CRYPTREC Report 2019

令和 2 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-2000-2019R1

「暗号技術評価委員会報告」

CRYPTREC Report 2019

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 2019 年度活動報告である。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 2019 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、3)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、4)新しい暗号技術に係る調査および評価を実施することを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、2015 年度から本委員会委員長を務められた太田和夫先生に代わって私がその職責を引き継ぐことになり、Post-Quantum Cryptography(耐量子計算機暗号)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していただくことになった。また、今年度は、量子コンピュータ時代に向けた暗号の在り方検討タスクフォースが暗号技術検討会の下に設置されて、量子コンピュータの出現など新たなコンピューティング環境における暗号に関する課題や次期 CRYPTREC 暗号リストが満たすべき要件や課題等について整理することになり、次期 CRYPTREC 暗号リストの策定に向けた議論が開始された。

1)では、例年通り、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、ゲート型の量子コンピュータが量子超越を実現したという報告があり、暗号技術の危殆化が一部で懸念されていることを鑑み、注意喚起レポートとして「現在の量子コンピュータによる暗号技術の安全性への影響」を作成して公表した。3)では、2018 年度に安全性評価を実施し、十分な安全性を有すると判断した暗号利用モード(秘匿モード)XTS の実装評価を実施し、その結果から CRYPTREC 暗号リストに追加するための実装性能要件を満たしていると判断した。4)では、暗号技術調査ワーキンググループ(暗号解析評価)にて、量子コンピュータによる共通鍵暗号の安全性への影響に関する調査及び評価を実施し、直近で現実的な脅威が生じる可能性は極めて低いと判断した。併せて、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ついて再検討し、今後の公開鍵暗号のパラメータ選択に関する対応方針を暗号技術検討会に提案した。

発足して以来 20 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。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の展開をしていきたい。

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。しかしながら、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）が共同で運営する下記のWebサイトで参照することができる。

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

本報告書ならびに上記Webサイトから入手したCRYPTREC活動に関する情報の利用に起因して生じた不利益や問題について、本委員会及び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

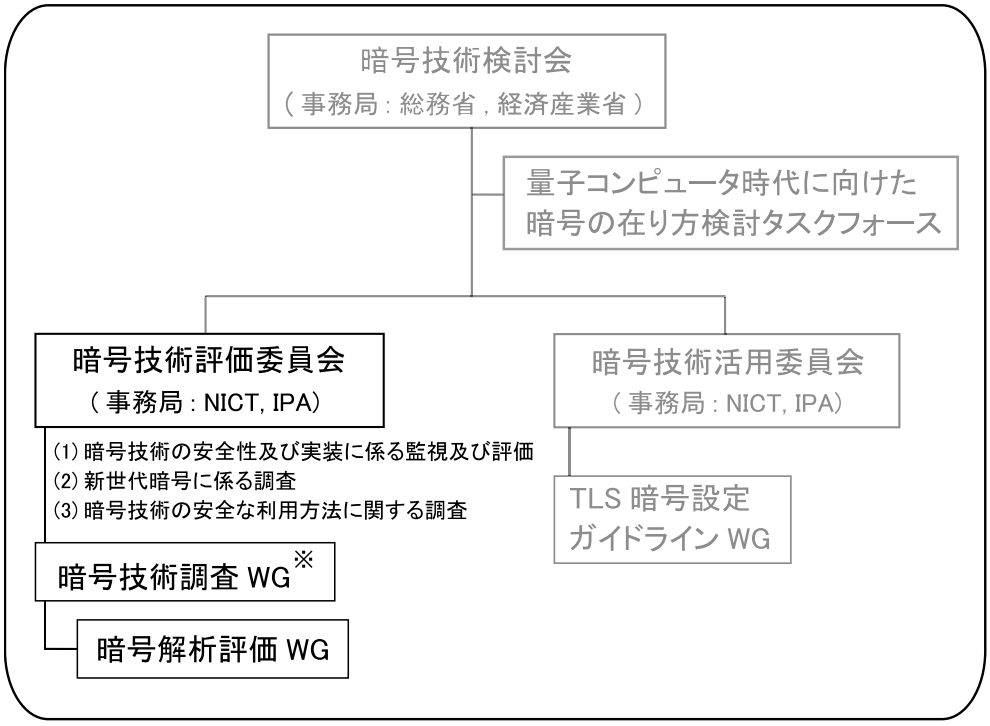
* GPKI: Government Public Key Infrastructure(政府認証基盤)

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。2019 年度、評価委員会の指示に基づき実施される調査項目は、「暗号解析評価 WG」にてそれぞれ検討された。

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	藤﨑 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	日本電信電話株式会社 グループリーダ
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	株式会社富士通研究所 主管研究員
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	九州大学 准教授

オブザーバー

徳永 竜一	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
岡田 崇志	個人情報保護委員会事務局（2020 年 2 月まで）
柏原 陽	個人情報保護委員会事務局（2020 年 2 月から）
中嶋 昌幸	警察庁 情報通信局(2019 年 8 月まで)
田嶋 龍	警察庁 情報通信局(2019 年 8 月から)
小高 久義	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
豊重 巨之	総務省 サイバーセキュリティ統括官室(2019 年 7 月まで)
梅城 崇師	総務省 サイバーセキュリティ統括官室(2019 年 7 月から)
黒田 淳	総務省 サイバーセキュリティ統括官室
遠藤 琢	総務省 サイバーセキュリティ統括官室（2019 年 7 月まで）
山下 恵一	総務省 サイバーセキュリティ統括官室（2019 年 7 月から）
荒木 美敬	外務省 大臣官房
林　巧	経済産業省 産業技術環境局
稲垣 良一	経済産業省 商務情報政策局(2019 年 6 月まで)
上田 翔太	経済産業省 商務情報政策局(2019 年 7 月から)
飯山 貴啓	経済産業省 商務情報政策局
小林 圭樹	防衛省 整備計画局
椛木 隆慎	防衛省整備計画局(2020 年 1 月から)
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（矢野博之[2019 年 7 月まで]、久保田実[2019 年 8 月から]、盛合志帆[2019 年 7 月まで]、野島良[2019 年 8 月から]、大久保美也子、篠原直行、黒川貴司、金森祥子、高橋しおり、吉田真紀、青野良範、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、菅野淳[2019年6月まで]、天内日紗子[2019年7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。

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きた。たとえば、最近では、128-bit key RC4 の脆弱性を利用した攻撃が現実的になる場合が指摘されたことから、2014 年度は、128-bit key RC4 に関する CRYPTREC 暗号リストの注釈を変更した [2]。また、2017 年度は、米国 NIST が Special Publication 800-67 を Revision 2 に更新し、今後 TLS や IPsec で TDEA(The Triple Data Encryption Algorithm)の利用を許容しない方針を打ち出したことから、3-key Triple DES を CRYPTREC 暗号リストの運用監視暗号リストに記載することになった[2]。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。たとえば、最近では、2016 年度に「SHA-1 の安全性低下について」[3]を、2017 年度に「768 ビット素数位数の有限体上の離散対数問題の状況と DSA,DH の今後のパラメータ選択について」 [4]を、2019 年度に「現在の量子コンピュータによる暗号技術の安全性への影響」[5]を Web に掲載した。

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 18 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

[1] https://www.cryptrec.go.jp/list/cryptrec-ls-0001-2012r4.pdf
[2] 2019 年度は、暗号技術活用委員会の下に設置され、「TLS 暗号設定ガイドライン」を策定している TLS 暗号設定ガイドラインワーキンググループにおいて、3-key Triple DES と 128-bit key RC4 を暗号スイートでの利用禁止暗号アルゴリズムに含めることになっている。
[3] https://www.cryptrec.go.jp/topics/cryptrec-er-0001-2016.html
[4] https://www.cryptrec.go.jp/topics/cryptrec-er-0001-2017.html
[5] https://www.cryptrec.go.jp/topics/cryptrec-er-0001-2019.html

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[6]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)」[7](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、

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

「電子政府推奨暗号リスト」として決定された。そして、「各府省の情報システム調達における暗号の利用方針（平成15年2月28日、行政情報システム関係課長連絡会議了承）」において、可能な限り、「電子政府推奨暗号リスト」に掲載された暗号の利用を推進するものとされた。

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

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

2009 年度には、2008 年度に検討した「電子政府推奨暗号リスト改訂のための暗号技術公募要項（2009 年度）」に基づき、電子政府推奨暗号リスト改訂のための暗号技術公募が行われた。2010 年度から 2012 年度にかけて、暗号方式委員会、暗号実装委員会及び暗号運用委員会にて評価が行われ、2012 年度に暗号技術検討会にて電子政府推奨暗号リストの改定が行われた。最終的に、総務省及び経済産業省がパブリックコメント(意見募集)[8]を行い、「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）」が決定された。

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

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

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

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推奨暗号リスト[9]掲載の暗号技術に対する考え方[10]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。図 1.1 に電子政府推奨暗号の削除等の手順を示す。

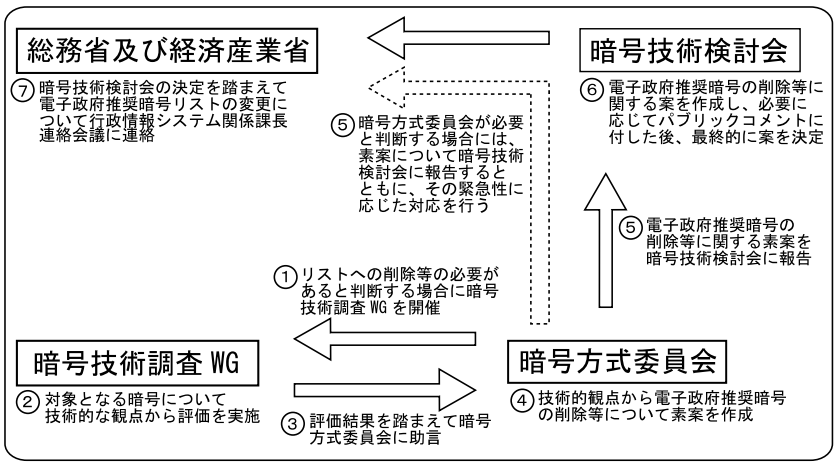


図1.1：電子政府推奨暗号の削除等の手順[11]

(1) 実運用環境において安全性に問題が認められた電子政府推奨暗号は原則としてリストから削除する。

[9] 2003 年 2 月 20 日に策定されたものを指す。
[10] 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
[11] 表中の「暗号方式委員会」は適宜、暗号技術評価委員会と読み替える。

(2) 電子政府推奨暗号の仕様変更は認めない。
(3) 電子政府推奨暗号の仕様変更に到らないパラメータの修正等の簡易な修正を行うことにより当該暗号の安全性が維持される場合には、修正情報を周知して当該暗号をリストに残す。

また、暗号アルゴリズムの脆弱性に関するCRYPTRECからの情報発信については、下記に示すフローチャート(図1.2)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。

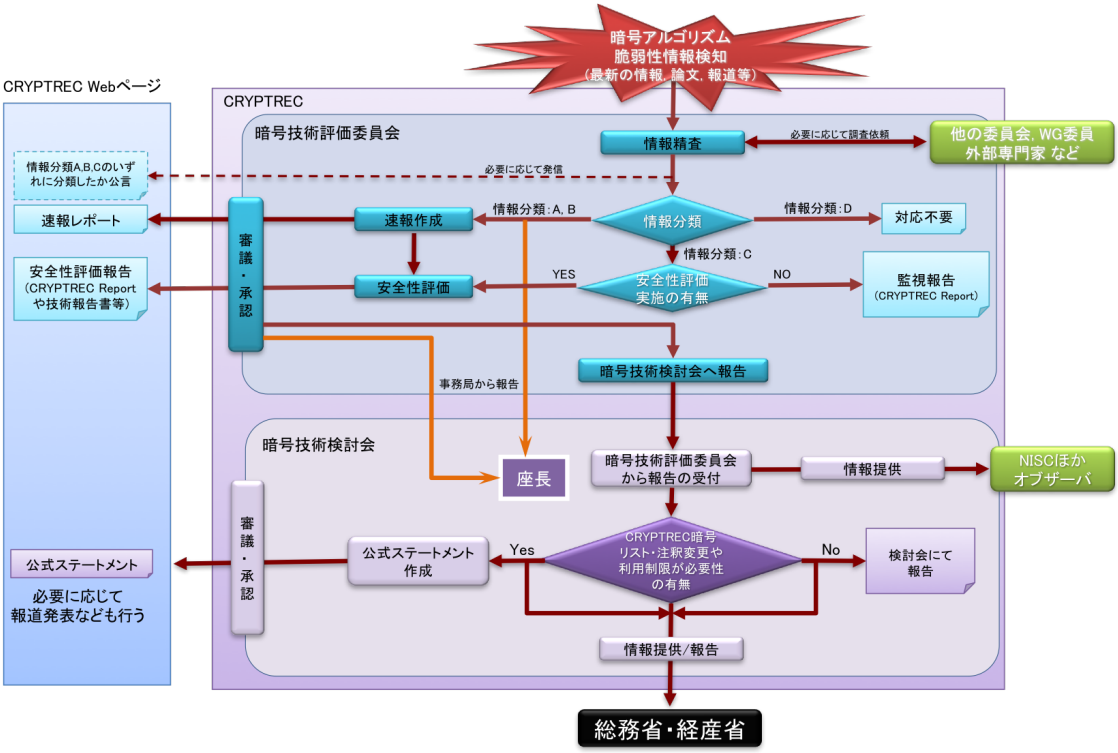


図1.2　暗号アルゴリズムの脆弱性に関する情報発信フロー

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 2019 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

