWE: Constructing more short vectors using its algebraic structure. *Cryptology ePrint Archive, Paper 2022/1661*, 2022. `https://eprint.iacr.org/2022/1661`.

[77] Keita Xagawa, Akira Ito, Rei Ueno, Junko Takahashi, and Naofumi Homma. Fault-injection attacks against NIST's post-quantum cryptography round 3 KEM candidates. In *Advances in Cryptology–ASIACRYPT 2021*, volume 13091 of *Lecture Notes in Computer Science*, pages 33–61. Springer, 2021.

[78] Yang Yu and Léo Ducas. Second order statistical behavior of LLL and BKZ. In Carlisle Adams and Jan Camenisch, editors, *Selected Areas in Cryptography (SAC 2017) - 24th International Conference, Ottawa, ON, Canada, August 16-18, 2017, Revised Selected Papers*, volume 10719 of *Lecture Notes in Computer Science*, pages 3–22. Springer, 2017.

[79] Ziyu Zhao, Jintai Ding, and Bo-Yin Yang. Sieving with streaming memory access. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2025(2):362–384, 2025.

CRYPTREC: ML-KEM Evaluation Report

PQShield

Thomas Espitau, Shuichi Katsumata, Niels Samwel, Thom Wiggers, Wessel van Woerden, Timo Zijlstra

Executive Summary

Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM) is a lattice-based key encapsulation mechanism (KEM), standardized by the U.S. National Institute of Standards and Technology (NIST) as Federal Information Processing Standard (FIPS) 203 [Nat24b] in August, 2024. It is derived from CRYSTALS-KYBER [Ava+21] and designed to provide confidentiality against attackers equipped with large-scale quantum computers. The evaluation covers the scheme's design rationale, provable security guarantees, concrete hardness against cryptanalytic attacks, implementation security regarding side-channels, and its applicability in secure network protocols such as TLS 1.3. The following is a summary of ML-KEM.

Construction: The scheme is based on the Fujisaki-Okamoto transform, transforming a base INDCPA secure public key encryption scheme called KPKE into an IND-CCA secure KEM. It has a non-zero but negligible decryption failure rate (2^{-139} to 2^{-174}), which is deemed operationally safe and does not pose a security risk under correct implementation.

Provable Security: It's security is based on the *Module Learning with Errors* (MLWE) problem, a structured variant of the standard LWE problem that balances efficiency with security. Tight reductions exist in the classical random oracle model (ROM). In the quantum ROM, while reductions are asymptotically looser, they still provide sufficient confidence in the scheme' s resistance to quantum adversaries.

Security Margins: Concrete cost estimates for the best known attacks (using conservative cost models such as Core-SVP and MATZOV) indicate that all ML-KEM parameter sets meet or exceed their targeted NIST security levels.

Algebraic Structure: Attacks exploiting the algebraic structure of module lattices (e.g., ideal lattice attacks) were analyzed. The report concludes that for the specific module ranks used in ML-KEM ($k \in \{2, 3, 4\}$), these structured attacks do not outperform generic lattice reduction techniques.

Performance: ML-KEM demonstrates excellent performance in software and hardware, significantly outperforming traditional elliptic-curve cryptography (ECC) in computation time, although key and ciphertext sizes are larger.

Side-Channel Attacks: Unprotected implementations are vulnerable to side-channel attacks, including differential power analysis and timing attacks on decryption failures.

Countermeasures: Effective countermeasures such as masking (arithmetic and boolean) and shuffling are available. While these introduce performance overheads, they are necessary for high-assurance deployments in hostile environments.

Application to TLS 1.3: ML-KEM is fully viable for TLS 1.3. The larger key sizes (encapsulation keys and ciphertexts) increase handshake traffic but result in negligible impact on overall connection latency in most network scenarios. The report discuss the use of "hybrid" key exchange mechanisms, combining ML-KEM with traditional elliptic-curve Diffie-Hellman (ECDH), as a robust transition strategy to mitigate risks associated with new cryptographic primitives.

Based on current cryptanalytic knowledge, ML-KEM is a robust and secure post-quantum KEM. Its theoretical foundations are sound, and its parameter sets provide adequate security margins against known classical and quantum threats. While it offers faster processing speeds compared to traditional cryptographic schemes, the increased key and ciphertext sizes may present implementation challenges for memory-constrained devices. However, it is judged to be viable for use in other general-purpose applications without issues. Furthermore, provided that implementations are rigorously protected against side-channel attacks, it is suitable for widespread deployment in government and critical infrastructure systems.

エグゼクティブ・サマリー

Module-Lattice-Based Key-Encapsulation Mechanism（ML-KEM）は，モジュール格子に基づく鍵カプセル化メカニズム（KEM）であり，2024 年 8 月に，米国国立標準技術研究所（NIST）によって連邦情報処理標準 FIPS203 として標準化された．本方式は CRYSTALS-KYBER [Ava+21] から派生したものであり，大規模な量子計算機に対しても安全であるように設計されている．本評価は，方式の設計根拠，証明可能安全性，暗号解読攻撃に対する具体的な困難性，サイドチャネルに関する実装セキュリティ，および TLS 1.3 などのインターネット通信を保護する暗号化プロトコルへの適用可能性を網羅している．以下，評価内容の概要を述べる．

構成：本方式は藤崎・岡本変換に基づいており，IND-CPA 安全な公開鍵暗号方式である KPKE を，IND-CCA 安全な KEM に変換している．本方式はゼロではないが無視可能な復号失敗率（2^{-139} から 2^{-174}）を持つ．これは運用上安全であるとみなされ，正しく実装されている限り安全性を損ねるものではない．

証明可能安全性：安全性は，*Module Learning with Errors*（MLWE）問題に基づいている．これは，効率性と安全性のバランスをとるために，標準的な LWE 問題を構造化した変種である．古典的ランダムオラクルモデル（ROM）においては緊密な帰着が存在する．量子 ROM においては，帰着は漸近的に緩くなるものの，量子敵対者に対する耐性について十分な信頼性を与えるものである．

セキュリティマージン：既知の最良の攻撃に対する具体的なコスト見積もり（Core-SVP や MATZOV などの保守的なコストモデルを使用）は，すべての ML-KEM パラメータセットが，目標とする NIST 安全性レベルを満たしているか，あるいは上回っていることを示している．

代数的構造：モジュール格子の代数的構造を利用する攻撃（例：イデアル格子攻撃）についても分析を行った．本報告書では，ML-KEM で使用される特定のモジュールランク（$k \in \{2, 3, 4\}$）において，これらの構造を利用した攻撃は，構造を利用しない一般的な格子基底簡約アルゴリズムを上回るものではないと結論付ける．

性能：ML-KEM はソフトウェアおよびハードウェアにおいて優れたパフォーマンスを示し，鍵や暗号文のサイズは大きくなるものの，計算時間については従来の楕円曲線暗号（ECC）より大幅に高速である．

サイドチャネル攻撃：対策が施されていない実装は，電力差分解析や復号失敗に対するタイミング攻撃などのサイドチャネル攻撃に対して脆弱である．

対策：マスキング（算術およびブール）やシャフリングといった効果的な対策が利用可能である．これらは効率性を損なう対策だが，敵対的な環境における安全性を保証するために不可欠である．

TLS 1.3 への適用：ML-KEM は TLS 1.3 において十分に利用可能である．鍵長（カプセル化鍵および暗号文）の増大によりハンドシェイクのデータ送量は増加するが，多くのネットワークシナリオにおいて，全体的な接続遅延時間への影響は無視できる範囲である．本報告書では，新しい暗号プリミティブに伴うリスクを軽減するための堅牢な移行戦略として，ML-KEM と従来の楕円曲線 Diffie-Hellman（ECDH）を組み合わせたハイブリッド鍵交換メカニズムの性能についても言及する．

現在の暗号解析に関する知見に基づき，ML-KEM は堅牢かつ安全な耐量子 KEM であると考える．その理論的基盤は健全であり，各パラメータセットは既知の古典，および，量子の暗号解析アルゴリズムに対して十分なセキュリティマージンを提供している．計算時間は従来の暗号方式に比べより高速である一方で，鍵や暗号文長は増加するため，メモリ制約があるデバイス等においては実装上の課題が生じる可能性がある．しかし，それ以外の用途においては問題なく利用できると判断される．また，サイドチャネル攻撃に対して厳密に保護された実装が行われることを前提として，政府および重要インフラシステムへの広範な展開にも適している．

References

[Abd+05] Michel Abdalla, Mihir Bellare, Dario Catalano, Eike Kiltz, Tadayoshi Kohno, Tanja Lange, John Malone-Lee, Gregory Neven, Pascal Paillier, and Haixia Shi. "Searchable Encryption Revisited: Consistency Properties, Relation to Anonymous IBE, and Extensions". In: *CRYPTO 2005*. Ed. by Victor Shoup. Vol. 3621. LNCS. Springer, Berlin, Heidelberg, Aug. 2005, pp. 205–222. DOI: 10.1007/11535218_13.

[ABD16] Martin R. Albrecht, Shi Bai, and Léo Ducas. "A Subfield Lattice Attack on Overstretched NTRU Assumptions - Cryptanalysis of Some FHE and Graded Encoding Schemes". In: *CRYPTO 2016, Part I*. Ed. by Matthew Robshaw and Jonathan Katz. Vol. 9814. LNCS. Springer, Berlin, Heidelberg, Aug. 2016, pp. 153–178. DOI: 10.1007/978-3-662-53018-4_6.

[ABN10] Michel Abdalla, Mihir Bellare, and Gregory Neven. "Robust Encryption". In: *TCC 2010*. Ed. by Daniele Micciancio. Vol. 5978. LNCS. Springer, Berlin, Heidelberg, Feb. 2010, pp. 480–497. DOI: 10.1007/978-3-642-11799-2_28.

[ACW19] Martin R. Albrecht, Benjamin R. Curtis, and Thomas Wunderer. "Exploring Trade-offs in Batch Bounded Distance Decoding". In: *SAC 2019*. Ed. by Kenneth G. Paterson and Douglas Stebila. Vol. 11959. LNCS. Springer, Cham, Aug. 2019, pp. 467–491. DOI: 10.1007/978-3-030-38471-5_19.

[AD21] Martin Albrecht and Léo Ducas. *Lattice Attacks on NTRU and LWE: A History of Refinements*. Cryptology ePrint Archive, Report 2021/799. 2021. URL: https://eprint.iacr.org/2021/799.

[Adr+24] David Adrian, Bob Beck, David Benjamin, and Devon O'Brien. *Advancing Our Amazing Bet on Asymmetric Cryptography*. May 23, 2024. URL: https://blog.chromium.org/2024/05/advancing-our-amazing-bet-on-asymmetric.html.

[Aes] *Advanced Encryption Standard (AES)*. National Institute of Standards and Technology, NIST FIPS PUB 197, U.S. Department of Commerce. Nov. 2001.

[AFG14] Martin R. Albrecht, Robert Fitzpatrick, and Florian Göpfert. "On the Efficacy of Solving LWE by Reduction to Unique-SVP". In: *ICISC 13*. Ed. by Hyang-Sook Lee and Dong-Guk Han. Vol. 8565. LNCS. Springer, Cham, Nov. 2014, pp. 293–310. DOI: 10.1007/978-3-319-12160-4_18.

[AG11] Sanjeev Arora and Rong Ge. "New Algorithms for Learning in Presence of Errors". In: *ICALP 2011, Part I*. Ed. by Luca Aceto, Monika Henzinger, and Jiri Sgall. Vol. 6755. LNCS. Springer, Berlin, Heidelberg, July 2011, pp. 403–415. DOI: 10.1007/978-3-642-22006-7_34.

[Agg+20] Divesh Aggarwal, Jianwei Li, Phong Q. Nguyen, and Noah Stephens-Davidowitz. "Slide Reduction, Revisited - Filling the Gaps in SVP Approximation". In: *CRYPTO 2020, Part II*. Ed. by Daniele Micciancio and Thomas Ristenpart. Vol. 12171. LNCS. Springer, Cham, Aug. 2020, pp. 274–295. DOI: 10.1007/978-3-030-56880-1_10.

[Alb+14] Martin R. Albrecht, Carlos Cid, Jean-Charles Faugère, and Ludovic Perret. *Algebraic Algorithms for LWE*. Cryptology ePrint Archive, Report 2014/1018. 2014. URL: https://eprint.iacr.org/2014/1018.

[Alb17] Martin R. Albrecht. "On Dual Lattice Attacks Against Small-Secret LWE and Parameter Choices in HElib and SEAL". In: *EUROCRYPT 2017, Part II*. Ed. by Jean-Sébastien Coron and Jesper Buus Nielsen. Vol. 10211. LNCS. Springer, Cham, 2017, pp. 103–129. DOI: 10.1007/978-3-319-56614-6_4.

[Alb+19] Martin R. Albrecht, Léo Ducas, Gottfried Herold, Elena Kirshanova, Eamonn W. Postlethwaite, and Marc Stevens. "The General Sieve Kernel and New Records in Lattice Reduction". In: *EUROCRYPT 2019, Part II*. Ed. by Yuval Ishai and Vincent Rijmen. Vol. 11477. LNCS. Springer, Cham, May 2019, pp. 717–746. DOI: 10.1007/978-3-030-17656-3_25.

[Alb+20a] Martin R. Albrecht, Shi Bai, Pierre-Alain Fouque, Paul Kirchner, Damien Stehlé, and Weiqiang Wen. "Faster Enumeration-Based Lattice Reduction: Root Hermite Factor $k^{1/(2k)}$ Time $k^{k/8+o(k)}$". In: *CRYPTO 2020, Part II*. Ed. by Daniele Micciancio and Thomas Ristenpart. Vol. 12171. LNCS. Springer, Cham, Aug. 2020, pp. 186–212. DOI: 10.1007/978-3-030-56880-1_7.

[Alb+20b] Martin R. Albrecht, Vlad Gheorghiu, Eamonn W. Postlethwaite, and John M. Schanck. "Estimating Quantum Speedups for Lattice Sieves". In: *ASIACRYPT 2020, Part II*. Ed. by Shiho Moriai and Huaxiong Wang. Vol. 12492. LNCS. Springer, Cham, Dec. 2020, pp. 583–613. DOI: 10.1007/978-3-030-64834-3_20.

[Alb+21] Martin R. Albrecht, Shi Bai, Jianwei Li, and Joe Rowell. "Lattice Reduction with Approximate Enumeration Oracles - Practical Algorithms and Concrete Performance". In: *CRYPTO 2021, Part II*. Ed. by Tal Malkin and Chris Peikert. Vol. 12826. LNCS. Virtual Event: Springer, Cham, Aug. 2021, pp. 732–759. DOI: 10.1007/978-3-030-84245-1_25.

[Alk+16] Erdem Alkim, Léo Ducas, Thomas Pöppelmann, and Peter Schwabe. "Post-quantum Key Exchange - A New Hope". In: *USENIX Security 2016*. Ed. by Thorsten Holz and Stefan Savage. USENIX Association, Aug. 2016, pp. 327–343. URL: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/alkim.

[Alm+24] José Bacelar Almeida, Santiago Arranz Olmos, Manuel Barbosa, Gilles Barthe, François Dupressoir, Benjamin Grégoire, Vincent Laporte, Jean-Christophe Léchenet, Cameron Low, Tiago Oliveira, Hugo Pacheco, Miguel Quaresma, Peter Schwabe, and Pierre-Yves Strub. "Formally Verifying Kyber - Episode V: Machine-Checked IND-CCA Security and Correctness of ML-KEM in EasyCrypt". In: *CRYPTO 2024, Part II*. Ed. by Leonid Reyzin and Douglas Stebila. Vol. 14921. LNCS. Springer, Cham, Aug. 2024, pp. 384–421. DOI: 10.1007/978-3-031-68379-4_12.

[Alp+24] Estuardo Alpirez Bock, Gustavo Banegas, Chris Brzuska, Lukasz Chmielewski, Kirthivaasan Puniamurthy, and Milan Sorf. "Breaking DPA-Protected Kyber via the Pair-Pointwise Multiplication". In: *ACNS 2024, Part II*. Ed. by Christina Pöpper and Lejla Batina. Vol. 14584. LNCS. Springer, Cham, Mar. 2024, pp. 101–130. DOI: 10.1007/978-3-031-54773-7_5.

[ANS23] ANSSI. *ANSSI views on the Post-Quantum Cryptography transition (2023 follow up)*. Dec. 21, 2023. URL: https://messervices.cyber.gouv.fr/documents-guides/follow_up_position_paper_on_post_quantum_cryptography.pdf.

[Aon+16] Yoshinori Aono, Yuntao Wang, Takuya Hayashi, and Tsuyoshi Takagi. "Improved Progressive BKZ Algorithms and Their Precise Cost Estimation by Sharp Simulator". In: *EUROCRYPT 2016, Part I*. Ed. by Marc Fischlin and Jean-Sébastien Coron. Vol. 9665. LNCS. Springer, Berlin, Heidelberg, May 2016, pp. 789–819. DOI: 10.1007/978-3-662-49890-3_30.

[App] Apple. *Network.framework*. URL: https://developer.apple.com/documentation/network/.

[App+09] Benny Applebaum, David Cash, Chris Peikert, and Amit Sahai. "Fast Cryptographic Primitives and Circular-Secure Encryption Based on Hard Learning Problems". In: *CRYPTO 2009*. Ed. by Shai Halevi. Vol. 5677. LNCS. Springer, Berlin, Heidelberg, Aug. 2009, pp. 595–618. DOI: 10.1007/978-3-642-03356-8_35.

[App25] Apple. *Prepare your network for quantum-secure encryption in TLS*. July 23, 2025. URL: https://support.apple.com/en-me/122756.

[APS15] Martin R. Albrecht, Rachel Player, and Sam Scott. "On the concrete hardness of Learning with Errors". In: *Journal of Mathematical Cryptology* 9.3 (2015), pp. 169–203. DOI: doi:10.1515/jmc-2015-0016. URL: https://doi.org/10.1515/jmc-2015-0016.

[ARM] ARM Limited. *mbed TLS*. URL: https://tls.mbed.org/.

[Aus25] Australian Signals Directorate. *Guidelines for Cryptography*. Information Security Manual (ISM), first published 4 December 2025, last updated 4 December 2025. Dec. 2025. URL: https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism/cyber-security-guidelines/guidelines-for-cryptography (visited on 01/13/2026).

[Ava+21] Roberto Avanzi, Joppe W. Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M. Schanck, Peter Schwabe, Gregor Seiler, and Damien Stehlé. *CRYSTALS-Kyber: Algorithm Specifications and Supporting Documentation (version 3.02)*. Submission to NIST PQC Round 3. Version 3.02. Aug. 2021. URL: https://pq-crystals.org/kyber/data/kyber-specification-round3-20210804.pdf.

[Bac+23] Linus Backlund, Kalle Ngo, Joel Gärtner, and Elena Dubrova. "Secret Key Recovery Attack on Masked and Shuffled Implementations of CRYSTALS-Kyber and Saber". In: *Applied Cryptography and Network Security Workshops: ACNS 2023 Satellite Workshops, ADSC, AIBlock, AIHWS, AIoTS, CIMSS, Cloud S&P, SCI, SecMT, SiMLA, Kyoto, Japan, June 19–22, 2023, Proceedings*. Kyoto, Japan: Springer-Verlag, 2023, pp. 159–177. DOI: 10.1007/978-3-031-41181-6_9.

[Bar+25] Manuel Barbosa, Matthias J Kannwischer, Thing-han Lim, Peter Schwabe, and Pierre-Yves Strub. *Formally Verified Correctness Bounds for Lattice-Based Cryptography*. To Appear in *ACM CCS 2025*. 2025. URL: https://eprint.iacr.org/2025/1562.

[BDF20] Koen de Boer, Léo Ducas, and Serge Fehr. "On the Quantum Complexity of the Continuous Hidden Subgroup Problem". In: *EUROCRYPT 2020, Part II*. Ed. by Anne Canteaut and Yuval Ishai. Vol. 12106. LNCS. Springer, Cham, May 2020, pp. 341–370. DOI: 10.1007/978-3-030-45724-2_12.

[Bec+16] Anja Becker, Léo Ducas, Nicolas Gama, and Thijs Laarhoven. "New directions in nearest neighbor searching with applications to lattice sieving". In: *27th SODA*. Ed. by Robert Krauthgamer. ACM-SIAM, Jan. 2016, pp. 10–24. DOI: 10.1137/1.9781611974331.ch2.

[Bel+01] Mihir Bellare, Alexandra Boldyreva, Anand Desai, and David Pointcheval. "Key-Privacy in Public-Key Encryption". In: *ASIACRYPT 2001*. Ed. by Colin Boyd. Vol. 2248. LNCS. Springer, Berlin, Heidelberg, Dec. 2001, pp. 566–582. DOI: 10.1007/3-540-45682-1_33.

[Ber06] Daniel J. Bernstein. "Curve25519: New Diffie-Hellman Speed Records". In: *PKC 2006*. Ed. by Moti Yung, Yevgeniy Dodis, Aggelos Kiayias, and Tal Malkin. Vol. 3958. LNCS. Springer, Berlin, Heidelberg, Apr. 2006, pp. 207–228. DOI: 10.1007/11745853_14.

[Ber22] Daniel J. Bernstein. *Multi-ciphertext security degradation for lattices*. Cryptology ePrint Archive, Report 2022/1580. 2022. URL: https://eprint.iacr.org/2022/1580.

[Ber23] Daniel J. Bernstein. *Asymptotics of hybrid primal lattice attacks*. Cryptology ePrint Archive, Report 2023/1892. 2023. URL: https://eprint.iacr.org/2023/1892.

[BF14] Jean-François Biasse and Claus Fieker. "Subexponential class group and unit group computation in large degree number fields". In: *LMS Journal of Computation and Mathematics* 17.A (2014), pp. 385–403. DOI: 10.1112/S1461157014000345.

[BF25] Koen de Boer and Joël Felderhoff. "Quantumly Computing S-unit Groups in Quantified Polynomial Time and Space". In: *Cryptology ePrint Archive* (2025).

[BGJ15] Anja Becker, Nicolas Gama, and Antoine Joux. *Speeding-up lattice sieving without increasing the memory, using sub-quadratic nearest neighbor search*. Cryptology ePrint Archive, Report 2015/522. 2015. URL: https://eprint.iacr.org/2015/522.

[Bha+21] Shivam Bhasin, Jan-Pieter D'Anvers, Daniel Heinz, Thomas Pöppelmann, and Michiel Van Beirendonck. "Attacking and Defending Masked Polynomial Comparison". In: *IACR TCHES* 2021.3 (2021), pp. 334–359. ISSN: 2569-2925. DOI: 10.46586/tches.v2021.i3.334-359. URL: https://tches.iacr.org/index.php/TCHES/article/view/8977.

[Bia+17] Jean-François Biasse, Thomas Espitau, Pierre-Alain Fouque, Alexandre Gélin, and Paul Kirchner. "Computing Generator in Cyclotomic Integer Rings - A Subfield Algorithm for the Principal Ideal Problem in $L_{|\Delta_{\mathbb{K}}|}(\frac{1}{2})$ and Application to the Cryptanalysis of a FHE Scheme". In: *EUROCRYPT 2017, Part I*. Ed. by Jean-Sébastien Coron and Jesper Buus Nielsen. Vol. 10210. LNCS. Springer, Cham, 2017, pp. 60–88. DOI: 10.1007/978-3-319-56620-7_3.

[Bin+19] Nina Bindel, Mike Hamburg, Kathrin Hövelmanns, Andreas Hülsing, and Edoardo Persichetti. "Tighter Proofs of CCA Security in the Quantum Random Oracle Model". In: *TCC 2019, Part II*. Ed. by Dennis Hofheinz and Alon Rosen. Vol. 11892. LNCS. Springer, Cham, Dec. 2019, pp. 61–90. DOI: 10.1007/978-3-030-36033-7_3.

[BKW00] Avrim Blum, Adam Kalai, and Hal Wasserman. "Noise-tolerant learning, the parity problem, and the statistical query model". In: *32nd ACM STOC*. ACM Press, May 2000, pp. 435–440. DOI: 10.1145/335305.335355.

[BL16] Anja Becker and Thijs Laarhoven. "Efficient (Ideal) Lattice Sieving Using Cross-Polytope LSH". In: *AFRICACRYPT 16*. Ed. by David Pointcheval, Abderrahmane Nitaj, and Tajjeeddine Rachidi. Vol. 9646. LNCS. Springer, Cham, Apr. 2016, pp. 3–23. DOI: 10.1007/978-3-319-31517-1_1.

[BLS16] Shi Bai, Thijs Laarhoven, and Damien Stehlé. "Tuple lattice sieving". In: *LMS Journal of Computation and Mathematics* 19.A (2016), pp. 146–162. DOI: 10.1112/S1461157016000292.

[Bon+11] Dan Boneh, Özgür Dagdelen, Marc Fischlin, Anja Lehmann, Christian Schaffner, and Mark Zhandry. "Random Oracles in a Quantum World". In: *ASIACRYPT 2011*. Ed. by Dong Hoon Lee and Xiaoyun Wang. Vol. 7073. LNCS. Springer, Berlin, Heidelberg, Dec. 2011, pp. 41–69. DOI: 10.1007/978-3-642-25385-0_3.

[Bon+23] Xavier Bonnetain, André Chailloux, André Schrottenloher, and Yixin Shen. "Finding Many Collisions via Reusable Quantum Walks: Application to Lattice Sieving". In: *EUROCRYPT 2023, Part V*. Ed. by Carmit Hazay and Martijn Stam. Vol. 14008. LNCS. Springer, Cham, Apr. 2023, pp. 221–251. DOI: 10.1007/978-3-031-30589-4_8.

[Bos+15] Joppe W. Bos, Craig Costello, Michael Naehrig, and Douglas Stebila. "Post-Quantum Key Exchange for the TLS Protocol from the Ring Learning with Errors Problem". In: *2015 IEEE Symposium on Security and Privacy*. IEEE Computer Society Press, May 2015, pp. 553–570. DOI: 10.1109/SP.2015.40.

[Bos+16] Joppe W. Bos, Craig Costello, Léo Ducas, Ilya Mironov, Michael Naehrig, Valeria Nikolaenko, Ananth Raghunathan, and Douglas Stebila. "Frodo: Take off the Ring! Practical, Quantum-Secure Key Exchange from LWE". In: *ACM CCS 2016*. Ed. by Edgar R. Weippl, Stefan Katzenbeisser, Christopher Kruegel, Andrew C. Myers, and Shai Halevi. ACM Press, Oct. 2016, pp. 1006–1018. DOI: 10.1145/2976749.2978425.

[Bos+18] Joppe W. Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M. Schanck, Peter Schwabe, Gregor Seiler, and Damien Stehlé. "CRYSTALS - Kyber: A CCA-Secure Module-Lattice-Based KEM". In: *2018 IEEE European Symposium on Security and Privacy*. IEEE Computer Society Press, Apr. 2018, pp. 353–367. DOI: 10.1109/EuroSP.2018.00032.

[Bos+21] Joppe W. Bos, Marc Gourjon, Joost Renes, Tobias Schneider, and Christine van Vredendaal. "Masking Kyber: First- and Higher-Order Implementations". In: *IACR TCHES* 2021.4 (2021), pp. 173–214. ISSN: 2569-2925. DOI: 10.46586/tches.v2021.i4.173-214. URL: https://tches.iacr.org/index.php/TCHES/article/view/9064.

[Bou+21] Katharina Boudgoust, Corentin Jeudy, Adeline Roux-Langlois, and Weiqiang Wen. "On the Hardness of Module-LWE with Binary Secret". In: *CT-RSA 2021*. Ed. by Kenneth G. Paterson. Vol. 12704. LNCS. Springer, Cham, May 2021, pp. 503–526. DOI: 10.1007/978-3-030-75539-3_21.

[Bou+22] Katharina Boudgoust, Corentin Jeudy, Adeline Roux-Langlois, and Weiqiang Wen. "Entropic Hardness of Module-LWE from Module-NTRU". In: *INDOCRYPT 2022*. Ed. by Takanori Isobe and Santanu Sarkar. Vol. 13774. LNCS. Springer, Cham, Dec. 2022, pp. 78–99. DOI: 10.1007/978-3-031-22912-1_4.

[Boy+09] Colin Boyd, Yvonne Cliff, Juan M. Gonzalez Nieto, and Kenneth G. Paterson. "One-round key exchange in the standard model". In: *International Journal of Applied Cryptography* 1.3 (Feb. 2009), pp. 181–199. DOI: 10.1504/IJACT.2009.023466.

[BP] Joseph Birr-Pixton. *Rustls: A modern TLS library in Rust*. URL: https://github.com/rustls/rustls (visited on 12/22/2022).

[BR93] Mihir Bellare and Phillip Rogaway. "Random Oracles are Practical: A Paradigm for Designing Efficient Protocols". In: *ACM CCS 93*. Ed. by Dorothy E. Denning, Raymond Pyle, Ravi Ganesan, Ravi S. Sandhu, and Victoria Ashby. ACM Press, Nov. 1993, pp. 62–73. DOI: 10.1145/168588.168596.

[Bra+13] Zvika Brakerski, Adeline Langlois, Chris Peikert, Oded Regev, and Damien Stehlé. "Classical hardness of learning with errors". In: *45th ACM STOC*. Ed. by Dan Boneh, Tim Roughgarden, and Joan Feigenbaum. ACM Press, June 2013, pp. 575–584. DOI: 10.1145/2488608.2488680.

[Bru+16] Leon Groot Bruinderink, Andreas Hülsing, Tanja Lange, and Yuval Yarom. "Flush, Gauss, and Reload - A Cache Attack on the BLISS Lattice-Based Signature Scheme". In: *CHES 2016*. Ed. by Benedikt Gierlichs and Axel Y. Poschmann. Vol. 9813. LNCS. Springer, Berlin, Heidelberg, Aug. 2016, pp. 323–345. DOI: 10.1007/978-3-662-53140-2_16.

[BS15] J.-F. Biasse and F. Song. *A note on the quantum attacks against schemes relying on the hardness of finding a short generator of an ideal in* $\mathbb{Q}(\zeta_{2^n})$. Tech. rep. 2015-12. Revision of September 28th 2015. The University of Waterloo, 2015.

[BS+20] Kevin Bürstinghaus-Steinbach, Christoph Krauß, Ruben Niederhagen, and Michael Schneider. "Post-Quantum TLS on Embedded Systems: Integrating and Evaluating Kyber and SPHINCS+ with mbed TLS". In: *ASIACCS 20*. Ed. by Hung-Min Sun, Shiuh-Pyng Shieh, Guofei Gu, and Giuseppe Ateniese. ACM Press, Oct. 2020, pp. 841–852. DOI: 10.1145/3320269.3384725.

[BSW18] Shi Bai, Damien Stehlé, and Weiqiang Wen. "Measuring, Simulating and Exploiting the Head Concavity Phenomenon in BKZ". In: *ASIACRYPT 2018, Part I*. Ed. by Thomas Peyrin and Steven Galbraith. Vol. 11272. LNCS. Springer, Cham, Dec. 2018, pp. 369–404. DOI: 10.1007/978-3-030-03326-2_13.

[BW25] Kaveh Bashiri and Andreas Wiemers. "On the independence heuristic in the dual attack". In: *Journal of Mathematical Cryptology* 19.1 (2025), p. 20240028. DOI: doi:10.1515/jmc-2024-0028. URL: https://doi.org/10.1515/jmc-2024-0028.

[Car+25] Kevin Carrier, Charles Meyer-Hilfiger, Yixin Shen, and Jean-Pierre Tillich. "Assessing the Impact of a Variant of MATZOV's Dual Attack on Kyber". In: *Advances in Cryptology – CRYPTO 2025*. Ed. by Yael Tauman Kalai and Seny F. Kamara. Cham: Springer Nature Switzerland, 2025, pp. 444–476. ISBN: 978-3-032-01855-7.

[CC21] Matt Campagna and Eric Crockett. *Hybrid Post-Quantum Key Encapsulation Methods (PQ KEM) for Transport Layer Security 1.2 (TLS)*. Internet-Draft draft-campagna-tls-bike-sike-hybrid-07. Work in Progress. Internet Engineering Task Force, Sept. 2, 2021. 17 pp. URL: https://datatracker.ietf.org/doc/html/draft-campagna-tls-bike-sike-hybrid-07.

[CDM24] Cas Cremers, Alexander Dax, and Niklas Medinger. "Keeping Up with the KEMs: Stronger Security Notions for KEMs and Automated Analysis of KEM-based Protocols". In: *ACM CCS 2024*. Ed. by Bo Luo, Xiaojing Liao, Jun Xu, Engin Kirda, and David Lie. ACM Press, Oct. 2024, pp. 1046–1060. DOI: 10.1145/3658644.3670283.

[CDW17] Ronald Cramer, Léo Ducas, and Benjamin Wesolowski. "Short Stickelberger Class Relations and Application to Ideal-SVP". In: *EUROCRYPT 2017, Part I*. Ed. by Jean-Sébastien Coron and Jesper Buus Nielsen. Vol. 10210. LNCS. Springer, Cham, 2017, pp. 324–348. DOI: 10.1007/978-3-319-56620-7_12.

[CDW21] Ronald Cramer, Léo Ducas, and Benjamin Wesolowski. "Mildly Short Vectors in Cyclotomic Ideal Lattices in Quantum Polynomial Time". In: *J. ACM* 68.2 (Jan. 2021). DOI: 10.1145/3431725.

[Cel+21] Sofía Celi, Armando Faz-Hernández, Nick Sullivan, Goutam Tamvada, Luke Valenta, Thom Wiggers, Bas Westerbaan, and Christopher A. Wood. "Implementing and Measuring KEMTLS". In: *LATINCRYPT 2021*. Ed. by Patrick Longa and Carla Ràfols. Vol. 12912. LNCS. Springer, Cham, Oct. 2021, pp. 88–107. DOI: 10.1007/978-3-030-88238-9_5.

[Che+20] Cong Chen, Oussama Danba, Jeffrey Hoffstein, Andreas Hulsing, Joost Rijneveld, John M. Schanck, Peter Schwabe, William Whyte, Zhenfei Zhang, Tsunekazu Saito, Takashi Yamakawa, and Keita Xagawa. *NTRU*. Tech. rep. available at https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions. National Institute of Standards and Technology, 2020.

[Che+23] Zhao Chen, Xianhui Lu, Dingding Jia, and Bao Li. "IND-CCA Security of Kyber in the Quantum Random Oracle Model, Revisited". In: *Information Security and Cryptology*. Springer Nature Switzerland, 2023, pp. 148–166. DOI: 10.1007/978-3-031-26553-2_8.

[CL01] Jan Camenisch and Anna Lysyanskaya. "An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation". In: *EUROCRYPT 2001*. Ed. by Birgit Pfitzmann. Vol. 2045. LNCS. Springer, Berlin, Heidelberg, May 2001, pp. 93–118. DOI: 10.1007/3-540-44987-6_7.

[CL21] André Chailloux and Johanna Loyer. "Lattice Sieving via Quantum Random Walks". In: *ASIACRYPT 2021, Part IV*. Ed. by Mehdi Tibouchi and Huaxiong Wang. Vol. 13093. LNCS. Springer, Cham, Dec. 2021, pp. 63–91. DOI: 10.1007/978-3-030-92068-5_3.

[CL23] André Chailloux and Johanna Loyer. "Classical and Quantum 3 and 4-Sieves to Solve SVP with Low Memory". In: *Post-Quantum Cryptography - 14th International Workshop, PQCrypto 2023*. Ed. by Thomas Johansson and Daniel Smith-Tone. Springer, Cham, Aug. 2023, pp. 225–255. DOI: 10.1007/978-3-031-40003-2_9.

[Clo] Cloudflare. *Cloudflare Radar – Adoption & Usage – Post-quantum encryption*. URL: https://radar.cloudflare.com/adoption-and-usagexpost-quantum-encryption (visited on 11/11/2025).

[CN11] Yuanmi Chen and Phong Q. Nguyen. "BKZ 2.0: Better Lattice Security Estimates". In: *ASIACRYPT 2011*. Ed. by Dong Hoon Lee and Xiaoyun Wang. Vol. 7073. LNCS. Springer, Berlin, Heidelberg, Dec. 2011, pp. 1–20. DOI: 10.1007/978-3-642-25385-0_1.

[Con25] Deirdre Connolly. *ML-KEM Post-Quantum Key Agreement for TLS 1.3*. Internet-Draft draft-ietf-tls-mlkem-05. Work in Progress. Internet Engineering Task Force, Nov. 2025. 10 pp. URL: https://datatracker.ietf.org/doc/draft-ietf-tls-mlkem/05/.

[CPS19] Eric Crockett, Christian Paquin, and Douglas Stebila. *Prototyping post-quantum and hybrid key exchange and authentication in TLS and SSH*. Workshop Record of the Second PQC Standardization Conference. 2019. iacr: 2019/858. URL: https://csrc.nist.gov/CSRC/media/Events/Second-PQC-Standardization-Conference/documents/accepted-papers/stebila-prototyping-post-quantum.pdf.

[Cra+16] Ronald Cramer, Léo Ducas, Chris Peikert, and Oded Regev. "Recovering Short Generators of Principal Ideals in Cyclotomic Rings". In: *EUROCRYPT 2016, Part II*. Ed. by Marc Fischlin and Jean-Sébastien Coron. Vol. 9666. LNCS. Springer, Berlin, Heidelberg, May 2016, pp. 559–585. DOI: 10.1007/978-3-662-49896-5_20.

[CS03] Ronald Cramer and Victor Shoup. "Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack". In: *SIAM Journal on Computing* 33.1 (2003), pp. 167–226. DOI: 10.1137/S0097539702403773.

[D'A+19] Jan-Pieter D'Anvers, Qian Guo, Thomas Johansson, Alexander Nilsson, Frederik Vercauteren, and Ingrid Verbauwhede. "Decryption Failure Attacks on IND-CCA Secure Lattice-Based Schemes". In: *PKC 2019, Part II*. Ed. by Dongdai Lin and Kazue Sako. Vol. 11443. LNCS. Springer, Cham, Apr. 2019, pp. 565–598. DOI: 10.1007/978-3-030-17259-6_19.

[Dac+20] Dana Dachman-Soled, Léo Ducas, Huijing Gong, and Mélissa Rossi. "LWE with Side Information: Attacks and Concrete Security Estimation". In: *CRYPTO 2020, Part II*. Ed. by Daniele Micciancio and Thomas Ristenpart. Vol. 12171. LNCS. Springer, Cham, Aug. 2020, pp. 329–358. DOI: 10.1007/978-3-030-56880-1_12.

[DB22] Jan-Pieter D'Anvers and Senne Batsleer. "Multitarget Decryption Failure Attacks and Their Application to Saber and Kyber". In: *PKC 2022, Part I*. Ed. by Goichiro Hanaoka, Junji Shikata, and Yohei Watanabe. Vol. 13177. LNCS. Springer, Cham, Mar. 2022, pp. 3–33. DOI: 10.1007/978-3-030-97121-2_1.

[DEP23] Léo Ducas, Thomas Espitau, and Eamonn W. Postlethwaite. "Finding Short Integer Solutions When the Modulus Is Small". In: *CRYPTO 2023, Part III*. Ed. by Helena Handschuh and Anna Lysyanskaya. Vol. 14083. LNCS. Springer, Cham, Aug. 2023, pp. 150–176. DOI: 10.1007/978-3-031-38548-3_6.

[DEP25] Léo Ducas, Lynn Engelberts, and Paola de Perthuis. "Predicting Module-Lattice Reduction". In: *Cryptology ePrint Archive* (2025).

[Din+22] Xiaohui Ding, Muhammed F. Esgin, Amin Sakzad, and Ron Steinfeld. "An Injectivity Analysis of Crystals-Kyber and Implications on Quantum Security". In: *ACISP 22*. Ed. by Khoa Nguyen, Guomin Yang, Fuchun Guo, and Willy Susilo. Vol. 13494. LNCS. Springer, Cham, Nov. 2022, pp. 332–351. DOI: 10.1007/978-3-031-22301-3_17.

[DLW20] Léo Ducas, Thijs Laarhoven, and Wessel P. J. van Woerden. "The Randomized Slicer for CVPP: Sharper, Faster, Smaller, Batchier". In: *PKC 2020, Part II*. Ed. by Aggelos Kiayias, Markulf Kohlweiss, Petros Wallden, and Vassilis Zikas. Vol. 12111. LNCS. Springer, Cham, May 2020, pp. 3–36. DOI: 10.1007/978-3-030-45388-6_1.

[DM13] Nico Döttling and Jörn Müller-Quade. "Lossy Codes and a New Variant of the Learning-With-Errors Problem". In: *EUROCRYPT 2013*. Ed. by Thomas Johansson and Phong Q. Nguyen. Vol. 7881. LNCS. Springer, Berlin, Heidelberg, May 2013, pp. 18–34. DOI: 10.1007/978-3-642-38348-9_2.

[DMG23] Viet Ba Dang, Kamyar Mohajerani, and Kris Gaj. "High-Speed Hardware Architectures and FPGA Benchmarking of CRYSTALS-Kyber, NTRU, and Saber". In: *IEEE Transactions on Computers* 72.2 (2023), pp. 306–320. DOI: 10.1109/TC.2022.3222954.

[Don+22] Jelle Don, Serge Fehr, Christian Majenz, and Christian Schaffner. "Online-Extractability in the Quantum Random-Oracle Model". In: *EUROCRYPT 2022, Part III*. Ed. by Orr Dunkelman and Stefan Dziembowski. Vol. 13277. LNCS. Springer, Cham, 2022, pp. 677–706. DOI: 10.1007/978-3-031-07082-2_24.

[Dor+24] Joao F. Doriguello, George Giapitzakis, Alessandro Luongo, and Aditya Morolia. *On the practicality of quantum sieving algorithms for the shortest vector problem*. Cryptology ePrint Archive, Report 2024/1692. 2024. URL: https://eprint.iacr.org/2024/1692.

[DP23a] Léo Ducas and Ludo N. Pulles. *Accurate Score Prediction for Dual-Sieve Attacks*. Cryptology ePrint Archive, Report 2023/1850. 2023. URL: https://eprint.iacr.org/2023/1850.

[DP23b] Léo Ducas and Ludo N. Pulles. "Does the Dual-Sieve Attack on Learning with Errors Even Work?" In: *CRYPTO 2023, Part III*. Ed. by Helena Handschuh and Anna Lysyanskaya. Vol. 14083. LNCS. Springer, Cham, Aug. 2023, pp. 37–69. DOI: 10.1007/978-3-031-38548-3_2.

[DPW19] Léo Ducas, Maxime Plançon, and Benjamin Wesolowski. "On the Shortness of Vectors to Be Found by the Ideal-SVP Quantum Algorithm". In: *CRYPTO 2019, Part I*. Ed. by Alexandra Boldyreva and Daniele Micciancio. Vol. 11692. LNCS. Springer, Cham, Aug. 2019, pp. 322–351. DOI: 10.1007/978-3-030-26948-7_12.

[DSW21] Léo Ducas, Marc Stevens, and Wessel P. J. van Woerden. "Advanced Lattice Sieving on GPUs, with Tensor Cores". In: *EUROCRYPT 2021, Part II*. Ed. by Anne Canteaut and François-Xavier Standaert. Vol. 12697. LNCS. Springer, Cham, Oct. 2021, pp. 249–279. DOI: 10.1007/978-3-030-77886-6_9.

[Dub+23] Elena Dubrova, Kalle Ngo, Joel Gärtner, and Ruize Wang. "Breaking a Fifth-Order Masked Implementation of CRYSTALS-Kyber by Copy-Paste". In: *Proceedings of the 10th ACM Asia Public-Key Cryptography Workshop*. APKC '23. Melbourne, VIC, Australia: Association for Computing Machinery, 2023, pp. 10–20. ISBN: 9798400701832. DOI: 10.1145/3591866.3593072. URL: https://doi.org/10.1145/3591866.3593072.

[Duc18] Léo Ducas. "Shortest Vector from Lattice Sieving: A Few Dimensions for Free". In: *EUROCRYPT 2018, Part I*. Ed. by Jesper Buus Nielsen and Vincent Rijmen. Vol. 10820. LNCS. Springer, Cham, 2018, pp. 125–145. DOI: 10.1007/978-3-319-78381-9_5.

[Duc22a] Léo Ducas. *Comment on "Improved Dual Lattice Attack"*. NIST PQC Forum. May 2022. URL: https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/Fm4cDfsx65s/m/BZFRC8hiAAAJ.

[Duc22b] Léo Ducas. "Estimating the Hidden Overheads in the BDGL Lattice Sieving Algorithm". In: *Post-Quantum Cryptography - 13th International Workshop, PQCrypto 2022*. Ed. by Jung Hee Cheon and Thomas Johansson. Springer, Cham, Sept. 2022, pp. 480–497. DOI: 10.1007/978-3-031-17234-2_22.

[dv25] Koen de Boer and Wessel P. J. van Woerden. *Lattice-based Cryptography: A survey on the security of the lattice-based NIST finalists*. Cryptology ePrint Archive, Report 2025/304. 2025. URL: https://eprint.iacr.org/2025/304.

[DVV18] Jan-Pieter D'Anvers, Frederik Vercauteren, and Ingrid Verbauwhede. *On the impact of decryption failures on the security of LWE/LWR based schemes*. Cryptology ePrint Archive, Report 2018/1089. 2018. URL: https://eprint.iacr.org/2018/1089.

[DW21] Léo Ducas and Wessel P. J. van Woerden. "NTRU Fatigue: How Stretched is Overstretched?" In: *ASIACRYPT 2021, Part IV*. Ed. by Mehdi Tibouchi and Huaxiong Wang. Vol. 13093. LNCS. Springer, Cham, Dec. 2021, pp. 3–32. DOI: 10.1007/978-3-030-92068-5_1.

[Eis+14] Kirsten Eisenträger, Sean Hallgren, Alexei Kitaev, and Fang Song. "A quantum algorithm for computing the unit group of an arbitrary degree number field". In: *46th ACM STOC*. Ed. by David B. Shmoys. ACM Press, 2014, pp. 293–302. DOI: 10.1145/2591796.2591860.

[EJK20] Thomas Espitau, Antoine Joux, and Natalia Kharchenko. "On a Dual/Hybrid Approach to Small Secret LWE - A Dual/Enumeration Technique for Learning with Errors and Application to Security Estimates of FHE Schemes". In: *INDOCRYPT 2020*. Ed. by Karthikeyan Bhargavan, Elisabeth Oswald, and Manoj Prabhakaran. Vol. 12578. LNCS. Springer, Cham, Dec. 2020, pp. 440–462. DOI: 10.1007/978-3-030-65277-7_20.

[EK20] Thomas Espitau and Paul Kirchner. *The nearest-colattice algorithm*. Cryptology ePrint Archive, Report 2020/694. 2020. URL: https://eprint.iacr.org/2020/694.

[Esp+17] Thomas Espitau, Pierre-Alain Fouque, Benoît Gérard, and Mehdi Tibouchi. "Side-Channel Attacks on BLISS Lattice-Based Signatures: Exploiting Branch Tracing against strongSwan and Electromagnetic Emanations in Microcontrollers". In: *ACM CCS 2017*. Ed. by Bhavani M. Thuraisingham, David Evans, Tal Malkin, and Dongyan Xu. ACM Press, 2017, pp. 1857–1874. DOI: 10.1145/3133956.3134028.

[FH05] Paul Ford-Hutchinson. *Securing FTP with TLS*. RFC 4217. Oct. 2005. DOI: 10.17487/RFC4217.

[Flu+25] Scott Fluhrer, Quynh Dang, John Preuß Mattsson, Kevin Milner, and Daniel Shiu. *ML-KEM Security Considerations*. Internet-Draft draft-sfluhrer-cfrg-ml-kem-security-considerations-03. Work in Progress. IETF, May 2025. URL: https://datatracker.ietf.org/doc/draft-sfluhrer-cfrg-ml-kem-security-considerations/.

[FO13] Eiichiro Fujisaki and Tatsuaki Okamoto. "Secure Integration of Asymmetric and Symmetric Encryption Schemes". In: *Journal of Cryptology* 26.1 (Jan. 2013), pp. 80–101. DOI: 10.1007/s00145-011-9114-1.

[FO99] Eiichiro Fujisaki and Tatsuaki Okamoto. "Secure Integration of Asymmetric and Symmetric Encryption Schemes". In: *CRYPTO'99*. Ed. by Michael J. Wiener. Vol. 1666. LNCS. Springer, Berlin, Heidelberg, Aug. 1999, pp. 537–554. DOI: 10.1007/3-540-48405-1_34.

[Fuj+13] Atsushi Fujioka, Koutarou Suzuki, Keita Xagawa, and Kazuki Yoneyama. "Practical and post-quantum authenticated key exchange from one-way secure key encapsulation mechanism". In: *ASIACCS 13*. Ed. by Kefei Chen, Qi Xie, Weidong Qiu, Ninghui Li, and Wen-Guey Tzeng. ACM Press, May 2013, pp. 83–94. DOI: 10.1145/2484313.2484323.

[Fuj+15] Atsushi Fujioka, Koutarou Suzuki, Keita Xagawa, and Kazuki Yoneyama. "Strongly secure authenticated key exchange from factoring, codes, and lattices". In: *DCC* 76.3 (2015), pp. 469–504. DOI: 10.1007/s10623-014-9972-2.

[Gen09] Craig Gentry. "Fully homomorphic encryption using ideal lattices". In: *41st ACM STOC*. Ed. by Michael Mitzenmacher. ACM Press, 2009, pp. 169–178. DOI: 10.1145/1536414.1536440.

[GJ21] Qian Guo and Thomas Johansson. "Faster Dual Lattice Attacks for Solving LWE with Applications to CRYSTALS". In: *ASIACRYPT 2021, Part IV*. Ed. by Mehdi Tibouchi and Huaxiong Wang. Vol. 13093. LNCS. Springer, Cham, Dec. 2021, pp. 33–62. DOI: 10.1007/978-3-030-92068-5_2.

[GJN20] Qian Guo, Thomas Johansson, and Alexander Nilsson. "A Key-Recovery Timing Attack on Post-quantum Primitives Using the Fujisaki-Okamoto Transformation and Its Application on FrodoKEM". In: *CRYPTO 2020, Part II*. Ed. by Daniele Micciancio and Thomas Ristenpart. Vol. 12171. LNCS. Springer, Cham, Aug. 2020, pp. 359–386. DOI: 10.1007/978-3-030-56880-1_13.

[GKV10] S. Dov Gordon, Jonathan Katz, and Vinod Vaikuntanathan. "A Group Signature Scheme from Lattice Assumptions". In: *ASIACRYPT 2010*. Ed. by Masayuki Abe. Vol. 6477. LNCS. Springer, Berlin, Heidelberg, Dec. 2010, pp. 395–412. DOI: 10.1007/978-3-642-17373-8_23.

