CRYPTREC Report 2018

平成 31 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-2000-2018

「暗号技術評価委員会報告」

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 2018 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 2018 年度の活動として、

1)暗号技術の安全性及び実装に係る監視及び評価

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

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。

1) では、公開鍵暗号 RSA や楕円曲線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」、「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」の更新を行うために、T.Kleinjung 氏および A.K.Lenstra 氏に計算量評価の主要部の評価を依頼し、素因数分解の困難性に関する計算量の再評価を実施した。

2) では、ディスク暗号化で利用が進んでいる暗号利用モード(秘匿モード) XTS の安全性評価を行うために、峯松一彦 氏に安全性評価を依頼し、その評価結果から、XTS モードは利用条件を満たす範囲においては、十分な安全性を有すると判断した。

3) 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、昨年度から継続して検討してきた Post-Quantum Cryptography(耐量子計算機暗号)の研究動向調査報告書を完成させ、CRYPTREC ホームページにて公開した。併せて、素因数分解問題の困難性および楕円曲線上の離散対数問題の困難性に関する計算量評価の更新について検討を行った。 例年、これら計算量評価に対して、解読の脅威の尺度を、スーパーコンピュータの性能の伸びを用いて、グラフ化していた。しかし、近年のスーパーコンピュータの性能の伸びの鈍化、解読の要因となる脅威の多様化(多種デバイスや多種アーキテクチャが解読に利用できる可能性が出てきている)が進みつつあることから、従来手法に基づく予測と実際とに乖離が生じ始めている。これらをどのように表現していくかについて、次年度継続検討を行うこととした。

CRYPTREC は、客観的な評価による安全性及び実装性に優れると判断された暗号技術をリスト化する暗号技術評価プロジェクトとして 2000 年に発足して以来、19 年にわたりその活動は、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。暗号技術に対する顕在化した、あるいは顕在化していない社会のニーズは近年より一層大きくなっている。そこに応えうる CRYPTREC の活動の重要性はより高まっていると考えている。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是非、続けて頂きたい。

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　　太田 和夫

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。

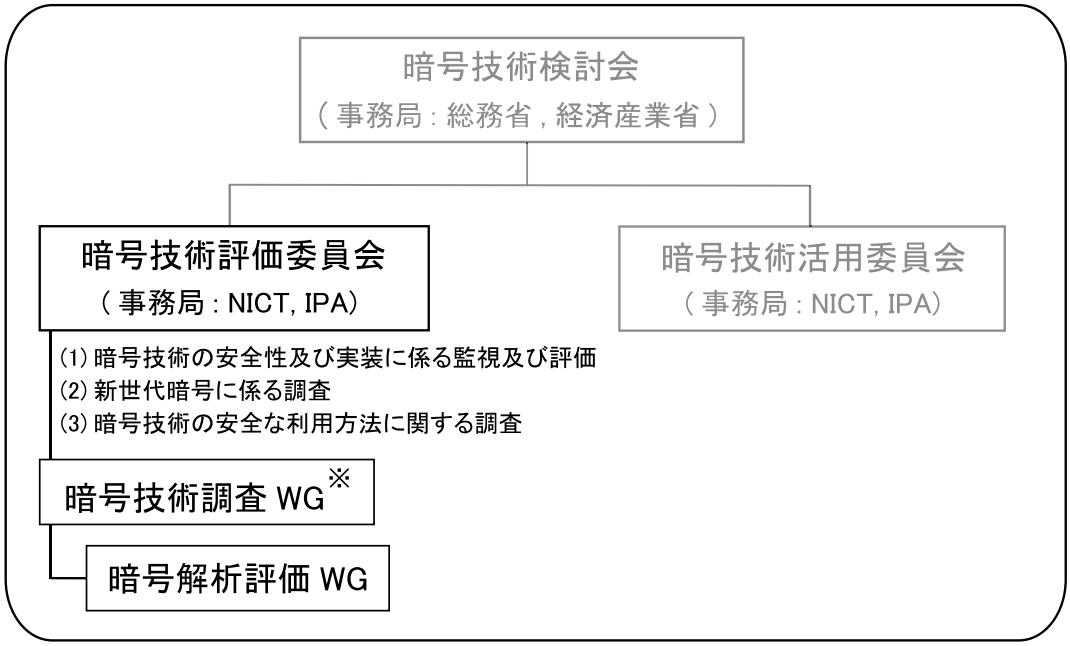
【問合せ先】　info@cryptrec.go.jp

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もと、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。2018 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	太田 和夫	電気通信大学 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	金子 敏信	東京理科大学 教授
委員	高木 剛	東京大学 教授
委員	手塚 悟	慶應義塾大学 特任教授
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 ディビジョンマネージャー
委員	盛合 志帆	国立研究開発法人情報通信研究機構 研究室長
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	高木 剛	東京大学 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 研究主任
委員	國廣 昇	東京大学 准教授
委員	下山 武司	株式会社富士通研究所 主管研究員
委員	高島 克幸	三菱電機株式会社 主管技師長
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

内田 稔	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
高木 浩光	内閣官房内閣サイバーセキュリティセンター
徳永 竜一	内閣官房内閣サイバーセキュリティセンター
岡田 崇志	個人情報保護委員会事務局
中嶋 昌幸	警察庁 情報通信局
小高 久義	総務省 行政管理局
三輪 亮介	総務省 自治行政局 住民制度課
上東 孝旭	総務省 情報流通行政局[2018 年 7 月まで]
守屋 潤一	総務省 情報流通行政局[2018 年 7 月まで]
豊重 巨之	総務省 情報流通行政局
吉永 勇輝	総務省 情報流通行政局
遠藤 琢	総務省 情報流通行政局
本原 拓也	外務省 大臣官房[2018 年 6 月まで]
荒木 美敬	外務省 大臣官房[2018 年 6 月から]
三島 崇	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
飯山 貴啓	経済産業省 商務情報政策局
今泉 隆文	防衛省 整備計画局
山口 義隆	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（宮崎哲弥、盛合志帆、大久保美也子、篠原直行、黒川貴司、金森祥子、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（江口純一[2018年7月まで]、瓜生和久[2018年7月から]、時田俊雄、小暮淳、神田雅透、橋本徹、兼城麻子[2018年10月まで]、菅野淳[2018年11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・ソフトウェアかが市場に提供されているかが、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。そして、2017 年度は、米国 NIST が Special Publication 800-67 を Revision 2(DRAFT)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が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。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」[2]を Web に掲載した。また、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」[3]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 17 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] https://www.cryptrec.go.jp/list/cryptrec-ls-0001-2012r4.pdf
[2] https://www.cryptrec.go.jp/topics/cryptrec-er-0001-2016.html
[3] https://www.cryptrec.go.jp/topics/cryptrec-er-0001-2017.html

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[4]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)」[5](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

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

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[6]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、すなわち、

(a) 暗号技術の安全性及び実装に係る監視及び評価
(b) 新世代暗号に係る調査(軽量暗号、セキュリティパラメータ、ペアリング暗号、耐量子計算機暗号技術等)
(c) 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。

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[7]掲載の暗号技術に対する考え方[8]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。

---

[6] https://www.cryptrec.go.jp/topics/cryptrec_201212_listpc.html
[7] 2003 年 2 月 20 日に策定されたものを指す。
[8] 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

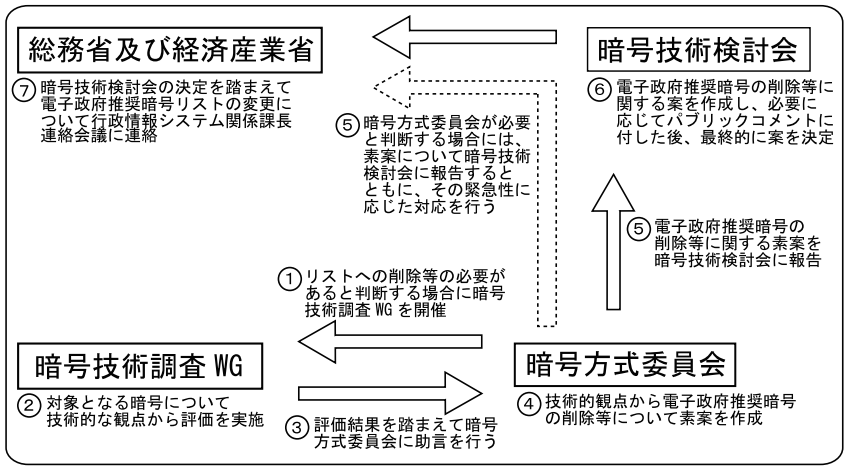


図1.1: 電子政府推奨暗号の削除等の手順[9]

(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。
(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

[9] 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。

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。

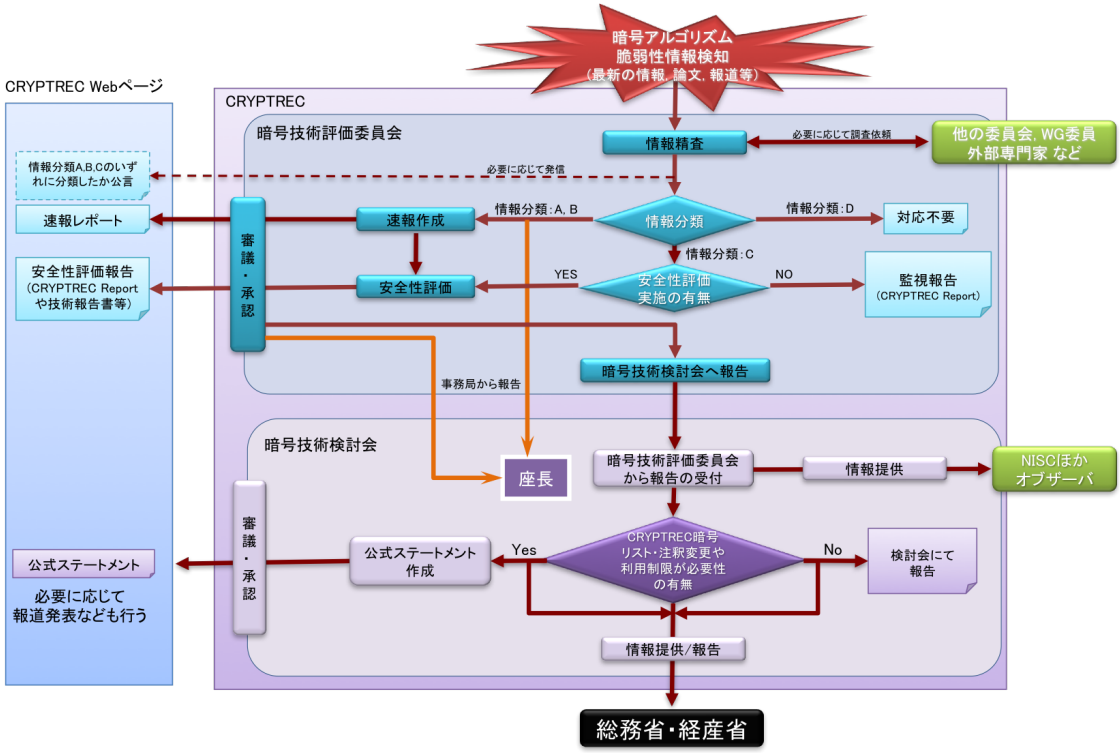


図1.2 暗号アルゴリズムの脆弱性に関する情報発信フロー

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 2018 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

CRYPTREC 暗号リスト掲載の共通鍵暗号については、CRYPTO 2018 においてイスラエル・バル＝イラン大学の Achiya Bar-on らが、AES の縮退版(10 段中 5 段)に対して、データ/メモリ/時間計算量が $2^{22.5}$(従来の 2^{32} よりも約 500 倍高速)で鍵回復攻撃できることを示し、実験により実証も行った。更に 7 段 AES に拡張することにより、18 年振りに AES-192 に対する攻撃記録を破った。縮退版であるため、まだ安全性にはマージンがあるが、今後の攻撃の進展には注意が必要である。CHES 2018 および FDTC 2018 において、故障利用攻撃により AES の鍵回復実験にしたという報告がなされており、これらの攻撃の前提がどの程度現実的であるかの評価も含め注意が必要である。また、Eurocrypt 2018 において、フランス国立情報学自動制御研究所の Leurent、Aivleyras らにより、暗号利用モード CTR、メッセージ認証コード Poly1305 への攻撃と安全性解析が発表され、その影響及び今後の研究の進展には注意が必要である。認証付き秘匿モード GCM に関しては、CRYPTO 2018 において Leurent らによる GCM-SIV2 に対する攻撃が発表された。

CRYPTO 2018 において NTT の藤堂、青木、兵庫県立大学の五十部らは、LFSR ベースのストリーム暗号に対する高速相関攻撃(FCA: Fast Correlation Attack)を有限体の視点から見ることにより新しい性質およびそれに基づくアルゴリズムにより時間／空間計算量を削減した。この手法を Grain ファミリー(Grain-128a、Grain-128、Grain-v1)に適用することによりすべて解読した。Grain-v1 は eSTREAM のポートフォリオに掲載されており、Grain-128a は ISO/IEC において標準化されており、Grain-128a の完全版に対する暗号解析は初めてである。Grain ファミリーへの攻撃としては、Eurocrypt 2018 での Zhang らの Grain v1 への攻撃、CRYPTO 2018 での藤堂、五十部らによる Grain-128a への攻撃もある。eSTREAM のポートフォリオに掲載されたストリーム暗号 Trivium に対する攻撃としては、Eurocrypt 2018 の Liu らによる攻撃、CRYPTO 2018 での藤堂、五十部らによる攻撃、CRYPTO 2018 での Fu らによる攻撃が発表された。

認証暗号 Caesar コンペティションに関する暗号攻撃としては、Eurocrypt 2018 での NTT の佐々木らによる Deoxys-BC への攻撃、ASIACRYPT 2018 での佐々木らによる MORUS への攻撃が発表された。

ASIACRYPT 2018 のランプセッションにおいて、NEC の井上、峯松は、ISO/IEC 標準の認証暗号 OCB2 の偽造攻撃を発表した。本攻撃を受け、ISO/IEC では標準の見直しを開始している。

2.1.2. 公開鍵暗号に関する安全性評価について

NIST による耐量子計算機暗号の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。既存の実用的公開鍵暗号の安全性の根拠とする数学的問題に関しては、楕円曲線離散対数問題(ECDLP: Elliptic Curve Discrete Logarithm Problem)に対する解読法の新たな可能性に関する発表があった(論文は未出版)。CRYPTO 2018 関連イベントの一つである「数学暗号ワークショップ」において、南カリフォルニア大学の Ming-Deh Huang 教授らが、ある条件を満たす楕円曲線に対し、全数探索よりも小さい計算量で指数計算法を用いて ECDLP を解くことができると発表した。現実的には非効率的な計算量ではあるが、条件付きで指数計算法を用いた解読法の可能性を示したため、今後の進展に注意が必要である。

2.1.3. その他の注視すべき技術動向

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）の標準化が本格的に開始され、2017 年 11 月 30 日に暗号公募が締め切られた時点では、25 ヶ国 6 大陸から応募があり、応募総数は 82 件と発表されたが、仕様の精査を経て第 1 ラウンドの対象は計 69 件となった。