AES もしくはその縮退版について、いくつかの攻撃の進展が見られたが、現実的な脅威となる計算量には至っていない。例えば FSE 2019 においては、6 段 AES-128 の識別攻撃、10 段 AES-256 の関連鍵攻撃、8 段 AES-128 の識別攻撃、5 段 AES-128 の混合差分攻撃等が発表された。

2.1.2. 公開鍵暗号に関する安全性評価について

NIST による耐量子暗号標準化の影響もあり、近年の公開鍵暗号研究は次世代技術に焦点を当てたものが多く、既存の実用暗号に対する攻撃研究の割合は減少している。耐量子暗号標準化の近況については、2.1.4 にて記載する。格子問題に基づく暗号に対する汎用的な攻撃手法として格子縮約アルゴリズムがあるが、Eurocrypt 2019 において Martin R. Albrecht らは、汎用篩カーネル(G6K: General Sieve Kernel)という抽象的状態マシンを導入・実装し格子チャレンジ問題の記録を塗り替えるという話題があった。

2.1.3. ハッシュ関数に関する安全性評価について

SHA-1 に対して、Eurocrypt 2019 において Chosen-prefix collision attack が発表された。これは普通の collision attack より強力な攻撃であり、まだ計算量は大きいものの、この攻撃は証明書の偽造につながり、ひいては TLS などのインターネットプロトコルの安全性を揺るがす可能性があるものである。既に運用監視リストに移行した SHA-1 であるが、その使用がますます推奨されなくなりつつあると考えられる。

推奨候補暗号リストに入っている SHA-3 に関して、3～4 段に縮退させた Keccak-224 及び Keccak-256 に対する攻撃が発表された。直ちに危殆化につながる攻撃ではないが、今後の攻撃の発展に注視すべきである。

2.1.4. その他の注視すべき技術動向について

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

NIST による「量子計算機に耐性を持つ暗号（耐量子計算機暗号、PQC：Post-Quantum Cryptography)」の標準化は、2019 年 1 月 30 日に候補を 64 件から 26 件に絞って第 2 ラウンドに入り、耐量子計算機暗号を対象とする公開鍵暗号研究は益々盛んになっている。2019 年 8 月 24 日～26 日に米国カリフォルニア州サンタバーバラにて、第 2 回 NIST PQC 標準化会議が、その直前に行われた暗号国際会議 Crypto と併催される形で開催された。各候補暗号の前回からの変更点紹介および安全性・処理性能・消費電力等様々な観点からの評価研究が発表された。第 1 ラウンドから第 2 ラウンドへの内訳件数の変化を下表に示す。

表 2.1: NIST PQC コンペティション応募暗号数（第 1 ラウンド→第 2 ラウンド）

	署名	鍵確立／暗号化	合計
格子ベース	5→3	21→9	26→12
符号ベース	2→0	17→7	19→7
多変数	7→4	2→0	9→4
対称/ハッシュベース	3→2	0→0	3→2
その他	2→0	5→1	7→1
合計	19→9	45→17	64→26

会議冒頭に NIST の Dustin Moody 氏から開会挨拶があり、候補のマージはまだ許容されること、第 2 ラウンドは 12 ヵ月～18 ヵ月かかり、その後第 3 ラウンドに入ると予想していること、それでもドラフト標準は 2022 年頃を期待していること、第 2 ラウンドは処理性能が大きな役割を果たすであろうこと等が述べられた。従って今後は 2020 年 7 月頃に第 3 回標準化会議が開催され、更に候補を絞り、第 3 ラウンドに入ることが予想される。2022 年～2024 年頃のドラフト標準作成の後、2030 年頃に向けて移行を進めていく予定である。

2.2. 注意喚起レポートについて

ゲート型の量子コンピュータが量子超越を実現したと主張する論文が 2019 年 10 月に Nature 誌に発表された[1]。暗号技術検討会の下に設置されている「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」(2019 年 12 月 24 日に開催)[2]にて、過剰な反応を防止することを目的とした情報発信の必要性が提言された。暗号技術評価委員会では、情報発信フロー[3]の B)、すなわち、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の目的で注意喚起レポートを公表した[4]。詳細については、付録 3 を参照のこと。

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. 暗号利用モード XTS の安全性評価について

暗号利用モード XTS の実装性能評価を行い、十分な実装性能があることを確認した[5]。安全性評価については、2018 年度に実施済みであり、2018 年度第二回暗号技術評価委員会(2019 年 3 月 11 日)にて、下記の見解を得ていた。

> XTS モードは、下記 3 点の条件下では、暗号利用モード(秘匿モード)として CRYPTREC 暗号リストへ追加するための安全性要件を満たしている。
> (条件 1) 利用用途は IEEE および NIST SP 800-38E の規格に沿ったストレージやディスクの暗号化に限る。
> (条件 2) XTS 内のブロック暗号には、 CRYPTREC 暗号リスト掲載の 128 ビットブロック暗号を使う。
> (条件 3) 同一の鍵を用いて暗号化する場合、2^{20} ブロックまでとする。

今年度、第二回暗号技術評価委員会(2020 年 2 月 18 日開催)の審議により、(条件 3)は表現が不明瞭であり、また、意図した内容は、参照先仕様書にその制限事項の記載があることから、(条件 1)に包含されるとの解釈の基、安全性要件を満たす条件から(条件 3)を削除することした。また、(条件 1)は、冗長性が高かったため、表現の改善を行った。

---

[1] Quantum supremacy using a programmable superconducting processor (https://www.nature.com/articles/s41586-019-1666-5)

[2] CRYPTREC MT-1430-2019 (https://www.cryptrec.go.jp/report/cryptrec-mt-1430-2019.pdf)

[3] 情報発信フローについては第 1 章を参照のこと。

[4] CRYPTREC ER-0001-2019 (https://www.cryptrec.go.jp/topics/cryptrec-er-0001-2019.html)

[5] 今度実施した評価の概要については、付録 5 または外部評価報告書 CRYPTREC EX-2902-2019(https://www.cryptrec.go.jp/exreport/cryptrec-ex-2902-2019.pdf)を参照のこと。

最終的に、安全性要件を満たす条件は下記の通りとなった。

安全性要件を満たす条件： 1)利用用途はNIST SP 800-38Eの規格に沿ったストレージデバイスの暗号化に限る。 2)XTS 内のブロック暗号には、CRYPTREC暗号リスト掲載128 ビットブロック暗号を使う。

以上の議論を踏まえ、2018年度に実施した安全性評価および今年度実施した実装性能評価の結果に基づき、暗号利用モードXTSは、安全性要件を満たす条件の下で、暗号利用モード(秘匿モード)として十分な安全性及び実装性能を有していると判断した。上記判断に基づき、XTS利用モードはCRYPTREC暗号リストに掲載するために十分な安全性および実装性能を満たしていると判断し、CRYPTREC 暗号リストへの追加を暗号技術検討会に提言した。併せて、追加先としては、大分類「暗号利用モード」_中分類「秘匿モード」とすること、安全性要件を満たす条件を注釈につけることを提言した[6]。

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。その中で、電子政府推奨暗号リストに掲載されているRSA暗号（RSA-PSS、RSASSA-PKCS1-v1_5、RSA-OAEP及び運用監視暗号リストに掲載されているRSAES-PKCS1-v1_5）に関するURLがリンク切れのため、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：RSA暗号の新旧仕様書

暗号技術名	旧仕様書	新仕様書
RSA-PSS	EMC Corporation Public-Key Cryptography Standard (PKCS), PKCS #1 v2.2: RSA Cryptography Standard (October 27, 2012)	Internet Engineering Task Force (IETF) Request for Comments: 8017, PKCS #1: RSA Cryptography Specification Version 2.2 (November 2016)
RSASSA-PKCS1-v1_5		
RSA-OAEP		
RSAES-PKCS1-v1_5	http://www.emc.com/collateral/white-papers/h11300-pkcs-1v2-2-rsa-cryptography-standard-wp.pdf	https://tools.ietf.org/html/rfc8017

[6]（事務局注）2020年度暗号技術検討会(2020年6月19日）の審議結果により、暗号技術評価委員会の提言が承認され、提言内容の通りXTS利用モードは、CRYPTREC暗号リストに追加されることとなった。

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
RSA-PSS	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。	・誤記等の軽微な修正はいくつか存在するが、章・節の構成及び記述内容にほぼ変更はない。 ・旧版では、「F. Intellectual Property Considerations」があったが、新版ではなくなった。 ・新版では、「10. Security Considerations」、「Acknowledgements」と「Authors' Addresses」が出来た。
RSASSA-PKCS1-v1_5			
RSA-OAEP			
RSAES-PKCS1-v1_5			

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
CT-RSA 2019	The Cryptographers' Track at the RSA Conference 2019	米国・サンフランシスコ	2019年3月4日～2019年3月8日
FSE 2019	International Conference on Fast Software Encryption	フランス・パリ	2019年3月25日～2019年3月28日
PKC 2019	22nd IACR International Conference on Practice and Theory of Public-Key Cryptography	中国・北京	2019年4月14日～2019年4月17日
Eurocrypt 2019	The 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques	ドイツ・ダルムシュタット	2019年5月19日～2018年5月23日
PQCrypto 2019	The Tenth International Conference on Post-Quantum Cryptography	中国・重慶	2019年5月8日～5月10日
Crypto 2019	International Cryptology Conference	米国・サンラバーバラ	2019年8月19日～2019年8月22日
FDTC 2019	Fault Tolerance and Diagnosis in Cryptography	米国・アトランタ	2018年8月24日

CHES 2019	Conference on Cryptographic Hardware and Embedded Systems	米国・アトランタ	2019年8月26 日 ～ 2019年8月28日
Asiacrypt 2019	Annual International Conference on the Theory and Application of Cryptology and Information Security	日本・神戸	2018 年 12 月 9 日～ 2018 年 12 月 12 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 6 を参照のこと。

2.5.1. 共通鍵暗号の解読技術

・Boomerang Connectivity Table Revisited: Applications to SKINNY and AES [FSE 2019]

Ling Song, Xianrui Qin, Lei Hu

Eurocrypt 2018 において Cid らが提案したブーメラン接続テーブル(BCT: Boomerang Connectivity Table)では、ブロック暗号 E を $E=E_1 \cdot E_m \cdot E_0$ の合成と書いたとき、既存のスイッチテクニックと不整合を統合し、E_m が単一 S-box 層であるときに E_m の確率を理論的に評価した。

本論文はより一般的なフレームワークを提案し、2 つの差分トレイルの依存関係を含む E_m の実際の境界を特定し、任意のラウンド数に対して E_m の確率を体系的に評価する。AES への適用では、不整合を排除し、関連サブ鍵設定のもとで AES-128 の高確率識別を発見することができた。結果として確率 $2^{-109.42}$ の 6 段識別を構成した。

・Boomerang Switch in Multiple Rounds – Application to AES Variants and Deoxys [FSE 2019]

Ling Song, Xianrui Qin, Lei Hu

ブーメラン攻撃は攻撃者に 2 つの短い差分特性を結合することを許す暗号解析のテクニックである。いくつかの研究結果は、スイッチラウンドにおけるこれらの 2 つの特性間の依存性は、攻撃の計算量に多大の影響を与える、もしくは潜在的に無効にしてしまうことを示している。

本論文ではブーメランスイッチ影響の問題を再訪し、複数ラウンドが含まれる場合に、それを利用する。解析支援のため、ブーメラン差分テーブル(BDT: Boomerang Difference Table)と呼ぶツールを導入する。それはブーメラン接続テーブル(BCT: Boomerang Connectivity Table)の改良と見ることができ、複数ラウンドのブーメランスイッチを体系的に評価することができる。本テクニックが強力であることを示すため、10 ラウンド AES-256 に対する新しい関連鍵攻撃を提示する。この場合 2 つの単純関連鍵と 2^{75} の計算しか必要としない。更に、フル AES-192 および縮退版 Deoxys に対する改良攻撃を提示する。

・New Yoyo Tricks with AES-based Permutations [FSE 2019]

Dhiman Saha, Mostafizar Rahman, Goutam Paul

Asiacrypt 2017 で、Rønjom らは Yoyo Trick と呼ばれる攻撃を提案し、最も効率的な distinguisher を見つけるために AES に適用した。

本論文では、Yoyo アイディアを初めて public permutation の識別に適用した。Yoyo のアイディアを拡張してより高い段数に適用している。その応用として、AES ベースの public permutation で、認証暗号 PAEQ 内で使用されている AESQ を解析し、これまでの AESQ に対する攻撃のすべての記録をかなり更新した。さらに別の応用として、known-key setting の 8 段 AES に対して計算量 2^{30} で distinguisher を見つけ出す攻撃を提示した。

・Mixture Differential Cryptanalysis: a New Approach to Distinguishers and Attacks on round-reduced AES [FSE 2019]

Lorenzo Grassi

本論文では、“Mixture Differential Cryptanalysis”と名付けられた、段数を縮退させた AES 類似暗号に対する攻撃を紹介している。5 段 AES-128 に対して、攻撃のコストは選択平文 $2^{33.6}$ 個、計算コスト $2^{33.28}$ である。

