CRYPTREC Report 2015

平成 28 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

「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た暗号技術評価委員会の 2015 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。今年度は暗号技術検討会座長が今井秀樹座長から松本勉座長へと引き継がれた CRYPTREC 新体制発足の節目の年であった。暗号技術は 2015 年 9 月に閣議決定された「サイバーセキュリティ戦略」においてサイバーセキュリティのコア技術として国が維持すべき重要な技術という位置づけになっている。このような情勢の中、暗号技術検討会の活動の一環として、「CRYPTREC の在り方に関する検討グループ」が発足し、その後、「重点課題検討タスクフォース」が設置された。これまで取り組んできた暗号アルゴリズムのセキュリティ（安全性）確保の推進に加え、暗号アルゴリズムが利用されている情報システム全体のセキュリティ確保に向けた貢献が求められていることから、暗号技術評価委員会に深くかかわる課題も議論された。

暗号技術評価委員会の活動としては、1）暗号技術の安全性及び実装に係る監視及び評価、2）暗号技術に関する注意喚起レポートの公表、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が確認された。本年度、当該委員会委員長については今井秀樹委員長の職責を小生が引き継ぐことになった。 1）については、SHA-3 等のハッシュ関数を CRYPTREC 暗号リストへ追加するための安全性・実装性能に関する最終的な判断を行った。 2）については、推奨候補リストに掲載されているブロック暗号 MISTY1 への解析論文が公開されたことを受けて速報を公開し、さらに、外部評価を実施し、当面、MISTY1 の安全性に現実的な脅威は生じないことを確認して情報発信を行った。併せて、今後の研究で攻撃が進展する可能性についても専門家の見解を調べた。また、ハッシュ関数 SHA-1 の衝突困難性の解析結果について、SHA-1 の衝突発見に直接つながるものではないものの、一連の研究動向から、近い将来に SHA-1 の衝突が発見されるという警鐘を鳴らした。3）については、2 つのワーキンググループ（以下、WG）を設置し、暗号解析評価 WG では、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の評価に基づく予測図の更新を行い、また、離散対数問題、多重線形写像、及び難読化技術の最新動向に関する調査を行った。軽量暗号 WG では、IoT 等において軽量暗号の活用が期待されることから、軽量暗号の方式を選択・利用する際の技術的判断に資すること、今後の利用促進をはかることを目的とした軽量暗号技術に関するガイドラインの次年度発行を目指して作成方針を決定した。

発足以来 15 年にわたる CRYPTREC の活動はセキュアな ICT 社会の実現に貢献し、世界的にも通用する CRYPTREC ブランドの信頼の醸成につながっていると認識している。今後も社会の情勢を踏まえ、新設された重点課題検討タスクフォースとも連携し、社会のニーズに対して、暗号技術の安全性という観点から必要とされる活動を展開していきたいと考えている。

これら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説明してある。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。

http://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。

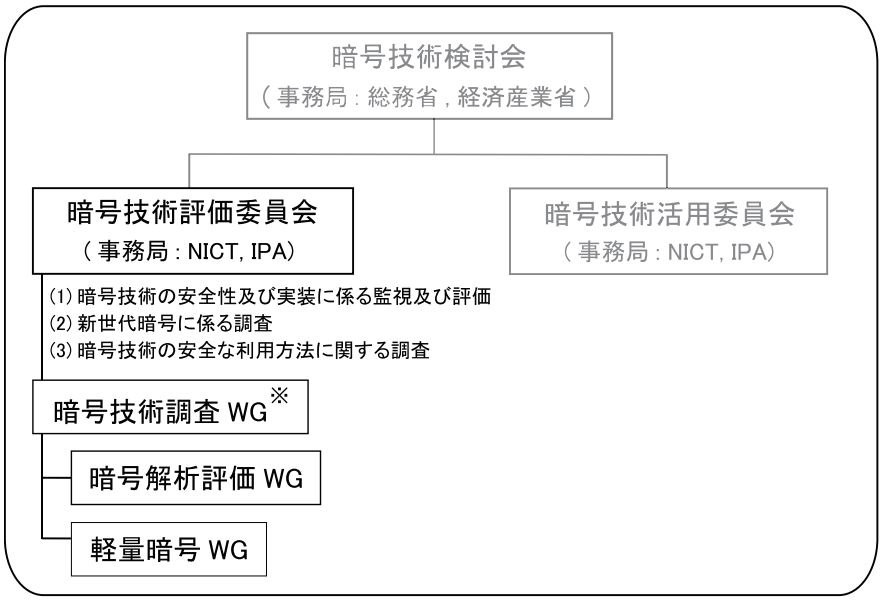
【問合せ先】　info @ cryptrec.go.jp

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。2015 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」及び「軽量暗号 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：

- 多重線形写像、難読化及び離散対数問題の困難性に関する調査
- リソースの制限が厳しいデバイスにも実装可能な軽量暗号に関する調査

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	国立大学法人電気通信大学 大学院 教授
委員	岩田 哲	国立大学法人 名古屋大学 大学院 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	佐々木 良一	東京電機大学 教授
委員	高木 剛	国立大学法人九州大学 教授
委員	手塚 悟	東京工科大学 教授
委員	本間 尚文	国立大学法人東北大学 大学院 准教授
委員	松本 勉	国立大学法人横浜国立大学 大学院 教授
委員	松本 泰	セコム株式会社 IS 研究所 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	国立大学法人秋田大学 大学院 教授
委員	渡邊 創	国立研究開発法人産業技術総合研究所 上級主任研究員

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	国立大学法人九州大学 教授
委員	青木 和麻呂	日本電信電話株式会社 主任研究員
委員	太田 和夫	国立大学法人電気通信大学 大学院 教授
委員	草川 恵太	日本電信電話株式会社 研究員
委員	國廣 昇	国立大学法人東京大学 大学院 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	安田 雅哉	国立大学法人九州大学 准教授

暗号技術調査ワーキンググループ(軽量暗号)

主査	本間 尚文	国立大学法人東北大学 大学院 准教授
委員	青木 和麻呂	日本電信電話株式会社 主任研究員
委員	岩田 哲	国立大学法人名古屋大学 大学院 准教授
委員	小川 一人	日本放送協会 上級研究員
委員	小熊 寿	株式会社トヨタ IT 開発センター シニアリサーチャー
委員	崎山 一男	国立大学法人電気通信大学 大学院 教授
委員	渋谷 香士	ソニー株式会社
委員	鈴木 大輔	三菱電機株式会社 主席研究員
委員	成吉 雄一郎	ルネサスエレクトロニクス株式会社 主任技師
委員	峯松 一彦	日本電気株式会社 主任研究員

委員	三宅 秀享	株式会社東芝 研究主務
委員	渡辺 大	株式会社日立製作所 主任研究員

オブザーバー

大川 伸也	内閣官房内閣サイバーセキュリティセンター[2015 年 12 月まで]
久保山 拓	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
眞弓 隆浩	内閣官房内閣サイバーセキュリティセンター[2015 年 12 月から]
森安 隆	内閣官房内閣サイバーセキュリティセンター
中山 慎一	警察庁 情報通信局
新家 研介	総務省 行政管理局
内海 隆明	総務省 自治行政局 住民制度課
筒井 邦弘	総務省 情報流通行政局
近藤 直光	総務省 情報流通行政局[2015 年 7 月まで]
丸橋 弘人	総務省 情報流通行政局[2015 年 8 月から]
中村 一成	総務省 情報流通行政局[2015 年 7 月まで]
今野 孝紀	総務省 情報流通行政局
佐久間 明彦	外務省 大臣官房
岩永 敏明	経済産業省 産業技術環境局[2015 年 6 月まで]
加藤 誠司	経済産業省 産業技術環境局[2015 年 7 月から]
中野 辰実	経済産業省 商務情報政策局
室井 佳子	経済産業省 商務情報政策局[2015 年 4 月まで]
中村 博美	経済産業省 商務情報政策局[2015 年 5 月から]
谷口 晋一	防衛省 運用企画局[2015 年 4 月まで]
松本 裕悟	防衛省 整備計画局[2015 年 4 月から]
多賀 文吾	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 （平和昌、盛合志帆、野島良、大久保美也子、黒川貴司、金森祥子、笠井祥、大川晋司）

独立行政法人情報処理推進機構（伊藤毅志[2015 年 7 月まで]、頓宮裕貴[2015 年 8 月から]、近澤武、小暮淳、大熊建司、神田雅透、稲垣詔喬、初田瑠里[2016 年 1 月まで]、兼城麻子[2016 年 2 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] 等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、2005 年度に実施されたハッシュ関数の安全性評価に基づき、2006 年 6 月に SHA-1 の安全性に関する見解を、2006 年度に実施された素因数分解問題の困難性に関する評価に基づき、RSA1024 の安全性の評価結果をそれぞれ公表した。これらの見解に基づき、情報セキュリティ政策会議において「政府機関の情報システムにおいて使用される暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針」[2] が 2008 年度に決定されるに至った。また、CRYPTREC 暗号リスト策定中に実施した安全性評価において、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、128-bit key RC4 は SHA-1 とともに CRYPTREC 暗号リストの運用監視暗号リストに記載されることになった。現在、暗号技術評価委員会では、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、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いる。

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 15 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] http://www.cryptrec.go.jp/images/cryptrec_ciphers_list_2016.pdf

[2] http://www.nisc.go.jp/active/general/pdf/crypto_pl.pdf (2008 年 4 月 22 日決定情報セキュリティ政策会議決定)

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[3]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)」[4](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 年度以降は、暗号技術調査ワーキンググループ（暗号解析評価）及び暗号技術調査ワーキンググループ（軽量暗号）の 2 つのワーキンググループが設置されている。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、

[3] http://www.cryptrec.go.jp/list_2003.html
[4] http://www.cryptrec.go.jp/list.html

「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。

http://www.cryptrec.go.jp/report.html

なお、2009 年度は、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[5]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[6]掲載の暗号技術に対する考え方[7]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

[5] http://www.cryptrec.go.jp/topics/cryptrec_201212_listpc.html
[6] 2003 年 2 月 20 日に策定されたものを指す。
[7] たとえば、暗号技術検討会 2008 年度報告書を参照のこと。
http://www.cryptrec.go.jp/report/c08_kentou_final.pdf

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。

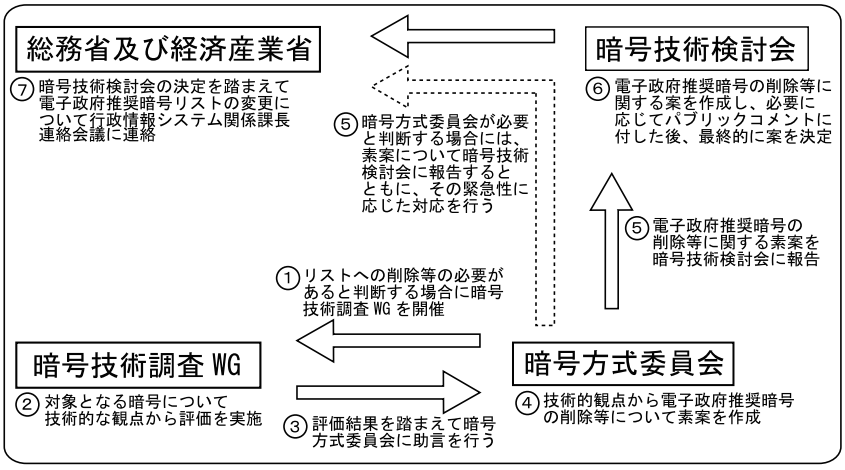


図1.1：電子政府推奨暗号の削除等の手順[8]