2018 年 4 月 9 日～13 日に米国フロリダ州フォートローダーデールにて国際会議 PQCrypto 2018 および第 1 回 NIST PQC 標準化会議が開催されたが、更に 5 件の取り下げを経て、その時点での対象暗号は 64 件となった。その内訳件数を表 2.1 に示す。

表 2.1: NIST PQC 標準化応募暗号(第 1 ラウンド、取り下げ分を除く)

	電子署名	鍵カプセル化機構／暗号化	合計
格子ベース	5	21	26
符号ベース	2	17	19
多変数多項式	7	2	9
ハッシュベース	3	0	3
その他	2	5	7
合計	19	45	64

CRYPTO 2018 関連イベントの一つである「暗号における攻撃ワークショップ」において、Bernstein、Lange らによる NIST コンペティション候補暗号に対する攻撃状況に関する報告があり、その時点において第 1 ラウンド 69 暗号の内、完全解読は 13 件、部分解読は 8 件、無傷で残っているものは 48 件とのことであった。内訳は以下の表 2.2 の通りである。

表 2.2: 第 1 ラウンド暗号解読状況(Bernstein/Lange による、CRYPTO 2018 時点)

	応募数	完全解読数	部分解読数
符号ベース暗号	17	1	6
格子ベース暗号	20	1	1
その他暗号	11	6	0
署名	21	5	1

2018 年 12 月 22 日以降、約 1 か月にわたり米国政府機関閉鎖の影響で発表が遅れたが、再開後の 2019 年 1 月 30 日に、第 2 ラウンドへ進む 26 件が発表された。その内訳件数を下表 2.3 に示す。

表 2.3: NIST PQC 標準化候補暗号(第 2 ラウンド)

	電子署名	鍵カプセル化機構／暗号化	合計
格子ベース	3	8	11
符号ベース	0	7	7
多変数	4	0	4
ハッシュベース	2	0	2
その他	0	2	2
合計	9	17	26

具体的な暗号名は、以下のように分類される。

●公開鍵暗号／鍵カプセル化機構アルゴリズム

－格子ベース：CRYSTALS-KYBER、FrodoKEM、LAC、NewHope、NTRU、NTRU Prime、Round5、SABER

－符号ベース：BIKE、Classic McEliece、HQC、LEDAcrypt、NTS-KEM、ROLLO、RQC

－その他：SIKE(同種写像ベース)、Three Bears(整数環ベース)

●電子署名アルゴリズム

－格子ベース：CRYSTALS-DILITHIUM、FALCON、qTESLA

－多変数：GeMSS、LUOV、MQDSS、Rainbow

－ハッシュベース：Picnic、SPHINCS+

今後は 2019 年 8 月に第 2 回 NIST PQC 標準化会議が開催され、2020 年～2021 年に最終アルゴリズムを選択するか第 3 ラウンドへ進み、2022 年～2024 年に標準ドラフトを公開する予定となっている。

2.2. 注意喚起レポートについて

2018 年度に公表した注意喚起レポートはなかった。

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. 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（秘匿モード)の一つである XTS モードは、2007 年にストレージデバイス上のデータの暗号化の規格として IEEE Standard 1619-2007 で標準化され、NIST でも、2010 年に NIST SP 800-38E として規定された。大きな市場を持つ製品に搭載されるなどの実績があり、例えば、Microsoft Windows 搭載の BitLocker や macOS 搭載の FileVault 等のディスク暗号化機能に XTS モードが使われている。

暗号利用モードは、2012 年度の CRYPTREC 暗号リスト改定に合わせて、2009 年度に事務局選出の暗号技術候補として複数の暗号利用モードを NIST SP 800-38 シリーズから選出して、安全性評価・実装性能評価を実施し、6 つの暗号利用モード(CBC, CFB, CTR, OFB, CCM, GCM)を CRYPTREC 暗号リストに追加した。

XTS モードは、2009 年当時 NIST SP 800-38 シリーズにおいて規定されていない技術であったため、評価対象外であったが、昨今、情報漏えい対策として OS 搭載のディスク暗号化機能が一般的に利用されていることから、2018 年度外部評価として、安全性評価を行うこととした。

＜外部評価者による安全性評価結果の概要＞

○ ストレージ暗号化の用途に対して、IEEE や NIST SP 800-38E の仕様書に沿って使う場合、安全性は保たれる。
- ✓ 他の利用用途では、攻撃が可能な場合もある。
- ✓ 保証する安全性に本質的な限界がある。
- ✓ CBC モードなどで暗号化するよりも高い安全性を有している。

○ (新規の結果)ストレージ暗号化の用途に対して、1 ラウンドの Even-Mansour 暗号の鍵回復攻撃を応用・適用し平文回復攻撃が可能であることが示された。攻撃に必要なデータ量は、XTS-AES の場合で 2^{64} ブロック以上となり、攻撃に必要となるデータ量が大量であるため、すぐさま現実的な脅威にはなりにくい。
- ✓ AES-128 及び AES-256 を適用して XTS モードを用いる場合については、学術的にも現実的にも攻撃は見つかっておらず、高い安全性を有すると考えられる。
- ✓ 64 ビットブロック暗号を用いる場合は 2^{32} ブロックとなり現実的な脅威となりうる。

○ 鍵を変えずに処理するデータ量は、IEEE で規定されている上限値 2^{20} ブロックの範囲で使用すべきである。
- ✓ IEEE で標準化されたのち、NIST が SP-800-38E に採用するまでに IEEE の仕様の妥当性が検討され、鍵を変えずに処理するデータ量の上限値を制限することが妥当であるとの見解が出ている。この制限は、XTS モードとして同一の鍵を用いて処理した場合の暗号文の取りうる値に上限があるため、暗号文が識別可能となり、例えば、

2 つの暗号文が同一のメッセージを暗号化したものであるか否かを判別されてしまうことを避けるためである。

この評価結果から、暗号技術評価委員会としては、下記 3 点の条件①～③のもと、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と判断し、次年度以降に実装性能評価を行い、その結果を踏まえた上で、CRYPTREC 暗号リストへの追加を検討することとなった。

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。
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。
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。

2.4. 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2.4に示す通りである。

表 2.4: 国際会議への参加状況

学会名・会議名		開催国・都市	期間
PQC2018	The Ninth International Conference on Post-Quantum Cryptography	米国・フォートローダーデール	2018 年 4 月 9 日～2018 年 4 月 11 日
First PQC Standardization Conference	First PQC Standardization Conference	米国・フォートローダーデール	2018 年 4 月 11 日～2018 年 4 月 13 日
Eurocrypt 2018	the 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques	イスラエル・テルアビブ	2018 年 4 月 30 日～2018 年 5 月 3 日
CRYPTO 2018	International Cryptology Conference	米国・サンラバーバラ	2018 年 8 月 20 日～2018 年 8 月 23 日
CHES 2018	Conference on Cryptographic Hardware and Embedded Systems	オランダ・アムステルダム	2018 年 9 月 9 日～2018 年 9 月 12 日
FDTC 2018	Fault Tolerance and Diagnosis in Cryptography	オランダ・アムステルダム	2018 年 9 月 13 日
ECC 2018	Workshop on Elliptic Curve Cryptography	日本・大阪	2018 年 11 月 19 日～2018 年 11 月 21 日
Asiacrypt 2018	Annual International Conference on the Theory and Application of Cryptology and Information Security	オーストラリア・ブリスベン	2018 年 12 月 3 日～2018 年 12 月 6 日

以下に、国際学会等に発表された論文を中心に、暗号解読技術の最新動向を示す。詳しくは、付録 4 を参照のこと。

2.4.1. 共通鍵暗号の解読技術

・The Missing Difference Problem, and Its Applications to Counter Mode Encryption [Eurocrypt 2018]

Gaetan Leurent and Ferdinand Aivleyras

「Missing Difference 問題」を定義し、この問題とブロック暗号のカウンターモード(CTR)の関係を示した。また、任意の「Missing Difference」の場合と、「Missing Difference が低次元のベクトル空間内にあることが判っている場合において、問題を効率的に解くアルゴリズムを示した。これらのアルゴリズムによってカウンターモード（CTR）へのメッセージ回復攻撃がオーダー： Õ（$2^{n/2}$）であること、GMAC や Poly1305 の普遍的偽造攻撃がオーダー：Õ（$2^{2n/3}$）であることが示された。尚、カウンターモード（CTR）は電子政府推奨暗号リストの秘匿モードとして掲載されており、Poly1305 は、推奨候補暗号リストの認証暗号として掲載されている「ChaCha20－Poly1305」の認証機能に相当している。

・Generic Attacks against Beyond-Birthday-Bound MACs [Crypto 2018]

Gaëtan Leurent, Mridul Nandi, and Ferdinand Sibleyras

いくつかの最近のバースデー限界を超える証明可能安全性を持った MAC 構成の安全性において、SUM-ECBC、PMAC+、3kf9、GCM-SIV2 とその変種(LigheMAC+、1kPMAC+)のようなダブルブロック内部状態を持つブロック暗号ベースの構成を考える。これらすべての MAC は $2^{2n/3}$ クエリまでのセキュリティが証明されているが、2^n クエリ未満での攻撃は知られていない。

SUM-ECBC 及び GCM-SIV2 に対する、時間及びデータ計算量が $O\tilde{}(2^{6n/7})$ である攻撃のバリアントを提示する。これは知る限りにおいて計算量が 2^n 未満である決定的なバースデー限界を超えるセキュア MAC に対する最初の攻撃である。

・Improved Key Recovery Attacks on Reduced-Round AES with Practical Data and Memory Complexities [CRYPTO 2018]

Achiya Bar-On, Orr Dunkelman, Nathan Keller, Eyal Ronen, and Adi Shamir

イスラエル・バル＝イラン大学の Achiya Bar-on らが AES の縮退版(10 段中 5 段)に対して、データ/メモリ/時間計算量が $2^{22.5}$(従来の 2^{32} よりも約 500 倍高速)で鍵回復攻撃できることを示し、実験により実証も行った。更に 7 段 AES に拡張することにより、18 年振りに AES-192 に対する攻撃記録を破った。縮退版であるため、まだ安全性にはマージンがあるが、今後の攻撃の進展には注意が必要である。

・Programming the Demirci-Selçuk Meet-in-the-Middle Attack with Constraints [Asiacrypt 2018]

Danping Shi, Siwei Sun, Patrick Derbez, Yosuke Todo, and Bing Sun Lei Hu

中国科学院の Shi、NTT の藤堂らによる制約プログラム （以下 CP: Constraind Programing)ベースの暗号解析改良が発表された。CP ベースのアプローチは既存の SAT (SATisfiability Problem) ソルバー等を利用し暗号解析を自動化するものであるが、一方で国際会議 FSE2008 において発表された Demirci と Selçuk らの手法は、自動化ではなく専用探索アルゴリズムにより縮退版 AES に対する解読記録を達成した。今回の Shi らの手法は、新しいモデリングにより自動化で解ける範囲を広げるものであり、SKINNY、TWINE、LBlock 等の軽量暗号に適用され、各々解読記録を更新したが、AES への適用では自動化されていない専用部分が残っているため記録達成には至っていない。

・FPGAhammer: Remote Voltage Fault Attacks on Shared FPGAs, suitable for DFA on AES. [CHES 2018]

Jonas Krautter, Dennis R. E. Gnad, and Mehdi B. Tahoori

1 個の FPGA での利用できるリソースの増大により、FPGA に複数のユーザのロジックが同居する使い方をするケースが見られるようになってきている。このような状況において、FPGA 内に暗号実装があるときに、同じ FPGA 上にリングオシレータを配置してそれを動作させることで FPGA 全体に影響する電圧降下を引き起こし、暗号実装に誤動作を起こさせる攻撃が提案されている。この攻撃で実際に AES 実装を攻撃し、鍵を復元することに成功している。

・Persistent Fault Analysis on Block Ciphers [CHES 2018]

Fan Zhang, Xiaoxuan Lou, Xinjie Zhao, Shivam Bhasin, Wei He, Ruyi Ding, Samiya Qureshi1, and Kui Ren

通常の故障利用攻撃はレーザ等によって一瞬だけ誤動作を引き起こすことによって攻撃するが、攻撃を成功させるためのタイミングが厳しく、また冗長性による対策によって防がれやすい。本論文では持続的なフォールトを起こすことによる攻撃を提案している。S-Box をテーブル参照で実装しているような AES の実装に対し、暗号演算実行前に S-Box テーブルの値を改変し、その改変が 1 回の暗号演算の間持続するようにすることで誤動作を起こさせ、それによって出力された暗号文を解析することで鍵を復元することに成功している。暗号化を 2 回行って比較するような対策に対しても、暗号演算で使用する S-Box の参照テーブルを共有していればこの攻撃は成功する。また、繰り返し DRAM にアクセスすることで隣接する行のメモリを化けさせる Rowhammer の手法が持続的フォールトを引き起こすために使えることも言及している。

2.4.2. 公開鍵関数の解読技術

・Quasi-subfield Polynomials and the Elliptic Curve Discrete Logarithm Problem [CRYPTO 2018 affiliated event MathCrypt]

Ming-Deh A. Huang, Michiel Kosters, Christophe Petit, Sze Ling Yeo, and Yang Yun

MathCrypt2018 において、南カリフォルニア大学の Ming-Deh Huang 教授らが、ある条件を満たす楕円曲線に対し、全数探索よりも小さい計算量で指数計算法を用いて楕円曲線離散対数問題を解くことができることを示した。現実的には非効率的な計算量ではあるが、指数計算法を用いた解読としては進歩が見られたため、今後の進展に注意が必要である。

・Dissection-BKW [CRYPTO 2018]

Andre Esser, Felix Heuer, Robert Kübler, Alexander May, and Christian Sohler

Blum、Kala、Wasserman による準指数時間アルゴリズム BKW は、LPN/LWE セキュリティ評価の基礎となるものであるが、メモリ消費が巨大であるため実用性が限られ、暗号用途での正確な安全性評価が困難であった。本論文では、CRYPTO 2012 における Dinur らの「分解(dissection)」テクニックとその一般化を用い、BKW アルゴリズムの時間－空間トレードオフを初めて与えた。例えば、次元 k の LPN を時間計算量 $2^{4k/3\log k}$、空間計算量 $2^{2k/3\log k}$ で解く方法を示す。メモリ消費削減により BKW の量子版である QBKW を初めて提示した。

・Lower Bounds on Lattice Enumeration with Extreme Pruning [CRYPTO 2018]

Yoshinori Aono, Phong Q. Nguyen, Takenobu Seito, and Junji Shikata

Eurocrypt 2010 において Gama らが導入したエクストリーム枝刈りを用いた数え上げ手法は格子縮小アルゴリズムにおいて用いられ記録チャレンジにおいて利用されているが、その効率性の限界については知られておらず、格子ベース暗号の長期セキュリティを見積もる上で課題となっていた。本論文では、成功確率の下限が与えられたときの同手法の下限計算量を初めて与えた。

2.4.3. その他の暗号技術の解読技術

・New MILP Modeling: Improved Conditional Cube Attacks on Keccak-based Constructions [Asiacrypt 2018]