・The Exchange Attack: How to Distinguish Six Rounds of AES with $2^{88.2}$ Chosen Plaintexts [Asiacrypt 2019]

Navid Ghaedi Bardeh and Sondre Rønjom

CRYPTREC 暗号リストに掲載されている米国標準暗号 AES に対する識別可能性に関する解析論文で、SPN 構造のブロック暗号に適した新しい攻撃手法(exchange-equivalence attacks)を提案した。本発表では、exchange-invariant と呼ぶ特性（直感的にはあるルールで決められた場所の値が交換された平文組の集合）を満たす $2^{88.2}$ の選択平文と $2^{88.2}$ の暗号化によって 6-round AES 秘密鍵識別器(Secret-key distinguishers)を始めて構成し、それら exchange-invariant な集合を利用すると少なくとも AES の 6 段目では偏りがあることを示した。また 2^{30} の選択平文と 2^{30} の暗号化に改善した 5-round AES 秘密鍵識別器を構成し、スケールダウンしたバージョンでの実機検証を行った。

この攻撃手法は、任意の SPN 構造のブロック暗号に拡張可能であり、特に軽量暗号のような拡散が小さい設計方針の暗号に対してより強力に適用できる。

2.5.2. 公開鍵暗号の解読技術

・The General Sieve Kernel and New Records in Lattice Reduction [Eurocrypt 2019]

Martin R. Albrecht, Leo Ducas, Gottfried Herold, Elena Kirshanoa, Eamonn W. Postlethwaite, Marc Stevens

本論文では、篩アルゴリズムに基づいた広い範囲の様々な格子縮約戦略をサポートする抽象的状態マシンである汎用篩カーネル G6K(General Sieve Kernel)を提案する。本マシンの基本命令セットを用いて既存の篩戦略の簡潔な定式化を与え、更に新しい戦略や BKZ の変形を与える。更に、与えられた縮約品質に求められる篩計算を最小化する新しいトリックを与える。また、本マシンを実現するマルチスレッド化され変更可能な最適実装をオープンソースで公開した。これまで解かれていなかった Darmstadt SVP (151, 153, 155)、LWE(例えば(75, 0.005))を解くことができた。これまでの SVP-150 の記録よりも本提案の SVP-151 は 400 倍高速に解を見つけることができた。

・A Novel CCA Attack using Decryption Errors against LAC [Asiacrypt 2019]

Qian Guo, Thomas Johansson, Jing Yang

復号誤り可能性を持ち、誤り訂正符号を利用する暗号スキームに対する秘密鍵回復攻撃の提示および議論を行った。特に NIST 耐量子計算機暗号標準化において第 2 ラウンドへ進んだ LAC に対する攻撃を示す。LAC256 に関しては、事前計算コスト 2^{162} を除けば、2^{79} の計算量で、約 2^{64} 個の公開鍵の内 1 つを回復することができた。LAC256-v2 の場合は、事前計算は 2^{162} から 2^{171} に増える。

・Crypto 2019 ランプセッションの話題

カリフォルニア大学サンディエゴ校の Nadia Henninger 氏が、Bitcoin の楕円曲線署名で利用されているドメインパラメータ secp256k1 等の生成元座標に人為的な痕跡があることを発表した。

2.5.3. ハッシュ関数の解読技術

・From Collisions to Chosen-Prefix Collisions - Application to Full SHA-1 [Eurocrypt 2019]

Yunwen Liu, Glenn De Witte, Adrian Ranea, Friedrich Wiemer

Chosen-prefix collision attack は collision attack のより強力な変種で、任意の challenge prefix のペアを衝突に変換することができる。Chosen-prefix collision は (identical-prefix) collision よりも通常は作成が著しく困難であるが、このような攻撃の実際的なインパクトははるかに大きい。多くの暗号学的構成がそのセキュリティ証明を衝突耐性に依存しているが、攻撃者が衝突するメッセージに対するコントロールは限られているため、衝突攻撃を具体的なプロトコルを破ることにつなげることは難しい。一方、chosen-prefix collision は(不正な CA を作成することで)証明書を破り、多くのインターネットプロトコル(TLS、SSH、IPsec)を破ることが示されている。

本論文では、collision attack を chosen-prefix collision attack に変換する新しいテクニックを提案している。これらのテクニックを MD5 と SHA-1 に適用することで、改良さ

れた攻撃方法を得る。特に、現在知られている最良の攻撃が $2^{77.1}$ である中で、$2^{66.9}$～$2^{69.4}$ の複雑さの SHA-1 に対する攻撃が得られた。これは SHA-1 に対する古典的な collision attack の複雑さ($2^{64.7}$ と見積もられている)に近い。これは、SHA-1 を使用している産業界及びユーザが可能な限り素早く SHA-1 から移行すべきであるとの警告を意味する。

・Preimage Attacks on Round-reduced Keccak-224/256 via an Allocating Approach [Eurocrypt 2019]

Ting Li and Yao Sun

本論文では、3 段の Keccak-224 及び 4 段の Keccak-256 に対する新しい原像攻撃を提示する。攻撃には allocating approach と呼ばれる手法を使用し、複雑性は 2 つのステージに、考慮すべき制約はより少なく、各ステージにおいて複雑性が小さくなるように配置される。特に、与えられたハッシュ値に対して、1 ブロックではなく 2 ブロックの原像を見つけることを試み、1 ブロック目と 2 ブロック目のメッセージブロックがそれぞれ 2 つのステージで見つけるようにしている。そのため、2 つのステージの複雑性は 1 ブロックの原像を直接見つけることより小さい。さらに、3 段の Keccak-224 に対し計算量 $2^{39.39}$ で(2 番目の)原像を実現する攻撃を提示した。

・Efficient Collision Attack Frameworks for RIPEMD-160 [Crypto 2019]

Fukang Liu, Christoph Dobraunig, Florian Mendel, Takanori Isobe, Gaoli Wang, Zhenfu Cao

兵庫県立大学の五十部らは、CRYPTREC 運用監視暗号リストに掲載されており、ISO/IEC 標準であり Bitcoin アドレス生成等に利用されているハッシュ関数 RIPEMD-160 の縮退版に対する衝突攻撃を行い、30/31 段(80 段中)に対し各々 $2^{35.9}$/$2^{41.5}$ の時間計算量で攻撃できることを示した。まだセキュリティマージンは大きく残っているが、これまでの攻撃に比べて約 8000 倍高速となる結果であるため今後の進展に注意が必要である。

2.5.4. その他の暗号技術の解読技術

・An Analysis of NIST SP 800-90A [Eurocrypt 2019]

Joanne Gikkiway and Dan Shumow

本論文では、NIST SP800-90A で定義されている疑似乱数生成器を分析している。SP800-90A には、HASH-DRBG、HMAC-DRBG、CTR-DRBG が定義されているが、その実装の仕方にはかなりの柔軟性が認められており、実装時に選択できる事項がいくつかあるが、その選択によっては十分なセキュリティが得られないことを示している。HMAC-DRBG は、additional input なしで実装すると forward security を破る攻撃があることを示している。CTR-DRBG の derivation function なしでの実装に対する攻撃も提示している。一度に出力するビット数

が大きすぎる場合にもセキュリティが弱まることを示している。CTR-DRBG に対するサイドチャネル攻撃についても言及している。

本論文では CTR-DRBG のオープンソース実装についても調査しており、OpenSSL は出力ビット長が無制限であり、derivation function なしの実装も可能であるというセキュリティを弱めかねない実装を行っていることも指摘している。

実装の選択による脆弱性を避けるため、可能な限り additional input を使用すること、現実的な範囲で可能な限り頻繁に reseed を行うこと、必要な長さの乱数を取得するために出力長を巨大にした 1 度の呼び出しにまとめるようなことは避けること、CTR-DRBG においては derivation function を必ず使用すること、サイドチャネル攻撃が脅威として考えられ、その対策が十分でない場合には CTR-DRBG の使用は避けるべきであること、を推奨している。

・Cryptanalysis of OCB2: Attacks on Authenticity and Confidentiality [Crypto 2019]

Akiko Inoue, Tetsu Iwata, Kazuhiko Minematsu, Bertram Poettering

NEC の峯松、井上、名古屋大学の岩田らによる認証暗号 OCB2 に対する偽造攻撃が、Asiacrypt 2018 ランプセッションで発表され、OCB2 が ISO/IEC 標準から除外されることとなったことは報告済であるが、Crypto 本会議にて最優秀論文賞を受賞した。

2.6. 委員会開催記録

2019 年度、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	2019 年 6 月 28 日	・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 ・外部評価(暗号利用モード XTS の実装性能に関する調査及び評価)実施についての審議 ・監視状況報告
第 2 回	2020 年 2 月 18 日	・暗号技術調査ワーキンググループ(暗号解析評価)の活動報告 ・外部評価(暗号利用モード XTS の実装性能に関する調査及び評価)実施報告 ・注意喚起レポート発行の報告 ・仕様書参照先変更の報告 ・監視状況報告 ・CRYPTREC Report 2019(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

2019 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: 2019 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	2018 年度の暗号技術評価委員会において、量子コンピュータを使用した共通鍵暗号の解読に関する論文が近年、増加していることが委員から指摘されていることから、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、量子コンピュータによる共通鍵暗号の安全性への影響について調査を行う。 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	2019 年 7 月 29 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 ・量子コンピュータによる共通鍵暗号の安全性への影響に関する調査の進め方についての検討 ・予測図の今後の在り方に関する対応案の検討
第 2 回	2020 年 1 月 24 日	・量子コンピュータによる共通鍵暗号の安全性への影響に関する調査報告の内容確認及びそれに対する暗号技術調査ワーキンググループにおける見解の検討 ・今後の予測図の在り方及び更新方法に関する検討と了承 ・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

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. 活動目的

2019 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」の活動として下記二点について実施することが暗号技術検討会において承認された。

・量子コンピュータによる共通鍵暗号の安全性への影響に関する調査及び評価
・「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」の予測図の在り方についての検討

暗号技術評価委員会では、2019 年度も引き続き、暗号技術調査ワーキンググループ(暗号解析評価)(以下、暗号解析評価 WG という。)の設置を継続し、当該調査を実施した。

3.1.2. 委員構成

(敬称略、五十音順)

主査：	國廣 昇	筑波大学
委員：	青木 和麻呂	日本電信電話株式会社
委員：	草川 恵太	日本電信電話株式会社
委員：	桑門 秀典	関西大学
委員：	下山 武司	株式会社富士通研究所
委員：	高木 剛	東京大学
委員：	高島 克幸	三菱電機株式会社
委員：	峯松 一彦	日本電気株式会社
委員：	安田 貴徳	岡山理科大学
委員：	安田 雅哉	九州大学

3.1.3. 活動概要

本ワーキンググループの開催スケジュールは下記の通りであった。

・2019 年 7 月 29 日 第 1 回 暗号解析評価 WG：活動内容の審議・承認
・2020 年 1 月 24 日 第 2 回 暗号解析評価 WG：調査結果の報告の審議・承認

3.1.3.1. 量子コンピュータによる共通鍵暗号の安全性への影響に関する調査及び評価

① 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。特に米国では NIST が公開鍵暗号について PQC を公募し、現在では提案された暗号方式の安全性評価が進められている。また、欧州の ETSI や ISO/IEC でも標準化に向けた議論が始まっている。

国内では 2017 年度から 2018 年度にかけて、暗号解析評価 WG が公開鍵暗号について PQC の研究動向調査を行い、その調査結果を報告書としてまとめ、2019 年 4 月に公開した。また、2018 年度の暗号技術評価委員会において、量子コンピュータを使用した共通鍵暗号の解読に関する論文が近年、増加していることが委員から指摘されている。

② 実施内容

量子コンピュータによる共通鍵暗号の安全性への影響の調査について、外部専門家による評価を依頼することが、第一回暗号技術評価委員会(2019 年 6 月 28 日）で承認され、具体的な評価内容が、第一回暗号解析評価 WG（2019 年 7 月 29 日）にて承認された。

【件名】量子コンピュータによる共通鍵暗号の安全性への影響に関する調査及び評価
【依頼内容】大規模な量子コンピュータによる解析を想定した場合の共通鍵暗号の安全性への影響について、安全性評価及び調査を行う。具体的には以下の内容を評価に含める。

1）本評価結果の概要（エグゼクティブサマリー）
2）量子コンピュータを用いた共通鍵暗号に対する解析の重要性について
3）量子コンピュータを用いた共通鍵暗号に対する攻撃モデルの解説
4）量子コンピュータを用いた共通鍵暗号への攻撃について、公開されている攻撃の調査
5）現在の電子政府推奨暗号リストに含まれる主要な方式や将来電子政府システム等で利用が見込まれる暗号方式への影響の考察

なお、4）については、2019 年 8 月末までに公開された攻撃を調査対象とする。5）については、網羅性は問わない。
【依頼先】細山田 光倫 様（NTT セキュアプラットフォーム研究所）

③ 外部評価報告書[1]の見解（評価報告書のまとめ）

共通鍵暗号（ブロック暗号、ストリーム暗号)、ハッシュ関数、暗号利用モード（秘匿モード、認証付き秘匿モード)、メッセージ認証コードに対して、量子コンピュータを利用した下記の攻撃モデルが存在する。