(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。

[8] 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。

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 2015 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

Crypto 2015 において、NTT の藤堂氏が CRYPTREC 暗号の推奨候補暗号リストに掲載されている 64 ビットブロック暗号 MISTY1 に対する解析結果を発表し、鍵の総当りより少ない暗号化 $2^{107.9}$ 回の計算量で攻撃可能であることを示した。同ランプセッションにおいて Bar-On は解読に必要な計算量を $2^{69.5}$ 回まで減らせることを示した。両研究とも、従来から知られている Integral Analysis という攻撃法に、Division Property という新規の概念を導入した改良法を利用している。これらの成果において、解読に必要な（平文，暗号文）の可能な組数は 2^{64} の半分以上と膨大であることから、現実的な脅威には至っていないと考えられる。Division Property を利用した攻撃研究は進展中であり、他のブロック暗号への適用など、今後の動向が注目される。本件については、2.2.1 節を参照のこと。

CRYPTREC 暗号リスト掲載のストリーム暗号について、安全性については特に大きな変更はなかった。

2.1.2. 公開鍵暗号に関する安全性評価について

公開鍵暗号の安全性の根拠とする数学的問題に関しては、離散対数問題(DLP: Discrete Logarithm Problem)の解読法に引き続き進展があり、また、楕円曲線離散対数問題(ECDLP: Elliptic Curve DLP)に関しても、新たな知見が得られた。

DLP に関しては、Eurocrypt 2015 / Asiacrypt 2015 における Barbulescu らの攻撃、Eurocrypt 2015 における Pierrot の攻撃、Asiacrypt 2015 における Guillevic の攻撃において、計算量削減・高速化の進展が見られたが、電子政府推奨暗号のパラメータは攻撃の適用条件に当てはまらない。

ECDLP に関しては、Asiacrypt 2012 において Petit らは、ある仮定(「First Fall Degree」仮定と呼ばれる)の元に楕円曲線暗号の解読計算量が準指数時間オーダーになることを示したが、Crypto 2015 においてアメリカ・南カリフォルニア大学の Huang 教授らは、この仮定の正当性に疑問を投げかけるデータを示し、解読計算量評価はより慎重に行うべきであると主張した。本論文の結果が正しいとすると、楕円曲線暗号は Petit らによる評価結果より安全であると考えられる。また、PKC 2016 において、Petit らは、拡大体上の ECDLP

に対する指数計算法を素体上の ECDLP に適用する方法を提案したが、解読できるパラメータは小さなものであり、現実的脅威には至っていない。

2.1.3. ハッシュ関数に関する安全性評価について

広く利用されているハッシュ関数 SHA-1 に対し、攻撃の進展が見られた。2015 年 8 月の Crypto 2015 において、フランスの Karpman, Peyrin, Stevens らオランダ・フランス・シンガポールの共同研究チームは SHA-1 に対し、Free-Start 衝突攻撃の条件で 76 段(フルは 80 段)を約 5 日で攻撃できることを示した[1]。Free-Start とは仕様で固定されている初期ベクターを可変とすることで難度を下げた攻撃法であり、これを 80 段まで伸ばしただけでは SHA-1 の衝突発見には至らなかった。しかしながら、2015 年 10 月には、同チームは Free-Start 衝突攻撃の条件ではあるものの、SHA-1 のフルラウンド（全 80 ステップ中 80 ステップ）に対し、初めて衝突発見に成功したと発表した[2]。本件については、2.2.2 節を参照のこと。

2.2. 注意喚起レポートについて

2.2.1. MISTY1 の安全性について

CRYPTREC暗号リストの推奨候補暗号リストに掲載されているMISTY1に対する新たな解析結果を示した論文が、国際暗号学会（International Association for Cryptologic Research (IACR)）が主催する国際会議Crypto 2015で採録され、国際会議に先立ち、その詳細がIACR ePrint Archiveにて発表された。この論文では、Integral Cryptanalysisという従来から知られているブロック暗号に対する攻撃法の解読計算量を新たな手法で改良し、仕様通りのMISTY1の128ビットの鍵が、鍵の全数探索（すべての鍵の総当たり）よりも少ない解読計算量で導出できることが初めて示された。

表2.1：Integral Cryptanalysis によるMISTY1の解読計算量

	解読に必要なデータ量	解読に必要な計算量
藤堂による解析結果	$2^{63.58}$	2^{121}
藤堂による解析結果	$2^{63.994}$	$2^{107.9}$
Bar-Onによる解析結果	2^{64}	$2^{69.5}$

[1] Pierre Karpman, Thomas Peyrin, Marc Stevens, “Practical Free-Start Collision Attacks on 76-step SHA-1”, CRYPTO 2015. LNCS 9215, pp. 623-642. Springer, 2015

[2] Marc Stevens, Pierre Karpman, and Thomas Peyrin, “Freestart collision for full SHA-1”. IACR ePrint Archive. https://eprint.iacr.org/2015/967

このため、CRYPTREC の Web ページに注意喚起の意味で「64 ビットブロック暗号 MISTY1 の安全性について」（平成 27 年 7 月 16 日）[3]及び「64 ビットブロック暗号 MISTY1 の安全性について（続報）」（平成 27 年 8 月 12 日）[4]を公表した。

64ビットブロック暗号MISTY1の安全性について

平成27年7月16日
CRYPTREC暗号技術評価委員会

CRYPTREC暗号リストの推奨候補暗号リスト[1]に掲載されている64ビットブロック暗号MISTY1 に対する新たな解析結果を示した論文[2]が、国際暗号学会 （International Association for Cryptologic Research (IACR)）が主催する国際会議 CRYPTO 2015[3]で採録され、国際会議に先立ち、その詳細がIACR ePrint Archive[4]にて発表されました。

この論文では、Integral Cryptanalysisという従来から知られているブロック暗号に対する攻撃法の解読計算量を新たな手法で改良し、仕様通りのMISTY1の128ビットの鍵が、鍵の全数探索（すべての鍵の総当たり）よりも少ない解読計算量で導出できることが初めて示されました。この論文では、解読に必要なデータ量と計算量にトレードオフのある2種類の攻撃法が示されており、下記の表にその解読計算量を示します。

これらの攻撃法において、解読に必要なデータ量は$2^{63.58}$, $2^{63.994}$と非常に多く、64ビットブロック暗号では鍵を固定すると2^{64}通りの（平文,暗号文）の組しか存在しないことから、ほとんどすべての（平文,暗号文）の組を集める必要があること、かつ、解読に必要な計算量も2^{121}, $2^{107.9}$と非常に多いことから、現実的な脅威につながることはないものと考えられます。本件に関する調査結果については、今後、CRYPTREC Webサイトにて報告する予定です。

表：Integral Cryptanalysis によるMISTY1の解読計算量 （[2]による）

	解読に必要なデータ量[5]	解読に必要な計算量[6]
MISTY1 (full round)	$2^{63.58}$	2^{121}
MISTY1 (full round)	$2^{63.994}$	$2^{107.9}$

[1] http://www.cryptrec.go.jp/images/cryptrec_ciphers_list_2013.pdf
[2] Yosuke Todo, “Integral Cryptanalysis on Full MISTY1”, to appear in the proceedings of CRYPTO 2015.
[3] http://www.iacr.org/conferences/crypto2015/
[4] https://eprint.iacr.org/2015/682
[5] 1単位は（平文,暗号文）の1組で、平文、暗号文ともに64ビットである。本攻撃では、攻撃に使える条件を満たす平文を選択し、それに対応する暗号文の組を収集する必要がある（選択平文攻撃）。
[6] 1単位は1回の暗号化に要する計算量である。128ビット鍵の全数探索（すべての鍵の総当たり）の計算量は2^{128}である。

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

64ビットブロック暗号MISTY1の安全性について（続報）

平成27年8月12日
CRYPTREC暗号技術評価委員会

CRYPTREC暗号リストの推奨候補暗号リスト[1]に掲載されている64ビットブロック暗号MISTY1 に対する解析結果を示した論文が発表され[2]、CRYPTRECより本論文に対する見解[3]を7月16日に出したところですが、このたび、この解読計算量をさらに削減した新たな解析結果が国際暗号学会 （International Association for Cryptologic Research (IACR)）のアーカイブサイトIACR ePrint Archiveにて7月30日に発表されました[4]。

新たな解析結果では、解読に必要なデータ量は2^{64}と非常に多く、すべての（平文,暗号文）の組を集める必要があるものの、$2^{69.5}$回の暗号化演算に相当する現実的な計算量でMISTY1の128ビットの鍵を導出することができると示されています。しかしながら、この攻撃は、解読に必要なデータ量が膨大であることから、現実的な脅威ではないと考えられます。CRYPTREC では、MISTY1の安全性に関して引き続き調査を行い、CRYPTREC Webサイトにて報告する予定です。

表：Integral Cryptanalysis によるMISTY1の解読計算量

	解読に必要なデータ量[5]	解読に必要な計算量[6]
藤堂による解析結果[2]	$2^{63.58}$	2^{121}
藤堂による解析結果[2]	$2^{63.994}$	$2^{107.9}$
Bar-Onによる解析結果[4]	2^{64}	$2^{69.5}$

[1] http://www.cryptrec.go.jp/images/cryptrec_ciphers_list_2013.pdf
[2] Yosuke Todo, “Integral Cryptanalysis on Full MISTY1”, Advances in Cryptology – CRYPTO 2015, Lecture Notes in Computer Science, Volume 9215, pages 413–432. https://eprint.iacr.org/2015/682
[3] http://www.cryptrec.go.jp/topics/cryptrec_20150716_misty1_cryptanalysis.html
[4] Achiya Bar-On, “A 2^{70} Attack on the Full MISTY1”. https://eprint.iacr.org/2015/746
[5] 1単位は（平文,暗号文）の1組で、平文、暗号文ともに64ビットである。本攻撃では、攻撃に使える条件を満たす平文を選択し、それに対応する暗号文の組を収集する必要がある（選択平文攻撃）。
[6] 1単位は1回の暗号化に要する計算量である。128ビット鍵の全数探索（すべての鍵の総当たり）の計算量は2^{128}である。

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

その後、暗号技術評価委員会において、NTT の藤堂氏に安全性評価を依頼した。その結果、以下のような評価結果を藤堂氏より得た。

（１） MISTY1 について

A） 本レポートで報告した攻撃の実行には，少なくとも$2^{63.58}$ 個の選択平文暗号文ペアを収集する必要がある．またBar-On による最適化により，計算量は$2^{69.5}$ まで下がったが，$2^{63.58}$ 個以上の選択平文を要求する．したがって現在知られている2つの解析手法は共にMISTY1 の現実的な利用における安全性を脅かすものではない．

B） 一方でMISTY1の今後の新規利用は控えるべきである．MISTY1のセキュリティレベルが70ビット前後まで低下したことは事実であり，より優れた暗号方式の採用が推奨される．

[3] http://www.cryptrec.go.jp/topics/cryptrec_20150716_misty1_cryptanalysis.html
[4] http://www.cryptrec.go.jp/topics/cryptrec_20150812_misty1_cryptanalysis.html

C) MISTY1のIntegral 特性を改良する傍証がいくつかあり，攻撃手法の改良可能性がある．

（２） 電子政府推奨暗号リスト掲載の共通鍵暗号への適用

A) AESについてDivision Propertyの活用により従来手法を上回るIntegral特性が見つかったが、効率よく鍵回復を実行する方法は未解決であり、現段階ではAESの安全性に影響はない。その他、Camellia，3-key Triple DES，KCipher-2については、最新のIntegral攻撃手法を適用する方針について考察がなされている。