[GLX24] Jiangxia Ge, Heming Liao, and Rui Xue. *Measure-Rewind-Extract: Tighter Proofs of One-Way to Hiding and CCA Security in the Quantum Random Oracle Model*. Cryptology ePrint Archive, Report 2024/777. 2024. URL: https://eprint.iacr.org/2024/777.

[GMP22] Paul Grubbs, Varun Maram, and Kenneth G. Paterson. "Anonymous, Robust Post-quantum Public Key Encryption". In: *EUROCRYPT 2022, Part III*. Ed. by Orr Dunkelman and Stefan Dziembowski. Vol. 13277. LNCS. Springer, Cham, 2022, pp. 402–432. DOI: 10.1007/978-3-031-07082-2_15.

[GN08] Nicolas Gama and Phong Q. Nguyen. "Predicting Lattice Reduction". In: *EUROCRYPT 2008*. Ed. by Nigel P. Smart. Vol. 4965. LNCS. Springer, Berlin, Heidelberg, Apr. 2008, pp. 31–51. DOI: 10.1007/978-3-540-78967-3_3.

[GNR10] Nicolas Gama, Phong Q. Nguyen, and Oded Regev. "Lattice Enumeration Using Extreme Pruning". In: *EUROCRYPT 2010*. Ed. by Henri Gilbert. Vol. 6110. LNCS. Springer, Berlin, Heidelberg, 2010, pp. 257–278. DOI: 10.1007/978-3-642-13190-5_13.

[Goo] Google Inc. *BoringSSL*. URL: https://boringssl.googlesource.com/boringssl/.

[Gro25] NIS Cooperation Group. *Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography*. June 11, 2025. URL: https://digital-strategy.ec.europa.eu/en/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography.

[GW22] Ruben Gonzalez and Thom Wiggers. "KEMTLS vs. Post-quantum TLS: Performance on Embedded Systems". In: *Security, Privacy, and Applied Cryptography Engineering*. Ed. by Lejla Batina, Stjepan Picek, and Mainack Mondal. Cham: Springer Nature Switzerland, 2022, pp. 99–117. ISBN: 978-3-031-22829-2. DOI: 10.1007/978-3-031-22829-2. URL: https://thomwiggers.nl/publication/kemtls-embedded/.

[Hei21] Max Heiser. *Improved Quantum Hypercone Locality Sensitive Filtering in Lattice Sieving*. Cryptology ePrint Archive, Report 2021/1295. 2021. URL: https://eprint.iacr.org/2021/1295.

[Hei+22] Daniel Heinz, Matthias J. Kannwischer, Georg Land, Thomas Pöppelmann, Peter Schwabe, and Amber Sprenkels. *First-Order Masked Kyber on ARM Cortex-M4*. Cryptology ePrint Archive, Report 2022/058. 2022. URL: https://eprint.iacr.org/2022/058.

[Her+23] Julius Hermelink, Erik Mårtensson, Simona Samardjiska, Peter Pessl, and Gabi Dreo Rodosek. "Belief Propagation Meets Lattice Reduction: Security Estimates for Error-Tolerant Key Recovery from Decryption Errors". In: *IACR TCHES* 2023.4 (2023), pp. 287–317. DOI: 10.46586/tches.v2023.i4.287-317.

[HHK17] Dennis Hofheinz, Kathrin Hövelmanns, and Eike Kiltz. "A Modular Analysis of the Fujisaki-Okamoto Transformation". In: *TCC 2017, Part I*. Ed. by Yael Kalai and Leonid Reyzin. Vol. 10677. LNCS. Springer, Cham, Nov. 2017, pp. 341–371. DOI: 10.1007/978-3-319-70500-2_12.

[HHM22] Kathrin Hövelmanns, Andreas Hülsing, and Christian Majenz. "Failing Gracefully: Decryption Failures and the Fujisaki-Okamoto Transform". In: *ASIACRYPT 2022, Part IV*. Ed. by Shweta Agrawal and Dongdai Lin. Vol. 13794. LNCS. Springer, Cham, Dec. 2022, pp. 414–443. DOI: 10.1007/978-3-031-22972-5_15.

[Hir+09] Philip S. Hirschhorn, Jeffrey Hoffstein, Nick Howgrave-Graham, and William Whyte. "Choosing NTRUEncrypt Parameters in Light of Combined Lattice Reduction and MITM Approaches". In: *ACNS 2009*. Ed. by Michel Abdalla, David Pointcheval, Pierre-Alain Fouque, and Damien Vergnaud. Vol. 5536. LNCS. Springer, Berlin, Heidelberg, June 2009, pp. 437–455. DOI: 10.1007/978-3-642-01957-9_27.

[HK25] Kathrin Hövelmanns and Mikhail A. Kudinov. "Treating Dishonest Ciphertexts in Post-quantum KEMs - Explicit vs. Implicit Rejection in the FO Transform". In: *Post-Quantum Cryptography - 16th International Workshop, PQCrypto 2025, Part II*. Ed. by Ruben Niederhagen and Markku-Juhani O. Saarinen. Springer, Cham, Apr. 2025, pp. 325–350. DOI: 10.1007/978-3-031-86602-9_12.

[HKL18] Gottfried Herold, Elena Kirshanova, and Thijs Laarhoven. "Speed-Ups and Time-Memory Trade-Offs for Tuple Lattice Sieving". In: *PKC 2018, Part I*. Ed. by Michel Abdalla and Ricardo Dahab. Vol. 10769. LNCS. Springer, Cham, Mar. 2018, pp. 407–436. DOI: 10.1007/978-3-319-76578-5_14.

[HM24] Kathrin Hövelmanns and Christian Majenz. "A Note on Failing Gracefully: Completing the Picture for Explicitly Rejecting Fujisaki-Okamoto Transforms Using Worst-Case Correctness". In: *Post-Quantum Cryptography - 15th International Workshop, PQCrypto 2024, Part II*. Ed. by Markku-Juhani Saarinen and Daniel Smith-Tone. Springer, Cham, June 2024, pp. 245–265. DOI: 10.1007/978-3-031-62746-0_11.

[Hof02] Paul E. Hoffman. *SMTP Service Extension for Secure SMTP over Transport Layer Security*. RFC 3207. Feb. 2002. DOI: 10.17487/RFC3207.

[Höv+20] Kathrin Hövelmanns, Eike Kiltz, Sven Schäge, and Dominique Unruh. "Generic Authenticated Key Exchange in the Quantum Random Oracle Model". In: *PKC 2020, Part II*. Ed. by Aggelos Kiayias, Markulf Kohlweiss, Petros Wallden, and Vassilis Zikas. Vol. 12111. LNCS. Springer, Cham, May 2020, pp. 389–422. DOI: 10.1007/978-3-030-45388-6_14.

[How07] Nick Howgrave-Graham. "A Hybrid Lattice-Reduction and Meet-in-the-Middle Attack Against NTRU". In: *CRYPTO 2007*. Ed. by Alfred Menezes. Vol. 4622. LNCS. Springer, Berlin, Heidelberg, Aug. 2007, pp. 150–169. DOI: 10.1007/978-3-540-74143-5_9.

[HS07] Guillaume Hanrot and Damien Stehlé. "Improved Analysis of Kannan's Shortest Lattice Vector Algorithm". In: *CRYPTO 2007*. Ed. by Alfred Menezes. Vol. 4622. LNCS. Springer, Berlin, Heidelberg, Aug. 2007, pp. 170–186. DOI: 10.1007/978-3-540-74143-5_10.

[HS08] Guillaume Hanrot and Damien Stehlé. "Worst-case Hermite-Korkine-Zolotarev reduced lattice bases". In: *arXiv preprint arXiv:0801.3331* (2008).

[HS10] Guillaume Hanrot and Damien Stehlé. "A complete worst-case analysis of Kannan' s shortest lattice vector algorithm". In: *Manuscript* (2010). Full version of [HS07; HS08], pp. 1–34.

[Hua+20] Yiming Huang, Miaoqing Huang, Zhongkui Lei, and Jiaxuan Wu. "A Pure Hardware Implementation of CRYSTALS-KYBER PQC Algorithm through Resource Reuse". In: *IEICE Electronics Express* advpub (2020), p. 17.20200234. DOI: 10.1587/elex.17.20200234.

[Hül+17] Andreas Hülsing, Joost Rijneveld, John M. Schanck, and Peter Schwabe. "High-Speed Key Encapsulation from NTRU". In: *CHES 2017*. Ed. by Wieland Fischer and Naofumi Homma. Vol. 10529. LNCS. Springer, Cham, Sept. 2017, pp. 232–252. DOI: 10.1007/978-3-319-66787-4_12.

[HW20] Jonathan Hoyland and Christopher Wood. *TLS 1.3 Extended Key Schedule*. Internet-Draft draft-jhoyla-tls-extended-key-schedule-03. Work in Progress. Internet Engineering Task Force, Dec. 2020. 1–7. URL: https://datatracker.ietf.org/doc/html/draft-jhoyla-tls-extended-key-schedule-03.

[Hö20] Kathrin Hövelmanns. "Generic constructions of quantum-resistant cryptosystems". PhD Thesis. PhD thesis. Bochum: Ruhr-Universität Bochum, 2020. URL: https://research.tue.nl/en/publications/generic-constructions-of-quantum-resistant-cryptosystems.

[ISB25] German Federal Office for Information Security (BSI). *Cryptographic Mechanisms: Recommendations and Key Lengths*. Tech. rep. BSI TR-02102-1. BSI, Jan. 2025. URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.html.

[Jao+22] David Jao, Reza Azarderakhsh, Matthew Campagna, Craig Costello, Luca De Feo, Basil Hess, Amir Jalali, Brian Koziel, Brian LaMacchia, Patrick Longa, Michael Naehrig, Joost Renes, Vladimir Soukharev, David Urbanik, Geovandro Pereira, Koray Karabina, and Aaron Hutchinson. *SIKE*. Tech. rep. available at https://csrc.nist.gov/Projects/post-quantum-cryptography/round-4-submissions. National Institute of Standards and Technology, 2022.

[Jen+23] Sönke Jendral, Kalle Ngo, Ruize Wang, and Elena Dubrova. *A Single-Trace Message Recovery Attack on a Masked and Shuffled Implementation of CRYSTALS-Kyber*. Cryptology ePrint Archive, Report 2023/1587. 2023. URL: https://eprint.iacr.org/2023/1587.

[Jia+18] Haodong Jiang, Zhenfeng Zhang, Long Chen, Hong Wang, and Zhi Ma. "IND-CCA-Secure Key Encapsulation Mechanism in the Quantum Random Oracle Model, Revisited". In: *CRYPTO 2018, Part III*. Ed. by Hovav Shacham and Alexandra Boldyreva. Vol. 10993. LNCS. Springer, Cham, Aug. 2018, pp. 96–125. DOI: 10.1007/978-3-319-96878-0_4.

[JZM19a] Haodong Jiang, Zhenfeng Zhang, and Zhi Ma. "Key Encapsulation Mechanism with Explicit Rejection in the Quantum Random Oracle Model". In: *PKC 2019, Part II*. Ed. by Dongdai Lin and Kazue Sako. Vol. 11443. LNCS. Springer, Cham, Apr. 2019, pp. 618–645. DOI: 10.1007/978-3-030-17259-6_21.

[JZM19b] Haodong Jiang, Zhenfeng Zhang, and Zhi Ma. "Tighter Security Proofs for Generic Key Encapsulation Mechanism in the Quantum Random Oracle Model". In: *Post-Quantum Cryptography - 10th International Conference, PQCrypto 2019*. Ed. by Jintai Ding and Rainer Steinwandt. Springer, Cham, 2019, pp. 227–248. DOI: 10.1007/978-3-030-25510-7_13.

[Kam+22] Tendayi Kamucheka, Alexander Nelson, David Andrews, and Miaoqing Huang. "A Masked Pure-Hardware Implementation of Kyber Cryptographic Algorithm". In: *2022 International Conference on Field-Programmable Technology (ICFPT)*. 2022, pp. 1–1. DOI: 10.1109/ICFPT56656.2022.9974404.

[Kan+] Matthias J. Kannwischer, Richard Petri, Joost Rijneveld, Peter Schwabe, and Ko Stoffelen. *pqm4: Post-quantum crypto library for the ARM Cortex-M4*. URL: https://github.com/mupq/pqm4.

[Kan83] Ravi Kannan. "Improved Algorithms for Integer Programming and Related Lattice Problems". In: *15th ACM STOC*. ACM Press, Apr. 1983, pp. 193–206. DOI: 10.1145/800061.808749.

[Kar+25a] Alexander Karenin, Elena Kirshanova, Alexander May, and Julian Nowakowski. "Fast Slicer for Batch-CVP: Making Lattice Hybrid Attacks Practical". In: *Cryptology ePrint Archive* (2025).

[Kar+25b] Alexandr Karenin, Elena Kirshanova, Julian Nowakowski, Eamonn W Postlethwaite, and Fernando Virdia. "Cool+Cruel=Dual". In: *Cryptology ePrint Archive* (2025).

[KEF20] Paul Kirchner, Thomas Espitau, and Pierre-Alain Fouque. "Fast Reduction of Algebraic Lattices over Cyclotomic Fields". In: *CRYPTO 2020, Part II*. Ed. by Daniele Micciancio and Thomas Ristenpart. Vol. 12171. LNCS. Springer, Cham, Aug. 2020, pp. 155–185. DOI: 10.1007/978-3-030-56880-1_6.

[KF15] Paul Kirchner and Pierre-Alain Fouque. "An Improved BKW Algorithm for LWE with Applications to Cryptography and Lattices". In: *CRYPTO 2015, Part I*. Ed. by Rosario Gennaro and Matthew J. B. Robshaw. Vol. 9215. LNCS. Springer, Berlin, Heidelberg, Aug. 2015, pp. 43–62. DOI: 10.1007/978-3-662-47989-6_3.

[KF17] Paul Kirchner and Pierre-Alain Fouque. "Revisiting Lattice Attacks on Overstretched NTRU Parameters". In: *EUROCRYPT 2017, Part I*. Ed. by Jean-Sébastien Coron and Jesper Buus Nielsen. Vol. 10210. LNCS. Springer, Cham, 2017, pp. 3–26. DOI: 10.1007/978-3-319-56620-7_1.

[KK18] Franziskus Kiefer and Krzysztof Kwiatkowski. *Hybrid ECDHE-SIDH Key Exchange for TLS*. Internet-Draft draft-kiefer-tls-ecdhe-sidh-00. Work in Progress. Internet Engineering Task Force, Nov. 2018. 13 pp. URL: https://datatracker.ietf.org/doc/html/draft-kiefer-tls-ecdhe-sidh-00.

[KL21] Elena Kirshanova and Thijs Laarhoven. "Lower Bounds on Lattice Sieving and Information Set Decoding". In: *CRYPTO 2021, Part II*. Ed. by Tal Malkin and Chris Peikert. Vol. 12826. LNCS. Virtual Event: Springer, Cham, Aug. 2021, pp. 791–820. DOI: 10.1007/978-3-030-84245-1_27.

[Kre24] Katharina Kreuzer. "Verification of Correctness and Security Properties for CRYSTALS-KYBER". In: *CSF 2024 Computer Security Foundations Symposium*. IEEE Computer Society Press, July 2024, pp. 511–526. DOI: 10.1109/CSF61375.2024.00016.

[KS23] Ehren Kret and Rolfe Schmidt. *The PQXDH Key Agreement Protocol*. Protocol documentation. Oct. 18, 2023. URL: https://signal.org/docs/specifications/pqxdh/.

[Kuc+20] Veronika Kuchta, Amin Sakzad, Damien Stehlé, Ron Steinfeld, and Shifeng Sun. "Measure-Rewind-Measure: Tighter Quantum Random Oracle Model Proofs for One-Way to Hiding and CCA Security". In: *EUROCRYPT 2020, Part III*. Ed. by Anne Canteaut and Yuval Ishai. Vol. 12107. LNCS. Springer, Cham, May 2020, pp. 703–728. DOI: 10.1007/978-3-030-45727-3_24.

[KV19] Kris Kwiatkowski and Luke Valenta. *The TLS Post-Quantum Experiment*. Post on the Cloudflare blog. Cloudflare, 2019. URL: https://blog.cloudflare.com/the-tls-post-quantum-experiment/ (visited on 12/22/2022).

[Kwi+19] Krzysztof Kwiatkowski, Nick Sullivan, Adam Langley, Dave Levin, and Alan Mislove. *Measuring TLS key exchange with post-quantum KEM*. Workshop Record of the Second PQC Standardization Conference. 2019. URL: https://csrc.nist.gov/CSRC/media/Events/Second-PQC-Standardization-Conference/documents/accepted-papers/kwiatkowski-measuring-tls.pdf.

[Kwi+25] Kris Kwiatkowski, Panos Kampanakis, Bas Westerbaan, and Douglas Stebila. *Post-quantum hybrid ECDHE-MLKEM Key Agreement for TLSv1.3*. Internet-Draft draft-ietf-tls-ecdhe-mlkem-01. Work in Progress. Internet Engineering Task Force, Sept. 2025. 10 pp. URL: https://datatracker.ietf.org/doc/draft-ietf-tls-ecdhe-mlkem/01/.

[Laa15] Thijs Laarhoven. "Sieving for Shortest Vectors in Lattices Using Angular Locality-Sensitive Hashing". In: *CRYPTO 2015, Part I*. Ed. by Rosario Gennaro and Matthew J. B. Robshaw. Vol. 9215. LNCS. Springer, Berlin, Heidelberg, Aug. 2015, pp. 3–22. DOI: 10.1007/978-3-662-47989-6_1.

[Laa16] Thijs Laarhoven. "Search problems in cryptography: from fingerprinting to lattice sieving". English. PhD Thesis. PhD thesis. Mathematics and Computer Science, Feb. 2016. ISBN: 978-90-386-4021-1.

[Lan16] Adam Langley. *CECPQ1 results*. Blog post. 2016. URL: https://www.imperialviolet.org/2016/11/28/cecpq1.html.

[Lan18] Adam Langley. *CECPQ2*. Blog post. 2018. URL: https://www.imperialviolet.org/2018/12/12/cecpq2.html.

[Lee+19] Changmin Lee, Alice Pellet-Mary, Damien Stehlé, and Alexandre Wallet. "An LLL Algorithm for Module Lattices". In: *ASIACRYPT 2019, Part II*. Ed. by Steven D. Galbraith and Shiho Moriai. Vol. 11922. LNCS. Springer, Cham, Dec. 2019, pp. 59–90. DOI: 10.1007/978-3-030-34621-8_3.

[Li+21] Shuaigang Li, Xianhui Lu, Jiang Zhang, Bao Li, and Lei Bi. "Predicting the Concrete Security of LWE Against the Dual Attack Using Binary Search". In: *ICICS 21, Part I*. Ed. by Debin Gao, Qi Li, Xiaohong Guan, and Xiaofeng Liao. Vol. 12919. LNCS. Springer, Cham, Nov. 2021, pp. 265–282. DOI: 10.1007/978-3-030-88052-1_16.

[LM18] Thijs Laarhoven and Artur Mariano. "Progressive Lattice Sieving". In: *Post-Quantum Cryptography - 9th International Conference, PQCrypto 2018*. Ed. by Tanja Lange and Rainer Steinwandt. Springer, Cham, 2018, pp. 292–311. DOI: 10.1007/978-3-319-79063-3_14.

[LMP15] Thijs Laarhoven, Michele Mosca, and Joop van de Pol. "Finding shortest lattice vectors faster using quantum search". In: *DCC* 77.2-3 (2015), pp. 375–400. DOI: 10.1007/s10623-015-0067-5.

[LN25] Jianwei Li and Phong Q Nguyen. "A complete analysis of the BKZ lattice reduction algorithm". In: *Journal of Cryptology* 38.1 (2025), p. 12. DOI: 10.1007/s00145-024-09527-0.

[LP11] Richard Lindner and Chris Peikert. "Better Key Sizes (and Attacks) for LWE-Based Encryption". In: *CT-RSA 2011*. Ed. by Aggelos Kiayias. Vol. 6558. LNCS. Springer, Berlin, Heidelberg, Feb. 2011, pp. 319–339. DOI: 10.1007/978-3-642-19074-2_21.

[LPR10] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. "On Ideal Lattices and Learning with Errors over Rings". In: *EUROCRYPT 2010*. Ed. by Henri Gilbert. Vol. 6110. LNCS. Springer, Berlin, Heidelberg, 2010, pp. 1–23. DOI: 10.1007/978-3-642-13190-5_1.

[LS15] Adeline Langlois and Damien Stehlé. "Worst-case to average-case reductions for module lattices". In: *DCC* 75.3 (2015), pp. 565–599. DOI: 10.1007/s10623-014-9938-4.

[MAT22] MATZOV. *Report on the Security of LWE: Improved Dual Lattice Attack*. Tech. rep. 2022. DOI: https://doi.org/10.5281/zenodo.6493704.

[Mat25] John Preuss Mattsson. *PQC Dialogue with Government Stakeholders*. Transcript of an IETF side-meeting posted on a mailing list. May 13, 2025. URL: https://mailarchive.ietf.org/arch/msg/pqc/14f3hjUlpiwSbusornAjRN98QLc/.

[Mic] Microsoft. *Schannel (Security Support Provider)*. URL: https://learn.microsoft.com/en-us/windows/win32/secauthn/schannel.

[Mic18] Daniele Micciancio. "On the Hardness of Learning With Errors with Binary Secrets". In: *Theory of Computing* 14.13 (2018), pp. 1–17. DOI: 10.4086/toc.2018.v014a013.

[Mic25] Microsoft. *Microsoft Edge browser policy PostQuantumKeyAgreementEnabled*. Sept. 18, 2025. URL: https://learn.microsoft.com/en-us/deployedge/microsoft-edge-browser-policies/postquantumkeyagreementenabled.

[MM11] Daniele Micciancio and Petros Mol. "Pseudorandom Knapsacks and the Sample Complexity of LWE Search-to-Decision Reductions". In: *CRYPTO 2011*. Ed. by Phillip Rogaway. Vol. 6841. LNCS. Springer, Berlin, Heidelberg, Aug. 2011, pp. 465–484. DOI: 10.1007/978-3-642-22792-9_26.

[Moh10] Payman Mohassel. "A Closer Look at Anonymity and Robustness in Encryption Schemes". In: *ASIACRYPT 2010*. Ed. by Masayuki Abe. Vol. 6477. LNCS. Springer, Berlin, Heidelberg, Dec. 2010, pp. 501–518. DOI: 10.1007/978-3-642-17373-8_29.

[Moo+24] Dustin Moody, Ray Perlner, Andrew Regenscheid, Angela Robinson, and David Cooper. *Transition to Post-Quantum Cryptography Standards*. NIST Interagency Report 8547. Initial Public Draft. National Institute of Standards and Technology, Nov. 2024. DOI: 10.6028/NIST.IR.8547.ipd. URL: https://csrc.nist.gov/pubs/ir/8547/ipd.

[Moz] Mozilla Foundation. *Network Security Services (NSS)*. URL: https://developer.mozilla.org/en-US/docs/Mozilla/Projects/NSS.

[MP12] Daniele Micciancio and Chris Peikert. "Trapdoors for Lattices: Simpler, Tighter, Faster, Smaller". In: *EUROCRYPT 2012*. Ed. by David Pointcheval and Thomas Johansson. Vol. 7237. LNCS. Springer, Berlin, Heidelberg, Apr. 2012, pp. 700–718. DOI: 10.1007/978-3-642-29011-4_41.

[MP13] Daniele Micciancio and Chris Peikert. "Hardness of SIS and LWE with Small Parameters". In: *CRYPTO 2013, Part I*. Ed. by Ran Canetti and Juan A. Garay. Vol. 8042. LNCS. Springer, Berlin, Heidelberg, Aug. 2013, pp. 21–39. DOI: 10.1007/978-3-642-40041-4_2.

[MR09] Daniele Micciancio and Oded Regev. "Lattice-based Cryptography". In: *Post-Quantum Cryptography*. Ed. by Daniel J. Bernstein, Johannes Buchmann, and Erik Dahmen. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 147–191. DOI: 10.1007/978-3-540-88702-7_5.

[MS20] Tamalika Mukherjee and Noah Stephens-Davidowitz. "Lattice Reduction for Modules, or How to Reduce ModuleSVP to ModuleSVP". In: *CRYPTO 2020, Part II*. Ed. by Daniele Micciancio and Thomas Ristenpart. Vol. 12171. LNCS. Springer, Cham, Aug. 2020, pp. 213–242. DOI: 10.1007/978-3-030-56880-1_8.

[Muj+24] Catinca Mujdei, Lennert Wouters, Angshuman Karmakar, Arthur Beckers, Jose Maria Bermudo Mera, and Ingrid Verbauwhede. "Side-channel Analysis of Lattice-based Post-quantum Cryptography: Exploiting Polynomial Multiplication". In: *ACM Transactions on Embedded Computing Syststems* 23.2 (Mar. 2024). DOI: 10.1145/3569420. URL: https://doi.org/10.1145/3569420.

[MX23] Varun Maram and Keita Xagawa. "Post-quantum Anonymity of Kyber". In: *PKC 2023, Part I*. Ed. by Alexandra Boldyreva and Vladimir Kolesnikov. Vol. 13940. LNCS. Springer, Cham, May 2023, pp. 3–35. DOI: 10.1007/978-3-031-31368-4_1.

[Nat16] National Institute of Standards and Technology. *Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process*. Dec. 2016. URL: https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf (visited on 05/09/2023).

[Nat24a] National Cyber Security Centre. *Next steps in preparing for post-quantum cryptography. How system owners can begin planning for the migration to post-quantum cryptography (PQC)*. Originally published November 2023; updated August 2024. National Cyber Security Centre (NCSC). Aug. 14, 2024. URL: https://www.ncsc.gov.uk/whitepaper/next-steps-preparing-for-post-quantum-cryptography (visited on 01/13/2026).

[Nat24b] National Institute of Standards and Technology. *Module-Lattice-Based Key-Encapsulation Mechanism Standard*. Federal Information Processing Standards Publication (FIPS) FIPS 203. NIST has assigned NIST FIPS 203 as the publication identifier for this FIPS. Department of Commerce, Washington, D.C., 2024.

[Nat24c] National Security Agency. *The Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ*. Dec. 2024. URL: https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/0/CSI_CNSA_2.0_FAQ_.PDF.

[New99] Chris Newman. *Using TLS with IMAP, POP3 and ACAP*. RFC 2595. June 1999. DOI: 10.17487/RFC2595. URL: https://www.rfc-editor.org/info/rfc2595.

[Ngu10] Phong Q. Nguyen. "Hermite's Constant and Lattice Algorithms". In: ed. by Phong Q. Nguyen and Brigitte Vallée. ISC. Springer, 2010, pp. 19–69. ISBN: 978-3-642-02294-4. DOI: 10.1007/978-3-642-02295-1.

[NV08] Phong Q Nguyen and Thomas Vidick. "Sieve algorithms for the shortest vector problem are practical". In: *Journal of Mathematical Cryptology* 2.2 (2008), pp. 181–207.

[O'B23] Devon O'Brien. *Protecting Chrome Traffic with Hybrid Kyber KEM*. Aug. 10, 2023. URL: https://blog.chromium.org/2023/08/protecting-chrome-traffic-with-hybrid.html.

[Ode+18] Tobias Oder, Tobias Schneider, Thomas Pöppelmann, and Tim Güneysu. "Practical CCA2-Secure Masked Ring-LWE Implementations". In: *IACR TCHES* 2018.1 (2018), pp. 142–174. ISSN: 2569-2925. DOI: 10.13154/tches.v2018.i1.142-174. URL: https://tches.iacr.org/index.php/TCHES/article/view/836.

[Opea] *OpenSSL: The Open Source toolkit for SSL/TLS*. OpenSSL project. URL: https://www.openssl.org/ (visited on 05/09/2023).

[Opeb] *OpenVPN Protocol*. URL: https://openvpn.net/community-resources/openvpn-protocol/ (visited on 11/10/2025).

[Ope25] Open Quantum Safe. *liboqs: An open-source C library for quantum-safe cryptography*. Version 0.14.0. July 11, 2025. URL: https://github.com/open-quantum-safe/liboqs.

[PBY17] Peter Pessl, Leon Groot Bruinderink, and Yuval Yarom. "To BLISS-B or not to be: Attacking strongSwan's Implementation of Post-Quantum Signatures". In: *ACM CCS 2017*. Ed. by Bhavani M. Thuraisingham, David Evans, Tal Malkin, and Dongyan Xu. ACM Press, 2017, pp. 1843–1855. DOI: 10.1145/3133956.3134023.

[Pei09] Chris Peikert. "Public-key cryptosystems from the worst-case shortest vector problem: extended abstract". In: *41st ACM STOC*. Ed. by Michael Mitzenmacher. ACM Press, 2009, pp. 333–342. DOI: 10.1145/1536414.1536461.

[PG14] Thomas Pöppelmann and Tim Güneysu. "Towards Practical Lattice-Based Public-Key Encryption on Reconfigurable Hardware". In: *SAC 2013*. Ed. by Tanja Lange, Kristin Lauter, and Petr Lisonek. Vol. 8282. LNCS. Springer, Berlin, Heidelberg, Aug. 2014, pp. 68–85. DOI: 10.1007/978-3-662-43414-7_4.

[PHS19] Alice Pellet-Mary, Guillaume Hanrot, and Damien Stehlé. "Approx-SVP in Ideal Lattices with Pre-processing". In: *EUROCRYPT 2019, Part II*. Ed. by Yuval Ishai and Vincent Rijmen. Vol. 11477. LNCS. Springer, Cham, May 2019, pp. 685–716. DOI: 10.1007/978-3-030-17656-3_24.

[PS24] Amaury Pouly and Yixin Shen. "Provable Dual Attacks on Learning with Errors". In: *EUROCRYPT 2024, Part VII*. Ed. by Marc Joye and Gregor Leander. Vol. 14657. LNCS. Springer, Cham, May 2024, pp. 256–285. DOI: 10.1007/978-3-031-58754-2_10.

[PST20] Christian Paquin, Douglas Stebila, and Goutam Tamvada. "Benchmarking Post-quantum Cryptography in TLS". In: *Post-Quantum Cryptography - 11th International Conference, PQCrypto 2020*. Ed. by Jintai Ding and Jean-Pierre Tillich. Springer, Cham, 2020, pp. 72–91. DOI: 10.1007/978-3-030-44223-1_5.

[PV21] Eamonn W. Postlethwaite and Fernando Virdia. "On the Success Probability of Solving Unique SVP via BKZ". In: *PKC 2021, Part I*. Ed. by Juan Garay. Vol. 12710. LNCS. Springer, Cham, May 2021, pp. 68–98. DOI: 10.1007/978-3-030-75245-3_4.

[PV25] Ludo N Pulles and Paul Vié. "Accelerating the Primal Hybrid Attack against Sparse LWE using GPUs". In: *Cryptology ePrint Archive* (2025).

[Raj+23] Gokulnath Rajendran, Prasanna Ravi, Jan-Pieter D'Anvers, Shivam Bhasin, and Anupam Chattopadhyay. "Pushing the Limits of Generic Side-Channel Attacks on LWE-based KEMs - Parallel PC Oracle Attacks on Kyber KEM and Beyond". In: *IACR TCHES* 2023.2 (2023), pp. 418–446. DOI: 10.46586/tches.v2023.i2.418-446.

[Rav+20a] Prasanna Ravi, Romain Poussier, Shivam Bhasin, and Anupam Chattopadhyay. "On Configurable SCA Countermeasures Against Single Trace Attacks for the NTT: A Performance Evaluation Study over Kyber and Dilithium on the ARM Cortex-M4". In: *Security, Privacy, and Applied Cryptography Engineering: 10th International Conference, SPACE 2020, Kolkata, India, December 17–21, 2020, Proceedings*. Berlin, Heidelberg: Springer-Verlag, 2020, pp. 123–146. DOI: 10.1007/978-3-030-66626-2_7.

[Rav+20b] Prasanna Ravi, Sujoy Sinha Roy, Anupam Chattopadhyay, and Shivam Bhasin. "Generic Side-channel attacks on CCA-secure lattice-based PKE and KEMs". In: *IACR TCHES* 2020.3 (2020), pp. 307–335. ISSN: 2569-2925. DOI: 10.13154/tches.v2020.i3.307-335. URL: https://tches.iacr.org/index.php/TCHES/article/view/8592.

[Rav+22] Prasanna Ravi, Shivam Bhasin, Sujoy Sinha Roy, and Anupam Chattopadhyay. "On Exploiting Message Leakage in (Few) NIST PQC Candidates for Practical Message Recovery Attacks". In: *IEEE Transactions on Information Forensics and Security* 17 (2022), pp. 684–699. DOI: 10.1109/TIFS.2021.3139268.

[Reg05] Oded Regev. "On lattices, learning with errors, random linear codes, and cryptography". In: *37th ACM STOC*. Ed. by Harold N. Gabow and Ronald Fagin. ACM Press, May 2005, pp. 84–93. DOI: 10.1145/1060590.1060603.

[Rep+15] Oscar Reparaz, Sujoy Sinha Roy, Frederik Vercauteren, and Ingrid Verbauwhede. "A Masked Ring-LWE Implementation". In: *CHES 2015*. Ed. by Tim Güneysu and Helena Handschuh. Vol. 9293. LNCS. Springer, Berlin, Heidelberg, Sept. 2015, pp. 683–702. DOI: 10.1007/978-3-662-48324-4_34.

[Res00] Eric Rescorla. *HTTP Over TLS*. RFC 2818. May 2000. DOI: 10.17487/RFC2818.

[Res18] Eric Rescorla. *The Transport Layer Security (TLS) Protocol Version 1.3*. RFC 8446. Aug. 2018. DOI: 10.17487/RFC8446.

[Saa18] Markku-Juhani O. Saarinen. "Arithmetic coding and blinding countermeasures for lattice signatures - Engineering a side-channel resistant post-quantum signature scheme with compact signatures". In: *Journal of Cryptographic Engineering* 8.1 (Apr. 2018), pp. 71–84. DOI: 10.1007/s13389-017-0149-6.

[Sak00] Kazue Sako. "An Auction Protocol Which Hides Bids of Losers". In: *PKC 2000*. Ed. by Hideki Imai and Yuliang Zheng. Vol. 1751. LNCS. Springer, Berlin, Heidelberg, Jan. 2000, pp. 422–432. DOI: 10.1007/978-3-540-46588-1_28.

[Sch+17] John M. Schanck, Andreas Hulsing, Joost Rijneveld, and Peter Schwabe. *NTRU-HRSS-KEM*. Tech. rep. available at https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-1-submissions. National Institute of Standards and Technology, 2017.

[Sch22a] Peter Schwabe. *CRYSTALS-Kyber Update*. Talk at the Fourth NIST PQC Standardization Conference. Slides: https://csrc.nist.gov/csrc/media/Presentations/2022/crystals-kyber-update/images-media/session-1-schwabe-crystals-kyber-pqc2022.pdf. Nov. 2022. URL: https://csrc.nist.gov/Presentations/2022/crystals-kyber-update.

[Sch22b] Peter Schwabe. *Kyber decisions, part 2: FO transform*. Message to the `pqc-forum@list.nist.gov` mailing list. Explains hashing of (hash of) the public key into coins/shared key and its robustness rationale. Dec. 2022. URL: https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/C0D3W1KoINY.

[Sch24] Sophie Schmieg. *Unbindable Kemmy Schmidt: ML-KEM is neither MAL-BIND-K-CT nor MAL-BIND-K-PK*. Cryptology ePrint Archive, Report 2024/523. 2024. URL: https://eprint.iacr.org/2024/523.

[Sch87] Claus-Peter Schnorr. "A hierarchy of polynomial time lattice basis reduction algorithms". In: *Theoretical computer science* 53.2-3 (1987), pp. 201–224. DOI: https://doi.org/10.1016/0304-3975(87)90064-8.

[SFG25] Douglas Stebila, Scott Fluhrer, and Shay Gueron. *Hybrid key exchange in TLS 1.3*. Internet-Draft draft-ietf-tls-hybrid-design-16. Work in Progress. Internet Engineering Task Force, Sept. 2025. 23 pp. URL: https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/16/.

[SH95] Claus-Peter Schnorr and Horst Helmut Hörner. "Attacking the Chor-Rivest Cryptosystem by Improved Lattice Reduction". In: *EUROCRYPT'95*. Ed. by Louis C. Guillou and Jean-Jacques Quisquater. Vol. 921. LNCS. Springer, Berlin, Heidelberg, May 1995, pp. 1–12. DOI: 10.1007/3-540-49264-X_1.

[She+23] Muyan Shen, Chi Cheng, Xiaohan Zhang, Qian Guo, and Tao Jiang. "Find the Bad Apples: An efficient method for perfect key recovery under imperfect SCA oracles - A case study of Kyber". In: *IACR TCHES* 2023.1 (2023), pp. 89–112. DOI: 10.46586/tches.v2023.i1.89-112.

[SM16] Douglas Stebila and Michele Mosca. "Post-quantum Key Exchange for the Internet and the Open Quantum Safe Project". In: *SAC 2016*. Ed. by Roberto Avanzi and Howard M. Heys. Vol. 10532. LNCS. Springer, Cham, Aug. 2016, pp. 14–37. DOI: 10.1007/978-3-319-69453-5_2.

[SS17] John M. Schanck and Douglas Stebila. *A Transport Layer Security (TLS) Extension For Establishing An Additional Shared Secret*. Internet-Draft draft-schanck-tls-additional-keyshare-00. Work in Progress. Internet Engineering Task Force, Apr. 2017. 1–10. URL: https://datatracker.ietf.org/doc/html/draft-schanck-tls-additional-keyshare-00.

[SSW20] Peter Schwabe, Douglas Stebila, and Thom Wiggers. "Post-Quantum TLS Without Handshake Signatures". In: *ACM CCS 2020*. Ed. by Jay Ligatti, Xinming Ou, Jonathan Katz, and Giovanni Vigna. ACM Press, Nov. 2020, pp. 1461–1480. DOI: 10.1145/3372297.3423350.

[SSW21] Peter Schwabe, Douglas Stebila, and Thom Wiggers. "More Efficient Post-quantum KEMTLS with Pre-distributed Public Keys". In: *ESORICS 2021, Part I*. Ed. by Elisa Bertino, Haya Shulman, and Michael Waidner. Vol. 12972. LNCS. Springer, Cham, Oct. 2021, pp. 3–22. DOI: 10.1007/978-3-030-88418-5_1.

[Ste24] Matthias Johann Steiner. "The Complexity of Algebraic Algorithms for LWE". In: *EUROCRYPT 2024, Part III*. Ed. by Marc Joye and Gregor Leander. Vol. 14653. LNCS. Springer, Cham, May 2024, pp. 375–403. DOI: 10.1007/978-3-031-58734-4_13.

[Sul17] Nick Sullivan. *Why TLS 1.3 isn't in browsers yet*. Cloudflare Blog. Dec. 26, 2017. URL: https://blog.cloudflare.com/why-tls-1-3-isnt-in-browsers-yet/.

[SWZ17] John M. Schanck, William Whyte, and Zhenfei Zhang. *Quantum-Safe Hybrid (QSH) Ciphersuite for Transport Layer Security (TLS) version 1.2*. Internet-Draft draft-whyte-qsh-tls12-02. Work in Progress. Internet Engineering Task Force, Jan. 2017. 1–19. URL: https://datatracker.ietf.org/doc/html/draft-whyte-qsh-tls12-02.

[SXY18] Tsunekazu Saito, Keita Xagawa, and Takashi Yamakawa. "Tightly-Secure Key-Encapsulation Mechanism in the Quantum Random Oracle Model". In: *EUROCRYPT 2018, Part III*. Ed. by Jesper Buus Nielsen and Vincent Rijmen. Vol. 10822. LNCS. Springer, Cham, 2018, pp. 520–551. DOI: 10.1007/978-3-319-78372-7_17.

[Tas+22] George Tasopoulos, Jinhui Li, Apostolos P. Fournaris, Raymond K. Zhao, Amin Sakzad, and Ron Steinfeld. "Performance Evaluation of Post-Quantum TLS 1.3 on Resource-Constrained Embedded Systems". In: *Information Security Practice and Experience: 17th International Conference, ISPEC 2022, Taipei, Taiwan, November 23–25, 2022, Proceedings*. Taipei, Taiwan: Springer-Verlag, 2022, pp. 432–451. ISBN: 978-3-031-21279-6. DOI: 10.1007/978-3-031-21280-2_24. URL: https://doi.org/10.1007/978-3-031-21280-2_24.

[Thea] The Go Authors. *crypto/tls package*. URL: https://pkg.go.dev/crypto/tls.

[Theb] The Legion of the Bouncy Castle. *Bouncy Castle Crypto APIs*. URL: https://www.bouncycastle.org/.

[TU16] Ehsan Ebrahimi Targhi and Dominique Unruh. "Post-Quantum Security of the Fujisaki-Okamoto and OAEP Transforms". In: *TCC 2016-B, Part II*. Ed. by Martin Hirt and Adam D. Smith. Vol. 9986. LNCS. Springer, Berlin, Heidelberg, 2016, pp. 192–216. DOI: 10.1007/978-3-662-53644-5_8.

[Uen+22] Rei Ueno, Keita Xagawa, Yutaro Tanaka, Akira Ito, Junko Takahashi, and Naofumi Homma. "Curse of Re-encryption: A Generic Power/EM Analysis on Post-Quantum KEMs". In: *IACR TCHES* 2022.1 (2022), pp. 296–322. DOI: 10.46586/tches.v2022.i1.296-322.

[Why+17] William Whyte, Zhenfei Zhang, Scott Fluhrer, and Oscar Garcia-Morchon. *Quantum-Safe Hybrid (QSH) Key Exchange for Transport Layer Security (TLS) version 1.3*. Internet-Draft draft-whyte-qsh-tls13-06. Work in Progress. Internet Engineering Task Force, Oct. 2017. 19 pp. URL: https://datatracker.ietf.org/doc/html/draft-whyte-qsh-tls13-06.

[Wig24] Thom Wiggers. "Post-Quantum TLS". PhD thesis. Nijmegen, The Netherlands: Radboud University, Jan. 9, 2024. URL: https://thomwiggers.nl/publication/thesis/.

[Xag22] Keita Xagawa. "Anonymity of NIST PQC Round 3 KEMs". In: *EUROCRYPT 2022, Part III*. Ed. by Orr Dunkelman and Stefan Dziembowski. Vol. 13277. LNCS. Springer, Cham, 2022, pp. 551–581. DOI: 10.1007/978-3-031-07082-2_20.

[Xia+22] Wenwen Xia, Leizhang Wang, GengWang, Dawu Gu, and Baocang Wang. *Improved Progressive BKZ with Lattice Sieving*. Cryptology ePrint Archive, Report 2022/1343. 2022. URL: https://eprint.iacr.org/2022/1343.

[Xia+24] Wenwen Xia, Leizhang Wang, Geng Wang, Dawu Gu, and Baocang Wang. "A Refined Hardness Estimation of LWE in Two-Step Mode". In: *PKC 2024, Part II*. Ed. by Qiang Tang and Vanessa Teague. Vol. 14603. LNCS. Springer, Cham, Apr. 2024, pp. 3–35. DOI: 10.1007/978-3-031-57725-3_1.

[XL21] Yufei Xing and Shuguo Li. "A Compact Hardware Implementation of CCA-Secure Key Exchange Mechanism CRYSTALS-KYBER on FPGA". In: *IACR TCHES* 2021.2 (2021), pp. 328–356. ISSN: 2569-2925. DOI: 10.46586/tches.v2021.i2.328-356. URL: https://tches.iacr.org/index.php/TCHES/article/view/8797.

[Xu+22] Zhuang Xu, Owen Pemberton, Sujoy Sinha Roy, David Oswald, Wang Yao, and Zhiming Zheng. "Magnifying Side-Channel Leakage of Lattice-Based Cryptosystems With Chosen Ciphertexts: The Case Study of Kyber". In: *IEEE Transactions on Computers* 71.9 (2022), pp. 2163–2176. DOI: 10.1109/TC.2021.3122997.

[XWT25] Dejun Xu, Kai Wang, and Jing Tian. "A Hardware-Friendly Shuffling Countermeasure Against Side-Channel Attacks for Kyber". In: *IEEE Transactions on Circuits and Systems II: Express Briefs* 72.3 (2025), pp. 504–508. DOI: 10.1109/TCSII.2025.3528751.

[YD17] Yang Yu and Léo Ducas. "Second Order Statistical Behavior of LLL and BKZ". In: *SAC 2017*. Ed. by Carlisle Adams and Jan Camenisch. Vol. 10719. LNCS. Springer, Cham, Aug. 2017, pp. 3–22. DOI: 10.1007/978-3-319-72565-9_1.

[YZ21] Takashi Yamakawa and Mark Zhandry. "Classical vs Quantum Random Oracles". In: *EUROCRYPT 2021, Part II*. Ed. by Anne Canteaut and François-Xavier Standaert. Vol. 12697. LNCS. Springer, Cham, Oct. 2021, pp. 568–597. DOI: 10.1007/978-3-030-77886-6_20.

[ZDY25] Ziyu Zhao, Jintai Ding, and Bo-Yin Yang. "Sieving with Streaming Memory Access". In: *IACR TCHES* 2025.2 (2025), pp. 362–384. DOI: 10.46586/tches.v2025.i2.362-384.

[Zha19] Mark Zhandry. "How to Record Quantum Queries, and Applications to Quantum Indifferentiability". In: *CRYPTO 2019, Part II*. Ed. by Alexandra Boldyreva and Daniele Micciancio. Vol. 11693. LNCS. Springer, Cham, Aug. 2019, pp. 239–268. DOI: 10.1007/978-3-030-26951-7_9.

[ZLJ25] Biming Zhou, Yiting Liu, and Haodong Jiang. "SoK: Post-Quantum Key Encapsulation Mechanisms—Security Definitions and Proof Techniques". In: *Security Standardisation Research*. Springer Nature Switzerland, 2025. DOI: 10.1007/978-3-031-87541-0_6.

付録 D

耐量子計算機暗号への移行に関する技術同行調査

2025 年度外部評価報告書「耐量子計算機暗号への移行に関する技術動向調査」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-3503-2025.pdf）から取得可能である。

耐量子計算機暗号への移行に関する
技術動向調査

株式会社日立製作所

2026 年 1 月

エグゼクティブサマリ

本報告書は、耐量子計算機暗号（PQC）への移行を、暗号アルゴリズムの置換にとどまらないシステム全体の取り組みとして整理する。移行は、業務や、業務で使用する機器が利用する暗号方式の把握（クリプト・インベントリ）、影響評価と優先度付け、方針・計画の策定、段階的な導入・運用という複数段階で進める。移行期には既存の暗号と PQC の併用（ハイブリッド構成）が中心的な選択肢となる。

ハイブリッド構成は、アルゴリズム・プロトコル・システムの各レイヤーで設計される。本報告書では、既存の暗号と PQC を組み合わせる構成を、両者を同時に必須利用して結果を統合する合成（composite）方式と、処理をそれぞれ独立に行い後方互換性を実現する混成（hybrid）方式に分類して整理する。具体的には、鍵共有では複数の鍵共有方式から得られた共有秘密を鍵導出関数（KDF）に入力して統合する枠組みが用いられ、署名では合成方式の署名（コンポジット署名）による安全性維持や代替署名・複数証明書の活用といった混成方式により後方互換性を確保する。安全性に関する整理は、複数要素の組み合わせに依存することから、設計目標と仕様が保証する範囲の区別、実装・運用に起因するリスクへの留意が必要である。

実装・運用面では、OQS／liboqs、OQS-OpenSSL、Bouncy Castle、wolfSSL 等のオープンソースソフトウェア（OSS）やライブラリが検証基盤を提供しており、PKI／メール等では段階的導入の事例が提案されている。性能影響はユースケースに依存するが、クリプトグラフィック・アジリティ（暗号の俊敏性）の確保が移行コストを大きく左右する。

標準化動向として、NIST（ML-KEM／ML-DSA、SP 800-227、SP 800-56C Rev.2）、IETF（TLS ハイブリッド鍵共有、ハイブリッド KEM／署名、MLS コンバイナ、RFC 9794）、ETSI（TS 103 744）が挙げられ、産業連携では Post-Quantum Cryptography Coalition（PQCC）がロードマップ等を通じて、移行戦略と設計指針の枠組みを提供している。

本報告書では、移行課題、導入プロセス、ハイブリッド構成の具体化、安全性整理、実装・運用事例、標準化動向を体系的に記述する。最終的な完全移行を見据えつつ、移行期間のリスク低減と相互運用性の確保を重視する。

9. 参考文献

[1] CRYPTREC 暗号技術調査ワーキンググループ（耐量子計算機暗号），“CRYPTREC 暗号技術ガイドライン（耐量子計算機暗号）2024 年度版，” 3 2025. [オンライン]. Available: https://www.cryptrec.go.jp/report/cryptrec-gl-2007-2024.pdf.

[2] CRYPTREC 暗号技術調査ワーキンググループ（耐量子計算機暗号），“耐量子計算機暗号の研究動向調査報告書，” 3 2025. [オンライン]. Available: https://www.cryptrec.go.jp/report/cryptrec-tr-2001-2024.pdf.

[3] レピダム，“ハイブリッドモードの技術動向調査，” 12 2020. [オンライン]. Available: https://www.cryptrec.go.jp/exreport/cryptrec-ex-3004-2020.pdf.

[4] NIST, “Mechanisms Recommendations for Key-Encapsulation Mechanisms,” 9 2025. [オンライン]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-227.pdf.

[5] デジタル庁・総務省・経済産業省，“電子政府における調達のための参照すべき暗号のリスト（CRYPTREC 暗号リスト），” 16 5 2023. [オンライン]. Available: https://www.cryptrec.go.jp/list/cryptrec-ls-0001-2022r1.pdf.

[6] K. Moriarty, B. Kaliski, J. Jonsson , A. Rusch, “PKCS #1: RSA Cryptography Specifications Version 2.2,” 11 2016. [オンライン]. Available: https://datatracker.ietf.org/doc/html/rfc8017.

[7] R. Housley , S. Turner, “Use of the RSA-KEM Algorithm in the Cryptographic Message Syntax (CMS),” 2 2025. [オンライン]. Available: https://datatracker.ietf.org/doc/rfc9690/.

[8] PQCC, “Post-Quantum Cryptography (PQC) Migration Roadmap,” 5 2025. [オンライン]. Available: https://pqcc.org/wp-content/uploads/2025/05/PQC-Migration-Roadmap-PQCC-2.pdf.