- 攻撃モデル: 攻撃者は量子コンピュータを持っており、秘密鍵の埋め込まれた攻撃対象のオラクル（暗号化/復号オラクル、認証タグ生成オラクル）へクエリ可能である。このオラクルへのクエリに対して、古典クエリ攻撃モデル（Q1 モデル）と量子クエリ攻撃モデル(Q2 モデル)の二種類の攻撃モデルが存在する。
  - 古典クエリ攻撃モデル（Q1 モデル）
    - ✓ オラクルへのクエリが古典情報。
  - 量子クエリ攻撃モデル（Q2 モデル）
    - ✓ オラクルへのクエリが量子重ね合わせ状態。
- Q1 と Q2 の比較：Q2 では、秘密鍵が埋め込まれたオラクルが量子回路上に実装されており、攻撃者がその量子回路に量子重ね合わせ状態のクエリができる状況を想定しているため、Q1 より強い攻撃モデルである。CRYPTREC の電子政府推奨暗号リストにあるアルゴリズムは古典計算機向けであるため、通常は Q2 の攻撃モデルには該当しない。しかしながら、難読化処理等で秘密鍵を秘匿して埋め込んだこれらの暗号化処理プログラムを、量子コンピュータをもった攻撃者に渡した場合は、攻撃者は量子オラクルをシミュレート可能であるため Q2 モデルが成立する。

CRYPTREC の電子政府推奨暗号リストに掲載されている共通鍵暗号、暗号利用モード、メッセージ認証コード、ハッシュ関数に対する量子コンピュータを用いた場合の安全性については以下の通りである。

- **共通鍵暗号（ブロック暗号、ストリーム暗号）：** Q1、Q2 モデルにおいては、現行の CRYPTREC の電子政府推奨暗号リストに記載のアルゴリズムに対しては、Grover のアルゴリズムが最良の攻撃であり、k-bit 鍵の全数探索が $2^{k/2}$ の計算量で可能である。長期保存を想定し、耐量子安全性を考慮する場合は、192-bit 鍵や 256-bit 鍵を使用することが賢明である。
- **暗号利用モード・メッセージ認証コード：**Q2 モデルでは認証付き秘匿モードである GCM とメッセージ認証コードである CMAC への偽造攻撃が多項式時間で実行可能になる。ただし、このモデルでの攻撃を実行するためには、攻撃対象の暗号技術が量子回路上に実装されている必要があり、そのような特殊な状況でない限り、Q2 モデルの攻撃が影響を及ぼすことは現状ではないと考えられる。Q1 モデルにおいては、耐量子安全性を考慮する場合は、暗号利用モードの内部で用いるブロック暗号の鍵を 192-bit 鍵や 256-bit 鍵にすればよい。

[1] 詳細については、付録 4 または外部評価報告書 CRYPTREC EX-2902-2019 (https://www.cryptrec.go.jp/exreport/cryptrec-ex-2901-2019.pdf)を参照のこと。

- **ハッシュ関数：**量子コンピュータを用いた場合、ハッシュ関数の原像探索に関して Grover のアルゴリズムが最良の攻撃であり、n-bit 出力のハッシュ関数の原像探索に必要な計算量は $2^{n/2}$ である。衝突探索に必要な計算量は BHT のアルゴリズムを用いると $2^{n/3}$ になるが、この攻撃は $2^{n/3}$ のサイズという非常に多くの量子メモリの使用を必要とするため実際のハッシュ関数の安全性に影響を及ぼすか否かは不透明である。最も現実的に影響を及ぼすと思われるのは CNS のアルゴリズムであり $2^{2n/5}$ の計算量で衝突を発見する。CNS のアルゴリズムは n の多項式オーダのサイズの量子計算機と $O(2^{n/5})$ の古典メモリにて実行可能である。現行の CRYPTREC の電子政府推奨暗号リストに記載のハッシュ関数の出力は 256 ビット以上であり、n = 256 とした場合でも、原像探索の計算量は 2^{128}、衝突探索の計算量は CNS のアルゴリズムで $2^{102.4}$ となるため現実的な脅威となるとは考えづらい。

④ 暗号解析評価 WG の見解

外部評価報告書の結論をもとに表 3.1 と表 3.2 に CRYPTREC の電子政府推奨暗号リストに掲載されている共通鍵暗号、暗号利用モード、メッセージ認証コード、ハッシュ関数に対する量子コンピュータを用いた場合の安全性について、古典計算機を用いた場合の比較とともに示す。表 3.2 では参考のため、$2^{n/3}$ のサイズという多くの量子メモリを必要とする BHT のアルゴリズムが実行できる場合の計算量も併記している。

表 3.1 より共通鍵暗号および暗号利用モードに対して多項式時間で実行可能な攻撃は Q2 モデルにおける Kaplan らのアルゴリズムによる GCM や CMAC への偽造攻撃であるが、外部評価報告書の見解のとおり Q2 モデルは特殊な環境下での攻撃であり現実的な脅威となるとは考え難い。また、表 3.2 のハッシュ関数への攻撃では BHT のアルゴリズムが動作した場合に SHA-256 は $2^{85.3}$ の計算量で衝突探索が可能であるが、$2^{85.3}$ の量子メモリを必要とするため、直近で現実的な脅威となるとは考えづらい。

以上のように、外部評価報告書の評価結果は妥当であると判断する。従って、CRYPTREC の電子政府推奨暗号リストにある共通鍵暗号、暗号利用モード、ハッシュ関数に対する直近で現実的な脅威が生じる可能性は極めて低く、現状では CRYPTREC での具体的な対応は不要である。但し、Even-Mansour 暗号への攻撃のように安全性に現実的な影響を及ぼす可能性がある攻撃が発見される可能性もあるため、攻撃手法および量子コンピュータの発展に関して継続的な監視・評価が必要である。

なお、今回の評価は電子政府推奨暗号リストに掲載されている共通鍵暗号を対象にしているが、推奨候補暗号リストに掲載されている共通鍵暗号も Even-Mansour 暗号や FX 構成への攻撃をそのまま応用できるものではないことから同様の評価結果になると考えられる。

表 3.1： 共通鍵暗号、暗号利用モード、メッセージ認証コードに対する量子コンピュータを用いた場合の安全性（k: 鍵長、b: ブロック長）

	暗号技術	古典クエリ攻撃モデル (Q1 モデル)	量子クエリ攻撃モデル (Q2 モデル)
共通鍵暗号	AES	鍵回復攻撃*1 $2^{k/2}$（古典 2^k）	鍵回復攻撃*1 $2^{k/2}$（古典 2^k）
	Camellia		
	KCipher-2		
暗号利用モード (秘匿モード)	CBC	鍵回復攻撃*1 $2^{k/2}$（古典 2^k）	鍵回復攻撃*1 $2^{k/2}$（古典 2^k）
	CFB		
	CTR		
	OFB		
暗号利用モード (認証付き秘匿モード)	GCM	鍵回復攻撃*1 $2^{k/2}$（古典 2^k）	鍵回復攻撃*1 $2^{k/2}$（古典 2^k） 偽造攻撃*2 多項式時間（古典 $2^{b/2}$）
メッセージ認証コード	CMAC	鍵回復攻撃*1 $2^{k/2}$（古典 2^k）	鍵回復攻撃*1 $2^{k/2}$（古典 2^k） 偽造攻撃*2 多項式時間（古典 $2^{b/2}$）

*1 Grover のアルゴリズム

*2 Kaplan らのアルゴリズム

表 3.2：ハッシュ関数に対する量子コンピュータを用いた場合の安全性

ハッシュ関数	SHA-256	衝突探索: BHT*3 $2^{85.3}$, CNS*4 $2^{102.4}$, （古典 2^{128}） 原像探索*5:2^{128}, （古典 2^{256}）
	SHA-384	衝突探索: BHT*3 2^{128}, CNS*4 $2^{153.6}$, （古典 2^{192}） 原像探索*5:2^{192}, （古典 2^{384}）
	SHA-512	衝突攻撃: BHT*3 $2^{170.7}$, CNS*4 $2^{204.8}$, （古典 2^{256}） 原像探索*5:2^{256}, （古典 2^{512}）

*3 BHT のアルゴリズム（多くの量子メモリが必要な方式）

*4 CNS のアルゴリズム（使用量子ビット数の観点から現実的な方式）

*5 Grover のアルゴリズム

3.1.3.2. 「素因数分解の困難性に関する計算量評価」、「楕円曲線上の離散対数計算の困難性に関する計算量評価」の予測図の在り方についての検討

① 背景

「素因数分解の困難性に関する計算量評価」、「楕円曲線上の離散対数計算の困難性に関する計算量評価」の予測図（以下、予測図と略す）は2006年度に設置された暗号技術調査WG(公開鍵暗号)において作成された。当時、米国NISTは「NIST SP 800-57 Part 1 (Revised)(May,2006)」[2]において暗号技術の鍵サイズに関して「80ビットセキュリティの利用期限を2010年まで」と推奨していた。当該予測図は、これを踏まえ、公開鍵暗号方式のセキュリティパラメータの選択について検討を行うため、RSA1024の危殆化の様子を分かり易く示すために作成されたものである。

近年、計算機の性能向上が鈍化傾向にあることを踏まえ、以下について検討が必要である。

(1)今後の予測図の取り扱い

(2)今後の公開鍵暗号のパラメータ選択

② 今後の予測図の取り扱いについて

これまでの暗号の鍵長の推奨値は、いわゆるムーアの法則（集積回路上のトランジスタ数が18ヶ月毎に2倍になる）を主な根拠として設定されてきた。ところが、近年、計算機の性能向上は以前と比べて鈍化してきている。今後の予測図のあり方に対して、下記のとおり、対応方針を決定した。

対応方針

〈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今まで引いていた範囲（2040年[3]）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。

〈今後の公開鍵暗号のパラメータ選択〉

(2) 公開鍵暗号のパラメータ選択に関する対応方針については、安全性以外にも相互接続性など、運用上の観点もあるため、今後は、暗号技術評価委員会だけではなく、暗号技

[2] 現在は、米国NISTでは「NIST SP 800-57 Part 1 (Revision 4)(January,2016)」において暗号技術の鍵サイズに関して「112ビットセキュリティの利用期限を2030年まで」と推奨している。

[3] 当該範囲については、ルート証明書の有効期限の長いものがあるため、第二回暗号技術評価委員会(2020年2月18日開催)において、現在(2020年)から20年後まで安全であることを分かり易く示すことが必要であると決定された。

術検討会、暗号技術活用委員会や関係各所などを含めて検討することを本 WG として提案する。

③ 予測図の更新について

上記②の(1)の対応方針に基づいて、予測図の更新を下記の通り行った(図 3.1 及び図 3.2)。

- 篩処理の評価を 2006 年度版に基づく評価から 2018 年版(表 3.3)に基づくもの[1]に変更した。

表 3.3: 篩処理時間の推測結果 (単位は、Intel Xeon E5-2680 v3 2.5 GHz コア・年)

法サイズ (ビット)	768	1024	1536	2048
見積もり	561.99	1.52×10^{6}	0.92×10^{12}	1.28×10^{17}

- 近年、ハードウェアを用いた新たな研究成果が無く、古い情報のみに依存した信頼性の低い評価となるため、「専用ハードウェアとソフトウェア処理との性能比較」に対応する外挿線は削除した。
- FactorWorld のサイト(http://www.crypto-world.com/FactorWorld.html)がなくなったので、Integer Factoring Records (https://members.loria.fr/PZimmermann/records/factor.html)に変更した。
- 3072 ビット RSA と 256 ビット ECDLP に関する計算量を表す横線(点線)を入れた。

なお、3072 ビット RSA に関する横線については他のビット長とは異なる評価方法であるため、より精度を高めるためにはさらなる検討が必要である。

参考文献

[1] Evaluation of complexity of the sieving step of the general number field sieve, T. Kleinjung and A. K. Lenstra, December 5, 2018
https://www.cryptrec.go.jp/exreport/cryptrec-ex-2802-2018.pdf