Ling Song, Jian Guo, Danping Shi, and San Ling

シンガポール南洋理工大学/中国科学院の Song らにより、新しい MILP(Mixed Integer Linear Programming)モデル化による、Keccak(SHA-3)ベース認証等に対するキューブ攻撃の改良が発表された。SHA-3 から構成されたメッセージ認証コードである KMAC (NIST SP 800-135 で規定される)に適用し、7 段 KMAC128 および 9 段 KMAC256 への攻撃に成功した。段数のセキュリティマージンは十分に残っており、まだ実用的な脅威とはなっていないが、今後の攻撃の進展には注意が必要である。

・Fast Correlation Attack Revisited - Cryptanalysis on Full Grain-128a, Grain-128, and Grain-v1 [CRYPTO 2018]

Yosuke Todo, Takanori Isobe, Willi Meier, Kazumaro Aoki, and Bin Zhang

NTT の藤堂らは、LFSR ベースのストリーム暗号に対する高速相関攻撃(FCA: Fast Correlation Attack)を有限体の視点から見ることにより新しい性質およびそれに基づくアルゴリズムにより時間／空間計算量を削減した。この手法を Grain ファミリー(Grain-128a、Grain-128、Grain-v1)に適用することによりすべて解読した。Grain-v1 は eSTREAM のポートフォリオに掲載されており、Grain-128a は ISO/IEC において標準化されており、Grain-128a の完全版に対する暗号解析は初めてである。

・Correlation Cube Attacks: From Weak-Key Distinguisher to Key Recovery [Eurocrypt 2018]

Meicheng Liu, Jingchun Yang, Wenhao Wang, and Dongdai Lin

ストリーム暗号への Cube 攻撃の拡張として Correlation Cube 攻撃を提案した上で、軽量ストリーム暗号「Trivium」へ適用した結果を示している。「Trivium」は欧州の eSTREAM プロジェクトにおいて portfolio に掲載された鍵長：80 ビット（IV 長：80 ビット）のストリーム暗号で、CRYPTREC が 2017 年度に発行した『CRYPTREC 暗号技術ガイドライン（軽量暗号)』でも評価対象となっている。結果として、Correlation Cube 攻撃によって初期化段数がフル仕様で 1152 段の「Trivium」を 805 段/835 段に縮退した版に対して、全数攻撃よりも少ない時間（計算量）で攻撃が可能であることを示した。具体的には、805 段の場合は、$2^{47}/2^{51}$ の事前計算、2^{37}／2^{44} のデータによって、2^{77}／2^{73} の時間（計算量）で鍵回復攻撃が可能であること、835 段の場合は 2^{51} の事前計算、2^{44} のデータによって、2^{75} の時間（計算量）で鍵回復攻撃が可能であること、が各々示された。

・Fast Near Collision Attack on the Grain v1 Stream Cipher [Eurocrypt 2018]

Bin Zhang, Chao Xu, and Willi Meier

ストリーム暗号への汎用的な攻撃として FNCA（Fast Near Collision attack）を提案した上で、軽量ストリーム暗号「Grain v1」へ適用し、計算機による実証実験も行っている。「Grain v1」は欧州の eSTREAM プロジェクトにおいて portfolio に掲載された鍵長：80/128 ビット（IV 長：64/80 ビット）のストリーム暗号で、CRYPTREC が 2017 年度に発行した『CRYPTREC 暗号技術ガイドライン（軽量暗号)』でも評価対象となっている。結果として、FNCA によって鍵長 80 ビットの「Grain v1」に対してこれまで知られているどの攻撃結果よりも時間（計算量）の面で最も効率のよい攻撃が可能であり、具体的には、$2^{8.1}$ の事前計算／2^{19} のデータ／2^{28} のメモリによって、$2^{75.7}$ の時間（計算量）で鍵回復攻撃が可能であることが示された。

・A Key-recovery Attack on 855-round Trivium [CRYPTO 2018]

Ximing Fu, Xiaoyun Wang, Xiaoyang Dong, and Willi Meier

855 段に縮退されたストリーム暗号 Trivium に対する鍵回復攻撃が提示された。秘密鍵と初期ベクトル上のブール多項式からゼロ化と次数の上限を決める手法により、正しい鍵を求める。本手法は NFSR に基づくほとんどのストリーム暗号に適用することができ、855 段の Trivium は 2^{77} の時間計算量で鍵を回復できる。

・Improved Division Property Based Cube Attacks Exploiting Algebraic Properties of Superpoly [CRYPTO 2018]

Qingju Wang, Yonglin Hao, Yosuke Todo, Chaoyun Li, Takanori Isobe, and Willi Meier

キューブ攻撃はストリーム暗号解析において重要なテクニックである。CRYPTO 2017 における藤堂らの分割性質ベースのキューブ攻撃を、より広い範囲のキューブ・インデックス集合に拡張することにより、鍵回復攻撃を 839 段 Trivium、891 段 Kreyvium、184 段 Grain-128a、750 段 Acorn に対して適用することに成功した。

・Boomerang Connectivity Table: A New Cryptanalysis Tool [Eurocrypt 2018]

Carlos Cid, Tao Huang, Thomas Peyrin, Yu Sasaki, and Ling Song

ブロック暗号への Boomerang 攻撃とそれに類する様々な攻撃らを統一的に取り扱えるようにするためのツールとして BCT (Boomerang Connectivity Table) を提案している。また BCT による解析でこれまで考慮されなかった差分パス経路による伝搬確率の増分効果 (Generalized Switching Effect) が見込まれることを示し、AES ベースの Tweakable ブロック暗号「Deoxys-BC-384」のフラウラウンド 16 段に対して、縮退版 (8 段、9 段,10 段) の Boomerang distinguisher の確率 (2^{-6}、2^{-18}、2^{-42}) が、各々、確率が高まる ($2^{-5.4}$、$2^{-17.4}$、$2^{-41.4}$) ことが示された。尚、「Deoxys-BC」は認証暗号の国際コンペである『CAESAR』の第 4 次選考を通過した認証暗号 Deoxys の内部で利用されている Tweakable ブロック暗号であり、「Deoxys」は CRYPTREC が 2017 年度に発行した『CRYPTREC 暗号技術ガイドライン (軽量暗号)』でも評価対象となっている。

・Cryptanalysis of MORUS [Asiacrypt 2018]

Tomer Ashur, Maria Eichlseder, Martin M. Lauridsen, Gaëtan Leurent, Brice Minaud, Yann Rotella, Yu Sasaki, and Benoît Viguier

MORUS は CAESAR コンペティションに応募された高性能認証暗号であり、ファイナリストに選出されている。MORUS には MORUS-640(128 ビット鍵)、MORUS-1280(128 ビット鍵／256 ビット鍵) と 3 つのバージョンがあり、安全性は鍵のサイズに一致すると主張されている。本論文では、フルバージョンの MORUS の鍵ストリームに線型相関を示す。256 ビット鍵 MORUS-1280 に対し、2^{152} 暗号化で 2^{-76} 相関が得られることが示された。

・Cryptanalysis of MORUS [Asiacrypt 2018]

Tomer Ashur, Maria Eichlseder, Martin M. Lauridsen, Gaëtan Leurent, Brice Minaud, Yann Rotella, Yu Sasaki, and Benoît Viguier

MORUS は CAESAR コンペティションに応募された高性能認証暗号であり、ファイナリストに選出されている。MORUS には MORUS-640(128 ビット鍵)、MORUS-1280(128 ビット鍵／256 ビット鍵) と 3 つのバージョンがあり、安全性は鍵のサイズに一致すると主張されている。本論文では、フルバージョンの MORUS の鍵ストリームに線型相関を示す。256 ビット鍵 MORUS-1280 に対し、2^{152} 暗号化で 2^{-76} 相関が得られることが示された。

2.5. 委員会開催記録

2018 年度、暗号技術評価委員会は、表 2.5 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 2.5: 暗号技術評価委員会の開催

回	年月日	議題
第 1 回	2018 年 7 月 19 日	・CRYPTREC 暗号リストの更新・公開についての報告 ・委員会及びワーキンググループ活動計画案の検討 ・外部評価についての了承 ・監視状況の報告 ・CRYPTREC における耐量子計算機暗号への対応についての検討
第 2 回	2019 年 3 月 11 日	・ワーキンググループ活動報告 ・外部評価結果についての了承 ・監視状況の報告 ・CRYPTREC Report 2018(暗号技術評価委員会報告)目次案の提示 ・CRYPTREC シンポジウム 2019 開催について

2.6. 暗号技術調査ワーキンググループ開催記録

2018 年度、各暗号技術調査ワーキンググループ（WG）が活動した主要活動項目は、表 2.6 の通りである。表 2.7 の通り、各 WG は計 3 回開催された。各会合の開催日及び主な議題は以下の通りである。

表 2.6: 2018 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
暗号解析評価ワーキンググループ	高木 剛	近年、量子計算機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おり、PQC の研究動向を把握する必要性が高まっている。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、PQC の技術動向を調査する。また、素因数分解の困難性や楕円曲線上の離散対数問題の困難性に関しては、例年公表している予測図の更新を行う。

表 2.7: 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	2018 年 6 月 27 日	・耐量子計算機暗号の研究動向調査報告書の執筆方針及び導入部分の章の検討 ・暗号技術調査ワーキンググループ活動計画及び進捗報告(案)の検討 ・今年度の調査の進め方の検討
第 2 回	2018 年 10 月 12 日	・第 2～4 章(格子に基づく暗号・多変数多項式に基づく暗号・符号に基づく暗号・同種写像に基づく暗号)及び第一章(導入部分)の執筆内容の検討
第 3 回	2019 年 2 月 15 日	・耐量子計算機暗号の研究動向調査報告書(案)の執筆内容の確認 ・予測図の更新に関する検討 ・ワーキンググループ活動報告案の了承

第３章　暗号技術調査ワーキンググループの活動

3.1. 暗号解析評価ワーキンググループ

3.1.1. 活動目的

(1)　耐量子計算機暗号の研究動向調査

近年、量子計算機が実用化されても安全性を保つことができると期待される暗号（耐量子計算機暗号：PQC）の調査・検討が各国で進められている。特に米国では NIST が PQC の公募を開始しており、欧州では ETSI が PQC の調査活動を行い、ISO/IEC でも標準化に向けた議論が始まっている。このように国内でも PQC の研究動向を把握する必要性がさらに高まっている。

2017 年度及び 2018 年度において、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、PQC の技術動向を調査することが暗号技術検討会において承認された。暗号技術評価委員会では、暗号技術調査ワーキンググループ(暗号解析評価)を設置し、本調査を実施した。

- 耐量子計算機暗号（PQC）に関する近年の研究動向を調査し、報告書を作成する。(完成予定は 2018 年度末。)
- PQC の代表的な候補である、4 つの分類（格子に基づく暗号技術、符号に基づく暗号技術、多変数多項式に基づく暗号技術、同種写像に基づく暗号技術）を調査対象とする。
- 上記の各分類において、該当する方式及び文献について 3 つの機能（暗号化、鍵交換、署名）の観点による整理等を実施する。

(2) 予測図の更新

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して CRYPTREC が例年公表している予測図の更新を行う。

3.1.2. 委員構成

(敬称略、五十音順)

主査：	高木　剛	東京大学
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：	國廣　昇	東京大学
委員：	下山　武司	株式会社富士通研究所
委員：	高島　克幸	三菱電機株式会社
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

3.1.3.1. 耐量子計算機暗号の研究動向調査

(1) NIST PQC 標準化動向

- NIST PQC 標準化の公募では、締め切り(2017 年 11 月 30 日)までに、82 件の方式が提案され、そのうち 69 件が書類基準を満たし、その後、5 件の暗号方式が取り下げられた。
- NIST PQC 標準化プロジェクトにおいて提案された暗号方式の絞り込みが実施された(Second Round Candidates)。暗号方式は 26 件に絞り込まれ、2019 年 1 月 30 日にその候補リストが公開された。提案された暗号方式の安全性を 2018 年から約 5 年をかけて検証することが予定されている。

**This is a tentative timeline, provided for information, and subject to change.*

Date	
Feb 24-26, 2016	NIST Presentation at PQCrypto 2016: *Announcement and outline of NIST's Call for Submissions (Fall 2016)*, *Dustin Moody*
April 28, 2016	NIST releases NISTIR 8105, Report on Post-Quantum Cryptography
Dec 20, 2016	Formal Call for Proposals
Nov 30, 2017	Deadline for submissions
Dec 4, 2017	NIST Presentation at AsiaCrypt 2017: *The Ship Has Sailed: The NIST Post-Quantum Crypto "Competition"*, *Dustin Moody*
Dec 21, 2017	Round 1 algorithms announced (69 submissions accepted as "complete and proper")
Apr 11, 2018	NIST Presentation at PQCrypto 2018: *Let's Get Ready to Rumble - The NIST PQC "Competition"*, *Dustin Moody*
April 11-13, 2018	First PQC Standardization Conference - Submitter's Presentations
January 30, 2019	Second Round Candidates announced
August 22-24, 2019 *(tentative)*	Second PQC Standardization Conference
2020/2021	Round 3 begins or select algorithms
2022/2024	Draft Standards Available

(2019 年 3 月 1 日:https://csrc.nist.gov/projects/post-quantum-cryptography/workshops-and-timeline)

(2) 耐量子計算機暗号の研究動向調査

(a)2017 年度第 1 回 WG での実施内容及び決定事項

- 調査対象とする 4 つの分類項目(下記の①から④)について担当者を決定した。

表 3-1: 担当委員の一覧

	とりまとめ委員	執筆者
導入	高木主査・事務局	高木主査・事務局
①格子に基づく暗号技術	下山委員	下山委員、安田(雅)委員、青野(事務局)
②多変数多項式に基づく暗号技術	安田(貴)委員	安田(貴)委員
③符号に基づく暗号技術	草川委員	草川委員
④同種写像に基づく暗号技術	高島委員	高島委員