審議の結果、暗号技術評価委員会としては、MISTY1の安全性については、解読に必要なデータ量が膨大（2^{64}）であることから、現実的な脅威ではないと今年度は判断した。しかしながら、来年度もIntegral攻撃の最新動向については検討を継続し、技術的根拠が揃った時点で新たな見解を示すこととなった。

2.2.2. SHA-1 の安全性について

2015 年 10 月 8 日に、CWI(オランダ)、INRIA(フランス)、NTU(シンガポール)の共同研究チームは、国際暗号学会(International Association for Cryptologic Research (IACR))のアーカイブサイト IACR ePrint Archive に論文を公開し、ハッシュ関数 SHA-1 のフルラウンド(全 80 ステップ中 80 ステップ)に対して、仕様より緩い条件下ながら初めて衝突発見に成功したと発表した。このため、CRYPTREC の Web ページに注意喚起の意味で「SHA-1 の安全性について」（平成 27 年 12 月 18 日）[5]を公表した。

SHA-1の安全性について

平成27年12月18日
CRYPTREC暗号技術評価委員会

2015年10月8日に、CWI(オランダ)、INRIA(フランス)、NTU(シンガポール)の共同研究チームは、ハッシュ関数SHA-1のフルラウンド(全80ステップ中80ステップ)に対して、仕様より緩い条件下ながら初めて衝突発見に成功したと発表しました[1]。本発表のもとになっている論文は国際暗号学会(International Association for Cryptologic Research (IACR))のアーカイブサイト IACR ePrint Archiveで公開されています[2]。

今回の発表された内容は、SHA-1の衝突発見に直接つながるものではありませんが、SHA-1の衝突発見に至るまでの節目となる出来事、マイルストーンの1つであり、近い将来にSHA-1の衝突が発見されるという予測を強く裏付けるものです。当委員会としては、従前通り、SHA-1に関する移行対策を実施して頂きたいと考えています。

当委員会(当時は暗号技術監視委員会)では、2005年にSHA-1に対する衝突発見アルゴリズムが論文発表された後、安全性評価を行った結果、近い将来この攻撃アルゴリズムが実際に実装可能になり、衝突発見困難性に対して脅威になるものと判断しました[3]。その後、情報セキュリティ政策会議から、2008年にSHA-1に関して移行指針[4]が発表されています。現在、CRYPTRECでは、SHA-1を「CRYPTREC暗号リスト」の「運用監視暗号リスト」[5]に掲載し、互換性維持以外の目的での利用を推奨していません。また、SHA-1の用途ごとの具体的な利用指針として、「CRYPTREC暗号技術ガイドライン(SHA-1)」[6]を公開しています。

引き続き、CRYPTRECでは、暗号技術などの監視・評価を行い、SHA-1の取り扱いなどについて変更が生じた場合は、CRYPTREC Web サイトなどを通じてお知らせします。

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

【参考文献】

[1] Press Release “Researchers urge: industry standard SHA-1 should be retracted sooner”, CWI, Inria, NTU, October 8, 2015. https://www.cwi.nl/news/2015/researchers-urge-industry-standard-sha-1-should-be-retracted-sooner

[2] Marc Stevens, Pierre Karpman, and Thomas Peyrin, “Freestart collision for full SHA-1”, IACR ePrint Archive. https://eprint.iacr.org/2015/967

[3] CRYPTREC Report 2005 「暗号技術監視委員会報告」(2006年3月): http://www.cryptrec.go.jp/report/c05_wat_final.pdf

[4] 「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22日 情報セキュリティ政策会議決定、平成24年10月26日 情報セキュリティ対策推進会議改定) : http://www.nisc.go.jp/active/general/pdf/angou_ikoushishin.pdf

[5] 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) (2013年3月1日 総務省・経済産業省、2015年3月27日改定) : http://www.cryptrec.go.jp/images/cryptrec_ciphers_list_2015.pdf

[6] CRYPTREC暗号技術ガイドライン(SHA-1) (2014年3月): http://www.cryptrec.go.jp/report/c13_tech_guideline_SHA-1_web.pdf

[5] http://www.cryptrec.go.jp/topics/cryptrec_20151218_sha1_cryptanalysis.html

2.3. Post Quantum Cryptography に関する動向について

NIST から、NISTIR 8105 DRAFT Report on Post-Quantum Cryptography[6]というレポートが出され、耐量子計算機暗号に関する見解や標準化に関する計画が公表されている。NIST のこのレポートでは、もし大規模な量子計算機が実現した際には Shor や Grover のアルゴリズムによって現在利用されている多くの暗号技術が解読されてしまう場合があることから、大規模な量子計算機がいつ実現されるかは不明であるものの、現行の計算機及び量子計算機の両方に耐性がある情報システムの実現に向けて準備する必要があると主張されている。また、国際会議 PQCrypto 2016(2016 年 2 月 24 日～26 日、九州・福岡市)[7]の招待講演において、Dustin Moody 氏(NIST)による Post-Quantum Cryptography: NIST's Plan for the Future[8]と題する講演が行われ、これから NIST として耐量子計算機暗号の標準化を開始するという発表があった。表 2.2 は、NIST がこれまでに公表している公募計画の概要である。

表 2.2：NIST による耐量子計算機暗号の公募の概要

公募カテゴリ：	公開鍵暗号（守秘、署名、鍵共有） 各カテゴリから少なくとも 1 つのアルゴリズムを選出するが、AES や SHA-3 のようなアルゴリズムを唯一つ選択するようなものではない。	
スケジュール：	Fall 2016：	Call For Proposals のパブリックコメント開始
	End of 2016：	Call For Proposals の確定
	End of 2017：	Submission の〆切
解析フェーズ：	3 年から 5 年間	
ワークショップ：	Early 2018：	Workshop の開催(応募者のプレゼンテーション)
	解析フェーズ中に、1、2 回開催予定。	

（出典元：D. Moody, Post-Quantum Cryptography: NIST's Plan for the Future）

2.4. 暗号アルゴリズムの脆弱性に関する情報発信フローについて

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暗号技術検討会が設置した重点課題検討タスクフォースで議論され、下記に示す情報発信フロー(図 2.1)にて取り扱うことが提案され、第 2 回暗号技術評価委員会にて報告された。本提案は、第 2 回暗号技術検討会にて承認された。

[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

[6] http://csrc.nist.gov/publications/drafts/nistir-8105/nistir_8105_draft.pdf
[7] https://pqcrypto2016.jp
[8] https://pqcrypto2016.jp/data/pqc2016_nist_announcement.pdf

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。

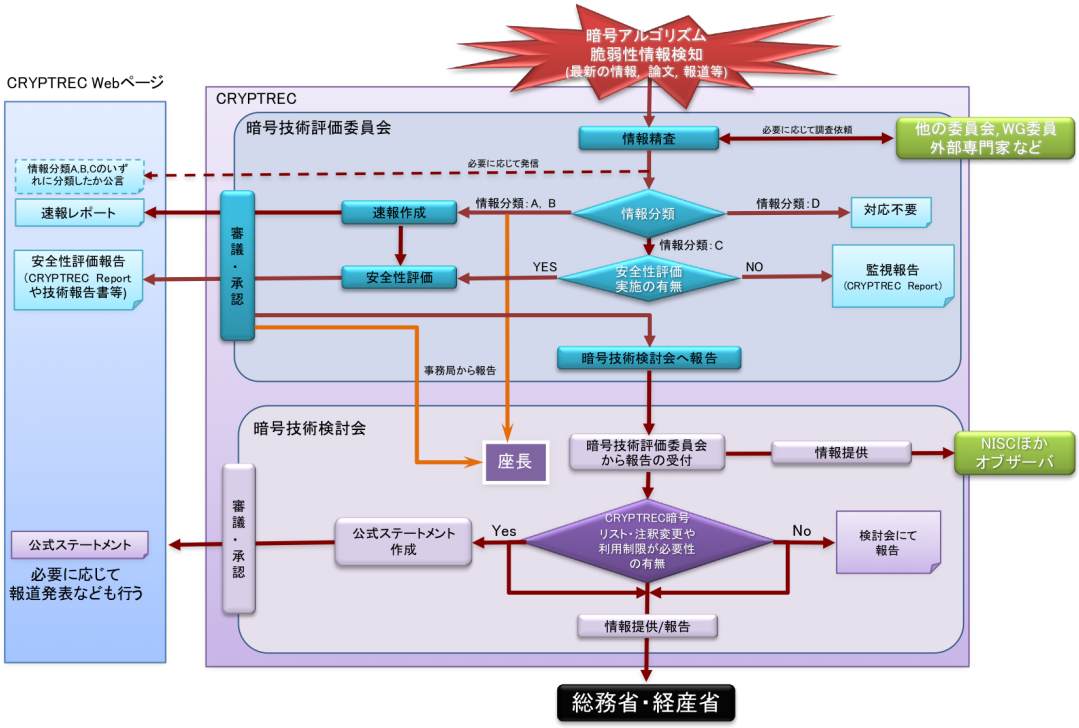


図 2.1　暗号アルゴリズムの脆弱性に関する情報発信フロー

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2.3に示す通りである。

表 2.3　国際会議への参加状況

学会名・会議名		開催国・都市	期間
Eurocrypt 2015	International Conference on the Theory and Applications of Cryptographic Techniques	ブルガリア・ソフィア	2015 年 4 月 27 日～2015 年 4 月 30 日
Lightweight Cryptography Workshop 2015	Lightweight Cryptography Workshop 2015	米国・ゲイザースバーグ	2015 年 7 月 20 日～2015 年 7 月 21 日
Crypto 2015	International Cryptology Conference	米国・サンタバーバラ	2015 年 8 月 17 日～2015 年 8 月 20 日
FDTC 2015	Workshop on Fault Diagnosis and Tolerance in Cryptography	フランス・サンマロ	2015 年 9 月 13 日
CHES 2015	Workshop on Cryptographic Hardware and Embedded Systems	フランス・サンマロ	2015 年 9 月 13 日～2015 年 9 月 16 日
PROOFS 2015	Security Proofs for Embedded Systems Workshop	フランス・サンマロ	2015 年 9 月 17 日
Asiacrypt 2015	International Conference on the Theory and Application of Cryptology and Information Security	ニュージーランド・オークランド	2015 年 11 月 30 日～2015 年 12 月 3 日
PKC2016	International Conference on Practice and Theory in Public-Key Cryptography	台湾・台北	2016 年 3 月 6 日～2016 年 3 月 9 日
FSE 2016	International Workshop on Fast Software Encryption	ドイツ・ボーフム	2016 年 3 月 20 日～2016 年 3 月 23 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。

2.5.1. ブロック暗号の解読技術

・Integral Cryptanalysis on Full MISTY1 [Crypto 2015]

NTT の藤堂氏が 64 ビットブロック暗号 MISTY1 に対する暗号解読を発表した。Eurocrypt 2015 で発表した一般的な攻撃法を MISTY1 に適用した結果、1997 年の MISTY1 発表から 18 年目にして、解読計算量が初めて総当たり法を下回った。本結果により、藤堂氏は、最優秀論文賞および最優秀若手研究者賞をダブル受賞した。その後、藤堂氏の結果をイスラエ

ルの Bar-On 氏が改良し、解読計算量は $2^{69.5}$ にまで下がっているが、解読に必要なデータ量は 2^{64} であり、まだ現実的な脅威とは言えない。