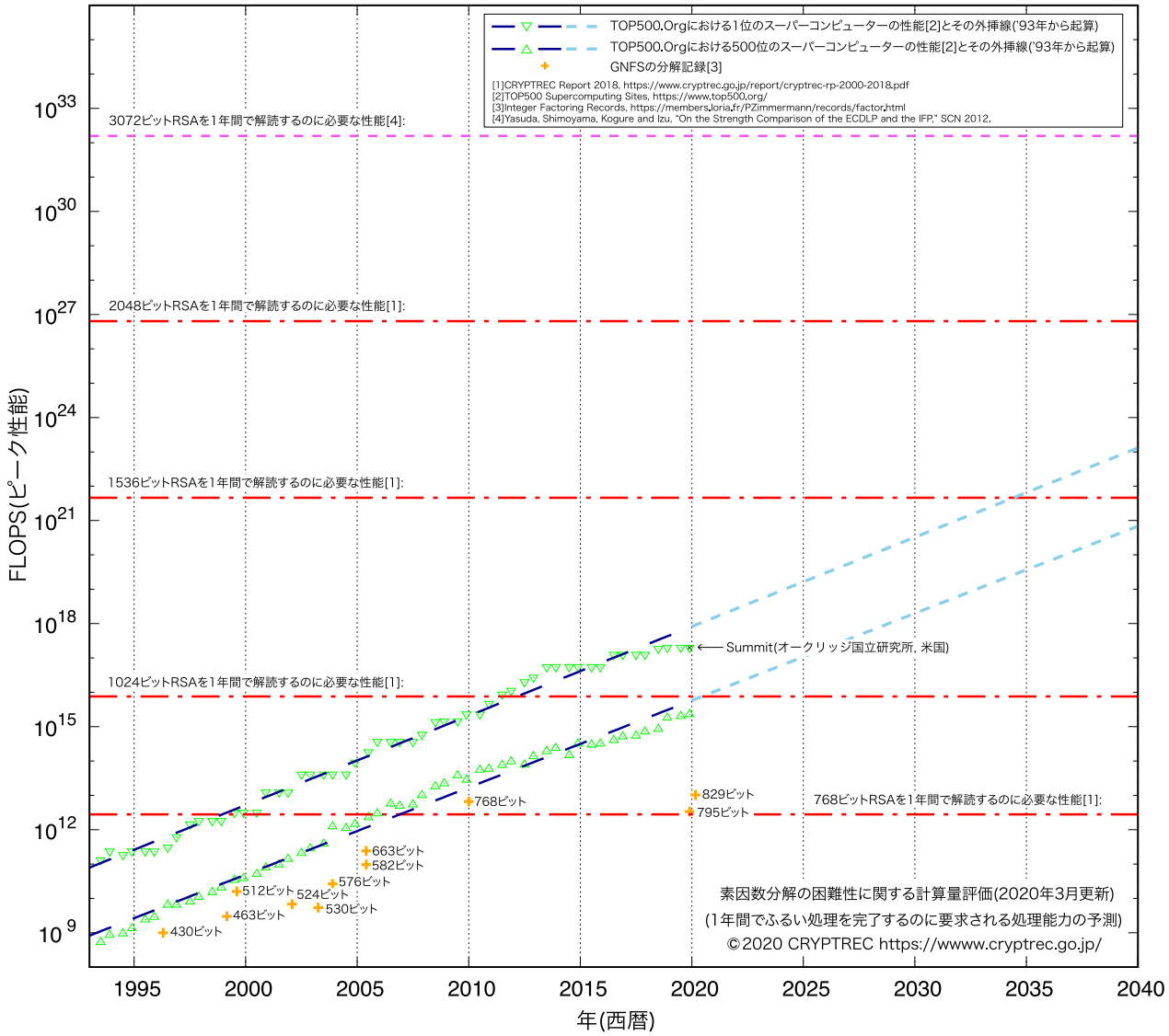


図 3.1：素因数分解の困難性に関する計算量評価
（1 年間でふるい処理を完了するのに要求される処理能力の予測、2020 年 3 月更新）[4]

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

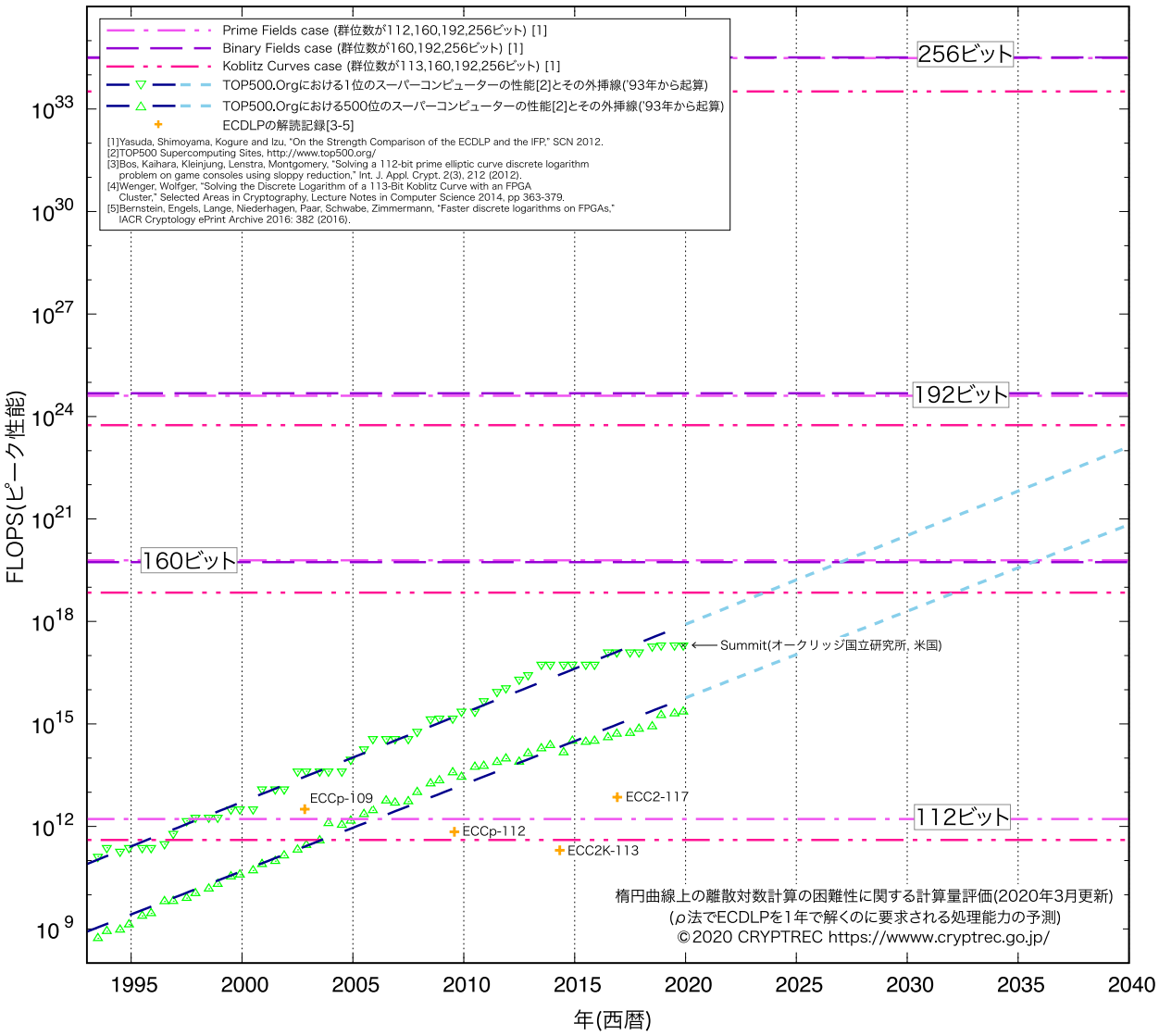


図 3.2：楕円曲線上の離散対数計算の困難性に関する計算量評価
（ρ法で ECDLP を 1 年で解くのに要求される処理能力の予測、2020 年 3 月更新）[5]

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

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

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] 総務省政策統括官（情報セキュリティ担当）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。
http://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	該当なし
	認証付き秘匿モード(注14)	該当なし
メッセージ認証コード		PC-MAC-AES
認証暗号		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。

[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	128-bit RC4(注10)
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。
http://www.nisc.go.jp/active/general/pdf/angou_ikoushishin.pdf
（平成25年 3 月 1 日 現在）

（注9） SSL 3.0 / 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。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。

（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	[削除]

		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。	
	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）		

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/resources/tech/external-activities/crypto/ 英文： https://www.fujitsu.com/jp/group/labs/en/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/resources/tech/external-activities/crypto/ 英文： https://www.fujitsu.com/jp/group/labs/en/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: 0422-59-3897, 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　情報セキュリティグループ グループリーダー　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: 0422-59-3897　　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.toshiba.co.jp/rdc/security/hierocrypt/ 英文：https://www.toshiba.co.jp/rdc/security/hierocrypt/index.htm
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.toshiba.co.jp/rdc/security/hierocrypt/ 英文：https://www.toshiba.co.jp/rdc/security/hierocrypt/index.htm
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/resources/tech/external-activities/crypto/ 英文： https://www.fujitsu.com/jp/group/labs/en/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	〒140-8572 東京都品川区南大井 6-27-18 株式会社日立製作所 セキュリティ事業統括本部 セキュリティ事業統括本部 サイバーセキュリティ技術本部 HIRT センタ 主任技師 栗田 博司 TEL：03-5471-2388(ダイヤルイン), 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　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	〒140-8572 東京都品川区南大井 6-27-18 株式会社日立製作所 セキュリティ事業統括本部 セキュリティ事業統括本部 サイバーセキュリティ技術本部 HIRT センタ 主任技師 栗田 博司 TEL：03-5471-2388(ダイヤルイン), 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　セキュリティ研究所　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。	

付録３

CRYPTREC ER-0001-2019

現在の量子コンピュータによる暗号技術の安全性への影響

（注意喚起レポート）

2020 年 2 月 17 日

CRYPTREC 暗号技術評価委員会

今般、ゲート型の量子コンピュータが量子超越を実現したという報告があり、暗号技術の危殆化が一部で懸念されております。しかし、現在の量子コンピュータの開発状況をふまえると、暗号解読には規模の拡大だけでなく量子誤り訂正などの実現が必要であるため、CRYPTREC としては、CRYPTREC 暗号リスト記載の暗号技術が近い将来に危殆化する可能性は低いと考えています。

今後も、本暗号リスト記載の暗号技術の監視活動を引き続き実施していきます。

今般、ゲート型の量子コンピュータが量子超越を実現したと主張する論文が Nature 誌に発表されました[1]。この論文では、ランダム量子回路からのサンプリング問題を、古典計算機を用いた場合には 1 万年かかるところ、量子コンピュータを用いると 200 秒で完了すると主張しています。この主張は、ランダム量子回路からのサンプリング問題を、量子コンピュータが古典計算機よりも高速に解くことを示しています。これにより、現在広く使用されている公開鍵暗号である RSA 暗号及び楕円曲線暗号などの安全性が大きく低下することが一部で懸念されています。その理由としては、それらの暗号技術が安全性の根拠として利用している素因数分解問題と離散対数問題が、大規模な量子コンピュータと Shor のアルゴリズムを使用することで高速に解読されることが知られているためです。

現在、CRYPTREC 暗号リストの電子政府推奨暗号リストに記載されている RSA-PSS、RSASSA-PKCS1-v1_5、RSA-OAEP は素因数分解問題を、DSA、ECDSA、DH、ECDH などは離散対数問題を安全性の根拠にしています。CRYPTREC では、以前より RSA 合成数の素因数分解などにおける安全なパラメータサイズについて、通常の計算機だけでなく、量子コンピュータによる影響に関しても評価を行っておりますが、今までの評価結果をふまえると、CRYPTREC としては、近い将来に CRYPTREC 暗号リスト記載の暗号技術が危殆化する可能性は低いと考えています。

論文[1]で使用されている量子コンピュータは 53 量子ビットであり、計算は合計 1543 回のゲート演算で構成されています。このとき、1 回当たりの計算時間は、1 マイクロ秒程度であると見積もられています。なお、ターゲットとする問題の性質上、量子誤り訂正は組み込まれていません。

その一方で、例えば、量子コンピュータを用いて2048ビットRSA合成数の素因数分解を行う場合には、量子誤りが一切ないという理想的な環境下でも、4098 量子ビットが必要であり、10^{12}～10^{13}回のゲート演算が必要であると見積もられています[2, 3]。また、量子誤りがあるという現実的な環境下では、2000 万量子ビットが必要であるという見積もりもあります[4]。

このため、実現されている量子コンピュータと素因数分解を行うのに必要とされる量子コンピュータの性能に関しては、依然として大きな乖離があります。これは離散対数問題を利用する暗号についても同様です。量子コンピュータの性能を測る上での指標（量子ビット数、量子誤りの大きさ、演算可能回数など）や、量子コンピュータの開発状況もあわせて考慮にいれると、近い将来に、2048 ビットの素因数分解や 256 ビットの楕円曲線上の離散対数問題が解かれる可能性は低いと考えます。

しかしながら、革新的な技術の発展などにより、量子コンピュータで暗号解読を実現する可能性は否定できません。このため、CRYPTREC では、量子コンピュータによる暗号技術に対する影響、及び量子コンピュータ実現後にも安全な暗号技術（耐量子計算機暗号）に関する監視評価活動を継続していきます。

ご意見・コメントなどの問い合わせがございましたら、下記までお願いいたします。

CRYPTREC 事務局
E-mail: info@cryptrec.go.jp

参照

[1] Quantum supremacy using a programmable superconducting processor
https://www.nature.com/articles/s41586-019-1666-5

[2] National Academies of Sciences, Engineering, and Medicine. 2019. Quantum Computing: Progress and Prospects. Washington, DC: The National Academies Press.
https://doi.org/10.17226/25196
日本語訳版：
E. Grumbling, M. Horowitz 編, 西森 秀稔 訳, “米国科学・工学・医学アカデミーによる量子コンピュータの進歩と展望,” 共立出版, 2020.

