CRYPTREC Report 2020

令和３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-2000-2020

「暗号技術評価委員会報告」

CRYPTREC Report 2020

暗号技術評価委員会報告書 目次

はじめに

本報告書は、総務省及び経済産業省が主催する暗号技術検討会の下に設置され運営されている暗号技術評価委員会の 2020 年度活動報告書である。暗号技術評価委員会は、国立研究開発法人情報通信研究機構及び独立行政法人情報処理推進機構が共同で運営している。本委員会の 2020 年度の活動として、主に、1)暗号技術の安全性及び実装に係る監視及び評価、2)CRYPTREC 注意喚起レポートの発行、2)推奨候補暗号リストへの追加候補(事務局選出)となる暗号方式の安全性評価、3)新しい暗号技術に係る調査および評価の実施などについて暗号技術検討会より承認を得て、活動を実施した。

今年度は、昨年度に引き続き耐量子計算機暗号（Post-Quantum Cryptography）の研究動向を調査している暗号技術調査ワーキンググループ(暗号解析評価)の主査を國廣昇先生にご担当いただき、本ワーキンググループにおいて主に次の 3 点の調査を実施した。a) Shor の量子アルゴリズムによる現代暗号への脅威に関する調査、b) 耐量子計算機暗号(PQC)に関する技術動向に関する調査（PQC を導入する際の技術の調査)、c) 公開鍵暗号の安全性に直結する素因数分解の困難性に関する計算量評価や楕円曲線上の離散対数計算の困難性に関する計算量評価に関する予測図の更新。また、量子コンピュータ時代に向けた暗号の在り方検討タスクフォースにて、引き続き検討が必要とされた CRYPTREC 暗号リストの３リスト構成の在り方に関して検討するとともに、量子コンピュータや耐量子計算機暗号の状況を把握する監視活動を実施した。

その他、1)では、多くの国際会議がオンラインで実施される中、国際会議等で発表される暗号の安全性及び実装に係る技術に関する監視を行い、CRYPTREC 暗号リストに掲載されている暗号の危殆化が進んでいないかどうかの判断を行った。2)では、IETF で標準化され、TLS 1.3 で実導入されるなど、今後、利用が見込まれる暗号技術（署名）である EdDSA の安全性評価を行った。その結果として、EdDSA で利用する曲線および方式の構成いずれについても安全性に問題はなく、CRYPTREC 暗号リストに追加するための安全性要件を満たしていると判断した。3)では、上述の暗号技術調査ワーキンググループ(暗号解析評価)の活動のほか、次期 CRYPTREC 暗号リストとは別文書として分類することとなった耐量子計算機暗号、高機能暗号、及び、軽量暗号に関するガイドラインの作成・更新に関わる今後の方針を議論した。

発足して以来 21 年にわたる CRYPTREC 活動は、安全・安心な ICT 社会の実現に貢献してきた。CRYPTREC は世界的にも広く知られ、その活動の一つ一つが CRYPTREC ブランドの信頼の醸成につながっていると考えている。コロナパンデミックを経て、人々の生活により密着する形で暗号技術は使われ、暗号技術に対する社会のニーズは近年、より一層大きくなっている。今後も、社会の情勢を踏まえ、未来の安心・安全な ICT 社会の実現・維持につなげるべく、暗号技術の安全性という観点から必要とされる活動を展開していきたい。

暗号技術評価委員会の活動は暗号技術やその実装及び運用に携わる研究者及び技術者の献身的な協力により成り立っている。末筆ではあるが、本活動に様々な形でご協力頂いている関係者の皆様に深甚なる謝意を表する次第である。

暗号技術評価委員会　委員長　　高木 剛

本報告書の利用にあたって

本報告書の想定読者は、一般的な情報セキュリティの基礎知識を有している方である。たとえば、電子政府において電子署名やGPKIシステム等暗号関連の電子政府関連システムに関係する業務についている方などを想定している。さらに、個別テーマの調査報告等については、ある程度の暗号技術の知識を備えていることが望まれる。

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

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

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

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

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

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

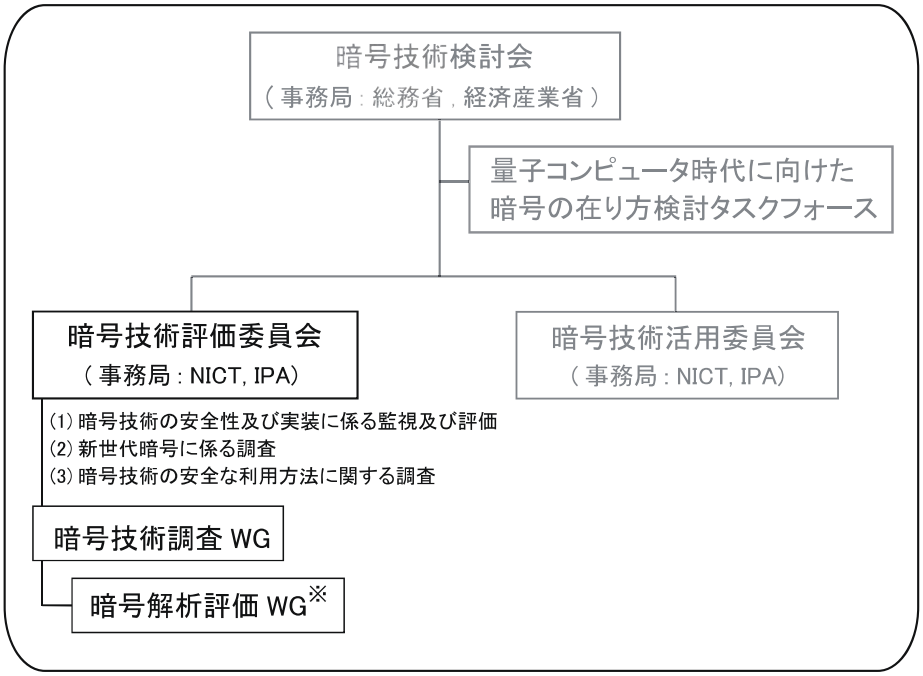
【問合せ先】　info@cryptrec.go.jp

委員会構成

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

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

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



※ 今年度実施されている調査項目：

・ 耐量子計算機暗号技術に関する調査

図 0.1：CRYPTREC 体制図

委員名簿

暗号技術評価委員会

委員長	高木 剛	東京大学 教授
委員	岩田 哲	名古屋大学 准教授
委員	上原 哲太郎	立命館大学 教授
委員	大東 俊博	東海大学 准教授
委員	國廣 昇	筑波大学 教授
委員	四方 順司	横浜国立大学　教授
委員	手塚 悟	慶應義塾大学 教授
委員	藤崎 英一郎	北陸先端科学技術大学院大学 教授
委員	本間 尚文	東北大学 教授
委員	松本 勉	横浜国立大学 教授
委員	松本 泰	セコム株式会社 マネージャー
委員	盛合 志帆	国立研究開発法人情報通信研究機構 上席研究員
委員	山村 明弘	秋田大学 教授
委員	渡邊 創	国立研究開発法人産業技術総合研究所 副研究センター長

暗号技術調査ワーキンググループ（暗号解析評価）

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	草川 恵太	日本電信電話株式会社 主任研究員
委員	桑門 秀典	関西大学 教授
委員	下山 武司	国立情報学研究所 特任研究員
委員	高木 剛	東京大学 教授
委員	高島 克幸	三菱電機株式会社 主管技師長
委員	峯松 一彦	日本電気株式会社 主席研究員
委員	安田 貴徳	岡山理科大学 准教授
委員	安田 雅哉	立教大学 准教授

オブザーバー

小林 宏至	内閣官房内閣サイバーセキュリティセンター
東　隆夫	内閣官房内閣サイバーセキュリティセンター
木村 誠一郎	内閣官房内閣サイバーセキュリティセンター
川崎 明彦	内閣官房内閣サイバーセキュリティセンター
高木 浩光	内閣官房内閣サイバーセキュリティセンター
衛門 愛子	個人情報保護委員会 事務局[2020 年 7 月まで]
柏原 陽	個人情報保護委員会 事務局[2020 年 7 月から]
田嶋 龍	警察庁 情報通信局
千葉 英之	総務省 行政管理局
仁木 孝明	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
黒田 淳	総務省 サイバーセキュリティ統括官室［2021 年 3 月まで］
山下 恵一	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
林　巧	経済産業省 産業技術環境局
上田 翔太	経済産業省 商務情報政策局
飯山 貴啓	経済産業省 商務情報政策局［2020 年 8 月まで］
村山 裕紀	経済産業省 商務情報政策局［2020 年 9 月から］
小林 圭樹	防衛省 整備計画局
椛木 隆慎	防衛省 整備計画局
伊藤 愼崇	警察大学校
滝澤 修	国立研究開発法人情報通信研究機構
花岡 悟一郎	国立研究開発法人産業技術総合研究所

事務局

国立研究開発法人情報通信研究機構（久保田実、野島良、大久保美也子、篠原直行、高安敦、黒川貴司、金森祥子、高橋しおり、吉田真紀、青野良範、小川一人、伊藤竜馬、笠井祥、大川晋司）

独立行政法人情報処理推進機構（瓜生和久、神田雅透、小暮淳、橋本徹、天内日紗子[2020年9月まで]、木島慶子[2020年10月から]、石川 誠[2021年1月から]）

第１章　活動の目的

1.1 電子政府システムの安全性確保

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

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

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

1.2 暗号技術評価委員会

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

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

そのため、2007年度に電子政府推奨暗号の安全性に関する継続的な評価、電子政府推奨暗号リストの改訂に関する調査・検討を行うことが重要であるとの認識の下に、暗号技術評価

[1] https://www.cryptrec.go.jp/list/cryptrec-ls-0001-2012r4.pdf
[2] https://www.cryptrec.go.jp/list_2003.html

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

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

2013 年度からは、名称を「暗号方式委員会」から「暗号技術評価委員会」と変更し、暗号技術の安全性に係る監視・評価及び実装に係る技術(暗号モジュールに対する攻撃とその対策も含む)の監視・評価を実施することになった。引き続き、暗号技術評価委員会では、その下に暗号技術調査ワーキンググループを設置し、暗号技術に関する具体的な検討を行っている。2013 年度から 2016 年度まで、暗号技術調査ワーキンググループ（暗号解析評価）及び暗号技術調査ワーキンググループ（軽量暗号）の 2 つのワーキンググループが設置され、2017 年度からは、暗号技術調査ワーキンググループ（暗号解析評価）が設置されている。詳細については、第 3 章を参照のこと。

1.3 CRYPTREC 暗号リスト

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

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

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

2009 年度には、2008 年度に検討した「電子政府推奨暗号リスト改訂のための暗号技術公募要項（2009 年度)」に基づき、電子政府推奨暗号リスト改訂のための暗号技術公募が行われた。2010 年度から 2012 年度にかけて、暗号方式委員会、暗号実装委員会及び暗号運用委

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

員会にて評価が行われ、2012 年度に暗号技術検討会にて電子政府推奨暗号リストの改定が行われた。最終的に、総務省及び経済産業省がパブリックコメント(意見募集)[4]を行い、「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト)」が決定された。

選定方法及びその結果については、CRYPTREC Report 2012(暗号技術評価委員会報告)に記載されている。

1.4 活動の方針

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

I) 暗号技術の安全性及び実装に係る監視及び評価

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

を実施する。I)の内容をさらに詳細に分けると、下記の①～⑤となる。

① CRYPTREC 暗号リストに掲載されている暗号技術等の監視：
国際会議等で発表される CRYPTREC 暗号リストの安全性及び実装に係る技術（暗号モジュールに対する攻撃とその対策も含む）に関する監視を行い、会議や ML を通して報告する。

② 電子政府推奨暗号リスト及び推奨候補暗号リストからの運用監視暗号リストへの降格及び 運用監視暗号リストからの危殆化が進んだ暗号の削除：
CRYPTREC 暗号リストの安全性に係る監視活動を継続的に行い、急速に危殆化が進んだ暗号技術やその予兆のある暗号技術の安全性について評価を行う。また、リストからの降格や削除、注釈の改訂が必要か検討を行う。

③ CRYPTREC 注意喚起レポートの発行：
CRYPTREC 暗号リストの安全性及び実装に係る技術の監視活動を通じて、国際会議等で発表された攻撃等の概要や想定される影響範囲、対処方法について早期に公開することが望ましいと判断された場合、注意喚起レポートを発行する。

④ 推奨候補暗号リストへの新規暗号（事務局選出）の追加：
標準化動向に鑑み電子政府システム等での利用が見込まれると判断される暗号技術の追加を検討する。

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

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

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

推奨暗号リスト[5]掲載の暗号技術に対する考え方[6]と基本的に同じである。つまり、暗号技術の安全性及び実装に係る監視及び評価とは、研究集会、国際会議、研究論文誌、インターネット上の情報等を監視すること（情報収集）、CRYPTREC 暗号リストに掲載されている暗号技術の安全性に関する情報を分析し、それを暗号技術評価委員会に報告すること（情報分析)、安全性等において問題が認められた場合、暗号技術評価委員会において内容を審議し、評価結果を決定すること（審議及び決定)、の 3 つの段階からなる。また、仕様書の参照先の変更を検討する際にも、監視に関する基本的な考え方を参考にしている。

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

[情報発信フローの概要]

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

A) 暗号アルゴリズムの完全な危殆化による緊急対応

B) 正確で信頼性の高い情報を発信することによる過剰反応防止

C) 長期的なシステムの安全性維持のための対策喚起

D) 対応不要

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

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

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

[5] 2003 年 2 月 20 日に策定されたものを指す。

[6] たとえば、暗号技術検討会 2008 年度報告書を参照のこと。
https://www.cryptrec.go.jp/report/cryptrec-rp-1000-2008.pdf

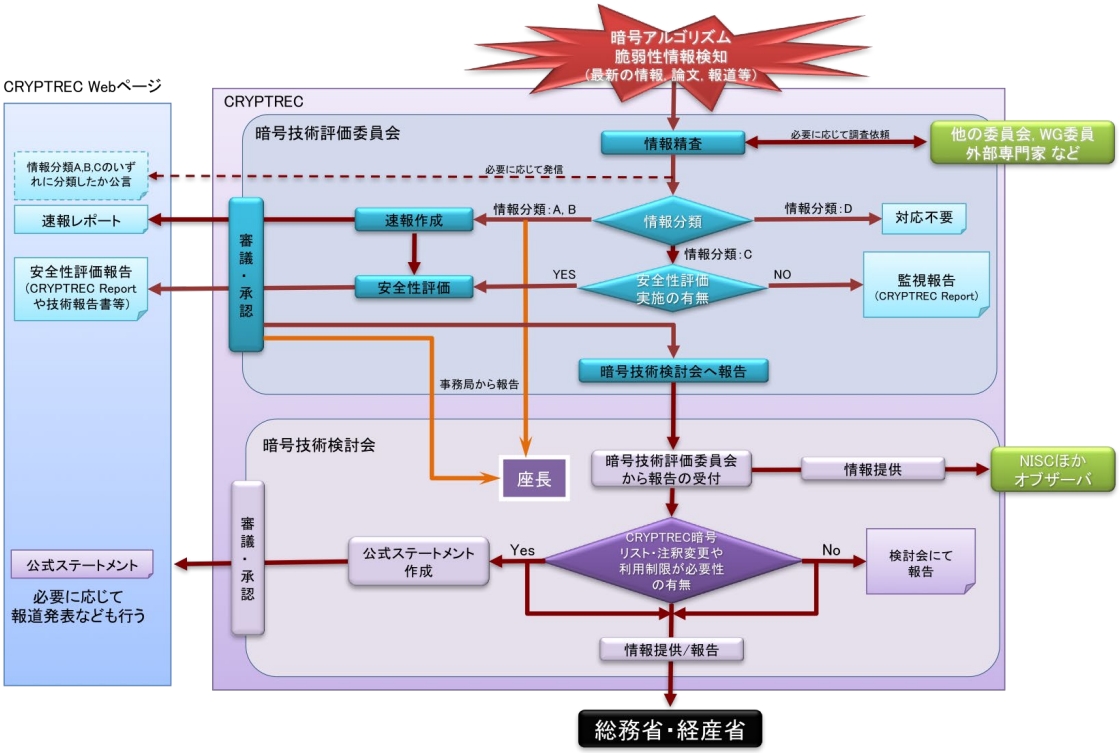


図1.1　暗号アルゴリズムの脆弱性に関する情報発信フロー

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 2020 年度の報告時点では収集した全ての情報が引き続き「情報収集」、「情報分析」フェーズに留まり、「審議及び決定」には至らず、電子政府推奨暗号の安全性に懸念を持たせるような事態は生じていないと判断した。以降、収集、分析した主たる情報について報告する。

2.1.1. 共通鍵暗号に関する安全性評価について

共通鍵暗号技術に対する攻撃としては、既存の暗号アルゴリズムへの攻撃について、攻撃に必要な計算量の削減等の進展があった。ここでは主な発表を紹介する。

差分攻撃の拡張である Boomerang Attack の改良版が発表され、ラウンド数 5 の AES に適用した結果は計算量が $2^{16.5}$（すなわち、全鍵復元において 9 万回の暗号化／復号操作しか要求しない）にまで改良した。AES に対する攻撃は 2020 年度も進展は見られたが、安全性マージンはまだあり、AES の安全性に直ちに影響を与えるものではない。

その他の暗号については、ARX（Addition, Rotation, and XOR）ベースの暗号に対する差分線形解析の改良が発表された。ストリーム暗号の一種である ChaCha が、このタイプに属する。ラウンド数 6 の ChaCha では時間計算量が $2^{77.4}$、データ計算量が 2^{58}、ラウンド数 7 の ChaCha では時間計算量が $2^{230.86}$、データ計算量が $2^{48.83}$ という結果になっており、これまでの記録を上回っているが、ChaCha20 のラウンド数 20 にはまだ安全性マージンがあり、早急な対策が必要となるものではない。

2.1.2. 公開鍵暗号に関する安全性評価について

公開鍵暗号に関しては、Crypto2020 においてフランス・リモージュ大学の Fabrice Boudot らにより、795 ビットの素因数分解（RSA-240）及び離散対数計算(DLP-240)に対する新記録が報告され、前者は約 1,000 コア年、後者は約 3,200 コア年の計算量であったこれまでの記録はいずれも 768 ビット（2009 年の RSA-768 と 2016 年の 768 ビット離散対数）であったが、例えば離散対数の関係探索においては前回時間よりも 25%少ない時間で済む等、両計算においてかなりの高速化が実現された。また離散対数計算の素因数分解に対する計算量比率も約 3 倍と、これまで考えられていた程差があるわけではないことが判明した。更に、別の記録となる RSA-250 に対する素因数分解の結果も報告された。

2.1.3. その他の注視すべき技術動向

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

NIST PQC 標準化プロセスは 3 ラウンド目に入り、7 つの最終候補および 8 つの代替候補の評価が進められている。PQC Forum メーリングリストにおいて、NIST から「最近の暗号解析が多変数署名 Rainbow および GeMSS に影響を与えたため、NIST はセキュリティおよびアプリケーションの観点から多様性欠如の懸念を持っている」旨のメールが投稿された。更に NIST は、2 ラウンド時のレポートから、SPHINCS+が 3 ラウンドの終わりの時点で標準のアルゴリズムになる可能性について言及した部分および標準化プロセスにないスキームを採用する可能性について言及した部分を議論のスタートポイントとして提示し、意見を募った。予断を許さない状況となったが、第 3 回標準化会議は 2021 年 6 月 7 日～9 日に開催される予定で論文募集が出されている（投稿締切り：4 月 23 日、採録通知：5 月 7 日)。

	電子署名	鍵カプセル化機構／暗号化	合計
格子ベース	2 Crystals-Dilithium(F), Falcon(F)	5 Crystals-Kyber(F), FrodoKEM(A), NTRU(F), NTRU Prime(A), Saber(F)	7
符号ベース	0	3 Classic McEliece(F), BIKE(A), HQC(A)	3
多変数	2 Rainbow(F), GeMSS(A)	0	2
ハッシュベース	2 Sphincs+(A), Picnic(A)	0	2
その他	0	1 SIKE(A)	1
合計	6(F:3, A:3)	9(F:4, A:5)	15

F: Finalist、A: Alternate

表 2.1:NIST PQC コンペティション応募暗号(第 3 ラウンド)

2.2. 注意喚起レポートについて

今年度は、注意喚起レポートの発行はなかった。

2.3. 推奨候補暗号リストへの新規暗号（事務局選出）の追加

2.3.1. ディジタル署名 EdDSA の安全性評価について

下記において EdDSA の安全性評価について記す。①で背景について、②と③で具体的な評価結果について、④で暗号技術評価委員会における安全性に関する見解について、最後に⑤で今後の予定について述べる。

① 背景

EdDSA は、RFC8032[1]で規定され、TLS1.3 で採用された（RFC 8446[2]）署名アルゴリズムである。さらに、TLS1.2 のような TLS1.3 より前のバージョンでは、ECDSA と同じ暗号スイートを使って EdDSA も利用可能となった（RFC8422[3]）。TLS1.3 では楕円曲線暗号がベース仕様になると記載されており、また NIST は、2018 年以降、米国の連邦情報処理標準におけるディジタル署名の改定版となる FIPS186-5 において EdDSA を追加する方針を明らかにしている[4][5]。実際、2019 年 11 月に公表された FIPS186-5 ドラフト版に EdDSA が追加されている[6]。

このように EdDSA が広く一般に使われる環境が整いつつあり、その安全性が損なわれる場合甚大な影響を及ぼしかねない。2019 年度暗号技術活用委員会 TLS ワーキンググループ活動報告においてもその安全性評価の必要性が示され、EdDSA の安全性評価を暗号技術評価委員会において実施することが 2020 年度第一回暗号技術検討会において審議され承認された。

② 評価概要

EdDSA について、事務局選出の暗号アルゴリズムとして CRYPTREC 暗号リストへの追加を視野に入れ、安全性評価を下記 2 点の観点による評価を実施した。

I. EdDSA で使われている曲線の安全性評価（安全性の根拠となる仮定の強度）
II. 方式の構成そのものの安全性評価

I)に関する評価概要

[件名]：EdDSA が用いている曲線の安全性に関する調査及び評価
[依頼先]：安田雅哉 様（立教大学）
Steven Galbraith (University of Auckland)
[依頼内容]：EdDSA で利用される曲線の安全性に関わる脆弱性について、公開されてい

る攻撃方法の有無を調査し、存在する場合はその影響の範囲などについてまとめるなど、対象となる曲線の安全性評価を実施する。報告書には以下の項目を含めることとする。

- EdDSA で利用される曲線に関する解説
- EdDSA で利用される曲線に関して公開されている攻撃・脆弱性の調査、および、存在する場合は、その攻撃の適用条件や計算量等に関する解説
- EdDSA で利用される曲線の安全性評価
- ECDSA と比較した場合の曲線としての効率性に関する考察

なお、調査の範囲は、2020 年 8 月末までに公開された文献等を対象とした。

II)に関する評価概要

[件名]：EdDSA の構成の安全性に関する調査及び評価

[依頼先]：藤崎英一郎 様（北陸先端科学技術大学院大学）

Steven Galbraith（University of Auckland）

[依頼内容]：EdDSA の構成に関わる脆弱性について、公開されている攻撃方法の有無を調査し、存在する場合はその影響の範囲などについてまとめ、また、安全性評価を実施する。報告書には以下の項目を含めることとする。

- EdDSA の構成の解説
- EdDSA の構成に関して公開されている攻撃・脆弱性の調査、および、存在する場合は、その攻撃の有用性に関する解説
- EdDSA の構成としての安全性評価
- ECDSA と比較した場合の方式としての効率性に関する考察

なお、調査の範囲は、2020 年 8 月末までに公開された文献等を対象とした。

③ 評価レポートの概要（ア、イ）

EdDSA は、有限体上のツイスト Edwards 曲線といわれる楕円曲線上の Schnorr 署名の署名内部乱数(ノンス)[1]を署名者の秘密情報と署名される平文のハッシュ値に置き換えた確定的(deterministic)な Schnorr 署名である。EdDSA で推奨されるツイスト Edwards 曲線は RFC7748[7]で規定されるものであり Ed25519, Ed448 と記述される。

(ア) 曲線に関する安全性評価レポートの概要（a～d）（付録 3、5）

(a)EdDSA で利用される曲線

[1] 本来、ノンスという言葉は同じ値が用いられることのない 1 回のみ使用される値を意図して使われることが多く、その値が確率的に決められるか否かについては制約がない。一方、多くの文献(例えば[8][9][10]など)で確率的署名の内部乱数がノンスと呼ばれており、これを踏襲して Schnorr 署名や ECDSA の署名時の内部乱数も本資料ではノンスと呼ぶ。さらに、EdDSA の署名時に用いる確定的な値である「署名者の秘密情報と署名される平文のハッシュ値」も複数の論文(例えば[11]など)でノンスと呼ばれており、本資料においてもこれをノンスと呼ぶ。

EdDSA では Edwards 曲線と呼ばれる特殊な楕円曲線やそのツイスト曲線が利用され、これらの曲線上の点の加算と 2 倍算を効率的に計算することができる。RFC8032[1]によると、EdDSA では計算機による攻撃に対して約 128 ビットのセキュリティレベルの Ed25519 と約 224 ビットのセキュリティレベルの Ed448 の 2 種類が推奨されている。また、Ed25519 では Curve25519、Ed448 では Curve448 と呼ばれるツイスト Edwards 曲線パラメータを利用する。

(b)EdDSA で利用される曲線に関して公開されている攻撃・脆弱性

EdDSA の安全性の根拠とされている楕円曲線離散対数問題(ECDLP)に対する攻撃法は、Pollard の ρ 法や指数計算法などの任意の楕円曲線に適用できる汎用攻撃アルゴリズムと、MOV 攻撃法や SSSA 攻撃などの特殊な楕円曲線にのみ適用可能な特殊攻撃アルゴリズムに大別される。Curve25519 や Curve448 では、これらの特殊な曲線に適した既存の攻撃方法が有効にならないような曲線パラメータが選択されているため、汎用攻撃アルゴリズムの中で最良の ρ 法が EdDSA に対する最良の攻撃法である。

(c)EdDSA で利用される曲線の安全性評価

EdDSA に対する最良の攻撃法である ρ 法は誕生日の逆理に基づく確率的アルゴリズムであるため、付録 3 ではこの攻撃法に基づいて、Curve25519 及び Curve448 における ECDLP を解くにはそれぞれ $2^{125.8257}$ 回と $2^{222.8257}$ 回の楕円加算が必要であると見積もっている。そのためそれぞれの ECDLP はほぼ 128 ビットのセキュリティレベルとほぼ 224 ビットセキュリティレベルを持つとしている。

また、付録 5 では量子アルゴリズムによる脅威に関しても言及されている。これまでの見積もりでは、256 ビット ECDLP を解くためには 2000-3000 量子ビットが必要だと思われ、誤り訂正などを考慮に入れると 600 万量子ビットが必要だと考えられる。近年の量子コンピュータの実装の進展を考えると、今後の発展を注視する必要はあるものの、これから 10 年間 EdDSA を使い続けて問題はないと考える。

(d)ECDSA と比較した場合の曲線としての効率性

楕円曲線を利用したディジタル署名では、与えられた自然数 n に対して署名生成時に楕円曲線の点 P のスカラー倍算[n]P を行い、与えられた自然数 n1、n2 に対して署名検証時には楕円曲線の点 P1、P2 の複数スカラー倍算[n1]P1+[n2]P2 を主に行う。

付録 3 では同じ基礎体を利用した場合に、通常の楕円曲線と Edwards 曲線における上記 2 種類の演算のコストを比較している。その結果、Edwards 曲線の方がスカラー倍算の場合に最大約 33%、複数スカラー倍算は最大約 28%効率的に計算できると見積もっている。

(イ)　方式の構成に関する安全性評価レポート概要（a～d）（付録 4、5）

(a)EdDSA 構成の特徴

Schnorr 署名との一番大きな違いは署名内部乱数(ノンス)を署名者の秘密情報と平文のハッシュ値で生成し署名を確定的かつ異なる平文に対してノンスを衝突させにくくしたことであると述べている。そのほかの違いとしては、内部で使うハッシュ関数の出力長を長くし、群の位数で剰余を取っていること、Key-prexing を採用していること、さらに群要素チェックが通常の Schnorr 署名より緩くなっていることなどを挙げている。また、PureEdDSA と HashEdDSA のどちらかのオプションを選ぶ必要がある。

(b)EdDSA の構成に関して公開されている攻撃・脆弱性

近年はサイドチャネル攻撃による解析結果などがいくつか示されているが、すぐさま現実的な脅威につながる結果などは報告されていない。

(c)EdDSA の構成に関する安全性

- 総評：下記の観点から、EdDSA の構成に関わる安全性において、EdDSA が ECDSA に劣ると考えられる点は無いと思われると述べている。
  - ✓ Schnorr 署名をもとに EdDSA は構成されているため、ランダムオラクルモデルで安全性が証明されている Schnorr 署名に対する安全性評価を参考にすることができる。
  - ✓ Schnorr 署名との大きな違いはノンスの生成方法であるが、EdDSA におけるノンスの生成方法は、署名の内部乱数を弱い疑似乱数生成器に委ねることによる危険を排除し、現実的な脅威を回避するための配慮が施されている。
  - ✓ 比較対象となる ECDSA については、既存結果として generic group model でのみ安全性が証明されている。
- 証明可能安全性：ランダムオラクルモデルや generic group model での安全性証明に関する考察結果が示されている。