[9] NIST, “NIST Special Publication 800-56C Recommendation for Key-Derivation Methods in Key-Establishment Schemes, ” 8 2020. [オンライン]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Cr2.pdf.

[10] D. Connolly, R. Barnes , P. Grubbs, “Hybrid PQ/T Key Encapsulation Mechanisms,” 20 10 2025. [オンライン]. Available: https://datatracker.ietf.org/doc/draft-irtf-cfrg-hybrid-kems/07/.

[11] M. Ounsworth, J. Gray, M. Pala, J. Klaußner , S. Fluhrer, “Composite ML-KEM for use in X.509 Public Key Infrastructure, ” 7 1 2026. [オンライン]. Available: https://datatracker.ietf.org/doc/draft-ietf-lamps-pq-composite-kem/12/.

[12] M. Ounsworth, J. Gray, M. Pala, J. Klaußner , S. Fluhrer, “Composite ML-DSA for use in X.509 Public Key Infrastructure, ” 8 1 2026. [オンライン]. Available: https://datatracker.ietf.org/doc/draft-ietf-lamps-pq-composite-sigs/14/.

[13] E. Rescorla, “The Transport Layer Security (TLS) Protocol Version 1.3,” 7 3 2020. [オンライン]. Available: https://datatracker.ietf.org/doc/rfc8446/.

[14] D. Stebila, S. Fluhrer , S. Gueron, “Hybrid key exchange in TLS 1.3,” 18 11 2025. [オンライン]. Available: https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/16/.

[15] X. Tian, B. Hale, M. Mularczyk , Joël, “Amortized PQ MLS Combiner,” 4 11 2025. [オンライン]. Available: https://datatracker.ietf.org/doc/draft-ietf-mls-combiner/02/.

[16] ETSI, “ETSI TS 103 744 V1.2.1 CYBER; Quantum-Safe Cryptography (QSC); Quantum-safe Hybrid Key Establishment, ” 3 2025. [オンライン]. Available: https://www.etsi.org/deliver/etsi_ts/103700_103799/103744/01.02.01_60/ts_103744v010201p.pdf.

[17] IEEE, “Proposed Texts for Hybrid PQC, ” 25 11 2025. [オンライン]. Available: https://mentor.ieee.org/802.11/dcn/25/11-25-2051-01-00bt-proposed-texts-for-hybrid-pqc.docx.

[18] T. Okubo, C. Bonnell, J. Gray, M. Ounsworth , J. Mandel, “A Mechanism for X.509 Certificate Discovery,” 19 11 2025. [オンライン]. Available: https://datatracker.ietf.org/doc/draft-ietf-lamps-certdiscovery/02/.

[19] ITU, “ITU-T Recommendations,” 10 2019. [オンライン]. Available: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.509.

[20] M. Ounsworth, “ “Architecting PKI Hierarchies for Graceful Post-Quantum Migration,” presented at the PKI Consortium Post-Quantum Cryptography Conference 2025,” 1 2025. [オンライン]. Available: https://pkic.org/events/2025/pqc-conference-austin-us/WED_BREAKOUT_1200_Mike-Ounsworth_Architecting-PKI-Hierarchies-for-Graceful-PQ-Migration.pdf.

[21] J. Klaußner, “ “Hybrid PQC E-Mail Communication: Easing Migration Pain,” presented at the Post-Quantum Cryptography Conference 2025, ” 1 2025. [オンライン]. Available: https://pkic.org/events/2025/pqc-conference-austin-us/WED_BREAKOUT_1430_Jan-Klaussner_Hybrid-PQC-E-Mail-Communication-Easing-Migration-Pain.pdf.

[22] NIST, “NIST IR 8547 ipd Transition to Post-Quantum,” 11 2024. [オンライン]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf.

[23] F. D, M. P , B. Hale, “RFC 9794 Terminology for Post-Quantum Traditional Hybrid Schemes,” 13 6 2025. [オンライン]. Available: https://datatracker.ietf.org/doc/rfc9794/.

[24] N. Bindel, B. Hale, D. Connolly , F. D, “Hybrid signature spectrums,” 17 9 2025. [オンライン]. Available: https://datatracker.ietf.org/doc/draft-ietf-pquip-hybrid-signature-spectrums/07/.

[25] L. Chen, “Cryptographic Agility and Transition R&D and Plans,” 21 3 2024. [オンライン]. Available: https://csrc.nist.gov/Presentations/2024/cryptographic-agility-and-transition-rd-and-plans.

[26] Open Quantum Safe Project, “Open Quantum Safe, ” [オンライン]. Available: https://openquantumsafe.org/.

[27] Open Quantum Safe Project, “liboqs: C library for post-quantum cryptography,” [オンライン]. Available: https://github.com/open-quantum-safe/liboqs.

[28] Open Quantum Safe Project, “OQS-OpenSSL, ” [オンライン]. Available: https://github.com/open-quantum-safe/openssl.

[29] The Legion of the Bouncy Castle, “Bouncy Castle Crypto APIs,” [オンライン]. Available: https://www.bouncycastle.org/.

[30] wolfSSL Inc., “Hybrid Post-Quantum Key Exchange in wolfSSL,” [オンライン]. Available: https://www.wolfssl.com/hybrid-post-quantum-key-exchange-in-wolfssl-5-8-0/.

[31] PKI Consortium, “Post-Quantum Cryptography Conference,” 15-16 1 2025. [オンライン]. Available: https://pkic.org/events/2025/pqc-conference-austin-tx/.

[32] PKI Consortium, “Post-Quantum Cryptography Conference,” 28-30 10 2025. [オンライン]. Available: https://pkic.org/events/2025/pqc-conference-kuala-lumpur-my/.

[33] M. Marcus, “"Real-World Post-Quantum Migrations: Lessons Learned and Performance Results,” presented at the Post-Quantum Cryptography Conference 2025,” 10 2025. [オンライン]. Available: https://pkic.org/events/2025/pqc-conference-kuala-lumpur-my/THU_P_1400_michiel-marcus_real-world-post-quantum-migrations-lessons-learned-and-performance-results_merged.pdf.

[34] S. Kelly, “The Internet Is Ready for Some PQC Certificates,” presented at the Post-Quantum Cryptography Conference 2025, ” 10 2025. [オンライン]. Available: https://pkic.org/events/2025/pqc-conference-kuala-lumpur-my/WED_B_1130_shane-kelly_the-internet-is-ready-for-some-pqc-certificates_merged.pdf.

[35] S. Barker, “X25519Kyber768: Paving the Way for Post-Quantum Security,” 21 9 2024. [オンライン]. Available: https://expertbeacon.com/x25519kyber768-paving-the-way-for-post-quantum-security/.

[36] Google, “Protecting Chrome Traffic with Hybrid Kyber KEM,” 10 8 2023. [オンライン]. Available: https://blog.chromium.org/2023/08/protecting-chrome-traffic-with-hybrid.html.

[37] NIST, “ Post-Quantum Cryptography, ” 3 1 2017. [オンライン]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/call-for-proposals.

[38] NIST, “ NIST SP 1800-38 Migration to Post-Quantum Cryptography: Preparation for Considering the Implementation and Adoption of Quantum Safe Cryptography,” 19 12 2023. [オンライン]. Available: https://csrc.nist.gov/pubs/sp/1800/38/iprd-(1).

[39] B. Halee, X. Tiane , L. Wang, “Benchmarking of the Amortized Post Quantum Combiner for MLS,” 8 1 2026. [オンライン]. Available: https://eprint.iacr.org/2026/034.pdf.

[40] ITU, “Overview of hybrid approaches for key exchange with quantum key distribution,” 20 5 2022. [オンライン]. Available: https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-ICTS-2022-1-PDF-E.pdf.

[41] ETSI, “ETSI TR 103 966 V1.1.1 CYBER Security (CYBER);Quantum-Safe Cryptography (QSC); Deployment Considerations for Hybrid Schemes,” 10 2024. [オンライン]. Available: https://www.etsi.org/deliver/etsi_tr/103900_103999/103966/01.01.01_60/tr_103966v010101p.pdf.

[42] ETSI, “ETSI TS 104 015 V1.1.1 Cyber Security (CYBER); Quantum-Safe Cryptography (QSC); Efficient Quantum-Safe Hybrid Key Exchanges withHidden Access Policies,” 2 2025. [オンライン]. Available: https://www.etsi.org/deliver/etsi_ts/104000_104099/104015/01.01.01_60/ts_104015v010101p.pdf.

[43] IEEE, “ Standard for Post-Quantum Network Security, ” [オンライン]. Available:

https://standards.ieee.org/ieee/1943/10957/.

[44] L. CHEN, “PAVING THE RUNWAY FOR STANDARDIZATION OF POST-QUANTUM CRYPTOGRAPHY,” *SC27 Journal,* 第 巻 Vol 1, 第 Issue 3, pp. pp. 11-19, 2 2022.

[45] ASC X9, “New X9 Report Supplies Guidance on Migrating to Post-quantum Cryptography Safely and Cost-effectively,” 8 2025. [オンライン]. Available: https://x9.org/new-x9-report-migrating-to-post-quantum-cryptography/.

[46] NSA, “Announcing the Commercial National Security,” 9 2022. [オンライン]. Available: https://media.defense.gov/2025/May/30/2003728741/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS.PDF.

[47] NSA, “CSfC Post Quantum Cryptography Guidance Addendum 1.0,” 4 4 2025. [オンライン]. Available: https://www.nsa.gov/Portals/75/documents/resources/everyone/csfc/capability-packages/CSfC%20Post%20Quantum%20Cryptography%20Guidance%20Addendum%201_0%20Draft%20_5.pdf.

[48] CSA, “A Practitioner’s Guide to Post-Quantum Cryptography,” 10 11 2025. [オンライン]. Available: https://cloudsecurityalliance.org/artifacts/a-practitioners-guide-to-post-quantum-cryptography.

[49] PQCRYPTO , “Post-Quantum Cryptography for Long-Term Security,” 9 4 2018. [オンライン]. Available: https://pqcrypto.eu.org/deliverables/d5.2-final.pdf.

[50] P. Kampanakis , D. V. Geest, “Artifact Signing: Dual, Post-Quantum/Traditional Hybrid Signatures and Downgrades,” 4 2025. [オンライン]. Available: https://pqcc.org/artifact-signing-dual-post-quantum-traditional-hybrid-signatures-and-downgrades/.

付録 E

学会等での主要論文一覧

目次

E.1 暗号技術の安全性評価に関する論文一覧

表 E.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 E.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
★	pyecsca: Reverse engineering black-box elliptic curve cryptography via side-channel analysis	CHES 2024	114
	Exploiting Small-Norm Polynomial Multiplication with Physical Attacks: Application to CRYSTALS-Dilithium	CHES 2024	115
★	Defeating Low-Cost Countermeasures against Side-Channel Attacks in Lattice-based Encryption: A Case Study on Crystals-Kyber	CHES 2024	115
★	Carry Your Fault: A Fault Propagation Attack on Side-Channel Protected LWE-based KEM	CHES 2024	116
	Correction Fault Attacks on Randomized CRYSTALS-Dilithium	CHES 2024	116
★	Hints from Hertz: Dynamic Frequency Scaling Side-Channel Analysis of Number Theoretic Transform in Lattice-Based KEMs	CHES 2024	117
★	Kleptographic Attacks against Implicit Rejection	PKC 2025	119
	Public-Algorithm Substitution Attacks: Subverting Hashing and Verification	PKC 2025	120
	The Security of Hash-and-Sign with Retry Against Superposition Attacks	PKC 2025	121
	Thorough Power Analysis on Falcon Gaussian Samplers and Practical Countermeasure	PKC 2025	121
	Finding a polytope: A practical fault attack against Dilithium	PKC 2025	122
	One Bit to Rule Them All - Imperfect Randomness Harms Lattice Signatures	PKC 2025	123
	Intermundium-DL: Assessing the Resilience of Current Schemes to Discrete-Log-Computation Attacks on Public Parameters	PKC 2025	124
	Memory-Efficient BKW Algorithm for Solving the LWE Problem	PKC 2025	124
	Worst and Average Case Hardness of Decoding via Smoothing Bounds	PKC 2025	125
	Multiple Group Action Dlogs With(out) Precomputation	PKC 2025	126
	Giant Does NOT Mean Strong: Cryptanalysis of BQTRU	PQCrypto 2025	131
	Analysis of REDOG: The Pad Thai Attack	PQCrypto 2025	132
	Efficient Theta-Based Algorithms for Computing (ℓ, ℓ)-Isogenies on Kummer Surfaces for Arbitrary Odd ℓ	PQCrypto 2025	132
	Cryptanalysis of an Efficient Signature Based on Isotropic Quadratic Forms	PQCrypto 2025	133
	Shifting Our Knowledge of MQ-Sign Security	PQCrypto 2025	133
	Et tu, Brute? Side-Channel Assisted Chosen Ciphertext Attacks Using Valid Ciphertexts on HQC KEM	PQCrypto 2025	134

	Significantly Improved Cryptanalysis of Salsa20 with Two-Round Criteria	FSE 2025	126
	Perfect Monomial Prediction for Modular Addition	FSE 2025	127
	Finding Complete Impossible Differential Attacks on AndRX Ciphers and Efficient Distinguishers for ARX Designs	FSE 2025	127
	Exact Formula for RX-Differential Probability through Modular Addition for All Rotations	FSE 2025	128
	On Impossible Boomerang Attacks: Application to Simon and SKINNYee	FSE 2025	128
	Extending the Quasidifferential Framework: From Fixed-Key to Expected Differential Probability	FSE 2025	129
	AutoDiVer: Automatically Verifying Differential Characteristics and Learning Key Conditions	FSE 2025	129
	Links between Quantum Distinguishers Based on Simon's Algorithm and Truncated Differentials	FSE 2025	130
★	Improved Cryptanalysis of ChaCha: Beating PNBs with Bit Puncturing	Eurocrypt 2025	20
★	Guess-and-Determine Rebound: Applications to Key Collisions on AES	Crypto 2025	21
★	Triangulating Meet-in-the-Middle Attack	Crypto 2025	22
	Unlocking Mix-Basis Potential: Geometric Approach for Combined Attacks	Crypto 2025	159
	Breaking the IEEE Encryption Standard – XCB-AES in Two Queries	Crypto 2025	160
	Improved Resultant Attack against Arithmetization-Oriented Primitives	Crypto 2025	160
★	Practical Opcode-based Fault Attack on AES-NI	CHES 2025	22
	All You Need is XOR-Convolution: A Generalized Higher-Order Side-Channel Attack with Application to XEX/XE-based Encryptions	CHES 2025	168
★	Scrutinizing the Security of AES-based Hashing and One-way Functions	Asiacrypt 2025	23
★	Divide-and-Conquer Trail Enumeration Puncturing: Application to Salsa and ChaCha	Asiacrypt 2025	23
★	Quantum Circuit Synthesis for AES with Low DW-cost	Asiacrypt 2025	24
	Understanding Unexpected Fixed-Key Differential Behaviours: How to Avoid Major Weaknesses in Lightweight Designs	Asiacrypt 2025	179
	Vectorial Fast Correlation Attacks	Asiacrypt 2025	180
	Persistence of Hourglass(-like) Structure: Improved Differential-Linear Distinguishers for Several ARX Ciphers	Asiacrypt 2025	180
	Enhancing the DATF Technique in Differential-Linear Cryptanalysis	Asiacrypt 2025	181
	Integral cryptanalysis in characteristic p	Asiacrypt 2025	182
	SPEEDY: Caught at Last	Asiacrypt 2025	182
	The State-Test Technique on Differential Attacks: a 26-Round Attack on CRAFT and Other Applications	Asiacrypt 2025	182
	Quantum Periodic Distinguisher Construction: Symbolization Method and Automated Tool	Asiacrypt 2025	183

	Algebraic Cryptanalysis of AO Primitives Based on Polynomial Decomposition: Applications to RAIN and Full AIM-I/III/V	Asiacrypt 2025	183
暗号利用モード		会議名	頁
	How to Recover the Full Plaintext of XCB	Crypto 2025	161
ハッシュ関数		会議名	頁
★	Practical Preimage Attacks on 3-Round Keccak-256 and 4-Round Keccak[$r = 640, c = 160$]	FSE 2025	25
	An Efficient Collision Attack on Castryck-Decru-Smith's Hash Function	PQCrypto 2025	139
★	Preimage Attacks on up to 5 Rounds of SHA-3 Using Internal Differentials	Eurocrypt 2025	25
★	New Collision Attacks on Round-Reduced SHA-512	Crypto 2025	26
★	Improved Semi-Free-Start Collision Attacks on RIPEMD-160	Asiacrypt 2025	26
認証暗号		会議名	頁
	SoK: Security of the Ascon Modes	FSE 2025	130
	Dynamic Cube Attacks against Grain-128AEAD	FSE 2025	131
	Improved Conditional Cube Attacks on Ascon AEADs in Nonce-Respecting Settings: with a Break-Fix Strategy	FSE 2025	131
その他		会議名	頁
	Quantum Circuit Reconstruction from Power Side-Channel Attacks on Quantum Computer Controllers	CHES 2024	119
	Password-Hardened Encryption Revisited	Asiacrypt 2025	184
	Universally Composable Password-Hardened Encryption	Asiacrypt 2025	184
	A Crack in the Firmament: Restoring Soundness of the Orion Proof System and More	Asiacrypt 2025	185

E.2 FDTC 2024

Fault injection attacks exploiting high voltage pulsing over Si-substrate backside of IC chips

Yusuke Hayashi, Rikuu Hasegawa, Takuya Wadatsumi, Kazuki Monta, Takuji Miki, Makoto Nagata

フリップチップ BGA（Ball Grid Array）パッケージは、従来のワイヤボンディングフェースアップパッケージと比較して、短い信号線と小さいフットプリントといった利点を持つ。これらの性質は 2.5D や 3D パッケージのような高度なパッケージ技術にもよく適している。ハードウェアセキュリティの観点では、攻撃者は IC チップの裏面に容易にアクセスでき、シリコン substrate をコンタクトポイントとしてフォールトインジェクションやサイドチャネル攻撃を行うことができる。

この論文では、IC チップがロープロファイルやチップのスタッキングのためより薄くなることで high voltage pulsing（HVP）injection が IC にとって深刻な脅威になり得ることを示している。最初に、表面からと裏面からのインジェクションを比較するシミュレーションを行うことで、裏面からの HVP injection が対象の回路の小さい領域へのフォールトを引き起こす特性があり、この特性の背後にある物理的なメカニズムを説明する。さらに、この特性は IC チップがより薄くなるにつれより顕著になることも示す。次に、シリコンプロトタイプチップを用意し、この特性を実験結果によって確かめる。シリコン substrate の裏面からの HVP がエリア内のフリップフロップ（各フリップフロップのサイズは 13 µm × 3µm）を 50µm × 50µm の精度で標的にし、標的のバイトに対応するビット反転を再現性をもって引き起こすことができることが示される。最後に、AES-128 への differential fault analysis（DFA）を実行して秘密鍵全体を復元することでこの攻撃の脅威を実証している。

E.3 CHES 2024

pyecsca: Reverse engineering black-box elliptic curve cryptography via side-channel analysis

Jan Jancar, Vojtech Suchanek, Petr Svenda, Vladimir Sedlacek, Lukasz Chmielewski

楕円曲線暗号に対するサイドチャネル攻撃は、攻撃対象において選択された実装に関する詳細な知識があるホワイトボックス攻撃者であることを仮定していることが多い。しかし、楕円曲線暗号の実装は低レベルの算術処理から高レベルのプロトコル処理まで多段階の要素からなり、その実装には多くの選択肢がある。具体的には楕円曲線のモデル、座標系、加算演算の式、スカラー倍の計算方式や、有限体上の乗算方法のような実装の詳細が含まれる。この複雑さは攻撃に要求される理想的な攻撃者と、実装の知識を持たないブラックボックス的なアクセスしか持ち合わせない現実の攻撃者とのギャップをもたらす。そのギャップが埋まることで TPM-Fail、Minerva、Side Journey to Titan、TPMScan に代表される攻撃のように、現実的な楕円曲線の実装へのサイドチャネル攻撃が可能となる。

本論文では、オープンソースの楕円曲線ライブラリの解析を通じて現実的に選択される実装を分類、それらの組み合わせを網羅する枠組みを固定、楕円曲線暗号のブラックボックス実装に対して自動的にリバースエンジニアリングを行う手法を与えた。楕円曲線暗号のサイドチャネル攻撃に使えるオープンソースでドキュメントつきのツールキット pyecsca を発表した。

pyecsca の実装コードは `https://github.com/J08nY/pyecsca` で、ドキュメントは `https://pyecsca.org/` で公開されている。

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

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

ML-DSA（CRYSTALS-Dilithium）に対するサイドチャネル攻撃に関する論文である。CRYSTALS-Dilithium は Module-LWE 問題を安全性の根拠とした Fiat-Shamir with abort 型の署名方式であり、実装時に多項式環 $\mathbb{Z}_q[X]/(X^{256}+1)$ 上での演算を多用している。署名生成サブルーチンでは、メッセージに対して署名生成 $z = y + sc \mod q$ を計算し、そのノルムが大きな場合には乱数を再サンプリングし再計算を行う。

この論文では、サイドチャネル情報として $x = c \cdot s$ と y に関するハミング重みの情報が漏洩した場合の、正規の署名からの鍵復元攻撃、z のノルムが大きく署名生成時に再サンプリングの対象となった署名からの鍵復元攻撃、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。解析として、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行っており、サイドチャネルの SNR 比にもよるがいずれも数個から数千個のトレースを用いた現実的な想定で Dilithium のレベル 2,3,5 の鍵復元が可能であるとの結論に達している。

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

NIST 標準化方式 ML-KEM のベースとなった 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攻撃に対する対策の多くは、低コストで実行可能な検出技術に基づく方法として分類できる。これらは悪意のある入力を検出し、それらをブロックすることで対策を行う。本論文では低コスト検出の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の 2 つを取り上げ、これらの対策手法を無効化する一般的な攻撃手法を提案する。

暗号文の整合性チェックに関する結果：サイドチャネル攻撃の先行研究の多くが、低エントロピーの暗号文をオラクルに入力するという特徴を持つ。その対策がエントロピーのチェック機構を持つ実装であると仮定し、攻撃に用いる暗号文の中でエントロピーが低いものを弾くことで、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結果：エラーを検出した際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行われないような対策が実装されていると仮定する。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を示す。復号関数のサイドチャネル情報から連立不等式を解くことで秘密鍵の復元が可能である。技術的には Pessl と Prokop（TCHES 2021）の信頼度伝搬法に基づいたものであり、先行研究と比較して必要な不等式の数を半分にしている。

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

NIST 標準化方式 ML-KEM のベースとなった CRYSTALS-Kyber および格子ベース公開鍵暗号 SABER のサイドチャネル攻撃に関する論文である。

LWE ベースの KEM に対する新たな故障注入攻撃の提案を行っている。攻撃の対象となる箇所は、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である。Delvaux（TCHES2022）での考察では、マスキングのために導入された機構と内部の乱数性により、攻撃者が得られるサイドチャネル情報が増えてしまい、故障注入攻撃の成功確率を上げることが示唆されていた。本来セキュリティを強化するために導入された仕組みがかえって脆弱性を生むという状況の発見であり、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。

著者らは多項式環の加算回路の保護を目的とした 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るかどうかの情報から秘密鍵が満たす連立不等式を構成し、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。

実験として、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。

Correction Fault Attacks on Randomized CRYSTALS-Dilithium

Elisabeth Krahmer, Peter Pessl, Georg Land, Tim Güneysu

ML-DSA（CRYSTALS-Dilithium）に対するサイドチャネル攻撃に関する論文である。CRYSTALS-Dilithium は NIST 耐量子計算機暗号標準化プロジェクトで 2022 年に標準化された格子ベース署名である。実装時の安全性のために、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。randomized mode 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でこのモードが選択される仕様である。この論文では、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を検討し、randomized mode でも安全ではない可能性を指摘している。

攻撃の基本的な戦略は署名生成ルーチンに対して故障注入を行い、不正な署名を複数生成しそれらが署名検証ルーチンで受理されるかどうかをチェック、得られた情報から格子基底簡約により秘密鍵情報を復元するという、先行研究のフレームワークを引き継いだものである。論文では命令スキップによる攻撃と、公開鍵行列 A の内容を操作する攻撃の検討が行われている。

Dilithium-2（128 ビットセキュリティ）のパラメータに対して、前者の攻撃では 1024 個の不正な署名から、後者では 512 個の不正な署名から鍵復元が可能であるとしている。また、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 KEM、特に CRYSTALS-Kyber、NTRU へのサイドチャネル攻撃を扱った論文である。

環構造や加群構造を持つ格子問題をベースとした格子暗号の実装においては、高速化のため数論変換（NTT: Number Theoretic Transform）が用いられる。NTT に関連する処理は重く、攻撃の対象となりやすい。本論文では、近年の CPU ハードウェアに備わる、処理内容に合わせた電圧や動作周波数の調節機構に対するサイドチャネル攻撃の可能性を検討している。具体的には、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が提案された。実証実験として、Intel Core-i7-9600K を用いた 20 万回の計測データを平均することで情報が抽出可能であること、CRYSTALS-Kyber、NTRU の復号ルーチンに対して解析を行うこと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明らかにしている。

Evict+Spec+Time: Exploiting Out-of-Order Execution to Improve Cache-Timing Attacks

Shing Hing William Cheng, Chitchanok Chuengsatiansup, Daniel Genkin, Dallas McNeil, Toby Murray, Yuval Yarom, Zhiyuan Zhang

投機的アウトオブオーダー実行は、後の命令を先の命令の前に実行することを許容することにより実行レイテンシを低減する技術である。この技術による暗号の安全性への影響はかつてはないと考えられてきたものの、2018 年に公表された Spectre 攻撃 [Koruyeh et al, USENIX 2018] および Meltdown 攻撃 [Lipp et al., USENIX 2018] の登場以来脚光を浴びている。これらの攻撃は、マイクロアーキテクチャのサイドチャネルが、通常のプログラム実行では実行されない投機的に実行される命令によってアクセスされる機密データを漏洩させ得ることを実証した。以来、投機的アウトオブオーダー実行からのデータ漏洩の原理的な理解と防御手法の調査に多大な努力が注がれているものの、依然として未知の部分が多い。

本論文では、投機的実行がどのように Evict+Time キャッシュ攻撃に影響するかを調査した。Evict+Time 攻撃の原理は、キャッシュミス時のコード実行時間がキャッシュヒット時よりも長くなることを用いて、実行時間の観測からキャッシュミスを検出することにある。しかしながら、キャッシュミス時においてもアウトオブオーダーでは待機している別の命令を先に実行することが可能であり、結果としてヒット時とミス時の実行時間の違いは検出できないほどに小さい。CPU の物理的な制限から、キャッシュミス時に命令を待機させるバッファは有限であり、それが溢れることで実行時間の違いが起きる。攻撃者が NOP 命令を挿入することでキャッシュを溢れさせ、実行コードのどこでキャッシュミスが発生したのかが判断可能であることを実証している。

著者らは、Evict+Time の変種でありキャッシュミスが起きたかどうかだけでなく攻撃対象のコードのどこで起きたかの情報が得られる Evict+Spec+Time 攻撃を設計し、T-table ベースの AES 実装に対する攻撃能力が桁違いに高いことを実証している。さらに、AES の S-Box ベースの実装への Evict+Spec+Time 攻撃が 14815 回の復号で鍵復元が可能であり、AES に対する最初の Evict+Time 型攻撃の成功例であると報告している。

Switching Off your Device Does Not Protect Against Fault Attacks

Paul Grandamme, Pierre-Antoine Tissot, Lilian Bossuet, Jean-Max Dutertre, Brice Colombier, Vincent Grosso

AES を実装した組込みシステムへの故障注入攻撃に関する論文である。

故障注入攻撃の中でもレーザーを用いたものは空間的に極めて正確であるという特徴があるため、多くの先行研究で故障注入の実証実験に用いられてきた。これらの攻撃を成功させるためには高精度のレーザー照射が必要であり、実装と攻撃対象コードの正確な実行タイミングをあらかじめ知っている必要がある。

本研究の主な貢献は、電源が入っていない装置へのレーザーによる故障注入攻撃が可能であることの実証実験である。具体的には 32 ビットマイクロコントローラ STM32F1 上の 128KB 内蔵不揮発性フラッシュメモリに対してレーザーを照射することで、128 ビット AES の S-Box が格納されているメモリ上に永続的な故障を引き起こし、鍵復元を行っている。

この攻撃は、ハードウェアに永続的な故障を引き起こす攻撃フレームワークである persistent fault analysis（PFA）として分類され、攻撃のタイミングとハードウェアの実行を同期させる必要が無いという特徴をもつ。論文では、物理レベルからソフトウェアレベルまでの故障モデルの説明と、この攻撃フレームワークの実験的特性を議論している。

All You Need Is Fault: Zero-Value Attacks on AES and a New λ-Detection

Haruka Hirata, Daiki Miyahara, Victor Arribas, Yang Li, Noriyuki Miura, Svetla Nikova, Kazuo Sakiyama

組込みシステムに暗号を組み込むには物理攻撃へのセキュリティが必要である。CHES 2019 において、Masks and Macs（M&M）が、サイドチャネル攻撃に対抗するマスキングとフォールトアタックに対抗する情報理論的 MAC タグを組み合わせた対策として提案された。

本論文では、M&M の論文にある AES のひとつの対策あり実装が zero-value SIFA2-like attack[*1]に対して脆弱であることを示す。実用的な攻撃を ASIC ボードで実証する。著者は 2 つのバージョンの攻撃を提案する。第一の攻撃は SIFA（Statistical Ineffective Fault Analysis）のアプローチに従って最後のラウンドにフォールトを注入するのに対し、第二の攻撃は SIFA と FTA（Fault Template Attacks）の拡張であり選択平文を用いて最初のラウンドに適用する。この 2 つのバージョンはバイトレベルで動作するが、後者は攻撃の効率を著しく向上させる。さらに、著者はこの zero-value SIFA2 攻撃が AES tower-field decomposed S-box 設計に特化していることも示す。したがって、そのような攻撃はこの AES S-Box アーキテクチャを特徴とするあらゆる実装に適用可能である。

そこで、著者はこれらの攻撃を防止する対策を提案する。著者は M&M を、zero-value グリッチ攻撃を検出できるきめ細かい検出ベースの機能で拡張する。この努力により、クロネッカーのデルタ関数を用いた M&M スキームの暗号文出力チェックに対する復号攻撃の問題も解決する。この対策を FPGA に実装し、フォールトとサイドチャネル攻撃の両方に対する安全性を実用的な実験により検証する。

[*1] Sayandeep Saha, Arnab Bag, Debapriya Basu Roy, Sikhar Patranabis, and Debdeep Mukhopadhyay, “Fault template attacks on block ciphers exploiting fault propagation”, Advances in Cryptology – EUROCRYPT 2020, pages 612–643. Springer, 2020.

Quantum Circuit Reconstruction from Power Side-Channel Attacks on Quantum Computer Controllers

Ferhat Erata, Chuanqi Xu, Ruzica Piskac, Jakub Szefer

近年量子コンピュータの開発が進んでいるが、それらは全て遠隔地に置かれたマシンをクラウドサービスなどを通じて扱うものであり、どのような情報が漏れているのかに関する研究は進んでいない。この論文では、量子デバイスの電力消費に関する情報から、量子コンピュータを制御するためのコントロールパルスの情報を復元し、入力された量子回路のゲートレベルでの記述を回復可能であることを示す。

具体的には量子ビットを制御するチャネルごとの観測結果から総当たり法により量子回路を復元する手法と、制御システム全体の消費電力の情報から Mixed-Integer Linear Programming（MILP）を用いて復元する手法が提案されており、どちらも single-shot のものである。

実験として、ibm_lagos デバイス上でいくつかのベンチマーク用回路を動かし、IBM Quantum の提供するパルスとキャリブレーションの情報から電力トレースを再構成し、その情報をもとに実際の量子回路が復元可能であることが示された。

E.4 PKC 2025

Kleptographic Attacks against Implicit Rejection

Antoine Joux, Julian Loss, Benedikt Wagner

藤崎-岡本変換により構成された KEM の安全性に関する論文である。NIST PQC 標準化方式である ML-KEM（CRYSTALS-Kyber）等の、鍵デカプセル化ルーチンで implicit rejection を用いる KEM の安全性に関連する。

kleptography は 1990 年代に作られた造語 [Young-Yung, Crypto 1996] であり、ギリシャ語由来の klepto（盗む）と cryptography を組み合わせた、暗号アルゴリズムの一部を不正なものに置き換えることで情報を盗み出すことを目的とした攻撃フレームワークを指す。Algorithm-substitution attacks (ASA) とも呼ばれる。（PKE 2025 の Bellare-Riepel-Shea も参照）

本論文が攻撃の対象とするのは、公開鍵暗号を藤崎-岡本変換（FO) した KEM のデカプセル化内の整合性チェックルーチンである。デカプセル化時の整合性チェックでは、復号された平文 m' を暗号化時と同一の乱数シードを用いて再暗号化し、入力と同じ暗号文が得られるかどうかが判定される。整合性チェックに失敗した場合の挙動として、失敗記号 $\perp$ を返す explicit rejection と疑似乱数生成器の出力を返す implicit rejection の変種が考えられる。

本論文では、Kleptographic な攻撃により KEM の鍵生成および鍵デカプセル化ルーチンが不正なアルゴリズムに、利用者から検出不可能な形で置き換えられた以下の 3 種の状況での大幅な安全性の低下を議論している。

(1) 鍵デカプセル化ルーチンの implicit rejection は通常、暗号文 c と鍵カプセル化時の秘密鍵 s のハッシュ値から計算されるが、その中に暗号化の秘密鍵 sk' の部分情報を含めるようなルーチンに置き換えることで攻撃者は implicit rejection の出力から秘密鍵を復元することが可能となる。このとき、攻撃者も自身の公開鍵暗号を用いて部分情報を暗号化することで、別の利用者からは implicit rejection の出力が疑似乱数と識別不可能となる。（ただし処理速度の低下から検出できる可能性はある。）また、別の攻撃者がリバースエンジニアリング等によりコードを復元したとしても、公開鍵暗号の安全性によりコードの情報から同様の攻撃を行うことは困難である。

(2) 鍵生成ルーチンにおける s（implicit rejection 時のハッシュ関数への入力の一部）の生成ルーチンを乱数生成器

から sk' の部分情報と攻撃者の鍵のハッシュ値に置き換えることで、implicit rejection の出力から秘密鍵の復元を行うことが可能となる。この攻撃の検出はコードのリバースエンジニアリングをしない限りは検出困難であるとしている。ただしコード内容を知られた場合、内部にある攻撃者の秘密鍵 ask を用いて同様の攻撃が可能となる点が (1) と異なる。

(3) (2) の攻撃におけるハッシュ関数の逆像探索の Hellman table を用いた時間-空間トレードオフが可能である。

本論文の手法による 256 ビットセキュリティ Kyber の安全性低下が具体的に求められている。特に、(1) のデカプセル化ルーチンの置き換え攻撃は非常に少ないリソースでほぼ完全に破られる。一方で、(2)(3) の鍵生成ルーチンの置き換えでは 2^7 空間 2^{130} 時間、もしくは Hellman table によるトレードオフの後にも 2^{111} 空間 2^{106} 時間（前処理 2^{154} 時間）と非常に大きく、ビットセキュリティは半分になるものの現実的な時間ではない。さらに量子計算機を用いても 2^{64} 程度のセキュリティは残るとしている。

著者らは implicit rejection 機構以外でもルーチンの置き換えによる攻撃は原理的には全ての個所が対象としながらも、暗号モジュールが正常に動作した場合 implicit rejection 部分が実行される頻度は非常に少なく、検出が困難であるという攻撃者にとっての利点を挙げている。対策を議論しているが、Cryptographic Reverse Firewall の利用に関しては実用的なものが知られていないこと、KEM の鍵を秘匿する実装への変更は完全秘匿性を前提に暗号方式を運用することの危険性、鍵長の増加は攻撃 (1) への耐性を上げないこと等それぞれの欠点があり、著者らは implicit rejection の利用を止めることが最も効果的な対策と結論している。

Public-Algorithm Substitution Attacks: Subverting Hashing and Verification

Mihir Bellare, Doreen Riepel, Laura Shea

アルゴリズム置換攻撃に関する論文である。RSA、DSA、ECDSA、EdDSA を含む一般的な署名の安全性、X.509 TLS 証明書の安全性などに関わる。

Algorithm Substitution Attack (ASA) は暗号方式のアルゴリズム Π を利用者から検出できない形で別のアルゴリズム Π' に置き換え、出力された暗号文から秘密情報を復元する攻撃である。初期の [Young-Yung, Crypto 1996, 1997][Bellare et al., Crypto 2014] では主に共通鍵暗号が対象とされていた。

本論文では、ソフトウェアへのバックドアの設置、サプライチェーン攻撃などを背景に、アルゴリズムが公開され秘密鍵を用いない設計であるハッシュ関数、署名の検証関数、非対話型アーギュメントなどに対する ASA を Public-Algorithm Substitution Attack（PA-SA）として定式化している。復元すべき秘密情報が存在しないため、攻撃者の目標は共通鍵の場合とは異なり、utility、undetectability、exclusivity の 3 種に分類される。utility は暗号で用いられる落とし戸付き一方向性関数のような、本来は逆像計算が困難である関数 f が別の $\tilde{f}$ に置き換えられた場合の逆像計算の容易さ、undetectability は第三者からみた関数の置き換えの検出困難性、exclusivity は PA-SA を行った攻撃者以外の第三者による、f と $\tilde{f}$ が異なる挙動をする入力を構成することの困難性を主張している。ただし、exclusivity が成り立てば undetectability も成り立つことが証明されるため、実際の構成では exclusivity に焦点を当てる。

以上の概念を用いて、ハッシュ関数、署名の検証関数、非対話型アーギュメントに対する PA-SA を構成している。この構成は一般的なハッシュ関数の他にも、PKCS#5 の PBKDF1 のような鍵導出関数もターゲットとなる。また、ハッシュ関数と署名の検証に対する攻撃を用いた実例として、RSA 署名と SHA-256 を用いた X.509 TLS 証明書を、ECDSA(secp256k1) と SHA-256 を用いた署名に置き換える偽造の実例を構成している。

The Security of Hash-and-Sign with Retry Against Superposition Attacks

Haruhisa Kosuge, Keita Xagawa

Hash-and-sign with retry（HSwR）型の署名方式の量子安全性を議論した論文である。NIST PQC 標準化プロジェクト追加署名候補の QR-UOV（第 2 ラウンド候補)、PROV（第 1 ラウンド候補）の安全性に関わる。

Hash-and-sign(HS) パラダイムは文書のハッシュ値に対して署名を付けるフレームワークである。構成に用いられる落とし戸付きトラップドア関数が preimage-sampleable function (PSF) である場合には安全性が証明できるものの、多変数多項式、符号を用いた PSF の構成は困難であった。対策として、ハッシュ値に対応する逆像を持たない場合に乱数のシード値を取り直して署名の再生成を行う Retry 構成が研究されてきた。この構成は [Sakumoto et al., PQCrypto 2011] の多変数多項式署名の構成を核に、HS with Retry(HSwR) パラダイムとして整理され、ROM、QROM での安全性が議論されている。

本論文では、HS パラダイムに基づく署名の近年の変種に対する、QROM での安全性を証明している。考察の対象となる署名の構成は 2 種類ある。一つ目は文書のハッシュ値の計算に乱数を用いる確率的 (Probabilistic)HS パラダイムに対してハッシュ計算および署名生成関数内で用いられる乱数のシードを鍵生成関数が生成した値に固定する脱乱択化 (derandomization) を行った DPHS パラダイムである。二つ目は HS 構成に対して脱乱択化を行い、さらにリトライ回数を制限した（bounded retry）変種である DHSwBR パラダイムであり、両者の QROM での安全性を考察している。ただし、DHSwBR においてリトライ回数を $B = 1$ とした場合の証明が DPHS に適用できるため技術的な証明は DHSwBR に対して行われる。

標準的な (s)EUF-CMA 安全性の他に、攻撃者に量子的な重ね合わせクエリーを許す以下の 2 種類の安全性が議論されている。q_s 回の量子クエリーに対して $q_s + 1$ 個の偽造署名を生成することが困難であることを要求する Plus-one unforgeability(PO)[Boneh-Zhandry, Crypto2013] が考えられている。PO では攻撃者が出力する $\{(m, \sigma)\}$ は組として全て異なる必要があるが、その弱いバージョンである wPO では組の中で m が異なれば良いものとする。（sEUF-CMA と EUF-CMA の関係に対応する）また、攻撃者が用いる署名生成オラクルが、署名の結果 (m, σ) が事前に定められた集合 B に含まれる場合には署名を返さないという制限の下で、B に含まれる (m, σ) を偽造することが困難であるという blind unforgeability（BU）が考えられている。通常の BU に対してその強いバージョンである sBU を考えることができ、EUF-CMA と sEUF-CMA との関係と同様に、偽造した集合の中で m が全て異なるか、(m, σ) が全て異なるかの違いがある。

以上の問題設定の下に、DHSwBR は (s)EUF-CMA、(w)PO、(s)BU の 6 種類の安全性を適当な仮定の下ですべて満たすことを証明している。

Thorough Power Analysis on Falcon Gaussian Samplers and Practical Countermeasure

Xiuhan Lin, Shiduo Zhang, Yang Yu, Weijia Wang, Qidi You, Ximing Xu, Xiaoyun Wang

NIST PQC 標準化格子ベース署名である FALCON のサイドチャネル攻撃に関する論文である。

FALCON は鍵生成および署名生成時に NTRU 格子上の離散ガウス分布からのサンプリングを行う。その実装では高次元離散ガウス分布からのサンプリングのため、1 次元の離散ガウス分布 $D_{\mathbb{Z},\sigma,c}$ および原点中心の離散ガウス分布の非負部分 $D^{+}_{\mathbb{Z},\sigma}$ からサンプリングを行うサブルーチンが用いられる。

$D^{+}_{\mathbb{Z},\sigma}$ からのサンプリングには累積分布関数のテーブル（reverse cumulative distribution table; RCDT）が用いられており、z^{+} をこのテーブルからサンプリングした後に $b \leftarrow \{0, 1\}$ により $z \leftarrow b + (2b - 1)z^{+}$ を計算、棄却サンプリ

ングにより $D_{\mathbb{Z},\sigma,c}$ の出力とする。先行研究 [Guerreau et al., TCHES 2022][Zhang et al., Eurocrypt 2023] の電力解析では、z^+ の部分情報 (Half Gaussian leakage)、符号 b (Sign leakage)、棄却判定サブルーチンの実行時間などを取得することが可能であり、その情報から秘密鍵を復元することが可能であると報告されていた。

本論文では、電力解析から得られる情報を NTRU 格子の構造情報の利用と符号の誤り訂正を組み合わせることで、鍵復元に必要な電力トレースの数を大幅に削減している。具体的には、Half Gaussian leakage からの鍵復元に必要なトレース数を 220,000 から 27,500 に、Sign leakage からの鍵復元に必要なトレース数を 170,000 から 25,000 に、両者を合わせた鍵復元では 45,000 から 6,500 まで削減している。実機実験として、ChipWhisperer-Lite 実験基盤を用いて STM32F415 UFO ボード上の ARM Cortex-M4 でリファレンス実装を実行し、Picoscope 3206D で電力を取得、ローパスフィルタを通したのちに波形を整理して Gaussian leakage と Gaussian leakage がどの程度起きるのかを確かめており、z^+ に関してはほぼ 100%、b などの他の値に関しても 80% 程度の正解率で漏洩すると報告している。

また、情報漏洩の元となる処理がサブルーチンのどの部分に対応するのかについて精査を行い、Half Gaussian leakage および Sign leakage の原因が浮動小数点演算、棄却サンプリングを含むほぼ全ての処理に波及していることを報告している。

対策として、サンプリングサブルーチン内のほぼすべての処理を単純ながらも情報を秘匿する形式へと変更した実装を提案している。電力波形からの変数の漏洩正解率を 65% 以下にすることが可能であり、この実装から秘密鍵復元を行うためには 1000 万回以上のトレース取得が必要となり現実的な攻撃ではないとしている。一方で、処理時間が 6 倍に、必要サイクル数が 19 倍に膨れ上がるとしている。これはサンプリングルーチンの処理時間であり、署名生成全体でみると 3 から 6 倍の増大となる。

攻撃の実験用コードは `https://github.com/lxhcrypto/FalconAnalysis` で公開されている。

Finding a polytope: A practical fault attack against Dilithium

Paco Azevedo Oliveira, Andersson Calle Viera, Benoît Cogliati, Louis Goubin

NIST PQC 標準化格子ベース署名である CRYSTALS-Dilithium（ML-DSA）の故障注入攻撃に関する論文である。

Dilithium は Fiat-Shamir with Aborts パラダイムに基づく署名方式であり、文書からの署名生成時には署名の候補をサンプリングし、条件を満たすものを出力するという棄却サンプリングが用いられる。Dilithium の仕様ではサンプリングされた署名の候補 $\boldsymbol{z}$ と補助情報 $\boldsymbol{r}_0$ の ℓ_∞ ノルムの大きさがしきい値よりも小さいことがチェックされ、続いて署名候補 $\boldsymbol{h}$ のハミング重み、および補助情報 $c\boldsymbol{t}_0$ の ℓ_∞ ノルムがチェックされる。全ての条件を満たす場合、$(\boldsymbol{z}, \boldsymbol{h})$ が乱数シード $\tilde{c}$ と共に出力される。

本論文では署名生成ルーチンに対する故障注入攻撃により補助情報 $\boldsymbol{r}_0$ のチェックがスキップされた場合に観測される情報から線形計画法ソルバーを用いて 30 分以内に鍵 $\boldsymbol{s}$ が復元可能であることを示す。対象とする実装により攻撃の順序が異なる。

まず、NIST 標準となった方式のリファレンス実装（`https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022` で公開）を用いた場合、チェックをスキップして出力された署名（faulty 署名）が検証アルゴリズムで非受理となる場合、高確率で $\boldsymbol{s}_2$ が満たすべき不等式を得ることができる。得られた不等式群を解くことで $\boldsymbol{w}_1, \boldsymbol{s}_2$ が復元可能であり、$\boldsymbol{t}_0$ と組み合わせることで $\boldsymbol{s}_1$ が復元される。

開発者の github に掲載されている実装（`https://github.com/pq-crystals/dilithium` で公開）では、前者と異なり出力された署名は常に検証アルゴリズムで受理されるものの、$\boldsymbol{t}_0$ の情報からそれが faulty であるかどうかを容易に検出することが可能であり、同様に不等式群を用いて秘密鍵が復元可能である。

また、本論文では別の攻撃も提案されており、署名の候補 $\boldsymbol{z}$ のノルムチェックをスキップさせるような故障注入攻撃

が可能である場合にも同様に線形計画法を用いて秘密鍵が復元可能である。$\boldsymbol{r}_0$ のチェックに対する攻撃と比較して $\boldsymbol{t}_0$ を必要とせず、より高速であるとしている。

計算機実験では Dilithium-2,3,5 のパラメータに対して、署名数 125 万、350 万、400 万の設定で Intel Core i7-10850H 2.70GHz を用いた攻撃実験を行い、それぞれ 261 秒、1239 秒、186 秒で鍵復元が可能と報告している。

攻撃の実装は `https://github.com/anders1901/Polytope_attack` で公開されている。

One Bit to Rule Them All - Imperfect Randomness Harms Lattice Signatures

Simon Damm, Nicolai Kraus, Alexander May, Julian Nowakowski, Jonas Thietke

NIST PQC 標準化格子ベース署名である ML-DSA のサイドチャネル攻撃に関する論文である。

ML-DSA は Fiat-Shamir with Aborts パラダイムに基づく署名方式であり、ベースの ID スキームの Fiat-Shamir 変換により構成された基本方式を実用にカスタマイズした方式と考えることができる。格子ベース ID スキーム [Lyubashevsky, Asiacrypt2009] では Prover の秘密鍵 $\boldsymbol{s}$ およびランダムネス $\boldsymbol{y}$、Verifier のチャレンジ c に対してレスポンスが $\boldsymbol{z} = \boldsymbol{y} + c \cdot \boldsymbol{s}$ の形で計算され、Fiat-Shamir 変換後には c が文書に、$\boldsymbol{z}$ が署名に対応する。

ID スキームおよび変換後の署名における秘密鍵 $\boldsymbol{s}$ の安全性はスキームのゼロ知識性に基づいており、それは $\boldsymbol{y}$ が一様乱数かつ $\boldsymbol{y}$ に関する情報が一切漏れていないという仮定が必要であった。先行研究 [Liu et al., IEEE-FS 16] により、署名および $\boldsymbol{y}$ の $j \geq 6$ ビット目のセットが大量に得られる場合、LWE 問題の変種である Integer LWE(ILWE) 問題への帰着を通じて部分秘密鍵 $\boldsymbol{s}_1$ の復元が可能であると報告されていた。([Azevedo-Oliveira et al., CRYPTO 2025] の議論により、公開鍵の $\boldsymbol{t}_1$ の他に秘密鍵の $\boldsymbol{t}_0$ も実質的には公開情報と考えられるため、$\boldsymbol{s}_1$ から秘密鍵全体を復元することは容易であると考えられる。) 一方で、ただしアルゴリズムの空間計算量は漏洩の位置 j に関して指数となり、上位ビットでの漏洩を用いた攻撃は事実上不可能であると考えられてきた。

本論文では Liu らの研究を押し進め、漏洩ビットからの ILWE への変換の際に役に立つ組 (Informative relation) のみを取り出す基準の確立を行い、さらに関係式を平行移動により調整することで、エラーの範囲が制限され ILWE の計算量を劇的に下げている。ただし、Informative relation を取り出す前に必要な署名と漏洩ビットの組の個数は j の指数であることに変わりはない。

本論文の提案攻撃は原理的には Fiat-Shamir パラダイムに基づくほぼ全ての格子ベース署名方式に対して、Module、Ring の構造に無関係に適用可能である。例えば、ℓ 次元の Module で定義される Module-LWE ベースの署名においては、署名 1 個につき 1 ビットの漏洩がある場合に秘密鍵の $1/\ell$ が復元可能である。Dilithium-II のパラメータでは $\ell = 4$ であるので、1024 次元の秘密鍵のうち 4 分の 1 が復元され、ビットセキュリティは 128 から 84 に落ちるとしている。

計算機実験では 1024 次元の Ring-LWE ベース暗号、Dilithium-2,3,5 のパラメータでの鍵復元実験が行われ、漏洩ビットの位置 j と必要な Informative relation 数の関係が調べられた。大まかにどの位置の漏洩においても、ML-DSA-44,65,87 においてそれぞれ 50 万、240 万、80 万程度の関係式があれば BKZ-100 程度のアルゴリズムを用いて実時間での鍵復元が可能であると報告している。