[3] NICT サイバーセキュリティシンポジウム
https://www.pco-prime.com/2019cybersympo/

[4] How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits
https://arxiv.org/abs/1905.09749

付録４

量子コンピュータが共通鍵暗号の安全性に及ぼす影響の調査及び評価

(エグゼクティブサマリー)

NTT セキュアプラットフォーム研究所
細山田　光倫

2020 年 1 月

エグゼクティブサマリー

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

- 量子コンピュータを用いた攻撃のモデル，特にハッシュ関数以外の（秘密鍵を用いる）共通鍵暗号系技術への攻撃のモデルには Q1 モデルと Q2 モデルの二種類のモデルが存在する．Q1 モデルにおいては鍵の埋め込まれたオラクルは古典的な攻撃モデルと同じ古典オラクルだが，Q2 モデルにおいては鍵の埋め込まれたオラクルが量子オラクルとなり，攻撃者はオラクルへの量子重ね合わせクエリを行える．Q2 モデルの攻撃を実行するには攻撃対象の暗号技術が（秘密鍵を埋め込んだうえで）量子回路上に実装されている必要がある．
- Q2 モデルにおいては，古典的に安全とされている共通鍵暗号系技術 (CBC-MAC や GCM など) に多項式時間の攻撃が存在する．多項式時間の攻撃には Simon の量子アルゴリズムが用いられる．
- Q1 モデルにおいては，古典的に安全とされている共通鍵暗号系技術に多項式時間の攻撃は現在の所存在しない．しかし従来より認識されていた Grover のアルゴリズムによる鍵全数探索の高速化のみならず，暗号技術の構造に依存した様々な攻撃が存在する．Even-Mansour 暗号および類似の構造を持つ暗号技術に対しては，Q1 モデルであっても Simon のアルゴリズムを活用して古典的攻撃より効率的な攻撃が実行できる．
- 既存研究において使用可能と想定されている量子計算のリソースは論文によって異なり，攻撃コストの評価方法も様々である．特にハッシュ関数への汎用攻撃 (衝突探索など) については，使用可能な量子計算のリソースに関する想定や攻撃コストの評価方法に応じて最良の攻撃が異なる．

また調査した文献の内容に考察を加えた結果，次のような結論を得た．

- ある関数を計算するための古典計算機向けのプログラムコードがあった場合その関数を量子回路上に実装することが可能になるため，Q2 モデルにおいて多項式時間の攻撃が可能な暗号技術については，例え難読化処理等を施しても，その関数 (例えば CBC-MAC でメッセー

ジからタグを計算する関数) を実装して秘密鍵を埋め込んだコードを，量子コンピュータを持った攻撃者に手渡すべきではない．しかし，攻撃対象となる暗号技術が量子回路上に実装されているような（あるいは量子回路上に移植可能となるような）非常に特殊な状況でない限り，既存の共通鍵暗号系技術，特に CRYPTREC の電子政府推奨暗号リストにある共通鍵暗号系技術に，Q2 モデルの攻撃の影響が及ぶことは現状では無いと考えられる．

- 従来から指摘されていた通り，Grover のアルゴリズムによって k ビット鍵の全数探索が時間 $\tilde{O}(2^{k/2})$ で実行可能になるため，長期的に保護したいデータには秘密鍵の鍵長が 128 ビットの暗号技術でなく 192 ビットや 256 ビットの暗号技術を使用するのが賢明であると考えられる．
- 古典的に 128 ビット安全性のあるハッシュ関数の安全性に量子攻撃が現実的な脅威を直接及ぼすとは現状考えづらい．
- CRYPTREC の電子政府推奨暗号リストにある共通鍵暗号系技術の安全性に量子コンピュータが直接与える影響は “Grover のアルゴリズムを用いると k ビット鍵の全数探索が時間 $\tilde{O}(2^{k/2})$ で実行できるため，長期的に保護したいデータには鍵長が 192 ビットや 256 ビットの暗号技術を使用した方が賢明である” という以上のものは現状では無いと考えられる．しかし Even-Mansour 暗号への Q1 モデルにおける攻撃のように安全性に現実的な影響を直接及ぼす可能性のある攻撃が今後も発見される可能性があるため，研究の動向には注意を払っておく必要がある．

付録５

XTS モードの実装性能調査

(エグゼクティブサマリー)

株式会社レピダム
2020 年 2 月

本評価結果の概要（エグゼクティブサマリー）

本調査では、ブロック暗号利用モードのひとつである XTS の実装性能評価を行い、その結果を報告する。現在、XTS は CRYPTREC 暗号リストへの追加候補として検討されているブロック暗号利用モードであり、2019 年に安全性の観点で峯松氏により評価 [1]が行われた。その結果、XTS は現実的に安全であると結論づけられ、CRYPTREC においても CRYPTREC 暗号リストに追加するための要件を満たしていると判断された。本報告書は、現実的に安全であると結論づけられた XTS に対して、電子政府システム等で利用する用途において十分な実装性能を有するか判断するための判断根拠として調査を実施した。本調査は大別して「XTS の市販品などでの実装採用状況」および「XTS の実装性能」の 2 つの観点から調査を実施した。

調査結果として、「XTS の市販品などでの実装採用状況」については、製品や OSS において XTS が広く採用されていることがわかった。代表的な製品としては、Microsoft 社の Windows においてディスク暗号化で用いられる BitLocker や Apple 社の macOS においてディスク暗号化で用いられる FileVault 2 などのストレージ暗号化製品が挙げられる。また、OSS においても、世界中で広く利用されている暗号ライブラリである OpenSSL や組み込み機器で利用される WolfCrypt や mbed TLS などでサポートされていることがわかった。

また、もう 1 つの調査観点である「XTS の実装性能」について、検索エンジンによる XTS の実装性能に関する公開情報による評価結果や、Windows 環境、macOS 環境および Linux 環境における OpenSSL および WolfCrypt を用いた実環境での実装性能測定を実施した。検索エンジンによる XTS の実装性能に関する公開情報に関する調査結果としては、2010 年など比較的古い実装性能に関する情報が公開されている。最新の実装性能としてはベンチマーク製品において拡張現実や機械学習といった高負荷な処理の代表である最先端テクノロジーと同様に、ベンチマークにおける性能測定項目として AES-XTS が含まれたスコアリングが行われていた。また、Windows 環境、macOS 環境および Linux 環境における OpenSSL および WolfCrypt を用いた実環境での実装性能を計測した結果として、CRYPTREC 暗号リストで採用されているブロック暗号利用モードと実装性能を比較した結果、実装性能において大きな遜色はないものと判断した。

付録６

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
	Assessment of the Key-Reuse Resilience of NewHope [CT-RSA 2019]	—
	Decryption Failure Attacks on IND-CCA Secure Lattice-based Schemes [PKC 2019]	68
	Factoring Products of Braids via Garside Normal Form [PKC 2019]	68
☆	Multi-Target Attacks on the Picnic Signature Scheme and Related Protocols [Eurocrypt 2019]	72
	Finding closest lattice vectors using approximate Voronoi cells [PQCrypto 2019]	—
	The impact of error dependencies on Ring/Mod-LWE/LWR based schemes [PQCrypto 2019]	—
	Recovering short secret keys of RLCE in polynomial time [PQCrypto 2019]	—
	Cryptanalysis of an NTRU-based Proxy Encryption Scheme from ASIACCS'15 [PQCrypto 2019]	—
	Preventing timing attacks against RQC using constant time decoding of Gabidulin codes [PQCrypto 2019]	—
	On the Decoding Failure Rate of QC-MDPC Bit-Flipping Decoders [PQCrypto 2019]	—
	On the Complexity of "Superdetermined" Minrank Instances [PQCrypto 2019]	—
	Approx-SVP in Ideal Lattices with Pre-processing [Eurocrypt 2019]	69
	The General Sieve Kernel and New Records in Lattice Reduction [Eurocrypt 2019]	69
	Misuse Attacks on Post-Quantum Cryptosystems [Eurocrypt 2019]	70
	New Results on Modular Inversion Hidden Number Problem and Inversive Congruential Generator [Crypto 2019]	72
	On the Shortness of Vectors to be found by the Ideal-SVP Quantum Algorithm [Crypto 2019]	72
☆	A Novel CCA Attack using Decryption Errors against LAC [Asiacrypt 2019]	75
	Quantum Algorithms for the Approximate k-List Problem and their Application to Lattice Sieving [Asiacrypt 2019]	76
	An LLL Algorithm for Module Lattices [Asiacrypt 2019]	76
	ブロック暗号	**頁**
	MILP-Based Differential Attack on Round-reduced GIFT [CT-RSA 2019]	—
	Quantum Chosen-ciphertext Attacks against Feistel Ciphers [CT-RSA 2019]	—
	Automatic Search for a Variant of Division Property Using Three Subsets	—

2. FSE 2019 の発表

2.1. FSE 2019 の発表(2 日目)

Boomerang Connectivity Table Revisited: Applications to SKINNY and AES [FSE 2019]

Ling Song, Xianrui Qin, and Lei Hu

Eurocrypt 2018 において Cid らが提案したブーメラン接続テーブル(BCT: Boomerang Connectivity Table)では、ブロック暗号 E を $E=E_1 \cdot E_m \cdot E_0$ の合成と書いたとき、既存のスイッチテクニックと不整合を統合し、E_m が単一 S-box 層であるときに E_m の確率を理論的に評価した。

本論文はより一般的なフレームワークを提案し、2 つの差分トレイルの依存関係を含む E_m の実際の境界を特定し、任意のラウンド数に対して E_m の確率を体系的に評価する。AES への適用では、不整合を排除し、関連サブ鍵設定のもとで AES-128 の高確率識別を発見することができた。結果として確率 $2^{-109.42}$ の 6 段識別を構成した。

Boomerang Switch in Multiple Rounds - Application to AES Variants and Deoxys [FSE 2019]

Ling Song, Xianrui Qin, and Lei Hu

ブーメラン攻撃は攻撃者に 2 つの短い差分特性を結合することを許す暗号解析のテクニックである。いくつかの研究結果は、スイッチラウンドにおけるこれらの 2 つの特性間の依存性は、攻撃の計算量に多大の影響を与える、もしくは潜在的に無効にしてしまうことを示している。

本論文ではブーメランスイッチ影響の問題を再訪し、複数ラウンドが含まれる場合に、それを利用する。解析支援のため、ブーメラン差分テーブル(BDT: Boomerang Difference Table)と呼ぶツールを導入する。それはブーメラン接続テーブル(BCT: Boomerang Connectivity Table)の改良と見ることができ、複数ラウンドのブーメランスイッチを体系的に評価することができる。本テクニックが強力であることを示すため、10 ラウンド AES-256 に対する新しい関連鍵攻撃を提示する。この場合 2 つの単純関連鍵と 2^{75} の計算しか必要としない。更に、フル AES-192 および縮退版 Deoxys に対する改良攻撃を提示する。

2.2. FSE 2019 の発表(3 日目)

New Yoyo Tricks with AES-based Permutations [FSE 2019]

Dhiman Saha, Mostafizar Rahman, and Goutam Paul

Asiacrypt 2017 で、Rønjom らは Yoyo Trick と呼ばれる攻撃を提案し、最も効率的な distinguisher を見つけるために AES に適用した。

本論文では、Yoyo アイディアを初めて public permutation の識別に適用した。Yoyo のアイデ

ィアを拡張してより高い段数に適用している。その応用として、AES ベースの public permutation で、認証暗号 PAEQ 内で使用されている AESQ を解析し、これまでの AESQ に対する攻撃のすべての記録をかなり更新した。さらに別の応用として、known-key setting の 8 段 AES に対して計算量 2^{30} で distinguisher を見つけ出す攻撃を提示した。

Mixture Differential Cryptanalysis: a New Approach to Distinguishers and Attacks on round-reduced AES [FSE 2019]

Lorenzo Grassi

本論文では、“Mixture Differential Cryptanalysis”と名付けられた、段数を縮退させた AES 類似暗号に対する攻撃を紹介している。5 段 AES-128 に対して、攻撃のコストは選択平文 $2^{33.6}$ 個、計算コスト $2^{33.28}$ である。

3. PKC 2019 の発表

3.1. PKC 2019 の発表(3 日目)

Decryption Failure Attacks on IND-CCA Secure Lattice-based Schemes [PKC 2019]

Jan-Pieter D'Anvers, Qian Guo, Thomas Johansson, Alexander Nilsson, Frederik Vercauteren, and Ingrid Verbauwhede

本論文では格子ベースプリミティブの選択暗号文安全性に対する復号失敗の影響を探る。復号失敗に基づく秘密鍵回復の一般的枠組みを議論し、NIST 耐量子計算機暗号標準化に提案された ss-ntru-pke に対する主張された安全性より低い計算量の攻撃を示す。初めに格子ベーススキームの失敗率を上げるテクニックを使い、次に失敗する暗号文から攻撃者が引き出すことのできる情報量を調べる。最後にこれらの方法を組み合わせることにより復号失敗攻撃における格子ベーススキームの安全性を解析する。

Factoring Products of Braids via Garside Normal Form ecryption Failure Attacks on IND-CCA Secure Lattice-based Schemes [PKC 2019]

Simon-Philipp Merz and Christophe Petit

組みひも群暗号では、公開組みひもはしばしば秘密組みひもを因子として含み、組みひもワードの積を書き直すことにより個々の因子を隠すことが望まれる。本論文では一般にはそうはならないという実験的証拠を示し、ある条件のもとでは因子の Garside 正規型の部分がそれらの積の Garside 正規型に見出されることを議論する。この観察により、ABC 型組みひもの積の内、B しか知られていないときに分解することができる。本アルゴリズムは NIST 耐量子計算機暗号標準化に提案された WalnutDSA 署名スキームの偽造攻撃に使うことができる。一つのランダムなメッセージ／署名ペアが与えられたときに、128/256-bit 安全性を持つ署名を数秒の内に偽造できる。実験で

は、それぞれの安全性レベルにおいて 99.8/100%成功した。

4. Eurocrypt 2019 の発表

4.1. Eurocrypt 2019 の発表(1 日目)

DLCT: A New Tool for Differential-Linear Cryptanalysis [Eurocrypt 2019]