2.5.2. ハッシュ関数の解読技術

・Practical Free-Start Collision Attacks on 76-Step SHA-1 [Crypto 2015]

フランスの Karpman らが SHA-1 圧縮関数の Free-Start 衝突攻撃評価を行った。GPU による実装を行い、76 段(フルは 80 段)を約 5 日で攻撃できることを示し、SHA-1 の使用を速やかに止めるように注意喚起を行った。なお、Free-Start とは仕様で固定されている初期ベクターを可変とすることで難度を下げた攻撃法であり、これを 80 段まで伸ばしただけでは SHA-1 の衝突発見には至らない。しかし、Free-Start による解析結果を利用して、仕様通りのハッシュ関数の衝突発見に導くことは可能であり、今後の進展を注視していく必要がある。

2.5.3. 暗号利用モードの解読技術

・Twisted Polynomials and Forgery Attacks on GCM [Eurocrypt 2015]

デンマークの Abdelraheem らが、認証暗号に対する偽造攻撃を発表した。多項式ハッシュを用いる方式に対し、偽造多項式を構成することによる攻撃が知られていたが、偽造多項式の構成法は見つかっていなかった。今回の発表では、偽造多項式の構成法を提案し、CRYPTREC 暗号リストに掲載されている認証つき秘匿モード GCM(Galois Counter Mode)を、弱鍵モデル（弱鍵を持つという条件）のもとで、ナンスを再利用せずに偽造する攻撃に初めて成功した。攻撃の成功する条件等の現実性について詳細に評価する必要がある。

2.5.4. 公開鍵暗号の解読技術

・Last Fall Degree, HFE, and Weil Descent Attacks on ECDLP [Crypto 2015]

Asiacrypt 2012 において Petit らは、ある仮定(「First Fall Degree」仮定と呼ばれる)の元に、楕円曲線暗号の解読計算量が準指数時間オーダーになることを示した。これに対し、アメリカ・南カリフォルニア大学の Huang 教授らは、この仮定の正当性に疑問を投げかけるデータを示し、解読計算量評価はより慎重に行うべきであると主張した。本論文の結果が正しいとすると、楕円曲線暗号は Petit らによる評価結果より安全であると考えられる。

・Algebraic Approaches for the Elliptic Curve Discrete Logarithm Problem over Prime Fields [PKC 2016]

近年、拡大体上の ECDLP に対する指数計算法がいくつか提案されているが、実世界においてよく利用される素体上の ECDLP へは適用できないと考えられていた。本論文では、バイナリ曲線から素体上の曲線に攻撃を拡張する方法および実験による計算量評価が示され

た。現状は小さなパラメータの場合にしか有効とならず、漸近計算量評価もグレブナ基底のアルゴリズムを用いるために制限されるが、今後の進展に注意する必要がある。

2.6. 委員会開催状況

2015 年度、暗号技術評価委員会は、表 2.4 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 2.4　暗号技術評価委員会の開催

回	年月日	議題
第 1 回	2015 年 11 月 18 日	委員会活動計画案、ワーキンググループ活動計画、外部評価、MISTY1 及び SHA-1 に関する注意喚起レポート、ハッシュ関数 SHA-2・SHA-3 の取り扱い、監視状況報告
第 2 回	2016 年 3 月 8 日	ワーキンググループ活動の年度報告、CRYPTREC Report 2015 目次案、ハッシュ関数 SHA-2・SHA-3 の取り扱い、暗号アルゴリズムの脆弱性に関する情報発信フロー、外部評価レポート結果、次年度活動計画案、監視状況報告

2.7. 暗号調査ワーキンググループ開催状況

2015 年度、各暗号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 2.5 の通りである。表 2.6 及び表 2.7 の通り、各 WG は計 5 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　2015 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	公開鍵暗号の安全性は、素因数分解の困難性や離散対数問題の困難性などさまざまな数学的問題に依存している。本ワーキンググループでは、楕円曲線上の離散対数問題の困難性に関する調査、多重線形写像及び難読化の最新動向に関する調査を行う。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。
軽量暗号ワーキンググループ	本間 尚文	軽量暗号ワーキンググループは、軽量暗号技術が求められるサービスにおいて、電子政府のみならず利用者が適切な暗号方式を選択でき、容易に調達できることをめざして設置された。軽量暗号を選択・利用する際の技術的判断に資すること、今後の利用促進をはかることを目的とした「暗号技術ガイドライン（軽量暗号）」を発行する。

表 2.6　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	2016 年 1 月 22 日	活動計画案の検討、今年度の調査の進め方の検討
第 2 回	2016 年 3 月 3 日	予測図の更新に関する検討、難読化の調査に関する検討 楕円曲線上の離散対数問題の調査に関する検討、来年度活動計画案に関する検討

表 2.7　暗号技術調査ワーキンググループ(軽量暗号)の開催

回	年月日	議題
第 1 回	2015 年 10 月 20 日	暗号技術ガイドライン(軽量暗号)の作成方針に関する検討、軽量暗号に関する実装詳細評価の方針に関する検討、NIST Lightweight Cryptography Workshop 報告、英語版作成方針に関する検討、CAESAR プロジェクト紹介
第 2 回	2015 年 12 月 24 日	暗号技術ガイドライン(軽量暗号)の目次案・掲載するアルゴリズムに関する検討、実装詳細評価に関する検討、英語版作成に関する検討
第 3 回	2016 年 2 月 9 日	暗号技術ガイドライン(軽量暗号)の作成スケジュールに関する検討、軽量暗号のユースケースに関する検討、暗号技術ガイドライン(軽量暗号)の掲載するアルゴリズムに関する検討、軽量暗号に関する実装詳細評価に関する検討、英語版作成に関する検討

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)楕円曲線上の離散対数問題(ECDLP)の困難性に関する調査

2012 年度の暗号技術調査 WG(計算機能力評価)における調査結果において言及があったように、ECDLP に対する指数計算法の計算量評価についての研究結果が近年発表されてきている。2015 年～2016 年度は、これらの研究内容を調査し、見解をまとめる。

(2)多重線形写像(multi-linear map)及び難読化(Obfuscation)の最新動向に関する調査

2013 年～2014 年度は、格子問題等の困難性に関する調査を行い、「格子問題等の困難性に関する調査」を作成した。2015 年～2016 年度は、近年研究が進展している多重線形写像及び難読化に関する研究動向を調査する。

(3)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	国立大学法人九州大学
委員：	青木　和麻呂	日本電信電話株式会社
委員：	太田　和夫	国立大学法人電気通信大学
委員：	草川　恵太	日本電信電話株式会社
委員：	國廣　昇	国立大学法人東京大学
委員：	下山　武司	株式会社富士通研究所
委員：	安田　雅哉	国立大学法人九州大学

3.1.3. 活動方針

（１） 楕円曲線上の離散対数問題の困難性に関する調査

CRYPTO2015 で発表された論文[HKY2015]などを精査し、論点や課題を事務局にて整理する。さらなる検討は来年度に行う。

[HKY2015] “Last fall degree, HFE, and Weil descent attacks on ECDLP,” Ming-Deh A. Huang, Michiel Kosters, Sze Ling Yeo

（プレゼン資料　“Sub-exponential algorithms for ECDLP?”[1])

（２） 多重線形写像及び難読化の最新動向に関する調査

[1] http://ecc2015.math.u-bordeaux1.fr/documents/kosters.pdf

(a) 多重線形写像については、既存の文献をリストアップし、それらを用いた応用やアプリケーションなどに関する調査を行う。来年度、必要に応じて外部評価を実施し、安全性評価を行う。

(b) 難読化技術については、今年度実施した外部評価者からのレポートに基づき現状を把握し、論点や課題を整理する。今年度の検討結果に基づき、来年度にさらなる評価を実施する。

（３） 予測図の更新

(a) 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の評価に大幅な変更がないかどうかの確認を行う。

(b) スーパーコンピュータのベンチマーク結果の 1 位から 500 位を 1993 年から半年毎に集計している Web サイト TOP500.Org[2]の 2015 年 6 月・11 月のベンチマーク結果の追加を行う。

3.1.4. 活動概要

スケジュール

第 1 回　2016 年 1 月 22 日(金) 活動計画案や作業内容についての審議と了承

第 2 回　2016 年 3 月 3 日(木)　調査内容についての審議と了承

（１） 楕円曲線上の離散対数問題の困難性に関する調査

(a) 下記の論文をリストアップし、ECDLP の計算量評価の概要を報告した。

(b) 標数 2 の有限体上の ECDLP の研究動向の解説を論文[GG2016]をベースに、素体上の ECDLP の研究動向の解説を論文[PKM2016]をベースに、次年度に記述することになった。

[S2004] Semaev, “Summation polynomials and the discrete logarithm problem on elliptic curves,” https://eprint.iacr.org/2004/031.pdf.

[D2011] Diem, “On the discrete logarithm problem in elliptic curves、” Compositio Math. 147、2011.

[FPPR2012] Faugère, Perret, Petit and Renault, “Improving the Complexity of Index Calculus Algorithms in Elliptic Curves over Binary Fields,” Eurocrypt 2012.

[PQ2012] Petit and Quisquater, “On polynomial systems arising from a Weil descent,” ASIACRYPT 2012.

[HKY2015] Huang, Kosters and Yeo, “Last Fall Degree, HFE, and Weil Descent Attacks on ECDLP,” CRYPTO 2015.

[2] http://www.top500.org/

[GG2016] Galbraith and Gaudry, “Recent progress on the elliptic curve discrete logarithm problem,” Designs, Codes and Cryptography. (2016) 78

[PKM2016] Petit, Kosters and Messeng, “Algebraic Approaches for the Elliptic Curve Discrete Logarithm Problem over Prime Fields,” PKC 2016.

（２）多重線形写像及び難読化の最新動向に関する調査

(a) 多重線形写像については、既存の文献をリストアップし、それらを用いた応用やアプリケーションなどに関する調査を行った。

(b) 難読化技術については、今年度実施した外部評価者からの評価レポート[3]のレビューを行い、サマリ[4]を作成した。

(c) 次年度は、多重線形写像と難読化の関係を整理しつつ、特に多重線形写像の安全性を重点的に調査・評価を実施する。

（３）予測図の更新

(a) 素因数分解問題の困難性および楕円曲線上の離散対数問題の困難性に関する計算量評価に大幅な進展はなかったため、2015 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。

(b) 過去の議論・経緯などを把握できるような資料を次年度に作成する。公開するかどうかについては今後検討する。

（４）Post-Quantum Cryptography の動向について

NIST が、NISTIR 8105 DRAFT Report on Post-Quantum Cryptography[5]を公表し、PQCrypto 2016 において、Post-Quantum Cryptography: NIST's Plan for the Future[6]と題してプレゼンテーションを行っているため、NIST の見解などについて意見交換を行った。

3.1.5. 成果概要

（１） 多重線形写像及び難読化の最新動向に関する調査

(a) 多重線形写像

多重線形写像(multi-linear map) は、多重の線形性を用いることで複雑な機能を提供できる可能性があり、様々なアプリケーションを具現化, 効率化に資する有用な技術の一つであると考えられる。既に提案されている代表的なアプリケ

[3] 評価レポートは技術評価レポートとして Web に掲載する予定である。
[4] サマリは付録 3 に掲載している。
[5] http://csrc.nist.gov/publications/drafts/nistir-8105/nistir_8105_draft.pdf
[6] https://pqcrypto2016.jp/data/pqc2016_nist_announcement.pdf

ーションの例を以下に挙げる。

〈多重線形写像(Multi-linear map) の応用例について言及されている論文〉

[1] Dan Boneh, Alice Silverberg:
Applications of Multilinear Forms to Cryptography. IACR Cryptology ePrint Archive 2002: 80 (2002)
＊ One-round n-way Diffie-Hellman key exchange protocol
＊ Unique signature
＊ Verifiable pseudo random functions
＊ Broadcast encryption

[2] Markus Rückert, Dominique Schröder:
Aggregate and Verifiably Encrypted Signatures from Multilinear Maps without Random Oracles. ISA 2009: 750-759
＊ Efficient aggregate and verifiable encrypted signatures without random oracle

[3] Charalampos Papamanthou, Roberto Tamassia, Nikos Triandopoulos:
Optimal Authenticated Data Structures with Multilinear Forms. Pairing 2010: 246-264
＊ Authenticated data structures

[4] Sanjam Garg, Craig Gentry, Amit Sahai, Brent Waters:
Witness encryption and its applications. STOC 2013: 467-476
＊ Witness encryption
⇒ Public-key encryption, Identity-based encryption,
Attribute-based encryption, etc...