- 4 つの分類において、調査対象を具体的に何にするかは、担当のとりまとめ委員を中心に決定した。

(b) 2017 年度第 2 回 WG での実施内容及び決定事項

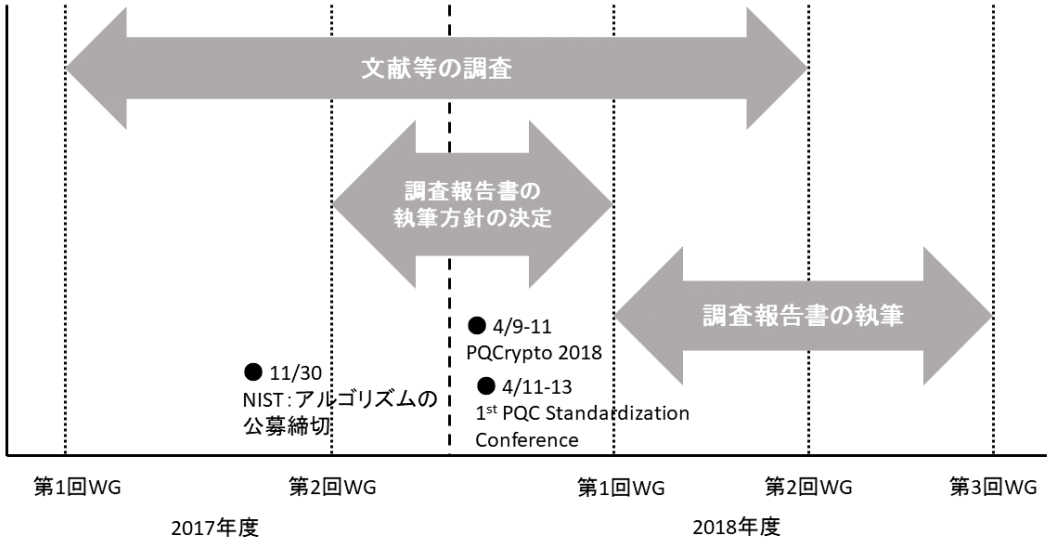
- スケジュールの修正について

  2018 年度は WG を 3 回実施する。

  2018 年度第 1 回 WG（6 月 27 日）：執筆方針を決定。

  2018 年度第 2 回 WG（10 月）：報告書（案）の中間報告。

  2018 年度第 3 回 WG（ 2 月）：報告書（案）完成。



(c) 2018 年度第 1 回 WG 及びその事前調整会議での実施内容及び決定事項

- 下記の日程で報告書の執筆方針（案）に関する事前調整会議を実施した。

  2018 年 5 月 23 日：主査打ち合わせ（導入の章）

  2018 年 6 月 11 日：執筆担当者打ち合わせ（符号に基づく暗号技術）

  2018 年 6 月 12 日：執筆担当者打ち合わせ（格子に基づく暗号技術）

  2018 年 6 月 14 日：執筆担当者打ち合わせ（多変数多項式に基づく暗号技術）

  2018 年 6 月 14 日：執筆担当者打ち合わせ（同種写像に基づく暗号技術）

- 事前調整会議での議論を基に、耐量子計算機暗号の研究動向調査報告書の執筆方針を決定した。

(d) 2018 年度第 2 回 WG での実施内容及び決定事項

- 報告書（案）の各章について執筆担当者が説明し、WG にて加筆・修正について議論された。

(e) 2018 年度第 3 回 WG での実施内容及び決定事項

- 報告書（案）の各章について執筆担当者が説明し、それらのおおよその内容が WG で了承された。報告書の微修正等の締め切りを 2019 年 3 月 15 日とし、発行日は同年 3 月、Web での公開日は同年 4 月 5 日とすることを決定した。

3.1.3.2. 予測図の更新

(1) 2017 年度

- 素因数分解問題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、2017 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。

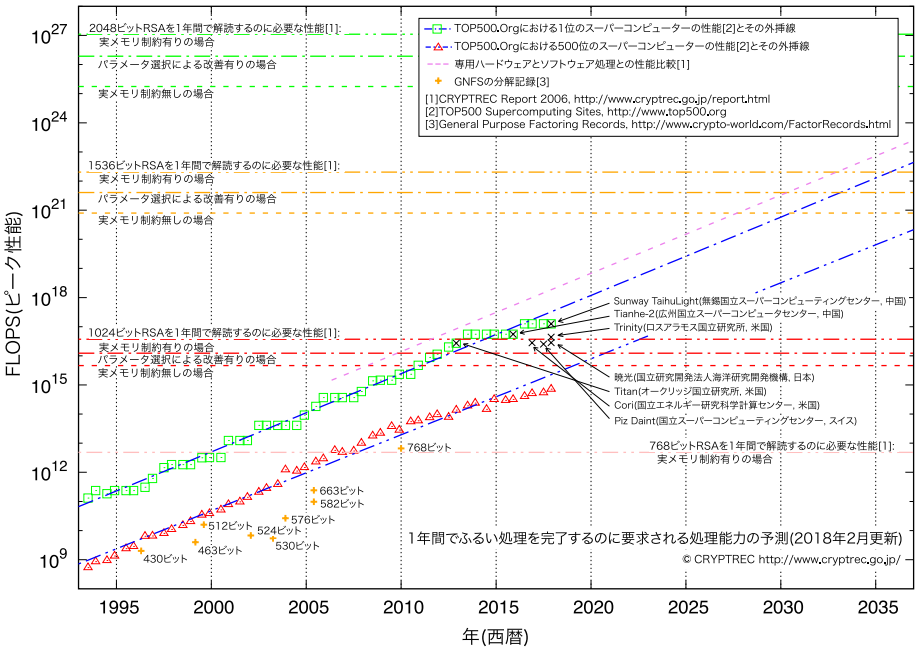


図 1: 素因数分解の困難性に関する計算量評価

(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、2018 年 2 月更新)

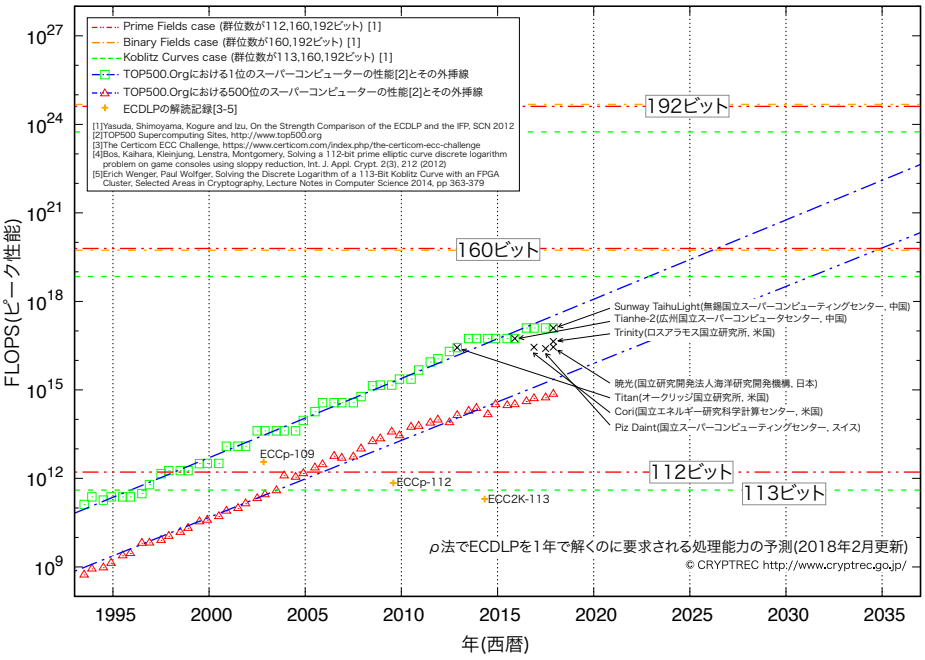


図 2: 楕円曲線上の離散対数計算の困難性に関する計算量評価

(ρ 法で ECDLP を 1 年で解くのに要求される処理能力の予測、2018 年 2 月更新)

(2) 2018 年度

予測図の更新に関して、下記の（a）及び（b）について対応を行った。

(a)　素因数分解問題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の評価に大幅な変更がないかどうかの確認

- 素因数分解問題の困難性に関する計算量評価については、2006 年度に実施した評価結果[1]の更新。

T. Kleinjung 氏及び A. K. Lenstra 氏に評価を依頼し、素因数分解を効率良く解くアルゴリズムとして知られている一般数体ふるい法において、計算時間の主要な部分を占める篩処理部分のソフトウェア評価の再評価を行った。評価結果は下記の表 1 の通りである。

以前の評価結果と比べて大幅な変更はないことが確認された。なお、評価レポート[1]は、技術報告書として Web 公開する予定である[2]。

表 1: 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}	128×10^{15}

[1] Evaluation of complexity of the sieving step of the general number field sieve, T. Kleinjung and A. K. Lenstra, December 5, 2018

(b) 素因数分解問題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及び計算機の処理性能の表示等についての検討

計算機の処理性能の表示等に対して、第一回暗号技術評価委員会において、下記の枠内のようなコメントがあった。

- 縦軸についても FLOPS でよいのかという点も含めて検討してもらいたい。
- 可能な範囲で計算機の専門家に協力してもらうなどの努力を重ねてもらいたい。
- 計算機能力の向上の線がなだらかになっている点については、HPC 分野でも認識されている。そうした計算機能力の進展について、専門家にヒアリングするのがよいと思われる。

これらのコメントに対して、計算機の専門家からヒアリングを行った結果、「半導体の微細化は限界が近づいている」、「将来、プロセッサの性能は頭打ちになる」、「計算の目的が多様化してきている」等が指摘された[3]。

[1] https://www.cryptrec.go.jp/exreport/cryptrec-ex-0601-2006.pdf（T. Kleinjung 氏による）

[2] https://www.cryptrec.go.jp/exreport/cryptrec-ex-2802-2018.pdf（掲載予定）

[3] 暗号技術委員会 上原委員及び高木委員のご協力により、それぞれ、筑波大学 朴泰祐教授及び東京大学 中島研吾教授からご意見を伺った。

第 3 回 WG において、素因数分解問題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及び計算機の処理性能の表示等についての検討を開始した。

・（１）で述べた 2018 年度に実施された評価結果を予測図に表示する方法について

- 従来通り 1 クロックにつき 2 FLOPS で換算して横線を引く。
- 2018 年度に実施した評価結果に関する横線を新たに引くと、2006 年度に実施された同じビット長の評価結果に関する横線の近くを通り、表示が複雑になるため、新たに引く横線より上方を通る「実メモリ制約有り」の横線を省く。

という提案が事務局からあったが、他に適切な表示があるのではないかという意見が出されたため、新たに得られた評価結果を含め、これら評価結果の解釈については継続審議とすることとなった。

・計算機の処理性能の表示について

以前から外挿線の傾きが徐々に下ってきていることが WG で指摘されていたが、今後どのように外挿するべきかについて検討された。

予測図では、TOP500.Org から公表されているスーパーコンピュータのうち、ピーク性能が 1 位(または 500 位)であるものをプロットして、1993 年から現在までのすべてのデータに最小自乗法を適用して外挿線を引いている。予測図は 2006 年度にはじめて作成され、RSA1024 ビットの危殆化のおおよその時期を予測するために利用された。外挿線の傾きが一定である範囲では解読に必要な計算量に相当する横線と交わる年が危殆化時期の目安となるからである。

外挿線の傾きの変化の様子を下記の図 3 に示す。これによると、2014 年頃から現在まで外挿線の傾きが鈍化し続けていることがわかる。

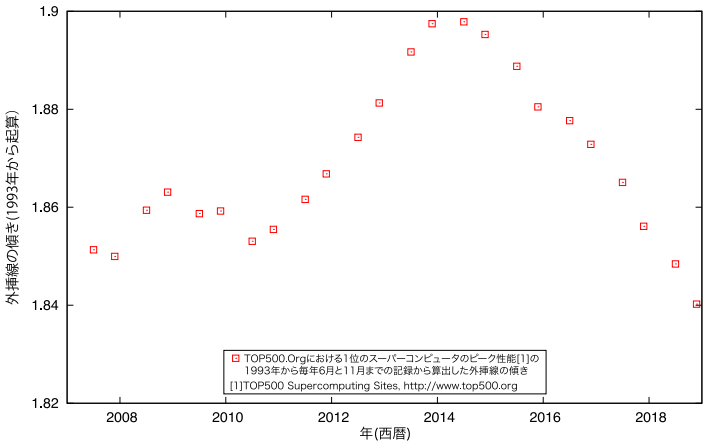


図 3:TOP500.Org における 1 位のスーパーコンピュータのピーク性能の
1993 年から毎年 6 月と 11 月までの記録から算出した外挿線の傾き

- スーパーコンピュータのピーク性能 1 位のプロットは、上述のヒアリングの中の指摘にもあるようにばらつきがある。

- 1位から500位のピーク性能の合計値(SUM)のプロットはなだらかで、外挿線の傾きの変化が分かり易いため、予測図にピーク性能の合計値のプロットを追加し、それらの外挿線を引く。

という提案が事務局からあったが、短い期間のデータから外挿した直線がどの範囲まで妥当であるかが不明である等、近年のこのような鈍化傾向を予測図にどのように反映するかについては慎重に検討する必要があるという意見があったため、予測図の更新については継続審議とすることとなった。

2018年度の予測図の更新については継続審議となったが、第二回暗号技術評価委員会において予測図の参照先が明確でないのは不都合であるという指摘があったので、2018年6月・11月のベンチマーク結果を追加して従来通りの方法で予測図を更新することになった（次のページの図4及び図5)。

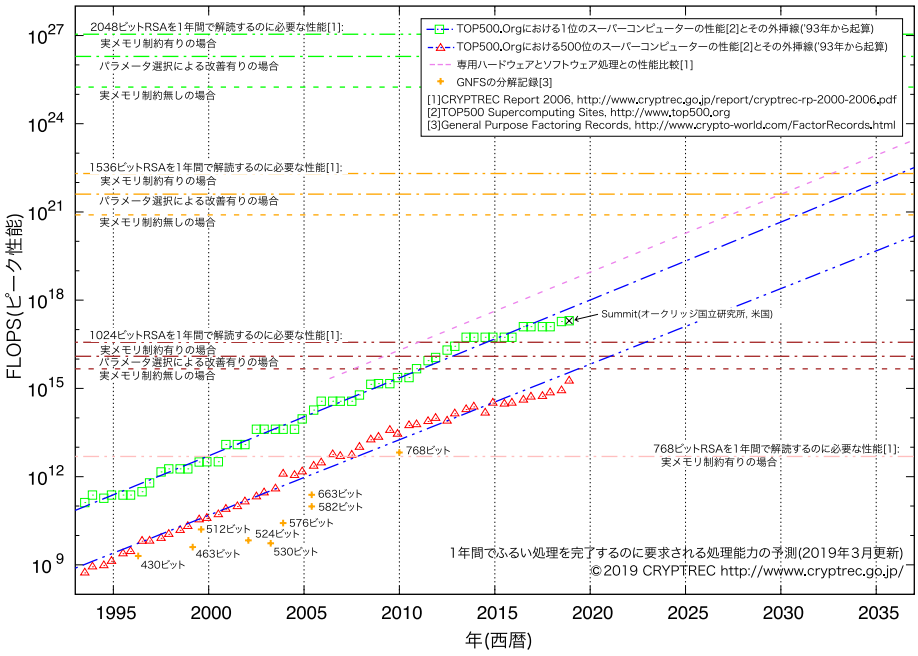


図 4: 素因数分解の困難性に関する計算量評価

(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、2019 年 3 月更新)