  付録 5 では構成に用いられているハッシュ関数をランダムオラクルとみなし、楕円曲線離散対数問題(ECDLP:Elliptic Curve Discrete Logarithm Problem)の計算量的困難性を仮定とするランダムオラクルモデルでの安全性証明を行い、その構成に問題がないことを示している。また、スタンダードモデルで安全性は示せないものの、EdDSA に用いるハッシュ関数に必要な性質を挙げ、EdDSA で利用される SHA-512 や SHA-3 はこれらの性質を満たしていると考えることが出来るだろうと述べている。

  付録 4 では厳密に仕様書に規定されているハッシュ関数を考慮に入れた考察を行っている。仕様書では用いるハッシュ関数が規定されており、Ed25519 では SHA-512 を、Ed448 では SHAKE256 が使われる。Ed25519 で利用される SHA-512 は、そ

の内部の Merkle-Damgard 構造によりランダム関数と識別がついてしまう。また、SHA-512 を使ったノンスは疑似ランダム関数の出力値とみなすことが出来ない。よって、SHA-512 を利用した Ed25519 をランダムオラクルモデルや generic group model で安全性解析を行うことは難しく証明可能安全性の意味では証明が付かなくなっていると述べている。一方、Ed448 で利用される SHAKE256 は、ランダム関数もしくは疑似ランダム関数とみなすことが許容される。よって、SHAKE256 を利用した Ed448 には、ランダムオラクルモデルや generic group model での Schnorr 署名の解析結果が利用でき、安全性にある程度の理論的根拠を与えることができると述べている。

- Key-prexing:EdDSA は key-prexing という署名者自身の公開鍵を平文と連結させ、公開鍵と平文に署名を付けさせる形を取っている。この仕様のため関連鍵攻撃のような攻撃を回避できるようになっていると述べている。
- 複数署名者での安全性：通常の署名方式は署名者が増えると署名者の数に応じて証明可能安全性で保障できるビットのセキュリティレベルは劣化するが、EdDSA は複数署名者の下でのセキュリティレベルが署名者の数に関係せず、単一署名者の Schnorr 署名のビットのセキュリティレベルで抑えることができると述べている。
- ノンスについて：Schnorr 署名との違いの一つに署名生成に用いるノンスの扱いが挙げられる。付録 4 では下記の考察を述べている。SHA-512 を利用した Ed25519 では、証明可能安全性の意味では証明がつかなくなっているが、現実の攻撃を考えると異なる平文に対するノンスの衝突こそが一番に回避しなければならないものであり、ハッシュ関数でノンスを生成することでこれを回避している。
- サイドチャネル攻撃耐性：付録 4 では EdDSA に関するサイドチャネル攻撃耐性として優位な点及び気を付けるべき点を挙げている。付録 4 では EdDSA はノンスが漏洩しづらくする工夫をしているためノンスの漏洩を利用する攻撃（タイミング攻撃や電力解析攻撃など)に対して ECDSA より安全と考えても良いと述べている。一方、ノンスを確定的にしたことに対する新たなフォールト攻撃も提案されており、サイドチャネル攻撃が可能な組み込みデバイスとして利用するような場合ではなんらかの対策をとることが望ましいということも述べている。付録 5 においても類似の見解を示している。

(d)EdDSA に関する効率評価

- ECDSA との比較：署名検証の計算時間については、EdDSA についてはバッチ処理を適用することができるが、ECDSA については同様のバッチ処理が適用可能であるかは明らかではなく、EdDSA 署名ほどの高速化技法は知られていない。そのため、一般的にはバッチ処理を適用した場合の EdDSA の署名検証は、ECDSA に比べ高速

になることが期待できると述べている。付録 4 ではさらに厳密な下記の考察を示している。署名される平文がさほど長くない（平文をハッシュする時間が十分短い）場合、署名生成時間および検証時間いずれについても EdDSA が ECDSA よりやや短い。ただし平文が極めて長い（署名生成時間はほぼハッシュ関数の計算時間となってしまう）場合、EdDSA の署名生成時間の方が長く、署名検証時間は両方式でほぼ同程度である。

④ 暗号技術評価委員会としての見解

（ア） 曲線に関する安全性評価について

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

（イ） 方式の構成に関する安全性評価について

評価レポートにおいて、現実的な脅威に結びつくような脆弱性は指摘されておらず、また、③（イ）－（c）の総評にて述べられているように ECDSA と比較してもその安全性に劣る点はないと考えられる。他、複数の観点から安全性に関わる考察が示されており、いずれも安全性に問題を与える点はないと考えられる。以上より、評価報告書により示された評価結果を総合し、EdDSA の構成については、現実的な利用シーンにおける安全性に問題はないと判断する。

評価レポート(付録 3,4,5)により、EdDSA の曲線の安全性及び方式構成の安全性に問題がないことを把握することができたことから、評価レポートを CRYPTREC の HP にて公開した[2]。

⑤ 今後の予定

EdDSA の曲線および方式の構成いずれについても安全性に問題は見つからなかった。このことから、「国際標準化等の実績がある」ことを根拠とした事務局で選出する暗号アルゴリズムの候補として、CRYPTREC 暗号リストへの追加を視野に入れ、実装性能評価も行うこととする。

[2] https://www.cryptrec.go.jp/exreport/cryptrec-ex-3001-2020.pdf,
https://www.cryptrec.go.jp/exreport/cryptrec-ex-3002-2020.pdf,
https://www.cryptrec.go.jp/exreport/cryptrec-ex-3003-2020.pdf

【参考文献】

[1] RFC8032, “Edwards-Curve Digital Signature Algorithm (EdDSA) ”, Jan. 2017
[2] RFC8446, “The Transport Layer Security (TLS) Protocol Version 1.3”, Aug. 2018
[3] RFC8422, “Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS) Versions 1.2 and Earlier”, Aug. 2018
[4] NIST, “NIST Update (CHES version)”, CHES rump talk, 2018
[5] NIST, “NIST status update on Elliptic Curves and Post-Quantum Crypto”, NIST Threshold Cryptography Workshop 2019, 2019
[6] NIST, “Digital Signature Standard (DSS)”, FIPS PUB 186-5 (Draft), 2019
[7] RFC7748, “Elliptic Curves for Security”, Jan. 2016
[8] Phong Q. Nguyen, Igor E. Shparlinski, “The Insecurity of the Digital Signature Algorithm with Partially Known Nonces”, J. Cryptol. 15(3): 151-176 (2002)
[9] Phong Q. Nguyen, Igor E. Shparlinski, “The Insecurity of the Elliptic Curve Digital Signature Algorithm with Partially Known Nonces”, Des. Codes Cryptogr. 30(2): 201-217 (2003)
[10] Diego F. Aranha, Pierre-Alain Fouque, Benoît Gérard, Jean-Gabriel Kammerer, Mehdi Tibouchi, Jean-Christophe Zapalowicz, “GLV/GLS Decomposition, Power Analysis, and Attacks on ECDSA Signatures with Single-Bit Nonce Bias”, ASIACRYPT (1) 2014: 262-281
[11] Diego F. Aranha, Claudio Orlandi, Akira Takahashi, Greg Zaverucha, “Security of Hedged Fiat-Shamir Signatures Under Fault Attacks”, EUROCRYPT (1) 2020: 644-674

2.4. 仕様書の参照先の変更

CRYPTREC の Web サイトでは、CRYPTREC 暗号リストに掲載している暗号技術の仕様書の参照先（https://www.cryptrec.go.jp/method.html）を記している。推奨候補暗号リストの認証暗号 ChaCha20-Poly1305 の ChaCha20 に関する仕様書に変更があったため、新旧仕様書の差分が軽微な修正であると判定し（表 2.4）、参照先の変更を行った（表 2.5）。

表 2.4：ChaCha20-Poly1305 の暗号の新旧仕様書

暗号技術名	旧仕様書	新仕様書
ChaCha20-Poly1305	Request for Comments: 7539, ChaCha20 and Poly1305 for IETF Protocols (May 2015)	Request for Comments: 8439, ChaCha20 and Poly1305 for IETF Protocols (June 2018)

表 2.5：判定結果とその理由

暗号技術名	判定結果	理由	備考
ChaCha20-Poly1305	仕様書の参照先の変更を認める。	アルゴリズム部分に変更なし。	https://www.rfc-editor.org/errata_search.php?rfc=7539

2.5. 学会等参加状況

国内外の学術会議に参加し、暗号解読技術に関する情報収集を実施した。参加した国際会議は、表2.6に示す通りである。

表 2.6 国際会議への参加状況

学会名・会議名		開催国・都市	期間
Eurocrypt 2020	the 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques	(Virtual Conference)	2020 年 5 月 11 日～2020 年 5 月 15 日
Crypto 2020	40th Annual International Cryptology Conference	(Virtual Conference)	2020 年 8 月 17 日～8 月 21 日
FDTC 2020	Fault Diagnosis and Tolerance in Cryptography	(Virtual Conference)	2020 年 9 月 13 日
CHES 2020	Conference on Cryptographic Hardware and Embedded Systems	(Virtual Conference)	2020 年 9 月 14 日～2020 年 9 月 18 日
PQCrypto 2020	The Eleventh International Conference on Post-Quantum Cryptography	(Virtual Conference)	2020 年 9 月 21 日～2020 年 9 月 23 日
FSE 2020	Fast Software Encryption conference	(Virtual Conference)	2020 年 11 月 9 日～2020 年 11 月 13 日
Asiacrypt 2020	26th International Conference on the Theory and Application of Cryptology and Information Security	(Virtual Conference)	2020 年 12 月 7 日～2020 年 12 月 11 日

以下に、国際学会等に発表された論文を中心に、暗号解読技術の最新動向を示す。詳しくは、付録 8 を参照のこと。

2.5.1. 共通鍵暗号の解読技術

・New Slide Attacks on Almost Self-similar Ciphers [Eurocrypt2020]

Orr Dunkelman, Nathan Keller, Noam Lasry, and Adi Shamir

スライド攻撃は、繰り返し構造のブロック暗号に対する強力な暗号解析手法であり、ラウンド数に依存しない計算量で攻撃できるという特性を備えている。しかし、この手法はすべてのラウンドが全く同一である場合にのみ適用可能である。この要件はFeistel 構造のブロック暗号では当てはまるが、最終ラウンドが追加の post-whitening subkey で終了しなければならないため、SPN 構造ではめったに当てはまることはない。それに加えて、SPN 構造では最終ラウンドに追加の非対称性があります。例えば、AES では最終ラウンドは MixColumns 演算を省略している。最終ラウンドにおけるこのような非対称性は、スライド攻撃のために開発された高度な手法の適用を困難にしている。

本論文では、4 個の新しいタイプのスライド攻撃を開発することで、この「最終ラウンドの問題点」を克服している。提案手法を AES のような構造を持ついくつかの方式に適用することで、提案手法の有効性を示している。ほとんどの場合において、攻撃にかかる計算量を $2^{n/2}$ に近似できる。

・Improved Differential-Linear Attacks with Applications to ARX Ciphers [Crypto2020]

Christof Beierle, Gregor Leander, and Yosuke Todo

本論文では、ARX (Addition, Rotation and XOR) ベースの暗号に特に焦点を当てた差分線形解析のフレームワークに対する改良を提案している。このインパクトを検証するため、これらの改良を Chaskey と ChaCha に適用し、現在公開されている最良の攻撃を著しく改良することを示した。6-round ChaCha では Time Complexity が $2^{77.4}$, Data Complexity が 2^{58}, 7-round ChaCha では Time Complexity が $2^{230.86}$, Data Complexity が $2^{48.83}$ という結果になっている。

2.5.2. 公開鍵暗号の解読技術

・Security of Hedged Fiat-Shamir Signatures Under Fault Attacks [Eurocrypt 2020]

Diego F. Aranha, Claudio Orlandi, Akira Takahashi, and Greg Zaverucha

署名ごとの乱数の決定論的な生成は、Fiat-Shamir 型の署名スキームにおける乱数性の欠落の致命的リスクを軽減するための広く受け入れられた解決策となっている。しかし、最近の研究では、そのような脱乱数スキーム (EdDSA を含む) は差分故障利用攻撃に脆弱で、乱数の再利用又はその他の手段による計算誤りを意図的に引き起こすことに

よって、攻撃者が署名鍵全体を復元することが可能になることが示されている。乱数性の欠陥の問題と故障利用攻撃の脅威とのバランスをとるため、署名の設計には、秘密鍵、メッセージ、及び nonce をハッシュすることによって、署名ごとの乱数の「ヘッジされた」派生を提唱しているものがある。実用的な署名スキームにおけるヘッジパラダイムが人気を博してきているにもかかわらず、ヘッジされた署名のフォールト耐性の形式的解析の試みはなされていない。

本論文では、Fiat-Shamir transform を介して構築された署名スキームのフォールト耐性の形式的なセキュリティ解析を実行している。著者は”bit-tampering”な故障利用攻撃を特徴づけるモデルを提案し、署名計算の異なるステップを横断したそれらのインパクトを解析している。その結果、ヘッジパラダイムはある種のフォールトに対しては攻撃を軽減できるが、その他のフォールトに対しては攻撃が依然有効であることを証明した。また、具体的なケーススタディとして、この結果を、シグナルメッセージプロトコルで使用されている、ヘッジされた版の EdDSA である XEdDSA、及び、NIST の耐量子計算機暗号標準化プロセスの第 2 ラウンドにある、ヘッジされた Fiat-Shamir 署名スキームである Picnic2 に適用している。

・Comparing the Difficulty of Factorization and Discrete Logarithm: A 240-Digit Experiment [Crypto2020]

Fabrice Boudot, Pierrick Gaudry, Aurore Guillevic, Nadia Heninger, Emmanuel Thomé, and Paul Zimmermann

本論文では、2 つの新たな記録を報告する。795 ビットレベルに相当する RSA-240 の素因数分解、そして 795 ビット素体上の離散対数計算である。以前の記録は 2009 年の RSA-768 の素因数分解と 2016 年の 768 ビット離散対数計算であった。本論文の 2 つの 795 ビットレベルの計算は同じハードウェアとソフトウェアを用いて行われ、離散対数を計算することは同じサイズの素因数分解よりも大きく難しくはないことを示している。更に、アルゴリズムの多様性と良く選ばれたパラメーターのおかげで、本論文での計算は以前の記録から予想されるよりも遥かに効率的であることを示した。また、本論文の最後のページで RSA-250 の素因数分解について報告する。

2.5.3. その他の暗号技術の解読技術

・Minerva: The curse of ECDSA nonces: Systematic analysis of lattice attacks on noisy leakage of bit-length of ECDSA nonces [CHES2020]

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

ECDSA の実装（FIPS140-2 認証されたスマートカード用 IC チップである Atmel 社製 AT90SC、および 5 個のソフトウェア暗号ライブラリ）に、サイドチャネル攻撃の一種で

あるタイミングアタックに対する脆弱性を発見した。ECDSA では、署名生成 1 回ごとに nonce が必要だが、nonce のビット長がサイドチャネル情報として(ノイズは大きいが)洩れる場合に、それを利用して秘密鍵を復元する手法を示し、実際の認証製品や暗号ライブラリに対する具体的な攻撃の結果も示している。EdDSA は、nonce が決定論的に生成され、また nonce が長いことから、この攻撃に耐性がある。

・Finding Collisions in a Quantum World: Quantum Black-Box Separation of Collision-Resistance and One-Wayness [Asiacrypt2020]

Akinori Hosoyamada and Takashi Yamakawa

STOC1989 における Impagliazzo と Rudich の論文から、多くのブラックボックス不可能性に関する結果が確立されたが、これらは暗号プリミティブ間の古典的なブラックボックス帰着を除外しただけであり、量子帰着を用いることにより可能となることが期待された。これらの可能性を除外するために、量子設定の下でブラックボックス不可能性を研究した。

本論文ではまず最初に、TCC2004 の Reingold, Trevisan, Vadhan による定式化に従い、完全ブラックボックス帰着に対する量子版を定式化し、衝突耐性ハッシュ関数から一方向性置換（もしくは落とし戸置換でさえ）への量子完全ブラックボックス帰着は存在しないことを証明した。本論文では、古典・量子両方のプリミティブ実装を考慮しており、この結果は古典設定において同様の結果を示した Eurocrypt1998 における Simon の手法を量子設定へと拡張したものとなっている。

・An Algebraic Formulation of the Division Property: Revisiting Degree Evaluations, Cube Attacks, and Key-Independent Sums [Asiacrypt2020]

Kai Hu, Siwei Sun, Meiqin Wang, and Qingju Wang

本論文では、ベクトルブール関数 f の座標関数の任意の積における単項式の有無を、その結合が f となるより単純な列にわたる所謂単項式トレイルの数を数えることにより決定する、分割プロパティの単純化とみなすことができる「単項式予測 (monomial prediction)」と名付けたテクニックを導入する。単項式予測を用いて、本論文では TRIVIUM の正確な代数的次数を 834 ラウンドまで初めて得ることができた。キューブ攻撃の文脈においては、より小さい次元でより多くのキューブを同定し、840, 841, 842 ラウンド TRIVIUM に対するほぼ最適な攻撃の改良を行った。

・An Algebraic Attack on Ciphers with Low-Degree Round Functions: Application to Full MiMC [Asiacrypt2020]

Maria Eichlseder, Lorenzo Grassi, Reinhard Lüftenegger, Morten Øygarden, Christian Rechberger, Markus Schofnegger, and Qingju Wang

本論文では初めて、F_2^n 上の MiMC における全てのフルラウンド版に対し、コードブックの半分を必要とする鍵回復攻撃を示した。選択暗号文攻撃シナリオにおいて、MiMC の n ビットフル版に対してこのデータから秘密鍵を復元するのに、MiMC に対する $2^{n-\log_2(n)+1}$ 呼び出しと無視できる量のメモリを必要とする。本攻撃は MiMC のトイ版において実際に検証された。本攻撃は素体上の MiMC の安全性には影響しないことに注意されたい。

・Improvements of Algebraic Attacks for solving the Rank Decoding and MinRank problems [Asiacrypt2020]

Magali Bardet, Maxime Bros, Daniel Cabarcas, Philippe Gaborit, Ray Perlner, Daniel Smith-Tone, Jean-Pierre Tillich, and Javier Verbel

本論文では、多変数ベースあるいはランク距離符号ベース暗号においていたるところに現れる MinRank 問題を解く代数的手法を著しく改良する方法を示す。後者に現れる構造的 MinRank 問題の場合は、最近の Eurocrypt2020 における Canteaut、Ishai らのブレークスルーを更に改良し、これまで最良と考えられていた組み合わせ攻撃を代数攻撃が凌ぐことを示した。このアプローチを少し改良することにより、本論文ではあるパラメーターに関してはグレブナー基底計算を完全に避け、線型連立方程式を解くことが残されたのみであった。これは本質的に計算量を改良するのみならず、この場合になぜ代数的テクニックが機能するかの確信的議論を与えるものである。NIST PQC 第 2 ラウンド候補の ROLLO-I-128/192/256 に適用した場合、本論文の新しい攻撃は、Eurocrypt2020 で得られたビット計算量 117, 144, 197 に対し、各々71, 87, 151 を与える。同様のアプローチにより通常の MinRank 問題に対し代数的的 MinRank ソルバーを改良した。NIST-PQC の第 2 ラウンド候補である GeMSS および Rainbow に適用した場合、本論文の攻撃はこれまでに知られている最良攻撃に非常に近いもしくは少し良い計算量を持つ。

・Lower Bounds on the Degree of Block Ciphers [Asiacrypt2020]

Phil Hebborn, Baptiste Lambin, Gregor Leander, and Yosuke Todo

ブロック暗号に対し代数的次数の上限を評価する手法はこれまでに知られているが、設計者にとって安全性を保証する役には立たない。本論文では現代的なブロック暗号の代数的次数の意味ある下限評価を与える。

2.6. 委員会開催記録

2020 年度に暗号技術評価委員会は、表 2.7 の通り 2 回開催された。各会合の開催日及び主な議題は以下の通りである。

表 2.7: 暗号技術評価委員会の開催

回	年月日	議題
第 1 回	2020 年 7 月 17 日	・暗号技術評価委員会活動計画の具体的な進め方についての審議 ・外部評価(ディジタル署名 EdDSA の安全性評価)実施についての審議 ・暗号技術調査ワーキンググループ(暗号解析評価)の活動計画案の審議 ・監視状況報告
第 2 回	2021 年 3 月 9 日	・暗号技術評価委員会活動報告(案)についての審議 ・ディジタル署名 EdDSA の安全性評価結果の報告と暗号技術評価委員会としての見解について審議 ・暗号技術調査ワーキンググループ(暗号解析評価)の活動内容の報告 ・耐量子計算機暗号、高機能暗号、及び、軽量暗号に関するガイドラインの今後について審議 ・仕様書参照先変更の報告 ・監視状況報告 ・CRYPTREC Report 2020(暗号技術評価委員会報告)目次案の提示

2.7. 暗号技術調査ワーキンググループ開催記録

2020 年度、暗号技術調査ワーキンググループ(暗号解析評価)の主要活動項目は、表 2.8 の通りである。表 2.9 の通り、当該 WG は計 2 回開催された。会合の開催日及び主な議題は以下の通りである。

表 2.8: 2020 年度の主要活動項目

ワーキンググループ名	主査	主要活動項目
暗号技術調査ワーキンググループ(暗号解析評価)	國廣　昇	Shor の量子アルゴリズムによる現代暗号への脅威に関する調査、及び、耐量子計算機暗号(PQC)に関する技術動向に関する調査（PQC を導入する際の技術の調査）を行う。 また、「素因数分解の困難性に関する計算量評価」、「楕円曲線上の離散対数計算の困難性に関する計算量評価」の予測図の今後の在り方についての検討を行う。

表 2.9: 暗号技術調査ワーキンググループ(暗号解析評価)の開催

回	年月日	議題
第 1 回	2020 年 8 月 26 日	・暗号技術調査ワーキンググループ(暗号解析評価)活動計画の検討 ・予測図の更新に関する検討 ・Shor の量子アルゴリズムによる現代暗号への脅威に関する調査についての検討 ・耐量子計算機暗号(PQC)に関する技術動向に関する調査(PQC を導入する際の技術の調査)についての検討
第 2 回	2021 年 2 月 3 日	・暗号技術調査ワーキンググループ活動報告案の検討と了承 ・今後の予測図の更新結果の了承 ・Shor の量子アルゴリズムによる現代暗号への脅威に関する調査結果の報告、及び、WG としての見解の検討・了承 ・耐量子計算機暗号(PQC)に関する技術動向に関する調査結果(PQC を導入する際の技術の調査結果)の報告、及び、WG としての見解の検討・了承

第３章　暗号技術調査ワーキンググループの活動

3.1.　暗号技術調査ワーキンググループ（暗号解析評価）

3.1.1. 活動報告の概要

2020 年度暗号技術評価委員会活動計画における「新技術等に関する調査及び評価」の活動として、暗号技術評価委員会の下に暗号技術調査ワーキンググループ(暗号解析評価)を継続して設置して、以下の 3 点について調査を実施することが、暗号技術検討会において承認された。

(1)「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

(2)Shor の量子アルゴリズムによる現代暗号[1]への脅威に関する調査

(3)耐量子計算機暗号(PQC)に関する技術動向に関する調査（PQC を導入する際の技術の調査）

3.1.2. 委員構成（敬称略）

主査：國廣 昇（筑波大学）
委員：青木 和麻呂（文教大学）
委員：草川 恵太（NTT）
委員：桑門 秀典（関西大学）
委員：下山 武司（国立情報学研究所）
委員：高木 剛（東京大学）
委員：高島 克幸（三菱電機）
委員：峯松 一彦（NEC）
委員：安田 貴徳（岡山理科大学）
委員：安田 雅哉（立教大学）

3.1.3. 「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

① 今後の予測図の取り扱いについて

2019 年度第 2 回暗号技術評価委員会にて決定した「今後の予測図の取り扱い」(下記の枠内左)の方針は、2020 年度第 1 回暗号技術検討会にて了承された。

今後はこの方針に従って予測図を更新する。ただし、外挿の範囲は年度末から 20 年後までとする（下記の枠内右)。

[1] 本資料では、安全性が素因数分解や離散対数問題と関連する暗号方式を現代暗号と呼ぶ。

<今後の予測図の取り扱い>（昨年度からの抜粋） (1)予測図を従来通り、いわゆるムーアの法則を仮定して外挿線を今まで引いていた範囲（2040 年）まで直線で引き、評価に大きな変動がないと考えられる限りにおいては、安全サイドに倒した評価として当面の間更新していくことを本 WG として提案する。 なお、予測図は各国・国際標準化機関等により示されている主要な暗号技術の安全性基準と比較すると、より現状に則した評価であり、危殆化時期がそれらよりも先に延びるものとなっている。	<今後の予測図の取り扱い> (1)予測図を従来通り、いわゆるムーアの法則を仮定して外挿線を年度末から 20 年後まで直線で引き、評価に大きな変動がないと考えられる限りにおいては、安全サイドに倒した評価として当面の間更新していく。 なお、予測図は各国・国際標準化機関等により示されている主要な暗号技術の安全性基準と比較すると、より現状に則した評価であり、危殆化時期がそれらよりも先に延びるものとなっている。

【2020 年度のスケジュール】

・2020 年 8 月 26 日　第 1 回 暗号解析評価 WG
　予測図の取り扱いの報告
・2021 年 2 月 3 日　第 2 回 暗号解析評価 WG
　予測図の更新の報告・承認

② 予測図の更新結果の報告

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、2020 年 6 月・11 月のベンチマーク結果を追加して予測図の更新を行った（図 3.1,3.2)。

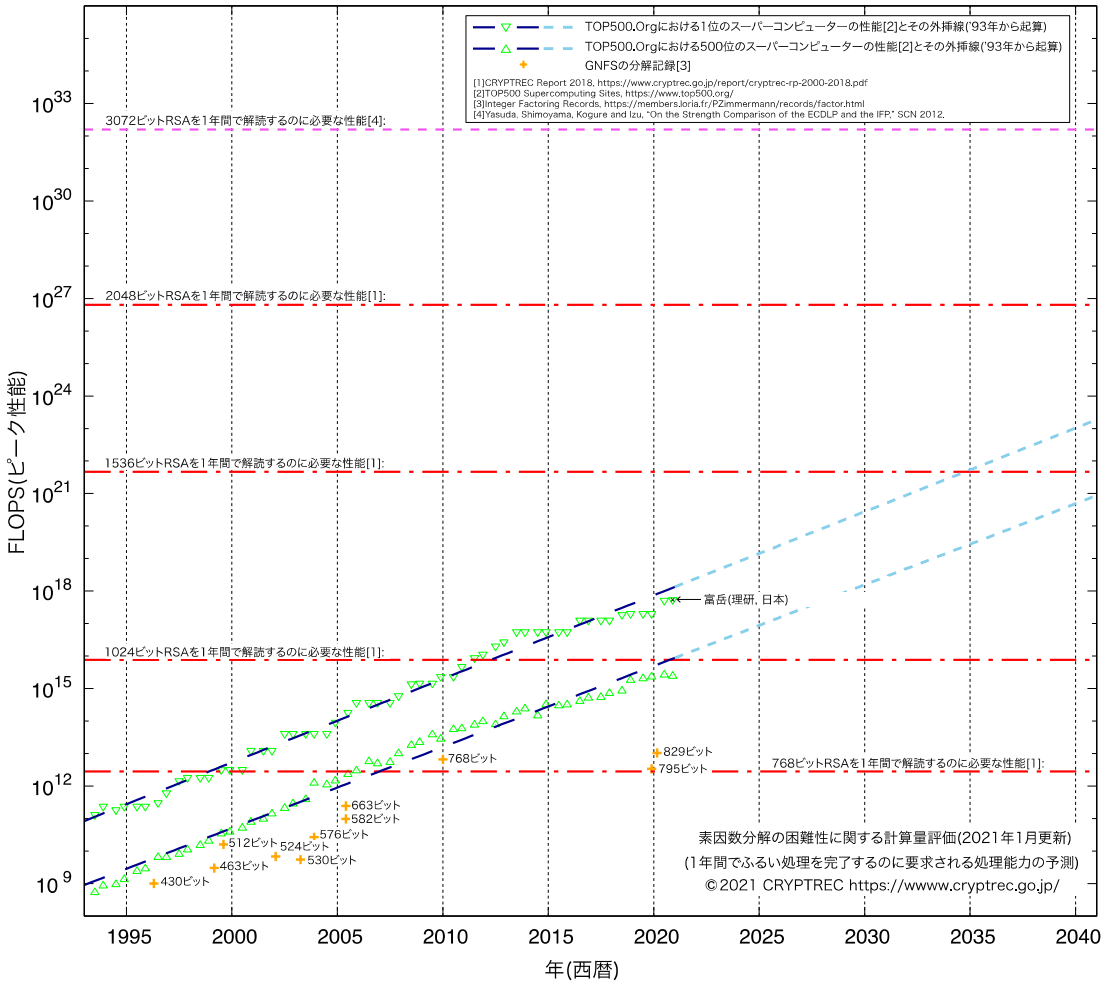


図 3.1：素因数分解の困難性に関する計算量評価(2021 年 1 月更新)