[5] Sanjam Garg, Craig Gentry, Shai Halevi:
Candidate Multilinear Maps from Ideal Lattices. EUROCRYPT 2013: 1-17
＊ Multipartite Diffie-Hellman key exchange
⇒ Attribute based encryption for general circuit

[6] Jean-Sébastien Coron, Tancrède Lepoint, Mehdi Tibouchi:
Practical Multilinear Maps over the Integers. CRYPTO (1) 2013: 476-493
＊ Multipartite Diffie-Hellman key exchange

[7] Eduarda S. V. Freire, Dennis Hofheinz, Kenneth G. Paterson, Christoph Striecks:
Programmable Hash Functions in the Multilinear Setting. CRYPTO (1) 2013: 513-530
＊ Programmable hash functions (PHFs)

[8] Susan Hohenberger, Amit Sahai, Brent Waters:
Full Domain Hash from (Leveled) Multilinear Maps and Identity-Based Aggregate Signatures. CRYPTO (1) 2013: 494-512

＊ Hash function with a Naor-Reingold-type structure

⇒ identity-based aggregate signature

[9] Dan Boneh, Brent Waters:

Constrained Pseudorandom Functions and Their Applications. ASIACRYPT (2) 2013: 280-300

＊ Constrained PRFs

⇒ Identity based encryption, broadcast encryption with optimal ciphertext size

[10] Adeline Langlois, Damien Stehlé, Ron Steinfeld:

GGHLite: More Efficient Multilinear Maps from Ideal Lattices. EUROCRYPT 2014: 239-256

＊ Efficient miltipartite Diffie-Hellman key exchange

＊ Efficient attribute based encryption

[11] Dan Boneh, Brent Waters, Mark Zhandry:

Low Overhead Broadcast Encryption from Multilinear Maps. CRYPTO (1) 2014: 206-223

＊ Broadcast encryption

[12] Sanjam Garg, Craig Gentry, Shai Halevi, Mark Zhandry:

Functional Encryption Without Obfuscation. TCC (A2) 2016: 480-511

＊ Functional encryption

(b)　難読化

難読化(Obfuscation)に関しては、近年の技術動向について、Sanjam Garg 氏(University of California, Berkeley, 米国)に評価を依頼した。本評価レポートの概要については、付録 3 を参照のこと。なお、本レポートは、CRYPTREC の Web サイトにおける技術報告書のページ[7]に掲載予定である。

（２）予測図の更新

「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」の更新後の図は、図 3.1 の通りとなる。

[7] http://www.cryptrec.go.jp/estimation.html

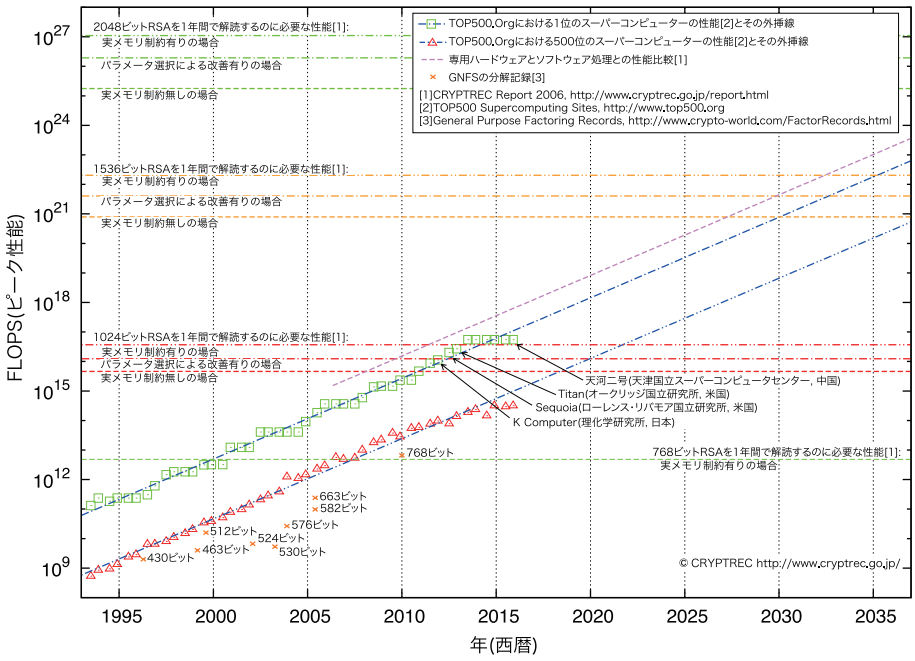


図 3.1：1 年間でふるい処理を完了するのに要求される処理能力の予測(2016 年 2 月更新)

また、「ρ 法で ECDLP を 1 年で解くのに要求される処理能力の予測」の更新後の図は、図 3.2 の通りとなる。

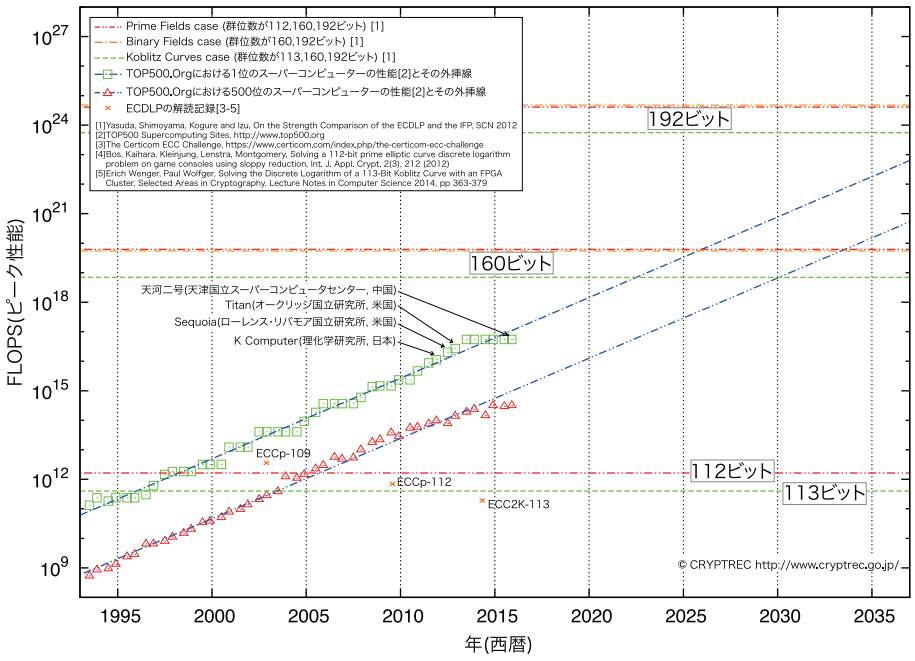


図 3.2： ρ 法で ECDLP を 1 年で解くのに要求される処理能力の予測(2016 年 2 月更新)

3.2. 軽量暗号ワーキンググループ

3.2.1. 活動目的

軽量暗号 WG は、軽量暗号技術が求められるサービスにおいて、電子政府のみならず一般のシステムにおいて、利用者が適切な暗号方式を選択でき、容易に調達できることをめざして活動を行っている。

2015 年度からは、軽量暗号を選択・利用する際の技術的判断に資すること、今後の利用促進をはかることを目的とした「暗号技術ガイドライン（軽量暗号)」を発行するために、2 年かけて詳細評価を行っている。

3.2.2. 委員構成(敬称略、五十音順)

主査：	本間　尚文	国立大学法人東北大学
委員：	青木　和麻呂	日本電信電話株式会社
委員：	岩田　哲	国立大学法人名古屋大学
委員：	小川　一人	日本放送協会
委員：	小熊　寿	株式会社トヨタIT開発センター
委員：	﨑山　一男	国立大学法人電気通信大学
委員：	渋谷　香士	ソニー株式会社
委員：	鈴木　大輔	三菱電機株式会社
委員：	成吉　雄一郎	ルネサスエレクトロニクス株式会社
委員：	峯松　一彦	日本電気株式会社
委員：	三宅　秀享	株式会社東芝
委員：	渡辺　大	株式会社日立製作所

3.2.3. 活動概要

2015 年度は、下記についての検討を行った。

ガイドラインの作成方針の決定（詳しくは、3.2.5 節を参照のこと。）

- 目的の確認、目次案の決定、各章の執筆担当の決定

① ガイドラインに記載する軽量暗号アルゴリズムの選択

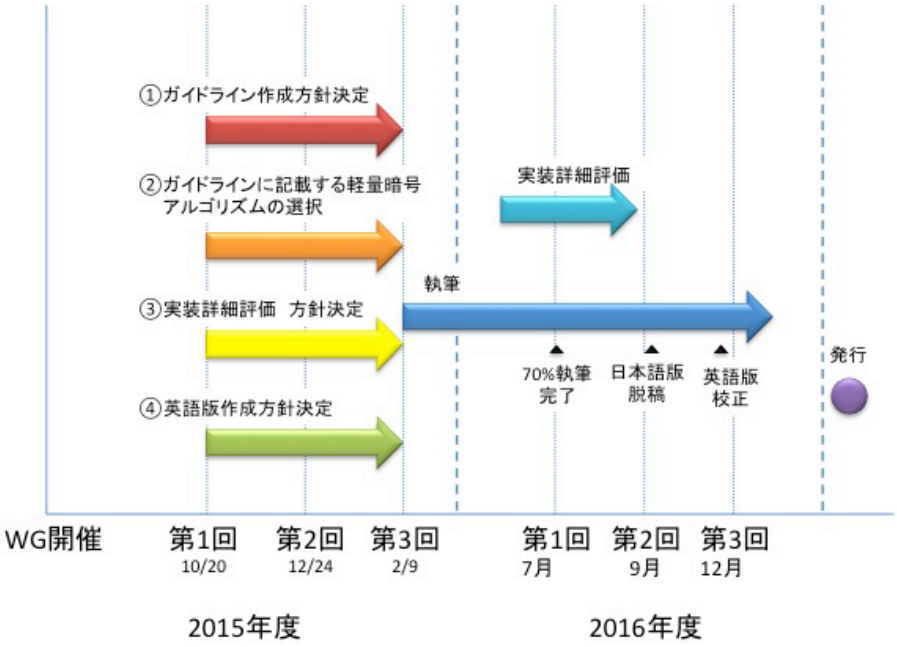
- どのような基準で選択するか

② 実装詳細評価の方針の決定（詳しくは、3.2.6 節を参照のこと。）

- 実装プラットフォーム、実装方法、評価（測定）指標、評価対象の軽量暗号アルゴリズム

③ 軽量暗号 WG 活動の対外的アピールのあり方に関する検討

- 「暗号技術ガイドライン（軽量暗号)」の英語版作成など



ガイドライン作成スケジュール案

3.2.4. 2016 年度の活動計画

① 「暗号技術ガイドライン（軽量暗号)」(日本語版・英語版）の執筆を行う

② 実装詳細評価を行う

3.2.5　暗号技術ガイドライン（軽量暗号）作成方針

1　作成目的と想定読者

IoT 等の次世代ネットワークサービスにおいて軽量暗号の活用が期待されることから、方式を選択・利用する際の技術的判断に資すること、今後の利用促進をはかることを目的として、暗号技術ガイドライン(軽量暗号)を作成する。

想定する読者は、情報システムのセキュリティ機能の設計・開発・実装において暗号技術を活用する技術者である。

2　目次案

I.　はじめに

軽量暗号に関するサマリー

II.　軽量暗号の活用例

1. 軽量暗号とは

   軽量暗号の特徴

2. 軽量暗号はどこに使えるか？

   軽量暗号の代表的なユースケース

3. どんな軽量暗号、パラメータを選べばいいか？

   軽量暗号の分類と一覧、条件やニーズに対応した軽量暗号の選択

   鍵長、ブロック長の説明と選び方

4. 軽量暗号を使う時の留意点

   鍵更新のタイミング、鍵更新の方法

   鍵更新の頻度を減らすことができる暗号利用モードの紹介

   関連鍵攻撃が指摘されているブロック暗号を利用する時の注意点

5. ユースケースごとの軽量暗号活用例と効果

   ユースケース別に推奨される軽量暗号とその鍵長、ブロック長、暗号利用モードなどを示す.