Intermundium-DL: Assessing the Resilience of Current Schemes to Discrete-Log-Computation Attacks on Public Parameters

Mihir Bellare, Doreen Riepel, Laura Shea

本論文では、Intermundium-DL という、近い将来に高機能な量子コンピュータを一部の機関のみが持ち、僅かな数ではあるが暗号学的なサイズの離散対数問題を解くことが出来る状況を想定する。標準化された方式のようにごく少数の公開パラメータを持つ方式に対して、それらの離散対数を知ることができる攻撃者が他の利用者に及ぼす影響について調査した。攻撃は DL-equipped として定式化され、群 G の生成元 g と位数 p、および公開パラメータ $h_1, \ldots, h_w \in G$ が公開されている状態において、攻撃者はそれらの離散対数 $\log_g(h_1), \ldots$ を保持しているものとする。

本論文では 5 種類の暗号方式に対して、安全性ゲーム中の攻撃者が公開パラメータの離散対数（論文中では Advice と呼ばれ、以下の A-はこの頭文字である）を持つオラクルへの追加アクセスが可能な状況を考え、方式がどの程度危殆化するのかを Fully A-secure、Partially A-secure、A-Insecure の 3 つのランクとして分類している。

Okamoto 署名は UF-CMA 安全性を、Katz-Wang 署名は離散対数の古典困難性を仮定しての安全性が示せるため、追加オラクルによる危殆化は無く Fully A-secure に分類されている。

一方で、Cramer-Shoup 暗号はオリジナルでは DDH 仮定の下で IND-CCA2 安全であったものが、攻撃者が DL-equipped オラクルを持つことで DT-DDH 仮定の下での IND-CCA1 安全性に落ちるとしている。通常の DDH 仮定が (g, g^a, g^b, g^c) を一度に受け取って $c = ab$ かどうかを判定するのに対して、DT(Delayed target)-DDH は先に (g, g^a) を受け取ったのちに h に対して h^a を返すオラクルへのアクセスを行い、十分な情報を得たのちに (g^b, g^c) を受け取り判定を行う変種である。また、SPAKE2 パスワード認証鍵交換プロトコルではオフラインでの辞書攻撃が可能となるものの、パスワード空間が十分大きい場合に強 CDH(SCDH) 仮定からの安全性が保証できるとしている。最後に、KOY-style PAKE protocols に関しては事前のバックドアの構成が可能となることで破られるとしている。これらの方式は Partially A-secure に分類されている。

最後に、A-Insecure は、Intermundium-DL モデルですでに安全ではない暗号プロトコルが該当する。該当する暗号方式として、離散対数問題の困難性に依存する暗号方式（Diffie-Hellman 鍵共有、ElGamal 暗号、Schnorr 署名）のほかに、Katz-Ostrovsky-Yung により提案された KOY PAKE protocol とその変種が該当するとされ、これらの古典的方式は量子計算機開発の初期段階ですでに危険に晒される可能性があると報告されている。

著者らは対策として、公開パラメータを用いない方式を用いることを提案している。そのような方式はパラメータフリーなものを中心に数多く提案されており、開発が続けられるだろうとしている。バックドアの文脈からの議論も行われ、量子コンピュータを保持しているかどうかに関わらず、公開パラメータを自ら生成している機関はその離散対数を保持している可能性があり信用できないという結論となる。この文脈において、過去に起きた疑似乱数生成器 Dual EC におけるパラメータの点 $Q = dP$ における P, Q 選択の不透明性と離散対数 d の情報から将来の出力を推測可能であるという問題を取り上げ、本論文のフレームワーク内に含まれるものであるとしている。

Memory-Efficient BKW Algorithm for Solving the LWE Problem

Yu Wei, Lei Bi, Xianhui Lu, Kunpeng Wang

格子暗号の安全性の根拠となる LWE 問題の困難性に関する論文である。

BKW アルゴリズム [Blum-Kalai-Wasserman, J. ACM 2003] は元々 LPN 問題に対する指数時間・空間アルゴリズムとして提案されたが、自然な形で LWE 問題の解析に拡張可能であり暗号の解析に用いられてきたものの、指数的な

メモリ空間を要求することから暗号学的に用いられるよりも小さいパラメータ領域においても実現性は小さいと考えられてきた。

本論文では、[Bogos-Vaudenay, Asiacrypt 2016] の LPN 問題に対するアルゴリズムを拡張し、メモリ空間の小さいアルゴリズムを与える。先行研究からの第一の改良点は縮約 (reduction) に関するものである。BKW 型アルゴリズムでは与えられた LWE サンプルの列 $\{(\boldsymbol{a}_i, b_i)\}$ に対して、$\boldsymbol{a}_i \pm \boldsymbol{a}_j$ で 0 成分が多くなる組を探索する操作を縮約と呼び、縮約を繰り返し低次元の LWE 問題に変換する。オリジナルの BKW アルゴリズムでは 2 つのベクトルの組を逐次的に調べる形式であったが、$\boldsymbol{s}$ の変数変換など多くの改良が提案されてきた。本論文では既存の縮約手法を統一するフレームワークを与え、c 個の $\boldsymbol{a}_i$ の和で特定の成分が 0 になるものを探索する c-sum 法と衝突探索のための PCS(Parallel Collision Search) を組み合わせた c-sum-PCS 縮約法を提案する。提案アルゴリズムを含め BKW 系のアルゴリズムは時間-空間トレードオフが存在するが、メモリの少ない領域では先行研究よりも高速化されている。

縮約の 1 ステップごとに、縮約アルゴリズムの選択、縮約対象の変数の個数選択に自由度がありその選択の順序により計算量が変化する。本論文では、最適な縮約戦略の選択を有限オートマトンの形で記述し、メモリ制約のある状態での最適パスと計算量を求めるアルゴリズムを与えている。また、メモリ制約のある場合、最適パスの中で Discard-reduce が他の縮約手法の次に来ることが無いということが証明されたため、戦略計算の大幅な簡略化が可能である。

[Regev, J. ACM 2009] での公開鍵暗号のパラメータに対して、現時点で提案されている BKW 型アルゴリズムの中で最良の結果を与える Coded-BKW[Guo et al., Crypto 2015] と比較したところ、$n = 64, \ldots, 512$ の範囲で計算時間の削減が $2^{3.3}$ から $2^{26.2}$、空間計算量の削減が $2^{9.7}$ から $2^{71.3}$ 程度可能であると報告している。

Worst and Average Case Hardness of Decoding via Smoothing Bounds

Thomas Debris-Alazard, Nicolas Resch

符号ベース暗号の安全性の根拠となる符号の復号問題の困難性に関する論文である。

暗号方式の安全性の根拠となる計算問題の計算量的困難性として求められる性質は最悪計算量の困難性ではなく平均計算量の困難性であることが認識され、長年議論され続けている。格子暗号では早くから最悪-平均計算量の関係が示されていたものの、符号ベース暗号においてその議論が現れたのは LPN 問題の平均計算量と特殊な符号問題の最悪計算量を結び付けた [Brakerski et al., Eurocrypt 2019] と比較的最近である。

本論文では、上述の最悪-平均計算量の帰着の議論を smoothing bound を用いて再考し、その限界について議論している。

帰着フレームワークは先行研究を踏襲し、復号問題の入力 $(G, \boldsymbol{m}G + \boldsymbol{t})$ に対して、対応する LPN オラクルを構成する。解析には LPN ノイズ $\boldsymbol{r}$ を符号 C で割った共役類 $\boldsymbol{r}/C$ が一様分布のように見える smoothing bound の解析を通じて LPN オラクルのシミュレーションが可能であることを示している。技術的には [Debris-Alazard et al., IEEE-IT 69(6)] により示されたほぼ全ての符号に対する最適な smoothing bound の議論を本論文が対象とする状況に使えるように拡張している。

著者らはこのフレームワークの限界として、帰着先の LPN 問題のノイズを暗号学的に必要とされる $1/2 - 1/\mathrm{poly}(n)$ 程度とするためには符号のレートを $o(1)$ としなければならず、逆にレートを定数とすると帰着先の LPN 問題のノイズが $1/2 - 2^{-\Omega(n)}$ となってしまうことを発見している。また、Debris-Alazard らにより用いられた符号の重みに関する second linear programming bounds がレート $o(1)$ の領域では符号の要素数 2^k よりも大きくなることを指摘し、再解析を行っている。

以上のフレームワークの限界に関する議論から、帰着対象の問題を構成する符号が balanced、つまりある $\delta \in (0, 1)$

に対して符号の最小距離が δn かつ全ての符号語のハミング重みが $(1-\delta)n$ 以下であるという条件を外すことは困難であると結論付けている。

Multiple Group Action Dlogs With(out) Precomputation

Alexander May, Massimo Ostuzzi

群作用から定義される離散対数問題（group action dlog）の困難性に関する論文である。同種写像ベースの鍵共有プロトコル CSIDH の安全性に関連する。

位数 N の有限群 $\mathcal{G}$ の集合 X に対する作用 $\star : \mathcal{G} \times \mathcal{X} \to \mathcal{X}$ が定義されているとする。この時、群作用 dlog は $(x, y = g \star x)$ から g を復元する計算問題として定式化される。[Galbraith-Hess-Smart, Eurocrypt 2002] による GHS 衝突探索アルゴリズムは $N^{1/2}$ 時間、多項式空間で離散対数を発見することが知られている。

本論文では、群作用 dlog が事前計算により高速化可能であることを示す。パラメータ s, t に対して、事前に st 時間で計算した大きさ s のヒント表を用いることで群作用 dlog が t 時間で計算可能となる。例えば、$s = t = N^{1/3}$ と取ることで事前計算の時間 $N^{2/3}$、空間 $N^{1/3}$、dlog の計算を $N^{1/3}$ とすることができ、既存の GHS アルゴリズムよりも高速に計算可能である。

同様の改良は multiple group action dlog の問題設定でも可能であり、m 個の群作用 dlog インスタンスが同時に与えられたときにも 1 つの場合とほぼ同様の、事前計算の時間 $mN^{2/3}$、空間 $m^2N^{1/3}$、dlog の計算を $N^{1/3}$ 時間で可能であり、その他のトレードオフを考えることもできるとしている。

技術的には古典的な離散対数問題に対する前処理計算と同様に、衝突探索において特定のインスタンスに依存しないランダムウォーク部分を前処理として取り出しヒント表として構成、オンライン部分でその表の探索（ランダムウォークの終点とのマッチング）を行うという方針を群作用に適用している。ランダムウォークの構成に当たり、集合 $\mathcal{X}$ の構造を使うことができないため単純に通常の離散対数問題に対する古典的な手法を用いることができず、$\mathcal{G}$ の生成元から導かれる格子の剰余類から $\mathcal{X}$ への写像を考えることで実現している。

応用として、CSIDH の攻撃計算量の再評価を行っており、CSIDH-512 に対しては 2^{171} の事前計算と 2^{85} のメモリを用いることで解読計算量が 2^{85} に下がるとしているが、現時点で現実的な攻撃ではないとしている。CSIDH の小さいパラメータに対して攻撃実験を行い、確実に解けることを確認している。CSIDH に対する解析実験のコードは `https://github.com/maxostuzzi/precomputation_attack` で公開されている。

E.5 FSE 2025

Significantly Improved Cryptanalysis of Salsa20 with Two-Round Criteria

Sabyasachi Dey, Subhamoy Maitra, Santanu Sarkar, Nitin Kumar Sharma

軽量ストリーム暗号 Salsa20 に対する安全性評価について報告したものである。Salsa20 に対する暗号解析は長年にわたって進展しており、特に 2008 年に Aumasson らによって提案された Probabilistic Neutral Bits（PNB）を用いた手法が解析の基盤となっている。しかし、過去 15 年以上の研究を通じて、Salsa20 の 8 ラウンドを超える暗号解析は達成されていない。そこで本研究は、Salsa20 の解析をさらに前進させ、8 ラウンドの壁を突破することを主たる目的とする。

本研究では、既存の攻撃手法における計算量およびデータ量の効率化に加えて、Salsa20 の 8.5 ラウンドに対する世界初の有効な鍵回復攻撃を提案する。解析手法として、従来の差分線形解析、適切な key-IV 組の選定、PNB の概

念を活用する一方で、複数の新しいアイデアも導入している。特に注目すべきは、2 ラウンド基準（2-round criteria）と呼ばれる新たな概念である。これは、従来の 1 ラウンド基準を拡張し、2 ラウンド目の内部状態に対して制約を課すことで、出力ビットのバイアス精度を向上させるものである。また、確率的に独立な IV ビット（Probabilistically Independent IV Bits）と呼ばれる手法を導入し、IV の特定ビットが統計的に独立である性質を利用することで、必要なデータ量の確保を可能にしている。

結果として、8 ラウンド Salsa20 に対する鍵回復攻撃に関し、従来の計算量 $2^{217.14}$ を $2^{186.01}$ へと大幅に削減することに成功した。さらに、8.5 ラウンド Salsa20 に関しては、計算量 $2^{245.84}$、データ量 $2^{99.47}$ という条件下での世界初の鍵回復攻撃を実現した。

Perfect Monomial Prediction for Modular Addition

Kai Hu and Trevor Yap

ARX（Addition-Rotation-XOR）型ブロック暗号に対する汎用的な解析手法について報告したものである。ARX 暗号において、算術加算（modular addition）は唯一の非線形演算であり、その安全性解析は極めて重要である。現在、積分識別子の探索手法としては、分割特性（division property）が広く用いられており、特にその中でも two subset bit-based division property（2BDP）に基づくモデルが算術加算に適用されてきた。しかし、2BDP に基づく手法は理論的に不正確であり、積分識別子の一部、特にいくつかのバランスビット（balanced bits）を見逃す可能性がある。この問題に対処するため、three subset bit-based division property without unknown subsets（3BDPwoU）や単項式予測（monomial prediction）といった、より精密な分割特性が提案されてきたが、これらはいずれも算術加算への適用は考慮されていない。一方で、FSE 2005 において Braeken と Semaev が提唱した定理は、算術加算における単項式の伝搬規則を数学的に定式化しており、この定義を活用すれば積分識別子の探索が理論的に可能となる。しかし、これまでその定理が積分解析に利用された例はなかった。

本研究では、Braeken と Semaev の定理を基盤とし、ARX 暗号に対する積分識別子の探索手法を構築した。具体的には、彼らの定理を SMT/MILP モデルに直接実装することで、正確かつ効率的な積分識別子の探索が可能となる。このツールを用いることで、ARX 暗号における積分識別子を高精度に検出できるだけでなく、対象プリミティブの正確な代数次数、またはその下界を導出することができる。まず、提案手法を Speck ファミリーに適用し、既存の結果を再現できることを示すとともに、探索時間を従来の数時間〜数日から、数秒〜数分へと大幅に短縮した。さらに、Speck-48/64/96/128 の各バリアントに対し、既存成果を上回る新たな積分識別子を発見した。加えて、Speck-32 において 7 ラウンド後の出力ビットの正確な代数次数が 31 であることを初めて理論的に証明した。最後に、Speck における回転パラメータの選定基準を再検討し、本手法が積分攻撃に対する耐性向上に資することを示した。

Finding Complete Impossible Differential Attacks on AndRX Ciphers and Efficient Distinguishers for ARX Designs

Debasmita Chakraborty, Hosein Hadipour, Phuong Hoa Nguyen, Maria Eichlseder

ARX（Addition-Rotation-XOR）暗号および AndRX（And-Rotation-XOR）暗号に対する不能差分（ID: Impossible Differential Attack）攻撃の自動化ツールについて提案したものである。ID 攻撃はブロック暗号の安全性評価における有力な手法の一つであり、識別子の探索と鍵回復という 2 つのフェーズで構成される。しかし、既存研究の多くは識別子の自動探索に重点を置いており、鍵回復フェーズは手動で実行されることが多く、全体として最適な攻撃戦略の確立には至っていなかった。また、従来のアプローチは直接的な矛盾（direct contradiction）の検出に依存しており、この

アプローチでは ARX 暗号や AndRX 暗号における一部の識別子を見逃す可能性があるという課題が指摘されていた。

本研究では、Eurocrypt 2023 および IACR ToSC 2024 にて Hossein らが提案した ID 攻撃の自動化ツールを拡張する。最初に、識別子の探索フェーズに関し、直接的な矛盾に加えて間接的な矛盾（indirect contradiction）も考慮可能な新しい制約プログラミング（CP: Constraint Programming）モデルを提案する。このモデルは ARX 暗号や AndRX 暗号に限らず、S-box ベースの暗号を含む多様な構造の暗号にも適用可能である。次に、識別子の探索フェーズと鍵回復フェーズを統合した最適化モデルを新たに構築する。これは、攻撃に用いるペア数、フィルタリング戦略、探索範囲などのパラメータを自動的に最適化することで、鍵回復の計算コストを大幅に削減することを目的としている。最後に、提案ツールを複数の代表的な ARX/AndRX 暗号（Simon、Speck、Simeck、ChaCha、LEA、SipHash）に適用し、その有効性を実証した。特に、Simon に対し、既存の攻撃手法を 1〜2 ラウンド分改善する結果を得ることに成功した。

Exact Formula for RX-Differential Probability through Modular Addition for All Rotations

Alex Biryukov, Baptiste Lambin, Aleksei Udovenko

ARX（Addition-Rotation-XOR）暗号に対する回転 XOR 差分（RXD: Rotational-XOR Differential）攻撃に関する研究について報告したものである。算術加算に対する任意の回転量を持つ RXD 確率を正確かつコンパクトな数式で提示することは長年の未解決問題であり、本研究ではこの問題への解を与える。提案された数式には厳密な証明が付随しており、広範な実験によってその妥当性が検証されている。

回転量が 1 より大きい場合に関しては、2022 年に既存の式が提示されていたが、本研究の結果によりその式に誤りがあることを明らかにした。また、IACR ToSC 2016 にて回転量が 1 の場合に関する式が提示されていたが、本研究でより正確な式に改善された。具体的には、IACR ToSC 2016 で示された式で使用される仮定が成り立たない稀なケースが存在することが明らかとなった。任意の回転量に対する正確かつコンパクトな式を使用することで、RXD の探索空間が広がり、より良い RXD トレイルの発見に繋がる可能性が高い。

また、提示した式に基づき、最適な RXD トレイルを探索するための MILP（Mixed Integer Linear Programming）モデリング手法を提案する。Salsa、Alzette、Speck への適用により、多数の新たな RXD 識別子を発見し、それらが最適であることを証明した。

On Impossible Boomerang Attacks: Application to Simon and SKINNYee

Xavier Bonnetain, Margarita Cordero, Virginie Lallemand, Marine Minier, María Naya-Plasencia

不能ブーメラン攻撃の改良に関する結果について報告したものである。不能ブーメラン攻撃は 2008 年に Lu によって提案されたものであり、ブーメラン識別子を用いて誤った鍵候補を排除する不能差分攻撃の拡張手法である。Lu の研究において考慮された不能差分ブーメラン識別子は、4 つの異なる確率 1 差分から構築され、その差分は miss-in-the-middle アプローチの文脈における中間ラウンドで合計が 0 とならない 4 つの差分へと繋がる。

本研究では、ブーメランスイッチ制約に起因するより精緻な矛盾に着目し、この識別子の概念のさらなる拡張可能性を検討する。まず、2 次の Feistel 構造を持つ Simon 暗号を例として、非常に特殊なブーメランスイッチ制約を利用して矛盾を強制し、SMT ソルバーを用いて探索可能な新たなタイプの不能ブーメラン識別子を構築する。次に、ワードベースの暗号に対象を移し、ブーメラン接続表にて生じる矛盾を活用する手法を提案する。この手法を SKINNYee に適用することで、最大 21 ラウンドに及ぶ不能ブーメラン識別子の構築が可能であることを示す。

さらに、single-(twea)key モデルおよび related-(twea)key モデルにおける不能ブーメラン攻撃の手法とその計算量

について詳細に検討した後、構築した識別子を用いた攻撃手法へと展開する。その結果、Simon-32/64（全 32 ラウンド）に対する 23 ラウンドの不能ブーメラン攻撃、および SKINNYee（全 59 ラウンド）に対する 29 ラウンドの攻撃が実現可能であることを示した。

Extending the Quasidifferential Framework: From Fixed-Key to Expected Differential Probability

Christina Boura, Patrick Derbez, Baptiste Germon

ブロック暗号に対する差分攻撃の解析手法について報告したものである。多くの共通鍵暗号プリミティブでは特定の鍵に対する差分確率が大きく変動するため、従来用いられてきた独立性仮説（Markov cipher assumption、stochastic equivalence hypothesis、など）や確率の平均化手法（key-average probability）を適用できないという課題があった。この課題に対し、Beyne と Rijmen が提案した準差分フレームワーク（quasidifferential framework）は有力な解決策となりうるが、その計算コストの高さが問題であり、特に 8 ビット S-box のように大規模な構造を持つ暗号への適用は依然として困難である。例えば、8 ビット S-box に対して構成される準差分遷移行列（QDTM: QuasiDifferential Transition Matrix）はサイズが $2^{16} \times 2^{16}$ にも及び、そのような大規模行列を扱うモデリングは現実的ではない。また、Peyrin と Tan が提案した鍵制約を利用する手法は直感的で扱いやすいように見えるが、制約条件を正確に定式化することが難しく、誤った解析結果につながる可能性がある。

本研究では、準差分フレームワークの拡張を通じて、これらの課題の克服を試みる。まず、8 ビット S-box を含む大規模な QDTM を効率的に処理可能な新たな MILP モデリング手法を提案し、指定された差分特性に対応するすべての準差分トレイルの探索を実現した。この際、既存の差分分布表を用いたモデリング技法を応用し、計算負荷の低減を図った。次に、このフレームワークを関連鍵攻撃の設定に対応可能な形に拡張し、関連鍵差分特性の確率を容易に評価できるようにした。また、キースケジュールの影響を考慮し、差分特性の確率を平均的に評価する新しい手法を提案した。最後に、提案手法を AES および SKINNY に適用し、ツールの有効性を検証した。AES のすべてのバリアントに対して関連鍵差分特性解析を行い、既存の解析結果を再現可能であることを確認した。さらに、SKINNY に対する差分特性解析では、Peyrin と Tan の手法の再現に成功するとともに、それを上回る精度の結果を得ることに成功した。

AutoDiVer: Automatically Verifying Differential Characteristics and Learning Key Conditions

Marcel Nageler, Shibam Ghosh, Marlene Jüttler, Maria Eichlseder

ブロック暗号に対する差分攻撃の解析手法について報告したものである。共通鍵暗号プリミティブにおける差分特性の探索手法の多くは、確率的同値性仮説（hypothesis of stochastic equivalence）など、理論的には一般化しづらい前提に依拠している。こうした仮定は、特定の暗号プリミティブや鍵に対して必ずしも成立するとは限らず、その有効性を実験的に検証することが望ましい。しかし、解析対象となる差分特性の確率が極めて低い場合、この検証作業は非常に困難となる。

この課題に対処するために、本研究では、与えられた差分特性を徹底的に検証するための、自動的、正確、多用途、かつ使いやすいツールである AutoDiVer を提案する。AutoDiVer は主に次の 3 つの機能を提供する。1 つ目は、全ての鍵に対して与えられた差分特性に関する差分確率の期待値を高精度で推定することである。2 つ目は、与えられた差分特性を満たす有効な秘密鍵の個数を高精度で推定することである。3 つ目は、与えられた差分特性を満たす秘密鍵に関する特定の条件を取得することである。

本ツールはSATモデリング手法に基づいて実装されており、Approximate Model Counting や clause learning など、最新の SAT ソルバーに搭載された先進的な技術を活用している。AutoDiVer の有効性を確認するため、GIFT、SKINNY、Midori、PRESENT、RECTANGLE、WARP、SPECK、SPEEDY などの様々な種類のブロック暗号に対してツールが適用された。

Links between Quantum Distinguishers Based on Simon's Algorithm and Truncated Differentials

Zejun Xiang, Xiaoyu Wang, Bo Yu, Bing Sun, Shasha Zhang, Xiangyong Zeng, Xuan Shen, Nian Li

Simon のアルゴリズムに基づくブロック暗号の量子安全性について報告したものである。Simon のアルゴリズムを使用する上で最も重要なことは、解析対象のプリミティブにおける周期関数を構築することである。

本研究では周期関数と切り詰め差分の関係性についてより詳細に分析し、量子識別攻撃に関する新たな知見を提示する。この目的のために、確率 1 の切り詰め差分を使用して 2 種類の周期関数を構築できることを示す。これら 2 種類の周期関数は、差分消滅行列（difference-annihilation matrix）と呼ばれる新しい概念から導出可能である。このような手法により、周期関数を手作業で検証する必要がなくなる。

提案手法を LBlock と Simon に適用し、7 ラウンド LBlock の量子識別子と、9/10/11/13/15 ラウンド Simon-32/48/64/96/128 の量子識別子を発見することに成功した。なお、これらの識別子は古典設定での識別子よりもラウンド数が少ないことに注意が必要である。

SoK: Security of the Ascon Modes

Charlotte Lefevre, Bart Mennink

軽量認証暗号 Ascon の安全性について、既存の知見を体系的に整理・分析し、その包括的な評価結果を報告したものである。Ascon は NIST 軽量暗号プロジェクトにおいて標準暗号に選定されており、認証暗号およびハッシュ関数の機能を提供する。その認証暗号方式である Ascon-AE は、SpongeWrap 構造に類似した設計を基盤としつつも、独自のキー・ブラインディング機構を採用している。この特性により、SpongeWrap 構造に対する一般的な安全性解析とは異なるアプローチで、Ascon-AE 固有の安全性を多様な攻撃モデルの下で精査する必要がある。従来の研究では、Ascon-AE に対する安全性解析が個別に行われており、攻撃シナリオごとの整合性や安全性証明の網羅性に課題が残されていた。これにより、分野全体としての知識の体系化が求められていた。

本研究はこの課題に対応し、Ascon-AE の安全性に関する完全かつ包括的な評価を提供することを目的とする。具体的には、以下の 6 種類の攻撃シナリオを対象とし、それぞれに対する安全性の境界と解析結果を体系的に整理した：(1) Nonce-respecting security、(2) Nonce-misuse resistance、(3) Nonce-misuse resilience、(4) Leakage resilience、(5) State-recovery security、そして (6) Release of unverified plaintext である。これらのシナリオに対して、既存の安全性証明における下界および上界を明確化し、複数の既存研究に内在する欠陥や問題点を指摘した上で、新たな安全性境界および汎用的な攻撃手法を導出した。さらに、(3), (4), (6) のシナリオに関しては、新しい安全性証明を提示し、Ascon-AE に対する既存の安全性証明をより厳密なモデルの下で再構築するとともに、全ての安全性証明に対応する matching attacks も構成した。

まとめると、本研究は Ascon-AE の安全性証明を体系的に整理・強化し、厳密な安全性モデルに基づく新たな証明の提供を通じて、同方式に関する理論的理解の深化に貢献するものである。なお、本研究は Ascon-AE の実装における脆弱性や設計上の欠陥を指摘するものではない点に留意されたい。

Dynamic Cube Attacks against Grain-128AEAD

Chen Liu and Tian Tian

軽量認証暗号 Grain-128AEAD に対する安全性評価について報告したものである。Grain-128AEAD はストリーム暗号型の認証暗号として提案されている。ストリーム暗号に対する代表的な暗号解析手法の一つにキューブ攻撃があり、その拡張として動的キューブ攻撃（dynamic cube attack）が提案されている。

本研究では、Grain-128AEAD に対する動的キューブ攻撃の有効性を分析し、従来手法（特に、Hao らによるフルラウンドの Grain-128 に対する動的キューブ攻撃）における問題点を指摘するとともに、新たな解析手法を提案する。従来手法の主な問題は、動的キューブ攻撃で使用する MILP モデリング手法の構築方法に欠陥があること、そして推定したバイアスと実際のバイアスに大きな乖離があることである。まず、前者に関して、Three-Subset Division Property without Unknown Subset と呼ばれる手法をベースとした、より精緻な MILP モデリング手法を開発した。次に、後者に関して、バイアスに関する多項式近似（PAB: Polynomial Approximation with regard to Bias）と呼ばれる手法を提案し、より正確なバイアスの推定を可能とした。さらに、正しい鍵推測との識別が困難となりうる可能性のある全ての誤った鍵推測を特定するアプローチを代数的側面から構築することに成功した。これらの提案手法に関する妥当性検証が行われるとともに、190 ラウンドの Grain-128AEAD に対して提案手法を適用し、結果として計算量 $2^{103.44}$、成功確率 99.68% で 3 ビットの鍵回復に成功した。

Improved Conditional Cube Attacks on Ascon AEADs in Nonce-Respecting Settings: with a Break-Fix Strategy

Kai Hu

軽量認証暗号 Ascon に対する安全性評価について報告したものである。本研究と最も関連性の深い既存の攻撃は、7 ラウンド Ascon の初期化フェーズに対するキューブ識別子である。この識別子は、ナンスの先頭 64 ビットと末尾 64 ビットが異なる特別な構造を用いている。その後、分割特性（division property）モデルを構築し、7 ラウンド出力ビットの代数次数が高々 59 であるということを特定した。一方、この識別子を鍵回復へと拡張する手法については知られていない。これはキューブ識別子が特別な構造に依存していることが大きな要因の 1 つとなっている。

本研究では、キューブ攻撃の一種である条件付きキューブ攻撃に着目し、既存手法の課題を克服するために break-fix と呼ばれる新たな戦略を導入する。この戦略は、break フェーズと fix フェーズの 2 段階から構成される。break フェーズでは、60 次元キューブの構造をわずかに改変することで、出力ビットの代数次数を 59 よりも大きくなるようにし、既存の構造を破壊する。続く fix フェーズでは、改変された構造による影響を修正する鍵条件の集合を特定し、代数次数を再び 59 に戻す。これら一連の過程において、代数次数が 59 に戻るかどうかを観察することで、対応する鍵情報の復元が可能となる。結果として、7 ラウンドの Ascon-128、Ascon-128a、Ascon-80pq に対して有効な鍵回復攻撃を実現し、計算量およびメモリ使用量の観点で既存手法を上回る成果を得た。

E.6 PQCrypto 2025

Giant Does NOT Mean Strong: Cryptanalysis of BQTRU

Ali Raya, Vikas Kumar, Aditi Kar Gangopadhyay, Sugata Gangopadhyay

格子暗号 BQTRU の解析に関する論文である。

BQTRU[Bagheri et al., Des. Codes. Crypt., 2018] は格子ベース公開鍵暗号方式 NTRU を 2 変数多項式を要素とする四元数環（quaternion algebra）に拡張し処理の効率化を図ったものである。Bagheri らの論文では、パラメータ設定のために四元数環の要素を格子に埋め込んだ Coppersmith-Shamir 型の攻撃を考え、鍵復元の困難性と平文復元の安全性を格子問題の計算量から見積もっていた。

本論文では、Bagheri らの解析で用いられる格子の構造に着目し、パラメータ n に対して $4n^2$ 次元の格子問題を解く必要があると主張されていた安全性に関して、folding と呼ばれる次元削減手法を用いることで半分の $2n^2$ 次元の格子問題へと帰着している。

結果として、Bagheri らの論文では鍵復元、平文復元にかかる計算量がそれぞれ $(2^{166}, 2^{92})$ と主張されていた moderate parameter に関して、標準的なデスクトップで 1 週間程度での攻撃が可能であるとしている。また、highest parameter はその計算量困難性が $(2^{396}, 2^{212})$ とされていたが、新たな解析では $(2^{125}, 2^{82})$ まで下がると報告されている。検証用コードは `https://github.com/Mr-PQ-Crypto/BQTRU_cryptanalysis` で公開されている。

本論文の背景には、[Gentry, Eurocrypt 2001] の円分体上の NTRU 型格子に対する次元削減手法があり、適用可能な体の範囲が拡張されたものと報告している。

Analysis of REDOG: The Pad Thai Attack

Alex Pellegrini, Marc Vorstermans

符号ベース公開鍵暗号方式 REDOG の解析に関する論文である。

本論文では、韓国の耐量子計算機暗号コンペティション KpqC の候補として提出された REDOG[Kim et al.] の平文復元攻撃を与えている。REDOG の特徴として、拡大体 $\mathbf{F}_{2^m}$ 上のベクトル $\mathbf{x} = (x_1, \ldots, x_n)$ のランクを用いた効率化がある。ここで、$\mathbf{x}$ のランクは拡大体の適当な基底に関して x_i を展開した列ベクトル表示 $(x_{i,1}, \ldots, x_{i,m})^T$ を並べた行列の階数により定義される。REDOG の暗号文は拡大体上の公開鍵行列 M, F を用いて (1) $c_1 = mM + e_1$ および (2) $c_2 = mF + e_2$ の形で計算される。攻撃では適当な基底を選ぶことで、(1)(2) を変形し、さらに列を削ることでノイズの無い方程式 $c_1' = mM'$ および $c_2' = mF'$ を得ることができ、連立方程式を解くことで平文が復元可能となる。ノイズの無い方程式を選ぶためには基底（およびアレンジメントとよばれるその分割）をうまく選ぶ必要がある。REDOG の仕様上平文に付加されるノイズベクトル e_1, e_2 のランクが非常に低いため、考慮すべき基底とアレンジメントの個数は限られており、Kim らの提案書で主張されているパラメータよりも攻撃計算量が小さくなる。具体的には、提案書内で 128,192,256 ビットセキュリティとされていたものが、それぞれ $2^{91.22}, 2^{135.78}, 2^{229.9}$ 回の体演算で平文復元が可能であると報告されている。

Efficient Theta-Based Algorithms for Computing (ℓ, ℓ)-Isogenies on Kummer Surfaces for Arbitrary Odd ℓ

Ryo Yoshizumi, Hiroshi Onuki, Ryo Ohashi, Momonari Kudo, Koji Nuida

同種写像ベースの鍵共有方式 B-SIDH の解析に関する論文である。

鍵共有方式 SIDH およびその変種である B-SIDH[Costello, Asiacrypt 2020] はどちらも、鍵共有のための補助点情報与えられている条件のもとでの超特異楕円曲線上の同種写像問題（Supersingular Isogeny with Torsion Problem）を安全性の根拠としている。SIDH に対しては [Castryck-Decru, Eurocrypt 2023] により効率的な鍵復元アルゴリズムが与えられており、同論文内で B-SIDH に対しても同様の攻撃が可能であると言及されていたものの詳細が与えられておらず具体的な計算量は不明であった。

計算量評価が未解決であった一因として、楕円曲線を定義する体を指定するアリス側のパラメータ N_A とボブ側のパラメータ N_B の制限がある。SIDH においては $N_A = 2^a, N_B = 3^b$ の形であり、攻撃において要求される $(2,2)$-および $(3,3)$-同種写像の計算手法および計算量は良く知られている。一方で、B-SIDH においては小さいが 2,3 ではない素数 ℓ に対して (ℓ,ℓ)-同種写像の計算を行う必要があるため、この部分の計算アルゴリズムと計算量が未解決であった。

本論文では Lubicz-Robert の公式 [Res. Number Theory 9(1), 7., 2023] を用いた、クンマー曲面の間の (ℓ,ℓ)-同種写像を計算するアルゴリズムを与え、それをサブルーチンとして B-SIDH の具体的な攻撃アルゴリズムを提案している。著者らは攻撃のコードを `https://github.com/Yoshizumi-Ryo/ellell-isogeny_sage` にて公開しており、Costello の論文で 128 ビットセキュリティとされた B-SIDH のパラメータが 11 時間程度で解けたと報告している。

Cryptanalysis of an Efficient Signature Based on Isotropic Quadratic Forms

Henry Bambury, Phong Q. Nguyen

署名方式 DEFI の解析に関する論文である。

DEFI[Feussner and Semaev, ePrint 2024/679] は 2024 年に pqc-forum 上で発表された、Hash-and-Sign パラダイムに基づく署名方式である。安全性の根拠が多変数代数方程式の絶対値が小さな解を求める問題であり、多変数代数方程式の求解問題、格子の近似最短ベクトルの計算問題の困難性からの類推から、高いセキュリティを持つと主張されていた。

DEFI が pqc-forum で公開された直後に本論文の著者による解析が行われており、本論文はその内容を拡張したものとなる。また、攻撃後に Feussner らは新たな方式として DEFIv2 を公開しているが、本論文では v1 への攻撃手法を直接適用することは難しいと述べられている。

本攻撃では公開鍵を用いず、同じ秘密鍵で署名された署名の集合のみから秘密鍵復元を行う。DEFI の署名は文書のハッシュ値 h と、ある関係式 $f(pk, h, z') = 0$ を満たすように調整されたナンス z' から構成されている。署名は秘密鍵行列 B の成分を係数とした z', h の線形結合として表現され、必然的に署名の中には秘密鍵およびナンスの情報が含まれることになる。本論文ではまず、ナンスおよびその生成アルゴリズム内で用いられた中間変数との関係式に着目し、十分な数の署名を用いることで B の成分の線形結合の値、および中間変数の一部が格子基底簡約により復元可能であることを示す（Observation 1）。続いて、得られた情報と署名の集合から別の格子基底を構成し、その中から残りの B の成分の一部および中間変数が復元可能なことを示す（Observation 2）。ここまでに得られた B の成分に関する情報と公開鍵行列 C を組み合わせると、秘密鍵が完全に復元できる。

論文内で構成される格子はランダム格子からは遠く、Gaussian Heuristic よりもかなり小さい格子ベクトルを含むことを証明している。その結果を用いて攻撃に必要な署名の個数を 10 個程度と見積もっている。`https://gitlab.inria.fr/hbambury/defi-nitely-broken` で検証用コードを公開しており、Feussner らが安全であるとしたパラメータ DEFI-64,128 は数分で攻撃可能であるとしている。

最後に、DEFI で用いられる秘密鍵と公開鍵の関係は格子の同型性判定問題（Lattice Isomorphism Problem: LIP）と似ており、さらに解析が可能であるのではないかと著者らは予想している。

Shifting Our Knowledge of MQ-Sign Security

Lars Ran, Monika Trimoska

耐量子計算機署名方式 MQ-Sign および MQ-Sign-LR に対する攻撃論文である。

MQ-Sign および MQ-Sign-LR は、多変数署名方式 Unbalanced Oil and Vinegar（UOV）の鍵サイズを改良した変

種であり、韓国の耐量子計算機暗号コンペティション KpqC の第二ラウンド候補であった。

攻撃の第一報は KpqC の候補について議論する掲示板 KpqC-bulletin（`https://groups.google.com/g/kpqc-bulletin/`）で 2024 年 11 月に発表され、その後 PQCrypto に採録された形となる。MQ-Sign は第 1 ラウンド提出時に中心写像の構造を変えた RR/SR/RS/SS の 4 種類の変種が提案され、その後 RR 以外の変種は構造を用いた多項式時間鍵復元攻撃および高速な署名偽造が報告されていた。唯一残った RR に対して、第 2 ラウンドでは中心写像を巡回シフトで圧縮した変種 LR が追加された。

本論文では、変種 LR に対する指数時間偽造攻撃を提案している。技術的には鍵の偽造を行うための MQ 問題 $\boldsymbol{x}P\boldsymbol{x}^T = \boldsymbol{t}$ に対して、$\boldsymbol{t}$ が d-periodic と呼ばれる特徴を持つ場合に $t_i = t_{i+d}$ の周期性から、問題が d 変数の MQ 問題へと帰着され、大幅に計算量が下がることを利用している。さらに、MQ-Sign が Hash-and-Sign フレームワークを用いていることを利用することで任意の文書 M に対して、$H(M||r)$ が d-periodic となるまでシード r を変えることで偽造が可能となる。d はビネガー変数の個数 v の半分に取ることで攻撃が最適化される。

セキュリティレベル 1,3,5 のパラメータに対して、d-periodic な $\boldsymbol{t}$ を探索するのに必要なシードの個数はそれぞれ $2^{80}, 2^{128}, 2^{176}$ であり、$d = v/2$ 変数の MQ 問題を（論文内で改良された）FXL アルゴリズムを用いて解いた場合の計算量と組み合わせると署名の偽造にかかる計算量が $2^{108}, 2^{172}, 2^{216}$ となる。これは求められている解読計算量よりも 20 から 40 ビット下になる。

小さな周期 d を持つターゲットに対して実証実験を行っており、例えばセキュリティレベル 1 のパラメータに対して、$d = 18$-periodic である場合には 14.2 時間で解くことが可能であるとしている。ただしそのようなターゲットが自然に出る確率は 2^{-224} と極端に低く、現実的ではないと考えられる。

Et tu, Brute? Side-Channel Assisted Chosen Ciphertext Attacks Using Valid Ciphertexts on HQC KEM

Thales B. Paiva, Prasanna Ravi, Dirmanto Jap, Shivam Bhasin, Sayan Das, Anupam Chattopadhyay

NIST 耐量子計算機暗号標準化において標準選定された符号ベース KEM である HQC へのサイドチャネル攻撃に関する論文である。HQC へのサイドチャネル情報を用いた KEM への選択暗号文攻撃は全て、不正な暗号文（malformed ciphertext）からの鍵復元攻撃であり、そのような暗号文を検出する機構および鍵のリフレッシュ機構を用いることで対策が可能であった。本論文で考えられているのは上記対策フレームワークの範囲外にある、デカプセル処理への正規の暗号文の入力とサイドチャネル情報のみを用いた鍵復元攻撃である。

HQC で用いられる線形符号は内部を Reed-Muller 符号、外部を Reed-Solomon 符号とした連接符号である。復号ルーチンにおいて暗号文 (u, v) と秘密鍵 (x, y) から符号語 $c = \mathrm{Encode}(m) + x \cdot r_2 - y \cdot r_1 + (\text{error.})$ を計算しているため、その情報を集めることで x, y の復元を行うことが可能である。

本論文ではデカプセル処理時、Reed-Muller 符号の復号化で用いられる ExpandAndSum 関数と FindPeaks 関数からのサイドチャネル情報を集めることで c を復元し、そこからの秘密鍵の復元を行っている。pqm4 ライブラリを用いた実装からの電磁波漏洩によるサイドチャネル情報を用いた実験により、ExpandAndSum 関数の 2 個のトレース、または FindPeaks 関数の 20 万個のトレースから攻撃が成功することを確認している。さらに著者らは、提案攻撃の特徴として取得したサイドチャネル情報に乗るノイズに対して安定であること、プログラムの実行順序をランダムに変えるシャッフリングに対しても安定した結果が出ることを報告しており、既存の低コストで実装可能なサイドチャネル対策は効果が薄い可能性があるとしている。

SoK: On the Physical Security of UOV-Based Signature Schemes

Thomas Aulbach, Fabio Campos, Juliane Krämer

UOV ベースの多変数多項式署名方式への物理セキュリティに関する論文である。現在、多変数多項式暗号の研究は主に UOV ベースの署名方式に集中している。NIST による追加のデジタル署名の選定プロセスの第 2 ラウンドに残った多変数多項式ベースの方式は UOV そのものか、MAYO、QR-UOV、SNOVA のような変種である。これまでにも Rainbow や LUOV のような UOV ベースの署名が提案されており、最終選考に残らなかったものの多くの知見が得られている。本論文では、特にサイドチャネル攻撃のような物理セキュリティに関する知見を整理し、NIST PQC 追加署名第 2 ラウンドの方式 UOV, MAYO, QR-UOV, SNOVA を総合的に評価している。

UOV ベースの方式に対するサイドチャネル攻撃、故障攻撃は過去に多く提案されており、それに合わせていくつかの署名方式は修正されている。本論文では、既存の攻撃をサーベイし、最新版の署名方式に適用することで包括的な評価を行っている。検討された具体的な攻撃方法は論文内の Table 1,2 に述べられており多岐にわたるが、先行研究では考察されていなかった署名時の salt からの鍵の展開からのサイドチャネル攻撃、オイルベクトルのセットアップに対する故障注入攻撃、サイドチャネル攻撃が新たな脅威として提案されている。

上記 UOV ベース署名方式の物理セキュリティを向上させるための対策として、UOV と MAYO の pqm4 ライブラリでの公開実装から ARM Cortex-M4 上で一次マスキング実装を行い、NUCLEO-L4R5ZI ボード上でのベンチマークとテストベクトル漏洩評価（TVLA）を報告している。MAYO の方ではマスキング不要な処理が存在することから対策オーバーヘッドが小さくなるとしている。鍵圧縮技術やランダム化の選択などの実装上の決定が、物理的セキュリティ、特にフォールト攻撃の有効性に大きな影響を与えるとしている。

Reducing the Number of Qubits in Solving LWE

Barbara Jiabao Benedikt

ternary LWE 問題の解析に関する論文である。ternary LWE 問題は通常の LWE 問題の秘密ベクトル $\mathbf{s}$ の係数を三値 $0, \pm 1$ に制限した変種であり、探索空間の大きさ $\mathcal{S} = 3^n$ を基準として計算量が計られる。

先行研究として May（Crypto 2021）による $\mathcal{S}^{0.25}$ 時間の古典アルゴリズム、および van Hoof et al.（PQCrypto 2021）による $\mathcal{S}^{0.19}$ 時間の量子ウォークを用いたアルゴリズムが知られている。本論文のモチベーションとして、val Hoof らのアルゴリズムで必要とされている指数個の量子ビットの削減がある。既に van Hoof らにより $\mathcal{O}(n)$ 量子ビットで動作する $\mathcal{S}^{0.558}$ 時間の量子アルゴリズムが提案されているため、より小さい計算量を達成することが課題となる。

本論文のアルゴリズムは van Hoof らのアプローチとは異なり、May の meet-in-the-middle ベースのアルゴリズムと、Grover 探索の一般化となる Chailloux ら（Asiacrypt 2017）のアルゴリズムを組み合わせ、部分和問題（SSP）に適用することで ternary LWE を解いている。提案されたアルゴリズムでは、一般化 Dicke 状態を用意する必要がある。これは、$n, q, \ell_0, \ldots, \ell_{2^q-1}$ をパラメータとして、n 個 の q ビットの変数 $x_1 x_2 \cdots x_n$ で、$i = 0, \ldots, 2^q - 1$ に対して $x_j = i$ となる j が ℓ_i 個含まれるものの重ね合わせとして定義される（Definition 3）。$q = 1$ の場合が通常の Dicke 状態となる。本論文の技術的なコアとして、Bärtschi and Eidenbenz（FCT 2019）により得られていた Dicke 状態の再帰的な構成法の一般化を与え、それを用いた SSP のアルゴリズムを与えている。

この部分和問題の量子アルゴリズムを経由するアプローチにより、本論文では ternary LWE 問題を解く $\mathcal{O}(n)$ 量子ビット、$\mathcal{S}^{0.22}$ 古典メモリ、$\mathcal{S}^{0.379}$ 時間のアルゴリズムを得た。また一般化 Dicke 状態の構成アルゴリズムが、`https://github.com/bj-benedikt/Generalized-Dicke-States` にて公開されている。

Module Learning with Errors with Truncated Matrices

Katharina Boudgoust, Hannah Keller

Module-LWE 問題（MLWE）の変種とその解析に関する論文である。MLWE は、適切な環 R_q 上のベクトル s, e と行列 A を用いて計算された $b = As + e$ から s を復元する計算問題として定式化される。多くの先行研究では A は元を一様ランダムとし、s, e の確率分布を変えることでどのような応用が可能なのか、問題の困難性がどのように変化するのかという点に着目していた。A の分布を変える先行研究として、本論文では Jia ら（IET Info. Sec., 2023）による truncated MLWE を取り上げている。この問題は A を一様ランダムにサンプリングした後に下位ビットを 0 に丸めた分布から取る。Jia らの論文では Module 版 NTRU 問題と truncated LWE 問題の探索版との関係が示されている。

本論文では、truncated MLWE の困難性が MLWE 問題と等しいことを示す。技術的には 2 種類の異なるアプローチにより探索版と判定版の問題にして困難性の結果を示している。一つめの手法は格子暗号の安全性証明に用いられる Réyni divergence を用いて、A が一様ランダム分布の場合と下位ビットを削除した分布の統計距離から攻撃者のアドバンテージに関する不等式を導く。このアプローチでは探索版 truncated LWE の困難性を示すことはできるものの、判定版に対する同様の方針での証明はアドバンテージの上界評価が次元の指数関数となり失敗する。

そのため、二つ目のアプローチとして truncated LWE のインスタンスを、秘密ベクトル s に関する情報が漏れている approximate hint 付きの MLWE 問題（Bermudo Mera et al., PKC 2022）と捉えることで、探索版、判定版の困難性証明を与えている。

以上の二つのアプローチでは、攻撃者の得るアドバンテージが異なる。また、本論文では次数が 2 べきの円分体を仮定しているが、他の環でも同様の結果が得られるとしている。

Discrete Gaussian Sampling for BKZ-Reduced Basis

Amaury Pouly, Yixin Shen

LWE 問題の計算量評価に関する論文である。本論文は同著者らによる（Pouly and Shen, Eurocrypt 2024）の後続研究であり、LWE 問題に対する Dual 攻撃の計算量評価を、なるべく少ない仮定から導くというモチベーションで行われている。

LWE 問題のインスタンス $b = As + e$ に対して、Dual 攻撃では q-ary 格子 $L_q^\perp(A)$ の短いベクトル x をサンプリングし、$Ax - b$ を計算することで判定版 LWE 問題を解いていた。（インスタンスが LWE ならば $Ax - b$ のノルムは小さく、ランダムならば大きくなるという事実から判定を行う。）

近年のアプローチでは s の一部分を全数探索とすることで計算量を下げている。x をサンプリングするアルゴリズムは様々なものが提案されているが、著者らはマルコフ連鎖モンテカルロ（MCMC）を用いた Gaussian Sampler（Wang and Ling, IEEE-IT 2019）を取り上げている。

技術的な貢献として、著者らは分散パラメータ s の Gaussian Sampler の計算量を規定する量 Δ の近似式および幾何級数仮定（GSA）を満たす格子基底に対する簡易な計算式を与えている。また、実際の BKZ 基底を用いた評価とのずれを実験的に検証しており近似式の精度は暗号学的な範囲では問題ないとしている。

提案した解析手法を用いて CRYSTALS-Kyber の攻撃計算量評価を行っており、LWE サンプル数 m およびブロックサイズ β の再最適化を行った結果、Eurocrypt 2024 での結果と比較して 4 から 10 ビット程度攻撃計算量が削減されている。いずれも Kyber 開発者の主張するセキュリティパラメータを下回るものではないため、暗号の安全性への影響は小さいと考えられる。