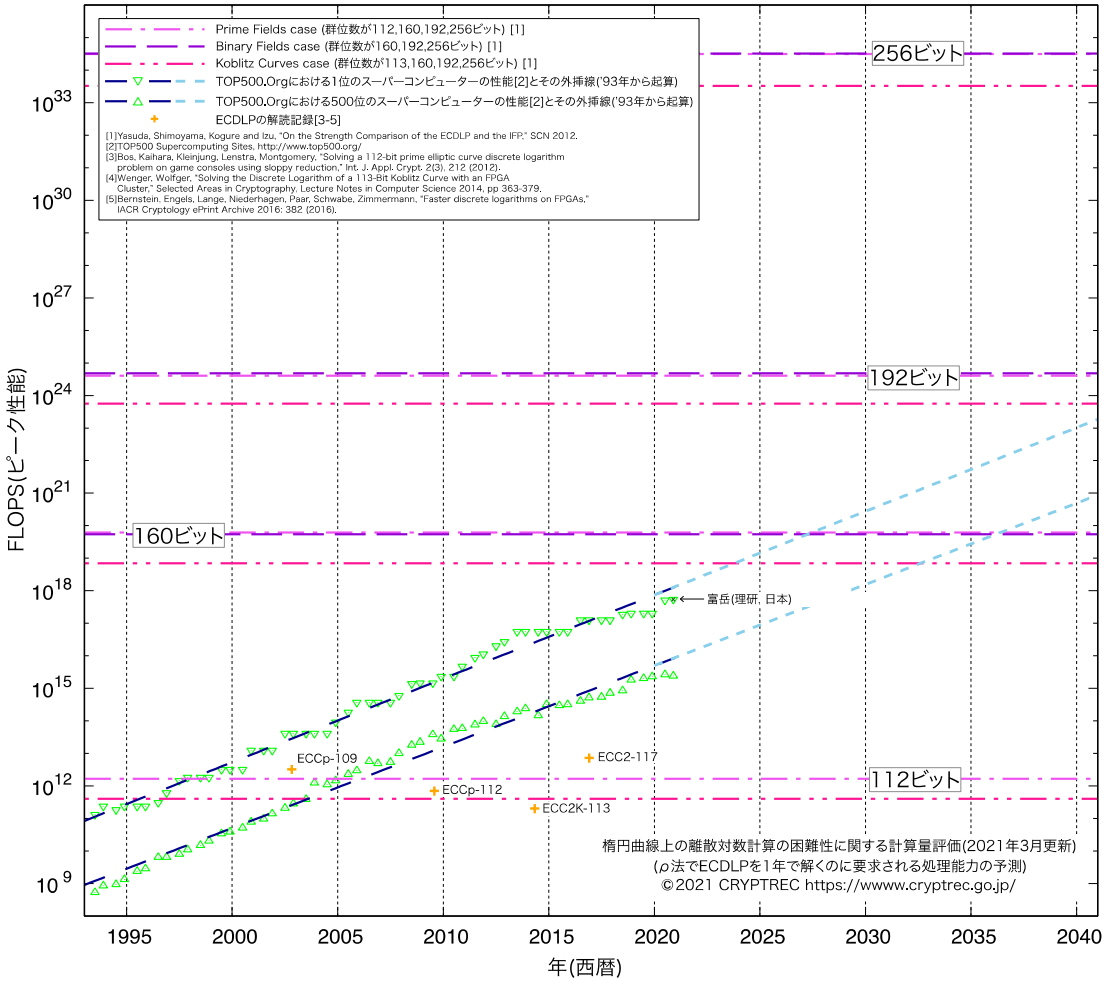


図 3.2：楕円曲線上の離散対数計算の困難性に関する計算量評価(2021 年 1 月更新)

3.1.4. Shor の量子アルゴリズムによる現代暗号への脅威に関する調査

（ア） 背景及び調査の概要

Shor の量子アルゴリズムにより、理論的には素因数分解問題や離散対数問題を効率的に解くことができ、RSA 暗号や楕円曲線暗号等の安全性が危殆化することは広く知られている。そのため、量子コンピュータが実用化されても安全性を保てると期待される暗号(耐量子計算機暗号：PQC)の調査・検討が各国で進められている。CRYPTREC でも PQC の導入について議論が進められており、PQC の必要性を明確にするためにも Shor のアルゴリズムを量子コンピュータ上で実装した研究動向を把握する必要性があるとの指摘を暗号技術調査 WG の委員から受けている。

以上より、Shor の量子アルゴリズムによる現代暗号への脅威を正確に把握するために、上記の研究及び暗号で実際に利用される大きさのパラメータを攻撃するために必要なリソース評価の研究について調査する[2]。

（イ） 実施内容

Shor の量子アルゴリズムによる現代暗号への脅威に関する調査について、事務局が本件を担当すること及び具体的な調査内容が第一回暗号解析評価 WG（2020 年 8 月 26 日）にて承認された。

【調査内容及び報告書の構成】

1）本評価結果の概要（エグゼクティブサマリー）

2）Shor のアルゴリズムの実装・リソース評価の把握の重要性について

3）Shor の量子アルゴリズムの解説

4）Shor の量子アルゴリズムについて報告されている実装結果の調査

5）暗号で用いるようなパラメータに対して Shor の量子アルゴリズムを実行する際のリソース評価

なお、4）と 5）については、2020 年 9 月末までに公開された結果(特に PQCrypto2020 で講演されるものを含む)を調査対象とする。ただし、確認されたものについては 2020 年 10 月以降の論文も調査している。

【2020 年度のスケジュール】

・2020 年 8 月 26 日 第 1 回 暗号解析評価 WG
調査の内容について WG で説明する。(事務局担当)

・2021 年 2 月 3 日 第 2 回 暗号解析評価 WG
調査報告書（案）に対する WG の見解をまとめる。

[2] 調査対象は Shor のオリジナルの量子アルゴリズム及びその変種を含む。

（ウ） WG としての見解

調査内容[3]及び報告書の概要の項目 2)について、第 2 章で Shor のアルゴリズムの実装・リソース評価の把握の重要性をまとめている。Shor のアルゴリズムは、多項式時間で素因数分解や離散対数問題を解けるために理論的には大きな脅威だが、実験的に暗号で用いるような大きなパラメータに対してこれらの問題を解いたという報告はこれまで行われていない。そのため、現状どの程度のパラメータまで実験的に適用可能なのか、実際に暗号で用いるような大きなパラメータの問題を解くにはどの程度の性能の量子コンピュータが必要なのかを把握しておくことは重要である。

調査内容及び報告書の概要の項目 3)について、第 3 章で量子計算の基礎を、第 4 章で Shor のアルゴリズムの概要をまとめている。第 3 章では、量子ビット、測定の概念と Shor のアルゴリズムを理解するのに必要な量子ゲートをまとめている。第 4 章では、量子フーリエ変換や位数計算アルゴリズム、周期計算アルゴリズムを説明した後に素因数分解や離散対数問題のための Shor のアルゴリズムをまとめている。

調査内容及び報告書の概要の項目 4)について、第 5 章で既存の Shor のアルゴリズムの実装結果をまとめている。これまでの実装結果では基本的に 15, 21 などの小さな合成数が対象とされており、いずれの実験においてもこれらの合成数に特化した効率化を行った量子回路を用いている。そのため、大半の実験では一般的な合成数に対しては適用できない大幅な量子ゲートの削減などを行うことで実験を成功させている。また、求めたい値を陽に利用した量子回路を用いた実験もあり、このような場合には任意の大きさの合成数が素因数分解可能であるが、一般の合成数に適用することはできない。また、他の実験と比べて極端な量子回路の効率化を行わずに 21 の素因数分解に成功した実験があるが、この論文では 35 の素因数分解にも試みており、このとき実験は成功しなかったと結論づけている。そのため、現状の量子コンピュータでは暗号で用いるほど大きなパラメータの合成数を素因数分解することは困難であり、暗号で用いるパラメータの問題を解くためには量子ビット数やゲート計算のエラー率など量子コンピュータの性能の大幅な向上が必要であると考える。

調査内容及び報告書の概要の項目 5)について、第 6 章で素因数分解や離散対数問題を実行する際のリソース評価を行った研究をまとめている。一連の研究は、Shor のアルゴリズム自体の改良や実装する際の計算の簡略化手法の提案も行っており、それまで 2048 ビットの合成数を素因数分解するためには 1.7 億個の量子ビットを用いて 1 日かかるとされていたが、2000 万個の量子ビットを用いて 5 時間程度で終わるという結果が 2019 年に報告されており、離散対数問題においても同様に様々な改良が報告されている。そのため、今後も様々な効率化が提案される可能性があるため、量子コンピュータの進歩に合わせて実装法の改良やそれに基づいたリソース評価は今後注視する必要があると考えられる。

[3] 詳しくは、付録 7、または、CRYPTREC EX-3005-2020(https://www.cryptrec.go.jp/exreport/cryptrec-ex-3001-2020.pdf)を参照のこと。

3.1.5. 耐量子計算機暗号(PQC)に関する技術動向に関する調査（PQC を導入する際の技術の調査）

（ア） 背景

近年、量子コンピュータが実用化されても安全性を保てると期待される暗号(耐量子計算機暗号：PQC）の調査・検討が各国で進められている。しかし、現代暗号を解読可能な量子コンピュータが実現される時期は不明瞭であるため、PQC の使用が必須となる時期を具体的に定めることは難しい。PQC が必要になった際にそれを利用する方法として、PQC と現代暗号の双方を併用するいわゆるハイブリッドモード[4]が NIST をはじめ､様々な企業･組織で世界的に議論されている[5][6]。

CRYPTREC では暗号技術検討会において PQC に関する技術動向調査を実施することが承認されている。また､「量子コンピュータ時代に向けた暗号の在り方検討タスクフォース」において PQC のガイドラインの作成について議論されており、ハイブリッドモードをガイドラインに含めるべきかを検討する必要性が生じている。その検討の準備として、PQC のハイブリッドモードの動向を把握しておく必要がある。

（イ） 実施内容

耐量子計算機暗号(PQC) と現代暗号の双方を併用するハイブリッドモードに関する標準化動向を中心とした技術調査について、外部専門家による評価を依頼することが、第 1 回暗号技術評価委員会(2020 年 7 月 17 日) で承認され、具体的な評価内容が、第 1 回暗号解析評価 WG (2020 年 8 月 26 日）にて承認された。

[件名]：ハイブリッドモードの技術動向調査

[依頼先]：菅野 哲 様（株式会社レピダム）

選出理由：IEEE や IETF などの標準化団体での暗号技術に関する標準化活動の推進などに多くの実績があり、本件の調査対象であるハイブリッドモードの近年の標準化動向について広い知見をお持ちであり、本評価報告書をご執筆いただくために必要な情報収集や調査を実施可能な方であるため。

[依頼内容]：ハイブリッドモードの標準化動向についてまとめ、評価報告書を作成する。評価報告書には、以下の内容を含める。

a) ハイブリッドモードの標準化動向調査

b) ハイブリッドモードの構成方法の解説、および、安全性の解析・評価などについて公開されている文献などの調査およびそれらの解説

なお､調査は 2020 年 8 月末までに公開された標準化に関わる文献などを主たる対象とし、それ以降、評価報告書の提出時期までに公開された文献については可能な範囲で評価報告書に含めることとする。

---

[4] 今回の調査でハイブリッドモードという用語については合意の取れた定義は定まっていないことが確認された。

[5] https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/faqs

[6] https://csrc.nist.gov/Events/2019/second-pqc-standardization-conference

【2020 年度のスケジュール】

・2020 年 8 月 26 日 第 1 回 暗号解析評価 WG
調査の内容について WG で説明する。(事務局担当)

・2021 年 2 月 3 日　第 2 回 暗号解析評価 WG
評価報告書（案）に対する WG の見解をまとめる。

（ウ）　評価報告書のまとめ（菅野氏による見解）

評価報告書[7]では、調査対象とした標準化団体・組織においては、PQC と現代暗号の双方を併用するハイブリッドモードについて明確に言及/定義している文書は見つからなかったことが報告されている。一方、調査によりハイブリッドモードに関わる以下の動向が明らかとなったと報告されている。

[動向 1] PQC と現代暗号の双方を併用するハイブリッドモードの導入が検討されている背景として、調査対象とした標準化団体・組織では 3 つの懸念を抱えている。

- 懸念 1) 従来の暗号技術の安全性への懸念：量子コンピュータによる暗号技術への脅威が現実的になった時には、従来の暗号技術が安全性を保てなくなることへの懸念。
- 懸念 2) PQC の安全性への懸念：従来の暗号技術と比較して、PQC そのものが長期間利用されていないことから PQC の安全性評価手法などが成熟していないために、今後、脆弱性が発見されることへの懸念。
- 懸念 3) PQC の運用上の懸念：ネットワーク上に配置されている機器が PQC に対応していない場合に通信できない可能性への懸念。および、PQC を利用できる製品や環境がないことへの懸念。

[動向 2] PQC と現代暗号の双方を併用するハイブリッドモードを検討している標準化団体・組織では、ハイブリッドモードを導入することによりこれらの懸念を解消し、下記を達成する方法が議論されている。

I. 安全性の確保：ハイブリッドモードの中で利用されているいくつかの暗号技術の安全性に問題があったとしても、問題のない他の暗号技術によってハイブリッドモードとしての安全性を保つ。(懸念 1 及び懸念 2 への対策)

II. 後方互換性の確保：標準化やソフトウェア/ハードウェアへの実装のためのバッファ期間を確保し、暗号技術の移行やシステムマイグレーションを円滑に行う一助となる。(懸念 3 への対策)

PQC と現代暗号の双方を併用するハイブリッドモードの適用領域に関する評価報告書の記載概要は次のとおり。

- 暗号アルゴリズムとしては、ハイブリッドモードでの「鍵交換」と「ディジタル署名」での

[7] 詳しくは、付録 6、または、CRYPTREC EX-3004-2020(https://www.cryptrec.go.jp/exreport/cryptrec-ex-3004-2020.pdf)を参照のこと。

利用が有望であると多くの標準化団体・組織が述べている。ハイブリッドモードでの鍵交換については学術的な研究成果も発表されている。「鍵交換」と「ディジタル署名」については、ハイブリッドモードを適用することにより“I.安全性の確保”を達成することが模索されている。

- ネットワークプロトコルや証明書としては、「TLS」、「SSH」、「X.509 証明書」等を対象として、ハイブリッドモードでの鍵交換やハイブリッドモードでのディジタル署名の導入に向けた議論が IETF、Open Quantum-Safe(OQS)[8] などで行われている。例えば、IETF の TLS WG においては、TLS1.3 でハイブリッドモードを利用可能にするための Internet Draft が Working Group の検討項目として採択されるなど重要なテーマとしてコンセンサスが得られている。Open Quantum-Safe (OQS) では、NIST が主催している標準化会議で候補として残っている PQC を OpenSSL などに実装し、実際の世の中で利用されている TLS プロトコルや SSH プロトコルでの実現可能性を検討している。「TLS」、「SSH」、「X.509 証明書」等については、ハイブリッドモードでの鍵交換やハイブリッドモードでのディジタル署名の導入による“I.安全性の確保”を達成する方法が議論されている一方、“II.後方互換性の確保”の実現も併せて検討されている。

PQC と現代暗号の双方を併用するハイブリッドモードの構成に関わる安全性解析については、評価報告書では下記のようにまとめられている。

- 本調査の範囲において、ハイブリッドモードの脆弱性に関する文献は発見されなかった。しかし、ハイブリッドモードの安全性評価については現在のところ明らかになっていないところもある。

(エ) WG としての見解

評価報告書により、主要な標準化団体・組織による PQC と現代暗号の双方を併用するハイブリッドモードに関する現在の検討状況を把握できたため、本報告書を CRYPTREC の外部評価レポートとして HP に公開する。

5.3 節の評価報告書のまとめに記載した通り、ハイブリッドモードという用語については合意の取れた定義はなく、ハイブリッドモードが持つべきさまざまな要件が議論されている。特に、以下の二つの要件について議論されることが多い。

I. 安全性の確保：(システム・プロトコル・方式などの)中で利用されているいくつかの暗号技術の安全性に問題があったとしても、問題のない他の暗号技術によって全体としての安全性を保つ[1][2]。
II. 後方互換性の確保：暗号技術の移行やシステムマイグレーションを円滑に行う一助となる[1]。

ハイブリッドモードの安全性評価について現在のところ明らかになっていないところがある。また、ハイブリッドモードを含めて、PQC の実社会システムへの導入に関しては議論している段階にあり、今後も新たな定義や達成すべき要件などが提案される可能性がある。そのため、本 WG はそれらの技術動向について引き続き把握する必要があると結論する。

[8] Waterloo 大学を中心とした「PQC の開発とプロトタイピングをサポートする」プロジェクト

[本節の参考文献]

[1] E. Crockett, C. Paquin, D. Stebila: Prototyping post-quantum and hybrid key exchange and authentication in TLS and SSH, NIST 2nd Post-Quantum Cryptography Standardization Conference 2019.

[2] N. Bindel, J. Brendel, M. Fischlin, B. Goncalves, D. Stebila: Hybrid Key Encapsulation Mechanisms and Authenticated Key Exchange, PQCrypto 2019: 206-226

付録１

CRYPTREC LS-0001-2012R6

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

平成２５年３月１日
総務省・経済産業省
（最終更新：令和3年4月1日）

電子政府推奨暗号リスト

暗号技術検討会[1]及び関連委員会（以下、「CRYPTREC」という。）により安全性及び実装性能が確認された暗号技術[2]について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリスト。

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

[1] 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、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。

（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/active/general/pdf/angou_ikoushishin.pdf
（平成25年3月1日現在）

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

（注4） 初期化ベクトル長は96ビットを推奨する。

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

推奨候補暗号リスト

CRYPTRECにより安全性及び実装性能が確認され、今後、電子政府推奨暗号リストに掲載される可能性のある暗号技術[3]のリスト。

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

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

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

（注7） 平文サイズは64ビットの倍数に限る。

（注12） ハッシュ長は256ビット以上とすること。

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

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

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

運用監視暗号リスト

実際に解読されるリスクが高まるなど、推奨すべき状態ではなくなったとCRYPTRECにより確認された暗号技術[4]のうち、互換性維持のために継続利用を容認するもののリスト。互換性維持以外の目的での利用は推奨しない。

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

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

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

（注11） 安全性の観点から、メッセージ長を固定して利用すべきである。

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

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

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

変更履歴情報

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

	（注13） （注14） （注16）	[新規追加]	CRYPTREC暗号リスト掲載のブロック暗号を、認証付き秘匿モードと組み合わせて、「認証暗号」として使うことができる。
	電子政府推奨暗号リスト（見出し）	名称	暗号技術
	推奨候補暗号リスト（見出し）		
	運用監視暗号リスト（見出し）		
令和２年12月21日	推奨候補暗号リスト（技術分類：暗号利用モード　秘匿モード）	該当なし	XTS（注17）
	（注17）	[新規追加]	ブロック暗号には、CRYPTREC暗号リスト掲載128ビットブロック暗号を使う。利用用途はストレージデバイスの暗号化に限り、実装方法はNIST SP800-38Eに従うこと。
令和３年4月1日	運用監視暗号リスト（技術分類：共通鍵暗号）	128-bit RC4（注10）	該当なし
	（注10）	互換性維持のために継続利用をこれまで容認してきたが、今後は極力利用すべきでない。TLSでの利用を含め、電子政府推奨暗号リストに記載された暗号技術への移行を速やかに検討すること。	[削除]

付録２

CRYPTREC 暗号リスト掲載暗号技術の問合せ先一覧

電子政府推奨暗号リスト

1. 公開鍵暗号

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

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

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

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

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

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

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

2. 共通鍵暗号

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

暗号名	Camellia
関連情報	公開ホームページ
和文：https://info.isl.ntt.co.jp/crypt/camellia/ 英文：https://info.isl.ntt.co.jp/crypt/eng/camellia/	
問い合わせ先	〒180-8585 東京都武蔵野市緑町 3-9-11
日本電信電話株式会社　NTT セキュアプラットフォーム研究所 Camellia 問い合わせ窓口　担当 TEL: 0422-59-3557, FAX:0422-59-2971 E-MAIL: camellia-ml@hco.ntt.co.jp	

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

3. ハッシュ関数

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

4. 暗号利用モード(秘匿モード)

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

5. 暗号利用モード(認証付き秘匿モード)

暗号名	CCM
関連情報	仕様
	・ NIST SP 800-38C, Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, May 2004 ・ 参照 URL https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38c.pdf

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

6. メッセージ認証コード

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

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

7. エンティティ認証

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

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

推奨候補暗号リスト

1. 公開鍵暗号

暗号名	PSEC-KEM Key agreement
関連情報	公開ホームページ 和文：https://info.isl.ntt.co.jp/crypt/psec/ 英文：https://info.isl.ntt.co.jp/crypt/eng/psec/
問い合わせ先	〒180-8585 東京都武蔵野市緑町 3-9-11 日本電信電話株式会社　NTT セキュアプラットフォーム研究所 PSEC-KEM 問い合わせ窓口　担当 TEL: 0422-59-3462　　FAX: 0422-59-2971 E-MAIL: publickey-ml@hco.ntt.co.jp

2. 共通鍵暗号

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

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

暗号名	MISTY1
関連情報	公開ホームページ https://www.mitsubishielectric.co.jp/corporate/randd/information_technology/security/code/misty01_b.html
問い合わせ先	〒247-8520 神奈川県鎌倉市上町屋 325 番地 三菱電機株式会社 インフォメーションシステム統括事業部 技術部 IoT 技術課　坂上 勉 TEL：0467-41-3516 E-MAIL：Sakagami.Tsutomu@bp.MitsubishiElectric.co.jp

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

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

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

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

暗号名	MUGI
関連情報	公開ホームページ
和文：https://www.hitachi.co.jp/rd/yrl/crypto/mugi/ 英文：https://www.hitachi.com/rd/yrl/crypto/mugi/	
問い合わせ先	
株式会社日立製作所　IoT・クラウドサービス事業部 サイバーセキュリティ技術本部　セキュリティテクニカルセンタ 担当部長 栗田 博司 TEL：070-3854-4514, FAX ： 03-5471-2343 E-MAIL：hiroshi.kurita.wp@hitachi.com	

暗号名	Enocoro-128v2
関連情報	公開ホームページ
和文:https://www.hitachi.co.jp/rd/yrl/crypto/enocoro/ 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　社会システムイノベーションセンタ セキュリティ研究部　主任研究員　渡辺 大 E-MAIL: dai.watanabe.td@hitachi.com	

暗号名	MULTI-S01
関連情報	公開ホームページ 和文：https://www.hitachi.co.jp/rd/yrl/crypto/s01/ 英文：https://www.hitachi.com/rd/yrl/crypto/s01/
問い合わせ先	株式会社日立製作所　IoT・クラウドサービス事業部 サイバーセキュリティ技術本部　セキュリティテクニカルセンタ 担当部長 栗田 博司 TEL：070-3854-4514, FAX ： 03-5471-2343 E-MAIL：hiroshi.kurita.wp@hitachi.com

3. ハッシュ関数

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

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

4. 暗号利用モード（秘匿モード）

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

5. メッセージ認証コード

暗号名	PC-MAC-AES
関連情報	
参照 URL：https://jpn.nec.com/rd/crl/code/research/pcmacaes.html	
問い合わせ先	〒211-8666 神奈川県川崎市中原区下沼部 1753 日本電気株式会社　セキュアシステム研究所　主席研究員 峯松 一彦 TEL：044-431-7686, FAX：044-431-7644 E-MAIL: k-minematsu@nec.com

6. 認証暗号

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

7. エンティティ認証

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

運用監視暗号リスト

1. 公開鍵暗号

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

2. 共通鍵暗号

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

暗号名	RC4
関連情報	仕様
・ RC4 は EMC Corporation 社のトレードマークである。 ・ 仕様 RC4 のアルゴリズムについては、RSA Laboratories が発行した CryptoBytes 誌 (Volume5, No.2, Summer/Fall 2002) に掲載された次の論文に記載されているもの。 Fluhrer, Scott, Itsik Mantin, and Adi Shamir, "Attacks On RC4 and WEP", CryptoBytes, Volume 5, No.2, Summer/Fall 2002 ・ 参照 URL https://www.cryptrec.go.jp/cryptrec_13_spec_cypherlist_files/PDF/cryptobytes_v5n2.pdf	

3. ハッシュ関数

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

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

4. メッセージ認証コード

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

ディジタル署名 EdDSA で使われている曲線の安全性に関する調査及び評価 (エグゼクティブサマリー) [*1]

安田 雅哉（立教大学理学部）

2020 年 11 月 24 日

[*1] 原文は, CRYPTREC EX-3001-2020
https://www.cryptrec.go.jp/exreport/cryptrec-ex-3001-2020.pdf
から入手可能.