   既存暗号を使った場合と比較したときの優位性を示す.(ハードウェア回路規模、消費電力量、レイテンシ、メモリサイズ)

III.　軽量暗号の性能比較

1. ハードウェア実装
   - ハードウェア回路規模で比較
   - 消費電力量で比較

- レイテンシで比較

2. ソフトウェア実装
   - 必要メモリサイズで比較

IV. 代表的な軽量暗号

1. ブロック暗号
2. ストリーム暗号
3. ハッシュ関数
4. メッセージ認証コード
5. 認証暗号

3 IV 章に記載するアルゴリズム

ブロック暗号

アルゴリズム名	発表された国際会議, 採録/提案されている標準等
LED	CHES 2011
Piccolo	CHES 2011
TWINE	SAC 2012
PRINCE	ASIACRYPT 2012
Midori	ASIACRYPT 2015
PRESENT	CHES 2007, ISO/IEC 29192-2
CLEFIA	FSE 2007, ISO/IEC 29192-2
SIMON	Cryptology ePrint Archive (Report 2013/404)
SPECK	Cryptology ePrint Archive (Report 2013/404)

ストリーム暗号

アルゴリズム名	発表された国際会議, 採録/提案されている標準等
Grain v1/-128A	eStream portfolio, ISO/IEC 29167-13
MICKEY 2.0	eStream portfolio
Trivium	eStream portfolio, ISO/IEC 29192-3
Enocoro	ISO/IEC 29192-3
ChaCha20	RFC 7539

ハッシュ関数

アルゴリズム名	発表された国際会議，採録/提案されている標準等
PHOTON	CRYPTO 2011, ISO/IEC 29192-5
SPONGENT	CHES 2011, ISO/IEC 29192-5
QUARK	CHES 2010
KECCAK	SHA-3 competition, FIPS 202

メッセージ認証コード

アルゴリズム名	発表された国際会議，採録/提案されている標準等
SipHash	Indocrypt 2012, DIAC

認証暗号

アルゴリズム名	発表された国際会議，採録/提案されている標準等
ACORN	DIAC 2014, DIAC 2015
ASCON	DIAC 2014, DIAC 2015, CT-RSA 2015(analysis)
AES-JAMBU	DIAC 2014, DIAC 2015
AES-OTR	EUROCRYPT 2014, DIAC 2015
CLOC and SILC	FSE 2014 (CLOC), DIAC 2014 (SILC), DIAC 2015
Deoxys	ASIACRYPT 2014 (TWEAKEY), DIAC 2014, DIAC 2015
Joltik	ASIACRYPT 2014 (TWEAKEY), DIAC 2014, DIAC 2015
Ketje	DIAC 2014, (SHA3)
Minalpher	DIAC 2014, IEEE GCCE 2015(ハードウェア実装)
OCB	ACM CCS 2001，ASIACRYPT 2004，FSE 2011
PRIMATES	FSE 2014 (APE), ASIACRYPT 2014 (RUP, bound), DIAC 2014, DIAC 2015
SCREAM	DIAC 2014, DIAC 2015

3.2.6　軽量暗号に関する実装詳細評価の方針

「暗号技術ガイドライン（軽量暗号)」の作成にあたって、複数の軽量暗号アルゴリズム及び比較対象となる代表的な既存暗号技術を、同一プラットフォーム上で、統一的な実装ポリシーにより実装し、統一的な評価環境で比較を行う「実装詳細評価」が必要と考えられる。以下の実装詳細評価の方針を示す。

1. ハードウェア実装　詳細評価方針
2. ソフトウェア実装　詳細評価方針
3. 実装対象分野およびアルゴリズム

1. ハードウェア実装　詳細評価方針

(ア) 実装プラットフォーム

- ASIC 実装評価
- 標準的な CMOS セルライブラリを利用

  NanGate Open Cell Library (45 nm プロセス)

  オープンソースであり第三者による検証が可能、半導体メーカーも採用

(イ) 実装方法 及び 評価指標

- 3 通りのアーキテクチャで実装

  ①各アルゴリズムの仕様に準じた標準的な実装（round 実装)

  ②処理速度を優先する実装(unrolled 実装)

  ③回路規模を優先する実装(serial 実装)

- 各実装アーキテクチャについて、以下の指標の測定を行う

  ①最大動作周波数

  ②処理速度

  ③ゲートカウント

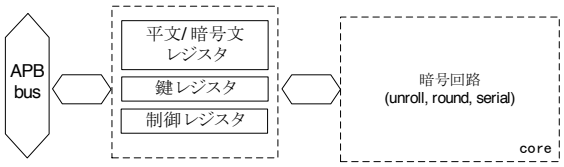
  ④サイクルカウント

  ⑤消費電力

  ⑥ピーク電流

(ウ) インターフェース

実装対象の各アルゴリズムに対して、平文・暗号文・鍵等の入出力データの与え方や測定方法を統一し、公平に比較可能なインターフェースで実装および測定を行う。



2. ソフトウェア実装　詳細評価方針

（ア）実装プラットフォーム

- 組込みプロセッサ上での実装評価
- ルネサスエレクトロニクスのプラットフォーム(組込みマイコン マーケットシェア１位)

（イ）実装方法 及び 評価指標

- 処理速度とメモリ(RAM, ROM) サイズを指標とし、処理速度を優先した高速版とメモリサイズを削減した小型版の 2 通りの実装を行う
- それぞれの実装について処理速度とメモリ(RAM, ROM) サイズを測定

（ウ）インターフェース

- 実装対象の各アルゴリズムに対して、平文、鍵、暗号文等の入出力データの与え方や測定方法を考慮し、公平に比較可能なインターフェースで実装および測定を行う
- 技術カテゴリ毎に記載

3. 実装対象分野およびアルゴリズム

（ア）軽量認証暗号

CAESAR プロジェクト 2nd Round に進んだ「軽量」な方式の中から選択

※先行調査で実装済みの方式：AES-GCM, Minalpher, AES-OTR, CLOC, SILC, Ketje

比較対象の既存技術：AES-GCM

（イ）軽量メッセージ認証コード

詳細実装評価までは行わないが、公知情報から速度等の目安が分かるように III 章に記載する。

（ウ）軽量ブロック暗号

CLEFIA, PRESENT, LED, Piccolo, TWINE, PRINCE, SIMON, SPECK, Midori

比較対象の既存技術：AES, Camellia

付録１

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		名称
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)	3-key Triple DES(注3)
	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	CCM
		GCM(注4)
メッセージ認証コード		CMAC
		HMAC
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（情報通信担当）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） 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。

（注3） 3-key Triple DES は、以下の条件を考慮し、当面の利用を認める。
1） NIST SP 800-67 として規定されていること。
2） デファクトスタンダードとしての位置を保っていること。

（注4） 初期化ベクトル長は 96 ビットを推奨する。

推奨候補暗号リスト

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

技術分類		名称
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
		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	該当なし
メッセージ認証コード		PC-MAC-AES
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） 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。

（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。

[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		名称
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	該当なし
	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	該当なし
メッセージ認証コード		CBC-MAC(注11)
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。

[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。

付録２

CRYPTREC 暗号リスト掲載暗号の問い合わせ先一覧

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 <http://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://jp.fujitsu.com/group/labs/techinfo/technote/crypto/ecc.html 英文：http://jp.fujitsu.com/group/labs/en/techinfo/technote/crypto/ecc.html ・参照 URL ・SEC 1: Elliptic Curve Cryptography (September 20, 2000 Version 1.0) <http://www.cryptrec.go.jp/cryptrec_03_spec_cypherlist_files/PDF/01_01sec1.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://japan.emc.com/emc-plus/rsa-labs/pkcs/files/h11300-wp-pkcs-1v2-2-rsa-cryptography-standard.pdf> 和文：なし 英文：http://www.emc.com/security/rsa-bsafe.htm
問い合わせ先	〒151-0053 東京都渋谷区代々木２丁目１番１号 新宿マインズタワー EMC ジャパン株式会社 RSA 事業本部 パートナー営業部 インサイド セールス チーム　左、高石 TEL：03-6830-3341, FAX：03-5308-8979 E-MAIL：Hanae.Hidari@rsa.com, Hiromi.Takaishi@rsa.com

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://japan.emc.com/emc-plus/rsa-labs/pkcs/files/h11300-wp-pkcs-1v2-2-rsa-cryptography-standard.pdf> 和文：なし 英文：http://www.emc.com/security/rsa-bsafe.htm
問い合わせ先	〒151-0053 東京都渋谷区代々木 2 丁目 1 番 1 号 新宿マインズタワー EMC ジャパン株式会社 RSA 事業本部 パートナー営業部 インサイド セールス チーム　左、高石 TEL：03-6830-3341, FAX：03-5308-8979 E-MAIL：Hanae.Hidari@rsa.com, Hiromi.Takaishi@rsa.com

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://japan.emc.com/emc-plus/rsa-labs/pkcs/files/h11300-wp-pkcs-1v2-2-rsa-cryptography-standard.pdf> 和文：なし 英文：http://www.emc.com/security/rsa-bsafe.htm
問い合わせ先	〒151-0053 東京都渋谷区代々木 2 丁目 1 番 1 号　新宿マインズタワー EMC ジャパン株式会社　RSA 事業本部　ソリューション営業部 インサイド　セールスチーム　左、高石 TEL：03-6830-3341, FAX：03-5308-8979, E-MAIL：Hanae.Hidari@rsa.com, Hiromi.Takaishi@rsa.com

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 1 (March 2007), Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revides) 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://csrc.nist.gov/publications/nistpubs/800-56A/SP800-56A_Revision1_Mar08-2007.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://jp.fujitsu.com/group/labs/techinfo/technote/crypto/ecc.html 英文:http://jp.fujitsu.com/group/labs/en/techinfo/technote/crypto/ecc.html ・参照 URL ・SEC 1: Elliptic Curve Cryptography (September 20, 2000 Version 1.0) <http://www.cryptrec.go.jp/cryptrec_03_spec_cypherlist_files/PDF/01_01sec1.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 1(March 2007), Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revides) において、C(2,0,ECC CDH)として規定されたもの。 ・参照 URL <http://csrc.nist.gov/publications/nistpubs/800-56A/SP800-56A_Revision1_Mar08-2007.pdf>