Heuristic Algorithm for Solving Restricted SVP and Its Applications

Geng Wang, Wenwen Xia, Dawu Gu

最短ベクトル問題の変種の解析に関する論文である。格子暗号の安全性の根拠となる計算問題を格子問題に変換して解く場合、多くは最短ベクトル問題に帰着されるが、元の暗号の特徴から、変換先の格子がランダム格子になるとは限らない。特に、LWE 問題から unique SVP 問題への帰着のように、最短ベクトルが Gaussian Heuristic で予想されるよりも非常に短い場合が研究の対象となる。また、暗号の構成から ℓ_∞ ノルムに関する制限などの、最短ベクトルのユークリッド長の情報以外にも利用可能なヒントがある場合も多い。このようなユークリッド長以外の制限のある最短ベクトル問題に対するアプローチとしては、篩アルゴリズムの出力を列挙し、その中から要件を満たすものを探索する手法があるが、より効率的な手法があると考えられる。

本論文での貢献は以下のようにまとめられる。

- 既存研究に現れる SVP の変種を含む計算問題として restricted SVP を定式化。求めるベクトルの上界と制限関数 $\mathcal{R}$ を用いて定式化される。
- Dimension-for-free technique の近似版 SVP への拡張と randomized slicer を用いた改良
- restricted SVP のヒューリスティックな解法アルゴリズムと cost estimator の提案

提案手法を用いて CRYSTALS-Dilithium の署名偽造の困難性の根拠となっている SIS 問題の計算量評価を行っている。Dilithium 提案書のレベル 2,3,5 のパラメータに対して、それぞれ計算量が $2^{159.9}, 2^{223.0}, 2^{300.0}$ であるとしており、これは元々の評価とほぼ同様であると主張している。Cost estimator は `https://github.com/Summwer/inf-cvp-estimator` で公開されている。

On the Structure of the Schur Squares of Twisted Generalized Reed-Solomon Codes and Application to Cryptanalysis

Alain Couvreur, Rakhi Pratihar, Nihan Tanisali, Ilaria Zappatore

構造化された符号を用いた McEliece 暗号の解析に関する論文である。McEliece 暗号は古典的な符号ベース暗号であり、トラップドア関数の構成に Goppa 符号を用いている。方式の提案以降、トラップドアの構成を様々な線形符号で置き換えた変種が提案されてきた。

これらの変種のうちいくつかは Schur square-distinguishing と呼ばれる攻撃に対して脆弱であることが知られている。符号語長 n の線形符号 C_1, C_2 に対して、Schur product は全ての $c_1 \in C_1, c_2 \in C_2$ の成分ごとの積 $c_1 * c_2$ で張られる線形符号として定義され、特に $C_1 = C_2$ の場合には Schur square と呼ばれる。2010 年代より、Schur square の次元を用いて構造付きの符号とランダム線形符号の識別が可能であり、その識別器を用いた McEliece 暗号の鍵復元が可能であることが発見された（Couvreur et al. Des. Codes Crypt., 2014 など）。以降、Schur square による識別攻撃に強く効率の良い符号を探索する研究が行われている。

本論文では、Beelen ら（ISIT 2018）により構成された Maximum Distance Separable（MDS）Twisted Reed – Solomon（TRS）符号、およびその一般化である Twisted generalized Reed-Solomon（TGRS）符号ベースの McEliece 暗号の安全性について議論される。Beelen らは TRS 符号を Schur square による識別攻撃に対して安全であると主張したが、本論文ではその主張が誤りであり、さらに一般化された TGRS 符号に対しても成り立たないことが示される。

本論文では、TRS と TGRS を含む quasi-GRS 符号という大きな符号のクラスを定義する。符号の縮小（n 次元の

成分のうち、$I \subset [n]$ 成分のみをとりだした符号）の Schur square を考えることで識別器が構成可能であること、およびそれを用いた鍵復元攻撃が与えられている。また、詳細な成功確率の評価が与えられている。

検証用の実装コードは `https://github.com/nihantanisali/TGRS` で公開されている。

Quadratic Modelings of Syndrome Decoding

Alessio Caminata, Ryann Cartor, Alessio Meneghetti, Rocco Mora, Alex Pellegrini

重み制限付きのシンドローム復号問題の解析に関する論文である。シンドローム復号問題を多変数の 2 次連立方程式に変換しグレブナー基底による手法で解く際の課題として、変換手法の効率性、変換後の方程式の規模、方程式が確実に元の問題の解を与えるかどうか、計算量評価などがある。

本論文では、符号の最尤復号問題と多変数多項式の求解問題の等価性を示した Meneghetti ら（Ann. Mat. Pura Appl., 202(2), 2023）の変換手法を改良し、重みを t 以下に制限した $\mathbf{F}_2$ 上のシンドローム復号問題から多変数方程式の帰着において変数の数と方程式の数を共に $O(n(\log_2 n)^2)$ から $O(n\log_2 t)$ へ削減している。また、重みがちょうど t のベクトルを復元する問題（Exact Weight Syndrome Decoding Problem、ESDP）ではさらに問題の規模を削減する手法を提案している。

後者の ESDP に関して、グレブナー基底を用いて解いた場合の計算量評価を行うため、基底の性質と degree of regularity の評価を与え、計算機実験により確認している。同時に Prange の ISD との比較が行われ、現在の多変数を用いた手法を符号ベース暗号で用いられるようなパラメータの符号に当てはめると ISD が圧倒的に優位であるとしているものの、代数的な手法により明らかになる脆弱性を発見できる可能性があることを強調している。

最後に、変換手法を $\mathbf{F}_q$ 上の符号問題へと一般化したものを与え、構造を解析している。

An Improved Algorithm for Code Equivalence

Julian Nowakowski

線形符号の等価性判定問題および署名方式 LESS の解析に関する論文である。$\mathbf{F}_q$ 上の (n,k)-線形符号 $\mathcal{C}_1, \mathcal{C}_2$ が等価であるとは、その生成行列 G_1, G_2 が適当なユニタリー行列と一般化置換行列（monomial matrix）Q を用いて $G_2 = UG_aQ$ の関係で結ばれることをいい、この関係を満たす U, Q を発見する計算問題を符号の等価性判定問題（linear code equivalence problem: LEP）と呼ぶ。

先行研究において Chou ら（ePrint, 2023/1533）は $G_i = [I_k|A_i], i = 1, 2$ に対して、一般化置換行列 Q_r, Q_c を用いて $A_2 = Q_r A_1 Q_c$ の関係をもつならば G_1, G_2 が等価であるという関係に着目した。この関係による代表元を符号の標準形（canonical form）として、標準形の計算を行うアルゴリズムをサブルーチンとして用いることで $2^{H(k/n)/n}$ 時間の確率的な等価性判定アルゴリズムを与えた。ただし、$H(\cdot)$ は 2 元エントロピー関数である。Chou らのアルゴリズムは $q = \Omega(n)$ に対して動作することが知られている。

本論文では、q の適用範囲を拡大し $q \geq 7$ に対する効率的なアルゴリズムを与えた。技術的には Chou らのアルゴリズムの再解釈を基礎としている。先行研究では $\mathcal{C}_1, \mathcal{C}_2$ の Information Set 上の等価性の関係を用いた meet-in-the-middle を用いており、q が小さい場合には成功確率が低かった。この欠点を、新たな canonical form を定義することで改良している。検証用ソースコードは `https://github.com/juliannowakowski/lep-cf` で公開されている。

An Improved Both-May Information Set Decoding Algorithm: Towards More Efficient Time-Memory Trade-Offs

Hiroki Furue, Yusuke Aikawa

シンドローム復号問題の解析に関する論文である。線形符号のシンドローム復号問題を解くための ISD（Information Set Decoding）アルゴリズムは多くの符号ベース暗号の解析に用いられる。Both と May（PQCrypto 2018）による時間-空間トレードオフを用いた復号アルゴリズムが漸近的に最速であり、多くの符号ベース暗号のパラメータ設定に用いられている。

本論文では Both-May アルゴリズムの改良である fastest ISD を提案した。技術的には Both-May で用いられていたインデックスの分割による再帰的な ISD の適用において、探索木の構成を簡素化することで高速化を行っている。具体的な計算量の削減として、メモリ量が $2^{0.07n}$ よりも小さい領域に対して Both-May アルゴリズムよりも計算時間の指数部分を数パーセント削減している。特に、メモリが $2^{0.04n}$ の場合に $2^{0.105n}$ 時間から $2^{0.101n}$ 時間へと削減されている。

計算量の評価プログラムは `https://github.com/Memphisd/Revisiting-NN-ISD` で公開されている。

An Efficient Collision Attack on Castryck-Decru-Smith's Hash Function

Ryo Ohashi, Hiroshi Onuki

同種写像によるグラフ構造を用いたハッシュ関数の解析に関する論文である。本論文では Castryck-Decru-Smith（J. Math. Cryptol. 14, 2020）による $(2,2)$-同種写像グラフを用いた Charles-Lauter-Goren 型のハッシュ関数（以下、CDS ハッシュ関数）の衝突発見アルゴリズムを新たに提案している。

CDS ハッシュ関数は適当な Abel 多様体間の $(2,2)$-同種写像を用いたハッシュ関数で、適当な同種写像 $\phi_0\colon A_0 \to A_1$ を初期値とする。入力文書に従い ϕ_i を ϕ_{i+1} に拡張していき、最終的な ϕ_n の像 A_n が種数 2 の曲線の Jacobi 多様体と同型であることを利用してその Igusa 不変量をハッシュ値として出力する。

Castryck らの提案論文では初期写像を逆向きに拡張した $A_{-1} \to A_0 \to A_1$ から $A_n \sim \mathrm{Jac}(C)$ へのパスを Meet-in-the-Middle により探索することで時間・空間計算量が $\tilde{O}(p^{3/2})$ のアルゴリズムを得ている。本論文ではこの写像の拡張をさらに後ろ向きに広げ、楕円曲線のペア $E_0 \times E_0$ から $E_1 \times E_2$ への写像列に拡張する。この列から適当な A_d $(d < n)$ までの写像 $A_0 \to A_d$ を構成することができ、残りの $A_d \to A_n$ を meet-in-the-middle で計算することで衝突発見が可能となる。パラメータを最適化することで $\tilde{O}(p^{3/10})$ 時間・空間のアルゴリズムが得られ、Castryck らの評価から大幅に改良されている。著者らはまた、MAGMA による Proof of Concept コードを `https://github.com/Ryo-Ohashi/CDScollision` で公開しており、提案者らにより 384 ビットセキュリティとされていたパラメータが 64 並列 17 時間で解かれたと報告している。

本論文ではまた、曲線 E_0 の 2^e-ねじれ部分群が小さい $k = O(1)$ に対する $\mathbf{F}_{p^k}$-有理点である場合には、$\log p$ の多項式時間で衝突が発見可能であることを示している。

最後に、攻撃に対するハッシュ関数の単純な countermeasure として、初期写像 $\phi_0\colon A_{-1} \to A_0$ を、既知の自己同型環をもつ超特異楕円曲線の積から十分に “遠い” ものとすることで、攻撃計算量を $\tilde{O}(p)$ 時間、$\tilde{O}(p^{3/5})$ まで増やすことができると報告している。

E.7 Eurocrypt 2025

The syzygy distinguisher

Hugues Randriambololona

符号ベース暗号の鍵安全性に関する論文である。NIST PQC 標準化第 4 ラウンド候補の符号ベース暗号 Classic McEliece の安全性に関係する。

McEliece 型の符号ベース公開鍵暗号においては、符号の復号問題が困難であるという復号困難性の他に、公開鍵行列とランダム行列が識別困難であることを主張する McEliece 仮定の成立を前提に方式の安全性が議論されている。McEliece 型の符号ベース暗号では OW-CPA を破ることで行列の識別が可能であり、逆の関係は示されないものの必要なデファクトスタンダード要件として置かれている。（多変数公開鍵暗号の構成においても同様の UOV 仮定が用いられるが、LWE ベースの格子暗号では LWE 仮定として暗号文の識別困難性に吸収される等、要求レベルにはばらつきがある。）

本論文では、Goppa 符号の生成行列とランダム線形符号の生成行列の識別器 “syzygy distinguisher” を提案する。計算量は誤り訂正能力 t の準指数時間であり、汎用の復号アルゴリズムよりも小さく指数時間の壁を破る初のアルゴリズムであるとしている。

識別に用いる不変量の構成は以下のとおりである。双対符号の短縮符号 $C =: C^{\langle 1\rangle}$ から Schur 積によって帰納的に符号の拡大 $C^{\langle r+1\rangle} = C^{\langle r\rangle} \star C$ を構成し、それらの直積による次数付き代数 $C^{\langle\cdot\rangle} := \bigoplus_{r\geq 0} C^{\langle r\rangle}$ を斉次座標環と同一視する。この斉次座標環 $M_0 := C^{\langle\cdot\rangle}$ に対して次数付き Betti 数を以下のように定義する。M_0 は有限生成な次数付き S-加群であり、F_0 を斉次生成元の最小系に基づく自由加群とする。ただし、$S = F[X_1, \ldots, X_k]$ は F 上多項式環。

$M_{i+1} = \ker(F_i \to M_i)$、$F_i$ を M_i の斉次生成元の最小系に基づく自由加群とすることで帰納的に $F_1, F_2, \ldots$ を定義し、完全列（$S/C^{\langle\cdot\rangle}$ の最小自由分解）$0 \to F_{k-1} \to \cdots \to F_2 \to F_1 \to F_0 = S \to C^{\langle\cdot\rangle} \to 0$ が得られる。このときの F_i を次数 j の元で生成される階数 1 の自由 S-加群 $S(-j)$ に分解した $F_i = \bigoplus_{j\geq 0} S(-j)^{\beta_{i,j}}$ における次数を次数付き Betti 数 $\beta_{i,j}$ と呼び不変量として用いる。

符号が Goppa 符号、一般化 Reed-Solomon 符号などの場合、符号の構造から最小自由分解に含まれる syzygy が多くなり、Betti 数が大きくなること、ランダム線形符号のように構造を持たない場合には小さくなるという性質を用いて $\beta_{r,r-1}$ の値から識別を行う。特に、双対 Goppa 符号、双対交代符号の場合には拡大体に持ち上げることで生成元が満たす関係式が行列の 2×2 マイナーとして書けることから Betti 数の下界が導かれるため、識別性能を上げることができる。

提案アルゴリズムを Classic McEliece に適用し計算量評価を行い、ヒューリスティックな仮定のもとでパラメータ Classic McEliece 348864 の方式に対して 2^{401} での識別が可能であるとしている。これは暗号方式自体のビットセキュリティよりも高く、現在のところ方式の安全性への影響は無いとしている。

Improved Cryptanalysis of SNOVA

Ward Beullens

NIST 耐量子計算機暗号標準化の追加署名第 2 ラウンド候補である多変数多項式ベース署名 SNOVA（Cho、Ding、Kuan、Li、Tseng、Tseng、Wang）に対する解析論文である。

SNOVA では、同系統の多変数多項式ベース署名である MAYO の構成に用いられている whipping のコアである、

オイル空間の分割からの直積の構成による次元拡張が暗黙に用いられていることを観測する。本論文ではこの関係を指摘したうえで、MAYO では構成後もランクが低下しないように注意深く構成が選ばれているのに対し、SNOVA では用いられている行列の性質からランクを大幅に低下させる線形結合が存在し、それを用いることで効率的な署名の偽造が可能となる。

新たな偽造攻撃により、方式の提案者がセキュリティレベル 1,3,5 としたパラメータセットの再評価が行われ、既知の攻撃よりも 2^8 から 2^{39} 程度攻撃計算量が下がっている。この評価はランダムに生成された鍵を仮定したものであり、さらに攻撃者に有利な構造を引き出すことのできる弱鍵に対しては著しい計算量の低下が指摘されている。

具体的にはセキュリティレベル 1 を達成すると主張されているパラメータセット SNOVA-37-17-2 に対して、公開鍵のうち 500 個に 1 個は 2^{97} 時間での偽造が可能である弱鍵であり、さらに約 14 万 3 千個に 1 個の割合で、数分程度で偽造が可能な鍵が含まれていることが確認された。

攻撃の検証用コードは `https://github.com/WardBeullens/BreakingSNOVA` で公開されている。

A Reduction from Hawk to the Principal Ideal Problem in a Quaternion Algebra

Clémence Chevignard, Guilhem Mureau, Thomas Espitau, Alice Pellet-Mary, Heorhii Pliatsok, Alexandre Wallet

NIST 耐量子計算機暗号標準化の追加署名方式の第 2 ラウンド候補である HAWK の安全性に関連する論文である。

格子同型性問題（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それらを変換する直交基底 O が存在するかどうかを判定、もしくは探索する計算問題である。Module 格子上での同型性判定問題（Module-LIP）も同様に、Module 格子の疑似的な基底に対応する疑似 Gram 行列間に成り立つ関係を判定、探索する計算問題として定義される。特に、次数 $d = 2^n$ の円分体上の Module-LIP は署名方式 HAWK の鍵安全性の根拠とされている。

本論文では、虚数乗法（CM）体 F 上の拡大体 $K = F(\sqrt{a})$ を用いて定義される rank-2 Module 格子における LIP（[Mureau et al., Eurocrypt 2024] で定式化された worst-case の計算問題である $\mathrm{wc} - \mathrm{smod}LIP_K^B$ 問題）から F 上の四元数環の整域における reduced-norm Principal Ideal Problem（nrdPIP）への多項式時間還元を与えている。ただし帰着は non-uniform であり、四元数環の特殊な元の情報を必要とする。

この還元の特殊ケースとして、Hawk の鍵復元攻撃で用いられる LIP では K が次数 d の円分体であり、帰着に必要な四元数環の元が多項式時間で計算可能となることから帰着が uniform となる。特に、この帰着が nrdPIP オラクルの呼び出し 1 回で済むという事実と PIP の既知の最良アルゴリズムが $2d$ 次元の SVP オラクルを 1 回呼び出すものであるという先行研究 [Kirschmer-Voight, SIAM J. Comp, 2010] により、Hawk の鍵復元には SVP オラクルの呼び出し 1 回で十分であることがわかる。

関連する研究として、rank-2 Module-LIP を定義する数体 K の性質による困難性の違いの分類がある。[Mureau et al., Eurocrypt 2024] での K が総実数体の場合、[Allombert et al., Eurocrypt 2025] での K が実埋め込みを一つでも持つ場合にヒューリスティックな古典多項式時間アルゴリズムの存在が示されている。HAWK の鍵復元困難性の根拠となる LIP で用いられる次数 $d = 2^n$ の円分体は総虚数体となり nrdPIP への還元が示されたため、rank-2 Module-LIP における困難性の分類が nrdPIP の困難性解析に収束したことになる。

Singular Points of UOV and VOX

Pierre Pébereau

署名方式 UOV および VOX に対する鍵回復攻撃論文である。UOV および VOX は、NIST 耐量子計算機暗号標準化の追加署名方式の候補である。これらの方式は、秘密鍵として隠されたアフィン変換を用いて、公開鍵として多変数二次多項式を構成している。これらの方式の安全性は、公開鍵の構造が十分にランダムであることが仮定されていた。

本論文では、公開鍵にある多項式系により定義される代数的集合（algebraic set）の幾何学的性質、特に特異点を解析することで、新しい鍵回復攻撃を提案している。この新しい攻撃は、UOV および VOX のセキュリティを漸近的にもゲート数の観点からも低下させるものであり、提案されたパラメータセットが NIST のセキュリティ要件を満たしていないことが報告された。より具体的には、VOX/UOV のセキュリティは、セキュリティレベル I、III、V においてそれぞれ過大評価されていたことを示される。特に VOX に対して、1 つのベクトルから鍵回復を行う多項式時間アルゴリズムを導入し、セキュリティレベル V において数秒で実行可能な実装が示されている。

Do Not Disturb a Sleeping Falcon: Floating-Point Error Sensitivity of the Falcon Sampler and Its Consequences

Xiuhan Lin, Mehdi Tibouchi, Yang Yu, Shiduo Zhang

NIST PQC 標準化の格子ベース署名方式 FALCON およびその変種に対するサイドチャネル攻撃の論文である。

FALCON は鍵生成および署名生成時に格子上の離散ガウス分布からのサンプリングを必要とする。この部分は処理の高速化のため、LDL 分解を用いた高速フーリエサンプリングのような複雑なアルゴリズムを用いており、実装ミスが誘導する脆弱性の他、正しい実装においても浮動小数点の仕様ごとの違いによる出力の不安定さに由来する脆弱性が存在する可能性が指摘されてきた。

本論文では、FALCON の署名生成で用いられる 1 次元の離散ガウス分布生成ルーチン内で発生する浮動小数点処理の数値的不安定性により、同じランダムネスの入力に対しても異なる格子点を出力する可能性があり、その差分から秘密鍵の復元が可能となることを報告している。

仕様書どおり正しく実装された FALCON では署名内の salt の機能により、サンプリングサブルーチンが完全に同一の入力を 2 回処理することは防がれるため現実でのインパクトは小さいとしている。繰り返し乱数使用の危険性に対する注意喚起を除けば、Falcon 署名そのもののセキュリティにはほとんど影響しないと報告されている。

発見された攻撃は FALCON で用いられる離散ガウス分布特有の性質に基づいており、同系統の署名方式である Mitaka、Antrag には問題は発見されていないとしている。一方で、ID ベース暗号、SNARK-friendly 署名、集約署名のような方式の設計には脱乱択化された FALCON の変種が用いられることもあり、本論文内の攻撃により秘密鍵の漏洩が起きる可能性を指摘している。

技術的には高次元の離散ガウス分布生成アルゴリズムから呼ばれる 1 次元の離散ガウス分布 $D_{\mathbb{Z},\sigma,c}$ の生成ルーチンにおいて、中心 c の小数部 $r = c - \lfloor c \rfloor \in [0,1)$ を求め、$D_{\mathbb{Z},\sigma,r}$ のサンプリングを行った後に結果に $\lfloor c \rfloor$ を足す操作を行っている。c が整数に非常に近い場合に浮動小数点演算の誤差により $\lfloor c \rfloor$ の計算結果が異なる可能性がある。

著者らはこの現象は FALCON の署名生成において用いられる、LDL 分解に対応する木構造の特徴から、最初の 2 回と最後の 2 回の離散ガウス分布サブルーチンにおいて上記のミスが無視できない確率で起きるとヒューリスティックな解析を行っている。

著者らはいくつかの要因を例として挙げている。第一には同一のソースコード、コンパイラオプションを用いてコン

パイルしたバイナリに同一の入力を与えた場合でもコンパイラ内部の乱数性、CPU のアウトオブオーダー実行におけるレジスタ処理が要因で異なる出力となる可能性である。第二には同一のソースコードからコンパイルされたバイナリでもターゲットアーキテクチャの違いにより異なるもの生成され実行環境ごとに処理順序がずれる可能性である。第三の可能性として、FALCON の API として 2 種類の実装が用意されている点を指摘している。これは実行速度と使用メモリのトレードオフのため、サンプリングに用いる木を動的に構成するもの（dynamic）と事前に用意されたものを呼び出して用いる（tree）もので、その間で処理の違いが生まれる可能性がある。

対策として、c が整数に近くなる現象を避けるために $\lfloor c \rceil$ を四捨五入に置き換える、$\|(g, -f)\|^2$ を奇数にすること、2 種類の API 内での挙動を一致させるように演算順序を指定する、fused multiply-add (FMA) 等のずれを生む可能性のある命令の使用を避ける等を提案している。

A Generic Framework for Side-Channel Attacks Against LWE-Based Cryptosystems

Julius Hermelink, Silvan Streit, Erik Mårtensson, Richard Petri

LWE ベース暗号方式のサイドチャネル攻撃に関する論文である。NIST PQC 標準化の格子ベース暗号方式 ML-KEM の安全性に関連する。

格子暗号に対するサイドチャネル攻撃は NIST 標準化の候補を中心に数多く提案されている。近年、サイドチャネル情報からの Bayesian updating を用いた用いた攻撃がそれまでの方法よりも高い攻撃性能を持つことが実験的に検証されつつある。このことを踏まえ本論文では、先行研究の攻撃フレームワークを統合し、サイドチャネル情報をエラーを含んだ確率分布 distribution hints として定式化し、得られた hints から秘密鍵を復元する確率伝搬法ベースの手法と、貪欲法ベースの手法を提案する。理論的に後者は前者の計算量を削減した近似手法と捉えることができる。

本手法の利点として、これまで格子暗号のサイドチャネル解析で取り上げられてきたような、値そのものの漏洩の他に、歪んだノイズの乗ったサイドチャネル情報、ハミング重みなどの二次的な変数にノイズが乗った情報を取り扱うことができ、実攻撃の成功確率を上げるとしている。

ML-KEM に対する漏洩シミュレーションからの攻撃実験が行われ、得られる情報の種類、ノイズを様々に変えて確率伝搬法、貪欲法での処理後に秘密鍵復元に要求される BKZ アルゴリズムのブロックサイズがシミュレーションされた。[Dachman-Soled et al., CRYPTO 2020] の問題設定のおいてヒント数が増加するに従い必要ブロックサイズ β が低下するものの、100 を下限としてそれ以上は下がらないという実験結果が報告されていた。本論文の手法では同等の問題設定において β は急速に 0 に近づき、実時間での攻撃が可能となる。

また、復号ルーチンの処理 $\boldsymbol{v} - \langle \boldsymbol{u}, \boldsymbol{s} \rangle$ からの秘密鍵の漏洩が、これまで考えられてこなかった形で可能であるとしている。具体的には先行研究においては平文が $\boldsymbol{m} = 0$ であるときのハミング重みの情報を直接用いていたのに対し、distribution hints を用いることで復元に必要な選択平文の個数が半減すると報告している。

検証用コードは `https://github.com/juliusjh/distribution_hintsandhttps://github.com/juliusjh/distribution_hints_solvers` で公開されている。

Cryptanalysis of Rank-2 Module-LIP: A Single Real Embedding Is All It Takes

Bill Allombert, Alice Pellet-Mary, Wessel van Woerden

格子ベース暗号の安全性の根拠となる格子同型性問題（Lattice Isomorphism Problem: LIP）の困難性に関する論文である。

LIP は与えられた 2 つの格子基底 B_1, B_2 に対してそれらを変換する直交基底 O の存在を判定、もしくは探索する

計算問題である。近年の暗号方式の構成に用いられる Module-LIP は数体 K 上の Module 格子を用いて定義されるが、この K の性質により問題の困難性が大きく変化することが知られている。特に K が総実数体の場合の rank-2 Module-LIP に対してはヒューリスティックな古典多項式時間アルゴリズムが存在することが知られており [Mureau et al., Eurocrypt 2024]、本論文はそれを拡張して K が実埋め込みを一つでも持つ場合にヒューリスティックな古典多項式時間アルゴリズムを与える。ただし論文内で扱われる Module-LIP は全て自由加群上での議論であることに注意。

本論文の結果は実際の暗号方式への影響は無いとしているものの、NIST PQC 標準化第 3 ラウンド候補であった NTRU Prime で用いられる $\Phi = x^p - x - 1$ を定義多項式とする体からの構成では実埋め込みを持つため、Module-LIP の構成に用いることができないことを注意している。（これは NTRU Prime 自体の危殆化を主張するものではない。）また、NIST PQC 標準化プロジェクト第 2 ラウンド候補である格子ベース署名方式 Hawk の安全性の根拠となる rank-2 Module-LIP では定義多項式を $x^d + 1, d = 2^n$ としているため、総虚数体となり本攻撃の対象ではない。Eurocrypt 2025 の Chevignard らの論文も参照。

数体 K 上の rank-r の Module-LIP、秘密の基底 $B \in \mathcal{O}_K^r$ により定義される Module 格子 $\mathcal{M} = B \cdot \mathcal{O}_K^r$ に対して対応するグラム行列 $G_1 = \overline{\sigma(B^T)}\sigma(B)$ および $\mathcal{M}$ の別の基底が与えられたときに、基底 B を復元する問題として定式化される。攻撃の順序は (i) 与えられたグラム行列からその二次形式 $B^T B$ を復元し、(ii) 二次拡大体 $L_1 = K(i)$ のイデアル $(a + bi)\mathcal{O}_{L_1}$ の生成元を復元。このとき a, b が基底 B の第 1 列となるため (iii) イデアルからの (a, b) の復元を行う。

(i) の復元において、実埋め込み σ_1 の性質から $\overline{\sigma_1(B^T)}\sigma_1(B) = \sigma_1(B^T B)$ が成り立つため、この値から格子基底簡約による integer relation-finding を用いて古典多項式時間で $B^T B$ を復元可能である。また、(ii) のイデアルの生成元の復元も古典多項式時間で計算される。(iii) では秘密情報の復元のため、前段階の計算中に得られた $z\mathcal{O}_{L_1}$ と $\overline{\sigma_1(B)}^T \sigma_1(B)$ に関する情報を用いて Log-unit lattice の復元を行い、最終的に $a + bi$ の情報を取り出す。この最終段階において Log-unit lattice の最短ベクトルの挙動がランダム格子に近いと仮定することで量子多項式時間アルゴリズムが示されるが、成り立たない場合にも $\mathrm{Gal}(\Phi)$ が Φ の根の集合に 2-transitive に作用するという仮定を用いると量子多項式時間であることが示せる。ただし、与えられた K に対して特定の条件を満たす素数を効率よく発見可能であるという別のヒューリスティック（Gentry-Szydlo friendly 条件）を置くことで、古典多項式時間での攻撃が可能であることが証明されており、この意味で実埋め込みを持つ K 上の rank-2 Module-LIP に対するヒューリスティックな古典多項式時間アルゴリズムが「ほぼ得られた」と主張している。

実験用コードは `https://github.com/WvanWoerden/modLIP_real_embedding` にて公開されている。

Fine-Grained Complexity in a World without Cryptography

Josh Alman, Yizhi Huang, Kevin Yeo

Fine-grained 暗号および離散対数問題についての理論的な解析論文である。Fine-grained 暗号とは、攻撃者と正直な当事者の間に多項式の差があればよいとする、標準的な暗号に比べてより弱い仮定に基づく暗号の考え方であり、k-SUM 問題や Zero-k-Clique 問題といった $\mathbf{P}$ に属する問題に困難性の根拠を置くプリミティブの構成を許す。Fine-grained 暗号は “Pessiland”、すなわち $\mathbf{P} = \mathbf{NP}$ が成り立つ、あるいは一方向関数が存在しないといった状況においても、依然として有効であることが期待されている。 本論文では、標準的な暗号仮定がすべて偽であると仮定したうえで、fine-grained な計算複雑性を調べることで fine-grained 暗号の妥当性が検討されている。

主な結果として、よく知られた多くの fine-grained 計算複雑性問題が、一方向関数が存在しないとき、平均計算量においては容易に解けることが示された。換言すれば、fine-grained 暗号を構築するための候補となる困難性仮定の多くが、Pessiland においては成り立たないことが報告された。例えば、一方向関数が存在しないと仮定したとき、十分大

きな定数 k に対して、平均計算量版の k-SUM や Zero-k-Clique 予想は偽であることが示されている。この結果の対偶として、すべての定数 k に対して、k-SUM あるいは Zero-k-Clique の平均計算量困難性が $n^{\omega_k(1)}$ であることを仮定すれば、一方向関数の明示的な構成が与えられることが報告された。

さらに、fine-grained 計算複雑性における帰着の障壁が、暗号における問題によって説明される可能性があることが本論文では報告されている。例えば、離散対数計算の高速化を与えることは、k-SUM とその巡回群への拡張である k-CYC の平均計算量が同値であることを示す設計を与えることと同値であることが示された。これは特に k-CYC から k-SUM への帰着が得られれば、離散対数、素因数分解、RSA、平方剰余性判定といった問題に対する画期的なアルゴリズムにつながる可能性があることを示唆する。著者らは、前処理付き離散対数問題が k-CYC-Index 問題に帰着可能であることを示し、さらに平均計算量版の k-SUM-Index および k-CYC-Index に対する高速アルゴリズムを提示している。

Computing the Endomorphism Ring of a Supersingular Elliptic Curve from a Full Rank Suborder

Mingjie Chen, Christophe Petit

超特異楕円曲線の自己準同型環計算（EndRing 問題）に関する論文である。この問題は、超特異楕円曲線ベースの暗号プロトコル（CGL ハッシュ関数、SQIsign、CSIDH、SCALLOP など）の安全性の根拠をなすものである。Kohel は 1996 年に、有限指数の部分環（suborder）を生成するアルゴリズムを提示したが、完全な自己準同型環の計算までは未解決だった。

本論文では、フルランクの部分環（suborder）が与えられたときに、自己準同型環を計算する問題が研究され、結果として、EndRing 問題に対する多項式時間量子アルゴリズムが与えられた。この結果を得るための研究のアプローチにおいて著者らは、ASIACRYPT 2023 で Chen らにより提案された IsERP 問題（既知の自己準同型環を持つ曲線 $\widetilde{E}$ と、弱同種表現（weak isogeny representation）をもつ同種 $\varphi\colon \widetilde{E} \to E$ が与えられたとき、E の自己準同型環を計算する問題）に対する多項式時間量子アルゴリズムも得ている。さらに量子帰着に関するいくつかの結果も得ている。特に EndRing 問題から OneEnd 問題（非自明な自己準同型を一つ見つける問題）への帰着のクエリ計算量について、古典的には $O(\mathrm{poly}(\log p))$ だったものを、量子的に $O(1)$ に改善できる方法を発見し、OneEnd 問題の量子解析を推進した。これは SQISign の安全性証明を強化するものでもある。他にも EndRing 問題の他問題への量子帰着についても研究している。これらの帰着もすべて多項式時間であり、量子クエリ計算量は $O(1)$ である。

E.8 Crypto 2025

KLPT^2: Algebraic Pathfinding in Dimension Two and Applications

Wouter Castryck, Thomas Decru, Péter Kutas, Abel Laval, Christophe Petit, Yan Bo Ti

superspecial 主偏極付きアーベル曲面に基づく同種写像暗号方式への攻撃に関する論文である。同種写像暗号では、supersingular あるいは superspecial なアーベル多様体間の同種写像探索問題の計算困難性が安全性の根拠として用いられてきた。1 次元の場合には、四元数代数 $B_{p,\infty}$ における KLPT アルゴリズムが知られており、これは同種写像暗号の設計および解析において重要な役割を果たしてきた。しかし、2 次元の superspecial 主偏極付きアーベル曲面に対しては、同様の構成的手法は確立されていなかった。

Ibukiyama、Katsura、Oort によれば、有限体 $\mathbb{F}_p$ 上の全ての主偏極付き superspecial アーベル曲面は、四元数代

数 $B_{p,\infty}$ の元を成分とする特定の 2×2 行列 g によって表現できることが知られている。本研究では、このような 2 つの行列 g_1, g_2 が与えられたとき、対応するアーベル曲面間の滑らかな次数を持つ偏極付き同種写像を表す「接続行列」を発見するための、ヒューリスティックな多項式時間アルゴリズムを提示された。提案手法は、Kohel、Lauter、Petit、Tignol による 2014 年の KLPT アルゴリズム（四元数代数 $B_{p,\infty}$ における 2 つの極大整環の間で滑らかなノルムを持つ接続イデアルを見つける手法）の 2 次元版と位置付けられる。KLPT アルゴリズムは、同種写像暗号において汎用的な道具として用いられてきたが、本研究の類似アルゴリズムも同様の応用を持つことが示されている。

主結果の応用として著者らは、構成的 Deuring 対応の 2 次元版が多項式時間で解けることを証明した。加えて、もっともらしい仮定の下で、superspecial 主偏極付きアーベル曲面から構成される Charles–Goren–Lauter 型ハッシュ関数において、初期曲面に対応する行列が既知である場合には、多項式時間で衝突が構成可能であることが示された。この結果から著者らは、当該ハッシュ関数は trusted setup を必要とすることを指摘している。また、偏極付き同種写像を滑らかな次数から接続行列へ多項式時間で変換する手法も提示されている。これは従来の Chu による手法では超多項式時間（準指数時間）を要していた処理であった。

Error Floor Prediction with Markov Models for QC-MDPC Codes

Sarah Arpin, Jun Bo Lau, Antoine Mesnard, Ray A. Perlner, Angela Robinson, Jean-Pierre Tillich, Valentin Vasseur

構造を持つ符号ベース KEM の安全性解析と NIST PQC 耐量子計算機暗号プロジェクト第 4 ラウンド候補 BIKE に関する論文である。符号ベース KEM の復号時には $\mathbb{F}_2$ 上のシンドローム復号問題 $\boldsymbol{s}' = H\boldsymbol{e}, |\boldsymbol{e}| = t$ を解き、エラーベクトル $\boldsymbol{e}'$ を復元する必要があるが、復号化アルゴリズムの挙動により僅かながら復号化エラーが発生する。論文内では復号化アルゴリズムの出力 $\boldsymbol{e}'$ が $\boldsymbol{s}' \neq H\boldsymbol{e}'$ もしくは $\boldsymbol{e} \neq \boldsymbol{e}'$ となる状況として定式化されている。失敗した復号結果を用いることで鍵復元が可能であることが知られている [Guo-Johansson-Stankovski, Asiacrypt 2016] ため、復号失敗確率（DFR: decoding failure rate）を正確に見積もることは符号ベース暗号方式の安全性評価において重要な意味を持つ。

DFR と符号のブロック長に関する既知の性質として、DFR が r に関して急激に低下する waterfall と呼ばれる領域（ブロック長 r が小さい範囲を主に指す）と、DFR の低下が緩やかになる error floor と呼ばれる領域（r が大きい範囲を指す）があることが知られている。[Sendrier-Valentin, PQCrypto2019] によるマルコフモデルを用いた解析では waterfall 領域の挙動は予測できていたものの、暗号で用いられる error floor 領域の挙動を説明できてはいなかった。waterfall 領域の挙動から外挿した DFR は実際のものよりも小さく見積もられていると考えられており、そこから逆算されたパラメータは十分な安全性を持たない可能性がある。

本論文では、error floor 領域の挙動を説明するモデルを与え、数値的な解析手法と暗号への応用を与えている。技術的には step-by-step decoder と呼ばれる、初期エラーベクトル $\boldsymbol{e}$ からスタートし、シンドローム $\boldsymbol{s} = H\boldsymbol{e}$ が減り続ける方向に $\boldsymbol{e}$ の各ビットを反転させ $|\boldsymbol{e}| = t$ を満たすエラーベクトルを探索するアルゴリズムを仮定し、2 種類のマルコフモデルを用いて解析を行う。一つ目は simplified model と呼ばれるもので、アルゴリズムの各ステップにおいて、$\boldsymbol{e}$ からある一つのランダムに選んだ近接符号語との距離を反映したモデル 1 と、さらに単純化して近接符号語を無視したモデル 2 から導かれる DFR の線形結合として全体の DFR 値を予測する。この単純化したモデルが error floor 領域の挙動を説明し、さらにこの領域でエラーが起きたときに出力される $\boldsymbol{e}$ は近接符号語とのハミング距離が小さいという経験則も説明している。

次に、refined model としてアルゴリズムの各ステップにおいて全ての近接符号語を考慮するモデルを提案し、より正確な DFR の予測が可能であることを示している。特に、simplified model では捉えられていなかった鍵ごとの

DFR の違いが正確に予測されている。これは、符号ベース暗号の中に DFR が大きくなる弱鍵が含まれているという経験則を理論的に説明したものとなる。

応用として、符号ベース KEM BIKE の再解析を行い、仕様書内の BIKE 1 パラメータの DFR が $2^{-91.7}$ 程度でありセキュリティパラメータの逆数よりも大きいため所望の安全性を満たしていない可能性があることを指摘している。また、提案パラメータと同等の DFR$2^{-131.2}$ を実現するためにはブロックサイズ（鍵長）を 10% 程度伸ばす必要があると結論付けている。

Assessing the Impact of a Variant of MATZOV's Dual Attack on Kyber

Kévin Carrier, Charles Meyer-Hilfiger, Yixin Shen, Jean-Pierre Tillich

NIST 標準方式である CRYSTALS–Kyber(ML–KEM) に関する解析論文である。

本論文が取り上げている MATZOV レポートは、2022 年に IDF（イスラエル国防軍）の Center of Encryption and Information Security から出版された Dual attack を用いた LWE 問題の計算量に関する報告である。Dual attack は判定版 LWE 問題のインスタンス (A, b) から導かれる SIS 問題の解 $\boldsymbol{w}$ と $\boldsymbol{b}$ の内積を取ることでインスタンスが正当かどうかを判定する。

レポート内では Dual attack に対して guessing の効率化と modulus switching による探索空間の削減による改良が行われている。guessing は n 次元秘密ベクトルの分割 $\boldsymbol{s} = (\boldsymbol{s}_1 || \boldsymbol{s}_2)$ の後半部分から $n-k$ 次元の LWE 問題を構成し、対応する SIS 問題の解 $\boldsymbol{w}_2$ に対して内積 $\langle \boldsymbol{w}_2, \boldsymbol{b} - A_1 \boldsymbol{s}_1 \rangle$ が小さくなるような $\boldsymbol{s}_1$ を総当たりで探索していく方法で、q が小さい場合には効果を発揮する。総当たり時の内積計算を高速フーリエ変換を用いて効率化することで計算量を下げられると主張されていた。MATZOV レポートでは Kyber, Dilithium, Saber の提案パラメータに対して再評価が行われ、特に Kyber の解読計算量に関して仕様書内で主張された値よりも 10 から 20 ビット程度低下し、NIST PQC での要求レベルを下回ると報告されていた。

その後、[Ducas-Pulles, CRYPTO 2023] によりレポート内の解析で仮定されている、正しい $\boldsymbol{s}_1$ を発見するためのスコア関数の評価に用いられたフーリエ変換後の成分の独立性仮定が Gaussian Heuristic を始めとする広く検証されたランダム格子上の仮定と矛盾することが指摘され、解析結果の妥当性に疑問が持たれていた。

本論文では、スコア関数の評価手法を変更することで独立性仮定を用いずに解析が可能なアルゴリズムを提案し、さらに modulus switching の一般化により解読計算量を下げている。結果として、Kyber-512/768/1024 の解読計算量が NIST PQC 標準化で要求されていた計算量をそれぞれ 3.5/11.9/12.3 ビット下回ると評価しており、Kyber の安全性が基準よりも下であるという MATZOV レポートの主張は覆ってはいないことが確認できたとしている。

技術的には、modulus switching が mod q 空間から mod p 空間への圧縮を行うことで探索範囲を削減するという方針を一般化し、線形符号を用いて $\mathbb{Z}_q^n$ から $\mathbb{Z}_q^k$ への圧縮を行う lossy source encoding による次元削減 [Carrier et al. Eurocrypt 2024] を提案している。論文内では具体的な線形符号として、復号処理が高速な polar code を用いている。また、スコア関数の解析における独立性仮定の問題を回避するため、Poisson の総和公式による表現に書き換える事で双対格子の中のベクトルの長さをもとに LWE のランダム性を判定可能な枠組みを構築している。

Improved Attacks for SNOVA by Exploiting Stability Under a Group Action

Daniel Cabarcas, Peigen Li, Javier A. Verbel, Ricardo Villanueva-Polanco

NIST PQC 標準化プロジェクト追加署名第 2 ラウンド候補である多変数多項式署名 SNOVA の攻撃に関する論文である。

SNOVA の鍵復元困難性、署名の偽造困難性は処理の効率化のために構造化された多変数 2 次方程式 (SNOVA system) の求解困難性に依存している。本論文では、SNOVA System から構築される $F_q[x_1, \ldots, x_{ln}]$ の斉次 2 次多項式の集合からからなるイデアル (SNOVA ideal) を考え、それが特定の可換行列のなす群の作用により安定であるという事実を用いた新たな求解アルゴリズムを構成している。

多変数多項式署名への攻撃アルゴリズムの一つである reconcilation attack による鍵復元では、公開鍵行列 $A = (a_1, \ldots, a_n)$ から中心写像 F を変換する線形写像 T を復元するため、$\{T^{-1}(a_1, \ldots, a_n)^T : a_1 = \cdots = a_\ell = 0\}$ の形式の空間 $\mathcal{O}$ を考え、その中の一つの成分を復元することで代理鍵を復元することが目的となる。このとき、イデアルが群作用により安定であるという性質を用いて変数変換を行うことで、SNOVA system を multi-homogeneous と呼ばれる方程式系へと変換可能である。論文では変換された multi-homogeneous 系の性質が調べられ、XL-like なアルゴリズムを用いることで先行研究よりも高速に方程式が解けることが示されている。理論的解析により reconcilation attack が先行研究 [Ikematsu-Akiyama, APKC2024][Li-Ding, PQCrypto2024] と比較し 2 から 2^{20} 倍程度高速化可能であることが示され、実験的に検証されている。また、本論文では同様の手法を用いて、[Bullens, Eurocrypt2025] による署名の偽造攻撃の改良が可能であることが示されている。

A Complete Security Proof of SQIsign

Marius A. Aardal, Andrea Basso, Luca De Feo, Sikhar Patranabis, Benjamin Wesolowski

NIST PQC 標準化プロジェクト追加署名第 2 ラウンド候補である同種写像ベース署名 SQISign の安全性証明に関する論文である。超特異楕円曲線上の自己準同型環の計算問題の困難性に関する結果を含む。

SQISign およびその変種は、基礎となる Σ プロトコルからの Fiat-Shamir 変換により構成されている。通常、Fiat-Shamir 変換により構成された署名方式において、署名の偽造不可能性はベースとなる Σ プロトコルが special-soundness(SS) や (weak)HVZK であることから保証される。

Fiat-Shamir 変換により構成された署名が特定の安全性を満たすための。Σ プロトコルが持つべき条件を特定の計算問題の困難性に基づいて構成する場合には証明の構成や効率化の側面から、SS や HVZK などの条件を少し変えつつ安全性証明を行うことがデファクトスタンダードであった。著者らは先行研究において、Σ プロトコルの SS が、SQISign が安全性の根拠とする超特異曲線上の自己準同型環上の関係 (relation)R_{SQI} と対応していないこと、EUF-CMA 安全性証明における Σ プロトコルの (weak)HVZK シミュレーターの構成が知られていないことから、安全性証明に穴があることを指摘している。

本論文では Fiat-Shamir with hints と名付けられた新たな変換フレームワークを導入し、EUF-CMA 安全性を示す際にシミュレーターに特定の分布から出力されたヒントを与えることで weak HVZK 性を与えている。著者らは構成した署名が ROM の下で EUF-CMA 安全となるための Σ プロトコルが満たすべき条件とその証明を与えている。続いて、SQISign の仕様書内で用いられている Σ プロトコルを微修正した Σ_{SQI} が必要な条件を満たしていることを確認し、ヒント付き OneEnd 問題の困難性のもとでの偽造困難性を示した。

ここで、ヒント付き OneEnd 問題は与えられた超特異楕円曲線と、Σ プロトコルのレスポンスに対応する同種写像と補助情報のセットからなるヒント分布からサンプリングされたヒントを用いて超特異楕円曲線上の非自明な自己準同型を一つ求める問題であり、論文内では同様の条件下で自己準同型環（の効率的な表現）を求める問題であるヒント付き EndRing 問題への帰着が示されている。続けて、ヒント付き EndRing 問題の自己ランダム帰着性、ヒントの確率分布からの多項式時間サンプリングを具体的に示すことで、署名の ROM のもとでの EUF-CMA 安全性が EndRing 問題へと帰着されたことになる。

On Deniable Authentication against Malicious Verifiers

Rune Fiedler, Roman Langrehr

鍵同意アルゴリズム Signal に関係する、否認可能認証（deniable authentication）への攻撃に関する論文である。否認可能認証は、Alice が Bob に対して認証を行いながらも、第三者に対してその事実を否認できることを目的とする暗号技術であり、Signal や off-the-record（OTR）メッセージングにおいて明示的に要求されている否認可能鍵交換の基盤技術として重要である。この文脈では、Bob 自身が悪意を持つ可能性を排除できず、検証者が攻撃者となる状況を考慮した安全性定義が必要とされてきた。これまで提案されてきた多くのプロトコルは、Extended Knowledge of Diffie–Hellman（EKDH）仮定に基づき、悪意ある検証者に対する否認可能性を主張していた。

本論文では、否認可能認証を実現するために広く用いられている暗号プリミティブである指定検証者署名（Designated Verifier Signatures、DVS）に焦点を当てる。DVS に対して著者らは、「悪意ある検証者に対する否認可能性」という新たな安全性を導入し。ランダムオラクル（RO）モデルにおいてこの定義を満たす構成を与えている。その一方、標準モデルにおいては、具体的な攻撃の提示により、当該定義が達成不可能であることが著者らにより示された。また、著者らにより、EKDH 仮定が成立しないことが示され、これに依拠していた X3DH や PQXDH などの既存プロトコルが、悪意ある検証者に対する否認可能性を達成していないことが明確化された。

Wagner's Algorithm Provably Runs in Subexponential Time for SIS$^\infty$

Léo Ducas, Lynn Engelberts, Johanna Loyer

格子暗号の安全性の根拠となる SIS$^\infty$ 問題に関する解析と、NIST 標準署名方式である CRYSTALS-Dilithium (ML-DSA) の安全性への影響を議論した論文である。

SIS 問題はパラメータ n, m, q, β により定義され、ランダムに与えられた行列 $A \in \mathbb{Z}_q^{n \times m}$ に対して、$A\boldsymbol{x} \equiv \mathbf{0} \pmod{q}$ かつ $\|\boldsymbol{x}\| \leq \beta$ を満たす非ゼロベクトル $\boldsymbol{x} \in \mathbb{Z}^m$ を探索する問題である。通常、$\boldsymbol{x}$ のノルムは ℓ_2-ノルムで測られるが、ℓ_∞ ノルムとしたものは SIS$^\infty$-問題と呼ばれる。

本論文では、パラメータ $\beta = q/\mathrm{polylog}(n), m = n + \omega(n/\mathrm{loglog}n)$ を持つ SIS$^\infty$ 問題に対して、準指数となる $\exp(O(n/\mathrm{loglog}n))$ 時間のアルゴリズムを与えている。また、ℓ_2-ノルム SIS 問題の変種である ISIS 問題、SIS$^\times$ 問題に対してもパラメータ $\beta = \sqrt{n} \cdot q/\mathrm{polylog(n)}$ に対して準指数時間アルゴリズムを与えている。

CRYSTALS-Dilithium の署名偽造の安全性が SIS$^\infty$ 問題に基づいていることから、本論文の結果がどのようにセキュリティに影響するかが議論されている。楽観的なヒューリスティックに基づいた計算量評価を用いても Dilithium のセキュリティカテゴリ 2,3,5 のパラメータに対して $\log_2$ 計算量がそれぞれ 269.9, 343.0, 450.2 と見積もられ、安全性への影響は無いとしている。解析スクリプトは `https://github.com/lducas/Provable-Wagner-SIS` で与えられている。