第 2 章

調査結果・評価結果の概要

■EdDSA で利用される曲線に関する解説　ディジタル署名 EdDSA では Edwards 曲線と呼ばれる特殊な楕円曲線やそのツイスト曲線を利用する．Edwards 曲線は xy 座標平面内の方程式 $x^2+y^2=1+dx^2y^2$ $(d\neq 0,1)$ で定義される曲線で，その曲線上の点の加算と 2 倍算を効率的に計算することができる．RFC8032 [31] によると，EdDSA では（古典計算機による）暗号攻撃に対して約 128 ビットのセキュリティレベルの Ed25519 と約 224 ビットのセキュリティレベルの Ed448 の 2 種類の実装のどちらかを安全性要件に応じて利用するよう推奨されている．また，Ed25519 では “Curve25519”，Ed448 では “Curve448” と呼ばれるツイスト Edwards 曲線パラメータを利用する．これらの曲線では，可能性のある暗号攻撃を避けるため，元の曲線とそのツイスト曲線の両方の位数が $4r$ または $8r$（ただし，r は巨大素数）の形となるように係数パラメータが選択されている．（ツイスト Edwards 曲線は位数 4 のねじれ点を持つので，4 以上の余因子を必ず持つことに注意する．）特に，Curve25519 は高速実装に適した 255 ビット素数 $p=2^{255}-19$ による素体 $\mathbb{F}_p$ を基礎体に持つ．

■EdDSA で利用される曲線に関して公開されている攻撃・脆弱性の調査　ディジタル署名を含む楕円曲線暗号の安全性は楕円曲線離散対数問題 (ECDLP) の求解困難性に基づく．ECDLP に対する攻撃法は，Pollard の ρ 法や指数計算法などの任意の楕円曲線に適用できる汎用攻撃アルゴリズムと，MOV 攻撃法や SSSA 攻撃などの特殊な楕円曲線にのみ適用可能な特殊攻撃アルゴリズムに大別される（攻撃法のまとめは 4.3 節を参照）．EdDSA で利用される Curve25519 や Curve448 では，MOV 攻撃法や SSSA 攻撃法が有効とならないような曲線パラメータが選択されているため，汎用攻撃アルゴリズムの中で最良の ρ 法が EdDSA に対する最良の攻撃法である．

■EdDSA で利用される曲線の安全性評価　EdDSA に対する最良の攻撃法である ρ 法攻撃は誕生日の逆理に基づく確率的アルゴリズムであるが，Edwards 曲線上の ECDLP に対する ρ 法は通常の楕円曲線とほぼ同じ振る舞いをすることが本報告書内の実験結果（後述の図 5.2）から分かる．これより，Edwards 曲線上の位数 r を持つ ECDLP の ρ 法による平均攻撃計算量は，誕生日の逆理から

$$\frac{\sqrt{\pi r}}{2}\cdot\mathbf{Ed}_{\mathrm{add}}\approx 0.8862\sqrt{r}\cdot\mathbf{Ed}_{\mathrm{add}}$$

と見積もれる．ここで，$\mathbf{Ed}_{\mathrm{add}}$ は Edwards 曲線上の点の加算コストとする．（ただし，攻撃者有利な条件として，Edwards 曲線上の逆元計算による $\sqrt{2}$ 倍の高速化も考慮した.）具体的には，Curve25519 の位数は $r \approx 2^{252}$ より，Curve25519 における ECDLP を攻撃するには，平均的に約 $0.8862 \cdot 2^{126} = 2^{125.8257}$ 回の点の加算が必要となる．また，Curve448 の位数は $r \approx 2^{446}$ より，Curve448 における ECDLP を攻撃するには，平均的に約 $0.8862 \cdot 2^{223} = 2^{222.8257}$ 回の点の加算が必要となる．一方，128 ビットセキュリティレベルの ECDSA での利用が推奨されている P-256 曲線に関して，P-256 の位数が $r \approx 2^{256}$ より，P-256 における ECDLP を攻撃するには，平均的に約 $0.8862 \cdot 2^{128} = 2^{127.8257}$ 回の点の加算が必要となる．これより，P-256 と同程度のセキュリティレベルに設定されている Curve25519 と安全性比較すると，Curve25519 上の方が平均的に約 4 倍少ない回数の楕円加算で攻撃できる．さらに，ツイスト Edwards 曲線は効率的な点の加算公式を持つため，P-256 よりも Curve25519 上の方がより効率的に点の加算が可能であり，ECDLP をより高速に攻撃できる．例えば，P-256 よりも Curve25519 の方が最大 2 倍高速に楕円加算ができたと想定すると，P-256 よりも Curve25519 における ECDLP の方が平均的に最大 8 倍高速に攻撃できる．ただし，Curve25519 における ECDLP を攻撃するには，少なくとも $2^{125.8257}$ 回の楕円加算が必要であり，ほぼ 128 ビットのセキュリティレベルを持つと結論付けれる．

■ECDSA と比較した場合の曲線としての効率性に関する考察　通常の楕円曲線と Edwards 曲線上の点の加算と 2 倍算の計算コスト比較は表 3.1 にまとめた．具体的には，基礎体上の乗算コスト $\mathbf{M}$ と 2 乗算コスト $\mathbf{S}$ の比が $\mathbf{S}/\mathbf{M} = 0.8$ の場合，通常の楕円曲線で標準的に利用する射影座標表現における点の加算コストは $10.8\mathbf{M}$ で 2 倍算コストは $9.8\mathbf{M}$ であるのに対し，Edwards 曲線の射影座標表現における点の加算コストは $9.8\mathbf{M}$ で 2 倍算コストは $6.2\mathbf{M}$ である．これより，同一の基礎体を利用した場合，射影座標表現では Edwards 曲線の方が点の加算で約 9.4%，点の 2 倍算で約 36.7% 効率的に計算できる．また，楕円曲線を利用したディジタル署名では，署名生成時に楕円曲線の点 P のスカラー倍算 nP を行い，署名検証時には楕円曲線の点 P_1, P_2 の複数スカラー倍算 $n_1P_1 + n_2P_2$ を主に行う．表 3.1 と同じように，表 5.1 に座標表現による楕円曲線上のスカラー倍算 nP の計算コスト比較をまとめた．表 5.1 より，同一の基礎体を利用した場合，スカラー倍算 nP に関しては Edwards 曲線の方が最大 33% 程度効率的に行うことができる．一方，表 5.2 に座標表現による楕円曲線上の複数スカラー倍算 $n_1P_1 + n_2P_2$ の計算コスト比較をまとめた．表 5.2 より，同一の基礎体を利用した場合，複数スカラー倍算 $n_1P_1 + n_2P_2$ に関しても Edwards 曲線の方が最大 28% 程度効率的に行うことができることが分かる．特に，EdDSA で利用される Curve25519 においては，高速実装に適した基礎体 $\mathbb{F}_p$ を選択しており，基礎体上の演算の高速化分を考慮すれば，更に効率的に（複数）スカラー倍算を行うことが可能となる．実際，図 5.3 に P-256 曲線による ECDSA と Curve25519 による EdDSA のハードウェア実装による処理時間の比較を示す．ただし，処理時間は鍵生成・署名生成・署名検証の合計時間で，その単位は cycles 数とする（詳細は [13] を参照）．ハードウェアの実装方法により処理時間が大きく異なるため参考程度ではあるが，図 5.3 より Curve25519 による EdDSA の方が最大 2 倍程度高速であることが分かる．

参考文献

[1] American National Standards Institute. American National Standard for Financial Services X9.62-2005, Public key cryptography for the financial services industry: The elliptic curve digital signature algorithm (ECDSA), 2005.

[2] Roberto M Avanzi. The complexity of certain multi-exponentiation techniques in cryptography. *Journal of Cryptology*, Vol. 18, No. 4, pp. 357–373, 2005.

[3] Daniel V Bailey, Lejla Batina, Daniel J Bernstein, Peter Birkner, Joppe W Bos, Hsieh-Chung Chen, Chen-Mou Cheng, Gauthier Van Damme, Giacomo de Meulenaer, Luis J Dominguez Perez, et al. Breaking ECC2K-130. *IACR ePrint Archive 2009/541*, 2009.

[4] Daniel J Bernstein. Curve25519: New Diffie-Hellman speed records. In *Public Key Cryptography–PKC 2006*, Vol. 3958 of *Lecture Notes in Computer Science*, pp. 207–228. Springer, 2006.

[5] Daniel J Bernstein, Peter Birkner, Marc Joye, Tanja Lange, and Christiane Peters. Twisted Edwards curves. In *Progress in Cryptology–AFRICACRYPT 2008*, Vol. 5023 of *Lecture Notes in Computer Science*, pp. 389–405. Springer, 2008.

[6] Daniel J Bernstein, Niels Duif, Tanja Lange, Peter Schwabe, and Bo-Yin Yang. High-speed high-security signatures. *Journal of Cryptographic Engineering*, Vol. 2, No. 2, pp. 77–89, 2012.

[7] Daniel J Bernstein, Susanne Engels, Tanja Lange, Ruben Niederhagen, Christof Paar, Peter Schwabe, and Ralf Zimmermann. Faster elliptic-curve discrete logarithms on FPGAs. *IACR ePrint Archive 2016/382*, 2016.

[8] Daniel J Bernstein, Simon Josefsson, Tanja Lange, Peter Schwabe, and Bo-Yin Yang. EdDSA for more curves. *IACR ePrint Archive 2015/677*, 2015.

[9] Daniel J Bernstein and Tanja Lange. Faster addition and doubling on elliptic curves. In *Advances in Cryptology–ASIACRYPT 2007*, Vol. 4833 of *Lecture Notes in Computer Science*, pp. 29–50. Springer, 2007.

[10] Daniel J Bernstein and Tanja Lange. Inverted Edwards coordinates. In *Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes (AAECC 2007)*, Vol. 4851 of *Lecture Notes in Computer Science*, pp. 20–27. Springer, 2007.

[11] Daniel J Bernstein and Tanja Lange. Explicit-formula database (EFD). https://www.hyperelliptic.org/EFD/, since 2007.

[12] Daniel J Bernstein and Tanja Lange. SafeCurves: Choosing safe curves for elliptic-curve cryptography. https://safecurves.cr.yp.to/, since 2014.

[13] Daniel J Bernstein and Tanja Lange. eBACS: ECRYPT benchmarking of cryptographic systems. http://bench.cr.yp.to/, version 2019.08.05.

[14] Daniel J Bernstein, Tanja Lange, and Peter Schwabe. On the correct use of the negation map in the Pollard rho method. In *Public Key Cryptography–PKC 2011*, Vol. 6571 of *Lecture Notes in Computer Science*, pp. 128–146. Springer, 2011.

[15] Ian Blake, Gerald Seroussi, Gadiel Seroussi, and Nigel Smart. *Elliptic Curves in Cryptography*, Vol. 265. Cambridge university press, 1999.

[16] Joppe W Bos, Marcelo E Kaihara, Thorsten Kleinjung, Arjen K Lenstra, and Peter L Montgomery. Solving a 112-bit prime elliptic curve discrete logarithm problem on game consoles using sloppy reduction. *International Journal of Applied Cryptography*, Vol. 2, No. 3, pp. 212–228, 2012.

[17] Joppe W Bos and Arjen K Lenstra. *Topics in Computational Number Theory Inspired by Peter L. Montgomery*. Cambridge University Press, 2017.

[18] ECC Brainpool. ECC Brainpool standard curves and curve generation. https://www.teletrust.de/fileadmin/files/oid/oid_ECC-Brainpool-Standard-curves-V1.pdf, 2005.

[19] Henri Cohen, Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen, and Frederik Vercauteren. *Handbook of Elliptic and Hyperelliptic Curve Cryptography*. CRC press, 2005.

[20] Harold Edwards. A normal form for elliptic curves. *Bulletin of the American mathematical society*, Vol. 44, No. 3, pp. 393–422, 2007.

[21] Gerhard Frey and Hans-Georg Rück. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. *Mathematics of computation*, Vol. 62, No. 206, pp. 865–874, 1994.

[22] Steven D Galbraith. *Mathematics of Public Key Cryptography*. Cambridge University Press, 2012.

[23] Steven D Galbraith and Pierrick Gaudry. Recent progress on the elliptic curve discrete logarithm problem. *Designs, Codes and Cryptography*, Vol. 78, No. 1, pp. 51–72, 2016.

[24] Robert Gallant, Robert Lambert, and Scott Vanstone. Improving the parallelized Pollard lambda search on anomalous binary curves. *Mathematics of Computation*, Vol. 69, No. 232, pp. 1699–1705, 2000.

[25] The Sage Group. SageMath: Open-source mathematical software system. https://www.sagemath.org/.

[26] Mike Hamburg. Ed448-Goldilocks, a new elliptic curve. *IACR ePrint Archive 2015/625*, 2015.

[27] Darrel Hankerson, Alfred J Menezes, and Scott Vanstone. *Guide to Elliptic Curve Cryptography*. Springer Science & Business Media, 2006.

[28] Huseyin Hisil, Kenneth Koon-Ho Wong, Gary Carter, and Ed Dawson. Twisted Edwards curves revisited. In *Advances in Cryptology–ASIACRYPT 2008*, Vol. 5350 of *Lecture Notes in Computer Science*, pp. 326–343. Springer, 2008.

[29] Ming-Deh Huang, Michiel Kosters, Christophe Petit, Sze Ling Yeo, and Yang Yun. Quasi-subfield polynomials and the elliptic curve discrete logarithm problem. *Journal of Mathematical Cryptology*, Vol. 14, No. 1, pp. 25–38, 2020.

[30] Michael J Jacobson, Neal Koblitz, Joseph H Silverman, Andreas Stein, and Edlyn Teske. Analysis of the xedni calculus attack. *Designs, Codes and Cryptography*, Vol. 20, No. 1, pp. 41–64, 2000.

[31] Simon Josefsson and Ilari Liusvaara. RFC 8032: Edwards-curve digital signature algorithm (EdDSA). Internet Engineering Task Force (IETF). `https://tex2e.github.io/rfc-translater/html/rfc8032.html`, 2017.

[32] Neal Koblitz. Elliptic curve cryptosystems. *Mathematics of computation*, Vol. 48, No. 177, pp. 203–209, 1987.

[33] Momonari Kudo, Yuki Yokota, Yasushi Takahashi, and Masaya Yasuda. Acceleration of index calculus for solving ECDLP over prime fields and its limitation. In *Cryptology and Network Security (CANS 2018)*, Vol. 11124 of *Lecture Notes in Computer Science*, pp. 377–393. Springer, 2018.

[34] Takuya Kusaka, Sho Joichi, Ken Ikuta, Md Al-Amin Khandaker, Yasuyuki Nogami, Satoshi Uehara, Nariyoshi Yamai, and Sylvain Duquesne. Solving 114-bit ECDLP for a Barreto-Naehrig curve. In *Information Security and Cryptology (ICISC 2017)*, Vol. 10779 of *Lecture Notes in Computer Science*, pp. 231–244. Springer, 2017.

[35] A Langley, M Hamburg, and S Turner. RFC 7748: Elliptic curves for security. Internet Engineering Task Force (IETF). `https://tools.ietf.org/pdf/rfc7748.pdf`, 2016.

[36] Alfred J Menezes, Tatsuaki Okamoto, and Scott A Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Transactions on information Theory*, Vol. 39, No. 5, pp. 1639–1646, 1993.

[37] Victor S Miller. Use of elliptic curves in cryptography. In *Advances in Cryptology–CRYPTO 1985*, Vol. 218 of *Lecture Notes in Computer Science*, pp. 417–426. Springer, 1985.

[38] Institute of Electrical and Electronics Engineers. IEEE 1363-2000: Standard specifications for public key cryptography. `https://perso.telecom-paristech.fr/guilley/recherche/cryptoprocesseurs/ieee/00891000.pdf`, 2000.

[39] Christophe Petit, Michiel Kosters, and Ange Messeng. Algebraic approaches for the elliptic curve discrete logarithm problem over prime fields. In *Public-Key Cryptography–PKC 2016*, Vol. 9615 of *Lecture Notes in Computer Science*, pp. 3–18. Springer, 2016.

[40] Stephen Pohlig and Martin Hellman. An improved algorithm for computing logarithms over GF(p) and its cryptographic significance. *IEEE Transactions on information Theory*, Vol. 24, No. 1, pp. 106–110, 1978.

[41] John M Pollard. Monte carlo methods for index computation (mod p). *Mathematics of computation*, Vol. 32, No. 143, pp. 918–924, 1978.

[42] John M Pollard. Kangaroos, monopoly and discrete logarithms. *Journal of cryptology*, Vol. 13, No. 4, pp. 437–447, 2000.

[43] Certicom Research. Standards for efficient crytography 2: Recommended elliptic curve domain parameters. `https://www.secg.org/SEC2-Ver-1.0.pdf`, 2000.

[44] Certicom Research. Standards for efficient crytography, SEC1: Elliptic curve cryptography (version 2.0). `https://www.secg.org/sec1-v2.pdf`, 2009.

[45] Certicom Research. The Certicom ECC Challenge. `https://www.certicom.com/content/certicom/en/the-certicom-ecc-challenge.html`, since 1997.

[46] Takakazu Satoh, Kiyomichi Araki, et al. Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves. *Rikkyo Daigaku sugaku zasshi*, Vol. 47, No. 1, pp. 81–92, 1998.

[47] Igor Semaev. Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p. *Mathematics of computation*, Vol. 67, No. 221, pp. 353–356, 1998.

[48] Igor A Semaev. Summation polynomials and the discrete logarithm problem on elliptic curves. *IACR ePrint Archive 2004/31*, 2004.

[49] Daniel Shanks. Class number, a theory of factorization, and genera. In *Symposia in Pure Mathematics*, Vol. 20, pp. 415–440, 1971.

[50] Joseph H Silverman. The xedni calculus and the elliptic curve discrete logarithm problem. *Designs, Codes and Cryptography*, Vol. 20, No. 1, pp. 5–40, 2000.

[51] Joseph H Silverman. *The Arithmetic of Elliptic Curves*, Vol. 106. Springer Science & Business Media, second edition, 2009.

[52] Nigel P Smart. The discrete logarithm problem on elliptic curves of trace one. *Journal of cryptology*, Vol. 12, No. 3, pp. 193–196, 1999.

[53] Edlyn Teske. Speeding up Pollard's rho method for computing discrete logarithms. In *Algorithmic Number Theory (ANTS 1998)*, Vol. 1423 of *Lecture Notes in Computer Science*, pp. 541–554. Springer, 1998.

[54] Edlyn Teske. On random walks for Pollard's rho method. *Mathematics of computation*, Vol. 70, No. 234, pp. 809–825, 2001.

[55] Paul C Van Oorschot and Michael J Wiener. Parallel collision search with cryptanalytic

applications. *Journal of cryptology*, Vol. 12, No. 1, pp. 1–28, 1999.

[56] Lawrence C Washington. *Elliptic Curves: Number Theory and Cryptography*. CRC press, second edition, 2008.

[57] Erich Wenger and Paul Wolfger. Solving the discrete logarithm of a 113-bit Koblitz curve with an FPGA cluster. In *Selected Areas in Cryptography (SAC 2014)*, Vol. 8781 of *Lecture Notes in Computer Science*, pp. 363–379. Springer, 2014.

[58] Michael J Wiener and Robert J Zuccherato. Faster attacks on elliptic curve cryptosystems. In *Selected Areas in Cryptography (SAC 1998)*, Vol. 1556 of *Lecture Notes in Computer Science*, pp. 190–200. Springer, 1998.

[59] Masaya Yasuda, Tetsuya Izu, Takeshi Shimoyama, and Jun Kogure. On random walks of Pollard's rho method for the ECDLP on Koblitz curves. *Journal of Math-for-Industry*, Vol. 3, No. 3, pp. 107–112, 2011.

[60] Masaya Yasuda, Takeshi Shimoyama, Jun Kogure, and Tetsuya Izu. Computational hardness of IFP and ECDLP. *Applicable Algebra in Engineering, Communication and Computing*, Vol. 27, No. 6, pp. 493–521, 2016.

[61] Kazuhiro Yokoyama, Masaya Yasuda, Yasushi Takahashi, and Jun Kogure. Complexity bounds on Semaev's naive index calculus method for ECDLP. *Journal of Mathematical Cryptology*, Vol. 14, No. 1, pp. 460–485, 2020.

[62] 富士通株式会社, 株式会社富士通研究所. 楕円曲線暗号と RSA 暗号の安全性比較. `https://www.fujitsu.com/jp/group/labs/documents/resources/tech/external-activities/crypto/eccvsrsa-20100820.pdf`, 2010 年 8 月 20 日.

[63] 篠原直行, 野呂正行, 横山和弘. 楕円曲線上の離散対数問題に関する指数計算法. CRYPTREC-EX-2602-2016: `https://www.cryptrec.go.jp/exreport/cryptrec-ex-2602-2016.pdf`, 2016.

ディジタル署名 EdDSA の構成の安全性に関する調査および評価 (エグゼクティブサマリー) [*1]

北陸先端科学技術大学院大学

藤崎　英一郎

2020 年 12 月

[*1] 原文は, CRYPTREC EX-3002-2020
https://www.cryptrec.go.jp/exreport/cryptrec-ex-3002-2020.pdf
から入手可能.

エグゼクティブサマリー

本報告書はディジタル署名 EdDSA の安全性に関する評価結果を報告するものである．EdDSA とは Internet Research Task Force (IRTF) の RFC8032 [62] で規定されるディジタル署名のことであり，有限体上のツイスト Edwards 曲線 [35, 12] といわれる楕円曲線上の Schnorr 署名 [66, 67] の署名内部乱数（ノンス）を署名者の秘密情報と署名される平文のハッシュ値に置き換えた確定的 (determinisitic) 版の Schnorr 署名である．EdDSA で推奨される ツイスト Edwards 曲線は IRTF の RFC7748 [61] で規定されるものであり Ed25519，Ed448 と記述される．以下評価結果の概要を述べる．

- **ツイスト Edwards 曲線の安全性について．** Ed25519 や Ed448 は Curve25519 や Curve448 と同型なため安全性の根拠となる離散対数問題に特に問題があると思えない．
- **Schnorr 署名との違い．**一番大きな違いは署名内部乱数（ノンス）を署名者の秘密情報と平文のハッシュ値で生成し署名を確定的かつ異なる平文に対してノンスを衝突させにくくしたことである．また内部で使うハッシュ関数の出力長をかなり長くし，群の位数で剰余を取っている，Key-prefixing を採用している（後述），さらに群要素チェックが通常の Schnorr 署名より緩くなっているなどがある．
- **証明可能安全性．**Schnorr 署名をもとに EdDSA 署名は構成されているため，Schnorr 署名に対する安全性評価を利用できるが，Ed25519 ではハッシュ関数に SHA512 を使用しているためその内部の Merkle-Damgård 構造によりランダム関数と識別がつきランダムオラクルモデルでの安全性解析が使えない．また generic group model でも同様に安全性解析をするのも障害がある．一方，Ed448 ではランダムオラクルモデルや generic group model での Schnorr 署名の解析結果が利用でき安全性にある程度の理論的根拠を与えることができる．
- **ビット安全性．**Ed448-EdDSA 署名はランダムオラクルモデルでの解析で 112 ビット程度の安全性，generic group model での解析では 224 ビット程度の安全性が期待できる．
- **Key-prefixing.** EdDSA 署名は key-prefixing という署名者自身の公開鍵を平文と連結させ，公開鍵と平文に署名を付けさせる形を取っている．この仕様のため関連鍵攻撃に対して耐性が上がっている．
- **複数署名者での安全性．** 通常の署名方式は署名者が増えると署名者の数に応じて証明可能安全性で保証できるビット安全性は劣化する．EdDSA 署名は複数署名者でのビット安全性が署名者の数に関係せず，単一署名者の Schnorr 署名のビット安全性で抑えることができる．
- **PureEdDSA と HashEdDSA.** EdDSA で署名するとき，PureEdDSA と HashEdDSA というどちらかのオプションを選ぶ必要がある．HashEdDSA では平文を署名する前に

ハッシュ関数で圧縮してから署名アルゴリズムに入力する．一方，PureEdDSA は平文を直接署名アルゴリズムに入力する．HashEdDSA では前処理で平文を圧縮しておくことができるため効率が良いが，ハッシュの衝突耐性以上の安全性を持たない．一方，PureEdDSA はハッシュの衝突耐性以上の安全性を持つ可能性がある．

- **ノンスについて．**Ed25519-EdDSA ではノンスの出力が疑似ランダム関数の出力とみることが出来ないため証明可能安全性の意味では証明がつかなくなっている．しかし，現実の攻撃を考えると異なる平文に対するノンスの衝突こそが 1 番に回避しなければならないものでありハッシュ関数でノンスを生成することでこれを回避している．
- **ECDSA 署名との比較．**安全性において EdDSA 署名が ECDSA 署名に劣ると考えられる点は無いと考えられる．単独の署名生成及び検証の計算時間について比べた時，署名される平文がさほど長くない（平文をハッシュする時間が十分短い）場合 EdDSA 署名が ECDSA 署名よりやや少ない．ただし平文が極めて長い場合，両署名の署名生成時間はほぼハッシュ関数の計算時間となってしまうため，2 回平文のハッシュ値を計算しなければいけない EdDSA 署名の署名生成時間は 1 回のハッシュ値生成で済む ECDSA 署名のほぼ 2 倍かかってしまう．この場合署名検証時間は両方式でほぼ同程度である．単独署名者の複数の署名を検証する場合，EdDSA 署名はバッチ検証処理が使え，同一署名者の場合署名検証をかなり高速にできる．一方，ECDSA 署名は EdDSA 署名ほどの高速化技法は知られていない．
- **サイドチャネル攻撃耐性．**ツイスト Edwards 曲線上の演算は加法と 2 倍算を計算式の切り替えなしに行うことが可能である．一方，より高速に計算するために加法と 2 倍算を別の式で切り替えるやり方も RFC8032 には記載されている．共通式を使うとタイミング攻撃や電力解析攻撃に強くなることが期待できるが，これらの攻撃が本格的にできる環境においてはさらなる対策が必要かもしれない．多くの実装に使用される SUPERCOP [71] の EdDSA 署名は（加法と 2 倍算を切り替える高速版を使った上で）スカラー倍算の加法と 2 倍算の呼び出しが（群位数のサイズの）定数回になるよう実装されており，タイミング攻撃と電力解析攻撃に対する本格的な対策が施されている．近年確定ノンスを使う EdDSA 署名のような確定型署名に対する新たなフォルト攻撃も提案されており，組み込みデバイスとして利用するような場合，将来的にはさらなる対策をとる必要があるかもしれない．

以上の評価により，EdDSA 署名は証明可能安全性という枠組みでは不十分であったり十分なビット安全性が保証されなかったりするが，Schnorr 署名という成熟した方式をもとにノンスの生成で既存の攻撃を注意深く回避する配慮がされており現実的には安全であるという結論を得た．

参考文献

[1] Christopher Ambrose, Joppe W. Bos, Björn Fay, Marc Joye, Manfred Lochter, and Bruce Murray. Differential attacks on deterministic signatures. In Nigel P. Smart, editor, *Topics in Cryptology – CT-RSA 2018*, Vol. 10808 of *Lecture Notes in Computer Science*, pp. 339–353. Springer, Heidelberg, April 2018.

[2] Diego F. Aranha, Pierre-Alain Fouque, Benoît Gérard, Jean-Gabriel Kammerer, Mehdi Tibouchi, and Jean-Christophe Zapalowicz. GLV/GLS decomposition, power analysis, and attacks on ECDSA signatures with single-bit nonce bias. In Palash Sarkar and Tetsu Iwata, editors, *Advances in Cryptology – ASIACRYPT 2014, Part I*, Vol. 8873 of *Lecture Notes in Computer Science*, pp. 262–281. Springer, Heidelberg, December 2014.

[3] Diego F. Aranha, Felipe Rodrigues Novaes, Akira Takahashi, Mehdi Tibouchi, and Yuval Yarom. LadderLeak: Breaking ECDSA with less than one bit of nonce leakage. In *ACM CCS 20: 27th Conference on Computer and Communications Security*, pp. 225–242. ACM Press, 2020.

[4] Diego F. Aranha, Claudio Orlandi, Akira Takahashi, and Greg Zaverucha. Security of hedged Fiat-Shamir signatures under fault attacks. Cryptology ePrint Archive, Report 2019/956, 2019. `https://eprint.iacr.org/2019/956`.

[5] Alessandro Barenghi and Gerardo Pelosi. A note on fault attacks against deterministic signature schemes. In Kazuto Ogawa and Katsunari Yoshioka, editors, *IWSEC 16: 11th International Workshop on Security, Advances in Information and Computer Security*, Vol. 9836 of *Lecture Notes in Computer Science*, pp. 182–192. Springer, Heidelberg, September 2016.

[6] Mihir Bellare, Juan A. Garay, and Tal Rabin. Fast batch verification for modular exponentiation and digital signatures. In Kaisa Nyberg, editor, *Advances in Cryptology – EUROCRYPT'98*, Vol. 1403 of *Lecture Notes in Computer Science*, pp. 236–250. Springer, Heidelberg, May / June 1998.

[7] Mihir Bellare and Gregory Neven. Multi-signatures in the plain public-key model and a general forking lemma. In Ari Juels, Rebecca N. Wright, and Sabrina De Capitani di Vimercati, editors, *ACM CCS 2006: 13th Conference on Computer and Communications Security*, pp. 390–399. ACM Press, October / November 2006.

[8] Daniel J. Bernstein. Curve25519: New Diffie-Hellman speed records. In Moti Yung, Yevgeniy Dodis, Aggelos Kiayias, and Tal Malkin, editors, *PKC 2006: 9th International Conference on Theory and Practice of Public Key Cryptography*, Vol. 3958 of *Lecture*

Notes in Computer Science, pp. 207–228. Springer, Heidelberg, April 2006.

[9] Daniel J. Bernstein. Multi-user Schnorr security, revisited. Cryptology ePrint Archive, Report 2015/996, 2015. http://eprint.iacr.org/2015/996.

[10] Daniel J. Bernstein, Peter Birkner, Marc Joye, Tanja Lange, and Christiane Peters. Twisted edwards curves. Cryptology ePrint Archive, Report 2008/013, 2008. https://eprint.iacr.org/2008/013.

[11] Daniel J. Bernstein, Peter Birkner, Marc Joye, Tanja Lange, and Christiane Peters. Twisted Edwards curves. Cryptology ePrint Archive, Report 2008/013, 2008. http://eprint.iacr.org/2008/013.

[12] Daniel J. Bernstein, Niels Duif, Tanja Lange, Peter Schwabe, and Bo-Yin Yang. High-speed high-security signatures. *J. Cryptogr. Eng.*, Vol. 2, No. 2, pp. 77–89, 2012.

[13] Daniel J. Bernstein, Simon Josefsson, Tanja Lange, Peter Schwabe, and Bo-Yin Yang. EdDSA for more curves. Cryptology ePrint Archive, Report 2015/677, 2015. http://eprint.iacr.org/2015/677.

[14] Daniel J. Bernstein and Tanja Lange. Faster addition and doubling on elliptic curves. Cryptology ePrint Archive, Report 2007/286, 2007. http://eprint.iacr.org/2007/286.

[15] Daniel Bleichenbacher. On the generation of one-time keys in dl signature schemes. Presentation at IEEE P1363 working group meeting, 2000.

[16] Dan Boneh and Ramarathnam Venkatesan. Hardness of computing the most significant bits of secret keys in Diffie-Hellman and related schemes. In Neal Koblitz, editor, *Advances in Cryptology – CRYPTO'96*, Vol. 1109 of *Lecture Notes in Computer Science*, pp. 129–142. Springer, Heidelberg, August 1996.

[17] Jurjen N. Bos and Matthijs J. Coster. Addition chain heuristics. In Gilles Brassard, editor, *Advances in Cryptology – CRYPTO'89*, Vol. 435 of *Lecture Notes in Computer Science*, pp. 400–407. Springer, Heidelberg, August 1990.

[18] Daniel R. L. Brown. The exact security of ECDSA. Contributions to IEEE P1363a, January 2001. http://grouper.ieee.org/groups/1363/.

[19] Daniel R. L. Brown. Generic groups, collision resistance, and ECDSA. Contributions to IEEE P1363a, February 2002. Updated version for "The Exact Security of ECDSA." Available from http://grouper.ieee.org/groups/1363/.

[20] Daniel R. L. Brown. Generic groups, collision resistance, and ECDSA. Cryptology ePrint Archive, Report 2002/026, 2002. http://eprint.iacr.org/2002/026.