2. 共通鍵暗号

暗号名	Triple DES
関連情報	仕様 ・NIST SP 800-67 Revision 1, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, January 2012. ・参照 URL <http://csrc.nist.gov/publications/nistpubs/800-67-Rev1/SP-800-67-Rev1.pdf>

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://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>

暗号名	Camellia
関連情報	公開ホームページ 和文：http://info.isl.ntt.co.jp/crypt/camellia/index.html 英文：http://info.isl.ntt.co.jp/crypt/eng/camellia/index.html
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:0422-59-3461, FAX:0422-59-4015 E-MAIL:camellia@lab.ntt.co.jp

暗号名	KCipher-2
関連情報	公開ホームページ 和文:http://www.kddilabs.jp/products/security/kcipher2/product.html 英文:http://www.kddilabs.jp/english/Products/Security/kcipher2/product.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 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:049-278-7885, FAX:049-278-7510 E-MAIL:kiyomoto@kddilabs.jp

3. ハッシュ関数

暗号名	SHA-256, SHA-384, SHA-512
関連情報	仕様 ・FIPS PUB 180-4, Secure Hash Standard (SHS) ・参照 URL <http://csrc.nist.gov/publications/fips/fips180-4/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 1	仕様 ・NIST SP 800-38A, Recommendation for Block Cipher Modes of Operation Methods and Techniques ・　参照 URL <http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.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 1	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://csrc.nist.gov/publications/nistpubs/800-38C/SP800-38C_updated-July20_2007.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://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf>

6. メッセージ認証コード

暗号名	CMAC
関連情報 1	仕様 ・NIST FIPS SP 800-38B, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, May 2005. ・ 参照 URL <http://csrc.nist.gov/publications/nistpubs/800-38B/SP_800-38B.pdf>

暗号名	HMAC
関連情報 1	仕様 ・NIST FIPS PUB 198-1, The Keyed-Hash Message Authentication Code (HMAC), July 2008. ・ 参照 URL <http://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.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　http://info.isl.ntt.co.jp/crypt/psec/index.html 英文　http://info.isl.ntt.co.jp/crypt/eng/psec/index.html
問い合わせ先	〒180-8585 東京都武蔵野市緑町 3-9-11 日本電信電話株式会社　NTT セキュアプラットフォーム研究所 PSEC-KEM 問い合わせ窓口　担当 TEL: 0422-59-3462　　FAX: 0422-59-4015 E-MAIL: publickey@lab.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：http://www.nec.co.jp/cced/SecureWare/sdk/cipherunicorn-e.html 英文：http://www.nec.co.jp/cced/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　スマートネットワーク事業部 E-MAIL：info@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 研究開発センター コンピュータアーキテクチャ・セキュリティラボラトリー 研究主幹 秋山 浩一郎 TEL：044-549-2156, FAX：044-520-1841 E-MAIL：crypt-info@isl.rdc.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 トータルソリューションシステム部 システム第三課　坂上 勉 TEL：0467-41-3560 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：http://www.nec.co.jp/cced/SecureWare/sdk/cipherunicorn-a.html 英文： http://www.nec.co.jp/cced/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　スマートネットワーク事業部 E-MAIL：info@security.jp.nec.com

暗号名	CLEFIA
関連情報	公開ホームページ 和文：http://www.sony.co.jp/Products/cryptography/clefia/ 英文：http://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 研究開発センター コンピュータアーキテクチャ・セキュリティラボラトリー 研究主幹 秋山 浩一郎 TEL：044-549-2156, FAX:044-520-1841 E-MAIL:crypt-info@isl.rdc.toshiba.co.jp

暗号名	SC2000
関連情報	公開ホームページ 和文： http://jp.fujitsu.com/group/labs/techinfo/technote/crypto/sc2000.html 英文： http://jp.fujitsu.com/group/labs/en/techinfo/technote/crypto/sc2000.html
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	〒244-0817 神奈川県横浜市戸塚区吉田町 292 番地 株式会社日立製作所 ICT 事業統括本部 IT プロダクツ統括本部 開発基盤本部 ソフトウェア生産技術部 主任技師 栗田 博司 TEL：050-3154-4218, FAX ： 045-865-9065 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：050-3135-3440, FAX：050-3135-3387 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	〒244-0817 神奈川県横浜市戸塚区吉田町 292 番地 株式会社日立製作所 ICT 事業統括本部 IT プロダクツ統括本部 開発基盤本部 ソフトウェア生産技術部 主任技師 栗田 博司 TEL：050-3154-4218, FAX ： 045-865-9065 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 ・FIPS PUB 180-4, Secure Hash Standard (SHS) ・参照 URL 〈http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf〉

暗号名	SHA3-256, SHA3-384, SHA3-512, SHAKE256
関連情報	仕様 ・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　主任研究員 峯松 一彦 TEL：044-431-7665, FAX：044-431-7707 E-MAIL: k-minematsu@ah.jp.nec.com

5. 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 3: 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://japan.emc.com/emc-plus/rsa-labs/pkcs/files/h11300-wp-pkcs-1v2-2-rsa-cryptography-standard.pdf〉 和文：なし 英文：http://www.emc.com/security/rsa-bsafe.htm
問い合わせ先	〒151-0053 東京都渋谷区代々木 2 丁目 1 番 1 号 新宿マインズタワー EMC ジャパン株式会社 RSA 事業本部 パートナー営業部 インサイド セールス チーム　左、高石 TEL：03-6830-3341, FAX：03-5308-8979 E-MAIL：Hanae.Hidari@rsa.com, Hiromi.Takaishi@rsa.com

2. 共通鍵暗号

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 ・FIPS PUB 186-4, Secure Hash Standard (SHS) ・参照 URL <http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf>

6. 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

難読化(Obfuscation)に関する評価レポート[1]の概要

[レポートの構成]

本評価レポートは、エクゼクティブサマリ、難読化の要素技術（構成技術)の紹介、難読化の紹介の 3 部構成となっている。1 章で、エクゼクティブサマリを示し、2 章で、難読化の有力な要素技術となる多重線形写像について紹介し、3 章で、難読化技術の詳細及びアプリケーションについて紹介している。レポートの概要は以下の通り。

[難読化の概念]

ごく自然な形での難読化に求められる性質の定義 は、プログラムにブラックボックスオラクルアクセスをして得られる情報と同程度しか情報を漏らさない［BGI+01］というものである。しかし、この要件は、いくつかの人工的な回路のクラスについてのみではあるが、実現不可能であることが示されている。

これに対して、若干弱い要件として識別不可能難読性（iO ： indistinguishability obfuscation）が提唱されている［BGI+01, GR07, GGH+13b]。この要件は、全く同じ回路計算を実行する難読化(プログラム)の 計算量的識別不可能性のみを要求している。

近年、[GGH+13b］をはじめとする複数の論文で、多重線形写像(multi-linear map）の具体的構成などが提唱され、 難読化の実現可能性に対する期待が高まっている。近年示されている結果の多くは、計算量的識別不可能性に基づくもの(iO)である。この難読化の安全性に関しては、明らかになっていない部分が多く残されている。さらには、難読化の効率については、近年考案されているものはいずれも効率が悪い。

[要素技術としての多重線形写像]

多重線形写像の大きな進展として、近年、ノイズがあったとしても暗号化されたデータが等しいものであるかどうかの検証が可能となる方式が提案されている[GGH13a, CLT13, GGH15]。[GGH13a］で示された 多重線形写像の他、[CLT13, CLT15, GGH15］では異なる仮定に基づく多重線形写像が用いられている。

多重線形写像に対する解析としては既にいくつか示されている[CHL+15, CLR15, CLLT15, CFL+16]。しかしこれらは典型的な多くの難読化の構成には影響を与えないものであり、これら解析の動向については本評価レポートでは割愛する。

最近の解析の動向として［JHC16, MA16］などがある。これらは従来の解析とは別のアプローチをとり、(多重線形写像を用いた)難読化の安全性にも影響を与える可能性があるが、

[1] http://www.cryptrec.go.jp/estimation.html にて公開予定である。

これらの攻撃は慎重にパラメータを選択することで防ぐことが可能である。

さらに、2016 年に入ってからは GGH 構成の多重線形写像に基づく難読化に対する直接的な攻撃が示されている[MSZ16]。この攻撃が実効性を持つダメージを与えるのかどうかまだ明らかではないが、証明可能な安全性の観点から、これらの解析を防ぐ技術を考案する必要がある。

[難読化技術]

難読化は、たいへん抽象度の高い概念であり、また、出力から漏れる情報に対する制約が大きい。多重線形写像を用いない難読化としては、point functions[Can97, CMR98, LPS04, Wee05, CD08, BC10]、testing hyperplane membership[CRV10]、その他単純なプログラム[HRsV07, HMLS07, Had10, CCV12] など、限られた単純なプログラムについていくつか結果が示されている。一方、多重線形写像を用いた任意のプログラムに適用可能な難読化が提案されている[GGH+15]。その後、数多くの関連論文が発表されている。

技術的な構成としては、難読化はプログラムを暗号化したうえで、本来求められる入力に対する処理を同様に実行することができ、また、含まれる値がゼロか否かのチェックが可能であることが求められる。安全性としては、”任意の多項式を処理し得られるランダムな値と区別がつかないことから、一切の情報を漏らしていない”、という扱いとなる。

難読化の理想的な挙動（難読化されたプログラムを攻撃者が入手したとしても、ブラックボックスにオラクルアクセスして得られる以上の情報を一切得られない）を定式化した概念として、Virtual black box obfuscation(VBB) がある。VBB については任意の function に対する構成不可能性は示されているものの、conjunctions [BR13, BR14a, BVWW16] などの特定の functions や idealized model 上での任意の回路[BR14b, BGK+14] などは示されている。

VBB の構成不可能性については、[BGI+01] で示され、さらに[BGK+14]でより一般的な結果が導かれている。しかしこれら不可能性の結果は、generic multilinear attack の設定の範囲内に対しては適用されない。実際 generic multilinear attack を想定したモデルでは VBB が構成可能であることが示されている [BR14b, BGK14+]。これらの結果は、少なくとも多重線形写像に対して algebraic attack が存在せず、″natural″ function に対して、強い(より好ましい) 安全性を満たす難読化が構成可能であることを意味している。

[アプリケーション]

難読化は多種多様なアプリケーションの提供に寄与できる可能性を秘めている。例えば、

1ラウンド複数人鍵交換[2](one-round multi-party key-exchange protocol)など、従来技術だけでは達成しえなかったアプリケーションの提供が可能となる。その他、Nash Equilibrium[3]の探索困難性の証明[BPR15, GPS15]や general circuit に対する関数暗号の構成[GGH+13b]などに用いられている。その他、[GGSW13] で提唱された witness encryption についても、indistinguishability obfuscation(iO) を用いることで構成可能であることを示している[GGH+13b]。

[参考文献]

[BGI+01] Boaz Barak, Oded Goldreich, Russell Impagliazzo, Steven Rudich, Amit Sahai, Salil P. Vadhan, Ke Yang: On the (Im)possibility of Obfuscating Programs. CRYPTO 2001: 1-18

[GGH+13b] Sanjam Garg, Craig Gentry, Shai Halevi, Mariana Raykova, Amit Sahai, Brent Waters: Candidate Indistinguishability Obfuscation and Functional Encryption for all Circuits. FOCS 2013: 40-49.