背景として、LWE 問題を解くアルゴリズムである BKW アルゴリズムの研究がある。近年の研究では、ノイズが狭い範囲から取られた LWE に対しては BKW アルゴリズムの Fine-tuning により準指数時間アルゴリズムが得られているものの、必要なサンプル数の下界について議論があった。本論文では、ノイズを狭い範囲に制限した LWE 問題が SIS$^\infty$ 問題の双対形と見做せること、および BKW アルゴリズムが双対格子上での Wagner アルゴリズムと [Aharonov-Regev, J. ACM 2005] の識別器の組み合わせと見做せるという観察を起点に、Wagner アルゴリズムをベースとしたガウシアンサンプラーおよびそれを用いた SIS$^\infty$ 問題の計算アルゴリズムを与えている。計算時間が準指数時間であることをヒューリスティック無しに証明している点も特徴である。

技術的には Wagner アルゴリズムの部分格子列 $\mathbb{Z}^{m-n} \supset \cdots \supset L_1 \supset L = \Lambda_q^{\perp}(A)$ を考え、左から順に和が $\mathbf{0}$ となるベクトルの集合をサンプリング、マージすることで最終的に L の短いベクトルを求めるという骨格の部分は変わっていない。リスト内のベクトルが離散ガウス分布となる形にアルゴリズムを改良することで、q-ary 格子上の離散ガウス分布サンプリングアルゴリズムを与え、その出力の確率分布を解析する事で SIS^{∞} 問題、ISIS 問題、$\mathrm{SIS}^{\times}$ 問題の解が出力される確率の解析と時間計算量を与えている。

How to Prove False Statements: Practical Attacks on Fiat-Shamir

Dmitry Khovratovich, Ron Rothblum, Lev Soukhanov

Fiat–Shamir 変換に基づく簡潔証明系（Succinct proof system）への攻撃に関する論文である。Fiat–Shamir 変換は、SNARK を含む多くの非対話型証明系の構成において中核的役割を果たしている。特に、ハッシュ関数が完全なランダム関数としてモデル化されている場合、すなわちランダムオラクルモデルでは、健全性が証明されている。一方具体的なハッシュ関数では、変換が健全でなくなるプロトコルの例が存在する。しかしこれまで知られていたそのような例は、すべて意図的に失敗するよう設計された作為的なプロトコルに限られていた。

本論文では、GKR プロトコルに基づく対話型簡潔証明系に対して、任意の Fiat–Shamir ハッシュ関数の選択においても、非対話化後に適応的健全性が成立しないことが示された。具体的には、偽の命題に対して受理される証明を生成可能な明示的回路が構成され、さらに任意の回路 C と任意の出力 y に対して、機能的に等価な回路 C^* を構成することで、C^* が y を出力するという受理される証明が生成可能であることが示された。この結果により、仮に安全性保証が存在するとしても、それは回路の機能ではなく、具体的な実装に依存することが示された。また、非適応的健全性を破る攻撃の変種も提示されたが、これらは回路深さが非常に大きい場合や、追加的な暗号仮定を置く場合に限られることが示された。またプロトコルの非適応的健全性（non-adaptive soundness）を破る攻撃の変種も示されている。ただしこれは基礎となる暗号オブジェクトから独立した攻撃用回路を生成することから、攻撃回路の深さが非常に大きくなるため実用性が低いか、あるいは基礎となる暗号プリミティブについていくつかの追加の仮定を必要とする。

A Plausible Attack on the Adaptive Security of Threshold Schnorr Signatures

Elizabeth Crites, Alistair Stewart

しきい値署名方式（threshold signature schemes）に対する適応的安全性への攻撃に関する論文である。しきい値署名方式は、秘密鍵を複数の参加者に分散し、一定数以上の参加者が協調した場合にのみ署名が生成可能となる仕組みであり、ブロックチェーンおよび分散システムにおいて重要な役割を果たしている。従来は、悪意ある参加者（corrupt party）集合が事前に固定される静的な安全性（static security）が主に検討されてきた。しかし標準化や実運用を見据え、プロトコル実行中に参加者が悪意ある参加者に変化するケースを取り扱う、適応的安全性（adaptive security）の重要性も高まっている。特にしきい値を t としたとき、最大 $t-1$ 人の参加者が悪意あるものに変化するケースを許すものを完全適応的安全性（full adaptive security）と呼ぶ。

本論文では、公開鍵分散値が $pk_i = g^{sk_i}$ の形を持ち、秘密鍵 sk_i がある多項式上に配置されているしきい値 Schnorr 署名方式に対して、完全適応的安全性を破るもっともらしい攻撃（plausible attack）が存在することが示された。結果、しきい値 Schnorr 署名方式の中でも、FROST、FROST2、FROST3、SimpleTSig、Sparkle、Sparkle、Lindell'22、Classic S、ROAST、SPRINT、HARTS、GJKR、Stinson-Strobl、Arctic、GKMN については、追加の修正を行うか、あるいは本論文の Definition 1. で定義された探索問題のインスタンスの困難性を仮定しない限り、完全適応的安全性を証明できないことが示された。さらに、$t-1$ 未満の適応的腐敗に対しても研究されている。

Uncompressing Dilithium's Public Key

Paco Azevedo Oliveira, Andersson Calle Viera, Benoît Cogliati, Louis Goubin

NIST 標準署名方式である CRYSTALS-Dilithium (ML-DSA) に関する解析論文である。

Dilithium は Fiat-Shamir with aborts フレームワークに基づく署名方式であり、秘密情報 s とそのハッシュ値 t がそれぞれ秘密鍵、公開鍵の一部として用いられる。Dilithium がひな形とする格子署名ではランダムに生成された行列 A に対して短いベクトル $\boldsymbol{s}_0, \boldsymbol{s}_1$ を秘密鍵、$\boldsymbol{t} = A\boldsymbol{s}_0 + \boldsymbol{s}_1$ を公開鍵として処理が行われる。実際の Dilithium では公開鍵サイズを圧縮するため、$\boldsymbol{t}$ を上位ビット $\boldsymbol{t}_1$ と下位ビット $\boldsymbol{t}_0$ に分割し、$\boldsymbol{t}_1$ のみを公開、$\boldsymbol{t}_0$ は秘密鍵の一部とされている。

本論文では、正当な署名を集めることで $\boldsymbol{t}_0$ が実時間で復元可能であるとしている。Dilithium のセキュリティレベル 2,3,5 のパラメータに対して、署名数 18 万から 52 万の攻撃により、標準的なデスクトップコンピュータを用いてそれぞれ約 1 時間、1 時間半、3 時間 20 分で復元可能であると報告している。

研究背景として、Dilithium の解析における $\boldsymbol{t}_0$ の扱いの曖昧さが挙げられている。理論的な安全性証明では $\boldsymbol{t}$ が攻撃者から既知であると仮定され $\boldsymbol{t}_0$ が公開情報であると扱われているものの、サイドチャネル攻撃の文脈においては $\boldsymbol{t}_0$ を既知とするか未知とするかは文献ごとに差があった。著者らは、本研究の結果は Dilithium の安全性を脅かすものではないが、今後は $\boldsymbol{t}_0$ が既知情報であると考えて安全性評価を行うことが妥当であると結論付けている。

技術的には正規の署名 $\sigma = (\tilde{c}, \boldsymbol{z}, \boldsymbol{h})$ から $\boldsymbol{t}_1$ が満たすべき線形不等式を構成、それらを LP ソルバーを用いて解が一意に定まるまで逐次的に署名を追加しながら解いている。このとき、一つの署名から $256 \cdot k$ 個の不等式が得られる（$k \in \{4, 5, 6\}$ は Module 格子の階数、仕様書内で規定）ため、これらを全て用いると問題のサイズが巨大になりソルバーで解くことが困難になる。そのため、不等式が役に立ちそうかどうかを判断する手法を提案し、不等式の本数をほぼ署名数と同等まで抑えている。

Key Recovery from Side-Channel Power Analysis Attacks on Non-SIMD HQC Decryption

Nathan Maillet, Cyrius Nugier, Vincent Migliore, Jean-Christophe Deneuville

NIST 耐量子計算機暗号標準化プロジェクト選定候補である符号ベース暗号 HQC のサイドチャネル攻撃に関する論文である。

これまで HQC のサイドチャネル攻撃に関する論文の多くが、標準化プロジェクトに提出されたリファレンス実装を対象としていた一方で、本論文は同プロジェクトに同時に提出された、性能指標のベンチマークとなる最適化実装をターゲットとしている。ただし最適化実装は x86-64 の SIMD 命令を用いており、移植可能性が低いことから第 4 ラウンド提出版の HQC パッケージに含まれる最適化実装を SIMD 命令を使わないコードに変更し、2 種類の鍵復元攻撃を扱っている。

HQC の暗号化はリード・ソロモン（RS）符号を外符号、リード・マラー（RM）符号を内符号とした連接符号により行われる。正規の秘密鍵 $\boldsymbol{y}$ と暗号文 $(\boldsymbol{u}, \boldsymbol{v})$ から語 $\boldsymbol{v} - \boldsymbol{u} \cdot \boldsymbol{v}$ を計算した後、$RM(1, 8)$ 復号器の中ではアダマール変換のための前処理として、$\boldsymbol{w}$ のデータを再配置するための `expand_and_sum` サブルーチンが複数回実行される。この部分の電力解析から $\boldsymbol{v} - \boldsymbol{u} \cdot \boldsymbol{v}$ の内容をビットごとに復元し、$(\boldsymbol{u}, \boldsymbol{v})$ の情報と組み合わせることで秘密鍵 $\boldsymbol{y}$ が復元可能であるとしている。ただし、復元の詳細はコンパイラが生成する `expand_and_sum` ルーチン内の命令とレジスタ操作により異なる。右シフト（SRL）命令の入出力レジスタが異なる場合の挙動から復元するバージョン（V0）と、同一レジスタ内でのシフトの場合でも続く AND 命令の挙動から復元するバージョン（V1）が提案されている。

攻撃者が復号デバイスに対して同じ入力の復号を複数回実行可能であるという仮定のもとに、この攻撃の性能が評価された。ARM Cortex-M4 を用いた実験では著者らは 83 回の復号から得られた電力解析により、99% の確率で鍵復元が可能であると結論付けている。実験では 65536 回の電力波形を取得するのに 34 分かかり、83 回分の波形取得には 2.5 秒しかかからないとしている。

著者らは対策として、RM 符号の復号アルゴリズムを最小距離復号アルゴリズムに変更し `expand_and_sum` ルーチンを用いないようにすること、復号アルゴリズムへの入力である $\boldsymbol{v} - \boldsymbol{u} \cdot \boldsymbol{v}$ にノイズを乗せること、適当な平文 m' を用いて $\boldsymbol{v} - \boldsymbol{u} \cdot \boldsymbol{v} + m'G$ を入力とすることの 3 点を挙げ、復号の性能低下を議論している。

Finding and Protecting the Weakest Link: On Side-Channel Attacks on y in Masked ML-DSA

Julius Hermelink, Kai-Chun Ning, Richard Petri

NIST 標準署名方式である ML-DSA に対するサイドチャネル攻撃の論文である。

ML-DSA は Fiat-Shamir with aborts フレームワークに基づく署名方式であり、その署名 (z, c) は文書 μ から生成される c と、秘密鍵の一部分 $\boldsymbol{s}_1$、マスク用乱数 y から $z \leftarrow y + \boldsymbol{cs}_1$ により計算される。本論文が対象としているのはサイドチャネル情報からの y の復元であり、ここから $z - y = \boldsymbol{cs}_1$ を通じて秘密鍵 $\boldsymbol{s}_1$ を復元する鍵復元攻撃の中核となる。

近年では ML-DSA のマスク付き実装が数多く提案されているものの、マスキングされていない実装と比較してどの程度安全性が向上しているのかが不明瞭であることを研究の背景としている。本論文では、[Coron et al., TCHES 2023] で用いられたマスキング実装を取り上げ、その中で $\boldsymbol{y}$ に関する処理が行われる部分をモデル化している。署名生成アルゴリズムの中での $\boldsymbol{y}$ に関する部分はマスキング実装の場合 3 段階に別れており、Boolean masking による $\boldsymbol{y}$ のサンプリング、Boolean masking から arithmetic masking への変換（B2A）、arithmetic masking による $\boldsymbol{cs}_1$ の計算部分からなる。Boolean と Arithmetic どちらか一方のマスキングのみを用いて処理する方法は知られておらず、特に arithmetic masking の下でサンプリングを行う行う方法が未知であるとしている。

上記のマスキング実装に対してサイドチャネル情報に乗るノイズの大きさと $x = \boldsymbol{cs}_1$ と攻撃者の得るマスキングのシェアに関する確率変数との相互情報量をシミュレーションを行い、Boolean masking での処理における情報漏洩が arithmetic masking よりもはるかに大きいことが確認された。続いて、LWE ベース暗号のサイドチャネル情報から得られたヒントから秘密鍵を復元するソルバー [Hermelink et al., Eurocrypt 2025] を用いて first-order leakage（$\boldsymbol{y}$ の部分情報が直接漏洩）および second-order leakage（$\boldsymbol{y}$ のシェアに関する情報が漏洩）の両モデルにおいて、ノイズと復元に必要な署名数の関係がシミュレーションされた。サイドチャネル情報に多くのノイズが乗る場合でも、現実的な時間で秘密情報が復元されることを確認している。

物理的な実験として、[Coron et al., ePrint 2024/1149] による first order マスキング実装を Cortex-M3 および M4 上で実行し、実験用ボードから取得した電力波形からの $\boldsymbol{s}_1$ の復元を行っている。実験はこれまでの理論から判明した、Boolean masking での処理部分がより多くの情報を漏洩するという事実に基づき、$\boldsymbol{y}$ のサンプリングと B2A 変換処理をターゲットとしている。$\boldsymbol{y}$ の下位 8 ビット（first-order leakage）およびシェア（second-order leakage）をノイズ付きで取得し、それぞれ 300 個、700 個の署名から $\boldsymbol{s}_1$ の復元が可能であるとしている。

最後に、問題への対策として Boolean masking の部分を中心に行い、masking のオーダーを上げることを提案している。著者らの実験では、サンプリングと B2A の部分に対策を施した場合でも、処理に必要なクロック数は 3 割程度しか上がらないと報告している。

Crowhammer: Full Key Recovery Attack on Falcon with a Single Rowhammer Bit Flip

Calvin Abou Haidar, Quentin Payet, Mehdi Tibouchi

NIST 標準署名方式である FALCON (FN-DSA) のサイドチャネル攻撃に関する論文である。

Rowhammer 攻撃は DRAM の特定の領域に継続的な負荷をかけることでメモリ内の隣接するセルのビット反転を引き起こす故障注入攻撃の一種である。

FALCON は Hash-and-Sign パラダイムに基づく署名方式であり、平文のハッシュ値からなるベクトル $\boldsymbol{c}$ の原像、つまり $\boldsymbol{t}B = \boldsymbol{c}$ を満たす短いベクトル $\boldsymbol{t}$ から署名を生成する。この原像生成に用いられる PreimageSampling アルゴリズムを高速化するため、FALCON では剰余環 $\mathbb{Z}[x]/(x^n+1)$ の分解と Fast Fourier Sampling と呼ばれる高速フーリエ変換と同様のアイディアを用いた高次元格子離散ガウス分布からの高速サンプリングを行う。署名生成関数の中で用いられるサブルーチンとして、中心を t とした大きさ σ の 1 次元離散ガウス分布を出力する $Sampler_{\mathbb{Z}}(\sigma, t)$ があり、その部品として用いられる、中心 0、大きさ σ の離散ガウス分布を非負領域に制限した分布からサンプリングを行う BaseSampler 関数が本論文の攻撃対象である。

FALCON のオフィシャル実装では、サイドチャネル対策で BaseSampler 関数の実装にハードコーディングされた累積分布関数のテーブル（reverse cumulative distribution table; RCDT）が用いられており、このテーブルの一部を Rowhammer 攻撃でビット反転させることにより以降の署名の確率分布が歪んだものとなる。歪んだ署名からの署名鍵の復元は hidden transformation problem[Lin et al., PKC 2024] として定式化されており、機械学習と同様の勾配降下法を用いた鍵復元 [Nguyen-Regev, JoC 2009] が可能である。

攻撃の成功率を上げる技術的な改良として、出力された署名ベクトルの主成分分析によりトラップドアを構成する基底の Gram-Schmidt 基底ベクトルの相関行列の固有値を求め、その情報から Gram-Schdmit 基底の一部分を復元するアプローチを取る。PCA の次元を増やすことで必要な署名数が下がる。

攻撃実験は FALCON のオフィシャル実装内のテーブルを手動でビット反転し出力した署名を用いて行われた。1 ビットと 8 ビット反転の場合が検討され、復元の容易さはビット反転の数と位置に大きく依存し、例えば最も影響の大きな 1 ビットの反転を狙って起こすことが可能であった場合には 2 億個の署名で 70% の鍵復元成功率であるとしている。

Rowhammer 攻撃自体への対策であるハードウェアのプロテクトの他に、テーブルの整合性をハッシュ関数等を用いて逐一チェックすること、攻撃が行われた場合署名長の分布が理論よりも短くなるため、極端にノルムの小さい署名は出力しないなどの対策が提案されている。

Reducing the Number of Qubits in Quantum Factoring

Clémence Chevignard, Pierre-Alain Fouque, André Schrottenloher

素因数分解問題および離散対数問題を計算する量子回路についての論文である。

近年の量子コンピュータの性能進化にともない、Shor のアルゴリズムを用いた素因数分解が実際に行われる実現可能性が高まりつつある。暗号学的なサイズである数千ビットの素因数分解を行う量子回路の具体的な構成およびリソースの削減に関する研究は長年続けられてきたものの、分解対象の数 N に対して $n = \log_2 N$ が必要な論理量子ビット数の下限と考えられてきた。一方で、近年の研究 [May-Schlieper, ToSC 2022] によれば Shor の周期発見に用いられる $a^x \mod N$ や $g^x a^{-y} \mod N$ は必ずしも値を正確に計算する必要はなく、よりビット数の少ないハッシュ値の重ね合わせ $\sum_x |x\rangle|h(a^x \mod N)\rangle$ からも周期が復元可能であることが示唆されていた。本論文では、ハッシュ関数 h

として、入力の下位 $r = o(n)$ ビットを取得する関数を構成し、周期を復元するアルゴリズムを与える。

[Ekerå-Håstad, PQCrypto 2017] による離散対数問題の後処理の改良により、解 z の上限が知られている場合には $d = \log_2 z$ に対して QFT サイズが $d + o(d)$ 程度で十分であるという結果と組み合わせると、$n/2 + o(n)$ 論理量子ビット、$O(n^3)$ ゲート、深さ $O(n^2 \log n)$ の素因数分解回路が与えられる。

具体的な数値例として、RSA-2048 の素因数分解には 1730 論理量子ビットと 2^{36} の Toffoli ゲートで構成される量子回路を 40 回実行する必要があり、2048 ビットの有限体上で定義された解の大きさが 224 ビットの離散対数問題を解くためには 684 論理量子ビットと 2^{32} の Toffoli ゲートで構成される量子回路を 20 回実行する必要があると見積もられている。

技術的には離散対数問題に対応する関数 $g^x a^{-y} \mod N$ の下位 r ビットを Residue Number System (RNS) を用いて効率的に計算している。RNS は適当な素数列 $p_1, \ldots, p_\ell$ を固定した後、自然数 A を $(A \mod p_1, \ldots, A \mod p_\ell)$ の形で表現し演算を行うシステムであり、中国剰余定理から逆方向の計算も効率的に可能である。論文では $\mod p_i$, $\mod N$, $\mod 2^r$ の計算を組み合わせさらに近似計算を用いることで、入力 $(X, 0)$ から $(X, h(X))$ を高確率で計算する $O(\log n + m/log(n))$ 論理量子ビット、$O(nm^2)$ ゲートの量子回路を構成している。ただし、$n = \log_2 N$ かつ $m = \log_2 X$ とする。このとき、確率 ε で計算に失敗し $h(X)$ ではないランダムな値が出力されるが、その確率が小さくなるように注意深くパラメータが選ばれており、周期発見には影響としている。

A Quasi-polynomial Time Algorithm for the Extrapolated Dihedral Coset Problem over Power-of-Two Moduli

Shi Bai, Hansraj Jangir, Elena Kirshanova, Tran Ngo, William Youmans

格子暗号の安全性の根拠となる LWE 問題の量子計算量に関する論文である。

LWE 問題は耐量子性を持つと信じられてきたが、その具体的な量子計算量に関しては古典で知られているアルゴリズムを Grover 探索などで量子化したもの以外にはほとんど知られていない。

本論文の背景として、[Brakerski et. al., PKC2018] による LWE と Extrapolated Dihedral Coset Problem (EDCP) の量子多項式時間等価性が示されている。EDCP は、一様ランダムにサンプリングされた $\mathbf{x}_1, \ldots, \mathbf{x}_\ell \in \mathbb{Z}_q^n$ に対応する ℓ 個の量子状態 $\sum_{j \in \mathbb{Z}_q} \chi(j) |j\rangle |\mathbf{x}_i + j \cdot \mathbf{s}\rangle$ から $\mathbf{s}$ を復元する問題である。ここで χ は LWE 問題のノイズに対応する。ノイズが離散ガウス分布に設定された問題を G-ECDP、一様分布に設定された問題を U-ECDP と呼ぶ。

本論文では、q を 2 べきとしたときの、ECDP に対する準多項式時間 $O(2^{O(\log n \log q)})$ 量子アルゴリズムを構成し、それをベースに χ の出力が $M = q/c$ 種類のみであるという制限を付けた U-ECDP に対する量子多項式時間アルゴリズムを与える。また、ECDP の特殊形として $\chi(j)$ が非負かつ $\chi(j)$ の最小値がパラメータ $n, q = \mathrm{poly}(n)$ に関して無視できないほど大きな場合に量子多項式時間アルゴリズムが存在することを示している。

ECDP に対するアルゴリズムの拡張として、[Brakerski et. al., PKC2018] の S $|\mathrm{LWE}\rangle$ 問題に対する準多項式時間量子アルゴリズムを与えている。この問題は、$\sum_{e \in \mathbb{Z}_q} \chi(e) |\langle \mathbf{a}_i, \mathbf{s}\rangle + e \pmod q\rangle$ から $\boldsymbol{s}$ を復元する問題であり、ECDP の変種となる $\overline{\mathrm{ECDP}}$ 問題への帰着が示された。

技術的には [Regev, arXiv:quant-ph/0406151] で与えられた tensoring の手法を引き継いでおり、与えられたサンプルをフーリエ変換した後にそれらのテンソル積を合成、測定をすることで既知のベクトル $\boldsymbol{y}$ と $\boldsymbol{s}$ の内積（の $\mod 2^\ell$）が得られる。複数回の実行を行うことで、$\boldsymbol{s}$ を未知数とする線型方程式の形となり、古典計算により復元が可能となる。

本論文の結果はただちに LWE ベース暗号の危殆化につながるものではない。提案された準多項式時間量子アルゴリズムは準多項式個のサンプルを必要とするのに対し、既知の Brakerski et. al. による量子帰着で生成されるのは多項式個のサンプルのみであることが理由である。

Computing Asymptotic Bounds for Small Roots in Coppersmith's Method via Sumset Theory

Yansong Feng, Hengyi Luo, Qiyuan Chen, Abderrahmane Nitaj, Yanbin Pan

多変数剰余方程式の小さな解を求める Coppersmith 法の解析に関する論文であり、同種写像鍵共有方式である CSIDH および CSURF の安全性が議論されている。

暗号の文脈において Coppersmith 法は公開情報と秘密情報が満たす代数関係に着目し、剰余付き（連立）多変数方程式 $f(x_1, ..., x_n) \equiv 0 \pmod{N}$ を解く問題へと変換することで秘密情報を復元する手法である。特に、実装ミスやサイドチャネル情報等により、x_i の範囲が N と比べて指数的に小さい場合には $\log N$ の多項式時間の攻撃が構成可能な状況が多く知られている。

Coppersmith 法の概要は元の方程式 $f = 0$ から、適当な指数 m に対して $f \equiv 0 \pmod{N} \Rightarrow g_j \equiv 0 \pmod{N^m}$ を満たす多変数多項式 g_k を生成し、格子基底簡約により係数の小さい多項式 $h_1, h_2, \ldots$ を見つける。この h_k は係数が小さいことから、変数の絶対値が小さいときに関係 $h_k = 0 \iff h_k \equiv 0 \pmod{N^m}$ が成り立つ。実数上の多変数方程式 $h_k = 0$ はグレブナー基底計算などを通じてヒューリスティックに高速な解法が知られているため $\mathrm{mod} N$ の方程式を直接解くよりも高速となる。

Coppersmith 法の性能は多項式時間で計算可能な解の範囲の大きさにより評価されるが、それは生成される多項式 g_j の選択とそこから構成される格子の行列式の解析に依存する。近年の Coppersmith 法の応用では変数の数が多く、解きたい方程式の形が複雑であり正確な評価が難しいケースが多いという背景を踏まえ、[Meers-Nowakowski, Asiacrypt 2023] で提案されたヒューリスティックベースの解析手法を先行研究としている。

Coppersmith 法で用いられるヒューリスティックは、格子基底簡約で得られる多項式集合 $h_1, h_2, ...$ が代数的に独立であるという仮定が用いられるが、それに加え行列式の解析のために（適当な単項式の順序のもとでの）先頭多項式の係数の積に関する新たなヒューリスティックを導入している。本論文では、後者のヒューリスティックが成り立たない状況が存在することを指摘している。技術的には g_j の単項式の指数部分に対応する Newton polygon を考え、その体積計算を高速に行うツールを開発することで自動化している。先行研究を踏まえ、$m \to \infty$ の場合の漸近的な結果の計算を行っている。

応用として、同種写像鍵共有方式である CSIDH および CSURF の共有曲線の上位ビットが漏洩した状況を Coppersmith 法を用いて解析した上記 Meers-Nowakowski の Commutative Isogeny Hidden Number Problem の再評価を行い、曲線の復元に必要な MSB の量が従来の 1% 程度の削減ではあるが、多く取る必要があると報告している。

検証用のソースコードは `https://github.com/fffmath/AsymptoticBounds` で公開されている。

Sample Efficient Search to Decision for kLIN

Andrej Bogdanov, Alon Rosen, Kel Zin Tan

ノイズ付き連立方程式を解く計算問題である kLIN 問題の困難性に関する理論論文である。符号ベース暗号の解読計算量解析に関係する。

LPN(learning parity with noise) 問題はランダムに与えられた　mod 2 上のノイズ付き連立方程式であり、この問題および変種が符号の復号に現れるため古くから知られている。[Alekhnovich, FOCS2003] により提案された変種である kLIN 問題は方程式の各行に含まれる変数の個数を k 個に制限したものであり、元々は SAT に関わる計算問題の近似困難性を議論するために導入された。[Applebaum et al., STOC2010] による公開鍵暗号の構成に用いられて以降

方式の研究が進み、ここ数年では準同型暗号や MPC 等の構成に用いられている。

ノイズ付き線型方程式に関する計算問題では LWE(learning with errors) 問題のように探索版と判定版の 2 種類が自然に導入され、それらの等価性が議論されてきた。本論文では、$O(m)$ 個のサンプルから判定版 $(k-1)$LIN 問題を解く識別器を用いると、サンプル数 $O(nm)$ 個の探索版 kLIN 問題を解くことが可能であることが示されている。[Applebaum, SIAM J. Comput., 42] による先行研究では探索版に必要なサンプル数が $O(m^3)$ であったことと比較して必要なサンプル数と帰着の成功確率が大幅に改善されている。

技術的なコアとして、識別器から Approximate search と呼ばれる計算問題を通じて解く手法を提案している。これは、秘密ベクトルの成分 s_1 と s_j が等しいかどうかに関する情報を識別器を用いて取得し、そこから秘密ベクトルの近似 $\hat{\boldsymbol{s}}$ を復元、複数の近似から多数決により近似を精密化することで元のベクトルを復元する手法である。同様の手法は mod 2 ではなく有限体上の kLIN に対しても適用可能であり、同様の結果が得られている。

本論文では、kLIN 問題を [Goldreich, ECCC TR00-090] の一方向性関数と同様の文脈で議論している箇所があり、ノイズ付き連立方程式そのままの形ではなく関数 $P:\{\pm1\}^n \to \{\pm1\}$ $((z_1,\ldots,z_n)\mapsto z_1\cdots z_n\cdot e)$ の形で表現している。この表現手法により、ランダム線形関数を含んだ広大な範囲の関数に対して同様の探索問題から k を一つ減らした判定問題への帰着が示され、回路計算量理論への影響が議論された。

Highway to Hull: An Algorithm for Solving the General Matrix Code Equivalence Problem

Alain Couvreur, Christophe Levrat

NIST PQC 耐量子計算機暗号プロジェクト追加署名に提案された MEDS と ALTEQ に関わる。行列符号の等価性判定問題の困難性に関する解析論文である。

Matrix Code Equivalence(MCE) 問題は自然数 m,n,k,q をパラメータとし、$\mathbb{F}_q^{m\times n}$ の k 次元部分空間 $\mathcal{C},\mathcal{D}$ に対してそれぞれ m 次、n 次の可逆行列 P,Q で $\mathcal{D}=P\mathcal{C}Q^{-1}$ を満たすものを探索する計算問題として定式化される。先行研究として [Narayanan-Qiao-Tang, Eurocrypt 2024] による MEDS と ALTEQ への応用を含んだ MCE 問題の解析論文が存在するが、部分空間の次元 k が明記されていない。$k=m=n$ の場合は Cubic MCE(CMCE) 問題と呼ばれ、署名方式 MEDS の安全性に対応している。

本論文の解法は一般的な MCE 問題のインスタンス $\mathcal{C},\mathcal{D}$ の解のうち、行列 P を見つけることを目的としている。P が見つかれば残りの Q は線形代数的な計算により復元可能である。アルゴリズムは 2 段階に別れる。まず、$B=(P^{-1})^TAQ^T$ を満たす $(A,B)\in\mathcal{C}^\perp\times\mathcal{D}^\perp$ を見つける。そのような (A,B) が見つかったとすると、線形符号 $\mathcal{C}_A=\mathcal{C}A^\perp$ と $\mathcal{D}_B=\mathcal{D}B^\perp$ は $\mathcal{D}_B=P\mathcal{C}_AP^{-1}$ の関係を持つため、符号の共役計算問題を解くことで P が復元できることになる。

ただし、最初の (A,B) を発見する段階で方程式に P,Q が含まれるため自明な線形代数的手法を用いることができないため、行列符号 $\mathcal{C}_A$ の hull $h(\mathcal{C}_A)=\{M\in\mathcal{C}_A:\forall C\in\mathcal{C}_A, Tr(MC)=0\}$ を用いた方法が新たに提案されている。$h(\mathcal{C}_A)$ が 1 次元集合となるとき、ある行列 U が存在して生成元となるため、対応する特性多項式 χ を含めてリスト $[\chi,A,U]$ として保存する。同様に、$\mathcal{D}_B$ の hull で 1 次元になるものからリスト $[\chi,B,V]$ を生成し、2 つのリスト内から同じ χ を持つ組を探索する。このときの A,B が求める行列であり、さらにある行列 R に対して $V=RUR^{-1}$ となっているという事実を用いて行列 P を復元する。

アルゴリズムの計算コストは $\tilde{O}(q^{\max(k/2,k-m+2)})$ であり、暗号に用いられる cubic の場合では $k=m=n$ を代入して $\tilde{O}(q^{k/2})$ となるため Narayanan らの先行研究と同じ時間計算量となる。しかしながら、空間計算量は本論文の方が n^2 倍小さい点、パラメータ k,m,n が異なる場合を許す一般化した場合のアルゴリズムを与えたことに利点があると報告されている。

Refined Attack on LWE with Hints: Constructing Lattice via Gaussian Elimination

Jinzheng Cao, Haodong Jiang, Qingfeng Cheng

格子暗号の安全性の根拠となる LWE 問題の変種に関する新たなアルゴリズムの提案および解析論文である。NIST PQC 標準化プロジェクトで議論された代表的な格子暗号である CRYSTALS-Kyber (ML-KEM)、CRYSTALS-Dilithium(ML-DSA)、FALCON、NTRU に関して安全性への影響を議論している。

通常の LWE 問題はインスタンス $(A, \boldsymbol{b} = A\boldsymbol{s} + \boldsymbol{e})$ から $\boldsymbol{s}$ を探索する問題である。論文で取り上げられたヒント付き LWE 問題 [Dachman-Soled et al., CRYPTO 2020] は、格子暗号に対するサイドチャネル攻撃の文脈で登場した変種であり、$(A, \boldsymbol{b})$ の他に既知ベクトル $\boldsymbol{v}$ およびベクトルとの内積値 $\langle \boldsymbol{s}, \boldsymbol{v} \rangle$ に関する情報が与えられる。

LWE 問題に対する標準的な解析手法である、Primal lattice 上の最短ベクトル問題に変換する際にヒントの情報を上手く使うことで格子の次元が下がる、格子が疎になるなどの効果があり、攻撃の効率が上がることが先行研究により知られていた。本論文では、Primal attack における新たな格子の構成方法を提案し、どの程度のヒントが与えられれば暗号学的なサイズの LWE 問題が実時間で計算可能になるのかが議論されている。特に、CRYSTALS-Kyber512 に対しては 200 個の perfect hints もしくは 380 個の mod-q hints を用いることで数時間での攻撃が可能であり、これは先行研究 [Yu et al.] よりも有意にヒント数が少なく、高速であるとしている。

また、too many hints と呼ばれる、ヒントが多く与えられたときに Primal lattice の LLL 簡約基底の第一ベクトルが解となる現象が知られており、その境界となるヒント数を Kyber, NTRU, FALCON, Dilithium の各パラメータに対して実験的に求め、先行研究よりも 3 から 20 程度少ないヒントでも同様の現象が起きると報告している。

技術的にはヒントの与えられ方を Perfect hints, modular hints, mod-q hints, approximate hints として分類、それらを統合し primal attack での格子の構成を $\mathbb{Z}$-SIS 問題として定式化し、その出力を用いて (unique)-SVP のインスタンスを構成するという分割戦略に新規性がある。

Simple and General Counterexamples for Private-Coin Evasive LWE

Nico Döttling, Abhishek Jain, Giulio Malavolta, Surya Mathialagan, Vinod Vaikuntanathan

格子暗号の安全性の根拠となる LWE 問題の変種に関する解析論文である。

Evasive LWE 仮定 [Wee, Eurocrypt 2022] は判定版 LWE 型の 2 種類の識別問題 Pre と Post により定式化される計算量的仮定である。Pre と Post の違いは攻撃者が格子基底の Preimage を持つかどうかであり、前者が困難であるならば後者も困難であることを主張するのが Evasive LWE 仮定となる。この仮定を用いてこれまでに null-IO、ABE、SNARGs 等多くの方式が設計されてきたが、それぞれが用いる Evasive LWE 仮定には小さいながらも違いがあった。

本論文では、private-coin 型の Evasive LWE 仮定が知られている全ての設定で成り立たないことを反例を用いて証明している。しかしながら著者らは、仮定から構成される様々な暗号方式の安全性が直接破られたわけではなく、方式の安全性証明を再構成することは未解決問題としている。また、本論文の解析は LWE 問題のインスタンスから Preimage の情報を用いて秘密ベクトルを消去する zeroizing 攻撃の Evasive 版と見做すことができ、仮定の根本にある設計思想に疑問を投げかける結果であるとしている。将来的な方向性として、private-coin 型の Evasive LWE 仮定の理論を再構成する可能性を模索するか、public-coin 型を用いて方式を構成する道のどちらかがあるとしている。

本論文で取り上げる定式化は [Brzuska et al., Asiacrypt 2024] で与えられた以下の形式である。P, B を成分を $\mathbb{Z}_q$ から一様ランダムに取った行列、S, E, E' を指定された（離散ガウス分布のような小さい）確率分布からサンプリングされた行列とする。このとき、$(B, P, SB + E, SP + E', \mathrm{aux})$ と $(B, P, \$, \$, \mathrm{aux})$ が識別困難であるという条件を

pre-condition とする。ただし、aux は B, P を生成するための補助情報、$ はランダム要素とする。次に、$B^{-1}(P)$ を格子基底 B に対する P の Preimage、つまり $BD = P \mod q$ を満たす行列 D で各列のノルムが小さいものとするとき、$(B, P, SB + E, D, \text{aux})$ と $(B, P, \$, D, \text{aux})$ が識別困難であるという条件を post-condition とする。

Pre 試行を識別可能な攻撃者は同様のアルゴリズムを用いて Post 試行を識別可能であることが、Preimage $B^{-1}(P)$ を用いたインスタンスの変換により可能である。Evasive LWE 仮定は逆に、Post 試行を識別可能な攻撃者は Pre 試行を識別可能であることを主張する。このことは逆に、Pre 試行を識別できなければ Post 試行も識別できず、攻撃者から見ると Pre 試行における $SP + E'$ による LWE 識別のアドバンテージと、Preimage を得たときに追加で得られるアドバンテージの差が非常に小さいことを主張する。

Evasive LWE の定式化は行列 B, P および aux が攻撃者に知られているかどうかによりいくつかに分類される。攻撃者が aux を得るものが public-coin、得られないものが private-coin と呼ばれる。また、B, P が攻撃者から見えているものが Binding、完全に隠されているものが Hiding と名付けられているが、それぞれの行列の隠され方によりさらに細かく分類される。補助情報 aux の中に S や B の情報を埋め込むことで Post 試行の攻撃者にアドバンテージを与え、仮定を不成立とすることが可能であることが Brzuska らの先行研究により示されている。

本論文では、private-coin 型の Evasive LWE が B, P の公開度合いの強さに関わらず成立しないことを単純な反例から示している。まず著者らは、ランダムな P、離散ガウス分布からの S、$[0, q/2)$ から成分を一様ランダムにサンプリングした行列 T を用いて、$aux = SP - 2T$ として補助情報の中に秘密行列の情報を埋め込むことが可能であることを示す。B, P が攻撃者から完全に見える設定において、Pre 試行では攻撃者はランダム行列との識別が不可能であるが、Post 試行においては $C = SB + E$ と $C = \$$ を識別するため、Preimage$D = B^{-1}(P)$ を用いて $CD - \text{aux}$ を計算する。正規のインスタンスの場合には $CD - aux = (SB + E)D - (SP - 2T) = ED + 2T \mod q$ は高確率で整数 $ED + 2T$ と一致するため、さらに $\mod 2$ をとることで ED の最下位ビットが得られることになる。D は既知であるため、$W = ED$ のある行が D の各行の線形結合となっているかどうかを mod 2 の連立方程式を解くことで確認可能で、同時に E を復元することができる。B, P が攻撃者から見えない場合の攻撃と解析を行っており、同様に Pre は識別困難だが Post は識別可能であることを示している。

LWE with Quantum Amplitudes: Algorithm, Hardness, and Oblivious Sampling

Yilei Chen, Zihan Hu, Qipeng Liu, Han Luo, Yaxin Tu

格子暗号の安全性の根拠となる LWE 問題の量子版変種に関する困難性評価の論文である。

元々の論文は 2023 年に Cryptology ePrint Archive に投稿されたものであり、何度かの修正を経て CRYPTO 2025 に採録された。2024 年に注目を集めた第一著者の論文 Quantum Algorithms for Lattice Problems (ePrint 2024/555) では LWE 問題を効率的に解くと主張する量子アルゴリズムが提案されたものの、技術的な瑕疵があり現在に至るまで修正の目途は立っていない。しかしながら、量子振幅の位相が quadratic phase amplitude と呼ばれる特殊な形をしている量子版 LWE 問題を解くための直感を整理しなおすことで、以下の $S|LWE\rangle$ 問題、$C|LWE\rangle$ 問題に対する結果を得たと報告されている。

LWE 問題は量子コンピュータを用いても困難であると予想されているものの、その実際の量子困難性や量子多項式時間に落ちるパラメータの範囲は未知であり特に暗号方式に用いられる範囲と被るかどうかの研究が続けられてきた。[Chen et al., Eurocrypt 2022] により定義された $S|LWE\rangle$ 問題、$C|LWE\rangle$ 問題（それぞれ Solve, Construct を表す）は古典的な LWE 問題のエラーを量子振幅としてエンコーディングした計算問題である。$S|LWE\rangle$ 問題は $i = 1, \ldots, \ell$ に対する $\boldsymbol{a}_i$ と $\sum_{e_i \in \mathbb{Z}_q} f(e_i)|\langle \boldsymbol{a}_i, \boldsymbol{s} \rangle + e_i \mod q\rangle$ から $\boldsymbol{s}$ を復元する問題、$C|LWE\rangle$ 問題は $i = 1, \ldots, \ell$ に対する $\boldsymbol{a}_i$

から量子状態

$$\sum_{\boldsymbol{s}\in\mathbb{Z}_q^n}\bigotimes_{i=1}^{n}\left(\sum_{e_i\in\mathbb{Z}_q} f(e_i)|\boldsymbol{s}\cdot\boldsymbol{a}_i+e_i\rangle\right)$$

を構成する問題として定式化される。(正規化定数は省略)。問題の構成から、$S|LWE\rangle$ を入力状態を壊さずに解くアルゴリズムが存在すれば $C|LWE\rangle$ のソルバーとして用いることができる。

このとき、エラー e_i に対応してその量子振幅 $f(e_i)$ を与える関数の性質により問題の困難性が変化する。いくつかの形の量子振幅に対しては効率的な量子アルゴリズムが知られていたものの、古典的な LWE 問題に対応する離散ガウス分布の振幅を持つ問題設定の困難性に関しては未知であった。本論文では、量子振幅がガウス分布の $S|LWE\rangle$ 問題に対して、$\ell = 2^{\Theta(\sqrt{n\log q})}$ 個のサンプルを用いて準指数となる $2^{\Theta(\sqrt{n\log q})}$ 時間の量子アルゴリズムを与える。

次に、量子振幅の位相が $\exp(-\pi i\cdot\sum_j e_j^2/q_j^2)$ の形を持つ quadratic phase amplitude と呼ばれる問題設定において、$S|LWE\rangle$、$C|LWE\rangle$ に対する量子多項式時間アルゴリズムを与える。要求されるサンプル数は $\tilde{O}(n)$ である。応用として、[Debris-Alazard et al., STOC2024] により与えられた、$\boldsymbol{s}$ を知らずに LWE サンプルを出力するオブリビアス LWE サンプラーの、振幅の絶対値が離散ガウス分布となる $C|LWE\rangle$ オラクルからの構成を改良し、必要サンプル数を $\tilde{(}nr)$ から $\tilde{O}(n)$ に削減している。

また、格子上の離散ガウス分布の重ね合わせ状態を生成する $|DGS\rangle$ 問題から $S|LWE\rangle^{\mathrm{phase}}$ 問題への量子多項式時間帰着を与えている。この問題は $S|LWE\rangle$ 問題において位相を未知とした変種である。振幅のノルムを与える非負の実関数 f は固定されているが、その位相はサンプルごとに異なり、問題のパラメータとして指定された分布 D_θ からサンプリングされた $\boldsymbol{y}_i$ を用いてサンプルが以下のように生成される $\sum_{e_i\in\mathbb{Z}_q} f(e_i)\exp(2\pi i\cdot e_i\theta(\boldsymbol{y}_i))|\langle\boldsymbol{a}_i,\boldsymbol{s}\rangle+e_i \mod q\rangle$。[Regev, J. ACM 2009] による最悪時の GapSVP を通じた LWE から $|DGS\rangle$ への量子帰着と合わせると、$S|LWE\rangle^{\mathrm{phase}}$ 問題の困難性が古典的な LWE から言えることになる。

以上の結果から、量子振幅が既知である場合には準指数時間量子アルゴリズムが得られるのに対し、未知である場合には少なくとも古典的な LWE 問題よりも困難であることがわかる。この、位相情報を持つかどうかによる困難性のギャップは LWE 問題を解く量子アルゴリズムを構築する際の障壁となるかもしれず、その検証を今後の研究のひとつとしている。

Unlocking Mix-Basis Potential: Geometric Approach for Combined Attacks

Kai Hu, Chi Zhang, Chengcheng Chang, Jiashu Zhang, Meiqin Wang, Thomas Peyrin

SKINNY や SIMECK などの共通鍵暗号に対する、幾何学的アプローチに基づく組合せ攻撃に関する論文である。幾何学的アプローチは、暗号の内部遷移をベクトル空間上の線形・非線形写像として捉え、integral 特性や multiple-of-2^t 特性を線形代数的に解析するための理論的基盤を提供してきた。しかし、従来の研究では単一の基底に固定した解析が主流であり、Beyne の博士論文で理論的に示唆されていた「異なる基底を混在させる解析」は、具体的な攻撃手法としては実現されていなかった。そのため、複数の攻撃パラダイム間の関係性や、より強力な識別器構成の可能性は十分に活用されていなかった。

本論文では、従来の幾何学的アプローチで用いられていた 3 種類の基底に加え、簡単な構成規則に基づく 4 種類の新たな基底が導入され、合計 7 種類の基底が体系化された。この結果、d 次の空間において 7^{2d} 種類の基底依存攻撃が構成可能であることが示された。この枠組みにより、integral 攻撃、multiple-of-2^t 攻撃、differential-linear 攻撃は、全て同一の自動探索手法の下で解析可能であることが示された。具体的な応用として、ASIACRYPT 2024 で Beyne と Verbauwhede により提案された ultrametric integral cryptanalysis における可除性（divisibility）の性質が、適切な基底対を選択することで、遷移行列の線形結合ではなく単一の行列要素として表現可能であることが示され、他の幾

何学的アプローチに基づく攻撃と同一の枠組みで捉えることができることが明らかにされた。さらに、EUROCRYPT 2017 で導入された multiple-of-2^t 性質についても本枠組みの下で再解析が行われ、SKINNY-64 に対して、第 1 次および第 2 次の両方の観点から、従来の最良結果を上回る multiple-of-2^t 識別器が構成可能であることが示された。これらの識別器は、従来よりも少ない仮定で成立し、幾何学的アプローチに基づく統一的解析の有効性を具体的に示す結果となっている。加えて、differential-linear 攻撃に対しては、一切の仮定を置かない一般的な closed form の評価式が導出された。この結果により、SIMECK-32 および SIMECK-48 に対して Hadipour らにより報告されていた 2 つの differential-linear 近似が、鍵値に依存せず決定的に成立するものであることが確認された。これは、従来経験的に観測されていた性質に対し、理論的根拠を与える結果である。

Breaking the IEEE Encryption Standard – XCB-AES in Two Queries

Amit Singh Bhati, Elena Andreeva

IEEE 1619.2 標準で規定されている Tweakable Enciphering Mode (TEM) である XCB-AES への攻撃に関する論文である。XCB-AES は、ディスク暗号化やストレージ暗号化といった実運用環境で利用される TEM として標準化されており、ブロック境界に整列したメッセージに対して形式的な安全性証明を備えているとされてきた。これらの安全性主張は、sprp、stprp、および vil-stprp といった擬似ランダム置換に基づく概念に依拠しており、長年にわたり安全であると認識されてきた。

本論文では、XCB-AES に対する最初の平文回復攻撃が示された。この攻撃は shared difference 攻撃と呼ばれ、暗号化クエリ 1 回および復号クエリ 1 回の合計 2 クエリのみで平文を回復できることが示された。その結果、XCB-AES が主張していた vil-stprp、stprp、および基本的な sprp 安全性が破られることが示された。さらに、この攻撃が多項式ハッシュ関数の分離可能性に起因する設計上の欠陥を利用していることが明確化された。

また、著者らにより、同一の shared difference 攻撃が XCBv1、HCI、MXCB といった他の XCB 系 TEM にも適用可能であることが示され、これら方式の安全性主張が同様に成立しないことが明らかにされた。結果として、20 年以上にわたり見過ごされてきた XCB 系設計戦略に内在する脆弱性が明示され、IEEE 1619.2 標準および XCB 系 TEM の安全性再評価の必要性があると報告されている。

Improved Resultant Attack against Arithmetization-Oriented Primitives

Augustin Bariant, Aurélien Boeuf, Pierre Briaud, Maël Hostettler, Morten Øygarden, Håvard Raddum

AO（Arithmetization-Oriented）プリミティブへの攻撃に関する論文である。ゼロ知識証明、マルチパーティ計算、完全準同型暗号といった暗号プロトコルでは、大きな有限体上での演算効率が重要となるため、共通鍵暗号技術のなかでも、AO プリミティブが広く採用されてきた。これらのプリミティブに対する暗号解析は、内部置換に関する CICO (Constrained-Input Constrained-Output) 問題を多項式系として解く問題に帰着され、従来は Gröbner 基底法を中心とした解析が主流であった。

本論文では、resultants に基づく攻撃フレームワークが導入され、高速な多変数乗算を用いた効率的な縮約手法により、既存の Gröbner 基底法および先行する resultants ベース攻撃を上回る性能が達成された。この結果として、Griffin に対しては 10 ラウンド中 8 ラウンド、Anemoi に対しては 21 ラウンド中 11 ラウンド、Rescue に対しては 18 ラウンド中 6 ラウンドまで CICO 問題が実際に解けることが示された。これは、それぞれ従来の最良の実装攻撃と比較して、1 ラウンド、3 ラウンド、1 ラウンドの改善に相当する。さらに、512 ビット安全性を主張していた Rescue のパラメータセットが初めて破られることが示され、多くの AO プリミティブが主張された安全性水準に到達してい

ないことが明確化された。

How to Recover the Full Plaintext of XCB

Peng Wang, Shuping Mao, Ruozhou Xu, Jiwu Jing, Yuewu Wang

IEEE Std. 1619.2 において規定されている tweakable enciphering mode である XCB への攻撃に関する論文である。XCB は共有ストレージ媒体向け暗号化方式として標準化されており、擬似ランダム置換に基づく安全性概念である strong tweakable pseudorandom permutation（STPRP）安全性を満たすことが期待されてきた。しかし、XCB の構造は、多項式に基づくユニバーサルハッシュ関数を内部で用いることから、入力ブロック数や攻撃者のクエリ能力に依存した安全性劣化の可能性が指摘されていた。

本論文では、XCB が単一ブロックメッセージに対して LRW1 型 tweakable ブロック暗号と同等に振る舞い、CCA 安全性を満たさないことが示された。さらに、平文回復攻撃として、3 クエリにより 1 ブロックの平文を回復する攻撃、4 クエリにより 1 ブロックを除いた平文を回復する攻撃、および 7 クエリにより完全な平文を回復する攻撃が可能であることが示された。また、基礎となるユニバーサルハッシュ関数の分離可能性を利用することで、後者 2 つの攻撃が全ての XCB バージョンに適用可能であることが示された。これらの結果を踏まえ、XCB に XOR 演算を 2 回追加した改良構造 XCB* が提案され、AXU ハッシュ関数、SPRPs、および安全なランダム IV に基づくストリーム暗号を用いることで、XCB* が STPRP 安全であることが示された。