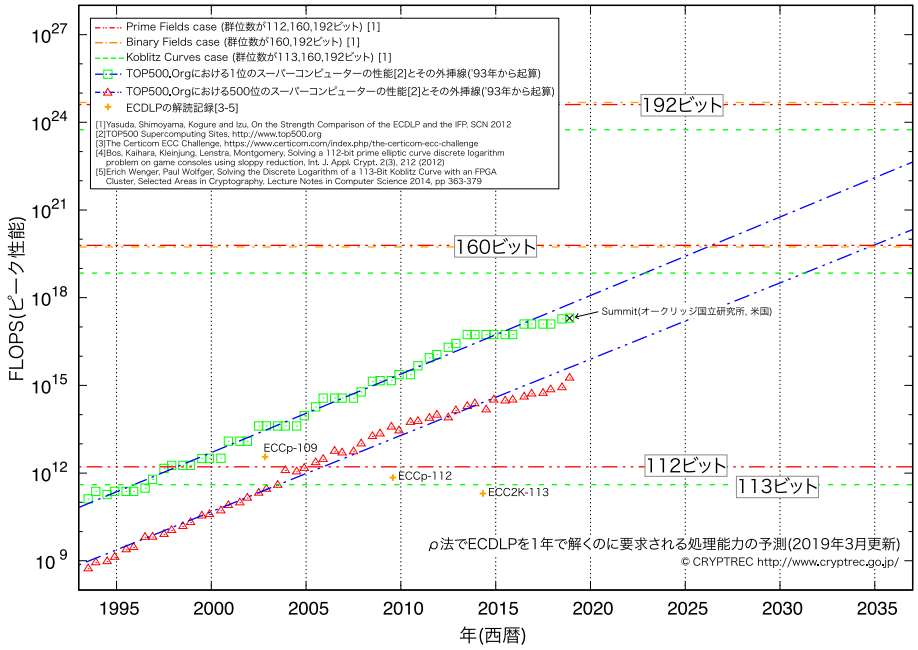


図 5: 楕円曲線上の離散対数計算の困難性に関する計算量評価

(ρ 法で ECDLP を 1 年で解くのに要求される処理能力の予測、2019 年 3 月更新)

3.1.3.3. 量子計算機による素因数分解について

米国学術機関の統合団体である全米アカデミーズが公表したレポート[2]によれば、十分な性能を有する量子計算機の登場の時期を現時点で予測することは困難であるため、大きな合成数の素因数分解問題が量子計算機によって解かれる時期について言及することは難しい。従って、量子計算機を用いた素因数分解の数値実験の現状について、[3]の表 1 をもとにまとめることになった。

表 2: 量子計算機による素因数分解の状況（[3]の表 1 を一部改変）

■量子ゲート計算（#QB は使用した量子ビット数）

分解法	計算手段	合成数	ビット長	発表年	ジャーナル名	備考
Shor※1	NMR	15	4	2001 年	Nature	#QB=7
	光子	21	5	2012 年	Nature Photonics	#QB=1+log3※2
	光集積回路	15	4	2009 年	Science	#QB=5
	ジョセフソン素子	15	4	2012 年	Nature Physics	#QB=3
	イオントラップ	15	4	2016 年	Science	#QB=5

※1: 分解対象の素因数分解結果を用い、Shor のアルゴリズムの演算の一部を省略している

※2: 2 進と 3 進で表現されている

■量子アニーリング計算（#QB は使用した量子ビット数）

分解法	計算手段	合成数	ビット長	発表年	ジャーナル名	備考
素朴法	NMR	21	5	2008 年	Physical Review Letters	#QB=3
筆算法	NMR	143	8	2012 年	Physical Review Letters	#QB=4
	D-Wave	200099	18	2016 年	Scientific Reports	#QB=897

[2] Quantum Computing: Progress and Prospects, The National Academies of Science, Engineering, and Medicine, 2018, http://nap.edu/25196

[3] 素因数分解の現状, 伊豆, 國廣, 2B2-3, 暗号と情報セキュリティシンポジウム 2018 (SCIS2018)

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： http://www.fujitsu.com/jp/group/labs/resources/tech/external-activities/crypto/ 英文： http://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) http://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 http://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 (Ver.2.2) ・ 参照 URL http://www.emc.com/collateral/white-papers/h11300-pkcs-1v2-2-rsa-cryptography-standard-wp.pdf 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 (Ver.2.2) ・ 参照 URL http://www.emc.com/collateral/white-papers/h11300-pkcs-1v2-2-rsa-cryptography-standard-wp.pdf 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 (Ver.2.2) ・ 参照 URL http://www.emc.com/collateral/white-papers/h11300-pkcs-1v2-2-rsa-cryptography-standard-wp.pdf 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 http://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 http://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： http://www.fujitsu.com/jp/group/labs/resources/tech/external-activities/crypto/ 英文： http://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) http://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 http://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 http://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: 0422-59-3212, FAX:0422-59-4015 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：http://www.kddi-research.jp/products/kcipher2.html 英文：http://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 http://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 http://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 http://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 http://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 http://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 http://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(http://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(http://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: 0422-59-3212　　FAX: 0422-59-4015 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：http://www.toshiba.co.jp/rdc/security/hierocrypt/ 英文：http://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 研究開発本部 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 http://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：http://www.toshiba.co.jp/rdc/security/hierocrypt/ 英文：http://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 研究開発本部 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： http://www.fujitsu.com/jp/group/labs/resources/tech/external-activities/crypto/ 英文： http://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：http://www.hitachi.co.jp/rd/yrl/crypto/mugi/ 英文：http://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:http://www.hitachi.co.jp/rd/yrl/crypto/enocoro/ 英文:http://www.hitachi.com/rd/yrl/crypto/enocoro/index.html	
問い合わせ先	〒244-0817 神奈川県横浜市戸塚区吉田町 292
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 TEL：045-860-3093, FAX：045-443-9842 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：http://www.hitachi.co.jp/rd/yrl/crypto/s01/ 英文：http://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 http://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 http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf

4. メッセージ認証コード

暗号名	PC-MAC-AES
関連情報	
参照 URL：http://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　主幹研究員 峯松 一彦 TEL：044-431-7686, FAX：044-431-7644 E-MAIL: k-minematsu@ah.jp.nec.com

5. 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

6. 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(http://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 (Ver.2.2)
- 参照 URL

http://www.emc.com/collateral/white-papers/h11300-pkcs-1v2-2-rsa-cryptography-standard-wp.pdf

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

http://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 http://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(http://www.jsa.or.jp/)から入手可能である。	

付録３

暗号利用モード XTS の安全性に関する調査及び評価 (概要版)

日本電気株式会社
峯松 一彦

2019 年 1 月

概要

本報告書は，ブロック暗号を利用した暗号利用モード（秘匿モード）である XTS の安全性評価を行い，その結果を報告するものである．XTS は IEEE Storage in Security Workgroup (SISWG) により，ハードディスクや USB メモリなどのストレージデバイスの暗号化の標準方式として設計された暗号利用モードである．2007 年には IEEE Standard P1619-2007 [IEE] として標準化されている．これに続いて 2010 年には，米国 国立標準技術研究所（National Institute of Standards and Technology, NIST) が，IEEE で標準化された仕様に対して若干のパラメータの制約を加えた上で，XTS を NIST の推奨する方式として選定した．NIST 推奨を記述した仕様書（実質的な標準化文書）として NIST SP800-38E [Dwo10] を発行している．

XTS 自体は汎用的な暗号利用モードとして定義することが可能であり，したがって任意のブロック暗号を用いることが可能である．しかし，上記の IEEE 標準化および NIST 推奨方式としては，利用するブロック暗号は AES に固定して仕様を定め，この場合の利用モードを XTS-AES と名付けて仕様を標準化している．本報告書では一般的な暗号利用モードとしての XTS および XTS-AES に関し， IEEE, NIST の標準化文書および関連文献を精査し安全性を評価した．以下に評価結果の概要を記す．

1. IEEE および NIST の標準化文書においては，安全性評価に関する言及は参考文献の引用程度で，明確には述べられていない．しかし，XTS がベースとする XEX に関しては Rogaway による論文 [Rog04] が存在し，また NIST へのパブリックコメント [LM06] において XEX と XTS の違いを考慮したうえでの安全性証明が与えられている．このことから，XTS のコアであるブロック単位の暗号化処理に関しては安全といえる．
2. XTS はブロック単位での暗号化（ Narrow-Block Encryption ）を行うため，ブロック単位の暗号化処理が安全であっても，提供できる安全性については本質的な限界がある．しかし，CBC などで暗号化するよりも高い安全性を有しており，現実的な安全性と効率のトレードオフから考えると妥当である．

3. XTS において Ciphertext Stealing (CTS) を用いた場合の安全性は平文の分布によるため，理論的評価は困難であり，積極的に利用を推奨する根拠に乏しい．ただし，単一平文での暗号文のみ攻撃が可能になる，などの致命的な問題を生じることはない．本来は CTS ではなく 2 ブロックの Tweakable ブロック暗号モードを用いるべきであろう．
4. XTS の安全性証明により，鍵を変えずに処理するデータ量が $2^{n/2}$ ブロック（n はブロックサイズ）より十分小さければ安全であることが知られているが，反対に $2^{n/2}$ ブロック以上のデータを処理した場合の影響について，ストレージ暗号化のシンプルなモデルにおいて平文回復攻撃の検討を行った．結果として，1 ラウンド Even-Mansour 暗号の鍵回復攻撃を応用することができると判明した．攻撃計算量は XTS-AES では 2^{64} 以上であり，必要とするデータが大量であるため，すぐさま現実的な脅威とはなるものではない．しかし，例えば $n = 64$ の 64 ビットブロック暗号を用いた場合では現実的な問題といえる．
5. XTS で規定されたブロック暗号である AES-128 および AES-256 については，学術的にも現実的にも攻撃は見つかっておらず，高い安全性を有すると考えられる．

以上の評価により，XTS-AES は全体としては現実的に安全であるという結論を得た．ただし，最終ブロックが $n = 128$ ビット未満の場合には CTS を用いることになり，保証される理論的安全性が特に明確でなく，このケースには注意が必要である．さらに利用における誤りやサイドチャネル攻撃の影響，また AES でなく 64 ビットブロック暗号などのよりブロックサイズの小さい暗号を使うことは一般に勧められない．

付録４

学会等での主要攻撃論文発表等一覧

目次

1. 具体的な暗号の攻撃に関する発表

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

表 1 具体的な暗号の攻撃に関する発表

公開鍵暗号		頁
☆	Decoding Linear Codes with High Error Rate and its Impact for LPN Security [PQCrypto 2018]	62
☆	QC-MDPC: A Timing Attack and a CCA2 KEM [PQCrypto 2018]	62
	Attacks on the AJPS Mersenne-based Cryptosystem [PQCrypto 2018]	63
☆	Implementing Joux-Vitse's Crossbred Algorithm for Solving MQ Systems over F_2 on GPUs [PQCrypto 2018]	63
	Practical Cryptanalysis of a Public-key Encryption Scheme Based on Non-linear Indeterminate Equations at SAC 2017 [PQCrypto 2018]	63
☆	Computing Isogenies between Montgomery Curves Using the Action of (0; 0) [PQCrypto 2018]	64
☆	Progressive lattice sieving [PQCrypto 2018]	64
☆	Rank Analysis of Cubic Multivariate Cryptosystems [PQCrypto 2018]	65
	Improved Cryptanalysis of HFEv- via Projection [PQCrypto 2018]	65
☆	Asymptotically faster quantum algorithms to solve multivariate quadratic equations [PQCrypto 2018]	66
☆	Dissection-BKW [Crypto 2018]	68
☆	Lower Bounds on Lattice Enumeration with Extreme Pruning [Crypto 2018]	68
	Practical attacks against the Walnut digital signature scheme [Asiacrypt2018]	74
	Two attacks on rank metric code-based schemes: RankSign and an IBE scheme [Asiacrypt2018]	75
	An efficient structural attack on NIST submission DAGS [Asiacrypt2018]	75
☆	Quantum Lattice Enumeration and Tweaking Discrete Pruning [Asiacrypt2018]	75
ブロック暗号		**頁**
☆	Boomerang Connectivity Table: A New Cryptanalysis Tool [Eurocrypt 2018]	67
★	Improved Key Recovery Attacks on Reduced-Round AES with Practical Data and Memory Complexities [Crypto 2018]	72
☆	Programming the Demirci-Selçuk Meet-in-the-Middle Attack with Constraints [Asiacrypt2018]	77
ストリーム暗号		**頁**
☆	Correlation Cube Attacks: From Weak-Key Distinguisher to Key Recovery [Eurocrypt 2018]	67
☆	Fast Near Collision Attack on the Grain v1 Stream Cipher [Eurocrypt 2018]	68
☆	Fast Correlation Attack Revisited - Cryptanalysis on Full Grain-128a, Grain-	72

2. PQCrypto 2018 の発表

2.1. PQCrypto 2018 の発表（1 日目）

Decoding Linear Codes with High Error Rate and its Impact for LPN Security [PQCrypto 2018]

Leif Both and Alexander May

本論文では、ランダムな次元 n の 2 元線型符号に対する新しい復号アルゴリズムを提案する。既存アルゴリズムと比べて、エラー率が高い場合に優位となる。全距離復号の場合、既知の最良下界は Becker、Joux、May、Meurer らの BJMM アルゴリズムにより達成された $2^{0.0953n}$ であるが、我々のアルゴリズムは $2^{0.0885n}$ まで大きく引き下げた。

技術的には、BJMM アルゴリズムは最近傍検索の利点を最後のステップにおいてのみ利用しているのに対し、本アルゴリズムでは構成のすべてのステップにおいて最近傍テクニックを多用することにより改良している。

LPN の暗号インスタンスは、通常高いエラー率であるため、本アルゴリズムは LPN の安全性に示唆を与える。

QC-MDPC: A Timing Attack and a CCA2 KEM [PQCrypto 2018]

Edward Eaton, Matthieu Lequesne, Alex Parent, and Nicolas Sendrier

2013 年に、Misoczki、Tillich、Sendrier、Barreto らは、QC-MDPC(Quasi-Cyclic Moderate Density Parity Check)符号に基づく McEliece 暗号の変形を提案した。この提案は復号処理において対話的なビット反転アルゴリズムを使っているが、このようなアルゴリズムは小さい確率で失敗することがある。

Asiacrypt 2016 において、Guo、Johansson、Stankovski (GJS) らは、これらの失敗を利用した鍵回復攻撃を行った。彼らは疎なベクトルの距離スペクトルという概念を導入し、スペクトルを知ることによりベクトルを見つけることができることを示し、多くの失敗する平文を観察することにより、QC-MDPC 秘密鍵の距離スペクトルを回復した。

本論文では、鍵のスペクトルとエラーのスペクトル間の相関がシンドローム重みの偏りをもたらすことを証明したため、シンドローム重みは秘密情報が漏れる基本的な量となる。シンドローム重みの観察を許すサイドチャネルを仮定することにより、復号失敗となる平文のみならずすべての既知平文を利用することができるという利点を持った鍵回復攻撃が可能となる。本研究に基づき、復号失敗確率が低い最近の変形に対しても有効に働く、QC-MDPC スキームに対する初めてのタイミング攻撃を導き出した。

最後に、QC-MDPC のパラメーターを変えずに、復号失敗確率をセキュリティ上無視できる程度に下げることのできる ParQ という新しい鍵カプセル化機構の構築方法を示す。

Attacks on the AJPS Mersenne-based Cryptosystem [PQCrypto 2018]

Koen de Boer, Léo Ducas, Stacey Jeffery, and Ronald de Wolf

近年、Aggarwal、Joux、Prakash、Santha (AJPS) らは、潜在的に耐量子計算機となる新しい公開鍵暗号を導入し、全数探索攻撃が本質的に最適であると示唆した。彼らは、中間一致攻撃と LLL ベースの攻撃を考慮したが、有効ではないとしたが、Beunardeau らは AJPS システムの安全性を大幅に減らすと考えられる実用的な LLL ベース技術を提案した。本論文では初めに、Aggarwal らが考えた困難を打ち負かす局所的に敏感なハッシシングにより、中間一致攻撃も AJPS に対して働くことを示した。次に、Beunardeau らの攻撃をより精密に解析し、その結果を確認し、洗練した。