Achiya Bar-On, Orr Dunkelman, Nathan Keller, and Ariel Weizman

本論文では、差分線型(DL: Differential-Linear)攻撃における 2 つのサブ暗号文間の依存性が多くの場合において DL 攻撃の計算量に大きく影響し、特に攻撃者が攻撃を効率的に行うように用いられることを示す。差分線型接続テーブル(DLCT: DL Connectivity Table)を導入し、2 つのサブ暗号文の依存性を考慮にいれ、E_0 の差分特性と E_1 の線型近似をこの依存性を利用できるように選ぶことができるようにした。DLCT は高速フーリエ変換を用いて効率的に構築することができる。DLCT の強さを、ICEPOLE と 8 ラウンド DES への DL 攻撃改良により示し、また通常の DL 枠組みには適合しない Serpent や CAESAR ファイナリスト Ascon への実験結果を説明する。

4.2. Eurocrypt 2019 の発表(2 日目)

Approx-SVP in Ideal Lattices with Pre-processing [Eurocrypt 2019]

Alice Pellet-Mary, Guillaume Hanrot, and Damien Stehle

本論文では、任意の数体 K の整数環イデアルに対応する格子の近似最短ベクトル問題(approximate SVP: Shortest Vector Problem)を解くアルゴリズムを記述する。Δを K の判別式とするとき、本アルゴリズムは log|Δ|に関して実行時間が指数的となる事前実行フェーズを持つ。重要なことに、本事前実行フェーズは K のみに依存する。本アルゴリズムは、Eurocrypt 2016 の Cramer らのアルゴリズムおよび Eurocrypt 2017 の Cramer らのアルゴリズムに基づいている。Buchmann(数の理論セミナー1990)の枠組みに基づきこれらの方法をマージし、素数べき円分体から全ての数体に適用できるようにした。コストの改良は体のみに依存する事前計算を許したことにより得られる。

The General Sieve Kernel and New Records in Lattice Reduction [Eurocrypt 2019]

Martin R. Albrecht, Leo Ducas, Gottfried Herold, Elena Kirshanoa, Eamonn W. Postlethwaite, and Marc Stevens

本論文では、篩アルゴリズムに基づいた広い範囲の様々な格子縮約戦略をサポートする抽象的状態マシンである汎用篩カーネル G6K(General Sieve Kernel)を提案する。本マシンの基本命令セットを用いて既存の篩戦略の簡潔な定式化を与え、更に新しい戦略や BKZ の変形を与える。更に、与えられた縮約品質に求められる篩計算を最小化する新しいトリックを与える。また、本マシ

ンを実現するマルチスレッド化され変更可能な最適実装をオープンソースで公開した。これまで解かれていなかったDarmstadt SVP(151, 153, 155)、LWE(例えば(75, 0.005))を解くことができた。これまでのSVP-150の記録よりも本提案のSVP-151は400倍高速に解を見つけることができた。

Misuse Attacks on Post-quantumCryptosystems [Eurocrypt 2019]

Ciprian Băetu, F.Betül Durak, Loïs Huguenin-Dumittan,Abdullah Talayhan, and Serge Vaudenay

NIST 耐量子計算機暗号標準化に提案された暗号システムの多くは、代数構造やエンコード方法は異なるが同じメタアルゴリズムに従っている。それらは通常 2 種類の構成(一つはより弱い版、もう一つはランダムオラクルを必要とする版)を提案している。本論文では 9 つの NIST 提案に関して、より弱い版の方に注目する。秘密鍵が複数回用いられるとき、提案者は何の安全性も主張していないが、本論文ではその場合に鍵回復がいかに容易であるかを分析する。平文チェックオラクルを用いた古典鍵回復と、復号オラクルに量子アクセスを仮定した選択暗号文攻撃による量子鍵回復攻撃とを示す。

Attacks only Get Better: How to Break FF3 on Large Domains [Eurocrypt 2019]

Viet Tung Hoang, David Miller, and Ni Trieu

本論文では、CRYPTO 2017 における Durak および Vaudenay の NIST SP 800-38G フォーマット保存暗号標準 FF3 に対する攻撃を改良し、領域 Z/NZ×Z/NZ に対し、実行時間を $O(N^5)$ から $O(N^{17/6})$ に改良した。具体的には、暗号化された 6 桁 PIN を復号するのに、Durak-Vaudenay の攻撃は 2^{50} 操作必要であるが、本攻撃は 2^{30} 操作しか必要としない。

An Analysis of NIST SP 800-90A [Eurocrypt 2019]

Joanne Gikkiway and Dan Shumow

本論文では、NIST SP 800-90A で定義されている疑似乱数生成器を分析している。SP 800-90A には、HASH-DRBG、HMAC-DRBG、CTR-DRBG が定義されているが、その実装の仕方にはかなりの柔軟性が認められており、実装時に選択できる事項がいくつかあるが、その選択によっては十分なセキュリティが得られないことを示している。HMAC-DRBG は、additional input なしで実装すると forward security を破る攻撃があることを示している。CTR-DRBG の derivation function なしでの実装に対する攻撃も提示している。一度に出力するビット数が大きすぎる場合にもセキュリティが弱まることを示している。CTR-DRBG に対するサイドチャネル攻撃についても言及している。

本論文では CTR-DRBG のオープンソース実装についても調査しており、OpenSSL は出力ビット長が無制限であり、derivation function なしの実装も可能であるというセキュリティを弱めかねない実装を行っていることも指摘している。

実装の選択による脆弱性を避けるため、可能な限り additional input を使用すること、現実的

な範囲で可能な限り頻繁に reseed を行うこと、必要な長さの乱数を取得するために出力長を巨大にした 1 度の呼び出しにまとめるようなことは避けること、CTR-DRBG においては derivation function を必ず使用すること、サイドチャネル攻撃が脅威として考えられ、その対策が十分でない場合には CTR-DRBG の使用は避けるべきであること、を推奨している。

4.3. Eurocrypt 2019 の発表(4 日目)

From Collisions to Chosen-Prefix Collisions - Application to Full SHA-1 [Eurocrypt 2019]

Gäetan Leurent and Thomas Peyrin

Chosen-prefix collision attack は collision attack のより強力な変種で、任意の challenge prefix のペアを衝突に変換することができる。Chosen-prefix collision は (identical-prefix) collision よりも通常は作成が著しく困難であるが、このような攻撃の実際的なインパクトははるかに大きい。多くの暗号学的構成がそのセキュリティ証明を衝突耐性に依存しているが、攻撃者が衝突するメッセージに対するコントロールは限られているため、衝突攻撃を具体的なプロトコルを破ることにつなげることは難しい。一方、chosen-prefix collision は(不正な CA を作成することで)証明書を破り、多くのインターネットプロトコル(TLS、SSH、IPsec)を破ることが示されている。

本論文では、collision attack を chosen-prefix collision attack に変換する新しいテクニックを提案している。これらのテクニックを MD5 と SHA-1 に適用することで、改良された攻撃方法を得る。特に、現在知られている最良の攻撃が $2^{77.1}$ である中で、$2^{66.9}$～$2^{69.4}$ の複雑さの SHA-1 に対する攻撃が得られた。これは SHA-1 に対する古典的な collision attack の複雑さ($2^{64.7}$と見積もられている)に近い。これは、SHA-1 を使用している産業界及びユーザが可能な限り素早く SHA-1 から移行すべきであるとの警告を意味する。

Preimage Attacks on Round-ReducedKeccak-224/256 via an Allocating Approach [Eurocrypt 2019]

Ting Li and Yao Sun

本論文では、3 段の Keccak-224 及び 4 段の Keccak-256 に対する新しい原像攻撃を提示する。攻撃には allocating approach と呼ばれる手法を使用し、複雑性は 2 つのステージに、考慮すべき制約はより少なく、各ステージにおいて複雑性が小さくなるように配置される。特に、与えられたハッシュ値に対して、1 ブロックではなく 2 ブロックの原像を見つけることを試み、1 ブロック目と 2 ブロック目のメッセージブロックがそれぞれ 2 つのステージで見つけるようにしている。そのため、2 つのステージの複雑性は 1 ブロックの原像を直接見つけることより小さい。さらに、3 段の Keccak-224 に対し計算量 $2^{39.39}$ で(2 番目の)原像を実現する攻撃を提示した。

Multi-Target Attacks on the Picnic Signature Scheme and Related Protocols [Eurocrypt 2019]

Itai Dinur and Niv Nadler

本論文では、NIST 耐量子計算機暗号標準化に提案された Picnic 署名スキームおよびその基礎となるゼロ知識(ZK)プロトコルである ZKB++に対するマルチターゲット攻撃を編み出した。一人もしくは複数ユーザにより生成された S 個の署名へのアクセスが与えられたとき、本攻撃は(情報理論的に)κビットの署名鍵を $2^{\kappa-7}/S$ の計算量で回復することができる。本攻撃は Picnic の署名アルゴリズムが疑似乱数生成を使っていることを利用しており、この脆弱性は Picnic2.0 版により修正された。更に、最近改良された Katz, Kolesnikov, Wang らによる ZKB++プロトコルに対しても同様のマルチターゲット攻撃を適用できることを示す。

5. Crypto 2019 の発表

5.1. Crypto 2019 の発表(1 日目)

New Results on Modular Inversion Hidden Number Problem and Inversive Congruential Generator [Crypto 2019]

Jun Xu, Santanu Sarkar, Lei Hu, Huaxiong Wang, and Yanbin Pan

Boneh, Halevi, Howgrave-Graham らにより Asiacrypt 2001 で導入されたモジュラー逆元隠れ数問題(MHINP: Modular Inversion Hidden Number Problem)について、本論文では Coppersmith の方法を再検討することにより、ヒューリスティックな多項式時間アルゴリズムを示す。MIHNP を解くための漸近計算量を 18 年振りに初めて更新し、また、逆元合同生成(Inversive Congruential Generator)の最良攻撃を得た。

On the Shortness of Vectors to be found by the Ideal-SVP Quantum Algorithm [Crypto 2019]

Léo Ducas, Maxime Plaçon, and Benjamin Wesolowski

円分体整数環イデアルの最小ベクトル問題(Ideal-SVP)は、ある領域においては一般の SVP よりも速い量子アルゴリズムがあることが知られている。ある仮定の下では、nを次元とした時、因子 $\alpha = \exp(\tilde{O}(n^{1/2}))$ の近似 SVP は量子多項式時間で求められる。本論文では、本漸近式に隠された係数を調べることにより、古典的な格子縮小アルゴリズムとの比較を行う。例えば、ランク 24000 以上の円分体整数環に対しては、BKZ-300 よりも量子アルゴリズムの方がより短いベクトルを求めるであろうことを予想する。

5.2. Crypto 2019 の発表(2 日目)

Efficient Collision Attack Frameworks for RIPEMD-160 [Crypto 2019]

Fukang Liu, Christoph Dobraunig, Florian Mendel, Takanori Isobe, Gaoli Wang, and Zhenfu Cao

兵庫県立大学の五十部らは、CRYPTREC 運用監視暗号リストに掲載されており、ISO/IEC 標準でありBitcoinアドレス生成等に利用されているハッシュ関数RIPEMD-160の縮退版に対する衝突攻撃を行い、30/31 段(80 段中)に対し各々$2^{35.9}/2^{41.5}$の時間計算量で攻撃できることを示した。まだセキュリティマージンは大きく残っているが、これまでの攻撃に比べて約 8000 倍高速となる結果であるため今後の進展に注意が必要である。

Improving Attacks on Round-Reduced Speck32/64 Using Deep Learning [Crypto 2019]

Aron Gohr

ドイツ情報セキュリティ庁の Aron Gohr 氏が、NSA が開発した軽量ブロック暗号 Speck32/64 の縮退版に対する攻撃を深層学習により改良したと発表した。暗号解析における深層学習の有効性の可能性を示す研究として注意が必要である。

Correlation of Quadratic Boolean Functions: Cryptanalysis of All Versions of Full MORUS [Crypto 2019]

Danping Shi, Siwei Sun, Yu Sasaki, Chaoyun Li, and Lei Hu

NTT の佐々木らは、任意の 2 次ブール関数の相関は所謂互いに素な 2 次形式により読み出されることを示した。更に任意の 2 次ブール関数を互いに素な 2 次形式に変換する多項式時間アルゴリズムを提案した。それにより 2 次ブール関数の正確な相関は効率的に計算される。本方法を認証暗号コンペティション CAESAR の最終候補 7 つに残っていた暗号 MORUS 完全版に対して適用し、識別攻撃および鍵回復攻撃を行った。本結果を受けて、MORUS は CAESAR 最終候補から除外された。

Low Memory Attacks against Two-Round Even-Mansour using the 3-XOR Problem [Crypto 2019]

Gaëtan Leurent and Ferdinand Sibleyras

単一鍵 2 ラウンドの Even-Mansour 構成は、基礎置換/暗号化 $2^{2n/3}$ の安全性証明を持ち、最良攻撃の計算量は、大まかに $2^n/n$ である。本論文ではブロックサイズ n の本スキームの攻撃は要素数 l=2n の 3-XOR 問題に関連することを示し、本関係性を用いて新しい攻撃を示す。特に、データ計算量もメモリ計算量も 2^n よりも遥かに小さい初めてのアルゴリズムを得た。あるコンスタント $0<\lambda<1$ に対し、λn の平文/暗号文対、$2^n/\lambda n$ 時間、$2^{\lambda n}$ メモリしか必要としない。更には漸近計算量 $O(2^n(\ln^2 n)n^2)$ のアルゴリズム($O(2^n/n)$を更新)を記述する。