E.9 FDTC 2025

Fault attacks against UOV-based signatures

Sven Bauer, Fabrizio De Santis, Kristjane Koleci

MAYO および PROV に対する故障利用攻撃に関する論文である。

Unbalanced Oil and Vinegar (UOV) 構成は、NIST の耐量子計算機暗号追加署名の候補の中で、いくつかの多変数多項式に基づく方式の基盤となっている。本論文では UOV 構成に基づく署名方式の中でも、署名生成において乱数を外部に求めない決定的署名を取り扱う。具体的には署名生成時の、ビネガー変数の選択および過小決定系の線型方程式からの解を選択するときに用いる乱数を、文書のハッシュ値と秘密の seed から決定的に生成する変種である。本論文では、この決定的変種に対する新たな故障注入攻撃を提案している。

NIST PQC 追加署名標準化プロジェクト第 2 ラウンド候補である MAYO および第 1 ラウンド候補である PROV に適用可能であることを示し、リファレンス実装を ChipWhisperer CW308-STM32F4 ターゲットボード上の ARM Cortex-M4 上で動作させることで実証した。

具体的には 2 つの攻撃が提案されている。一つ目は文書のハッシュ値から生成されるターゲットベクトル $t = H(M)$ の計算後に故障注入を行い t' へと変化させ不正な署名 (faulty signature) を生成、それと正規の署名をから秘密鍵復元を可能とする。

二つ目の攻撃は過小決定系の線型方程式から解を選ぶための乱数に故障を注入し、正しいが本来のものとは異なる署名を生成させるものである。本来の署名との差分を取ることで秘密鍵復元を可能とする。

以上 2 種類の攻撃は MAYO に適用可能であり、仕様書にある SHAKE256 の計算に故障注入を行うことで不正な署名を得ることができる。実験により、2 種類の不正な署名、もしくは不正な署名と正規の署名のペアから秘密鍵を復元可能であると報告している。

一方で、PROV に対しても同様に SHAKE256 への故障注入に基づく鍵復元攻撃が可能であるがこちらの仕様では解の選択は決定的に行われる仕様であり乱数が用いられないため、第二の攻撃は不可能であるとしている。実験により、正しい署名 1 件と不正な署名 2 件で秘密鍵を復元できると報告している。

本論文によればこれらの攻撃は精密な故障注入を必要とせず、ハッシュ関数の計算のような比較的長時間の処理に対して命令スキップやデータ破壊のような比較的粗い故障を注入できれば成功する。そのため、非常に安価な機材と単純なクロックグリッチ技術で実行可能であると主張している。

第一の攻撃に対しては不正な署名を検出するルーチンを追加することで対処可能であるが、第二の攻撃に対しては faulty signature も有効な署名であるため検出が困難である。そのため、疑似乱数生成のためのハッシュ関数の計算回路に故障耐性を持たせること、決定的な仕様ではなく外部の乱数を併用する非決定的な設計とすることを提案している。

E.10 CHES 2025

ECTester: Reverse-engineering side-channel countermeasures of ECC implementations

Vojtech Suchanek, Jan Jancar, Jan Kvapil, Petr Svenda, Łukasz Chmielewski

楕円曲線暗号のブラックボックス実装についてのリバースエンジニアリングに関する論文である。楕円曲線を実装する開発者は、長年に及ぶ楕円曲線暗号の研究によって生み出された多くの実装上の選択肢に直面している。楕円曲線の文献には、多様な曲線モデル、スカラー倍算、加算式などが載っているが、これらの豊富な手法の構造は、攻撃者にも利用され得るという代償を伴っている。この分野を扱うのは容易ではなく、開発者は、特にブラックボックスハードウェア実装において、その選択を隠すことがしばしばある。サイドチャネル攻撃者は実装の詳細を頼りにするため、リバースエンジニアリングは攻撃における非常に重要な部分である。本論文は、ブラックボックスの楕円曲線暗号の実装をテストするツールである ECTester を提案する。様々なテストスイートを通じて、ECTester は既知の攻撃に対するふるまいだけでなく、非標準の入力や楕円曲線パラメタに対する攻撃対象の実装の挙動を観察する。著者は主要な楕円曲線暗号ライブラリやスマートカードを解析し、一部のライブラリと大半のスマートカードが入力の点の位数をチェックせず、無限遠点の扱いが不適切であることを示した。これらの観察に基づき、スカラーのランダマイゼーションの対策をリバースエンジニアリングする新しい手法を設計した。この手法は、群のスカラーランダマイゼーション、加法的、乗法的、ユークリッド分割といった対策を区別できる。この手法はサイドチャネル測定を必要とせず、カスタムのドメインパラメタを設定することができれば、使用されたランダムマスクのサイズだけでなく正確な値を抽出することが可能になる。この手法を用いて、主要メーカー 5 社の 13 枚のスマートカードのほとんどの対策のリバースエンジニアリングに成功した。最後に、このようなリバースエンジニアリングを防ぐためにどのような緩和策が適用可能か、それが可能であるのかを議論する。

MulLeak: Exploiting Multiply Instruction Leakage to Attack the Stack-optimized Kyber Implementation on Cortex-M4

Fan Huang, Xiaolin Duan, Chengcong Hu, Mengce Zheng, Honggang Hu

NIST PQC 標準化方式である CRYSTALS-Kyber の pqm4 実装に対する攻撃論文である。

NIST 標準化プロジェクトの中で効率的かつ堅牢な実装が評価対象とされたことに対応し、2018 年に欧州委員会 H2020 中の PQCRYPTO プロジェクトの一環として、統一された環境での実装効率の比較のために pqm4 公開プロ

ジェクトが開始された。pqm4 ライブラリ (`https://github.com/mupq/pqm4`) では主に NIST PQC 標準化第 2 ラウンド以降の暗号方式の、ARM Cortex-M4 プロセッサ上での処理速度に特化した speed optimized 実装と実行時の RAM 削減に特化した stack optimized 実装が公開されている。

これまでのサイドチャネル攻撃では主に speed optimized 実装が対象とされており、stack optimized 実装ではメモリ移動の少なさからサイドチャネル情報を得ることが難しく、攻撃への耐性が高いと考えられてきた。しかしながら、本論文では stack optimized 実装において、さらにプロセッサがパイプライン処理を行い 1 サイクル内で複数の処理が混在している場合でも、比較的少ないトレース数での攻撃が可能であることを報告している。攻撃手法は先行研究による電力波形からの回帰モデルを用いた攻撃 (Schindler et al, CHES 2005) の改良による。

Kyber の復号プロセスにおいて、暗号文 $(\boldsymbol{u}, v)$ の復号は中間結果 $v - NTT^{-1}(\hat{s\boldsymbol{k}} \circ NTT(\boldsymbol{u}))$ をデコードする形で行われる。本論文での攻撃は既知暗号文または選択暗号文の条件下で、中間結果 $\hat{s\boldsymbol{k}} \circ NTT(\boldsymbol{u})$ の計算を行う電力波形から秘密鍵の NTT 空間における形 $\hat{s\boldsymbol{k}}$ の復元を行うものである。pqm4 実装では効率化のため、$\hat{s\boldsymbol{k}}$ と $NTT(\boldsymbol{u})$ は完全な NTT 形ではなく、高速数論変換の最後の 1 段を行わない Incomplete NTT と呼ばれる表現で保存されており、数学的には $\hat{s\boldsymbol{k}} = (\hat{sk}_0 + \hat{sk}_1 X, \hat{sk}_2 + \hat{sk}_3 X, \ldots)$ のように 1 次多項式が 128 個並んだベクトルとして扱われる。このとき、pair-pointwise multiplication として論文内 Algorithm 4 で示されるように、$r_0 \leftarrow \hat{ct}_0 \cdot \hat{sk}_0 + \hat{ct}_1 \cdot \hat{sk}_1 \cdot \zeta$ および $r_1 \leftarrow \hat{ct}_0 \cdot \hat{sk}_1 + \hat{ct}_1 \cdot \hat{sk}_0$ の形で計算されるため、この部分を計算する電力波形から $\hat{sk}_0, \hat{sk}_1$ を復元することが攻撃の概要である。この部分はアセンブリレベルでは `doublebasemul_frombytes_asm` マクロとして記述され、実際には 10 個程度の命令に分割されパイプライン実行される。

実験では Kyber-768 のプロテクト無し実装に対して、1 組の秘密鍵の要素 $\hat{sk}_{2i} + \hat{sk}_{2i+1} X$ を復元するのに既知暗号文の場合で 12-13 回のトレース、選択暗号文では 23-34 回のトレースが必要と報告されている。選択暗号文の方がトレースが多いのは暗号文が選択可能な代わりに $\hat{sk}_{2i}$ の復元に用いることのできる乗算命令の個所が 4 から 2 に減ることが原因と説明されている。一方で、1st-order マスク実装の場合には選択暗号文の設定で 201 回のトレースで復元可能であったと報告されている。

Avengers assemble! Supervised learning meets lattice reduction: A single power trace attack against CRYSTALS-Kyber Key Generation

Pierre-Alain Fouque, Damien Marion, Quyen Nguyen, Alexandre Wallet

NIST PQC 標準化方式である格子ベース暗号 CRYSTALS-Kyber (ML-KEM) に関するサイドチャネル攻撃論文である。

Kyber の鍵生成アルゴリズムは秘密鍵 $\boldsymbol{s}$ とエラー $\boldsymbol{e}$ に対して公開鍵を Module-LWE 関係式 $\boldsymbol{t} = A\boldsymbol{s} + \boldsymbol{e}$ により生成する。このとき、各 $\boldsymbol{s}, \boldsymbol{e}$ の要素は大きさ $\eta = 2, 3$ の中心二項分布から取られており、実装では疑似ランダムビットを切り出すことで $a, b \in \{0, \ldots, \eta\}$ を生成、その差分 $a - b$ を係数とする。

本論文では、中心二項分布生成ルーチン実行中の電力波形を用いた秘密鍵復元について考察する。攻撃モデルではまず、事前に機械学習を用いて電力波形の分類と a, b のハミング重み情報との対応づけを行い、実際の攻撃では単一の電力波形からの秘密鍵復元を狙う。

実験では pqm4 ライブラリの Kyber 実装を Cortex-M4 搭載のマイクロコントローラ STM32F4 上で動作させ、ChipWhisperer CW1200 を用いた電力波形の取得を行う。異なる 4 台の (同一型番の) マイクロコントローラから Kyber-512,768,1024 のそれぞれに対して 20000 回の波形を取得し a, b のハミング重みとの対応を学習後、単一波形からのハミング重みおよび $\boldsymbol{s}, \boldsymbol{e}$ の部分情報の復元、ヒント付き LWE 問題として定式化することで秘密情報の完全復元を行っている。

鍵復元実験による結果として、秘密情報 $\boldsymbol{s}, \boldsymbol{e}$ 内の係数の半分が取得可能な場合にはガウスの消去法で全ての係数が復元され、Kyber-512 に対しては係数の 37% のみが取得可能な場合でも格子基底簡約により 18 時間程度で復元が可能であるとしている。Kyber-768,1024 に対しても係数の 45% 程度の情報からブロックサイズ 70 程度の格子基底簡約により同程度の時間で復元可能であると報告されている。全体を通して、96% 以上の確率で単一トレースからの鍵復元が可能であるとしている。

著者らは考察として、既存のマスク実装による対策は複数回実行されることが前提の暗号化・復号ルーチンに対するものが主であり、鍵生成は基本的には一度しか実行されないため注目されてこなかったが、今後は鍵生成ルーチンに対するマスキングやシャッフリング実装などの対策を考える必要があるとしている。また、Kyber と同様のサンプリングアルゴリズムを用いる格子ベース署名 HAWK および準同型暗号ライブラリ SEAL にも同様の脆弱性が存在する可能性があるとしている。

Rejected Signatures' Challenges Pose New Challenges: Key Recovery of CRYSTALS-Dilithium via Side-Channel Attacks

Yuanyuan Zhou, Weijia Wang, Yiteng Sun, Yu Yu

NIST 標準署名方式である ML-DSA に対するサイドチャネル鍵回復攻撃の論文である。

Rejection Sampling は、ML-DSA / CRYSTALS-Dilithium のような Fiat-Shamir with Aborts パラダイムに従う格子ベース署名で重要なセキュリティ機構である。この手法は、秘密に依存する署名サンプルを (ランダムオラクルモデルにおいて) 秘密に非依存な分布に統計的に近づける役割を果たす。これまで多くのサイドチャネル攻撃がノンスや秘密鍵、分解されたコミットメントなどの秘密データを直接的に狙ってきたが、rejection sampling に関連した漏洩を詳しく扱った研究は少ない。特に、HOST 2021 で Karabulut らは、拒否された署名のチャレンジからの漏洩が Dilithium の安全性を弱め得ることを示しているが、完全に破るわけではないと報告している。

本研究はこの問題に基づき、(rejection sampling の漏洩からの) 鍵回復問題を線形整数計画問題に帰着させる。ここでは、ユニークなハミングウェイトの拒否応答が、チャレンジと秘密鍵の間の積に関する上限・下限の制約を与える。問題の最悪時の計算複雑度を形式的に解析するとともに、実験的に rejected signature's challenge attack の実用性を確認した。Dilithium-2、3、5 のいずれのパラメータにおいても、提案手法は数秒から数分で秘密鍵を完全に回復し、成功率は 100% であった。

本攻撃は rejected signature's challenge と応答の知識を前提とするため、数論変換 (NTT) 演算や応答生成手続きに関連する関数からの単一トレースのサイドチャネル漏洩を利用してチャレンジと応答を回収する方法を提案する。ARM Cortex-M4 上での実際の電力トレースを用いた実験により、本攻撃の実用性を実証した。筆者らの知る限り、rejected sampling procedure を標的とした ML-DSA / Dilithium に対する実用的かつ効率的なサイドチャネル鍵回復攻撃は本研究が初めてである。最後に、これらの脆弱性を緩和するための対策についても議論する。

Improved Attacks Against Lattice-Based KEMs Using Hints From Hertzbleed

Zhiwei Li, Jun Xu, Jun Song, Haomeng Xu, Yan Jia, Yanli Zou, Lei Hu

数論変換 (NTT) は格子ベース暗号で計算を高速化するために広く使われている。CHES 2024 で Yu らは、簡略化した Kyber と NTTRU スキームを対象に NTT 演算を標的とする一連のサイドチャネル攻撃を提案した。彼らの研究は、サイドチャネル漏洩を「剰余に関するヒント (modular hints)」としてモデル化し、それが秘密鍵の一部情報を明かすことを示した。これらの剰余ヒントはその後 Learning With Errors (LWE) や NTRU の高次元格子に組み込

まれ、鍵回復の計算量を下げるために用いられた。しかし、彼らの手法は剰余ヒントの潜在能力を完全には活用していない。本稿の主要な観察は、これらの剰余ヒントは元の高次元格子に組み込むのではなく、直接低次元格子を構成するのに十分である、という点である。

本論文では、簡略化した CPA 安全な Kyber に対して、抽出した剰余ヒントを直接用いて低次元格子を構築する。続いて攻撃者は格子 reduction アルゴリズムを用いてこれらの格子内の非ゼロ最短ベクトルを探索する。実験結果は、パーソナルコンピュータ上で秘密鍵全体を 400 秒以内に復元できることを確認する。したがって本攻撃は実用的に秘密鍵を回復するものであり、CHES 2024 の Yu らの手法ではこれを達成できない。

さらに、CCA 安全な NTTRU に対しては、Yu らのサイドチャネル手法に基づいて追加の剰余ヒントを抽出する。NTTRU の秘密鍵が持つ特殊な構造とガウス消去を組み合わせて低次元格子を生成し、続いて Yu らが用いた評価手法で非ゼロ最短ベクトル問題の難易度を推定する。その結果、鍵回復の計算量を 2^{34} まで低減できることが示され、これは CHES 2024 の報告 (2^{114}) よりも大幅な改善である。

Leaky McEliece: Secret Key Recovery From Highly Erroneous Side-Channel Information

Marcus Brinkmann, Chitchanok Chuengsatiansup, Alexander May, Julian Nowakowski, Yuval Yarom

McEliece 暗号は、耐量子計算機耐性を持つ暗号の有力な候補の一つであり、ネットワークプロトコルの鍵交換の機密保持のための鍵カプセル化にも用いられている。McEliece の秘密鍵は構造を持つパリティ検査行列であり、ガウス消去によって構造のない公開鍵へと変換される。本論文ではこの変換処理がサイドチャネル漏洩に関して非常に重要であることを示す。具体的には、ガウス消去中の基本的な行操作が漏洩することを仮定する（Classic McEliece や Botan の暗号ライブラリの実装から動機付けられる）。

著者らは、ガウス変換の漏洩から得られる情報を利用して公開鍵から秘密鍵を再構成する新しいデコードアルゴリズムを提案する。得られる漏洩が非常にノイジーで、各ビットの反転確率が高々 $\tau \approx 0.4$ であるような場合でも、提案した (Classic)McEliece の全インスタンスについて数分で秘密鍵を復元することに成功した。特に高セキュリティな McEliece パラメタでは本攻撃の許容するノイズ率 τ はさらに大きくなり、攻撃はより強力になることが分かった。STM32L592 ARM プロセッサ上の Classic McEliece の一定時間リファレンス実装に対する単一トレース環境で攻撃を実証した。

本結果は、McEliece のような構造化されたコードベーススキームをサイドチャネル漏洩から適切に保護する必要性を強調する。

Multi-Value Plaintext-Checking and Full-Decryption Oracle-Based Attacks on HQC from Offline Templates

Haiyue Dong, Qian Guo

Hamming Quasi-Cyclic (HQC) 鍵カプセル化機構 (KEM) は、NIST の PQC 標準化で選定されており、効率性、符号理論における難しい復号問題に基づく堅牢な設計、復号失敗率が良く特徴づけられている点が特長である。しかし、選定されたとはいえ、実装上の脅威、特に plaintext-checking (PC) オラクルを悪用する攻撃からの実用的な安全性には懸念が残る。格子ベース暗号の文脈では多値 PC(MV-PC) や完全復号 (FD) オラクル攻撃が広く研究されてきたが、HQC のような符号ベース方式に対する適用は比較的未検討だった。

本研究では、符号ベース KEM、とくに HQC を対象とした初の MV-PC および FD オラクル攻撃を提案する。提案する MV-PC 攻撃は従来の PC オラクル法に比べて必要なオラクル問い合わせ回数を大幅に削減し、サイドチャネ

ル、鍵不一致、故障利用攻撃にも影響を与える。FD 攻撃はトレース複雑度の点で極めて効率的で、完全なオラクルを想定すれば hqc-128 の秘密鍵をわずか 2 回の問い合わせで復元でき、hqc-192 および hqc-256 でも 4 回の問い合わせで復元できる。シミュレーションでも、回答が完全でないオラクルに対して攻撃が堅牢であることを示した。さらに、ARM Cortex-M4 マイクロコントローラ上で実験的に攻撃を検証し、堅牢な攻撃対策の必要性を強調する。特にこのようなプラットフォームではシンドローム計算などの処理中に大きなリーケージが生じ、FD オラクル攻撃の緩和に用いられるマスキング技術の有効性を著しく損なうという課題がある。

New Quantum Cryptanalysis of Binary Elliptic Curves

Kyungbae Jang, Vikas Srivastava, Anubhab Baksi, Santanu Sarkar, Hwajeong Seo

本論文は、バイナリ楕円曲線に対する Shor の攻撃に必要な量子回路を改良する、量子ビット数と回路深さの両方を考慮した、2 種類の点加算回路を提示する。要約すると、まず、in-place 点加算を提案し、CHES 2021 の Banegas らの手法を改良して量子ビット数と深さの積を変種に応じて約 73% - 81% 削減した。さらに、追加の量子ビットを使う out-of-place 点加算を開発した。この手法は最小の回路深さを達成するとともに、単一ステップについては量子ビット数と深さの積を 92% 以上改善した。

筆者らの知る限り、本手法は回路深さおよび量子ビット数と深さの積の点で、Banegas ら（CHES 2021）、Putranto ら（IEEE Access 2022 論文）、Taguchi & Takayasu（CT-RSA 2023）を含む先行研究すべてを上回っている。

実装に基づき、バイナリ楕円曲線暗号の耐量子計算機セキュリティについても議論する。NIST が提唱する MAXDEPTH 指標の下では、本論文で最も深さの大きい量子回路の深さは 2^{24} であり、MAXDEPTH の上限である 2^{40} を大きく下回る。さらに、量子攻撃コスト推定のためのゲート数と全深さの積指標では、次数 571 の曲線（古典的セキュリティが AES-256 に相当）に対する最大複雑度が 2^{60} であり、ポスト量子セキュリティレベル 1 のしきい値（およそ 2^{156}）をかなり下回っている。

Quantum security analysis of Module-LWE PQC based on practical cost estimates

Seong-Min Cho, Changyeol Lee, Seung-Hyun Seo

NIST PQC 標準化方式である格子ベース暗号 ML-KEM および電子署名方式 ML-DSA の量子計算量に関する論文である。

格子暗号のパラメータ設定は、方式の攻撃困難性を格子問題に帰着し、帰着先の問題を篩アルゴリズムをサブルーチンとした BKZ アルゴリズムの計算量評価を通じて行われるのが一般的である。特に、BKZ アルゴリズム内で用いられる最大のブロックサイズ β に対して、β-次元ランダム格子の最短ベクトルを求める計算量が Core-SVP 計算量と呼ばれ、暗号の解読計算量として扱われることが多い。

本論文では、篩アルゴリズムの量子計算量の見積もりを与えている。篩アルゴリズムは古典計算量の観点では最速のアルゴリズムであり、その量子版を考えた場合の計算量が耐量子計算機暗号として相応しいかどうかを確認することがモチベーションの一つとなっている。篩アルゴリズムの一般的な形では、(既存のリスト内または格子点サンプラーから) 与えられた格子点 $\boldsymbol{v}$ を簡約可能な格子ベクトル $\boldsymbol{w}$ をリスト L 内から探索し簡約を繰り返す。この探索が古典時間計算量の中で支配的であり、量子化することで高速化が見込まれる。先行研究の多くではこの探索を Grover の量子探索アルゴリズムに置き換え時間・空間計算量評価を行っているものの、回路内でのクエリー回数の評価に留まっており具体的な回路構成を与えているものは存在しなかった。

本論文では量子探索部分の具体的な回路構成と必要量子リソースの評価を行った上で、それ以外の部分が古

典で実装されたと仮定したときの ML-KEM、ML-DSA の解読計算量評価を行っている。論文内で用いられている篩アルゴリズムのモデルはスタック S または格子点サンプラーから取得した $\boldsymbol{v}$ に対して、量子探索を用いて $\boldsymbol{w} = \sum_{i=1}^{n} x_i \boldsymbol{b}_i, x_i \in [-T, T]$ の形の格子点で $\boldsymbol{v} - \boldsymbol{w}$ が $\boldsymbol{v}$ よりも短くなるものを発見し返すものであり、発見されたベクトルのさらなる簡約、スタックへの追加などは古典部分で行われる。このとき、Module の構造などは用いられていない。著者らはベクトル成分の加減算およびノルムの評価を行う量子回路を構成し、T ゲートでの深さ ($T-$depth) を最小化した構成での量子ビット数、T-ゲート数、$T-$depth を計算している。これらの値を基に、Grover のアルゴリズムを用いた論理量子回路の T ゲートを基準とした合計ゲート数および深さを評価している。

最後に、論文内 Table 13 で ML-KEM、ML-DSA に対する量子計算量と古典計算量の比較を行っている。古典側は Kyber および Dilithium の仕様書で主張された古典回路におけるゲート数を用い、本論文の量子計算量は表面符号を用いた場合の量子ビット数と計算中に行われる表面符号のサイクル数の積を量子計算コストとしている。結果として、ML-KEM に関しては 512,768,1024 の量子計算量が 18,17,27 ビット削減、ML-DSA に関しては 44,65,87 の量子計算量が 20,15,22 ビット削減されている。

Sieving with Streaming Memory Access

Ziyu Zhao, Jintai Ding, Bo-Yin Yang

格子暗号の安全性の根拠となる最短ベクトル問題の計算量に関する論文である。

多くの格子暗号のパラメータ設定では攻撃の困難性を格子問題に帰着し、格子問題の困難性を篩アルゴリズムをサブルーチンとした BKZ アルゴリズムの計算量により測る。BKZ アルゴリズム内で用いられる最大のブロックサイズ β に対して、β-次元ランダム格子の最短ベクトルを求める計算量が Core-SVP 計算量と呼ばれ、暗号の解読計算量として扱われることが多い。。

この Core-SVP 計算量評価は篩アルゴリズムの漸近計算量として $2^{O(c_t\beta)}$ 時間、$2^{O(c_s\beta)}$ 空間の形で与えられてきた。比例定数は篩アルゴリズムの種類ごとに異なるが、現在最速のものとして [Becker ら, ACM SODA 2016] による BDGL 篩アルゴリズムの $c_t = 0.292, c_s = 0.2075$ が暗号のパラメータ設定に用いられている。しかしながら、Bernstein らによる指摘で N ビットのメモリ空間にランダムアクセスを行う場合 1 回あたり $O(\sqrt{N})$ のコストがかかる可能性があり、計算量評価が適切であるかどうかは議論が続いていた。

本論文では、BDGL 篩アルゴリズムの原型となった、BGJ 篩アルゴリズム [Becker ら、Cryptology ePrint Archive, 2015/522] のメモリアクセス順序をランダムではない連続的なものに改良した streaming BGJ 篩法を提案し、その解析から格子暗号のパラメータ設定における議論を行い、結論として巨大なメモリに対するメモリアクセスのコストは無視できるものであり、セキュリティパラメータ決定の際に計算コストを上げる要素として用いるべきではないと結論付けている。

技術的には近年の篩アルゴリズムの改良で用いられいる局所鋭敏性ハッシュ関数 (LSH) によるベクトルの格納順序を改良することでメモリのアクセス順序を連続的なものとしている。篩アルゴリズムのコアは巨大な格子ベクトルのデータベース $L = \{\boldsymbol{v}_i\}$ 内から近い距離にあるペア $(\boldsymbol{v}_i, \boldsymbol{v}_j)$ を発見するサブルーチンであり、計算量を削減するために LSH による事前の分類を行い、同じハッシュ値を持つベクトルをバケツ $L_1, L_2, \ldots$ に分類、同じバケツ L_i の中に入るベクトルに対してはその距離を全数探索で計算し近いペアを探索する。ここでバケツへの分類にメモリへのランダムアクセスが入ることが課題であった。本論文では、BGJ 篩アルゴリズムの多段式バケツの考え方を用いてデータベース内のベクトルを数百個程度のバケツ $L_1, \ldots, L_{B_0}$ に配置、次の段では L_i 内のベクトルを LSH を用いて $L_{i,1}, \ldots, L_{i,B_1}$ にコピーすることでメモリへのシーケンシャルアクセスを保証している。ただし用いられる LSH の形は BGJ のランダムフィルタではなく、BDGL の球面キャップ型フィルタを用いている。

提案アルゴリズムの漸近計算量解析では $c_t = 0.292$ 付近であるが正確なところは不明としているものの、$c_s = 0.2075$ を実現しておりメモリ消費量の増加は無いとしている。実装上の改良点として、8 ビット浮動小数点を用いて格子ベクトルの情報を格納することでメモリ量を減らし、この精度でも dual-LLL 簡約基底の情報を使うことで元のベクトルが復元できるとされている。また、dimension-for-free において LSH の情報を用いて射影格子内のベクトル同士の組み合わせを増幅することで lifting 可能なベクトルの本数を増やし、free となる次元を増やす提案が行われている。

実験的な成果として、公開チャレンジである SVP Challenge において 183 次元の問題を 112 コア CPU、0.87TB メモリ、30 日で解き、Ideal-SVP チャレンジにおいて 796 次元の近似ベクトルを求めている。また、理論的な成果として NIST PQC 標準化プロジェクトの候補となっていた Falcon-512 の署名偽造の回路計算量が $2^{139.8}$ から $2^{145.8}$ の間であり、NIST がセキュリティカテゴリ 1 として求める 2^{143} に届かない可能性を指摘している。同様に Kyber-512 の解読計算量も $2^{140.1}$ から $2^{146.1}$ の間と評価されているが、この評価の帰結に関しては明確に言及されていない。

All You Need is XOR-Convolution: A Generalized Higher-Order Side-Channel Attack with Application to XEX/XE-based Encryptions

Rei Ueno, Akira Ito, Yosuke Todo, Akiko Inoue, Kazuhiko Minematsu, Hibiki Ishikawa, Naofumi Homma

XEX/XE スキームに対するサイドチャネル攻撃に関する論文である。XEX/XE スキームは、OCB・PMAC・XTS のような認証付き暗号 (AE)、メッセージ認証コード (MAC)、およびストレージ暗号化で広く用いられている。これらの方式は実運用で広く展開されているが、サイドチャネル攻撃 (SCA) に関する評価は限られている。

本論文では、XEX/XE スキームに適用可能な効率的なサイドチャネル攻撃を提案する。XEX/XE の各モードでは、生成されるオフセットがほとんど確実に「フルオフセット衝突」を起こさないことが保証されているが、本研究ではオフセット生成ルーチンを解析することで「部分的なオフセット衝突」を悪用できることを示す。これに基づき、XOR-convoluting collision analysis (XCCA) と呼ぶ新しいプロファイル型サイドチャネル攻撃を提案する。これは、漏洩をモデル化した確率分布に XOR-convolusion を適用することで、2 つの漏洩から鍵の和を推定する。XOR-convolusion を使用することでランダムオフセットの効果を効率的に打ち消すことができる。従来型の collision SCA が有効でないシナリオでも有効になる。

提案手法はシミュレーションと実トレースによる実験で検証されており、TCHES 2022 における OCB に対する最先端手法と同等の成功率を得るために必要なトレース数を最大で約 90 % 削減できることが示された。さらに、SCA の distinguisher (XCCA distinguisher) は、マスキング実装に対する非衝突型 SCA を含む高次 SCA の一般化であることも示す。マスキング実装に対するプロファイル型高次 SCA は、leaking and target selection function という新しい概念の XOR-convolusion を用いた XCCA distinguisher の形で記述できる。この一般化された表現により、ノイズ増幅という理論的観点から高次 SCA がなぜ性能が良くなったり悪くなったりするのかが明確になり、実験や Walsh-Hadamard 変換 (WHT) に基づくスペクトル解析で示されている。本解析から、XEX/XE におけるランダムオフセットは SCA の観点では一種のマスキングとして機能し、ある条件下では XEX/XE ベースの暗号化は一次の SCA に対して本質的な耐性を持つことが分かる。

E.11 TCC 2025

Sandwich BUFF: Achieving Non-Resignability Using Iterative Hash Functions

Serge Fehr, Yu-Hsuan Huang, Julia Kastner

BUFF 変換における非再署名性（non-resignability、NR）への攻撃に関する論文である。BUFF 変換は、既存のデジタル署名方式に対して、非再署名性などの追加的安全性性質を付与するために提案された軽量な変換であり、署名対象をメッセージそのものではなく、メッセージと公開鍵を含むハッシュ値とする点に特徴がある。しかし、非再署名性の元の定義は達成不可能であることが示され、その後、ランダムオラクルモデルにおいて成立可能な緩和版定義 sNR が導入された。これまでの肯定的結果は、ハッシュ関数全体をランダムオラクルとして扱う理想化に依存しており、実際に用いられる反復型ハッシュ関数を考慮した場合の安全性は未解明であった。

本論文では、反復型ハッシュ関数を用いて BUFF 変換を実装した場合に、補助情報を通じてハッシュ計算の中間ダイジェストが adversary に漏洩すると、非再署名性 sNR が破られることが示された。具体的には、Merkle – Damgård 型や Sponge 型ハッシュ関数の反復構造を利用し、未知のメッセージに対する再署名が可能となる攻撃が構成された。これに対して、本論文では、ハッシュ入力を $m \parallel pk \parallel m$ とする Sandwich BUFF が提案され、この構成により、中間値の漏洩が再署名に直結しないことが示された。さらに、Merkle – Damgård 型についてはランダムオラクルモデルで、Sponge 型についてはランダム置換モデルで、Sandwich BUFF が sNR を満たすことが示され、実用的ハッシュ関数設計において非再署名性を回復するための具体的指針が与えられた。

Dimensional eROSion: Improving the ROS Attack with Decomposition in Higher Bases

Antoine Joux, Julian Loss, Giacomo Santato

ROS（Overdetermined Solvable system of linear equations）問題およびそれに基づく署名方式への攻撃に関する論文である。ROS 問題は、Schnorr によるブラインド署名の解析に端を発し、その後、ブラインド署名、閾値署名、マルチ署名など、多くの対話型署名方式の安全性と密接に関係する基礎問題として研究されてきた。これまでの研究では、次元 $l > \log_2 p$ の場合に多項式時間攻撃が可能であることが知られていた一方、それ以下の次元では部分和型攻撃などに基づく準指数時間解法が最良であった。そのため、多項式時間で解ける次元範囲をどこまで拡張できるかは、ROS に依存する暗号方式の安全性評価において重要な課題であった。

本論文では、数の分解を二進法から高基数分解へ一般化する新しい多項式攻撃が導入され、ROS 問題が $l \gtrsim 0.725 \cdot \log_2 p$ の次元において多項式時間で解けることが示された。さらに、この攻撃を Wagner 攻撃と組み合わせることで、多項式解法が既知でなかった次元領域においても攻撃計算量が改善された。実装結果として、256 ビット楕円曲線上のブラインド Schnorr 署名に対し、192 並列セッションを用いることで one-more 非偽造性が平均約 13 秒で破られることが報告された。

Special Genera of Hermitian Lattices and Applications to HAWK

Guilhem Mureau

HAWK の安全性の根拠となる、判定 module-LIP への攻撃に関する論文である。モジュール格子同型問題（module-LIP）は、二つの格子が同型であるかどうかを判定、あるいはその同型写像を求める問題であり、近年、格子ベース署名方式 HAWK の安全性仮定として注目を集めている。判定版 module-LIP においては、数体の整数環上の格子に付

随する代数的不変量を用いた区別可能性が、攻撃の潜在的手段として検討されてきた。従来の研究では、$\mathcal{O}_F$ が単項イデアル整域であると仮定した下で、二次形式を備えた階数 2 の $\mathcal{O}_F$ 格子のスピノル種数（spinor genus）を区別する多項式時間アルゴリズムが与えられた。スピノル種数は二次形式格子について有力な不変量であるものの、HAWK が用いる円分体上のエルミート格子には直接適用できないという制約があった。

本論文では、エルミート格子に特有の不変量である特別種数（special genus）が導入され、Shimura による分類結果に基づき、二つのエルミート格子が同一の特別種数を有するかどうかを判定するアルゴリズムが与えられた。特に、HAWK の格子 $\mathcal{O}_K^2$（K は円分体）に対しては、疑似 Gram 行列のみを入力として、特別種数を持つかどうか古典的多項式時間で判定できることが示された。さらに、特別種数は種数（genus）よりも精緻な不変量であり、区別すべき同型類の数を $2^{\Omega(d)}$（d は体 K の次数）だけ減少させることが示された。一方で、数値的評価により、暗号サイズのパラメータにおいては、固定された特別種数において、なお指数個の同型類が残ることが示され、特別種数の識別が実用的な判定 module-LIP 攻撃に直結しないことが明確にされている。

(Multi-Input) FE for Randomized Functionalities, Revisited

Pratish Datta, Jiaxin Guan, Alexis Korb, Amit Sahai

ランダム化関数型暗号（randomized functional encryption、rFE）およびランダム化多入力関数型暗号（randomized multi-input functional encryption、rMIFE）への攻撃に関する論文である。関数型暗号（FE）は、暗号文に対して関数的な情報のみを抽出できる暗号方式であり、その拡張として rFE は、復号結果が確率分布として定義される機能を扱う。しかし、rFE では、悪意ある復号者に加えて、悪意ある暗号化者による攻撃も考慮する必要があり、特に不正な暗号文を用いて復号結果の分布を歪めたり、相関を導入したりする攻撃が問題となる。

本論文では、従来の rFE ／ rMIFE に対する IND 安全性定義において、悪意ある暗号化者に対する防御が不十分であることが示された。具体的には、既存の IND 定義を満たすにもかかわらず、暗号化者が不正な暗号文を生成することで復号出力の分布を操作できる rFE 構成の反例が与えられた。これにより、従来の定義では本質的な攻撃が排除されていないことが形式的に明らかにされた。さらに、本論文では、悪意ある復号者と悪意ある暗号化者を分離して扱う二つの実験からなる新しい IND 安全性定義が導入された。この定義の下で、 選択的安全性しか保障されていない Goldwasser らによる唯一の rMIFE 構成を、準指数的安全性を持つ識別不能化難読化（iO）を拡張した新たな rMIFE を提案している。

Zeroizing Attacks against Evasive and Circular Evasive LWE

Shweta Agrawal, Anuja Modi, Anshu Yadav, Shota Yamada

Evasive LWE 仮定の解析に関する論文である。Evasive LWE 仮定は、格子暗号における強力だが不安定と見なされがちな難読化関連仮定と、安定だが表現力に限界のある標準的 LWE 仮定との中間に位置付けられる仮定として導入された。特に、Zeroizing Attack と呼ばれる、低ノルムの線形方程式を大量に取得することで秘密を回復する攻撃を回避する目的で設計されており、放送型暗号、witness encryption、属性ベース暗号などの高機能な格子ベース暗号構成に用いられてきた。

本論文では、公開コイン型および秘密コイン型の双方の Evasive LWE 仮定に対して、Zeroizing Attack に基づく具体的な反例が与えられた。公開コイン型については、事前条件における誤差ノルムが事後条件における誤差ノルムよりも大きい場合に、事後条件の分布から秘密に関する情報が回復可能であることが示された。この結果により、Hsieh、Lin、Luo による巡回的 Evasive LWE に基づく無制限深さ属性ベース暗号の基礎仮定が成立しないこ

とが示唆された。さらに、秘密コイン型 Evasive LWE に基づく暗号プリミティブについても解析が行われた。特に Agrawal、Kumari、Yamada による pseudorandom functionalities（PRFE）および obfuscation for pseudorandom functionalities（PRIO）、Branco らによる PRIO に対して解析が進み、既存構成の仮定に修正が必要であることが報告された。これらの結果から、Evasive LWE は Zeroizing Attack を完全に排除するものではなく、成立にはパラメータ制約や追加条件が不可欠であることが明確にされた。

E.12 Asiacrypt 2025

Lattice-based Multi-message Multi-recipient KEM/PKE with Malicious Security

Zeyu Liu, Katerina Sotiraki, Eran Tromer, Yunhao Wang

格子ベースのマルチメッセージ・マルチ受信者暗号方式への攻撃に関する論文である。

公開鍵暗号および鍵カプセル化機構では、特に耐量子計算機暗号において暗号文サイズが大きいことが実用上の問題となっている。この問題を緩和するため、複数受信者に対して暗号文サイズを平均化する mmPKE（multi-message multi-recipient PKE、mmPKE）および mmKEM が提案されてきた。しかし、既存の格子ベース mmPKE 方式では、受信者公開鍵が正しく生成されていることが暗黙に仮定されており、悪意ある公開鍵に対する耐性は十分に検討されていなかった。

本論文では、悪意をもって生成された受信者公開鍵を用いることで、既存の格子ベース mmPKE 方式の Semantic Security および鍵プライバシを破る具体的な攻撃が示された。これらの攻撃は本質的に検出不能である。さらに、悪意ある公開鍵が存在する状況下でも完全なプライバシを達成する、初の格子ベース mmKEM が提示された。100 受信者の場合、本方式の暗号文サイズは、Crystals–Kyber を単純に適用した場合よりも小さいことが示された。また、本 mmKEM を mmPKE に拡張することで、安全性と効率性の両面において従来方式を上回る構成が得られることが示された。提案方式は、Oracle Module–LWE 仮定の下で安全性が証明され、さらに MLWE からの還元が一部パラメータ領域で与えられている。

On the Provable Dual Attack for LWE by Modulus Switching

Hongyuan Qu, Guangwu Xu

本論文は、Learning With Errors（LWE）問題に基づく耐量子暗号方式への双対攻撃に関する論文である。LWE 問題は、Kyber や Dilithium などの標準化された耐量子暗号方式の安全性基盤として用いられている。従来の LWE 双対攻撃は、実用的には有効である一方で、ヒューリスティックな仮定に依存しており、厳密な成功条件の評価が困難であった。近年 Pouly らが Eurocrypt 2024 において導入した provable dual attack の枠組みはこの問題を解消したが、攻撃コストを削減するためのモジュロ計算における法切替（modulus switching）をどのように形式的に組み込むかは未解決の課題として残されていた。

本論文では、法切替と中国剰余定理を組み込んだ改良型 provable dual attack が導入された。著者らはポアソン和公式を用いて、実用上の誤差を除去する法切替機構を設計した。これは法切替に内在するノイズを有理格子に吸収させることで、LWE ノイズとの混合による攻撃失敗を防止するという工夫が施されている。さらに著者らは、任意の秘密鍵の分布に対して機能する鍵回復手法として、中国剰余定理を援用し、独立の部分攻撃から得られる部分的秘密から、秘密鍵を回復する手法を導入した。著者らはこの攻撃を評価するために、Banaszczyk の不等式の改良版を用いて、攻撃が成功するパラメータ範囲を理論的に特定した。結果として、元の provable dual attack フレームワークと比較して、

15〜29 ビットの攻撃性能向上が報告された。

Cryptanalysis on Lightweight Verifiable Homomorphic Encryption

Daehyun Jang, Jung Hee Cheon

検証可能準同型暗号方式への攻撃に関する論文である。外部委託計算においては、計算結果の正当性と入力データの秘匿性を同時に保証する必要があり、準同型暗号と検証可能計算を統合した検証可能準同型暗号（Verifiable Homomorphic Encryption、VHE）が重要な役割を果たしてきた。特に、Chatel ら（CCS 2024）によって提案された Replication Encoding（REP）および Polynomial Encoding（PE）は、暗号文内部に秘密情報を埋め込むことで、軽量な検証を可能にする設計として注目されていた。REP に類似した設計思想は、Albrecht ら（EUROCRYPT 2024）によって、検証可能な Oblivious PRF（vADDG）方式の構成にも用いられている。これらは暗号文内部に秘密情報を埋め込むことで、準同型評価の正当性を検証するという構造を持っている。

本論文では、REP、PE、および vADDG が採用する秘密情報埋め込み構造に対する体系的な暗号解析が行われ、検証可能性を破る効率的な偽造攻撃が構成された。REP および vADDG に対しては、入力暗号文から暗号化された形で秘密情報を抽出し、それを再利用することで、検証アルゴリズムに検出されない出力暗号文の偽造が可能であることが示された。PE に対しては、検証に用いられる入力に対しては整合的である一方で、検証可能性の定義を満たさない出力暗号文を生成できることが示された。さらに、vADDG に対しては、80 ビットの安全性パラメータ設定が、具体的には高々 10 ビットの安全性しか提供しないことが定量的に示された。加えて、完全準同型暗号を用いる設定では、REP および PE に対する攻撃が線形時間で成功確率 1 を達成することが示され、軽量検証可能準同型暗号方式における設計指針の再検討が必要であることが報告された。

A search to distinguish reduction for the isomorphism problem on direct sum lattices

Daniël van Gent, Wessel van Woerde

HAWK の安全性の根拠となる、格子同型問題（Lattice Isomorphism Problem、LIP）の解析に関する論文である。格子同型問題には、二つの格子が等長同型であるかを判定する distinguish 問題と、実際にその等長写像を求める search 問題が存在する。Eurocrypt 2003 において Szydlo は、整数格子 $\mathbb{Z}^n$ を対象として、search 問題が distinguish 問題に帰着可能であることを示した。その後、暗号方式では、より一般の構造を持つ直和格子や数体上の加群格子が用いられるようになったが、これらに対して同様の search-to-distinguish 還元が成立するかどうかは明らかではなかった。

本論文では、固定された任意の base lattice Γ について、search-to-distinguish 還元が、Γ^n と同型な任意の格子を対象として一般化できることが示された。ここで base lattice は本論文で新しく導入された概念である（Definition 3.5）が、これは数体 K の整数環 $\mathcal{O}_K$ を含む広いクラスである。特に著者らは、$\Gamma = \mathcal{O}_K$ であるとき、還元は n に関して多項式時間で実行可能であることを示した（Theorem 7.3）。特に、 Module-LIP に基づく署名方式 HAWK において用いられる、円分体 $K = \mathbb{Q}(\zeta_{2^{\ell-1}})$ 上の格子 $\mathcal{O}_K^2$ については、distinguish オラクルを高々 $2d^2$ 回呼ぶことで search 問題が解かれることが示されている（Theorem 10.3）。ここで $d = 2^{\ell-1}$ は $\mathcal{O}_K$ の整環としての次数である。

Improved Cryptanalysis of SNOVA by Solving Multi-homogeneous Systems via Matrix Transformations

Hiroki Furue, Yasuhiko Ikematsu, Shuhei Nakamura, Rika Akiyama

SNOVA 署名方式への鍵回復攻撃に関する論文である。SNOVA は、非可換環上で構成された不均衡 Oil and Vinegar の変種として構成された、多変数系に基づく署名方式である。本方式は、NIST による耐量子計算機暗号標準化プロセスにおける追加署名方式の第 2 ラウンド候補の 1 つとして選定されており、その高い効率性とコンパクトさから大きな注目を集めている。SNOVA に対してはこれまでに様々な安全性解析が行われており、拡大体の構造を利用することで攻撃の効率を向上させた研究も存在する。特に Cabarcas らは、拡大体上に変換された公開鍵から導かれる多重同次（multi-homogeneous）構造を利用することで、偽造攻撃および再調整（reconciliation）攻撃をより効率的に実行できることを示した。しかしながら、拡大体上の多重同次構造を用いることで、他の鍵回復攻撃についても改良が可能であるかどうかは明らかになっていなかった。

本論文では、SNOVA の公開鍵を拡大体上へ写す変換が、具体的な行列変換として定式化され、その結果得られる行列が多重同次構造を持つことが示された。この構造を利用することで、従来は UOV に対して知られていた intersection 攻撃および rectangular MinRank 攻撃が、SNOVA に対しても多重同次系を解く問題として適用可能であることが示された。さらに、rectangular MinRank 攻撃において用いられる support minors 法を、多重同次 MinRank 問題に拡張し、その解次数（solving degree）が解析された。その結果、いくつかの SNOVA パラメータに対して、提案された intersection 攻撃および rectangular MinRank 攻撃の計算量が、既存の既知攻撃よりも小さくなることが示された。特に、パラメータ $(16, 29, 6, 5)$ に対しては、提案された rectangular MinRank 攻撃の計算量が、当該パラメータに主張されている安全性レベルの基準を満たさないことが定量的に示された。

The Order of Hashing in Fiat-Shamir Schemes

Barbara Jiabao Benedikt, Marc Fischlin

Fiat–Shamir 署名方式への攻撃に関する論文である。Fiat–Shamir 変換は、対話型識別プロトコルを非対話型署名方式へと変換するための基本的手法であり、Schnorr 署名や CRYSTALS-Dilithium など、多くの実用的署名方式に採用されている。理論的解析においては、ハッシュ関数は単一のランダムオラクルとしてモデル化されることが一般的であり、その入力順序は本質的な問題とはみなされてこなかった。しかし、実際の実装では、Merkle–Damgård 構造やスポンジ構造に基づくハッシュ関数が用いられており、入力順序やハッシュの構成方法が、内部状態の露出や再利用に影響を及ぼす可能性がある。そのため、Fiat–Shamir 署名におけるハッシュ入力順序が、攻撃耐性の観点からどのような影響を持つかを体系的に理解する必要があった。

本論文では、Merkle–Damgård 構造およびスポンジ構造に基づくハッシュ関数を用いた Fiat–Shamir 署名について、平坦なハッシュおよび入れ子状ハッシュの双方が、古典的設定および量子的設定において解析された。著者らはその過程で、Eaton–Stebila（PQCrypto 2021）による”quantum annoyance”の考え方に従い、「単一の署名偽造に成功した攻撃を、複数ユーザへの攻撃や単一ユーザに対する複数回の偽造へと拡張することの困難性」を定式化する新たな安全性概念 ”annoyance for user exposure and signature forgeries” を導入された。この解析に基づき、Fiat–Shamir 署名においては、コミットメントをメッセージよりも先にハッシュすることで、不適切なハッシュ順序に起因する攻撃の可能性が排除されることが示された。一方で、コミットメントとメッセージ以外の入力については、安全性に本質的な影響を与えないため、任意の順序で配置してよいことが明らかにされた。

On the Concrete Security of BBS/BBS+ Signatures

Rutchathon Chairattana-Apirom, Stefano Tessaro

BBS および BBS+ 署名方式の安全性に関する論文である。BBS および BBS+ 署名は、実用的かつ軽量な匿名クレデンシャル（anonymous credential）を実現するための有望な署名形式として広く用いられており、W3C および IRTF による標準化の取り組みの基盤となっている。これらの方式の安全性は、これまで主に q-SDH 仮定からの安全性帰着によって評価されてきたが、その帰着は具体的安全性（concrete security）の観点では必ずしも厳密ではなく、実際には「より安全なのではないか」という可能性が指摘されていた。実際、q-SDH 仮定は、いくつかの q の選択に対して、$O(\sqrt{p/q})$ 回の群指数演算を用いる攻撃（Cheon、EUROCRYPT 2006）を受けることが知られている一方で、BBS+ および決定論的 BBS に対しては、同様の計算量を持つ攻撃は知られていなかった。

本論文では、BBS+ および決定論的 BBS に対して、新たな秘密鍵回復攻撃が構成され、q 個の署名を観測した後に、$\Theta(q)$-離散対数問題を解くのと同等の計算量で秘密鍵が回復可能であることが示された。この結果により、多くの q の選択に対して、攻撃計算量が $O(\sqrt{p/q})$ に比例することが定量的に示され、「より安全なのではないか」という期待を否定的に解決している。さらにこの攻撃を用いて、BBS+ および決定論的 BBS の安全性が $\Theta(q)$-SDH 仮定を含意することを示す安全性帰着が与えられた。

Solving Concealed ILWE and its Application for Breaking Masked Dilithium

Simon Damm, Asja Fischer, Alexander May, Soundes Marzougui, Leander Schwarz, Henning Seidler, Jean-Pierre Seifert, Jonas Thietke, Vincent Quentin Ulitzsch