Implementing Joux-Vitse's Crossbred Algorithm for Solving MQ Systems over F_2 on GPUs [PQCrypto 2018]

Ruben Niederhagen, Kai-Chun Ning, and Bo-Yin Yang

多変数 2 次(MQ: Multivariate Quadratic)連立方程式を解く困難性は、耐量子計算機暗号の分野において、多変数ベーススキームの安全性根拠となっている。この問題の具体的かつ実用的な困難性は、最新かつ高性能の実装により、測られなければならない。本論文では、2017 年の Joux および Vitse による F_2 上の MQ 連立方程式を解く混合アルゴリズムの採用を記述・実装・評価した。採用したアルゴリズムは高度に並列化可能であり、GPU アーキテクチャーで MQ 連立方程式を解くのに適している。実装では 1 台の商用 Nvdia GTX 980 グラフィックカードを用いて 134 方程式・67 変数の MQ 連立方程式を 98.34 時間で解くことができる一方、オリジナルの Joux-Vitse アルゴリズムでは同サイズの問題を解くのに 6200 CPU 時間かかる。本論文の実装により、55 から 74 の n に対し、すべての福岡 Type-I MQ チャレンジを解くことができた。本実装に基づき、3600 台の GTX 980 グラフィックカードを用いて、80 方程式 84 変数の MQ 連立方程式を 1 年で解くことができると見積もった。これらのパラメーターは、Crypto 2011 において、作本、白井、樋渡らにより 80 ビット安全として提案されたものである。

Practical Cryptanalysis of a Public-key Encryption Scheme Based on Non-linear [PQCrypto 2018]

Keita Xagawa

SAC2017 において、秋山、後藤、奥村、高木、縫田、花岡らにより、耐量子計算機暗号として提案された不定方程式暗号(IEC: Indeterminate Equation Cryptosystem)の安全性を研究した。IEC では 2 つのパラメーター集合、PS1: (n, p, degX, q)=(80, 3, 1, 921601)および PS2: (n, p, degX, q)=(80, 3, 2, 58982400019)が与えられた。本論文では、格子基底縮小アルゴリズムにより、これらのパラメーター集合に対して、実用的な鍵回復攻撃およびメッセージ回復攻撃を与える。n=80 は合成数であるという事実と、Gentry の NTRU 合成数に対する攻撃(EUROCRYPT 2011)のアイディアを利用する。結果を要約すると以下の通りである。

－PS1 に関し、100 個の公開鍵から 84 個の秘密鍵を各々30～40 秒で回復

－PS1 に関し、100 個の暗号文すべてから部分情報を各々1 秒以内で回復

－PS2 に関し、100 個の暗号文すべてから部分情報を各々30 秒以内で回復

更に、例えば n=83 のように n が素数の場合にもメッセージ回復攻撃および識別攻撃を与える。格子ベース攻撃において格子次元を減らすために別の部分環を利用することにより、degX=2 の場合に攻撃に成功した。

－PS2': (n, p, degX, q)=(83, 3, 2, 68339982247)に対し、10 個のランダムな暗号文から 7 メッセージを各々61000 秒(約 17 時間)以内に回復した。

－より大きな n であっても、IEC の根拠を破る格子の短いベクトルを見つけることができる。実験では、n=113 に対して、このようなベクトルを 330000 秒(約 4 日)以内に見つけることができた。

Computing Isogenies between Montgomery Curves Using the Action of (0; 0) [PQCrypto 2018]

Joost Renes

Asiacrypt 2017 において、Costello と Hisil は、Montgomery 曲線上の奇数次巡回カーネルを持つ同種写像を計算する効率的な公式を示した。本論文では、この定理の拡張の構成的な証明を与え、同種写像の形と点(0, 0)の単純な作用との関係を示す。本拡張は巡回カーネルの制約をなくし、カーネルが(0,0)を含まない任意の分離的な同種写像を許容する。特別な場合として、Montgomery 曲線間の 2-同種写像に対する効率的な公式を与え、これらの公式が同種写像ベース暗号において、コストのかかる平方根計算や位数 8 の特別な点の知識なしに、利用できることを示す。更に、位数 3 の明示的な点を持つ三角型の楕円曲線を考える。

2.2. PQCrypto 2018 の発表(2 日目)

Progressive lattice sieving [PQCrypto 2018]

Thijs Laarhoven and Artur Mariano

困難な格子問題を解くアルゴリズムの多くは階数削減の原則に基づいている。即ち、d次元格子の問題を解くのに、まず階数 d-1 の部分格子で 1 つ以上の問題を解き、その情報を元の問題を解くのに利用する。しかしながら、既存の格子篩法は最短ベクトル問題(SVP: Shortest Vector Problem)のような格子問題に直接的に取り組み、初めからフル階数の格子を扱う。更に、格子篩は他の方法に比べ縮約格子から始めた時に受ける恩恵が少なく、近似解を見出すのに厳密解を見出すのと同じくらいの時間がかかる。

本論文では、格子篩への漸進的なアプローチを考え、篩が前の基底ベクトル上に安定したときにのみ新しい基底ベクトルを暫時導入していく。これにより近似最短ベクトルを求める保証を(ヒューリスティックに)改善し、実行時の基底の質により大きな実用的な影響を与え、メモリ管理をより良くし、アルゴリズムの振る舞いをより滑らかかつ予測しやすくし、大幅に速く収束する(従来のアプローチより SVP の時間計算量では 20～40 倍高速)ようにした。

Rank Analysis of Cubic Multivariate Cryptosystems [PQCrypto 2018]

John Baena, Daniel Cabarcas, Daniel Escudero, Karan Khathuria, and Javier Verbel

本論文では、階数の弱さに関する、3 次暗号構成の安全性を解析する。多変数暗号を構成する概念(Big Field Idea)を 2 次から 3 次に拡張する方法を詳述し、同様の階数の欠陥が起こることを示す。最小階数問題を拡張し、この設定における問題を解くアルゴリズムを提示し、固定した小さな階数に対する計算量は、2 次の場合より小さいことを示す。しかしながら、n 変数の 3 次多項式の階数は n よりも大きくなることがあり、このような場合にはアルゴリズムは非効率的となる。微分の階数は必ずしもより小さくはならないことを示し、階数が十分大きければこの種の攻撃は使えなくなる。同様に代数的攻撃は階数に関し指数的であるため、高い階数に対しては有効でない。

Improved Cryptanalysis of HFEv- via Projection [PQCrypto 2018]

Jintai Ding, Ray Perlner, Albrecht Petzoldt, and Daniel Smith-Tone

HFEv−署名スキームは最もよく研究された多変数スキームの一つであり、来るべき耐量子計算機電子署名スキーム標準化の最も有力な候補の一つである。本論文では、射影のアイディアを用いた、HFEv−に対する 3 つの新しい攻撃戦略を提示する。特に 3 つ目は非常に有効であり、あるパラメーター集合に対しては、HFEv−に対する既知攻撃の中で最も効率的である。更に、本攻撃は、直接攻撃や階数攻撃よりも、必要なメモリが大幅に少なくて済む。削減し、本論文は、HFEv−署名スキームの安全性に新しい洞察を与え、将来標準化されるかもしれない HFEv−インスタンスのパラメーター選択に制限を与えるものである。

Grafting trees: a Fault Attack against the SPHICS framework [PQCrypto 2018]

Laurent Castelnovi, Ange Martinelli, and Thomas Prest

ハッシュ関数の原像困難性もしくは衝突困難性以外に仮定を必要としないため、ハッシュベース署名は耐量子計算機プリミティブの独特でとても魅力的なクラスである。その中でも SPHINCS ファミリーのスキームは、おそらく最も実用的な状態を持たないスキームであり、FPGA やスマートカードのような組込デバイスに実装することができる。このことから、これらのスキームの実装攻撃に対する耐性への疑問が自然に起こる。

本論文では、SPHINCS、GRAVITY−SPHINCS、SPHINCS+が根拠とする枠組みへの初めての故障攻撃を示す。本攻撃は一つの故障メッセージのコストにより、任意のメッセージ署名を偽造することができる。更に、故障モデルはとても合理的であり、故障メッセージは有効のままとなるため、本攻撃は見つかりにくく現実的である。本攻撃は無視できない計算コストがかかるため、故障メッセージの数を少し増やすことにより計算コストを下げることのできる、きめ細かいトレードオフを示す。本攻撃は、利用するハッシュ関数に依存しないという意味において一般的な攻撃といえる。

Post-quantum security of the sponge construction [PQCrypto 2018]

Jan Czajkowski, Leon Groot Bruinderink, Andreas Hülsing, Christian Schaffner, and

Dominique Unruh

本論文では、スポンジ構成に基づいたハッシュ関数の耐量子計算機安全性を研究する。耐量子計算機設定においてハッシュ関数の重要な性質は、崩壊性(collapsing property：衝突耐性の強化)である。スポンジ構成は、基礎となるブロック関数に関する適切な仮定の下で、崩壊性を持つ(即ち量子衝突耐性を持つ)ことを示す。特に、ブロック関数がランダム関数もしくは(不可逆な)ランダム置換であれば、スポンジ構成は崩壊性を持つ。

2.3. PQCrypto 2018 の発表(3 日目)

Quantum Collision-Finding in Non-Uniform Random Functions [PQCrypto 2018]

Marko Balogh, Edward Eaton, and Fang Song

本論文では、出力が最小エントロピーk の分布に従う一様でないランダム関数の衝突を見出す量子攻撃を研究する。これは、一様ランダムな出力を仮定する標準的なヒューリスティックよりも緩和した仮定の元でハッシュ関数の一般的な安全性を示すことと見ることができる。これは藤崎-岡本変換の量子セキュリティ解析に役立つ。特に、本結果は PQCrypto 2016 において Targhi らにより未解決とされた誕生日下界との差を縮めるものである。

具体的には、D を集合 Y 上の最小エントロピーk の分布とする。f: X→Y を、各 x∈X に関して f(x)が独立に D に従う関数とする。本論文では、f の衝突を発見するには、$\Omega(2^{k/3})$量子クエリが必要なことを示し、以前の下界$\Omega(2^{k/9})$を更新した。実際、特殊な場合にはより強い下界 $2^{k/2}$ を示した。ほとんどの場合において、対応する下界に合致する明示的な量子アルゴリズムも示した。

Asymptotically faster quantum algorithms to solve multivariate quadratic equations [PQCrypto 2018]

Daniel J. Bernstein and Bo-Yin Yang

本論文では、有限体 F_q 上の n 変数、m 個の 2 次連立方程式を解く量子アルゴリズムを設計・解析する。m=n、q=2 の場合、標準仮定の下で、アルゴリズムはメッシュ接続された面積 $2^{(a+o(1))n}$ の計算機上で $2^{(t+o(1))n}$時間かかる。ただし、t は約 0.45743 であり、a は約 0.01467 である。空間・面積積は、漸近的な指数 t+a は約 0.47210 となる。

比較すると、Grover アルゴリズムの面積時間積は漸近的な指数 0.50000 を持つ。Grover アルゴリズムの並列化により漸近的な時間指数 0.45743 とするためには、漸近的な面積指数 0.08514 が必要であり、0.01467 よりかなり大きい。

3. Eurocrypt 2018 の発表

3.1. Eurocrypt 2018 の発表(3 日目)

Boomerang Connectivity Table: A New Cryptanalysis Tool [Eurocrypt 2018]

Carlos Cid, Tao Huang, Thomas Peyrin, Yu Sasaki, and Ling Song

本論文では、ブロック暗号への Boomerang 攻撃とそれに類する様々な攻撃らを統一的に取り扱えるようにするためのツールとして BCT（Boomerang Connectivity Table）を提案している。また BCT による解析でこれまで考慮されなかった差分パス経路による伝搬確率の増分効果（Generalized Switching Effect）が見込まれることを示し、AES ベースの Tweakable ブロック暗号「Deoxys-BC-384」のフラウラウンド 16 段に対して、縮退版（8 段、9 段,10 段）の Boomerang distinguisher の確率（2^{-6}、2^{-18}、2^{-42}）が、各々、確率が高まる（$2^{-5.4}$、$2^{-17.4}$、$2^{-41.4}$）ことが示された。尚、「Deoxys-BC」は認証暗号の国際コンペである『CAESAR』の第 4 次選考を通過した認証暗号 Deoxys の内部で利用されている Tweakable ブロック暗号であり、「Deoxys」は CRYPTREC が 2017 年度に発行した『CRYPTREC 暗号技術ガイドライン（軽量暗号）』でも評価対象となっている。

Correlation Cube Attacks: From Weak-Key Distinguisher to Key Recovery [Eurocrypt 2018]

Meicheng Liu, Jingchun Yang, Wenhao Wang, and Dongdai Lin

本論文ではストリーム暗号への Cube 攻撃の拡張として Correlation Cube 攻撃を提案した上で、軽量ストリーム暗号「Trivium」へ適用した結果を示している。「Trivium」は欧州の eSTREAM プロジェクトにおいて portfolio に掲載された鍵長：80 ビット（IV 長：80 ビット）のストリーム暗号で、CRYPTREC が 2017 年度に発行した『CRYPTREC 暗号技術ガイドライン（軽量暗号）』でも評価対象となっている。結果として、Correlation Cube 攻撃によって初期化段数がフル仕様で 1152 段の「Trivium」を 805 段/835 段に縮退した版に対して、全数攻撃よりも少ない時間（計算量）で攻撃が可能であることを示した。具体的には、805 段の場合は、$2^{47}/2^{51}$ の事前計算、2^{37}／2^{44} のデータによって、2^{77}／2^{73} の時間（計算量）で鍵回復攻撃が可能であること、835 段の場合は 2^{51} の事前計算、2^{44} のデータによって、2^{75} の時間（計算量）で鍵回復攻撃が可能であること、が各々示された。

The Missing Difference Problem, and Its Applications to Counter Mode Encryption [Eurocrypt 2018]

Gaetan Leurent and Ferdinand Aivleyras

本論文では「Missing Difference 問題」を定義し、この問題とブロック暗号のカウンターモード（CTR）の関係を示した。また、任意の「Missing Difference」の場合と、「Missing Difference が低次元のベクトル空間内にあることが判っている場合において、問題を効率的に解くアルゴリズムを示した。これらのアルゴリズムによってカウンターモード（CTR）へのメッセージ回復攻撃がオーダー：$\tilde{O}(2^{n/2})$であること、GMAC や Poly1305 の普遍的偽造攻撃がオーダー：$\tilde{O}(2^{2n/3})$であることが示された。尚、カウンターモード（CTR）は電子政府推奨暗号リストの秘匿モードとして掲載されており、Poly1305 は、推奨候補暗号リストの認証暗号として掲載されている「ChaCha20－Poly1305」の認証機能に相当している。

Fast Near Collision Attack on the Grain v1 Stream Cipher [Eurocrypt 2018]