[21] Daniel R. L. Brown. Generic groups, collision resistance, and ECDSA. *Des. Codes Cryptogr.*, Vol. 35, No. 1, pp. 119–152, 2005.

[22] Daniel R. L. Brown. Short Schnorr signatures require a hash function with more than just random-prefix resistance. Cryptology ePrint Archive, Report 2015/169, 2015. http://eprint.iacr.org/2015/169.

[23] Michael Brown, Darrel Hankerson, Julio Cesar López-Hernández, and Alfred Menezes. Software implementation of the NIST elliptic curves over prime fields. In David Naccache, editor, *Topics in Cryptology – CT-RSA 2001*, Vol. 2020 of *Lecture Notes in Computer Science*, pp. 250–265. Springer, Heidelberg, April 2001.

[24] Leon Groot Bruinderink and Peter Pessl. Differential fault attacks on deterministic lattice signatures. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, Vol. 2018, No. 3, pp. 21–43, 2018. https://tches.iacr.org/index.php/TCHES/article/view/7267.

[25] Jan Camenisch, Susan Hohenberger, and Michael Østergaard Pedersen. Batch verification of short signatures. In Moni Naor, editor, *Advances in Cryptology – EUROCRYPT 2007*, Vol. 4515 of *Lecture Notes in Computer Science*, pp. 246–263. Springer, Heidelberg, May 2007.

[26] Weiqiong Cao, Hongsong Shi, Hua Chen, Jiazhe Chen, Limin Fan, and Wenling Wu. Lattice-based fault attacks on deterministic signature schemes of ECDSA and EdDSA. Cryptology ePrint Archive, Report 2020/803, 2020. https://eprint.iacr.org/2020/803.

[27] Konstantinos Chalkias, FrançoisGarillot, Valeria Nikolaenko. Taming the many eddsas. Cryptology ePrint Archive, Report 2020/1244, 2020. Security Standardisation Research Conference (SSR 2020).

[28] Yuh-Jiun Chen, Chin-Chen Chang, and Wei-Pang Yang. Some properties of vectorial addition chains. *International Journal of Computer Mathematics*, Vol. 54, No. 3-4, pp. 185–196, 1994.

[29] Jung Hee Cheon and Jeong Hyun Yi. Fast batch verification of multiple signatures. In Tatsuaki Okamoto and Xiaoyun Wang, editors, *PKC 2007: 10th International Conference on Theory and Practice of Public Key Cryptography*, Vol. 4450 of *Lecture Notes in Computer Science*, pp. 442–457. Springer, Heidelberg, April 2007.

[30] Henri Cohen, Atsuko Miyaji, and Takatoshi Ono. Efficient elliptic curve exponentiation using mixed coordinates. In Kazuo Ohta and Dingyi Pei, editors, *Advances in Cryptology – ASIACRYPT'98*, Vol. 1514 of *Lecture Notes in Computer Science*, pp. 51–65. Springer, Heidelberg, October 1998.

[31] Cryptography Research and Evaluation Committees. https://www.cryptrec.go.jp/.

[32] Ivan Damgård. A design principle for hash functions. In Gilles Brassard, editor, *Advances*

in Cryptology – CRYPTO'89, Vol. 435 of *Lecture Notes in Computer Science*, pp. 416–427. Springer, Heidelberg, August 1990.

[33] Elke De Mulder, Michael Hutter, Mark E. Marson, and Peter Pearson. Using Bleichenbacher's solution to the hidden number problem to attack nonce leaks in 384-bit ECDSA: extended version. *Journal of Cryptographic Engineering*, Vol. 4, No. 1, pp. 33–45, April 2014.

[34] Peter de Rooij. Efficient exponentiation using procomputation and vector addition chains. In Alfredo De Santis, editor, *Advances in Cryptology – EUROCRYPT'94*, Vol. 950 of *Lecture Notes in Computer Science*, pp. 389–399. Springer, Heidelberg, May 1995.

[35] Harold M. Edwards. A normal form for elliptic curves. In *Bulletin of the American Mathematical Society*, pp. 393–422, 2007.

[36] Björn Fay. Double-and-add with relative Jacobian coordinates. Cryptology ePrint Archive, Report 2014/1014, 2014. `http://eprint.iacr.org/2014/1014`.

[37] Manuel Fersch, Eike Kiltz, and Bertram Poettering. On the provable security of (EC)DSA signatures. In Edgar R. Weippl, Stefan Katzenbeisser, Christopher Kruegel, Andrew C. Myers, and Shai Halevi, editors, *ACM CCS 2016: 23rd Conference on Computer and Communications Security*, pp. 1651–1662. ACM Press, October 2016.

[38] Steven D. Galbraith, Xibin Lin, and Michael Scott. Endomorphisms for faster elliptic curve cryptography on a large class of curves. In Antoine Joux, editor, *Advances in Cryptology – EUROCRYPT 2009*, Vol. 5479 of *Lecture Notes in Computer Science*, pp. 518–535. Springer, Heidelberg, April 2009.

[39] Steven D. Galbraith, John Malone-Lee, and Nigel P. Smart. Public key signatures in the multi-user setting. *Inf. Process. Lett.*, Vol. 83, No. 5, pp. 263–266, 2002.

[40] Pierrick Gaudry and Emmanuel Thome. The mpfq library and implementing curve-based key exchanges. Technical report, Institut National de Recherche en Informatique et en Automatique, 2007.

[41] Keisuke Hakuta, Yosuke Katoh, Hisayoshi Sato, and Tsuyoshi Takagi. Batch verification suitable for efficiently verifying a limited number of signatures. In Taekyoung Kwon, Mun-Kyu Lee, and Daesung Kwon, editors, *ICISC 12: 15th International Conference on Information Security and Cryptology*, Vol. 7839 of *Lecture Notes in Computer Science*, pp. 425–440. Springer, Heidelberg, November 2013.

[42] Nick Howgrave-Graham and N. Smart. Lattice attacks on digital signature schemes. *Designs, Codes and Cryptography*, Vol. 23, pp. 283–290, 2001.

[43] Jung Hee Cheon and Dong Hoon Lee. Use of sparse and/or complex exponents in batch verification of exponentiations. *IEEE Transactions on Computers*, Vol. 55, No. 12, pp.

1536–1542, 2006.

[44] Sabyasachi Karati and Abhijit Das. Faster batch verification of standard ECDSA signatures using summation polynomials. In Ioana Boureanu, Philippe Owesarski, and Serge Vaudenay, editors, *ACNS 14: 12th International Conference on Applied Cryptography and Network Security*, Vol. 8479 of *Lecture Notes in Computer Science*, pp. 438–456. Springer, Heidelberg, June 2014.

[45] Sabyasachi Karati, Abhijit Das, Dipanwita Roy Chowdhury, Bhargav Bellur, Debojyoti Bhattacharya, and Aravind Iyer. Batch verification of ECDSA signatures. In Aikaterini Mitrokotsa and Serge Vaudenay, editors, *AFRICACRYPT 12: 5th International Conference on Cryptology in Africa*, Vol. 7374 of *Lecture Notes in Computer Science*, pp. 1–18. Springer, Heidelberg, July 2012.

[46] John Kelsey and Tadayoshi Kohno. Herding hash functions and the Nostradamus attack. In Serge Vaudenay, editor, *Advances in Cryptology – EUROCRYPT 2006*, Vol. 4004 of *Lecture Notes in Computer Science*, pp. 183–200. Springer, Heidelberg, May / June 2006.

[47] Patrick Longa and Catherine H. Gebotys. Efficient techniques for high-speed elliptic curve cryptography. In Stefan Mangard and François-Xavier Standaert, editors, *Cryptographic Hardware and Embedded Systems – CHES 2010*, Vol. 6225 of *Lecture Notes in Computer Science*, pp. 80–94. Springer, Heidelberg, August 2010.

[48] Edwin El Mahassni, Phong Q. Nguyen, and Igor E. Shparlinski. The insecurity of nyberg-rueppel and other dsa-like signature schemes with partially known nonces. In Joseph H. Silverman, editor, *Cryptography and Lattices, International Conference, CaLC 2001, Providence, RI, USA, March 29-30, 2001, Revised Papers*, Vol. 2146 of *Lecture Notes in Computer Science*, pp. 97–109. Springer, 2001.

[49] Alfred Menezes and Nigel P. Smart. Security of signature schemes in a multi-user setting. *Des. Codes Cryptogr.*, Vol. 33, No. 3, pp. 261–274, 2004.

[50] Ralph C. Merkle. A certified digital signature. In Gilles Brassard, editor, *Advances in Cryptology – CRYPTO'89*, Vol. 435 of *Lecture Notes in Computer Science*, pp. 218–238. Springer, Heidelberg, August 1990.

[51] Hiraku Morita, Jacob C. N. Schuldt, Takahiro Matsuda, Goichiro Hanaoka, and Tetsu Iwata. On the security of the schnorr signature scheme and DSA against related-key attacks. In Soonhak Kwon and Aaram Yun, editors, *ICISC 15: 18th International Conference on Information Security and Cryptology*, Vol. 9558 of *Lecture Notes in Computer Science*, pp. 20–35. Springer, Heidelberg, November 2016.

[52] David Naccache, David M'Raïhi, Serge Vaudenay, and Dan Raphaeli. Can D.S.A. be improved? Complexity trade-offs with the digital signature standard. In Alfredo De

Santis, editor, *Advances in Cryptology – EUROCRYPT'94*, Vol. 950 of *Lecture Notes in Computer Science*, pp. 77–85. Springer, Heidelberg, May 1995.

[53] David Naccache, Phong Q. Nguyen, Michael Tunstall, and Claire Whelan. Experimenting with faults, lattices and the DSA. In Serge Vaudenay, editor, *PKC 2005: 8th International Workshop on Theory and Practice in Public Key Cryptography*, Vol. 3386 of *Lecture Notes in Computer Science*, pp. 16–28. Springer, Heidelberg, January 2005.

[54] Gregory Neven, Nigel P. Smart, and Bogdan Warinschi. Hash function requirements for schnorr signatures. *J. Math. Cryptol.*, Vol. 3, No. 1, pp. 69–87, 2009.

[55] Phong Q. Nguyen and Igor Shparlinski. The insecurity of the digital signature algorithm with partially known nonces. *Journal of Cryptology*, Vol. 15, No. 3, pp. 151–176, June 2002.

[56] Phong Q. Nguyen and Igor E. Shparlinski. The insecurity of the elliptic curve digital signature algorithm with partially known nonces. *Des. Codes Cryptogr.*, Vol. 30, No. 2, pp. 201–217, 2003.

[57] 岡本龍明. ECDSA 評価報告書. 外部評価報告書 CRYPTREC EX-0004-2002, CRYPTREC, 2002.

[58] D. Poddebniak, J. Somorovsky, S. Schinzel, M. Lochter, P.Rösler. Attacking deterministic signature schemes using fault attacks. In *2018 IEEE European Symposium on Security and Privacy (EuroS P)*, pp. 338–352, 2018.

[59] David Pointcheval and Jacques Stern. Security arguments for digital signatures and blind signatures. *Journal of Cryptology*, Vol. 13, No. 3, pp. 361–396, June 2000.

[60] Prasanna Ravi, Mahabir Prasad Jhanwar, James Howe, Anupam Chattopadhyay, and Shivam Bhasin. Exploiting determinism in lattice-based signatures: Practical fault attacks on pqm4 implementations of NIST candidates. In Steven D. Galbraith, Giovanni Russello, Willy Susilo, Dieter Gollmann, Engin Kirda, and Zhenkai Liang, editors, *ASIACCS 19: 14th ACM Symposium on Information, Computer and Communications Security*, pp. 427–440. ACM Press, July 2019.

[61] RFC7748: Request for Comments. `https://www.rfc-editor.org/info/rfc7748`.

[62] RFC8032: Request for Comments. `https://www.rfc-editor.org/info/rfc8032`.

[63] Y. Romailler and S. Pelissier. Practical fault attack against the ed25519 and eddsa signature schemes. In *2017 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*, pp. 17–24, 2017.

[64] Niels Samwel and Lejla Batina. Practical fault injection on deterministic signatures: The case of EdDSA. In Antoine Joux, Abderrahmane Nitaj, and Tajjeeddine Rachidi, editors, *AFRICACRYPT 18: 10th International Conference on Cryptology in Africa*, Vol. 10831

of *Lecture Notes in Computer Science*, pp. 306–321. Springer, Heidelberg, May 2018.

[65] Niels Samwel, Lejla Batina, Guido Bertoni, Joan Daemen, and Ruggero Susella. Breaking Ed25519 in WolfSSL. Cryptology ePrint Archive, Report 2017/985, 2017. `http://eprint.iacr.org/2017/985`.

[66] Claus-Peter Schnorr. Efficient identification and signatures for smart cards. In Gilles Brassard, editor, *Advances in Cryptology – CRYPTO'89*, Vol. 435 of *Lecture Notes in Computer Science*, pp. 239–252. Springer, Heidelberg, August 1990.

[67] Claus-Peter Schnorr. Efficient signature generation by smart cards. *Journal of Cryptology*, Vol. 4, No. 3, pp. 161–174, January 1991.

[68] 新保淳, 丹羽朗人, 岡田光司. ECDSA 評価報告書. 外部評価報告書 CRYPTREC EX-0003-2001, CRYPTREC, 2001.

[69] Victor Shoup. Lower bounds for discrete logarithms and related problems. In Walter Fumy, editor, *Advances in Cryptology – EUROCRYPT'97*, Vol. 1233 of *Lecture Notes in Computer Science*, pp. 256–266. Springer, Heidelberg, May 1997.

[70] Jacques Stern, David Pointcheval, John Malone-Lee, and Nigel P. Smart. Flaws in applying proof methodologies to signature schemes. In Moti Yung, editor, *Advances in Cryptology – CRYPTO 2002*, Vol. 2442 of *Lecture Notes in Computer Science*, pp. 93–110. Springer, Heidelberg, August 2002.

[71] SUPERCOP: eBACS: ECRYPT Benchmarking of Cryptographic Systems. `https://bench.cr.yp.to/supercop.html`.

[72] Akira Takahashi, Mehdi Tibouchi, and Masayuki Abe. New Bleichenbacher records: Fault attacks on qDSA signatures. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, Vol. 2018, No. 3, pp. 331–371, 2018. `https://tches.iacr.org/index.php/TCHES/article/view/7278`.

[73] Serge Vaudenay. The security of DSA and ECDSA. In Yvo Desmedt, editor, *PKC 2003: 6th International Workshop on Theory and Practice in Public Key Cryptography*, Vol. 2567 of *Lecture Notes in Computer Science*, pp. 309–323. Springer, Heidelberg, January 2003.

[74] S. . Yen and C. . Laih. Improved digital signature suitable for batch verification. *IEEE Transactions on Computers*, Vol. 44, No. 7, pp. 957–959, 1995.

CRYPTREC Review of EdDSA (Executive summary) *

Steven D. Galbraith

Mathematics Department, University of Auckland, Auckland, New Zealand. s.galbraith@auckland.ac.nz

1 Executive summary

The EdDSA signature scheme is a digital signature based on the Elliptic Curve Discrete Logarithm Problem (ECDLP). It was proposed by Bernstein, Duif, Lange, Schwabe and Yang in 2012 [18]. It builds on a long line of discrete logarithm based signature schemes, including Elgamal, Schnorr, DSA, and ECDSA. The security of signature schemes of this type is well-understood, and elliptic curve cryptography is a mature field.

My conclusions and opinions:

1. EdDSA is a good design for a signature scheme (except perhaps for the key clamping, see Section 6.1, which seems to cause more difficulties than it provides benefits).
2. EdDSA is more closely related to Schnorr signatures than ECDSA, and so enjoys many of the rigorous security guarantees that are known for Schnorr signatures, including recent work on tight security proofs.
3. Deterministic signatures solve some of the security problems of discrete log signatures, but constant time implementation is still critical in many settings.
4. EdDSA is superior to ECDSA when doing batch verification of a large number of signatures.
5. Curve 25519 provides a high level of security for the next 10-20 years, and 448-bit keys (such as in Ed448) are over-conservative and not recommended.
6. It is unlikely that quantum computers capable of solving 256-bit ECDLP instances can be built within the next 10 years.
7. I am confident that EdDSA using Curve25519 is a good signature scheme for use up to 2030.

* The original report (CRYPTREC EX-3003-2020) is available at https://www.cryptrec.go.jp/exreport/cryptrec-ex-3003-2020.pdf

References

1. ANSI, Public key cryptography for the financial services industry: The elliptic curve digital signature algorithm (ECDSA), ANS X9.62 (2005)
2. A. Antipa, D. R. L. Brown, R. P. Gallant, R. J. Lambert, R. Struik, and S. A. Vanstone, Accelerated verification of ECDSA signatures, in B. Preneel and S. E. Tavares (eds.), SAC 2005 Springer LNCS 3897 (2006) 307–318.
3. Diego F. Aranha, Felipe Rodrigues Novaes, Akira Takahashi, Mehdi Tibouchi and Yuval Yarom, LadderLeak: Breaking ECDSA With Less Than One Bit Of Nonce Leakage, IACR eprint 2020/615 (2020)
4. R. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen and F. Vercauteren, Handbook of elliptic and hyperelliptic cryptography, Chapman and Hall/CRC (2006)
5. D.V. Bailey, L. Batina, D.J. Bernstein, P. Birkner, J.W. Bos, H.C. Chen, C.M. Cheng, G. van Damme, G. de Meulenaer, L.J.D. Perez, J. Fan, T. Güneysu, F. Gurkaynak, T. Kleinjung, T. Lange, N. Mentens, R. Niederhagen, C. Paar, F. Regazzoni, P. Schwabe, L. Uhsadel, A.V. Herrewege and B.Y. Yang, Breaking ECC2K-130, IACR ePrint 2009/541 (2009)
6. Razvan Barbulescu, Pierrick Gaudry, Antoine Joux and Emmanuel Thomé, A Heuristic Quasi-Polynomial Algorithm for Discrete Logarithm in Finite Fields of Small Characteristic, in P. Q. Nguyen and E. Oswald (eds.), EUROCRYPT 2014, Springer LNCS 8441 (2014) 1–16.
7. Alessandro Barenghi and Gerardo Pelosi, A Note on Fault Attacks Against Deterministic Signature Schemes (Short Paper), IWSEC 2016, Springer (2016) 182–192.
8. M. Bellare and G. Neven, *Multi-signatures in the plain public-key model and a general forking lemma*, in A. Juels, R. N. Wright, and S. De Capitani di Vimercati (eds.) CCS 2006, ACM (2006) 390–399.
9. Mihir Bellare and Wei Dai, The Multi-Base Discrete Logarithm Problem: Concrete Security Improvements for Schnorr Identification, Signatures and Multi-Signatures, IACR ePrint 2020/416 (2020)
10. David Bernhard, Olivier Pereira and Bogdan Warinschi, How not to Prove Yourself: Pitfalls of the Fiat-Shamir Heuristic and Applications to Helios, IACR eprint 2016/771 (2016)
11. D. J. Bernstein, P. Birkner, M. Joye, T. Lange, and C. Peters, *Twisted Edwards curves*, in S. Vaudenay (ed.) Africacrypt 2008, Springer LNCS 5023, (2008) 389–405.
12. Daniel J. Bernstein, Curve25519: New Diffie-Hellman Speed Records. in M. Yung, Y. Dodis, A. Kiayias and T. Malkin (eds.), PKC 2006, Springer LNCS 3958 (2006) 207–228.
13. Daniel J. Bernstein, Multi-user Schnorr security, revisited, IACR ePrint 2015/996 (2015)
14. Daniel J. Bernstein and Tanja Lange, Faster Addition and Doubling on Elliptic Curves, in K. Kurosawa (ed.), ASIACRYPT 2007, Springer LNCS 4833 (2007) 29–50.
15. D.J. Bernstein, T. Lange and P. Schwabe, On the correct use of the negation map in the Pollard rho method. in D. Catalano, N. Fazio, R. Gennaro, A. Nicolosi (eds.) PKC 2011, Springer LNCS 6571 (2011) 128–146.
16. D.J. Bernstein and T. Lange, Two grumpy giants and a baby, in E.W. Howe and K.S. Kedlaya (eds.), Proceedings of the Tenth Algorithmic Number Theory Symposium, MSP, Vol. 1 (2013) 87–111.
17. D.J. Bernstein and T. Lange, Non-uniform cracks in the concrete: The power of free precomputation, in K. Sako, P. Sarkar (eds.) ASIACRYPT 2013, Springer LNCS 8270 (2013) 321–340.
18. Daniel J. Bernstein, Niels Duif, Tanja Lange, Peter Schwabe and Bo-Yin Yang, High-speed high-security signatures. J. Cryptogr. Eng. **2**, No. 2 (2012) 77–89.
19. Daniel J. Bernstein, Simon Josefsson, Tanja Lange, Peter Schwabe and Bo-Yin Yang, EdDSA for more curves, July 2015, IACR eprint 2015/677 (2015)
20. Daniel J. Bernstein, Why EdDSA held up better than ECDSA against Minerva, blog post (2019) `https://blog.cr.yp.to/20191024-eddsa.html`
21. I.F. Blake, G. Seroussi and N.P. Smart, Elliptic Curves in Cryptography, Cambridge (1999)
22. Daniel Bleichenbacher, Generating ElGamal signatures without knowing the secret key, EUROCRYPT'96, Springer LNCS 1070 (1996) 10–18.
23. Dan Boneh and Phillip Rogaway, Security Level of Cryptography-ECDSA, CRYPTREC EX-1006-2001 (2001) `https://www.cryptrec.go.jp/exreport/cryptrec-ex-1006-2001.pdf`
24. Dan Boneh and Victor Shoup, A Graduate Course in Applied Cryptography, version 0.5 (2020) `http://toc.cryptobook.us/`
25. Joppe W. Bos, Marcelo E. Kaihara, Thorsten Kleinjung, Arjen K. Lenstra and Peter L. Montgomery, On the Security of 1024-bit RSA and 160-bit Elliptic Curve Cryptography, IACR ePrint 2009/389 (2009)
26. Joppe W. Bos, Marcelo E. Kaihara, Thorsten Kleinjung, Arjen K. Lenstra and Peter L. Montgomery, Solving a 112-bit prime elliptic curve discrete logarithm problem on game consoles using sloppy reduction, Int. J. Appl. Cryptogr. **2**(3) (2012) 212–228.
27. Joppe W. Bos, Thorsten Kleinjung and Arjen K. Lenstra, On the use of the negation map in the Pollard Rho method. in G. Hanrot, F. Morain, E. Thomé (eds.) ANTS IX, Springer LNCS 6197 (2010) 66–82.

28. Joachim Breitner and Nadia Heninger, Biased Nonce Sense: Lattice Attacks Against Weak ECDSA Signatures in Cryptocurrencies, in I. Goldberg and T. Moore (eds.), Financial Cryptography, Springer LNCS 11598 (2019) 3–20
29. Daniel R. L. Brown, Generic Groups, Collision Resistance, and ECDSA, Designs, Codes and Cryptography, vol 35 (2005) 119–152.
30. Billy Bob Brumley and Nicola Tuveri, Remote Timing Attacks Are Still Practical, in V. Atluri and C. Díaz, ESORICS 2011, Springer LNCS 6879 (2011) 355–371.
31. J. Brendel, C. Cremers, D. Jackson and M. Zhao, The provable security of Ed25519: Theory and practice, to appear at IEEE Symposium on Security and Privacy, S&P 2020.
32. Status of quantum computer development, Version 1.2, June 2020, Federal Office for Information Security, Bonn, Germany.
33. Konstantinos Chalkias, François Garillot and Valeria Nikolaenko, Taming the Many EdDSAs, Security Standardisation Research SSR 2020, Springer LNCS 12529 (2020) 67–90.
34. Yilei Chen, Alex Lombardi, Fermi Ma and Willy Quach, Does Fiat-Shamir Require a Cryptographic Hash Function? IACR ePrint 2020/915 (2020)
35. Jung Hee Cheon and Jeong Hyun Yi, Fast Batch Verification of Multiple Signatures, in PKC 2007, Springer LNCS 4450 (2007) 442–457.
36. Henry Corrigan-Gibbs and Dmitry Kogan, The Discrete-Logarithm Problem with Preprocessing, in J. B. Nielsen and V. Rijmen (eds.) EUROCRYPT 2018, Springer LNCS 10821 (2018) 415–447.
37. H. M. Edwards, *A normal form for elliptic curves*, Bulletin of the AMS **44** (2007) 393–422.
38. Ericsson, What next in the world of post-quantum cryptography? May 2020. `https://www.ericsson.com/en/blog/2020/3/post-quantum-cryptography-symmetric-asymmetric-algorit`
39. IBM, IBM roadmap to quantum computing, Sept 2020. `https://www.ibm.com/blogs/research/2020/09/ibm-quantum-roadmap/`
40. P. Fouque, A. Joux and C. Mavromati, Multi-user collisions: Applications to discrete logarithm, Even-Mansour and PRINCE, in P. Sarkar, T. Iwata (eds.), ASIACRYPT 2014, Springer LNCS 8873 (2014) 420–438.
41. G. Frey and H.-G. Rück, A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves, Math. Comp., vol. 62 (1994) 865–874.
42. Steven D. Galbraith, John Malone-Lee and Nigel P. Smart, Public key signatures in the multi-user setting, Inf. Process. Lett., vol. 83, no. 5 (2002) 263–266.
43. Steven D. Galbraith, Mathematics of Public Key Cryptography, Cambridge, 2012.
44. Steven D. Galbraith, Ping Wang and Fangguo Zhang, Computing Elliptic Curve Discrete Logarithms with Improved Baby-step Giant-step Algorithm, Advances in Mathematics of Communications (AMC), vol. 11, no. 3 (2017) 453–469.
45. Craig Gidney and Martin Ekerå, How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits, arXiv:1905.09749 (2019)
46. Thomas Häner, Samuel Jaques, Michael Naehrig, Martin Roetteler and Mathias Soeken, Improved Quantum Circuits for Elliptic Curve Discrete Logarithms, in J. Ding and J.-P. Tillich (eds.), PQCrypto 2020, Springer LNCS 12100 (2020) 425–444.
47. D. Hankerson, A. Menezes and S. Vanstone, Guide to elliptic curve cryptography, Springer, 2004.
48. Y. Hitchcock, P. Montague, G. Carter and E. Dawson, The efficiency of solving multiple discrete logarithm problems and the implications for the security of fixed elliptic curves, Int. J. Inf. Secur., vol. 3 (2004) 86–98.
49. Nick Howgrave-Graham and Nigel P. Smart, Lattice Attacks on Digital Signature Schemes, Des. Codes Cryptogr., vol. 23, no. 3 (2001) 283–290.
50. Jan Jancar, Vladimir Sedlacek, Petr Svenda and Marek Sys, Minerva: The curse of ECDSA nonces (Systematic analysis of lattice attacks on noisy leakage of bit-length of ECDSA nonces), CHES 2020, IACR Trans. Cryptographic Hardware and Embedded Systems, vol. 4 (2020) 281–308.
51. Don Johnson, Alfred Menezes and Scott Vanstone, The Elliptic Curve Digital Signature Algorithm (ECDSA). International Journal of Information Security, vol. 1 (2001) 36–63.
52. S. Josefsson and I. Liusvaara, RFC 8032: Edwards-Curve Digital Signature Algorithm (EdDSA), Internet Research Task Force (IRTF) (2017) `https://tools.ietf.org/html/rfc8032`
53. S. Karati, A. Das, D. Roychowdhury, B. Bellur, D. Bhattacharya and A. Iyer, Batch verification of ECDSA signatures, in A. Mitrokotsa and S. Vaudenay (eds.), AFRICACRYPT 2012, Springer LNCS 7374 (2012) 1–18.
54. N. Koblitz and A. Menezes, Another look at non-uniformity, Groups Complexity Cryptology, vol. 5 (2013) 117–139.
55. F. Kuhn and R. Struik, Random walks revisited: Extensions of Pollard's rho algorithm for computing multiple discrete logarithms, in S. Vaudenay and A.M. Youssef (eds.), SAC 2001, Springer LNCS 2259 (2001) 212–229.
56. A. Langley, M. Hamburg and S. Turner, RFC: 7748: Elliptic Curves for Security, Internet Research Task Force (IRTF), January 2016. `https://tools.ietf.org/html/rfc7748`
57. Hyung Tae Lee, Jung Hee Cheon and Jin Hong, Accelerating ID-based Encryption based on Trapdoor DL using Precomputation, ePrint 2011/187 (2011)
58. Arjen K. Lenstra and Eric R. Verheul, Selecting Cryptographic Key Sizes, Journal of Cryptology, vol. 14, no. 4 (2001) 255–293.