マスク化された Dilithium 署名実装へのサイドチャネル攻撃に関する論文である。Dilithium は、整数 LWE サンプルを用いて秘密鍵に関する知識をゼロ知識的に証明する格子ベース署名方式である。ゼロ知識性を保証する棄却サンプリングの存在により、理想的には、多数の署名から秘密鍵を回復することは困難である。しかし、実装に対するサイドチャネル攻撃では、誤差項に関する部分的な情報が漏洩し、標準的な整数 LWE（Integer Learning With Errors、ILWE）仮定の前提が崩れることが知られていた。

本論文では、Concealed ILWE （CILWE）と呼ばれる新しい問題設定が導入された。この変種では ILWE サンプルの一部のみがゼロ知識であり、この割合を concealment rate と呼ぶ。この状況は、格子ベース署名に対するサイドチャネル攻撃において自然に現れる。具体例として、Dilithium 実装に対するプロファイリングサイドチャネル攻撃では、誤差があるかないかを判定することができるため、誤差がない場合は ILWE サンプルが、ある場合には通常のゼロ知識 ILWE サンプルが得られる。著者らは、従来用いられてきた最小二乗法は、concealment rate が小さい場合であっても実用的でないこと、そして整数線形計画に基づく既存手法も、理論保証の欠如および小さな独立誤差を活用できないという理由から不十分であることを指摘している。そのうえで本論文では、Huber 回帰および Cauchy 回帰を用いる統計的手法が導入され、concealment rate が 90% に達する場合でも秘密鍵回復が可能であることが示された。これらの手法を用いることで、従来回復不可能であった鍵回復を実現するマスク化された Dilithium 実装に対する新しいプロファイリング攻撃を達成している。

The Security of ML-DSA against Fault-Injection Attacks

Haruhisa Kosuge, Keita Xagawa

NIST 標準署名方式である ML-DSA へのフォールト注入攻撃に関する論文である。耐量子暗号として提案・標準化が進められてきた格子ベース署名方式においては、署名生成時に用いられる乱数の品質が安全性に直接影響することが知られている。そのため、乱数生成の不備を回避する目的で決定論的署名やヘッジ付き（hedge）乱数生成が導入されてきた。ヘッジ付き乱数生成では、疑似乱数関数がメッセージとナンスの両方を入力として受け取る。Aranha らは、EUROCRYPT 2020 において、ヘッジ付き Fiat–Shamir 署名の 1 ビットフォールトに対する安全性を調査し、特定の種類のビット改ざんフォールトに対する安全性を示している。さらに Grilo らは、ASIACRYPT 2021 において、この証明を量子ランダムオラクルモデルへと拡張した。昨年、NIST は、ヘッジ付き Fiat–Shamir with aborts を採用した格子ベース署名方式 ML-DSA を標準化した。一方で、実装レベルではフォールト注入攻撃が現実的な脅威となっており、特に署名アルゴリズムの内部状態や中間計算に対するビット改ざんが、秘密鍵漏洩や偽造につながる可能性が指摘されてきた。先行研究では、ヘッジ付き Fiat–Shamir 構造に対して限定的なフォールトモデル下での安全性が示されていたものの、NIST により標準化された ML-DSA に対しては、既存の証明手法が直接適用できない状況にあった。

本論文では、ML-DSA に対するマルチビットフォールト注入攻撃を対象として安全性解析が行われた。具体的には、内部関数の入力および出力に注入される特定のクラスのフォールトについて、それらが署名の安全性を損なわず、攻撃者によって悪用できないことが形式的に示された。これにより、Aranha らによって未解決として残されていた、ヘッジ付き Fiat–Shamir with aborts を採用する署名方式に対するフォールト耐性の問題に対して、理論的な解決が与えられた。一方で、より強力なフォールト耐性を期待することが困難であることを示すため、内部計算の他の中間点にフォールトが注入された場合に成立する鍵回復攻撃が新たに提示された。これらの結果から、ML-DSA においては、入力・出力レベルのフォールトに対しては安全性が保証される一方で、中間状態に対するフォールト注入に対しては、本質的な限界が存在することが示された。

Practical cryptanalysis of pseudorandom correlation generators based on quasi-Abelian syndrome decoding

Charles Bouillaguet, Claire Delaplace, Mickael Hamdad, Damien Vergnaud

準可換シンドローム復号（Quasi-Abelian Syndrome Decoding、QA-SD）問題の困難性に基づく暗号学的疑似相関生成器（PCG: pseudorandom correlation generator）の安全性に関連する論文である。

MPC による秘匿計算では、一般に加算よりも乗算の方がコストが高い。この課題を解決するため、[Beaver, Crypto91] により乗算をオフラインフェーズとオンラインフェーズに分けて処理する効率的な方法が提案された。このときのオフラインフェーズでは、Beaver triple と呼ばれる $ab = c$ を満たす三つ組み (a, b, c) のシェアを各参加者に配布する。Beaver triple はランダム性を持つ必要があり、本論文では Oblivious Linear Evaluation (OLE) correlations と呼ばれる $x_0x_1 = z_0 + z_1$ を満たす (x_0, z_0) と (x_1, z_1) の組を用いての生成が想定されている。

[Bombar ら, CRYPTO 2023, Asiacrypt 2024] は任意の有限体上での OLE 生成のため、プログラマブル PCG（変数の一部を固定した状態で他の変数を生成可能な PCG）と呼ばれるプリミティブを QA-SD 問題の困難性から構成している。また、プログラマブル PCG を用いて特に小標数の有限体上での Beaver triple の生成、参加者間でのシェア生成を行う F_4OLEAGE プロトコルを提案している。

QA-SD 問題は環 $R = \mathbb{F}_q[X_1, \ldots, X_n]/(X_1^d - 1, \ldots, X_n^d - 1), d = q - 1$ 上の計算問題であり、LWE 問題、LPN 問

題と類似の形式を持つ。公開されたランダムな $a_1, \ldots, a_{c-1} \in R$ と $\sigma = e_0 + \sum_{i=1}^{c-1} a_i e_i$ に対して、それぞれが t 個の項からなるスパースな多項式 $e_0, \ldots, e_{c-1}$ を復元する計算問題である。LWE 問題と同様に、探索版は e_i の復元が目的であり、判定版はこの σ がスパース多項式 e_i を使って計算されたものか、一様ランダムな R の元なのかを判定する問題である。

本論文では、QA-SD 問題を小標数の有限体上におけるスパース多項式の補間問題に帰着可能であることを示す。具体的には、方程式 $a_1(x) = \cdots = a_{c-1}(x) = 0$ を満たす点 $x \in R$ に対しては $\sigma(x) = e_0(x)$ となることから、有限個の $e_0(x)$ の値からスパース多項式 e_0 を復元する。$e_0(x)$ が復元できれば $\sigma(x) - e_(x)$ の値を $a_2(x) = \cdots = a_{c-1}(x) = 0$ を満たす点で評価・補間することで多項式 $e_1(x)$ が復元可能であり同様にして全ての多項式が復元可能となる。特に、多項式を構成する項の数が非常に少ない場合には $e_0 = \sum_{j=0}^{d-1} X_i^j P_j$ のような分解を考えると、各 P_j の項数が 2 以下である可能性が高い。このような場合には代入後に単純な線型方程式を解くか、因数分解により復元が可能であり、アルゴリズムの高速化が可能である。

さらに論文では、有限体上の多項式を 1 の $(q-1)$ 乗根による持ち上げ写像により $\mathbb{C}$ 上の多変数多項式として取り扱うことで多項式の補間問題を二次錐計画問題（SCOP: second-order cone programming）へと変換可能なことが示され、ソルバーを用いた数値実験が行われた。Bombar らの元論文 [CRYPTO 2023] に用いられた提案パラメータに対して、数時間程度、300GB 程度のメモリ消費で判定版問題の識別が可能であると報告している。特に、F_4OLEAGE[Asiacrypt 2024] のパラメータに対しては 1056CPU 時間で 60% 程度のアドバンテージ得られるとしている。

また、後続研究 [Li et al., Eurocrypt 2025] にて提案されているパラメータのいくつかに対しては分解 $e_0 = \sum_{j=0}^{d-1} X_i^j P_j$ の中で項数 2 以下になる多項式が複数存在し、元論文で 128 ビットセキュリティとされていたものが 24 時間以内に解けてしまったものの、他のいくつかのパラメータに対しては 1 週間で計算が終わらなかったもの、メモリ不足で計算が完了しなかったものがあったと報告されている。

対策として、単純にパラメータを大きくすることが効果的であると考えられるものの、プリミティブの効率が落ちることから、攻撃の出発点となる $a_1(x) = 0$ となる根を持たないような多項式を用いることに一定の効果があるのではないかと述べている。

Fast Slicer for Batch-CVP: Making Lattice Hybrid Attacks Practical

Alexandr Karenin, Elena Kirshanova, Alexander May, Julian Nowakowski

格子暗号の安全性の根拠となる LWE 問題および BDD 問題の古典計算量評価に関する論文である。NIST PQC 標準化方式である ML-KEM(CRYSTALS-Kyber) と第 3 ラウンド候補である NTRU の安全性に関わる。

LWE 問題の計算量評価では Kannan 埋め込みを用いた Primal 攻撃を用いたものがデファクトスタンダードとされている。暗号に関わる計算量評価では問題を uSVP に帰着し、最短ベクトルを求めるために必要な BKZ のブロックサイズ d の最小値に対応する篩アルゴリズムの計算量 $O(2^{0.292d})$ が用いられてきた。一方で、[Bernstein, ePrint 2023/1892] では Espitau と Kirchner のアイデアに基づいた Randomized Slicer による攻撃が漸近的に Primal 攻撃の計算量を下回る可能性が示唆されていた。Randomized Slicer による攻撃はハイブリッド攻撃の一種であり、LWE,BDD のインスタンスにおける秘密ベクトル、エラーベクトルの範囲が限られている場合にはいくつかの成分を固定することで、低次元での同じ格子に対する複数の CVP へと帰着される。このとき、複数の CVP がほぼ 1 回分の CVP 処理の計算量で実行可能であるかどうかが暗号学的に重要な課題として取り上げられていたものの、それを実現する Randomized Slicer が効率的に実装可能であるかどうかが不明であった。

本論文では、効率的な Slicer の実装とそれに基づく Bernstein のハイブリッド攻撃の LWE、BDD への一般化が与

えられている。エラー分布の各成分を $\mathcal{D}$ から独立にサンプリングした探索問題に対して、漸近的な攻撃計算量が既存の篩アルゴリズムによる $T = 2^{\Theta(d)}$ から $T^{1-K}, K \approx (1 + \frac{H(\mathcal{D})}{0.058})^{-1}$ へと下がると解析されている。ただし、$H(\mathcal{D})$ はシャノンエントロピーである。Kyber で用いられる中心二項分布 $B(3)$ ではエントロピーは約 2.33 であり、K の改善は 0.020 から 0.024 程度に留まるため、漸近的には改善があるものの、実用次元でどの程度効くかは実装で確認する必要があるとしている。また、Regev の元の LWE のように誤差分布のエントロピーが大きい場合には、hybrid attack による漸近的な改善は本質的に得られないと分析している。

計算機実験では BDD に対するアルゴリズムの比較として Randomized Slicer 単体と Babai の最近平面アルゴリズムの実験を行い、特に近似係数 $\gamma < 1$ が 1 に近い場合には前者の方が格子点の発見確率が高くなる報告している。

Primal 攻撃との比較では NTRU で用いられる ternary error ベクトルおよび Kyber で用いられる中心二項分布のエラーベクトルを用いた 200 次元程度のサンプル問題を用いて実験したところ、提案手法の方が 3 から 4.5 倍程度高速であったと報告されている。

結論として、Kyber や NTRU の実パラメータを破る攻撃を示すものではなく、計算量の改善があったとしても数倍程度であると考えられるものの、篩アルゴリズムで用いられているいくつかの改良手法と組み合わせることでさらなる解読計算量の低下の可能性がある。また、実装上も Randomized Slicer の GPU 実装や、G6K の on-the-fly lifting を導入することでさらに高速化する可能性があるとしている。

実験用コードは `https://github.com/ElenaKirshanova/g6k_hybrid/tree/ac_artifact` にて公開されている。

Predicting Module-Lattice Reduction

Léo Ducas, Lynn Engelberts, Paola de Perthuis

モジュール格子簡約を用いた格子暗号への攻撃に関する論文である。Kyber をはじめとするモジュール格子ベース暗号方式の安全性評価において、モジュール構造を利用した格子簡約が、非構造格子簡約と比較してどの程度有利であるかは、具体的安全性を左右する重要な問いであり、Kyber の NIST 標準化提出文書（Avanzi ら、2021）において「Q8」として強調されている。モジュール格子簡約に関する基礎的研究（Lee、Pellet-Mary、Stehlé、Wallet、ASIACRYPT 2019；Mukherjee、Stephens-Davidowitz、CRYPTO 2020）により、LLL やブロック簡約アルゴリズムのモジュール版が存在することは確認されてきたが、それらは証明可能な最悪時の漸近的挙動に焦点を当てるにとどまっていた。

本論文では、module-BKZ を適用した際の基底スロープの平均時挙動が解析され、数体 K の判別式 Δ_K がその主要な支配因子であることが示された。この解析により、ブロックサイズを β として、次数 d の数体 K における module-BKZ は、非構造 BKZ と同じスロープに到達するために、次元

$$\beta + \frac{\log(|\Delta_K|/d^d)}{d\log\beta}\beta + o\left(\frac{\beta}{\log\beta}\right)$$

の SVP オラクルを必要とすることが示された。さらに、2 の冪の巡回体では module-BKZ が不利となり、より大きなブロックサイズを要する一方で、それ以外の巡回体では劣線形のブロックサイズ削減が得られ、 $\exp(\tilde{O}(\beta/d))$ の準指数的な高速化が生じることが定量的に示された。

A Hybrid Algorithm for the Regular Syndrome Decoding Problem

Tianrui Wang, Anyu Wang, Kang Yang, Hanlin Liu, Yu Yu, Jun Zhang, Xiaoyun Wang

正則シンドローム復号問題（RSD）への攻撃に関する論文である。符号理論に基づく暗号構成において、シンドローム復号問題（SD）は中心的な計算困難性仮定として用いられており、その変種である正則シンドローム復号（RSD）は、誤りベクトルがブロック構造を持つという追加制約を特徴とする。この構造は、MPC、ゼロ知識証明、および OT プロトコルなどの実用的暗号方式において自然に現れるため、RSD に対する具体的安全性評価は重要な課題となっていた。従来、RSD に対する攻撃手法としては、Information Set Decoding（ISD）に基づく手法と、方程式系を解く代数的手法が主に検討されてきたが、それぞれ計算量や適用可能なパラメータ領域に制約が存在していた。

本論文では、ISD における meet-in-the-middle 列挙を二次方程式の解法で置き換える新しいハイブリッド攻撃アルゴリズムが導入された。この手法により、位数 $q = 2^{128}$ の体および二元体 $q = 2$ の双方において、既存の ISD 手法および代数的手法よりも低い計算量で RSD を解けることが示された。具体的には、既存研究で用いられていたパラメータ集合に対して、RSD の具体的安全性が最大で 20 ビット低下することが定量的に示された。さらに、二元体上において、RSD が多項式時間で解けるパラメータ領域が、従来の手法と比較して拡大されることが漸近解析によって示された。加えて、本アルゴリズムを Wolverine および Ferret に適用した結果、128 ビット安全性を目標としていた Wolverine の安全性が約 111 ビットに低下し、Ferret についても安全性が目標値をわずかに下回ることが示され、実用プロトコルに対する影響が定量的に明らかにされた。

A Complete Characterization of One-More Assumptions in the Algebraic Group Model

Jake Januzelli, Jiayu Xu

one-more 仮定に基づく暗号プリミティブへの攻撃に関する論文である。ブラインド署名、oblivious PRF、および非対称 PAKE などの対話的暗号プリミティブでは、One-More Discrete Logarithm（OMDL）や One-More Diffie–Hellman（OMDH）といった one-more 問題に基づいて安全性が定式化されることが多い。さらに、OMDH を一般化した Threshold OMDH（TOMDH）は、対話的プロトコルのしきい値版を構成するために有用であることが示されている。しかし、これらの仮定は構造が複雑であり、実際の困難性を評価することは容易ではないため、Generic Group Model や Algebraic Group Model といった理想化モデルにおいて解析が行われてきた。

本論文では、Algebraic Group Model において、既存の群ベース one-more 問題が Q-DL 仮定（Bauer–Fuchsbauer–Loss、CRYPTO 2020）の階層を用いて完全に特徴付けられた。その結果として、（T）OMDH が Q-DL 階層に属すること、特に Q-OMDH は Q-DL と等価が示された。これは従来存在していた TOMDH の困難性証明の欠陥の修正を与える。また、q-OMDL 問題が無限の階層を形成し、相互に比較不能であることが示された。これらの理論的結果に基づき、OPAQUE 非対称 PAKE に対する最良既知攻撃が Cheon（EUROCRYPT 2006）によるものであることに対する形式的根拠が与えられ、さらに、TOMDH に依拠するしきい値暗号方式が、非しきい値版と同等の具体的安全性を有することが示された。

On Wagner's k-Tree Algorithm Over Integers

Haoxing Lin, Prashant Nalini Vasudevan

k-SUM 問題の解析に用いられる、k-Tree アルゴリズムに関する論文である。k-SUM 問題は、「絶対値が $m/2$ 以下の整数による長さ n の順列が k 個与えられたとき、和が 0 になるように各順列から一つの元を選ぶ」という問題であ

り、いくつかの署名技術、ハッシュ関数、共通鍵暗号などを解読する一つのアプローチとして還元できる問題の一つである。Wagner により導入された k-Tree アルゴリズムは、k-SUM 問題を効率的に解くための手法である。この手法は Wagner 自身がヒューリスティックな解析を与えており、$n \approx m^{1/(\log k+1)}$ のときに定数確率で成功し、その場合の計算量は $O(kn)$ であると示唆された。その後も厳密解析が進み（Lyubashevsky 2005、Shallue 2008、Joux – Kippen – Loss 2024）、順列の長さ n が十分大きい場合に高い成功確率を与えることが示されていた。

本論文では、入力順列サイズ n の任意の設定に対して、k-Tree アルゴリズムの成功確率および計算量に関する上界と下界が与えられた。その結果、Wagner のヒューリスティックな結論が厳密な解析によって裏付けられた。また、既存研究では扱われていなかった広いパラメータ領域に対しても漸近的にタイトな評価が示された。さらに、具体的なパラメータに対して、理論的に正しい評価境界を効率的に計算するアルゴリズムも提示し、そのタイトな評価を検証するための実験をも与えている。著者らは、同様の解析を有限体上の k-Tree アルゴリズムについても行っている。

Understanding Unexpected Fixed-Key Differential Behaviours: How to Avoid Major Weaknesses in Lightweight Designs

Anne Canteaut, Merlin Fruchon

共通鍵暗号の差分解析に関する研究である。共通鍵暗号分野における多くの設計戦略や差分解析は、いわゆる確率的等価性と呼ばれる仮説に依存している。この仮説は、任意の固定鍵に対する差分挙動が、全ての鍵にわたる平均的な差分挙動に近似できる、というものである。しかし、この仮説は実際には成立しないことが知られている。例えば、AES における全ての 2 段差分特性はプラトー特性を持ち、その成立確率が鍵に強く依存することが知られている。従来、この種の不整合は少数段の場合にのみ生じると考えられてきたが、近年では準差分（quasi-differential）フレームワークの導入によって、多数段においても反例が示されている。

本研究の目的は、個々の差分特性ではなく、差分解析において重要となる差分（入力差分と出力差分の組）を解析対象とした場合に、固定鍵下での差分挙動と全鍵平均的な差分挙動の乖離がどのように拡大するかについて明らかにすることである。この目的のために、本研究では、プラトー特性および準差分フレームワークの概念に基づき、非線形層における差分挙動（例えば、super-planar differential や perfect square differential）や線形層の構造的特徴に着目した理論解析を行った。さらに、切り詰め差分解析など、確率的等価性仮説を満たさない多数の特性を集約した差分を考える場合において、弱鍵空間が特性間で一致する条件と分離される条件を理論的に導出し、固定鍵下でのクラスタリング効果の有無を判別可能にした。具体的には、全ての特性において弱鍵集合が共通である場合には強いクラスタリング効果が現れる一方で、特性ごとに弱鍵集合が完全に互いに素である場合にはクラスタリング効果は完全に打ち消されることを明らかにした。

提案手法はブロック暗号 Midori64、Scream、iScream に適用された。Midori64 および Scream では、「任意のラウンド数に対して成立する固定鍵切り詰め差分が存在する」という既知の脆弱性が、単一の異常な特性によって生じるものではなく、多数のプラトー特性が同一の弱鍵空間に対して同時に成立する。つまり強いクラスタリング効果が現れることによって生じることを明らかにした。一方で、iScream の場合にも類似の差分挙動が存在するものの、集約対象となる個々の特性ごとに弱鍵空間が異なる、つまり固定鍵下でのクラスタリング効果が打ち消されるため、ラウンド数の増加とともに差分確率が急激に低下することを明らかにした。さらに、最適な 4 ビット S-box を網羅的に解析し、この種の脆弱性を引き起こす S-box の性質を特定した。

Vectorial Fast Correlation Attacks

Bin Zhang, Ruitao Liu, Willi Meier, Siwei Sun, Dengguo Feng, Wenling Wu

LFSR 型ストリーム暗号に対する高速相関攻撃の拡張に関する研究である。従来の高速相関攻撃は、主としてビット単位の相関を対象とし、LFSR における初期状態の復元問題を低レート線形符号の復号問題として扱う。一方で、実際の暗号プリミティブでは、非線形フィルタと複数の内部状態が相互に結合した構造を有しているため、相関値が単一の線形近似に集中するのではなく、多数の線形近似に分散して現れる。それゆえに、最大相関値のみを利用する従来の攻撃手法では、攻撃に利用可能な情報の大部分が切り捨てられてしまうという課題があった。2005 年に、Golić らは複数の線形近似を同時に扱うベクトル型高速相関攻撃を提案したが、理論的な計算量評価が不十分であり、実用暗号への適用可能性については未解決のままであった。

これらの課題を解決するために、本研究では、ベクトル型高速相関攻撃に対する新しい理論的枠組みを構築した。まず、相関プロファイルという概念を導入した。これは、線形近似の相関値だけでなく、その相関値を持つ線形近似の個数を同時に評価するという概念であり、従来手法では捉えられなかった相関構造を体系的に表現することを可能にした。この新しい概念に基づき、多数の線形近似を線型空間として結合し、ベクトル全体としての相関容量を最大化する攻撃ベクトルの構成法を示した。次に、FSE 2024 で提案されたコードリダクション技術をベクトル設定へと一般化し、相関値を保持したまま秘密情報をより低次元の線形部分空間へと写像できるようにした。さらに、得られたベクトル型近似線形系を拡大体上のランダム線形符号の復号問題として定式化し、多次元高速フーリエ変換を用いる効率的な復号アルゴリズムを提案した。結果として、従来は NP 困難とみなされていた問題に対して実用的な計算量評価が可能となった。加えて、Grain 系ストリーム暗号の解析において未解決であった出力マスク検出問題に対し、従来の MILP 手法に依存しない、グラフ理論に基づく新しい手法を提案した。

提案手法の有効性は、Grain-128a、Grain v1、Sosemanuk という実用ストリーム暗号への適用によって実証された。Grain-128a に対しては、$2^{106.3}$ ビットのキーストリームを用いることで、計算量 $2^{107.7}$ の内部状態復元攻撃を実現した。Grain v1 に対しては、$2^{67.0}$ ビットのキーストリームで、計算量 $2^{69.6}$ の攻撃が可能である。これらはいずれも、Crypto 2018 における最良の結果と比べて、2^{12} 倍の改善となった。また、Sosemanuk に対しては、提案手法と従来の assign-and-solve 戦略と組み合わせることで、128 ビット鍵に対する全数探索よりも高速な情報漏洩型攻撃を初めて示した。

Persistence of Hourglass(-like) Structure: Improved Differential-Linear Distinguishers for Several ARX Ciphers

Xinxin Gong, Qingju Wang, Yonglin Hao, Lin Jiao, and Xichao Hu

ARX（Addition–Rotation–XOR）暗号の差分線形（DL: Differential-Linear）解析に関する研究である。近年、ARX 暗号に対する DL 識別子の構成に関して、MILP を用いた自動探索手法や理論的相関評価手法の発展により、従来よりも長いラウンド数に対する解析結果が報告されるようになった。しかし、得られた DL 識別子は、探索や評価の枠組みに強く依存して個別に導出されており、これらの枠組みによって得られた識別子同士の対応関係や、高い相関値を与える構造については十分に整理されていなかった。また、相関評価における独立性仮定や探索空間の著しい増加により、評価精度や計算効率の面でも課題が残されていた。

本研究の目的は、ARX 暗号に対する DL 識別子を構造的観点から統一的に理解し、高い相関値を有する識別子を体系的に構成可能な枠組みを提供することにある。そのために、Speck、Alzette、SipHash、Chaskey などの様々な ARX

暗号に対して、既存研究で報告されている最良の DL 識別子を詳細に分析した。その結果、これらの識別子が、中間ラウンド部分で差分や線形マスクが疎となり、それらが前後方向に向かって拡散するような砂時計型（hourglass-like）構造を有しているという、構造的共通性を明らかにした。この知見に基づき、本研究では、DL 識別子を前半の差分部、中間の DL 部、後半の線形部へと再分解する体系的手法を導入し、砂時計型構造を構成目標とした DL 識別子構成手法を新たに提案した。DL 近似の分解と再構成を通じて探索空間を整理し、明らかに高い相関値を有していない候補を早期に除外することで、効率的な識別子の探索を可能にした。

提案手法により、複数の ARX 暗号に対して既存結果を上回る DL 識別子の構成に成功した。具体的には、Alzette に対して、14 ラウンドまでの DL 識別子を初めて構成し、いずれも理論相関評価および実験的検証の双方によって有効性を確認した。Speck に関して、11 ラウンドの Speck32、12 ラウンドの Speck48、16 ラウンドの Speck96 に対する有効な DL 識別子を初めて示し、実験的に検証可能なデータ量および現実的な計算量で識別子が成立することを確認した。SipHash-2-4 に対しては、相関値が ± 1 の決定的な 3 ラウンド DL 識別子を構成するとともに、4 ラウンド DL 識別子の相関値を大幅に改善した。加えて、7/7.25 ラウンドの ChaCha、8 ラウンドの Salsa、5.5 ラウンドの Forró に対しても評価し、既存結果よりも低い計算量およびデータ量で識別子を構成できることを示した。

Enhancing the DATF Technique in Differential-Linear Cryptanalysis

Cheng Che, Tian Tian

共通鍵暗号の汎用的な差分線形解析に関する研究である。差分線形解析において、差分線形接続表やその拡張手法が主流となっているが、これらは表構築に基づく手法であるため、S-box を多用する暗号やビット指向の暗号に対して、計算量・メモリ量の観点で適用が困難となる場合が多いという問題があった。一方、DATF（Differential Algebraic Transitional Form）と呼ばれる技術では代数的手法に基づくものであり、表を必要としないという利点があるものの、従来手法では差分線形バイアスの推定精度が低く、バイアス計算および識別子探索の計算量が膨大になってしまうという問題が残されていた。

本研究では、DATF に基づく差分線形解析において、(1) 差分線形バイアスの推定精度の向上、(2) 多変数ブール関数に対するバイアス計算の高速化、(3) 大きなバイアスを有する差分線形識別子の効率的な探索、の三点を主要な研究課題として設定した。これらの課題を解決するために、まず、新たな遷移規則、バックトラッキング戦略、および分割技法を導入することで、遷移変数間の依存関係を適切に扱うことで、差分線形バイアスの推定精度を向上させた。次に、変数の値を固定することで出力の偏りが消失するケースを検出し、計算を早期に打ち切る新しいバイアス計算手法を提案した。これにより、従来の全数探索と比較して、計算量を数十倍から数百倍の削減に成功した。さらに、出力に対して単独で影響を与える変数を指標として用い、その偏りが小さい場合には候補全体を削除することで、差分線形識別子の探索を大幅に高速化した。

提案手法を Ascon、Serpent、Xoodyak、および Grain v1 に適用し、その有効性を検証した。Ascon に対しては、既存研究で主張されていた 6 ラウンド差分線形識別子が有効でないことを明らかにした上で、実際に有効な 6 ラウンド（条件付き）差分線形識別子を構成し、この識別子に基づく鍵回復攻撃を、既存手法よりも低い計算量とデータ量で実現した。Serpent、Xoodyak、および Grain v1 に対しても同様に、既存結果の更新を達成した。

Integral cryptanalysis in characteristic p

Tim Beyne, Michiel Verbauwhede

有限体および有限環上で定義された共通鍵暗号プリミティブに対する積分攻撃の枠組みを提案した論文である。従来の積分攻撃は、主として $\mathbb{F}_2^n$ のような 2 元体上の構造を対象として発展してきた。一方で近年は、素数 p のべき乗 q についての $\mathbb{F}_q^n$ や、標数 p の有限環上で動作する暗号プリミティブが設計されており、それらに対して従来手法を直接適用することは困難であった。このため、より一般の代数構造に対応した体系的な積分攻撃の枠組みが求められていた。

本論文では、積分攻撃および超距離的積分攻撃（ultrametric integral cryptanalysis）が、体の直積に同型な標数 p の有限環へと一般化されたことが報告されている。今までの標数 2 での解析を大きな標数上でも実用的に行うため、例えば Boura–Canteaut によって導入された parity set のアナロジーとして凸多面体を用いるといった新着想が導入されている。著者らはこれらの手法を自動的に適用するツールを構築し、Feistel-GMiMC、HadesMiMC、AES-Prime、small-pSquare、mid-pSquare といった具体的な共通鍵暗号プリミティブに対して解析を行った。その結果、最大の代数次数（maximal degree、暗号化関数を多項式写像として表した時の次数）の見積りが過度に楽観的であることが示され、特に AES-Prime を除く各プリミティブにおいては、設計時に想定された安全性基準を満たすためにはラウンド数を大幅に増加させる必要があることが報告されている。これらの評価は、標数 p における積分的性質を厳密に考慮した解析に基づいて与えられている。

SPEEDY: Caught at Last

Christina Boura, Patrick Derbez, Baptiste Germon, Rachelle Heim Boissier, Maria Naya-Plasencia

SPEEDY ブロック暗号の安全性評価に関する論文である。SPEEDY は、超低遅延を目的として設計されたブロック暗号ファミリである。完全 7 ラウンド版である SPEEDY-7-192 に対しては、2023 年に Boura らにより独立に差分攻撃が提案されたものの、後にその有効性が Beyne と Neyt により否定されていた。同年に Wang らが提案した差分攻撃についても同一の欠陥があり、結果として、SPEEDY-7-192 に対する差分攻撃は未解決だった。

本論文では、SPEEDY-7-192 に対する初の有効な差分攻撃が提示され、その識別子の正当性が準差分（quasidifferential）フレームワークを用いて検証された。探索は 1 ラウンド差分トレイルの集合から出発し、従来よりも広範な探索空間が調査された。さらに、確率的拡張を用いて鍵回復段階の最適化が行われた結果、選択暗号文攻撃として、計算量が $2^{186.36}$ 回の暗号化、メモリ量が 2^{84} 個の 192 ビット状態である攻撃が達成された。加えて、SPEEDY-5-192（4 ラウンド）および SPEEDY-6-192（5 ラウンド）に対する差分攻撃も提示され、これらは現時点で最良の既知攻撃と報告されている。

The State-Test Technique on Differential Attacks: a 26-Round Attack on CRAFT and Other Applications

Dounia M'Foukh, María Naya-Plasencia, Patrick Neumann

ブロック暗号の差分解析に関する論文である。state-test 技法は、鍵の一部を推測する代わりに内部状態の一部を推測することで推測量を削減する手法であり、不能差分攻撃や切り詰め差分を用いた中間一致攻撃において有効であることが知られていた。

本研究では、この state-test 技法の考え方を一般化し、通常の差分解析および差分線形解析にも適用可能であることが示されている。また、state-test 技法と確率的鍵回復を組み合わせた新たな手法が提案され、暗号アルゴリズムと差

分特性の相互作用に関する条件が整理されている。

これらの結果に基づき、Pride に対する最良の既存攻撃を改良するとともに、Serpent に対する最良の既存攻撃の一部についても改善を達成した。加えて CRAFT に対しては、全 32 ラウンドのうち 24、25、26 ラウンドを対象とする初めての攻撃を提示し、最良の既存攻撃と比較して最大 3 ラウンドの改善を実現している。

Quantum Periodic Distinguisher Construction: Symbolization Method and Automated Tool

Qun Liu, Haoyang Wang, Jinliang Wang, Boyun Li, Meiqin Wang

量子周期的識別子を用いた共通鍵暗号の安全性評価に関する論文である。量子計算の進展に伴い、Simon のアルゴリズムを用いた周期性検出が、共通鍵暗号に対する量子攻撃の重要な基盤技術として注目されている。しかし、Simon のアルゴリズムを適用するためには、暗号構造から周期関数を構成する必要があり、この構成の困難さが実用的な量子暗号解析の大きな障壁となっていた。既存研究では、全探索に基づくテスト手法（Canale ら、CRYPTO 2022）や、切り詰め差分理論（truncated differential theory）に基づく解析（Xiang ら、ToSC 2024）が提案されていたものの、未知差分を扱えないことや、自動化が不十分であることから、複雑な暗号構造に対して体系的に周期的識別器を導出することが困難であった。

本研究では、共通鍵暗号に対する周期的識別子構成の一般化が行われ、未知差分を含む場合にも適用可能な新たな構成手法が提示された。著者らはこの手法は確率的周期的識別子（probabilistic periodic distinguisher）へと拡張し、より広範な周期構造を捉えられることが示された。また、新しい記号的表現を導入することで周期条件を形式化し、初の自動 SMT ベース探索モデルが構築された。その結果、GFS-4F、LBlock、TWINE に対しては 10 ラウンド、Skipjack-B に対しては 16 ラウンドの量子周期的識別子が得られ、それぞれ最良の既存結果を 1、2、2、3 ラウンド更新したことが示された。さらに、SKINNY に対しては初めて 7、8、9 ラウンドの周期的識別子が発見された。加えて同一ラウンド数における既存の古典的識別子（Hadipour ら、CRYPTO 2024）と比較して、本研究で示した識別子はより低いデータ量を達成することが報告されている。

Algebraic Cryptanalysis of AO Primitives Based on Polynomial Decomposition: Applications to RAIN and Full AIM-I/III/V

Hong-Sen Yang, Qun-Xiong Zheng, Jing Yang

AO プリミティブ（arithmetic-oriented primitives）への代数攻撃に関する論文である。LowMC に基づく耐量子署名方式 Picnic が NIST 耐量子暗号標準化プロセスの第 3 ラウンド候補として選定されたことにより、共通鍵暗号技術を高度なプロトコルに適用する Symmetric Techniques for Advanced Protocols（STAP）を用いた、効率的かつ安全な耐量子署名方式の設計が広く注目を集めている。その中でも、安全なマルチパーティ計算（MPC）、完全準同型暗号（FHE）、およびゼロ知識（ZK）証明システムなどの高度なプロトコル向けに設計され、乗算回数の削減を目的とした共通鍵暗号技術は、AO プリミティブと呼ばれる。AO プリミティブは大きな有限体上で定義されることが多いことから、差分解析や線形解析といった従来の統計的攻撃手法は有効に機能せず、多項式方程式系の構造を直接利用する代数攻撃に依存してきた。

本研究では、耐量子署名方式 Rainier および AIMer に用いられている MPC フレンドリーなプリミティブである Rain（CCS 2022）および AIM（CCS 2023）の安全性を解析している。$\mathbb{F}_2$ 上での代数攻撃はすでに与えられていたが、著者らは多項式分解を用いることで方程式の次数を低減することで、$\mathbb{F}_{2^n}$ 上で動作する新しい代数攻撃手法を導入

した。この手法は、guess-and-determine 技法、meet-in-the-middle モデリング、および終結式計算を組み合わせることで、Rain および完全版 AIM に対する攻撃を可能にする。本攻撃の定量評価として、128/192/256 ビット鍵に対して、2 ラウンド Rain に対しては $2^{73.7}/2^{107.0}/2^{138.9}$ 回のプリミティブ呼び出しで、3 ラウンド Rain に対しては $2^{167.6}/2^{243.6}/2^{319.1}$ 回のプリミティブ呼び出しで、完全版 AIM に対しては $2^{114.0}/2^{163.2}/2^{228.3}$ 回のプリミティブ呼び出しで、それぞれ実現できることが報告された。

Password-Hardened Encryption Revisited

Ruben Baecker, Paul Gerhart, Dominique Schröder

Password-Hardened Encryption（PHE）への攻撃に関する論文である。シングルサインオン（SSO）サービスの普及により、パスワードの保存が集中化され、攻撃が成功した場合の被害が甚大になることから、安全な保存機構の必要性が一層高まっている。約 10 年前、Facebook は新しいパスワード保護手法を導入し、その後 Everspaugh らにより Pythia（USENIX 2015）として形式化され、パスワード強化（password hardening）の概念が提案された。これらの研究の主たる動機は、オフライン総当たり攻撃に対する証明可能な安全性を達成することであった。この流れは、CCS 2016、USENIX 2017 などの後続研究を生み、その後、Password–Hardened Encryption（PHE）（USENIX 2018、CCS 2020）が提案された。PHE は Virgil Security により SaaS として商用化され、メッセンジャープラットフォームに統合されている。

本論文では、PHE の元の設計における重大な弱点を特定し、PHE が本来防ぐことを目的としていたオフライン総当たり攻撃を可能にする実用的な暗号攻撃が提示された。著者らは PHE の弱点として、実世界の攻撃シナリオや、鍵を定期的に更新することで安全性を高めるための鍵ローテーション（key rotation）との相互作用を考慮していないと指摘したうえで、新しいオフライン総当たり攻撃を提案している。攻撃の評価として、Virgil Security が提供するオープンソース PHE を対象に、数秒以内にパスワードを抽出できることが報告された。加えて著者らはこれらの問題を解消する新しい PHE 構成を提案し、精緻化された安全性モデルの下で、現実的設定において安全であることの証明を提供している。提案方式に対しては、堅牢性および性能を評価する包括的な実験結果が報告されている。

Universally Composable Password-Hardened Encryption

Behzad Abdolmaleki, Ruben Baecker, Paul Gerhart, Mike Graf, Mojtaba Khalili, Daniel Rausch, Dominique Schröder

Password-Hardened Encryption（PHE）および Threshold Password-Hardened Encryption（TPHE）への攻撃に関する論文である。PHE は、外部レートリミッタによる復号回数制限を導入することで、パスワードや秘密鍵を明かすことなく、オフライン総当たり攻撃から保護する暗号化方式である。Brost ら（CSS 2020）によって導入された TPHE は、この信頼を複数のレートリミッタに分散することで、単一障害点を排除することを意図して導入されたが、その安全性を厳密に裏付ける形式的基盤は確立されていなかった。

本論文では、Brost らによって提案された TPHE 方式の安全性証明に欠陥が存在することが示された。そのうえで著者らは PHE および TPHE に対して初めて UC（Universal Composability）安全性に基づく定式化を与え、鍵ローテーションを含む現実的な運用条件を正確に捉えることが可能となった。このモデルの下で著者らは、ラウンド最適かつ UC 安全な TPHE 構成を提示した。さらに当該提案方式の実装および評価を行い、現実的な WAN 環境において、従来方式を上回る効率性が報告されている。

A Crack in the Firmament: Restoring Soundness of the Orion Proof System and More

Thomas den Hollander, Daniel Slamanig

ゼロ知識証明システム Orion への攻撃に関する論文である。Orion（Xie ら、CRYPTO 2022）は、線形時間の証明者を持つ、最近提案された plausibly post-quantum zk-SNARK である。これは Brakedown（Golovnev ら、ePrint 2021 および CRYPTO 2023）に比べてゼロ知識性を持つことに加え、証明サイズおよび検証者の計算量を多項式対数オーダーに削減し、証明者計算時間が既存のすべての簡潔証明システムの中で最速であり、証明サイズも Brakedown より 1 桁小さいことから、具体的効率性が示されていた。その後の解析研究の中で Orion はアップデートされ、ゼロ知識性の修正や健全性問題の修正に対する改定が加えられてきた。特に健全性問題については、 commit-and-prove SNARK を「外側の」SNARK として用いることで修正が行われた。

本論文では、改訂後の Orion が、ゼロ知識性の有無にかかわらず依然として健全性を満たしていないことが示され、実用的な攻撃が構成された。この結果を踏まえ、追加の仮定を導入することなく Orion を修復する手法が提示され、その修正版として多項式コミットメント方式 Scorpius が導入された。この修復により、線形時間の証明者計算量を維持しつつ、証明サイズおよび検証者計算時間が、初期版 Orion で主張されていた値よりもさらに小さくなることが示された。さらに、Diamond と Posen による手法（CiC 2024）を適用することで、検証者チャレンジのサイズが対数オーダに抑えられることが示され、複数点オープンおよび非対話性を明示的に考慮した安全性証明が与えられた。

E.13 その他の国際会議

AI for Code-based Cryptography

Mohamed Malhou, Ludovic Perret, Kristin Lauter

SAC 2025

機械学習を用いた符号ベース暗号への暗号解析に関する論文である。

符号ベース暗号では、公開鍵がランダム線形符号と計算量的に区別できないことが安全性の重要な前提となっている。Classic McEliece では Goppa 符号が、BIKE では Quasi-Cyclic Moderate Density Parity-Check (QC-MDPC) が用いられており、これらの符号がランダム符号と識別できないことが期待されている。従来研究では、代数的手法や統計的手法に基づく識別攻撃が検討されてきた。

本論文では、トランスフォーマモデルを用いた新しい識別アルゴリズム DeepDistinguisher が提案され、構造化符号とランダム線形符号とを識別できることが示された。Goppa 符号に対しては、高い識別精度が達成され、その構造が機械学習モデルによって有意に捉えられることが示された。また、一部の設定においては、従来の識別攻撃を上回る性能が得られることが示された。さらに、パンクチャリングを用いることで、追加の学習を行うことなく、より大きな符号長に対しても識別能力が一般化されることが示された。加えて、MDPC 符号および QC-MDPC 符号に対して、専用の識別結果が初めて与えられ、これらの符号族についても機械学習に基づく識別可能性が示された。

Quantum Advantage from Soft Decoders

André Chailloux, Jean-Pierre Tillich

STOC 2025

近年、[Regev, STOC2005] による LWE 問題の提案およびその量子的な困難性を議論した論文で用いられた計算問題の還元手法を効率的な量子アルゴリズムの構成と量子優位性の証明に用いる研究が活発化している。Regev による帰着テクニックを符号理論の言葉で記述しなおすと、以下のような双対符号からの coset sampling として捉えることができる。

q を有限体の位数、$C \subset \mathbb{F}_q^n$ を符号、$f : \mathbb{F}_q^n \to \mathbb{C}$ を $\sum_{x \in \mathbb{F}_q^n} |f(x)|^2 = 1$ を満たす関数とする。

符号 C のパリティ検査行列 H に対して、エラーベクトル e が $|f|^2$ からサンプリングされたときのシンドローム復号問題 $eH = s$ を解くオラクルと重ね合わせ状態 $\sum_e F(e) |e\rangle$ を準備可能な量子アルゴリズムが存在すれば双対符号 $C^\perp$ の coset sampling を多項式時間で行う量子アルゴリズムの存在が示される。

ただし先行研究においては復号化オラクルを硬判定による Berlekamp-Welch 復号から軟判定を用いる Koetter-Vardy 復号とすることで探索可能な範囲を広げるなどの技術的工夫が本論文では用いられている。

上記一般的なアルゴリズムにおいて C をリード・ソロモン符号とすることで、S-Polynomial Interpolation 問題を解く量子アルゴリズムが構成される。ここで、S-Polynomial Interpolation 問題は制限集合 $S \subset \mathbb{F}_q$ と次数 k に対して、ランダムな $y = (y_\alpha)_{\alpha \in \mathbb{F}_q} \in \mathbb{F}_q^q$ が与えられたときに

$$y_\alpha - P(\alpha) \in S \quad (\forall \alpha \in \mathbb{F}_q)$$

を満たす次数 $< k$ の多項式 $P(X) \in \mathbb{F}_q[X]$ を求める計算問題である。この問題は符号理論では、$n = q$ の Reed-Solomon 符号上で、全ての座標が S に含まれるベクトルを syndrome coset の中から探す問題と等価となる。

q を奇素数、$S = [-u, u] \subset \mathbb{F}_q$ と取ることで、ランダムなシンドローム s に対して $xH = s, \|x\|_\infty \leq u$ を満たす x を復元する問題が得られる。これは、リード・ソロモン符号上の Inhomogeneous な SIS 問題（RS-ISIS$_\infty$ 問題）と捉えることができる。

類似の問題として署名方式 CRYSTALS-Dilithium は Module 格子上の SIS$_\infty$ 問題を安全性の根拠としており、論文内ではその関連性が議論されているものの、現在のところ実用的な署名方式に対する量子多項式時間アルゴリズムの構成が与えられているわけではない。

The Jacobi Factoring Circuit: Quantum Factoring with Near-Linear Gates and Sublinear Space and Depth

Gregory D. Kahanamoku-Meyer, Seyoon Ragavan, Vinod Vaikuntanathan, Katherine Van Kirk

STOC 2025

素因数分解問題に対する量子解析論文である。素因数分解問題は RSA 暗号を始めとする現代暗号の安全性に深く関わり、インスタンスの大きさと計算時間の現実的な関係性はこの数十年研究され続けてきた。近年では量子コンピュータの発展により、分解に必要な量子的リソースの見積もりが深く研究されている。本論文では、$N = P^2Q$ 型の合成数を条件 $\log Q = \Theta(n^a), a \in (2/3, 1)$ のもとで素因数分解を行う量子アルゴリズムを提案している。これは Q が小さい場合に Shor のアルゴリズムよりも回路規模が小さく、特に n よりも小さな量子ビット数で素因数分解が可能な初の量子アルゴリズムであるとしている。応用として、古典で検証可能な量子性証明のより効率的な構成の可能性に言及している。

技術的には、[Li et al., Nature Scientific Reports 2012] により与えられた、ヤコビ記号の量子計算回路 $|x\rangle|0^S\rangle \mapsto \left(\frac{x}{N}\right)|x\rangle|0^S\rangle$ を構成要素とした、$N = A^2B$ 型の合成数の因数を発見する回路の改良により実現している。ただし、Li らのアルゴリズムでは A, B は素数である必要は無く、B が square-free であるという条件のみが要求されている。

本論文では Li らのヤコビ記号計算回路の出力について検討を行い、$N = P^2Q$ 型の合成数に対しては $\mathrm{poly}(Q)$ 程度の範囲に対して QFT を行うことで分解に必要な周期が高確率で出力されることを示した。これは Shor のアルゴリズムが必要とする $\mathrm{poly}(N)$ よりもはるかに小さいものである。また、ヤコビ記号の計算回路自体の改良も行い、$\tilde{O}(\log A)$ 量子ビット、$\tilde{O}(\log B)$ ゲートの回路を構成している。この構成手法は最大公約数の計算、剰余逆元の計算にも応用できるとしている。

また、本論文の帰結として与えられた因数発見アルゴリズムをサブルーチンとして複数回呼び出すことで、$N = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ 型の合成数で、指数部分 $\alpha_1, \ldots, \alpha_r$ が全て異なるものを分解することが可能であることも示されている。

Extending Regev's Quantum Algorithm to Elliptic Curves

Razvan Barbulescu, Mugurel Barcau, Vicentiu Pasol

Latincrypt 2025

楕円曲線上の離散対数問題に対する量子攻撃に関する論文である。

2023 年に Regev により、Shor のアルゴリズムよりも少ないリソースで計算を行う素因数分解アルゴリズムが提案された。Shor のアルゴリズムがその性質上、素因数分解問題以外にも離散対数問題をはじめとする隠れ部分群問題を処理することが可能であることから、同様の拡張が Regev のアルゴリズムに対しても可能であるかどうか、量子リソースの観点から効率的であるかどうかが近年集中的に研究されている。

本論文では、[Ekerå-Gärtner, PQCrypto 2024] による Regev アルゴリズムの離散対数問題への拡張を踏まえ、楕円曲線上の離散対数問題を解くアルゴリズムを構築し、その計算リソースについて議論している。曲線がいくつかの条件を満たし、論文内のヒューリスティックが成り立つならば Shor のアルゴリズムと比較して漸近的に $(\log n)^{1/2}$ 程度のゲート数の削減が可能であるとしている。論文内では条件や仮定が様々に与えられており、特に曲線の「高さ」や点の「小ささ」に関して制約がある。しかしながら、実用的な曲線の多くは係数が小さいことから、それらの条件を満たす可能性があるとして検討された。

アルゴリズムのフレームワークは先行研究と同様であり、Ekeraa らのアルゴリズムにおいて量子的に計算される $|g_1^{z_1} \cdots g_d^{z_d}\rangle$ の部分が曲線の multi-scalar product の計算 $|[z_1]g_1 + \cdots + [z_d]g_d\rangle$ へと置き換わっている。このとき、点 g_i が $\mathbb{Q}$ への持ち上げによる表現において（各成分が $O(\sqrt{n})$ ビットで表現できる程度に）小さいものであるならば、multi-scalar product の計算が効率化できることが古典的に知られており [Pippenger, SIAM J. Comp. 1980, 9(2)]、その効率化を量子的に実現している。このことは、与えられた曲線上の小さい点を計算することで Regev 型アルゴリズムの量子リソースを削減可能であることを示しており、古典的な前処理との組み合わせによる Regev のアルゴリズムの改良を示唆している。

特に、標準的に用いられてきた Curve25519, BLS12, BN254, secp256k1, Koblitz 曲線等の多くの曲線に対して、小さな点を計算するアルゴリズムと具体的な点列を与え、上記ゲート数の削減が可能であるかどうかの検討が行われた。P-256 では Shor のアルゴリズム以上のゲート数の削減は難しいものの、Curve25519, secp256k1 等に関してはより注意深く解析する必要があると結論付けている。

CRYPTREC Report 2025
（暗号技術評価委員会報告　CRYPTREC RP-2000-2025）

発行日：2026 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-SHI
  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）
  INNOVATION PLATFORM AGENCY, JAPAN
  2-28-8 HONKOMAGOME, BUNKYO-KU
  TOKYO, 113-6591 JAPAN