Bin Zhang, Chao Xu, and Willi Meier

この論文ではストリーム暗号への汎用的な攻撃として FNCA(Fast Near Collision attack)を提案した上で、軽量ストリーム暗号「Grain v1」へ適用し、計算機による実証実験も行っている。「Grain v1」は欧州の eSTREAM プロジェクトにおいて portfolio に掲載された鍵長:80/128 ビット(IV 長:64/80 ビット)のストリーム暗号で、CRYPTREC が 2017 年度に発行した「CRYPTREC 暗号技術ガイドライン(軽量暗号)」でも評価対象となっている。結果として、FNCA によって鍵長 80 ビットの「Grain v1」に対してこれまで知られているどの攻撃結果よりも時間(計算量)の面で最も効率のよい攻撃が可能であり、具体的には、$2^{8.1}$ の事前計算／2^{19} のデータ／2^{28} のメモリによって、$2^{75.7}$ の時間(計算量)で鍵回復攻撃が可能であることが示された。

4. Crypto 2018 の発表

4.1. Crypto 2018 の発表(1 日目)

Lower Bounds on Lattice Enumeration with Extreme Pruning [Crypto 2018]

Yoshinori Aono, Phong Q. Nguyen, Takenobu Seito, and Junji Shikata

Eurocrypt 2010 において Gama らが導入したエクストリーム枝刈りを用いた数え上げ手法は格子縮小アルゴリズムにおいて用いられ記録チャレンジにおいて利用されているが、その効率性の限界については知られておらず、格子ベース暗号の長期セキュリティを見積もる上で課題となっていた。本論文では、成功確率の下限が与えられたときの同手法の下限計算量を初めて与えた。

Dissection-BKW [Crypto 2018]

Andre Esser, Felix Heuer, Robert Kübler, Alexander May, and Christian Sohler

Blum、Kala、Wasserman による準指数時間アルゴリズム BKW は、LPN/LWE セキュリティ評価の基礎となるものであるが、メモリ消費が巨大であるため実用性が限られ、暗号用途での正確な安全性評価が困難であった。本論文では、CRYPTO 2012 における Dinur らの解体テクニックとその一般化を用い、BKW アルゴリズムの時間－空間トレードオフを初めて与えた。例えば、次元 k の LPN を時間計算量 $2^{4k/3\log k}$、空間計算量 $2^{2k/3\log k}$ で解く方法を示す。メモリ消費削減により BKW の量子版である QBKW を初めて提示した。

CAPA: The Spirit of Beaver against Physical Attacks [Crypto 2018]

Oscar Reparaz, Lauren De Meyer, Begül Bilgin, Victor Arribas, Svetla Nikova, Ventzislav Nikov, and Nigel P. Smart

本論文では、まず Tile-Probe-and-Fault Model という、組込システムへの物理攻撃における新しい攻撃モデルを紹介している。これは、複数の「コア」とそれらを結ぶチップ内の配線から成る現代のプロセッサのデザインにより近づけたモデルである。これは、Multi Party Computation (MPC)次

に、CAPA (Combined Countermeasure Against Physical Attacks) と呼ばれる対策を紹介している。この対策は、Tile-Probe-and-Fault Model に対抗することを目的に考えられ、高次サイドチャネルアタック、複数個所を攻撃する故障利用攻撃、及び複合攻撃に耐性を持つことを目指している。Tile-Probe-and-Fault Model はセキュアな Multi Party Computation (MPC) プロトコルに目を向けさせる。実際、CAPA は MPC プロトコルである SPDZ から大いにインスピレーションを受けている。このモデル及び CAPA(これは単に理論的な構造ではなく、実際的な対策を構築するために資すると考えられる)のデモンストレーションのため、CAPA の手法を使用した実証デザインの初期実験を提示している。具体的には、KATAN 及び AES のハードウェア実装と AES の bitslice ソフトウェア実装を対象としている。この論文ではこのデザインが、攻撃者が数十万のトレースを取得できる場合でも second-order DPA に耐えられることを示している。

GGH15 Beyond Permutation Branching Programs: Proofs, Attacks, and Candidates [Crypto 2018]

Oscar Reparaz, Lauren De Meyer, Begül Bilgin, Victor Arribas, Svetla Nikova, Ventzislav Nikov, and Nigel P. Smart

一般分岐プログラムと使用される GGH15 グレード化エンコードスキームについて体系的な研究を行った。一般分岐プログラムは置換分岐プログラムより効率的で、リードワンス設定においてはより表現が豊かであるという事実に触発されたものである。主結果は以下の通り:

・証明:一般分岐プログラムにより計算可能な制約(constraints)/難読化される関数(functions to be obfuscated)に対する、秘密制約擬ランダム関数(private constrained PRF(PseudoRandom Function))とロック可能難読化(lockable obfuscation)の新しい構成。

・攻撃:GGH15 エンコードを使った識別不能性難読化(iO: indistinguishability obfuscation)に対する既存攻撃を拡張。新攻撃は行列の階数を識別として単純に使うため、「階数攻撃(rank attack)」と呼ぶ。本攻撃は、CCS2017 の Halevi、Halevi、Shoup、Stephens-Davidowita による一般リードワンス分岐プログラムの iO 候補を破る。

・証人暗号(Witness Encryption)と iO の候補:上記知見を基に、GGH15 を使った、既存攻撃に耐える証人暗号と iO の単純な候補を提示する。

Improved Division Property Based Cube Attacks Exploiting Algebraic Properties of Superpoly [Crypto 2018]

Qingju Wang, Yonglin Hao, Yosuke Todo, Chaoyun Li, Takanori Isobe, and Willi Meier

キューブ攻撃はストリーム暗号解析において重要なテクニックである。CRYPTO 2017 における藤堂らの分割性質ベースのキューブ攻撃を、より広い範囲のキューブ・インデックス集合に拡張することにより、鍵回復攻撃を 839 段の Trivium、891 段の Kreyvium、184 段の Grain-128a、及び 750 段の Acorn に対して適用することに成功した。

Cryptanalysis via algebraic spans [Crypto 2018]

Adi Ben-Zvi, Arkadius Kalka, and Boaz Tsaban

非可換代数的暗号の証明可能な多項式時間解を得るための手法を提示する。この手法は広く適用可能で、以前の手法より、適用が容易で効率的である。主要な古典的な非可換プロトコルへの適用可能性を示したのち、この手法を、既存手法では解析できない唯一の古典群論ベースの鍵交換プロトコルである、三重分解(Triple Decomposition)鍵交換プロトコルに適用する。

Generic Attacks against Beyond-Birthday-Bound MACs [Crypto 2018]

Gaëtan Leurent, Mridul Nandi, and Ferdinand Sibleyras

本論文では、いくつかの最近のバースデー限界を超える証明可能安全性を持った MAC 構成の安全性について研究する。ここでは、SUM-ECBC、PMAC+、3kf9、GCM-SIV2 とその変種(LigheMAC+、1kPMAC+)のようなダブルブロック内部状態を持つブロック暗号ベースの構成を考える。これらすべての MAC は $2^{2n/3}$ クエリまでのセキュリティが証明されているが、2^n クエリ未満での攻撃は知られていない。

本論文ではダブルブロック MAC に対する暗号解析について、状態の半分における 4 ペアの衝突を持つ 4 つ組メッセージを見つけることをベースにした新しいテクニックを記載している。SUM-ECBC、PMAC+、3kf9、GCM-SIV2 及びその変種に $O(2^{3n/4})$のクエリで 4 つ組を検出する方法を示し、同じクエリの計算量で偽造攻撃を組み立てる方法を示す。これらの攻撃の時間計算量は 2^n を上回るが、これらのスキームは情報理論モデルにおいてフルセキュリティには達していないことを示す。驚くべきことに、LightMAC+に対する本論文の攻撃は内藤による最近のセキュリティ証明を無効にする。

さらに、SUM-ECBC 及び GCM-SIV2 に対する、時間及びデータ計算量が $\tilde{O}(2^{6n/7})$である攻撃のバリアントを提示する。これは知る限りにおいて計算量が 2^n 未満である決定的なバースデー限界を超えるセキュア MAC に対する最初の攻撃である。

付加的な結果として、証明の問題により取り下げられた、3kf9 の変種である 1kf9 に対する誕生日攻撃を示す。

The Curse of Small Domains: New Attacks on Format-Preserving Encryption [Crypto 2018]

Gaëtan Leurent, Mridul Nandi, and Ferdinand Sibleyras

フォーマット保存暗号(Format-preserving encryption (FPE)) は、平文と同じフォーマットの暗号文を生成する。安全な FPE の構築は非常に難しく、最近の攻撃が NIST SP800-38G 標準のセキュリティ欠陥を浮かび上がらせている。このことは、高セキュリティかつ実用的なスキームが存在するかどうかという問題を未解決問題として残した。

本論文では、FPE スキームに対する攻撃の研究を続けている。最初の貢献は、Feistel ベースの FPE(例えば、NIST SP800-38G の FF1/FF3)に対する新しい既知平文メッセージ復元攻撃である。

また、FF3 特有の脆弱性にも着目し、攻撃の効率化を達成している。

本論文ではまた、非 Feistel ベースの FPE に対する攻撃も示している。特に、Cisco によって提案された FNR に対する強力なメッセージ復元攻撃を提示している。Brightwell 及び Smith によって提案され、Protegrity によって商用アプリケーションに組み込まれて配布された DTP 構造のバリアントに対する強力な ciphertext-only attack も提示している。

本論文の攻撃は、FF1/FF3/FNR に対しては小さいドメインにのみ実用的であり、DTP に対してはいかなるドメインに対しても実用的であると結論付けている。DTP は使用せず、ANSI によって推奨されているように小さいドメイン上で FF1/FF3 のダブル暗号化を行うことを推奨している。

4.2. Crypto 2018 の発表（2 日目）

Quantum Attacks against Indistinguishability Obfuscators Proved Secure in the Weak Multilinear Map Model [Crypto 2018]

Alice Pellet-Mary

本論文では、Garg らによって TCC2016 に発表された GMMSSZ 分岐プログラム難読化(branching program obfuscator)が Garg らによる GGH13 多重線形写像（Eurorypt2013）によって具体化された場合に対する量子多項式時間攻撃を提示している。この難読化候補は Miles らによる(Crypto2016)弱い多重線形写像モデルにおいてセキュアであることが証明されている。

本論文の攻撃は、Cramer らによる短主イデアル・ソルバー(short principal ideal solver)(Eurocrypt2016) を使用して GGH13 多重線形写像の秘密の要素を量子多項式時間で復元する。本論文の主な結果は GMMSSZ obfuscator のセキュリティの short principal ideal problem（量子セッティングはこの問題を多項式時間で解くためだけに使われる)への帰結とみられる。

さらに、本論文は同じアイディアが Döttling らによる弱多重線型写像モデルにおいて安全な DGGMM 難読化への量子多項式時間の攻撃の実行にも応用できることを説明している。

Cryptanalyses of Branching Program Obfuscations over GGH13 Multilinear Map from the NTRU Problem [Crypto 2018]

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

本論文では、存在するすべての、GGH13 多重線形写像上の分岐問題（BP）ベースの識別不能性難読化(indistinguishability obfuscation（iO)）候補の暗号解析を提案している。これを達成するため、NTRU ソルバーを使用するプログラム変換(program converting)及び行列ゼロ化(matrix zeroizing)という 2 つの新しいテクニックを紹介する。存在する汎用 BP 難読化（TCC2016）はこの攻撃に対してセキュアでないことを証明する。

本論文の攻撃は、セキュリティの確保のためには、GGH13 の格子次元を以前考えられていたよりはるかに大きく設定しなければならないことを示している。

4.3. Crypto 2018 の発表(4 日目)

Improved Key Recovery Attacks on Reduced-Round AES with Practical Data and Memory Complexities [Crypto 2018]

Achiya Bar-On, Orr Dunkelman, Nathan Keller, Eyal Ronen, and Adi Shamir

イスラエル・バル＝イラン大学の Achiya Bar-on らが AES の縮退版(10 段中 5 段)に対して、データ/メモリ/時間計算量が $2^{22.5}$(従来の 2^{32} よりも約 500 倍高速)で鍵回復攻撃できることを示し、実験により実証も行った。更に 7 段 AES に拡張することにより、18 年振りに AES-192 に対する攻撃記録を破った。縮退版であるため、まだ安全性にはマージンがあるが、今後の攻撃の進展には注意が必要である。

Fast Correlation Attack Revisited - Cryptanalysis on Full Grain-128a, Grain-128, and Grain-v1 [Crypto 2018]

Yosuke Todo, Takanori Isobe, Willi Meier, Kazumaro Aoki, and Bin Zhang

NTT の藤堂らは、LFSR ベースのストリーム暗号に対する高速相関攻撃(FCA: Fast Correlation Attack)を有限体の視点から見ることにより新しい性質およびそれに基づくアルゴリズムにより時間／空間計算量を削減した。この手法を Grain ファミリー(Grain-128a、Grain-128、Grain-v1)に適用することによりすべて解読した。Grain-v1 は eSTREAM のポートフォリオに掲載されており、Grain-128a は ISO/IEC において標準化されており、Grain-128a の完全版に対する暗号解析は初めてである。

A Key-recovery Attack on 855-round Trivium [Crypto 2018]

Ximing Fu, Xiaoyun Wang, Xiaoyang Dong, and Willi Meier

855 段に縮退されたストリーム暗号 Trivium に対する鍵回復攻撃が提示された。秘密鍵と初期ベクトル上のブール多項式からゼロ化と次数の上限を決める手法により、正しい鍵を求める。本手法は NFSR に基づくほとんどのストリーム暗号に適用することができ、855 段の Trivium は 2^{77} の時間計算量で鍵を回復できる。

Bernstein Bound on WCS is Tight - Repairing Luykx-Preneel Optimal Forgeries [Crypto 2018]

Mridul Nandi

Eurocrypt2018 において、Luykx と Preneel は多項式ハッシュベースの Wegman-Carter-Shoup (WCS)authenticators に対するハッシュ鍵復元及び偽造攻撃を発表した。彼らの攻撃は n をハッシュキーのビット長とした時、$2^{n/2}$ 個のメッセージ-タグの組を必要とし、1.34×2^{-n} の成功確率である。Bernstein は Eurocrypt2005 において最大偽造アドバンテージの上限(Bernstein Bound として知られている)を提示した。この上限は $O(2^{n/2})$回のクエリを発行するすべての攻撃者は $O(2^{-n})$の

最大偽造アドバンテージを持てることを意味している。

本論文では、ハッシュキーを、少なくとも確率 1/2 で、$\sqrt{n} \times 2^{\frac{n}{2}}$個のメッセージ-タグの組に基づく攻撃を記述することで、Bernstein Bound が厳密であることを示している。また、本偽造をガロア・カウンター・モード(GCM: Galois Counter Mode)にも拡張している。

5. FDTC 2018 の発表

A Breaking Redundancy-Based Countermeasures with Random Faults and Power Side Channel [FDTC 2018]

Sayandeep Saha, Dirmanto Jap, Jakub Breier, Shivam Bhasin, Debdeep Mukhopadhyay, and Pallab Dasgupta

故障利用攻撃への対策として、暗号演算機能に冗長性を持たせる手法はよく知られているが、本論文ではこの冗長性を逆手に取り、対策回路からのリークを利用した攻撃手法を提案している。暗号演算を 2 系統のロジックで実施し、その結果を比較して結果の正しさを検証する実装に対し、この攻撃では最後に比較するロジックからのサイドチャネルリークを利用する。実際にこの攻撃を AES と PRESENT に対して適用し、128 ビット AES の場合平均して 2^{25} 回の故障注入で鍵を取得できることを示している。実装によっては 2^{25} 回の故障注入は 1 日で行うことが可能であり、このような攻撃は十分現実性があると考えられる。故障利用攻撃への対策を実装する上では、対策回路自体からのリークに注意する必要があると提言している。