59. M. Lochter and J. Merkle, Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, IETF RFC5639, March 2010. https://tools.ietf.org/html/rfc5639
60. A. Menezes, T. Okamoto and S. Vanstone, Reducing elliptic curve logarithms to logarithms in a finite field, IEEE Transactions on Information Theory, vol. 39 (1993) 1639–1646.
61. Joseph P. Mihalcik, An analysis of algorithms for solving discrete logarithms in fixed groups, Master thesis, Naval Postgraduate School, March 2010.
62. Daniel Moghimi, Berk Sunar, Thomas Eisenbarth and Nadia Heninger, TPM-FAIL: TPM meets Timing and Lattice Attacks, in S. Capkun and F. Roesner (eds.), USENIX Security (2020) 2057–2073.
63. Michele Mosca and Marco Piani, Quantum Threat Timeline, Global Risk Institute, October 2019. https://globalriskinstitute.org/publications/quantum-threat-timeline/
64. US National Academies of Sciences, Engineering, and Medicine, New Cryptography Must Be Developed and Deployed Now, Even Though A Quantum Computer That Could Compromise Today's Cryptography Is Likely At Least A Decade Away. December 4, 2018.
65. Phong Nguyen and Igor Shparlinski, The Insecurity of the Digital Signature Algorithm with Partially Known Nonces, Journal of Cryptology, vol. 15 (2002) 151–176.
66. Damian Poddebniak, Juraj Somorovsky, Sebastian Schinzel, Manfred Lochter and Paul Rösler, Attacking Deterministic Signature Schemes using Fault Attacks, 2018 IEEE European Symposium on Security and Privacy (EuroS&P), London (2018) 338–352.
67. David Pointcheval and Jacques Stern, Security Arguments for Digital Signatures and Blind Signatures, J. Cryptol., vol. 13, no. 3 (2000) 361–396.
68. J.M. Pollard, Kangaroos, Monopoly and discrete logarithms, J. Cryptology, vol. 13, no. 4 (2000) 437–447.
69. Jean-Luc Pons and Aleksander Zieniewicz, Pollard's kangaroo for SECPK1, 2020. https://github.com/JeanLucPons/Kangaroo
70. Martin Roetteler, Michael Naehrig, Krysta M. Svore and Kristin E. Lauter, Quantum Resource Estimates for Computing Elliptic Curve Discrete Logarithms, in T. Takagi and T. Peyrin (eds.), ASIACRYPT 2017, Springer LNCS 10625 (2017) 241–270.
71. H.-G. Rück, On the discrete logarithm in the divisor class group of curves, Math. Comp., vol. 68 (1999) 805–806.
72. T. Satoh and K. Araki, Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves, Commentarii Mathematici Universitatis Sancti Pauli, vol. 47 (1998) 81–92.
73. J. Schmidt and M. Medwed, A Fault Attack on ECDSA, 2009 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC) (2009) 93–99.
74. I. Semaev, Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p, Math. Comp., vol. 67 (1998) 353–356.
75. N.P. Smart, The discrete logarithm problem on elliptic curves of trace one, Journal of Cryptology, vol. 12 (1999) 193–196.
76. Jacques Stern, Evaluation Report on the ECDSA signature scheme, CRYPTREC EX-1004-2001 (2001) https://www.cryptrec.go.jp/exreport/cryptrec-ex-1004-2001.pdf
77. Thales, Cryptography for a post-quantum era, November 2018.
78. Henry de Valence, It's 255:19AM. Do you know what your validation criteria are?, (2020) https://hdevalence.ca/blog/2020-10-04-its-25519am
79. Serge Vaudenay, Hidden Collisions on DSS, CRYPTO 1996, Springer LNCS 1109 (1996) 83–88.
80. P. van Oorschot and M.J. Wiener, Parallel collision search with cryptanalytic applications, J. Cryptology, vol. 12, no. 1 (1999) 1–28.
81. L.C. Washington, Elliptic Curves: Number Theory and Cryptography, 2nd ed., CRC Press, 2008.
82. Michael J. Wiener, The Full Cost of Cryptanalytic Attacks, J. Cryptology, **17** No. 2, 105–124.

付録６

ハイブリッドモードの技術動向調査

（エグゼクティブサマリー）*

株式会社レピダム
2020 年 12 月

＊ 原文は，CRYPTREC EX-3004-2020
https://www.cryptrec.go.jp/exreport/cryptrec-ex-3004-2020.pdf
から入手可能.

本評価結果の概要（エグゼクティブサマリー）

2017 年から量子安全もしくは量子耐性のある暗号アルゴリズム（Post Quantum Cryptography, 以下、PQC）の標準化/選定が NIST などの組織において実施されている。この標準化/選定の終了後に実際のサービスや製品などへの適用には多くの時間がかかってしまうことが想定される。実際にすでに標準化されている暗号技術は、選定後サービスや製品への適用までに 10 年弱 *の年月を要している。従来の現代暗号から PQC への移行やシステムマイグレーションをした上で、新しい技術が浸透するまでには長期間必要であり、このタイムラグを緩和するための利用方法として「ハイブリッドモード」という概念が注目されている。このハイブリッドモードとは、従来の暗号技術と PQC を組み合わせることで、新しい技術である PQC が普及するまでの時間を確保できる効果や、従来の暗号技術の利用を規定している標準化仕様/ガイドラインにおいても、PQC を利用できるメリットがあると考えられる。しかしながら、ハイブリッドモードの目的や導入する背景、また、安全性に関する学術的なアプローチによる研究に関する情報が整理されていない。本調査では、ハイブリッドモードを導入する目的や背景を把握するために、ハイブリッドモードに関係することが期待される標準化団体やその組織の動向調査を実施した。また、現時点でハイブリッドモードを構成する際に想定されている PQC アルゴリズム及び、標準化動向や OSS などの実装状況に関する調査を実施した。

- ハイブリッドモードの標準化動向
  - IETF の tls WG において、TLS 1.3 でハイブリッドモードを利用可能にするための Internet Draft である「Hybrid key exchange in TLS 1.3」が、Working Group の検討項目として採択され、重要なテーマとしてコンセンサスが得られている。
  - Open Quantum-Safe プロジェクトにおいて、NIST の標準化会議で候補として残っているほぼ全ての PQC アルゴリズムが実装されており、TLS や SSH などのプロトコルで動作させる環境が準備されている。
- ハイブリッドモードで利用可能となるアルゴリズム候補
  - NIST が主催している標準化会議で候補として残っている PQC アルゴリズムは実装されており、それらのアルゴリズムが OpenSSL などに実装され、実際の世の中で利用されている TLS プロトコルや SSH プロトコルでの実現可能性が確認されている。いくつかの PQC アルゴリズムにおいてはデータサイズに関する問題が発生している。
  - ハイブリッドモードは、鍵交換とデジタル署名での利用が想定されており、ハイブリッド鍵交換については学術的な研究成果も発表されている。
- 各標準化団体・組織でのハイブリッドモードの取り扱い
  - ハイブリッドモードの導入に関する背景や目的について、明確に言及/定義している標準化団体・組織はなかったが、この調査を通して明らかになったことは以下のとおりである。
    - ✧ 従来の暗号技術と比較すると、PQC アルゴリズムへの安全性評価の実績や歴史が浅いため、PQC アルゴリズムにおける脆弱性の発見は社会へのインパクトを軽減する。そのため、ハイブリッドモードで利用している暗号アルゴリズム（従来の暗号技術または PQC アルゴリズム）のいずれかが安全であれば、セキュリティが最低限担保されることが期待できること。

---

* 認証付き暗号である Galois/Counter Mode （GCM） を暗号スイートとして利用するために規定された TLS 1.2 （2008 年 8 月に RFC として発行）が、実際に運用されているサーバやブラウザの 80%程度で TLS 1.2 が利用できるようになったのが 2016 年 9 月頃であるため、8 年の年月がかかっている。

- ✧ 標準化やソフトウェア/ハードウェアへの実装するためのバッファ期間としてのアルゴリズムの移行やシステムマイグレーションとしての役割が期待できること

・ ハイブリッドモードに関する安全性及び評価
  - ➢ 本調査の範囲において、ハイブリッドモードの構成法による安全性への実影響が報告された情報は発見されなかった。
  - ➢ ハイブリッドモードによって実現される安全性レベルは、従来の暗号アルゴリズムと PQC アルゴリズムで強い方の安全性は少なくとも達成できると考えられる。現在のところ、それ以上の安全性を達成しうるのかどうかは明らかになっていないと考えられる。

参考文献

[1] E. Crockett, C. Paquin , D. Stebi, “Prototyping post-quantum and hybrid key exchange and authentication in TLS and SSH,” 19 7 2019. . Available: https://csrc.nist.gov/CSRC/media/Events/Second-PQC-Standardization-Conference/documents/accepted-papers/stebila-prototyping-post-quantum.pdf.

[2] Cloud Security Alliance Quantum-Safe Security Working group, “The State of Post-Quantum Cryptography,” 23 5 2018. . Available: https://cloudsecurityalliance.org/artifacts/the-state-of-post-quantum-cryptography/.

[3] Cloud Security Alliance Quantum-Safe Security Working group, “Applied Quantum-Safe Security,” . Available: https://downloads.cloudsecurityalliance.org/assets/research/quantum-safe-security/applied-quantum-safe-security.pdf.

[4] PQCRYPTO Project, “PQCRYPTO Post-Quantum Cryptography for Long-Term Security D5.2 Standardization: Final report,” 4 2018. . Available: https://pqcrypto.eu.org/deliverables/d5.2-final.pdf.

[5] S. Douglas, “Hybrid key exchange in TLS 1.3,” . Available: https://tools.ietf.org/html/draft-ietf-tls-hybrid-design-00.

[6] A. Hopkins, “Post-quantum TLS now supported in AWS KMS,” 4 11 2019. . Available: https://aws.amazon.com/jp/blogs/security/post-quantum-tls-now-supported-in-aws-kms/.

[7] Microsoft Research, “Post-Quantum TLS,” . Available: https://www.microsoft.com/en-us/research/project/post-quantum-tls/.

[8] K. Kwiatkowski , L. Valenta, “The TLS Post-Quantum Experiment,” 30 10 2019. . Available: https://blog.cloudflare.com/the-tls-post-quantum-experiment/.

[9] B. W. Joppe, C. Costello, M. Naehrig , D. Stebila, “Post-quantum key exchange for the TLS protocol from the ring learning with errors problem,” ePrint, 2018. Available: https://eprint.iacr.org/2014/599.pdf

[10] J. Brendel, M. Fischlin , F. Günther, “Breakdown Resilience of Key Exchange Protocols: NewHope, TLS 1.3, and Hybrids,” ESORICS 2019, 2019.

[11] F. Giacon, F. Heuer , B. Poettering, “KEM Combiners,” PKC 2018, 2018.

[12] N. Bindel, J. Brendel, M. Fischlin, B. Goncalves , D. Stebila, “Hybrid Key Encapsulation Mechanisms and Authenticated Key Exchange,” PQCrypto 2019, 2019.

Shor のアルゴリズム実装動向調査（エグゼクティブサマリー）*

高安敦
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

2021 年 9 月 21 日

*原文は，CRYPTREC EX-3005-2020
https://www.cryptrec.go.jp/exreport/cryptrec-ex-3005-2020.pdf から入手可能.

第1章　エグゼクティブサマリー

Shor のアルゴリズムの実装・リソース評価の把握の重要性について．第 2 章で Shor のアルゴリズム [Sho94, Sho97] の実装・リソース評価の把握の重要性をまとめている．Shor のアルゴリズムは，多項式時間で素因数分解問題や離散対数問題を解けるために理論的には大きな脅威だが，実験的に暗号で用いるような大きなパラメータに対してこれらの問題を解いたという報告はこれまで行われていない．そのため，現状どの程度のパラメータまで実験的に適用可能なのか，実際に暗号で用いるような大きなパラメータの問題を解くにはどの程度の性能の量子コンピュータが必要なのかを把握しておくことは重要である．

Shor の量子アルゴリズムの解説．第 4 章において，Shor の量子アルゴリズムの解説を行う．それに先駆けて，第 3 章で量子計算について説明する．ここでは，Shor のアルゴリズムを理解できるよう，古典ビットとは異なる量子ビットの概念，計算基底による測定，基本的な量子ゲートの紹介を行う．Shor の量子アルゴリズムを解説する第 4 章ではまず，合成数 $N = pq$ を素因数分解するためには，$\gcd(a, N) = 1$ を満たす整数 a に対して $a^r = 1 \mod N$ を満たす最小の正整数 r である位数を計算することで素因数分解を行えること示す．また，上記の位数計算と類似の性質として，ある関数の周期を計算できれば離散対数問題を解けることを示す．次に，Shor のアルゴリズムの核となる量子フーリエ変換について説明する．最後に，冪乗剰余演算と量子フーリエ変換を用いることで，位数計算や周期計算を多項式時間で行う量子アルゴリズムが作れることを示す．これによって，素因数分解問題や素体・楕円曲線上の離散対数問題を多項式時間で解くことができる．

Shor の量子アルゴリズムについて報告されている実装結果の調査．第 5 章で，これまで確認されている Shor のアルゴリズムによる $N = 15$ または $N = 21$ の素因数分解 [ASK19, DLQ$^+$20, LBC$^+$12, LBYP07, MLLL$^+$12, LWL$^+$07, MNM$^+$16, PMO09, SSV13, VSB$^+$01] と $2^x = 1 \mod 3$ の素体上の離散対数問題 [AST$^+$20] の実装結果を紹介する．基本的にほとんどの実験は $N = 15$ の素因数分解であるため，この章の内容を平易に理解できるように，まず第 4 章の復習として $N = 15$ を素因数分解するための量子アルゴリズムを詳細にまとめる．特に，$\gcd(a, 15) = 1$ を満たす $a \in \{2, 4, 7, 8, 11, 13, 14\}$ の位数は $r = 2$ または $r = 4$ のいずれかであり，[VSB$^+$01] で考察されているように，実装の困難さは位数の値によって大きく異なる．そのため，位数が $r = 2$ または $r = 4$ の場合に分けて $N = 15$ を

素因数分解するための量子アルゴリズムを整理し，そのための量子回路を図 5.1–5.3 にまとめる．ただし，既存の Shor のアルゴリズムの実装実験においてはここで説明する一般的な量子回路が用いられることは稀で，ほとんど全ての論文で $N = 15$ や a または r の値に応じて効率化した量子回路を用いている．そのため，多くの論文で共通に用いられている効率化手法をまとめた後に，各実験で用いられている量子回路をまとめる．表 5.1 で各実験で用いた量子回路の量子ビット数や量子ゲートの数をまとめ，図 5.9–5.29 でそれらの量子回路を示す．ここで確認するように，ほとんどの結果は求めたい位数である $r = 2, 4$ の情報を用いて量子回路を設計するなど，一般的な合成数 $N = pq$ を素因数分解するときには適用できない効率化を行っている．さらに，[DLQ$^+$20] は図 5.25 の量子回路を用いることで $N = 21$ の素因数分解には成功したが，図 5.28 の量子回路を用いて行った $N = 35$ の素因数分解には成功しなかったと報告している．これらの調査を踏まえ，2048 ビット合成数 $N = pq$ の素因数分解など暗号で用いられるような大きなパラメータの問題を解くには，量子コンピュータの物理的な飛躍が必要であり，実用的には現在用いられている公開鍵暗号方式の安全性が直ちに損なわれるわけではないと考えられる．

暗号で用いるようなパラメータに対して Shor の量子アルゴリズムを実行する際のリソース評価．第 6 章に量子アルゴリズムによって素因数分解問題や離散対数問題を解くためのリソース評価の既存研究をまとめた．表 6.4 において，現在知られている素因数分解と ECDLP 計算のための量子アルゴリズムの漸近的なリソース評価，表 6.5, 6.6 において暗号で用いられるパラメータに対するリソース評価をまとめている．これまでの研究で量子アルゴリズム実装が大幅に進歩しており，最新の Gidney と Ekerå による素因数分解 [GE19] や Häner ら [HJN$^+$20] と Banegas ら [BBvHL20] による ECDLP 計算は従来の結果を大幅に効率化している．そのため，今後もこの分野の発展によって素因数分解や離散対数問題計算のための量子アルゴリズムがより効率化する可能性があるため，注意が必要である．これらには劣るが，Gheorghiu と Mosca [GM19] はゲートエラー率が 10^{-3} と 10^{-5} の場合に素因数分解と ECDLP 計算に必要な量子ビット数と計算時間のトレードオフを解析しており，その結果を図 6.2–6.12 にまとめている．また，前述の最も効率的な素因数分解アルゴリズムである Gidney と Ekerå [GE19] が用いた効率化技法をまとめ，この技法による素因数分解と素体上の離散対数計算のためのリソース評価を表 6.9–6.14 にまとめている．

関連図書

[ASK19] Mirko Amico, Zain H. Saleem, and Muir Kumph. Experimental study of Shor's factoring algorithm using the IBM Q experience. *Phys. Rev. A*, 100:012305, 2019.

[AST+20] 青野良範，Sitong Liu, 田中智樹，宇野隼平，Rodney Van Meter, 篠原直行，野島良．超伝導量子回路を用いた離散対数問題の求解実験．量子情報技術研究会 (2020-12-QIT), 2020.

[BBC+95] Adriano Barenco, Charles H. Bennett, Richard Cleve, David P. DiVincenzo, Norman Margolus, Peter Shor, Tycho Sleator, John A. Smolin, and Harald Weinfurter. Elementary gates for quantum computation. *Phys. Rev. A*, 52:3457–3467, 1995.

[BBvHL20] Gustavo Banegas, Daniel J. Bernstein, Iggy van Hoof, and Tanja Lange. Concrete quantum cryptanalysis of binary elliptic curves. *IACR Cryptol. ePrint Arch.*, 2020:1296, 2020.

[BCDP96] David Beckman, Amalavoyal N. Chari, Srikrishna Devabhaktuni, and John Preskill. Efficient networks for quantum factoring. *Phys. Rev. A*, 54:1034–1063, 1996.

[BCMS19] Colin D. Bruzewicz, John Chiaverini, Robert McConnell, and Jeremy M. Sage. Trapped-ion quantum computing: Progress and challenges. *Applied Physics Reviews*, 6(2):021314, 2019.

[Bea03] S. Beauregard. Circuit for Shor's algorithm using $2n + 3$ qubits. *Quantum Inf. Comput.*, 3:175–185, 2003.

[BEL+16] Daniel J. Bernstein, Susanne Engels, Tanja Lange, Ruben Niederhagen, Christof Paar, Peter Schwabe, and Ralf Zimmermann. Faster discrete logarithms on fpgas. *IACR Cryptol. ePrint Arch.*, 2016:382, 2016.

[BGB+18] Ryan Babbush, Craig Gidney, Dominic W. Berry, Nathan Wiebe, Jarrod McClean, Alexandru Paler, Austin Fowler, and Hartmut Neven. Encoding electronic spectra in quantum circuits with linear t complexity. *Phys. Rev. X*, 8:041015, 2018.

[BGG+20] Fabrice Boudot, Pierrick Gaudry, Aurore Guillevic, Nadia Heninger, Emmanuel Thomé, and Paul Zimmermann. Comparing the difficulty of factorization and discrete logarithm: A 240-digit experiment. In Daniele Micciancio and Thomas Ristenpart, editors, *Advances in Cryptology - CRYPTO 2020 - 40th Annual International Cryptology Conference, CRYPTO 2020, Proceedings, Part II*, volume 12171 of *Lecture Notes in Computer Science*, pages 62–91. Springer, 2020.

[BGM+19] Dominic W. Berry, Craig Gidney, Mario Motta, Jarrod R. McClean, and Ryan Babbush. Qubitization of arbitrary basis quantum chemistry leveraging sparsity and low rank factorization. *Quantum*, 3:208, 2019.

[BHL+16] C. J. Ballance, T. P. Harty, N. M. Linke, M. A. Sepiol, and D. M. Lucas. High-fidelity quantum logic gates using trapped-ion hyperfine qubits. *Phys. Rev. Lett.*, 117:060504, 2016.

[BKM+14] R. Barends, J. Kelly, A. Megrant, A. Veitia, D. Sank, E. Jeffrey, T. C. White, J. Mutus, A. G. Fowler, B. Campbell, Y. Chen, Z. Chen, B. Chiaro, A. Dunsworth, C. Neill, P. O'Malley, P. Roushan, A. Vainsencher, J. Wenner, A. N. Korotkov, A. N. Cleland, and John M. Martinis. Superconducting quantum circuits at the surface code threshold for fault tolerance. *Nature*, 508:500–503, 2014.

[BKRB08] Jan Benhelm, Gerhard Kirchmair, Christian F. Roos, and Rainer Blatt. Towards fault-tolerant quantum computing with trapped ions. *Nature Physics*, 4:463–466, 2008.

[BSH+15] C. J. Ballance, V. M. Schäfer, J. P. Home, D. J. Szwer, S. C. Webster, D. T. C. Allcock, N. M. Linke, T. P. Harty, D. P. L. Aude Craik, D. N. Stacey, A. M. Steane, and D. M. Lucas. Hybrid quantum logic and a test of Bell's inequality using two different atomic isotopes. *Nature*, 528:384–386, 2015.

[BXN+17] A. Bermudez, X. Xu, R. Nigmatullin, J. O'Gorman, V. Negnevitsky, P. Schindler, T. Monz, U. G. Poschinger, C. Hempel, J. Home, F. Schmidt-Kaler, M. Biercuk, R. Blatt, S. Benjamin, and M. Müller. Assessing the progress of trapped-ion processors towards fault-tolerant quantum computation. *Phys. Rev. X*, 7:041061, 2017.

[CBW+18] Kevin S. Chou, Jacob Z. Blumoff, Christopher S. Wang, Philip C. Reinhold, Christopher J. Axline, Yvonne Y. Gao, L. Frunzio, M. H. Devoret, Liang Jiang, and R. J. Schoelkopf.

Deterministic teleportation of a quantum gate between two logical qubits. *Nature*, 561:368–373, 2018.

[CCG+11] Jerry M. Chow, A. D. Córcoles, Jay M. Gambetta, Chad Rigetti, B. R. Johnson, John A. Smolin, J. R. Rozen, George A. Keefe, Mary B. Rothwell, Mark B. Ketchen, and M. Steffen. Simple all-microwave entangling gate for fixed-frequency superconducting qubits. *Phys. Rev. Lett.*, 107:080502, 2011.

[CDKM04] S. A. Cuccaro. T. G. Draper, S. A. Kutin, and D. P. Moulton. A new quantum ripple-carry addition circuit. arXiv preprint quantum-ph/0601097, 2004.

[CGC+13] Jerry M Chow, Jay M Gambetta, Andrew W Cross, Seth T Merkel, Chad Rigetti, and M Steffen. Microwave-activated conditional-phase gate for superconducting qubits. *New Journal of Physics*, 15(11):115012, 2013.

[CMQ+10] W. C. Campbell, J. Mizrahi, Q. Quraishi, C. Senko, D. Hayes, D. Hucul, D. N. Matsukevich, P. Maunz, and C. Monroe. Ultrafast gates for single atomic qubits. *Phys. Rev. Lett.*, 105:090502, 2010.

[CNR+14] Yu Chen, C. Neill, P. Roushan, N. Leung, M. Fang, R. Barends, J. Kelly, B. Campbell, Z. Chen, B. Chiaro, A. Dunsworth, E. Jeffrey, A. Megrant, J. Y. Mutus, P. J. J. O'Malley, C. M. Quintana, D. Sank, A. Vainsencher, J. Wenner, T. C. White, Michael R. Geller, A. N. Cleland, and John M. Martinis. Qubit architecture with high coherence and fast tunable coupling. *Phys. Rev. Lett.*, 113:220502, 2014.

[DH76] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Trans. Information Theory*, 22(6):644–654, 1976.

[DKRS06] Thomas G. Draper, Samuel A. Kutin, Eric M. Rains, and Krysta M. Svore. A logarithmic-depth quantum carry-lookahead adder. *Quantum Information and Computation*, 6(4):351–369, 2006.

[DLQ+20] Zhao-Chen Duan, Jin-Peng Li, Jian Qin, Ying Yu, Yong-Heng Huo, Sven Höfling, Chao-Yang Lu, Nai-Le Liu, Kai Chen, and Jian-Wei Pan. Proof-of-principle demonstration of compiled Shor's algorithm using a quantum dot single-photon source. *Optics Express*, 28:18917–18930, 2020.

[DSBP18] Avinash Dash, Deepankar Sarmah, B. Behera, and P. Panigrahi. Exact search algorithm to factorize large biprimes and a triprime on IBM quantum computer. *arXiv: Quantum Physics*, 2018.

[EH17] Martin Ekerå and Johan Håstad. Quantum algorithms for computing Short discrete logarithms and factoring RSA integers. In Tanja Lange and Tsuyoshi Takagi, editors, *Post-Quantum Cryptography - 8th International Workshop, PQCrypto 2017, Proceedings*, volume 10346 of *Lecture Notes in Computer Science*, pages 347–363. Springer, 2017.

[Eke16] Martin Ekerå. Modifying Shor's algorithm to compute Short discrete logarithms. *IACR Cryptol. ePrint Arch.*, 2016:1128, 2016.

[Eke18] Martin Ekerå. Quantum algorithms for computing general discrete logarithms and orders with tradeoffs. *IACR Cryptol. ePrint Arch.*, 2018:797, 2018.

[Eke19] Martin Ekerå. Revisiting Shor's quantum algorithm for computing general discrete logarithms. *CoRR*, abs/1905.09084, 2019.

[Eke20] Martin Ekerå. On post-processing in the quantum algorithm for computing Short discrete logarithms. *Des. Codes Cryptogr.*, 88(11):2313–2335, 2020.

[EWP+19] Alexander Erhard, Joel James Wallman, Lukas Postler, Michael Meth, Roman Stricker, Esteban Adrian Martinez, Philipp Schindler, Thomas Monz, Joseph Emerson, and Rainer Blatt. Characterizing large-scale quantum computers via cycle benchmarking. arXiv:1902.08543, 2019.

[FG19] Austin G. Fowler and Craig Gidney. Low overhead quantum computation using lattice surgery, 2019.

[FMMC12] Austin G. Fowler, Matteo Mariantoni, John M. Martinis, and Andrew N. Cleland. Surface codes: Towards practical large-scale quantum computation. *Phys. Rev. A*, 86:032324, 2012.

[Gid17] C. Gidney. Factoring with $n + 2$ clean qubits and $n - 1$ dirty qubits. arXiv preprint quantum-ph/1706.07884, 2017.

[Gid18] Craig Gidney. Halving the cost of quantum addition. *Quantum*, 2:74, 2018.

[Gid19a] C. Gidney. Windowed quantum arithmetic. arXiv preprint arXiv:1905.07682, 2019.

[Gid19b] Craig Gidney. Approximate encoded permutations and piecewise quantum adders, 2019.

[GE19] C. Gidney and M. Ekerå. How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. arXiv preprint arXiv:1905.09749, 2019.

[GM19] Vlad Gheorghiu and Michele Mosca. Benchmarking the quantum cryptanalysis of symmetric, public-key and hash-based cryptographic schemes, 2019.

[GN93] Robert B. Griffiths and Chi-Sheng Niu. Semiclassical Fourier transform for quantum computation. *Phys. Rev. Lett.*, 76(17):3228, 1993.

[Gor93] Daniel M. Gordon. Discrete logarithms in *GF(P)* using the number field sieve. *SIAM J. Discrete Math.*, 6(1):124–138, 1993.

[Gro96] Lov K. Grover. A fast quantum mechanical algorithm for database search. In Gary L. Miller, editor, *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing*, pages 212–219. ACM, 1996.

[GTL+16] J. P. Gaebler, T. R. Tan, Y. Lin, Y. Wan, R. Bowler, A. C. Keith, S. Glancy, K. Coakley, E. Knill, D. Leibfried, and D. J. Wineland. High-fidelity universal gate set for $^{9}Be^{+}$ ion qubits. *Phys. Rev. Lett.*, 117:060505, 2016.

[HAB+14] T. P. Harty, D. T. C. Allcock, C. J. Ballance, L. Guidoni, H. A. Janacek, N. M. Linke, D. N. Stacey, and D. M. Lucas. High-fidelity preparation, gates, memory, and readout of a trapped-ion quantum bit. *Phys. Rev. Lett.*, 113:220501, 2014.

[HFDM12] Clare Horsman, Austin G Fowler, Simon Devitt, and Rodney Van Meter. Surface code quantum computing by lattice surgery. *New Journal of Physics*, 14(12):123011, 2012.

[HJN+20] Thomas Häner, Samuel Jaques, Michael Naehrig, Martin Roetteler, and Mathias Soeken. Improved quantum circuits for elliptic curve discrete logarithms. In Jintai Ding and Jean-Pierre Tillich, editors, *Post-Quantum Cryptography - 11th International Conference, PQCrypto 2020, Paris, France, April 15-17, 2020, Proceedings*, volume 12100 of *Lecture Notes in Computer Science*, pages 425–444. Springer, 2020.

[HPS+19] Sabrina S. Hong, Alexander T. Papageorge, Prasahnt Sivarajah, Genya Crossman, Nicolas Didier, Anthony M. Polloreno, Eyob A. Sete, Stefan W. Turkowski, Marcus P. da Silva, Blake R. Johnson. Demonstration of a parametrically-activated entangling gate protected from flux noise. arXiv:1901.08035, preprint quantum-ph/0601097, 2004.