Cryptanalysis of OCB2: Attacks on Authenticity and Confidentiality [Crypto 2019]

Akiko Inoue, Tetsu Iwata, Kazuhiko Minematsu, and Bertram Poettering

NEC の峯松、井上、名古屋大学の岩田らによる認証暗号 OCB2 に対する偽造攻撃が、Asiacrypt 2018 ランプセッションで発表され、OCB2 が ISO/IEC 標準から除外されることとなったことは報告済であるが、Crypto 本会議にて最優秀論文賞を受賞した。

5.3. Crypto 2018 の発表(3 日目)

Statistical Zeroizing Attack: Cryptanalysis of Candidates of BP Obfuscation over GGH15 Multilinear Map [Crypto 2019]

Jung Hee Cheon, Wonhee, Cho, Minki Hhan, Jiseung Kim, and Changmin Lee

本論文では GGH15 多重線型写像に基づいた難読化に対する新しい暗号解析アルゴリズムを提案する。本統計的ゼロ化攻撃は、難読化プログラムの零点の評価を使うことで難読化からの 2 つの分布を直接区別する。本攻撃は CRYPTO 2018 における Chen らの識別不可性難読化候補を最適パラメタ設定で解読する。我々の結果は、代数的安全性証明だけではなく統計的証明を考慮しなくてはならないことを示している。特に、TCC 2018 における Bartusek らのスキームは、代数的安全性証明は成り立つにもかかわらず、あるパラメタ領域において望まれる安全性を達成していないことを示す。

6. FDTC 2019 の発表

Persistent Fault Analysis of OCB, DEOXYS and COLM [FDTC 2019]

Michael Gruber, Matthias Probst, and Michael Tempelmeier

暗号演算前に持続的なフォールトを起こす攻撃である Persistent Fault Analysis (PFA)による攻撃を発表した。PFA は昨年の CHES 2018 において浙江大学の Fan Zhang らが発表した攻撃手法で、S-Box のような暗号演算で使用する定数を改変することによる。このときの攻撃対象は AES128 ビットであった。今回の発表は、AES をベースにした認証暗号である OCB、Deoxys-II、COLM に対して PFA を適用する攻撃についてのものである。攻撃が有効となるためにはアルゴリズムや攻撃戦略によって細かい条件があるが、条件が合えば平均して約 2000 回の暗号化処理又はタグ生成処理を行わせることで攻撃が成功し、PFA がこれらの認証暗号の実装に対する脅威となりうることを示している。

7. CHES 2019 の発表

7.1. CHES 2019 の発表(2 日目)

Return of the Hidden Number Problem. [CHES 2019]

Keegan Ryan

“Hidden Number Problem”を利用した ECDSA 及び DSA に対する攻撃である。署名の計算過程

において、剰余演算を実行するときに、被除数が法 q 以上か未満かで条件分岐を行うような実装では、剰余演算にかかる時間が一定時間ではなくなるため、その時点での被除数が q 未満かどうかがサイドチャネル情報として洩れる。署名を複数回実行させ、その情報を使うことで、秘密鍵を Hidden Number Problem に帰着させて復元を行うことができることを示した。さらに、OpenSSL 等の 20 個のオープンソースの暗号ライブラリを調査し、その約半数にこの攻撃に対する脆弱性があることを示した。

7.2. CHES 2019 の発表(3 日目)

Cache-Timing Attacks on RSA Key Generation [CHES 2019]

Alejandro Cabrera Aldaya, Cesar Pereida García, Luis Manuel Alvarez Tapia, and Billy Bob Brumley

RSA 暗号の鍵生成に対するキャッシュタイミング攻撃についての発表である。近年、タイミングサイドチャネル攻撃の脅威が知られることにより、暗号演算が、パラメタによらず実行時間が一定であるように実装することがセキュリティ要件として必須とされるようになっているが、完全に行うのは容易ではない。OpenSSL では、BN_FLG_CONSTTIME フラグを設定することで実行時間が一定であるようなアルゴリズムを使用する実行パスとなるように実装しているが、この方法は堅牢ではなく、フラグが適切にセットされなかったり、ソフトウェアバグのためにフラグが正しく扱われなかったりする例がここ数年の間にいくつか見つかっている。本論文では、サイドチャネル攻撃に対して安全でない実行パスを横断的に探索し、アルゴリズム上の機密状態を漏えいする可能性のある 3 個の実行パスを特定している。本論文はそのような脆弱性を発見する新たな手法の提案であり、この手法を実際に OpenSSL ライブラリに適用することで、OpenSSL ライブラリにおける RSA 鍵生成時のキャッシュタイミング攻撃に対する新たな脆弱性を発見している。10,000 回の試行に対して統計的に約 27%の成功率という結果が得られている。なお、この脆弱性は CVE-2018-0737 として脆弱性情報に登録されており、最新版の OpenSSL では対策されている。

8. Asiacrypt 2019 の発表

8.1. Asiacrypt 2019 の発表(1 日目)

A Novel CCA Attack Using Decryption Errors Against LAC [Asiacrypt 2019]

Qian Guo, Thomas Johansson, and Jing Yang

復号誤り可能性を持ち、誤り訂正符号を利用する暗号スキームに対する秘密鍵回復攻撃の提示および議論を行った。特に NIST 耐量子計算機計算機暗号標準化において第 2 ラウンドへ進んだ LAC に対する攻撃を示す。LAC256 に関しては、事前計算コスト 2^{162} を除けば、2^{79} の計算量で、約 2^{64} 個の公開鍵の内 1 つを回復することができた。LAC256-v2 の場合は、事前計算は 2^{162} から

2^{171} に増える。

Quantum Algorithms for the Approximate k-List Problem and their Application to Lattice Sieving [Asiacrypt 2019]

Elena Kirshanova, Erik Mårtensson, Eamonn W. Postlethwaite, and Subhayan Roy Moulik

最短ベクトル問題(SVP: Shortest Vector Problem)は格子暗号の数学的基礎の一つであり、格子篩アルゴリズムはSVPを解く最も良い方法の一つである。d次元SVPを解く最良の既知古典／量子篩の漸近計算量は、ある定数 c,c’ に対し $2^{cd+o(d)}$ 時間と $2^{c'd+o(d)}$ メモリを必要とする。本論文では、計算ステップとメモリとをトレードする様々な量子篩アルゴリズムを与える。

Quantum Attacks without Superposition Queries: the Offline Simon's Algorithm [Asiacrypt 2019]

Xavier Bonnetain, Akinori Hosoyamada, María Naya-Plasencia, Yu Sasaki, and André Schrottenloher

本論文では、Simon のサブルーチンを新しい方法で利用する量子アルゴリズムを導入する。即ち、古典クエリとオフライン量子計算に制限された量子攻撃者の文脈において暗号システムの代数的構造を利用することを考える。Grover のアルゴリズムによる標準的な全数探索と同等な(量子／古典)ハードウェア要件しか使わないにもかかわらず、既存結果よりも良い量子時間／古典データのトレードオフを得た。特に、Even-Mansour 構成を $\tilde{O}(2^{n/3})$ 量子時間、$O(2^{n/3})$ 古典クエリ、$O(n^2)$ 量子ビットで解読することができる。更に、既知の量子重ね合わせ攻撃を、同じ時間計算量でデータ計算量を指数から多項式に削減する。他に FX 構成や暗号のスポンジ認証モード等への適用も与える。

8.2. Asiacrypt 2019 の発表(2 日目)

An LLL Algorithm for Module Lattices [Asiacrypt 2019]

Changmin Lee, Alice Pellet-Mary, Damien Stehlé, and Alexandre Wallet

任意の数体 K に対してその整数環を R としたとき、K^n に含まれる R 加群において、LLL アルゴリズムの拡張を与える。階数 2 の加群における短いベクトルを見つけるオラクルへのアクセスが与えられたとき、階数 n の加群における短いベクトルを効率的に見つけるアルゴリズム、および K のみに依存する格子の CVP オラクルへのアクセスが与えられたとき、階数 2 の加群の短いベクトルを効率的に見つけるアルゴリズムを与える。2 番目のアルゴリズムは、量子計算に依存し、分析はヒューリスティックである。

Cryptanalysis of CLT13 Multilinear Maps with Independent Slots [Asiacrypt 2019]

Jean-Sébastien Coron and Luca Notarnicola

CRYPTO2014 において、多重線型写像 CLT13 に対し Gentry らによる次元 2 の格子ベース攻撃で脆弱性が指摘され、著者らにより単純な対策が示された。本論文ではより高次元の格子縮約に基づいた攻撃により、幅広い領域のパラメタに対し、その対策を破ることができることを示す。Eurocrypt 2015 の Cheon らの攻撃と組み合わせることにより、ほとんど 0 の平文の低レベルエンコードを仮定すると CLT13 の全ての秘密パラメタを回復することができる。本攻撃を合成数位数の CLT13 に基づく様々な構成に適用することができる。しかしながら、分岐プログラムの識別不可能性を破れるかどうかは未解決である。

8.3. Asiacrypt 2019 の発表(4 日目)

The Exchange Attack: How to Distinguish Six Rounds of AES with $2^{88.2}$ Chosen Plaintexts [Asiacrypt 2019]

Navid Ghaedi Bardeh and Sondre Rønjom

CRYPTREC 暗号リストに掲載されている米国標準暗号 AES に対する識別可能性に関する解析論文で、SPN 構造のブロック暗号に適した新しい攻撃手法(exchange-equivalence attacks)を提案した。本発表では、exchange-invariant と呼ぶ特性(直感的にはあるルールで決められた場所の値が交換された平文組の集合)を満たす $2^{88.2}$ の選択平文と $2^{88.2}$ の暗号化によって 6-round AES 秘密鍵識別器(Secret-key distinguishers)を始めて構成し、それら exchange-invariant な集合を利用すると少なくとも AES の 6 段目では偏りがあることを示した。また 2^{30} の選択平文と 2^{30} の暗号化に改善した 5-round AES 秘密鍵識別器を構成し、スケールダウンしたバージョンでの実機検証を行った。

この攻撃手法は、任意の SPN 構造のブロック暗号に拡張可能であり、特に軽量暗号のような拡散が小さい設計方針の暗号に対してより強力に適用できる。

Algebraic Cryptanalysis of STARK-Friendly Designs: Application to MARVELlous and MiMC [Asiacrypt 2019]

Martin R. Albrecht, Carlos Cid, Lorenzo Grassi, Dmitry Khovratovich, Reinhard Lüftenegger, Christian Rechberger, and Markus Schofnegger

耐量子計算機ゼロ知識証明システム(例:ZK-STARK)に適したアルゴリズムとして提案されたブロック暗号 Jarvis とハッシュ関数 Friday－これらは MARVELlous family と呼ばれる暗号プリミティブを使っている―に対する代数攻撃に関する解析論文である。本発表では、グレブナー基底での代数攻撃に対してフルラウンドの Jarvis と Friday が安全ではないことを示した。

MILP-aided Method of Searching Division Property Using Three Subsets and Applications [Asiacrypt 2019]

Senpeng Wang, Bin Hu, Jie Guan, Kai Zhang, and Tairong Shi

FSE2016 で藤堂・森井が提案した Division property には CBDP (conventional bit-based division property)と BDPT (bit-based division property using three subsets)がある。Asiacrypt2016 で Xiang らは integral 識別器を探索するために CBDP をベースとした MILP (Mixed Integer Linear Programming)法を提案した。一方、BDPT は CBDP よりも正確な integral 識別器が得られるものの効率的なモデリングが出来ていなかった。本発表では、BDPT をベースとした integral 識別器の探索を目的に、BDPT の拡散に着目した MILP-aided 法を提案した。これを SIMON64, PRESENT, RECTANGLE に適用し、従来以上の成果を得ることができた。

また、BDPT ベースの Cube 攻撃法を提案し、Trivium に適用した。その結果、Crypto2018 での 839 段 Trivium の攻撃が practical になり、841 段までの theoretical attack を示した。

Cryptanalysis of GSM Encryption in 2G/3G Networks Without Rainbow Tables [Asiacrypt 2019]

Bin Zhang

第 2 世代／第 3 世代携帯電話での暗号化方式 GSM に使われている A5/1 に対する解読結果の報告である。GSM に対する解読手法そのものはすでに多く発表されており、それ自体に大きな意味があるわけではないが、従来の解読手法は膨大な事前計算を行い巨大な Rainbow Table を作る必要があった。これに対して、本発表では Eurocrypt 2018 で提案した Rainbow Table を作らない事前計算やメモリを大幅に削減した解読手法(near collision attack)を適用して、実際に A5/1 の解読したところ、鍵ストリームフレームの最初の 64 ビットが利用でき、約 1MB のメモリと 220.26 cipher ticks の事前計算があれば、秘密鍵が 231.79 cipher ticks (1 cipher ticks は約 100 CPU cycle)で見つけることができた。

CRYPTREC Report 2019
(暗号技術評価委員会報告 CRYPTREC RP-2000-2019R1)

発行日　2020年 7月 31日　第1版
　　2020年 10月 30日　第2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