6. CHES 2018 の発表

6.1. CHES 2018 の発表(2 日目)

FPGAhammer: Remote Voltage Fault Attacks on Shared FPGAs, suitable for DFA on AES. [CHES 2018]

Jonas Krautter, Dennis R. E. Gnad and Mehdi B. Tahoori

1 個の FPGA での利用できるリソースの増大により、FPGA に複数のユーザのロジックが同居する使い方をするケースが見られるようになってきている。このような状況において、FPGA 内に暗号実装があるときに、同じ FPGA 上にリングオシレータを配置してそれを動作させることで FPGA 全体に影響する電圧降下を引き起こし、暗号実装に誤動作を起こさせる攻撃が提案されている。DRAM において隣接する行への繰り返しアクセスによってメモリのデータを変化させる攻撃である rowhammer と呼ばれる手法が近年注目されているが、この攻撃は原理としては rowhammer と類似した考え方に基づいていることから FPGAhammer という名称をつけている。この攻撃で実際に AES 実装を攻撃し、鍵を復元することに成功している。

6.2. CHES 2018 の発表(4 日目)

Persistent Fault Analysis on Block Ciphers [CHES 2018]

Fan Zhang, Xiaoxuan Lou, Xinjie Zhao, Shivam Bhasin, Wei He, Ruyi Ding, Samiya Qureshi1 and Kui Ren

通常の故障利用攻撃はレーザ等によって一瞬だけ誤動作を引き起こすことによって攻撃するが、攻撃を成功させるためのタイミングが厳しく、また冗長性による対策によって防がれやすい。本論文では持続的なフォールトを起こすことによる攻撃を提案している。典型的にはアルゴリズムに関係する定数を格納する領域を標的とする。S-Box をテーブル参照で実装しているような AES の実装に対し、暗号演算実行前に S-Box テーブルの値を改変し、その改変が 1 回の暗号演算の間持続するようにすることで誤動作を起こさせ、それによって出力された暗号文を解析することで鍵を復元することに成功している。暗号化を 2 回行って比較するような対策に対しても、暗号演算で使用する S-Box の参照テーブルを共有していればこの攻撃は成功する。また、繰り返し DRAM にアクセスすることで隣接する行のメモリを化けさせるrowhammer の手法が持続的フォールトを引き起こすために使えることも言及している。

7. ECC 2018 の発表

7.1. ECC 2018 の発表(2 日目)

Lower-Level Verifications for Cryptographic Software Involving Elliptic Curves and Others [ECC 2018]

Bo-Yin Yang

暗号によるセキュリティを確保するためには、暗号アルゴリズムが正しく実装されていることが必要である。楕円曲線暗号は複雑な数学的構造を持ち、多倍長計算を必要とし、また性能が求められるソフトウェアではアセンブリ言語で記述されることすらある。そのことはプログラムが正しく書かれていることの検証を極めて難しくする。この問題に対応するため、CRYPTOLINE と呼ばれる暗号ソフトウェアの検証ツールを紹介している。このツールによって、楕円曲線暗号が正しく実装されていることの検証が容易に実行可能になることが期待される。

8. Asiacrypt 2018 の発表

8.1. Asiacrypt 2018 の発表(1 日目)

Practical attacks against the Walnut digital signature scheme [Asiacrypt 2018]

Ward Beullens and Simon R. Blackburn

NIST は耐量子計算機暗号アルゴリズムの標準化を開始している。WalnutDSA は標準化が検討されている 20 の提案された署名スキームのひとつである。Walnut は、豊富な代数構造を持つ E-

Multiplication と呼ばれる一方向関数に依存している。本論文は Walnut 暗号システムに対していくつかの実用的な攻撃を行うことでこの構造を悪用できることを示している。この攻撃は実際的に非常に有効であり、証明の偽造、及び NIST に提出された 128 ビットと 256 ビットのセキュリティパラメタと同等な秘密鍵の計算を、それぞれ 1 秒及び 1 分以内に行うことが可能である。

Two attacks on rank metric code-based schemes: RankSign and an IBE scheme [Asiacrypt 2018]

Thomas Debris-Alazard and Jean-Pierre Tillich

RankSign は耐量子計算機暗号の NIST コンペティションに提案されたコードベースの署名スキームであり、さらには、新しい ID ベース暗号(IBE)の基本的な構成要素である。この署名スキームは階数距離(rank metric)をベースにし、128 ビットセキュリティに対して約 10kB という小さい鍵サイズで済む。

本論文では、このスキームに提案されたすべてのパラメーターに対して、代数攻撃で破ることができることを示している。

An efficient structural attack on NIST submission DAGS [Asiacrypt 2018]

Elise Barelli and Alain Couvreur

本論文では、拡大次数 2 の準二項(quasi-dyadic)交互符号(alternant code)を使った符号ベース暗号に対する効率的な鍵回復攻撃を示す。本攻撃により、近年 NIST 耐量子計算機暗号標準化に提出された提案暗号 DAGS を解読することができる。DAGS のセキュリティレベル 128、192、256 と見積もられた鍵は、各々2^{70}、2^{80}、2^{58} の計算量で解読できる。別のアプローチでは計算量の見積もりはできていないが DAGS のあるパラメーターに対しては非常に有効であり、Magma の実装を用いて、256 ビットセキュリティと見積もられた鍵を 1 分以内に解読することができた。

Quantum Lattice Enumeration and Tweaking Discrete Pruning [Asiacrypt 2018]

Yoshinori Aono Phong Q. Nguyen, and Yixin Shen

数え上げ手法は格子アルゴリズムの基礎的なものである。本論文では、量子コンピューター上で数え上げ手法を高速化する方法を示し、NIST 耐量子計算機暗号標準化候補の格子ベース暗号安全性評価への影響を見る。T を数え上げ操作数とすると、本量子数え上げは約$\sqrt{T}$の操作で実行できる。本手法はエクストリーム枝刈り設定における 2 つの最も効率的な数え上げに適用できる。即ち、シリンダー枝刈り(cylinder pruning)と Eurocrypt 2017 において導入された離散枝刈り(discrete pruning)である。本結果は、近年の Montanaro と Ambainis-Kokainis らの量子木(quantum tree)アルゴリズムに基づいている。離散枝刈りの場合には、きわめて重要な微調整が必要となる。即ち、実行時間が本質的に最適であると厳密に証明できるよう前処理を修正するが、それは離散枝刈りにおける主要な未解決問題であった。更に、近接格子ベクトルを求めるより一般的な問題を解くための微調整を与える。

On the Statistical Leak of the GGH13 Multilinear Map and some Variants [Asiacrypt 2018]

Léo Ducas and Alice Pellet-Mary

本論文では、Eurocrypt 2013 で Garg、Gentry、Halevi らにより提案された多重線型写像(MMap: Multi-linear Map)の構成候補(GGH13)とその変形版に対する統計的漏洩に関して体系的な研究を行う。特に、GGH13 の素朴な版の脆弱性を確認する。また、Döttling らによる 2 つの変形版のうち、いわゆる保守的方法と呼ばれているものはそれほど効果がない(即ち、保護されていない版と同じ値を漏らす)ことを示す。幸運なことには、その漏洩は保護されていないものよりはノイズが多いため、単純な攻撃は成功しない。更に、他のすべての方法も秘密に関連した値を漏らすことを注意する。

結論として、本論文では、漏洩がすべての秘密とは関連がないようにする、別の対策を提案する。本対策において、MMap の効率を評価／改善するために、パラメーターサイズに隠された指数を明示し、限定する。

LWE Without Modular Reduction and Improved Side-Channel Attacks Against BLISS [Asiacrypt 2018]

Jonathan Bootle, Claire Delaplace, Thomas Espitau, Pierre-Alain Fouque, and Mehdi Tibouchi

本論文では、モジュラーリダクションのない LWE 問題(ILWE)の解析を行う。即ち、a と e が固定された分布に従うとき、多項式個の$(a, \langle a,s\rangle+e) \in Z^{n+1}$ から、ベクトル $s \in Z^n$ を求める問題である。驚くべきことではないが、この問題は LWE よりもかなり簡単である。即ち、分布に関してそれほど厳しくない条件の下で、e の分散が a の分散よりも超多項式時間ほど大きくなければ、本問題は効率的に解けることを示す。また、s を求めるのに必要なサンプル数のほとんど厳密な境界値を与える。

本論文の動機は、CSS2017 において Espitau らにより提示された格子ベース署名 BLISS に対するサイドチャネル攻撃から生じている。改良したサイドチャネル攻撃は、秘密鍵の 100%に適用することができ(CSS 論文では約 7%)、更に大幅に高速となる。

Quantum Algorithms for the k-xor Problem [Asiacrypt 2018]

Lorenzo Grassi, María Naya-Plasencia, and André Schrottenloher

本論文では、n ビット列の要素が、ランダム関数(もしくは k 個のランダム関数) $H: \{0,1\}^n \rightarrow \{0,1\}^n$ により生成されるときに、k-xor 問題(一般化された誕生日問題)を量子設定で研究する。限られた量子メモリ(O(n)量子ビット:Grover の探索アルゴリズムに必要なものと同じ設定)しか使用できない場合および指数オーダーの量子ビットを使用できる場合の 2 種類のシナリオを考慮する。

どちらの場合においても、既知の最良量子時間計算量を与える。特に、3-xor アルゴリズムを大幅に改良することができた。限られた量子ビットの場合には現状可能な量子衝突探索よりはるかに良い計算量を得、指数オーダーの量子メモリにアクセスできる場合には計算量を $O(2^{n/3})$にすること

ができた。これは量子衝突探索の良く知られた下界を下回る結果である。暗号応用(ストリーム暗号への相関攻撃等)におけるこれらの結果の重要性も記述する。

Hidden Shift Quantum Cryptanalysis and Implications [Asiacrypt 2018]

Xavier Bonnetain and María Naya-Plasencia

Eurocrypt 2017 において、Simon の量子攻撃に対する対策として、即ち、ビット毎加算をモジュラー加算等他の演算に置き替える微修正が発表された。本論文では、そのフォローアップを行う。

初めに、モジュラー加算を考慮した場合に Simon の代わりに適用できるアルゴリズムとなる隠れシフト問題(Hidden Shift Problem)を解く Kuperberg アルゴリズムを改良／一般化した新しいアルゴリズムを開発した。改良アルゴリズムにより、FSE 2005 において提案され、広く使われ量子安全と主張されている Poly 1305 への重ね合わせ(superposition)モデルにおける量子攻撃を行うことができ、FX 構成への微修正の影響を解析することにより未解決問題に答えることができた。また、アルゴリズムの一般化により、並列モジュラー加算により隠れシフト問題を解く初めての量子アルゴリズムを提案した。その計算量は、極端な場合に Simon と Kuperberg のそれに一致する。理論解析を検証し、アルゴリズムのコストを具体的に見積もるために、シミュレーションにより計算量見積もりを有効にした。

最後に、提案された微修正の影響および実用性を評価するために、具体的なパラメーターにおいて、いくつかの古典的な対象鍵構成の安全性を解析した。結論としては、微修正は効率的ではないようである。

8.2. Asiacrypt 2018 の発表（2 日目）

Programming the Demirci-Selçuk Meet-in-the-Middle Attack with Constraints [Asiacrypt 2018]

Danping Shi Siwei Sun Patrick Derbez Yosuke Todo Bing Sun Lei Hu

中国科学院の Shi、NTT の藤堂らによる制約プログラム（以下 CP: Constraind Programing)ベースの暗号解析改良が発表された。CP ベースのアプローチは既存の SAT（SATisfiability Problem）ソルバー等を利用し暗号解析を自動化するものであるが、一方で国際会議 FSE2008 において発表された Demirci と Selçuk らの手法は、自動化ではなく専用探索アルゴリズムにより縮退版 AES に対する解読記録を達成した。今回の Shi らの手法は、新しいモデリングにより自動化で解ける範囲を広げるものであり、SKINNY、TWINE、LBlock 等の軽量暗号に適用され、各々解読記録を更新したが、AES への適用では自動化されていない専用部分が残っているため記録達成には至っていない。

New MILP Modeling: Improved Conditional Cube Attacks on Keccak-based Constructions [Asiacrypt 2018]

Ling Song, Jian Guo, Danping Shi, and San Ling

シンガポール南洋理工大学/中国科学院の Song らにより、新しい MILP(Mixed Integer Linear Programming)モデル化による、Keccak(SHA-3)ベース認証等に対するキューブ攻撃の改良が発表された。SHA-3 から構成されるメッセージ認証コードである KMAC(NIST SP 800-135 で規定される)に適用し、7 段 KMAC128 および 9 段 KMAC256 への攻撃に成功した。段数のセキュリティマージンは十分に残っており、まだ実用的な脅威とはなっていないが、今後の攻撃の進展には注意が必要である。

On the Concrete Security of Goldreich's Pseudorandom Generator [Asiacrypt 2018]

Geoffroy Couteau Aurélien Dupin Pierrick Méaux Mélissa Rossi, and Yann Rotella

ローカルな疑似乱数生成器は短いランダムビット列を長い疑似ランダムビット列に拡張し、それぞれの出力ビットが入力ビットの定数 d に依存するようにすることを可能にする。その極めて効率的な機能のため、この興味深いプリミティブは暗号において幅広く応用されている。多項式レジームでは、シード長が n で出力長が n^s (s>1)であり、Goldreich's PRG として知られている唯一知られている解は、単純な d 変数の述語を公開のサイズ d のシードのサブセットに適用することで処理を進める。

Goldreich's PRG のセキュリティは徹底的に研究されているが、具体的なセキュリティと効率性についてはほとんど知られていない。数多くの理論的応用とそれらの一部への実用的な具現化を得る希望に触発されて、著者は Goldreigh's PRG の具体的なセキュリティの研究を開始し、暗号解析に対する耐性を評価した。その過程において、新しい guess-and-determine スタイルの攻撃を考案し、ローカル疑似乱数生成器候補のより精密な方法でのセキュリティ基準を精緻化している。

Cryptanalysis of MORUS [Asiacrypt 2018]

Tomer Ashur, Maria Eichlseder, Martin M. Lauridsen, Gaëtan Leurent, Brice Minaud, Yann Rotella, Yu Sasaki, and Benoît Viguier

MORUS は CAESAR コンペティションに応募された高性能認証暗号であり、ファイナリストに選出されている。MORUS には MORUS-640(128 ビット鍵)、MORUS-1280(128 ビット鍵／256 ビット鍵)と 3 つのバージョンがあり、安全性は鍵のサイズに一致すると主張されている。

本論文では、フルバージョンの MORUS の鍵ストリームに線型相関を示す。256 ビット鍵 MORUS-1280 に対し、2^{152} 暗号化で 2^{-76} 相関が得られることが示された。

CRYPTREC Report 2018
(暗号技術評価委員会報告 CRYPTREC RP-2000-2018)

不許複製 禁無断転載

発行日　2019年 6月 28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