[HRS17] Thomas Haener, Martin Roetteler, and Krysta M. Svore. Factoring using $2n + 2$ qubits with toffoli based modular multiplication. *Quantum Information and Computation*, 18(7-8):673–684, 2017.

[HSA+16] T. P. Harty, M. A. Sepiol, D. T. C. Allcock, C. J. Ballance, J. E. Tarlton, and D. M. Lucas. High-fidelity trapped-ion quantum logic using near-field microwaves. *Phys. Rev. Lett.*, 117:140501, 2016.

[IOK+12] 石坂智，小川朋宏，河内亮周，木村元，林正人．量子情報科学入門．共立出版，2012.

[JBM+18] Shuxian Jiang, Keith A. Britt, Alexander J. McCaskey, Travis S. Humble, and Sabre Kais. Quantum annealing for prime factorization. *Scientific Reports*, 8(17667), 2018.

[KGA+11] A. Keselman, Y. Glickman, N. Akerman, S. Kotler, and R. Ozeri. High-fidelity state detection and tomography of a single-ion Zeeman qubit. *New Journal of Physics*, 13(7):073027, 2011.

[KSB+20] Morten Kjaergaard, Mollie E. Schwartz, Jochen Braumüller, Philip Krantz, Joel I.-J. Wang, Simon Gustavsson, and William D. Oliver. Superconducting qubits: Current state of play. *Annual Review of Condensed Matter Physics*, 11(1):369–395, 2020.

[KSG+20] Morten Kjaergaard, Mollie E. Schwartz, Ami Greene, Gabriel O. Samach, Andreas Bengtsson, Michael O'Keeffe, Christopher M. McNally, Jochen Braumüller, David K. Kim, Philip Krantz, Milad Marvian, Alexander Melville, Bethany M. Niedzielski, Youngkyu Sung, Roni Winik, Jonilyn Yoder, Danna Rosenberg, Kevin Obenland, Seth Lloyd, Terry P. Orlando, Iman Marvian, Simon Gustavsson, William D. Oliver. Programming a quantum computer with quantum instructions. *arXiv: Quantum Physics*, arXiv:2001.08838, 2020.

[Kun05] Noboru Kunihiro. Exact analyses of computational time for factoring in quantum computers. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, 88-A(1):105–111, 2005.

[LBC+12] E. Lucero, R. Barends, Y. Chen, J. Kelly, M. Mariantoni, A. Megrant, P. O'Malley, D. Sank, A. Vainsencher, J. Wenner, T. White, Y. Yin, A. N. Cleland, and J. M. Martinis. Computing prime factors with a Josephson phase qubit quantum processor. *Nature Physics*, 8:719–723, 2012.

[LBYP07] Chao-Yang Lu, Daniel E. Browne, Tao Yang, and Jian-Wei Pan. Demonstration of a compiled version of Shor's quantum factoring algorithm using photonic qubits. *Phys. Rev. Lett.*, 99, 2007.

[Lit19] Daniel Litinski. A game of surface codes: Large-scale quantum computing with lattice surgery. *Quantum*, 3:128, 2019.

[LJMP90] Arjen K. Lenstra, Hendrik W. Lenstra Jr., Mark S. Manasse, and John M. Pollard. The number field sieve. In *Proceedings of the 22nd Annual ACM Symposium on Theory of Computing*, pages 564–572, 1990.

[LWL+07] B. P. Lanyon, T. J. Weinhold, N. K. Langford, M. Barbieri, D. F. V. James, A. Cilchrist, and A. G. White. Experimental demonstration of a compiled version of Shor's algorithm with quantum entanglement. *Phys. Rev. Lett.*, 99, 2007.

[MFM+16] David C. McKay, Stefan Filipp, Antonio Mezzacapo, Easwar Magesan, Jerry M. Chow, and Jay M. Gambetta. Universal gate for fixed-frequency qubits via a tunable bus. *Phys. Rev. Applied*, 6:064007, 2016.

[MLLL+12] E. Martin-Lopez, A. Laing, T. Lawson, R. Alvarez, X.-Q. Zhou, and J. L. O'Brien. Experimental realisation of Shor's quantum factoring algorithm using qubit recycling. *Nature Photon*, 6:773–776, 2012.

[MNM+16] T. Monz, D. Nigg, E. A. Martinez, M. F. Brandl, P. Schindler, R. Rines, S. X. Wang, I. L. Chuang, and R. Blatt. Realization of a scalable Shor algorithm. *Science*, 351:1068–1070, 2016.

[NC11] Michael A. Nielsenand and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, USA, 10th edition, 2011.

[NIST13] NIST. FIPS: 186-4: Digital Signature Standard (DSS). 2013.

[OC17] Joe O'Gorman and Earl T. Campbell. Quantum computation with realistic magic-state factories. *Phys. Rev. A*, 95:032338, 2017.

[OWC+11] C. Ospelkaus, U. Warring, Y. Colombe, K. R. Brown, J. M. Amini, D. Leibfried, and D. J. Wineland. Microwave quantum logic gates for trapped ions. *Nature*, 476:181–184, 2011.

[PGM+12] S. Poletto, Jay M. Gambetta, Seth T. Merkel, John A. Smolin, Jerry M. Chow, A. D. Córcoles, George A. Keefe, Mary B. Rothwell, J. R. Rozen, D. W. Abraham, Chad Rigetti, and M. Steffen. Entanglement of two superconducting qubits in a waveguide cavity via monochromatic two-photon excitation. *Phys. Rev. Lett.*, 109:240505, 2012.

[PMO09] A. Politi, J. C. F. Matthews, and J. L. O'Brien. Shor's quantum factoring algorithm on a photonic chip. *Science*, 325:1221, 2009.

[PMS+16] Hanhee Paik, A. Mezzacapo, Martin Sandberg, D. T. McClure, B. Abdo, A. D. Córcoles, O. Dial, D. F. Bogorin, B. L. T. Plourde, M. Steffen, A. W. Cross, J. M. Gambetta, and Jerry M. Chow. Experimental demonstration of a resonator-induced phase gate in a multiqubit circuit QED system. *Phys. Rev. Lett.*, 117:250502, 2016.

[RGR+18] S. Rosenblum, Y. Y. Gao, P. Reinhold, C. Wang, C. J. Axline, L. Frunzio, S. M. Girvin, Liang Jiang, M. Mirrahimi, M. H. Devoret, and R. J. Schoelkopf. A CNOT gate between multiphoton qubits encoded in two cavities. *Nature Communications*, 9, 652, 2018.

[RNSL17] Martin Roetteler, Michael Naehrig, Krysta M. Svore, and Kristin E. Lauter. Quantum resource estimates for computing elliptic curve discrete logarithms. 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, Proceedings, Part II*, volume 10625 of *Lecture Notes in Computer Science*, pages 241–270. Springer, 2017.

[RSA78] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2):120–126, 1978.

[SBT+18] V. M. Schäfer, C. J. Ballance, K. Thirumalai, L. J. Stephenson, T. G. Ballance, A. M. Steane, D. M. Lucas. Fast quantum logic gates with trapped-ion qubits. *Nature*, 555(7694):75-78, 2018.

[Sho94] Peter W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *35th Annual Symposium on Foundations of Computer Science*, pages 124–134. IEEE Computer Society, 1994.

[Sho97] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997.

[SMCG16] Sarah Sheldon, Easwar Magesan, Jerry M. Chow, and Jay M. Gambetta. Procedure for systematically tuning up cross-talk in the cross-resonance gate. *Phys. Rev. A*, 93:060302, 2016.

[SSV13] John A. Smolin, Graeme Smith, and Alexander Vargo. Oversimplifying quantum factoring. *Nature*, 499:163–165, 2013.

[TGL+15] T. R. Tan, J. P. Gaebler, Y. Lin, Y. Wan, R. Bowler, D. Leibfried, and D. J. Wineland. Multi-element logic gates for trapped-ion qubits. *Nature*, 528:380–383, 2015.

[VBE96] Vlatko Vedral, Adriano Barenco, and Artur Ekert. Quantum networks for elementary arithmetic operations. *Phys. Rev. A*, 54:147–153, 1996.

[VSB+01] L. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood, and I. L. Chuang. Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance. *Nature*, 414:883–887, 2001.

[WRW+16] S. Weidt, J. Randall, S. C. Webster, K. Lake, A. E. Webb, I. Cohen, T. Navickas, B. Lekitsch, A. Retzker, and W. K. Hensinger. Trapped-ion quantum logic with global radiation fields. *Phys. Rev. Lett.*, 117:220501, 2016.

[Zal98] Christof Zalka. Fast versions of Shor's quantum factoring algorithm. arXiv preprint quantum-ph/9806084, 1998.

[Zal06] Christof Zalka. Shor's algorithm with fewer (pure) qubits. arXiv preprint quantum-ph/0601097, 2006.

付録８

学会等での主要攻撃論文発表等一覧

目次

1. 具体的な暗号の攻撃に関する発表

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

表 1 具体的な暗号の攻撃に関する発表

	公開鍵暗号	頁
	He Gives C-Sieves on the CSIDH [Eurocrypt 2020]	100
	Quantum Security Analysis of CSIDH [Eurocrypt 2020]	100
	Rational Isogenies from Irrational Endomorphisms [Eurocrypt 2020]	101
★	Low Weight Discrete Logarithms and Subset Sum in $2^{0.65n}$ with Polynomial Memory [Eurocrypt 2020]	101
	Indistinguishability Obfuscation Without Maps: Attacks and Fixes for Noisy Linear FE [Eurocrypt 2020]	102
	On the Quantum Complexity of the Continuous Hidden Subgroup Problem [Eurocrypt 2020]	105
	Key Recovery from Gram − Schmidt Norm Leakage in Hash-and-Sign Signatures over NTRU Lattices [Eurocrypt 2020]	107
	An Algebraic Attack on Rank Metric Code-Based Cryptosystems [Eurocrypt 2020]	108
★	Comparing the Difficulty of Factorization and Discrete Logarithm: A 240-Digit Experiment [Crypto2020]	110
☆	Improvements of Algebraic Attacks for Solving the Rank Decoding and MinRank Problems [Asiacrypt2020]	115
	ブロック暗号	**頁**
	Improving Key-Recovery in Linear Attacks: Application to 28-round PRESENT [Eurocrypt 2020]	103
☆	New Slide Attacks on Almost Self-Similar Ciphers [Eurocrypt 2020]	103
★	The Retracing Boomerang Attack [Eurocrypt 2020]	104
	Implementing Grover oracles for quantum key search on AES and LowMC [Eurocrypt 2020]	
	Modeling for Three-Subset Division Property Without Unknown Subset — Improved Cube Attacks Against Trivium and Grain-128AEAD [Eurocrypt 2020]	104
	On the Usage of Deterministic (Related-Key) Truncated Differentials and Multidimensional Linear Approximations for SPN Ciphers [FSE 2020]	
	Quantum Security Analysis of AES [FSE 2020]	113
	Extended Truncated-differential Distinguishers on Round-reduced AES [FSE 2020]	
☆	An Algebraic Attack on Ciphers with Low-Degree Round Functions: Application to Full MiMC [Asiacrypt2020]	115
☆	Lower Bounds on the Degree of Block Ciphers [Asiacrypt2020]	115

ストリーム暗号		
★	Improved Differential-Linear Attacks with Applications to ARX Ciphers [Crypto 2020]	110
☆	An Algebraic Formulation of the Division Property: Revisiting Degree Evaluations, Cube Attacks, and Key-Independent Sums [Asiacrypt2020]	114
軽量暗号		
	Cryptanalysis Results on Spook: Bringing Full-Round Shadow-512 to the Light [Crypto2020]	109
	Automatic Verification of Differential Characteristics: Application to Reduced Gimli [Crypto2020]	109
	New results on Gimli: full-permutation distinguishers and improved collisions [Asiacrypt2020]	113
ハッシュ関数／メッセージ認証コード		
	Finding Hash Collisions with Quantum Computers by Using Differential Trails with Smaller Probability than Birthday Bound [Eurocrypt 2020]	105
	Mind the Composition: Birthday Bound Attacks on EWCDMD and SoKAC21 [Eurocrypt 2020]	103
	Out of Oddity – New Cryptanalytic Techniques Against Symmetric Primitives Optimized for Integrity Proof Systems [Crypto2020]	109
	Time-Space Tradeoffs and Short Collisions in Merkle-Damgård Hash Functions [Crypto2020]	110
☆	Finding Collisions in a Quantum World: Quantum Black-Box Separation of Collision-Resistance and One-Wayness [Asiacrypt2020]	114
サイドチャネル攻撃		
☆	Minerva: The curse of ECDSA nonces: Systematic analysis of lattice attacks on noisy leakage of bit-length of ECDSA nonces [CHES 2020]	112
	Cache vs. Key-Dependency: Side Channeling an Implementation of Pilsung [CHES 2020]	
★	SITM: See-In-The-Middle: Side-Channel Assisted Middle Round Differential Cryptanalysis on SPN Block Ciphers [CHES 2020]	111
	When one vulnerable primitive turns viral: Novel single-trace attacks on ECDSA and RSA [CHES 2020]	112
故障利用攻撃		
	Fault Template Attacks on Block Ciphers Exploiting Fault Propagation [Eurocrypt 2020]	106
☆	Security of Hedged Fiat–Shamir Signatures Under Fault Attacks [Eurocrypt 2020]	107
	Persistent Fault Attack in Practice [CHES 2020]	112
	Attacking Hardware Random Number Generators in a Multi-Tenant Scenario [FDTC 2020]	111
その他の攻撃		
	Private Information Retrieval with Sublinear Online Time [Eurocrypt 2020]	102
	Optimal Merging in Quantum k-xor and k-sum Algorithms [Eurocrypt 2020]	106

2. Eurocrypt 2020 の発表

2.1. Eurocrypt 2020 の発表(1 日目)

He Gives C-Sieves on the CSIDH [Eurocrypt 2020]

Chris Peikert

本論文は、CSIDH の秘密鍵復元攻撃に関する論文である。2003 年から 2004 年にかけて、Kuperberg と Regev は、公開鍵から CSIDH の秘密鍵を復元する際の可換群の隠れシフト問題について、漸近的に準指数計算量の量子アルゴリズムを発表した。2011 年末、Kuperberg は続編の量子アルゴリズムである平行ふるい (c-sieve: collimation sieve) を発表した。c-sieve はより少ない量子空間・量子時間計算量を実現しつつ、量子アクセス可能古典メモリ (QRACM: quantumly accessible classical memory といったパラメーターとのトレードオフを提供した。しかし、CSIDH に対する c-sieve の具体的なコストは分析されていなかった。

本論文はこのギャップを埋める。具体的には、Kuperberg の c-sieve を任意の有限巡回群に機能するよう一般化し、いくつかの実用的な効率の改良をおこない、さらに古典シミュレータを与え、実際の CSIDH-512 の群のオーダーに至るまでの幅広いパラメーターで実験し、CSIDH に対する c-sieve の計算量を算出した。

結論として、提案された CSIDH パラメーターは、一様重ね合わせにおける CSIDH の群作用を量子的に評価するためのコストにより与えられるものを若干上回る量子セキュリティを提供している。たとえば、CSIDH-512 の鍵回復のコストは、2^{40} ビットの QRACM を用いて、約 2^{16} 回の量子評価を行うだけである。これは Kuperberg のオリジナルのふるいの亜種についての、$2^{32.5}$ 回の評価と量子メモリの 2^{31} 量子ビットを必要とするという見積を下回る。

さらに、量子評価のコストが最近のベストケース分析で示されたものよりもはるかに高くはない、という仮定の下では、CSIDH-512 は 2^{64} 個の量子 T ゲートよりも大幅に少ない数の量子 T ゲートで破れることになる。このことは、特に MAXDEPTH 制限を考慮した場合、CISDH-512 で主張された NIST レベル 1 の量子セキュリティを強く無効にする。さらに同様の仮定の下では、CSIDH-1024 および 1792 についても MAXDEPTH 範囲の上限付近を除き、レベル 1 には達しない。

Quantum Security Analysis of CSIDH [Eurocrypt 2020]

Xavier Bonnetain and André Schrottenloher

本論文は、CSIDH の秘密鍵復元攻撃に関する論文である。CSIDH は Couveignes、Rostovtsev、Stolbunov による以前の方式と類似しているが、効率と安全性のバランスの改善を目的としている。そこでは、望ましいレベルの量子セキュリティを満たすための具体的なパラメーターを提案している。これらのパラメーターは、Childs、Jao、Soukharev による準指数計算量子アルゴリズムによる、2 つの楕円曲線の間の同種写像を復元攻撃の難しさに基づいている。この量子アルゴリズムは 2 つの

構成要素がある。1 つ目は、可換群の隠れシフト問題を解くための量子アルゴリズム、2 つ目は、ブラックボックスと呼ばれる、与えられた超特異楕円曲線からの全ての同種写像の重ね合わせ計算である。

本論文では、CSIDH のセキュリティを包括的に分析し、具体的な CSIDH-512 の攻撃法を提案する。まず可換群における隠れシフト問題に対する先行研究の 3 つの量子アルゴリズムを、量子計算量と古典計算量のトレードオフを考慮した上で、非漸近的コストの視点から再検討する。次に、隠れシフト問題アルゴリズムにおけるブラックボックスの非漸近的研究を行う。そして、CSIDH-512 を 40000 以下の量子論理ビットで評価する量子手順を示す。

これにより CSIDH の作者が提案したパラメーターは、期待される量子セキュリティを満たしていないことが示される。

Rational Isogenies from Irrational Endomorphisms [Eurocrypt 2020]

Wouter Castryck, Lorenz Panny, and Frederik Vercauteren

本論文は、CSIDH の秘密鍵復元攻撃に関する論文である。本論文では、有限素体 Fp 上の自己同型環 O を共有する 2 つの Fp 上の超特異楕円曲線を繋げる O のイデアルを計算する多項式時間アルゴリズムを導入する。このアルゴリズムは、CSIDH 暗号体系の安全性の、超特異楕円曲線の自己同型環の計算の問題への帰着を提供する。SIDH に関する同様の帰着は Asiacrypt2016 で現れたが、全く異なる技術に依存している。さらに、虚数乗法(CM)を用いて構築された任意の超特異楕円曲線は、既知のベース曲線へのパスを具体的に導出することで、超特異同種写像グラフのどこに位置するかを正確に求めることができることを示した。この結果は、超特異同種写像グラフへのハッシュ関数の構成要素として、このような曲線を用いることを禁止する。

Low Weight Discrete Logarithm and Subset Sum in $2^{0.65n}$ with Polynomial Memory [Eurocrypt 2020]

Andre Esser and Alexander May

本論文は、任意の可換群 G において、ハミング重みが小さいケースの離散対数問題に対する、衝突問題を多項式オーダーの空間計算量で解く、2 つのヒューリスティックアルゴリズムを提案する。1 つ目のアルゴリズムは、部分和問題の Becker-Coron-Joux のアルゴリズム(以下 BCJ)を、離散対数問題に直接適応したものである。2 つ目のものは、新しいマルコフ連鎖解析を用いた表現技術をより複雑に応用することで、全ての可能な重みに対してこの適応を大幅に改善したものである。他の重みが小さいケースの離散対数アルゴリズムとは対照的に、この 2 つ目のアルゴリズムの時間計算量は、一般の離散対数問題のインスタンスに対する Pollard の $|G|^{1/2}$ による評価に収まる。

また、多項式オーダーの空間計算量に収まる、部分和問題に関する新しいヒューリスティックアルゴリズムを提案する。これは n ビットの n 個のランダムな数に対する部分集合和に対する、BCJ の $2^{0.72n}$ という時間計算量を改善する。技術的に新しい点は、Crypto2016 で現れた NestedRho アル

ゴリズムに触発された、再帰的に衝突を発生させる、部分和問題に対するネスト化された衝突発見アルゴリズムである。結果的に、時間計算量を $2^{0.645n}$ まで改善した。

Indistinguishability Obfuscation Without Maps: Attacks and Fixes for Noisy Linear FE [Eurocrypt 2020]

Shweta Agrawal and Alice Pellet-Mary

本論文は、Agrawal による識別不能難読化 (iO: indistinguishability Obfuscation) への攻撃とその修正に関する論文である。iO の候補は「直接法 (direct)」と「ブートストラップ法 (bootstrapping based)」に分類される。直接法は、高次の多重線形写像に依存し、ヒューリスティックな保証を提供する。その一方、ブートストラップ法は、双線形写像、LWE(Learning With Errors)仮定の新種、そして疑似乱数生成器に依存している。最近では、他の仮定と共に、双線形写像から iO を構築する進展も見られている。

これらの手法の例外として、Agrawal による最近の研究は、こういった写像を用いることなく iO を構築した。この研究は新しいプリミティブであるノイズ線形関数型暗号 (NLinFE: Noisy Linear Functional Encryption) を導入することで、格子に関する仮定から NLinFE を直接構築した。この研究では、この新しい仮定に対する予備的な暗号解析が行われていたものの、この安全性を確定させるためにはより多くの暗号解析を行わければならないことも指摘され、さらに具体的なパラメーターの提案も行われていなかった。

本研究はこのギャップを埋めるために、NLinFE の暗号解析を行う。まず攻撃者がこのスキームの安全性を破壊することができる 2 つの攻撃を提案する。この攻撃は今までの iO に対する攻撃とは無関係である。さらに、暗号解析により得られた知見から、これまでに発見された脆弱性を克服した、スキームの修正を提案する。さらにこの方式のセキュリティ面を分析し、妥当な攻撃が通用しないことを論じる。さらにこの修正されたスキームをインスタンス化するための、具体的なパラメーターを提供する。

Private Information Retrieval with Sublinear Online Time [Eurocrypt 2020]

Henry Corrigan-Gibbs, Dmitry Kogan

本論文では、サーバ側のストレージ容量を増やすことなく、データベースの検索を高速(劣線形時間)に行うことができる、初めてのプライベート情報検索プロトコルを提案する。本論文のプロトコルはオフライン/オンラインモデルで動作する。クライアントがどのデータベースビットを読みたいかを決定する前に行われるオフラインフェーズでは、クライアントはサーバから短い文字列を取得する。その後のオンラインフェーズでは、クライアントはサーバに再度問い合わせを行うことで、個人的にデータベースの希望するビットを取得できる。このプロトコルでは、サーバ側の計算の大部分を (クライアントのクエリとは無関係な) オフラインフェーズに移行させることで、オンラインフェーズを非常に高速に完了することができる。本論文のプロトコルは、2 台のサーバでは統計的安全性を、1 台のサーバでは計算上の安全性を提供することができる。最後に、このモデルにおいて、本論文の

プロトコルは、通信時間と実行時間の間のトレードオフの観点から最適であることを証明する。

2.2. Eurocrypt 2020 の発表(2 日目)

Mind the Composition: Birthday Bound Attacks on EWCDMD and SoKAC21 [Eurocrypt 2020]

Mridul Nandi

Crypto2017 において、Minnink と Neves は EWCDM の dual 構成である EWCDMD を提案し、基礎となるブロック暗号のブロックサイズを n としたとき、この構成が n ビットセキュリティを有することを示した。Crypto2019 において、Chen らは置換ベースの設計の SoKAC21 を提案し、その基礎となる置換の入力サイズを n としたとき、この構成が 2n/3 ビットセキュリティを有することを示した。

本論文では、EWCDMD と SoKAC21 に対する birthday bound attack を示し、上記のセキュリティ主張が正しくないことを示している。どちらの攻撃も、それぞれの構造に内在する構成の性質を利用している。著者は、構成の性質を利用したこれら 2 つの攻撃に触発され、(理想的な置換とランダムオラクルモデルにおいて)理想的なプリミティブのある一般的な構成に基づく構造を考慮し、それらに対する birthday bound distinguisher を提案した。特に、(1)非公開のランダム置換とそれに続く公開されたランダム関数、(2)2 つの非公開のランダム関数の合成に対する birthday bound distinguisher を示している。SoKAC21 と EWCDMD に対する distinguishers はそれぞれ(1)と(2)からの直接の帰結である。

Improving Key-Recovery in Linear Attacks: Application to 28-round PRESENT [Eurocrypt 2020]

Antonio Flórez-Gutiérrez and María Naya-Plasencia

線形暗号解析は、共通鍵暗号のセキュリティ評価で使用する最も重要なツールのひとつである。導入以来多くの改良や精緻化が提案され、様々な暗号に対して広く適用されてきた。これらの改良や精緻化の中で、2007 年に Collard らは、FFT に基づく最終ラウンド攻撃のための Matsui’s Algorithm 2 における鍵復元部分の高速化を提案した。

本論文では、以前のアルゴリズムの一般化された行列ベースのバージョンを紹介している。これにより、任意の数の鍵復元ラウンドを考慮に入れることを可能にする。さらに、鍵スケジュールの関係を利用し、複数の線形攻撃と組み合わせることができる効率的な変種も提案している。

このアルゴリズムを使用して、28 ラウンドの PRESENT に対する史上初の攻撃となる新しい暗号解析結果も示している。

New Slide Attacks on Almost Self-similar Ciphers [Eurocrypt 2020]

Orr Dunkelman, Nathan Keller, Noam Lasry, and Adi Shamir

スライド攻撃は、繰り返し構造のブロック暗号に対する強力な暗号解析手法であり、ラウンド数に依存しない計算量で攻撃できるという特性を備えている。しかし、この手法はすべてのラウンドが全

く同一である場合にのみ適用可能である。この要件は Feistel 構造のブロック暗号では当てはまるが、最終ラウンドが追加の post-whitening subkey で終了しなければならないため、SPN 構造ではめったに当てはまることはない。それに加えて、SPN 構造では最終ラウンドに追加の非対称性があります。例えば、AES では最終ラウンドは MixColumns 演算を省略している。最終ラウンドにおけるこのような非対称性は、スライド攻撃のために開発された高度な手法の適用を困難にしている。

本論文では、4 個の新しいタイプのスライド攻撃を開発することで、この「最終ラウンドの問題点」を克服している。提案手法を AES のような構造を持ついくつかの方式に適用することで、提案手法の有効性を示している。ほとんどの場合において、攻撃にかかる計算量を $2^{n/2}$ に近似できる。

The Retracing Boomerang Attack [Eurocrypt 2020]

Orr Dunkelman, Nathan Keller, Eyal Ronen, and Adi Shamir

ブーメラン攻撃は差分攻撃の拡張版である。この攻撃では、暗号システムを 2 つに分割し、それぞれの部分において確率 p と q という異なる差分プロパティがある場合に、暗号システム全体として確率 p^2q^2 という差分(のような)プロパティに組み合わせることが可能となる。本論文では、暗号文における特定の値を利用するための手法を用いた新しいブーメラン攻撃について説明する。

この新しい攻撃を 5 ラウンド AES に適用することで有効性を明らかにする。5 ラウンド AES に対して多様な攻撃手法が適用されてきたが、20 年にわたってその計算量は 2^{32} で不変だった。しかし、Crypto2018 で(全鍵復元の)計算量が 2^{24} にまで低下し、本論文の攻撃では $2^{16.5}$(すなわち、5 ラウンド AES の全鍵復元が 90000 回の暗号化／復号操作しか要求しない)にまで改良した。

以前の攻撃の改良に加えて、この新しい手法はブーメラン攻撃と他の 2 つの暗号解析手法である yoyo game と mixture differential との間の隠された関係を明らかにする。

Modeling for Three-Subset Division Property Without Unknown Subset — Improved Cube Attacks Against Trivium and Grain-128AEAD [Eurocrypt 2020]

Yonglin Hao, Gregor Leander, Willi Meier, Yosuke Todo, and Qingju Wang

Division property は integral distinguisher の探索のための一般的なツールであり、MILP や SAT/SMT のような自動的なツールを使用することでその伝播を効率的に評価することを可能にする。ストリーム暗号に適用する場合には、キューブ攻撃に対する安全性を理論的に見積もることできるため、多くのストリーム暗号に対して最善の鍵復元攻撃へと導くことができる。しかし、いくつかの division property に基づく鍵復元攻撃は、division property の不正確さのために識別攻撃に退化することが報告された。(未知の subset なしの)Three-subset division property はこの不正確問題を解決するための手法であり、この手法を適用するための自動化ツールを使用した新しいアルゴリズムが Asiacrypt2019 で提案された。本論文では、まず、この最新のアルゴリズムが必ずしも効率的ではなく、既存の鍵復元攻撃を改良することができないことを示している。次に、未知の subset なしの three-subset division property の性質に注目し、自動化ツールを使用した新しいアルゴリズムを提案する。この新しいアルゴリズムは既存のアルゴリズムよりも効率的であ

り、既存の鍵復元攻撃を改良することが可能である。この新しいアルゴリズムを Trivium に適用することで、841 ラウンドの鍵復元攻撃が可能であることを示している。また、Crypto2018 で提案された 855 ラウンドの鍵復元攻撃に致命的な欠陥があり、攻撃が機能しないことも示している。結果として、本論文の 841 ラウンドへの攻撃が最善の鍵復元攻撃となる。さらに、この新しいアルゴリズムを Grain-128AEAD に適用することで、既知の 184 ラウンドへの鍵復元攻撃が識別攻撃に退化することを示している。また、この識別攻撃が 189 ラウンドへの攻撃に改良できるとともに、190 ラウンドに対する最善の鍵復元攻撃が可能であることを示している。

Finding Hash Collisions with Quantum Computers by Using Differential Trails with Smaller Probability than Birthday Bound [Eurocrypt 2020]

Akinori Hosoyamada, Yu Sasaki

本論文では、ハッシュ関数に対する量子衝突攻撃に焦点を当てている。古典的設定において、n ビットハッシュの衝突を発見する一般的な計算量は $O(2^{n/2})$ であり、差分暗号解析に基づくリバウンド攻撃のような古典的衝突攻撃では、$2^{-n/2}$ よりも高い確率で差分トレイルを構成できる。同様のアナロジーによると、BHT アルゴリズムのような一般的な量子アルゴリズムでは、$O(2^{n/3})$ の計算量で衝突を発見することが可能となる。量子アルゴリズムにおいて、確率 p の差分トレイルを満たすメッセージペアは、計算量 $p^{-n/2}$ で生成することができる。したがって、量子設定の下では、古典的設定では利用できない確率 $2^{-2n/3}$ までの差分トレイルを衝突攻撃に利用できるかもしれないと期待できる。さらに、攻撃可能ラウンド数の増加に繋がる可能性があると期待できる。

本論文では、2 つの国際的ハッシュ関数の標準方式 AES-MMO と Whirlpool を対象とする。AES-MMO に対し、古典的設定では 6 段までしか攻撃できないが、確率 2^{-80} の 7 段差分トレイルを使用して量子リバウンド攻撃で衝突が発見できることを示している。Whirlpool に対し、バースデイ境界よりも高い計算量で実行可能な古典リバウンド攻撃から得られる 6 段差分トレイルを使用して衝突攻撃を行う。これは 5 段に対する古典的攻撃を 1 段上回っている。結果として、古典的に安全なハッシュ関数は量子攻撃に対しても安全であるという通説は誤りであり、差分トレイル探索は $2^{-n/2}$ で止めるべきではなく $2^{-2n/3}$ まで考慮すべきであることを示した。

On the Quantum Complexity of the Continuous Hidden Subgroup Problem [Eurocrypt 2020]

Koen de Boer, Léo Ducas, and Serge Fehr

本論文は、Hidden Subgroup Problem (HSP) に関する論文である。この問題は、Shor の有名なアルゴリズムの設計図に従って、量子多項式時間でできる問題を網羅的に捉えることを目的としている。この問題を様々な可換群で解くことができれば、素因数分解問題や離散対数問題の求解を効率的に行うことができる。

最新の一般化 (Eisenträger ら、STOC 2014) では、ベクトル空間 R^m におけるフルランクな格子を見つける問題を扱っている。これは新しい暗号解読アルゴリズム (Biasse-Song SODA 2016,

Cramer et al. EUROCRYPT 2016 and 2017）、特にイデアル格子での比較的短いベクトル（mildly short vector）の発見に応用された。

このような問題の暗号解読的な関連性は、より洗練された量子計算量解析の問題を提起する。また、量子ビットの大きな重ね合わせを維持することが物理的に困難になっていることを考慮すると、上記アルゴリズムが必要とする量子ビット数の増加量は重要な研究対象である。

本論文では、前述の HSP アルゴリズム（とそのバリエーション）の詳細解析を提案し、その関連する全パラメーターの関数としての計算量について結論を出す。本論文のモジュール解析は、暗号解読に興味があるケースに将来的に特化した最適化をサポートするために調整されている。この方向性で、いくつかのアイディアも提案する。

Optimal Merging in Quantum k-xor and k-sum Algorithms [Eurocrypt 2020]

María Naya-Plasencia, André Schrottenloher

k-xor、もしくは一般化誕生日問題とは、k 個のビット列のリストが与えられたときに、XOR すると 0 になる長さ k の数列を見つけることを目的とする問題である。与えられたリストが非有界であるとき、最も優れた古典（指数）時間計算量は、Wagner の CRYPTO2002 での論文にとどまっている。仮に与えられたリストが（同サイズで）有界であり、さらに解が一意であった場合、Dinur らの解法アルゴリズム（CRYPTO2012）は、単純な中間一致攻撃よりもメモリ使用量を改善している。

本論文では、k-xor 問題の量子アルゴリズムを研究する。非有界なリストと量子アクセスを用いて、Grassi らによる過去の研究（ASIACRYPT 2018）をほぼすべての k について改善する。次に、本論文の研究を古典的アクセスのみ行う任意サイズのリストのケースに拡張する。本論文では、k-xor アルゴリズムにおける量子と古典をマージする最も知られている戦略を表現する、「マージツリー（merging trees）」の集合を定義し、この方法が最適であることを示す。本論文の計算量は、与えられた k-xor 問題に対する最良戦略を計算する混合整数線形計画によって確認される。本論文の全てのアルゴリズムは、ビット単位の xor の代わりに合同算術を考える場合にも適用可能である。この枠組みにより、全ての k とリストのサイズに対して、改良された新しい量子 k-xor アルゴリズムが与えられる。応用例としては、部分和問題、限られたメモリでの LPN、多重暗号問題などが挙げられる。

2.3. Eurocrypt 2020 の発表（4 日目）

Fault Template Attacks on Block Ciphers Exploiting Fault Propagation [Eurocrypt 2020]

Sayandeep Saha, Arnab Bag, Debapriya Basu Roy, Sikhar Patranabis, and Debdeep Mukhopadhyay

本論文では、与えられた組み合わせ回路を通してのフォールトの生起及び伝播がデータに依存することを利用し、このような組み合わせの性質が強力な「フォールトテンプレート攻撃」につながること、回路電力解析とフォールト攻撃の両方に対する防御を備える実装にすら適用可能であることを示している。この攻撃は、ブロック暗号の中間のラウンドにフォールトを注入した場合でも適用可能である。既知平文攻撃のシナリオに適用可能であるように見えるが、さらに、中間ラウンド攻撃では平文や暗号文へのアクセスも不要である。攻撃者は未知の平文を繰り返す能力さえあれば攻撃可能である。サイドチャネル-フォールト攻撃対策ありの PRESENT のハードウェア実装と、耐性ありの公開されている AES 実装への評価シミュレーションによってこの攻撃の効果を証明している。

Security of Hedged Fiat–Shamir Signatures Under Fault Attacks [Eurocrypt 2020]

Diego F. Aranha, Claudio Orlandi, Akira Takahashi, and Greg Zaverucha

署名ごとの乱数の決定論的な生成は、Fiat-Shamir 型の署名スキームにおける乱数性の欠落の致命的リスクを軽減するための広く受け入れられた解決策となっている。しかし、最近の研究では、そのような脱乱数スキーム(EdDSA を含む)は差分故障利用攻撃に脆弱で、乱数の再利用又はその他の手段による計算誤りを意図的に引き起こすことによって、攻撃者が署名鍵全体を復元することが可能になることが示されている。乱数性の欠陥の問題と故障利用攻撃の脅威とのバランスをとるため、署名の設計には、秘密鍵、メッセージ、及び nonce をハッシュすることによって、署名ごとの乱数の「ヘッジされた」派生を提唱しているものがある。実用的な署名スキームにおけるヘッジパラダイムが人気を博してきているにもかかわらず、ヘッジされた署名のフォールト耐性の形式的解析の試みはなされていない。

本論文では、Fiat-Shamir transform を介して構築された署名スキームのフォールト耐性の形式的なセキュリティ解析を実行している。著者は”bit-tampering”な故障利用攻撃を特徴づけるモデルを提案し、署名計算の異なるステップを横断したそれらのインパクトを解析している。その結果、ヘッジパラダイムはある種のフォールトに対しては攻撃を軽減できるが、その他のフォールトに対しては攻撃が依然有効であることを証明した。また、具体的なケーススタディとして、この結果を、シグナルメッセージプロトコルで使用されている、ヘッジされた版の EdDSA である XEdDSA、及び、NIST の耐量子計算機暗号標準化プロセスの第 2 ラウンドにある、ヘッジされた Fiat-Shamir 署名スキームである Picnic2 に適用している。

2.4. Eurocrypt 2020 の発表(5 日目)

Key Recovery from Gram − Schmidt Norm Leakage in Hash-and-Sign Signatures over NTRU Lattices [Eurocrypt 2020]

Pierre-Alain Fouque, Paul Kirchner, Mehdi Tibouchi, Alexandre Wallet, and Yang Yu

本論文は、 hash-and-sign の格子ベース署名におけるサイドチャネル漏洩について示している。特に、署名のために用いられるオリジナルの GPV 格子トラップドアパラダイムの 2 つの効率的な

実装である、NIST 第 2 ラウンド候補の Falcon とその前身であるより単純な DLP を対象とする。これらは NTRU 格子上で GPV 署名方式を実装し、一般的な格子の場合よりも大幅な高速化を実現している。

本論文の貢献は以下の 3 つである。1 つ目に、これらの方式のほとんどの実装において、サイドチャネルリークが起こる特定の原因が格子ガウシアンサンプリングにおける 1 次元ガウシアンサンプリングにあることを発見した。結果として、これらのステップの実装では、秘密である格子基底の Gram-Schmidt ノルムが漏洩していることがわかった。2 つ目に、この漏洩と秘密鍵との関係性を明らかにし、Gram-Schmidt ノルムから秘密鍵を再構成できることを示す。この結果は、2 べきの数の円分体上で動作しているスキームの代数的構造をフルに活用する。3 つ目に、離散対数問題に対するサイドチャネル攻撃を行う(ただし、Falcon ではない)。タイミング情報では Gram-Schmidt ノルムの近似値しか得られないため、本論文の代数的な復元技術を適用するには、刈り込み木探索との組み合わせが必要となる。結果として、2^{35} 個程度の離散対数問題の痕跡があれば、十分な確率で鍵全体を復元できることを示した。

An Algebraic Attack on Rank Metric Code-Based Cryptosystems [Eurocrypt 2020]

Magali Bardet, Pierre Briaud, Maxime Bros, Philippe Gaborit, Vincent Neiger, Olivier Ruatta, and Jean-Pierre Tillich

本論文は、ランク距離符号ベースの暗号に関する論文である。ランク距離とは、2 つの行列の差のランクを距離として取り扱うことであり、この暗号はランク距離復号問題の難しさに帰着される。最近では、この問題やその quasi-cyclic 版に基づいた非常に効率的な方式が提案されている。例えば、NIST Post-Quantum Cryptography Standardization Process における第 2 ラウンドでの ROLLO、RQC などが代表的である。この問題に対する組み合わせ攻撃は広く研究されているものの、代数的攻撃はいまだに研究されておらず、先行研究では暗号パラメーターに効果がないと示唆された。

本論文では、Ourivski と Johansson が問題を多項式による方程式系として、問題を代数的にモデル化したことを出発点として、簡単に計算できる方程式をこの方程式系を補強する方法を示し、さらにその補強された系を Gröbner 基底でより速く解くことができるようにした。さらに、このアプローチの計算量評価と、magma を使った実装の実用的な時間を示す。これにより、Gröbner 基底と(非量子)組み合わせ法の両方について、これまで知られていた計算量が改善される。例えば、256 ビットの安全性であった ROLLO-I-256 に対しては、200 ビットで攻撃できるようになる。

3. Crypto 2020 の発表

3.1. Crypto 2020 の発表(2 日目)

Out of Oddity – New Cryptanalytic Techniques Against Symmetric Primitives Optimized for Integrity Proof Systems [Crypto2020]

Tim Beyne, Anne Canteaut, Itai Dinur, Maria Eichlseder, Gregor Leander, Gaëtan Leurent, María Naya-Plasencia, Léo Perrin, Yu Sasaki, Yosuke Todo, and Friedrich Wiemer

SNARKs、STARKs、Bulletproofs のような多くの完全性証明システムの安全性と性能は、その元となるハッシュ関数に大きく依存する。このため、いくつかの新しい提案が最近開発されている。これらのプリミティブは、特に実装上の制限から標準的な設計アプローチに必ずしも沿っていないため詳細な安全性評価が必要である。

本論文では、最近のこのようなプリミティブの 2 つのファミリー、GMIMC と HADESMIMC の安全性を比較する。本論文では、最近公開された STARK に適したハッシュ関数チャレンジで提案されたほとんどのパラメーターにおいて、GMIMC と HADESMIMC の置換に対する低計算量の識別器を示す。ZK-STARK プロトコルで実用的な利用に対応するスポンジ構成のより具体的な設定において、GMIMC のラウンド削減版に対する実際的な衝突攻撃と HADESMIMC のいくつかの具体例に対する原像攻撃を提示する。これらの結果の達成のために、本論文では奇標数体のいくつかの暗号的テクニックを一般化し採用した。

Cryptanalysis Results on Spook: Bringing Full-Round Shadow-512 to the Light [Crypto2020]

Patrick Derbez, Paul Huynh, Virginie Lallemand, María Naya-Plasencia, Léo Perrin, and André Schrottenloher

Spook は NIST 軽量暗号標準化プロセスの 2 ラウンド 32 候補の 1 つであり、差分サイドチャネル耐性を主張している点において特に興味深い。本論文では Spook の基盤となる置換フル 6 ステップ版、即ち Shadow-512 および Shadow-384 の実用的な識別器を示し、置換に関して設計者たちにより提案されたチャレンジ問題を解いた。更に、著者らにより考案された CIML2 セキュリティゲームにより許容されるナンス誤用シナリオにおける S1P オペレーションモードの 4 ステップ Shadow に対する実用的な偽造を提示する。

Automatic Verification of Differential Characteristics: Application to Reduced Gimli [Crypto2020]

Fukang Liu, Takanori Isobe, and Willi Meier

差分特性検索のための MILP もしくは SAT ベースモデルの多くにおいては、差分変化のみ取り入れており異なるラウンドにおいて独立と扱われているため、元となる置換において無効なものを発見する可能性がある。この障害を克服するため、本論文では差分特性検索における不整合を自動的に避けるモデルを設計し、差分変化および値変化の両方を取り入れた。本論文の新しいテクニックを CHES2017 で提案された Gimli 置換に適用し、その内の 1 つは Gimli 文書にも載っている

縮退版 Gimli のいくつかの差分特性は実際に矛盾するものであることを示した。更に、NIST 軽量暗号標準化プロセスで第 2 ラウンド候補となっている Gimli 認証暗号スキームおよびハッシュスキームに対する包括的な研究を行い、ハッシュスキームに対しては、semi-free-start(SFS)衝突探索は途中のラウンドから開始して 8 ラウンドまで到達した。認証暗号スキームに対しては、内部状態復元攻撃が 9 ラウンドまで達成することを示した。ただし、本論文の解析は Gimli の安全性を脅かすものではないことを強調しておく。

Improved Differential-Linear Attacks with Applications to ARX Ciphers [Crypto2020]

Christof Beierle, Gregor Leander, and Yosuke Todo

本論文では、ARX (Addition, Rotation and XOR) ベースの暗号に特に焦点を当てた差分線形解析のフレームワークに対する改良を提案している。このインパクトを検証するため、これらの改良を Chaskey と ChaCha に適用し、現在公開されている最良の攻撃を著しく改良することを示した。6-round ChaCha では Time Complexity が $2^{77.4}$、Data Complexity が 2^{58}、7-round ChaCha では Time Complexity が $2^{230.86}$、Data Complexity が $2^{48.83}$ という結果になっている。

Time-Space Tradeoffs and Short Collisions in Merkle-Damgård Hash Functions [Crypto2020]

Akshima, David Cash, Andrew Drucker, and Hoeteck Wee

ランダムオラクルモデルにおいてランダムオラクルに関する任意 S ビット補助情報の入力および T クエリを用いる攻撃者による、Merkle-Damgård 型ハッシュ関数に対する衝突発券攻撃を研究した。最近の結果では、このような攻撃者は n を出力長とするとアドバンテージ $\Omega(ST^2/2^n)$ で(ランダム IV に関して)衝突を発見することができ、バースデイ境界を因子 S 分超えることができる。これらの攻撃は最適であることが示されている。

本論文ではこの攻撃により生成される衝突は T ブロックのオーダーになる非常に長いものであるため現実的な意義を制限しているものと考え、より短い衝突を発見する改良に関していくつかの結果を証明した。例えば、B ブロック長の衝突発見をアドバンテージ $\Omega(STB/2^n)$ で達成する単純な攻撃を提示する。

3.2. Crypto 2020 の発表(5 日目)

Comparing the Difficulty of Factorization and Discrete Logarithm: A 240-Digit Experiment [Crypto2020]

Fabrice Boudot, Pierrick Gaudry, Aurore Guillevic, Nadia Heninger, Emmanuel Thomé, and Paul Zimmermann

本論文では、2 つの新たな記録を報告する。795 ビットレベルに相当する RSA-240 の素因数分

解、そして 795 ビット素体上の離散対数計算である。以前の記録は 2009 年の RSA-768 の素因数分解と 2016 年の 768 ビット離散対数計算であった。本論文で示す 2 つの 795 ビットレベルの計算は同じハードウェアとソフトウェアを用いて行われ、離散対数を計算することは同じサイズの素因数分解よりも大きく難しくはないことを示している。更に、アルゴリズムの多様性と良く選ばれたパラメーターのおかげで、本論文での計算は以前の記録から予想されるよりも遥かに効率的であることを示した。また、本論文の最後のページで RSA-250 の素因数分解について報告する。

4. FDTC 2020 の発表

Attacking Hardware Random Number Generators in a Multi-Tenant Scenario [FDTC2020]

Yrjo Koyen, Adriaan Peetermans, Vladimir Rozic and Ingrid Verbauwhede

クラウド環境での FPGA アクセラレーションサービスの登場や、技術の進歩による FPGA の実装密度向上により、FPGA が同時に複数のアプリケーションを搭載することが現実的になってきている。現状のサービスでは同一の物理 FPGA に複数ユーザを割り当てることは禁止しているが、将来的に FPGA がスケールアップされて状況が変わった場合、同一 FPGA 上に異なる設計者による回路が同居する状況が考えられる。本論文では、そのような状況になった場合に、攻撃者による共通のプログラムロジックへのアクセスが、対象の回路の近傍に攻撃用回路を構築することによって FPGA 内のシステムを遠隔で攻撃することを試みるシナリオでの攻撃可能性を考察している。異なるユーザによる回路は論理的に分離する必要があるが、共有するシリコン基板や電源ネットワークの性質上避けられない相互作用もある。本論文では、FPGA 上に真正乱数生成器が実装されている場合、攻撃者はその FPGA に対するビットストリーム書き込みアクセスだけで(書き込める内容には、FPGA のハードウェア限界以外に制限はない)、FPGA への物理アクセスなしに乱数生成器に攻撃できることを示した。この発表では、電圧操作、リングオシレータロッキング、レプリカ観察の 3 つの攻撃シナリオを提案し、それぞれの攻撃の有効度を、乱数生成器のタイプ(ERO: Elementary Ring Oscillator 及び TERO: Transition Effect Ring Oscillator)ごとに考察している。ERO に対しては電圧操作及びリングオシレータロッキング攻撃が、TERO に対しては電圧操作攻撃が一定の効果があるとの結果が出ている。

5. CHES 2020 の発表

5.1. CHES 2020 の発表(2 日目)

SITM: See-In-The-Middle Side-Channel Assisted Middle Round Differential Cryptanalysis on SPN Block Ciphers [CHES2020]

Shivam Bhasin, Jakub Breier, Xiaolu Hou, Dirmanto Jap, Romain Poussier and Siang Meng Sim

AES などの SPN 構造 のブロック暗号に対する、side-channel assisted differential plaintext attack (SCADPA) と呼ばれる攻撃の改良を発表した。当初の SCADPA は暗号の最初のラウンドしか攻撃できなかったが、この発表では攻撃の設定や手法の改良によって、中間のラウンドを攻撃できるようになったとしている。サイドチャネル攻撃の攻撃対象は典型的には最初か最後に近いラウンドであるため、対策のオーバーヘッドを考えて中間のラウンドに対する対策は手薄になりがちであるが、そのような実装に対する脅威になると考えられる。

Minerva: The curse of ECDSA nonces: Systematic analysis of lattice attacks on noisy leakage of bit-length of ECDSA nonces [CHES2020]

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

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

When one vulnerable primitive turns viral: Novel single-trace attacks on ECDSA and RSA [CHES2020]

Alejandro Cabrera Aldaya and Billy Bob Brumley

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

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

5.2. CHES 2020 の発表(5 日目)

Persistent Fault Attack in Practice [CHES2020]

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

Persistent Fault Attack の実用的な適用可能性についての発表である。Persistent Fault Attack は、暗号実装ハードウェアに対して持続的なフォールトを起こす(例えば、S-Box 計算用テーブルを 1 バイト書き換え、1 ブロックの暗号演算中は誤ったテーブルが参照されるようにする)攻撃で、CHES2018 に初めてその原理が発表された。本発表では、AES の実装に対するこの攻撃手法を改良し、1641 個の暗号文を取得することで AES の鍵を復元できることをしており、これは以前の研究より 28%の改良となっている。さらに、軽量暗号のひとつである PRESENT に対しても適用できることを示した。

6. FSE 2020 の発表

6.1. FSE 2020 の発表(5 日目)

Quantum Security Analysis of AES [FSE2020]

Xavier Bonnetain, María Naya-Plasencia and André Schrottenloher

本論文は、AES に関する初めてのポスト量子セキュリティの解析である。まず、ラウンド数を減らした AES に対する既知の最善の暗号解析の一般化・量子化バージョンを提示し、さらに量子計算機による計算速度向上の利点を受けないように見える攻撃についても議論する。本論文で提示する古典的・量子的の両方にわたる構造的な探索の新しいフレームワークを提案し、その攻撃の複雑性を効率的に計算することを可能にする。

本論文での最善の攻撃は、量子 Demirci-Selçuk 中間一致攻撃である。意外にも、この設定原理の下になるアイディアを使用することで、新しい、直観に反する古典的タイムメモリデータトレードオフを得ることが可能になる。特に、AES-256 及び AES-128 に対するある種の攻撃におけるメモリ消費を軽減することができる。

本論文の攻撃の要素のひとつは、AES の S-Box の差分方程式を、reversible S-Box の量子コストを考慮しながら、効率的に解くことである。現状で得られた結果から判断すると、AES は古典環境だけでなくポスト量子環境においても、量子一般攻撃に関して十分セキュリティマージンがある暗号プリミティブであるように見える。

7. Asiacrypt 2020 の発表

7.1. Asiacrypt 2020 の発表(1 日目)

New results on Gimli: full-permutation distinguishers and improved collisions [Asiacrypt2020]

Antonio Flórez Gutiérrez, Gaëtan Leurent, María Naya-Plasencia, Léo Perrin, André Schrottenloher, and Ferdinand Sibleyras

Gimli は暗号プリミティブの族(ハッシュ関数と AEA スキーム)で、軽量暗号標準化プロセスのた

めの NIST コンペティションの第 2 ラウンド候補に選ばれている。この候補となっている Gimli は、CHES2017 で発表された置換 Gimli に基づいている。本論文では、置換とそれに基づく構築物の安全性を研究する。著者は、Gimli における拡散性の低さとその内部対称性を利用して、初めて 2^{64} の計算量で完全な置換に対する識別器を構築した。さらに、これまでに実装された Gimli の全 24 ラウンドのうち、23 ラウンドで実用的な識別器を導入する。

次に、Gimli ハッシュに対して各々12/18 ラウンドに達する(フルステート)衝突攻撃/Semi-Free-Start(SFS)衝突攻撃を与えた。実際には、8 ラウンド Gimli ハッシュの衝突を計算した。量子設定において、これらの攻撃はさらに 2 ラウンド拡張できる。最後に、置換における線形トレイルの研究を初めて行い、Gimli の 17 ラウンドに達する差分線型暗号解析を提示する。

Finding Collisions in a Quantum World: Quantum Black-Box Separation of Collision-Resistance and One-Wayness [Asiacrypt2020]

Akinori Hosoyamada and Takashi Yamakawa

STOC1989 における Impagliazzo と Rudich の論文から、多くのブラックボックス不可能性に関する結果が確立されたが、これらは暗号プリミティブ間の古典的なブラックボックス帰着を除外しただけであり、量子帰着を用いることで可能となることが期待された。これらの可能性を除外するために、量子設定の下でブラックボックス不可能性を研究した。

本論文では最初に、TCC2004 の Reingold、Trevisan、Vadhan による定式化に従い、完全ブラックボックス帰着に対する量子版を定式化し、衝突耐性ハッシュ関数から一方向性置換（もしくは落とし戸置換）への量子完全ブラックボックス帰着が存在しないことを証明した。本論文では、古典・量子両方のプリミティブ実装を考慮しており、この結果は古典設定において同様の結果を示した Eurocrypt1998 における Simon の手法を量子設定へ拡張したものとなっている。

7.2. Asiacrypt 2020 の発表(2 日目)

An Algebraic Formulation of the Division Property: Revisiting Degree Evaluations, Cube Attacks, and Key-Independent Sums [Asiacrypt2020]

Kai Hu, Siwei Sun, Meiqin Wang, and Qingju Wang

本論文では、ベクトルブール関数 f の座標関数の任意の積における単項式の有無を、その結合が f となるより単純な列にわたる所謂単項式トレイルの数を数えることにより決定する、分割プロパティの単純化とみなすことができる「単項式予測（monomial prediction）」と名付けたテクニックを導入する。単項式予測を用いて、本論文では TRIVIUM の正確な代数的次数を 834 ラウンドまで初めて得ることができた。キューブ攻撃の文脈においては、より小さい次元でより多くのキューブを同定し、840、841、842 ラウンド TRIVIUM に対するほぼ最適な攻撃の改良を行った。

An Algebraic Attack on Ciphers with Low-Degree Round Functions: Application to Full MiMC [Asiacrypt2020]

Maria Eichlseder, Lorenzo Grassi, Reinhard Lüftenegger, Morten Øygarden, Christian Rechberger, Markus Schofnegger, and Qingju Wang

本論文では初めて、F_2^n 上の MiMC における全てのフルラウンド版に対し、コードブックの半分を必要とする鍵回復攻撃を示した。選択暗号文攻撃シナリオにおいて、MiMC の n ビットフル版に対してこのデータから秘密鍵を復元するのに、MiMC に対する $2^{n-\log_2(n)+1}$ 呼び出しと無視できる量のメモリを必要とする。本攻撃は MiMC のトイ版において実際に検証された。本攻撃は素体上の MiMC の安全性には影響しないことに注意されたい。

Improvements of Algebraic Attacks for Solving the Rank Decoding and MinRank Problems [Asiacrypt2020]

Magali Bardet, Maxime Bros, Daniel Cabarcas, Philippe Gaborit, Ray Perlner, Daniel Smith-Tone, Jean-Pierre Tillich, and Javier Verbel

本論文では、多変数ベースあるいはランク距離符号ベース暗号においていたるところに現れる MinRank 問題を解く代数的手法を著しく改良する方法を示す。後者に現れる構造的 MinRank 問題の場合は、最近の Eurocrypt2020 における Canteaut、Ishai らのブレークスルーを更に改良し、これまで最良と考えられていた組み合わせ攻撃を代数攻撃が凌ぐことを示した。このアプローチを少し改良することにより、本論文ではあるパラメーターに関してはグレブナー基底計算を完全に避け、線型連立方程式を解くことが残されたのみであった。これは本質的に計算量を改良するのみならず、この場合になぜ代数的テクニックが機能するかの確信的議論を与えるものである。NIST PQC 第 2 ラウンド候補の ROLLO-I-128/192/256 に適用した場合、本論文の新しい攻撃は、Eurocrypt2020 で得られたビット計算量 117、144、197 に対し、各々71、87、151 を与える。同様のアプローチにより通常の MinRank 問題に対し代数的的 MinRank ソルバーを改良した。NIST-PQC の第 2 ラウンド候補である GeMSS および Rainbow に適用した場合、本論文の攻撃はこれまでに知られている最良攻撃に非常に近いもしくは少し良い計算量を持つ。

Lower Bounds on the Degree of Block Ciphers [Asiacrypt2020]

Phil Hebborn, Baptiste Lambin, Gregor Leander, and Yosuke Todo

ブロック暗号に対し代数的次数の上限を評価する手法はこれまでに知られているが、設計者にとって安全性を保証する役には立たない。本論文では現代的なブロック暗号の代数的次数の意味ある下限評価を与える。

CRYPTREC Report 2020
(暗号技術評価委員会報告 CRYPTREC RP-2000-2020)

発行日　2021年9月30日　第1版
発行者
・〒184-8795
東京都小金井市貫井北町四丁目2番1号
国立研究開発法人情報通信研究機構
（サイバーセキュリティ研究所 セキュリティ基盤研究室）
NATIONAL INSTITUTE OF
INFORMATION AND COMMUNICATIONS TECHNOLOGY
4-2-1 NUKUI-KITAMACHI,KOGANEI
TOKYO,184-8795 JAPAN

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