[CLT13]Jean-Sébastien Coron, Tancrède Lepoint, Mehdi Tibouchi: Practical Multilinear Maps over the Integers. CRYPTO (1) 2013: 476-493

[CLT15] Jean-Sébastien Coron, Tancrède Lepoint, Mehdi Tibouchi: New Multilinear Maps Over the Integers. CRYPTO (1) 2015: 267-286

[GGH15] Craig Gentry, Sergey Gorbunov, Shai Halevi: Graph-Induced Multilinear Maps from Lattices. TCC (2) 2015: 498-527

[CHL+15] Jung Hee Cheon, Kyoohyung Han, Changmin Lee, Hansol Ryu, Damien Stehlé: Cryptanalysis of the Multilinear Map over the Integers. EUROCRYPT (1) 2015: 3-12

[CLR15] Jung Hee Cheon, Changmin Lee, Hansol Ryu: Cryptanalysis of the New CLT Multilinear Maps. IACR Cryptology ePrint Archive 2015: 934 (2015)

[CLLT15] Jean-Sébastien Coron, Moon Sung Lee, Tancrede Lepoint, and Mehdi Tibouchi: Cryptanalysis of GGH15 Multilinear Maps. IACR Cryptology ePrint Archive 2015: 1037 (2015)

[JHC16] Jung Hee Cheon, Jinhyuck Jeong, Changmin Lee: An Algorithm for NTRU Problems and Cryptanalysis of the GGH Multilinear Map without an Encoding of Zero. IACR Cryptology ePrint Archive 2016: 139 (2016)

[MA16] Martin Albrecht, Shi Bai, Léo Ducas: A subfield lattice attack on overstretched NTRU assumptions: Cryptanalysis of some FHE and Graded Encoding Schemes. IACR Cryptology ePrint Archive 2016: 127 (2016)

[MSZ16] Eric Miles, Amit Sahai, Mark Zhandry: Annihilation Attacks for Multilinear Maps:

[2] 複数ユーザが各々の値を1回ブロードキャストすることで複数ユーザが同時に共通の鍵を共有する鍵交換プロトコル。

[3] ゲーム理論における非協力ゲームの解の一種であり、いくつかの解の概念の中で最も基本的な概念。

Cryptanalysis of Indistinguishability Obfuscation over GGH13. IACR Cryptology ePrint Archive 2016: 147 (2016)

[Can97] Ran Canetti: Towards Realizing Random Oracles: Hash Functions That Hide All Partial Information. CRYPTO 1997: 455-469

[CMR98] Ran Canetti, Daniele Micciancio, Omer Reingold: Perfectly One-Way Probabilistic Hash Functions (Preliminary Version). STOC 1998: 131-140

[LPS04] Ben Lynn, Manoj Prabhakaran, Amit Sahai: Positive Results and Techniques for Obfuscation. EUROCRYPT 2004: 20-39

[Wee05] Hoeteck Wee: On obfuscating point functions. STOC 2005: 523-532

[CD08] Ran Canetti, Ronny Ramzi Dakdouk: Obfuscating Point Functions with Multibit Output. EUROCRYPT 2008: 489-508

[BC10] Nir Bitansky, Ran Canetti: On Strong Simulation and Composable Point Obfuscation. CRYPTO 2010: 520-537

[HRsV07] Susan Hohenberger, Guy N. Rothblum, Abhi Shelat, Vinod Vaikuntanathan: Securely Obfuscating Re-encryption. TCC 2007: 233-252

[HMLS07] Dennis Hofheinz, John Malone-Lee, Martijn Stam: Obfuscation for Cryptographic Purposes. TCC 2007: 214-232

[Had10] Satoshi Hada: Secure Obfuscation for Encrypted Signatures. EUROCRYPT 2010: 92-112

[CCV12] Nishanth Chandran, Melissa Chase, Vinod Vaikuntanathan: Functional Re-encryption and Collusion-Resistant Obfuscation. TCC 2012: 404-421

[BR13] Zvika Brakerski, Guy N. Rothblum: Obfuscating Conjunctions. CRYPTO (2) 2013: 416-434

[BR14a] Zvika Brakerski, Guy N. Rothblum: Black-box obfuscation for d-CNFs. ITCS 2014: 235-250

[BVWW16] Zvika Brakerski, Vinod Vaikuntanathan, Hoeteck Wee, Daniel Wichs: Obfuscating Conjunctions under Entropic Ring LWE. ITCS 2016: 147-156

[BR14b] Zvika Brakerski, Guy N. Rothblum: Virtual Black-Box Obfuscation for All Circuits via Generic Graded Encoding. TCC 2014: 1-25

[BGK+14] Boaz Barak, Sanjam Garg, Yael Tauman Kalai, Omer Paneth, Amit Sahai: Protecting Obfuscation against Algebraic Attacks. EUROCRYPT 2014: 221-238

[BPR15] Nir Bitansky, Omer Paneth, Alon Rosen: On the Cryptographic Hardness of Finding a Nash Equilibrium. FOCS 2015: 1480-1498

[GPS15] Sanjam Garg, Omkant Pandey, Akshayaram Srinivasan: On the Exact Cryptographic Hardness of Finding a Nash Equilibrium. IACR Cryptology ePrint Archive 2015: 1078 (2015)

[GGSW13] Sanjam Garg, Craig Gentry, Amit Sahai, Brent Waters: Witness encryption and its applications. STOC 2013: 467-476

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
☆	Improving NFS for the Discrete Logarithm Problem in Non-prime Finite Fields [Eurocrypt 2015]	62
☆	The Multiple Number Field Sieve with Conjugation and Generalized Joux-Lercier Methods [Eurocrypt 2015]	62
	Cryptanalysis of the Multilinear Maps over the Integers [Eurocrypt 2015]	63
★	Last Fall Degree, HFE, and Weil Descent Attacks on ECDLP [Crypto 2015]	65
☆	Computing Individual Discrete Logarithms Faster in GF(p^n) with the NFS-DL Algorithm [Asiacrypt 2015]	72
☆	Multiple Discrete Logarithm Problem with Auxiliary Inputs [Asiacrypt 2015]	72
★	Solving Linear Equations Modulo Unknown Divisors: Revisted [Asiacrypt 2015]	73
☆	The Tower Number Field Sieve [Asiacrypt 2015]	74
	How to Sequentialize Independent Parallel Attacks? [Asiacrypt 2015]	77
★	Algebraic Approaches for the Elliptic Curve Discrete Logarithm Problem over Prime Fields [PKC 2016]	78
	Degenerate Curve Attacks: Extending Invalid Curve Attacks to Edwards Curves and Other Models [PKC 2016]	78
★	Easing Coppersmith Methods Using Analytic Combinatorics: Applications to Public-Key Cryhptography with Weak Pseudorandomness [PKC 2016]	78
	How to Generalize RSA Cryptanalyses [PKC 2016]	78
ブロック暗号		**頁**
	A Generic Approach to Invariant Subspace Attacks: Cryptanalysis of Robin, iSCREAM and Zorro [Eurocrypt 2015]	62
	Structural Evaluation by Generalized Integral Property [Eurocrypt 2015]	62
	Cryptanalysis of SP Networks with Partial Non-Linear Layers [Eurocrypt 2015]	62
	Differential Cryptanalysis of the BSPN Block Cipher Structure [Lightweight Cryptography Workshop 2015]	64
	On Reverse-Engineering S-Boxes with Hidden Design Criteria or Structure [Crypto 2015]	64
★	Integral Cryptanalysis on Full MISTY1 [Crypto 2015]	65
☆	New Attacks on Feistel Structures with Improved Memory Complexities [Crypto 2015]	65
	Key-Recovery Attacks on ASASA[Asiacrypt 2015]	73
	Optimized Interpolation Attacks on LowMC [Asiacrypt 2015]	75

2. Eurocrypt 2015 の発表

2.1. Eurocrypt 2015 の発表(1 日目)

Improving NFS for the Discrete Logarithm Problem in Non-prime Finite Fields [Eurocrypt 2015]

Razvan Barbulescu, Pierrick Gaudry, Aurore Guillevic, François Morain

GF(p^n)の n が小さい場合に、多項式選択を改良することにより漸近計算量を Lp^n(1/3,2.201)に改良した。P が 90 桁、GF(p^2)が 180 桁/595 ビットの場合の記録を達成した。トーラスベース暗号やペアリングベース暗号の安全性評価に影響がある。

The Multiple Number Field Sieve with Conjugation and Generalized Joux-Lercier Methods[Eurocrypt 2015]

Cécile Pierrot

中程度の標数の場合に、Multiple NFS と Conjugation Method を組合せ、漸近計算量をこれまでの最良計算量 Lp^n (1/3,2.201)から Lp^n (1/3, 2.156)に改良した。同様に、MNFS と一般 Joux-Lercier 法と組み合わせることにより、中程度から大標数の境界ケースにおいて、漸近計算量を改良した。

A Generic Approach to Invariant Subspace Attacks: Cryptanalysis of Robin, iSCREAM and Zorro [Eurocrypt 2015]

Gregor Leander, Brice Minaud, Sondre Rønjom

不変部分空間攻撃は、Crypto 2011 において PRINTCIPHER の暗号解析のために導入された。この場合不変部分空間はややアドホックな方法で発見されたため、他の暗号に対する不変部分空間を一般的に発見する方法は未解決問題となっていたが、本論文ではそのアルゴリズムを提示する。更にそのアルゴリズムを、CAESAR 候補である iSCREAM、関係の深い Robin、軽量暗号 Zorro に適用する。これらの不変部分空間は発見され、現実的な解読につながった。

Structural Evaluation by Generalized Integral Property [Eurocrypt 2015]

Yosuke Todo

Feistel ネットワークおよび SPN に対する構造的暗号解析を示す。integral 暗号解析において Division property と呼ぶ新しい性質を導入し、integral distinguisher を改良した。Keccak-f および SIMON に適用し、有効性を確認した。例えば、Keccak-f に対する 10 段識別に必要な選択平文の数を 2^{1025} から 2^{515} に削減した。Feistel 暗号に対しては、SIMON 32, 48, 64, 96,128 はそれぞれ 9, 11, 11, 13, 13 段 integral 識別を持つことを理論的に証明した。今後他の暗号に適用した場合の影響を注視する必要がある。

Cryptanalysis of SP Networks with Partial Non-Linear Layers [Eurocrypt 2015]

Achiya Bar-On, Itai Dinur, Orr Dunkelman, Nathan Keller, Virginie Lallemand, Boaz Tsaban

本論文では、部分的非線型層を持つ SP ネットワーク構造の一般的な差分・線型攻撃テクニックを提示する。本技術は暗号解析にも安全性証明にも利用することができる。本暗号解析を Zorro に適用し、デスクトップ PC1 台で数日間でシミュレートできる現実的な攻撃を得た。また、Zorro に若干の変更を加え、基本的な差分・線型攻撃に対する安全性を証明した。

2.2. Eurocrypt 2015 の発表(2 日目)

Cryptanalysis of the Multilinear Maps over the Integers [Eurocrypt 2015]

Jung Hee Cheo, Kyoohyung Han, Changmin Lee, Hansol Ryu, Damien Stehlé

Coron-Lepoint-Tibouchi に対する多項式時間攻撃を提案し、最優秀論文賞を受賞した。本攻撃は GGH(Garg-Gentry-Halevi)の多重線型写像候補に対するゼロ攻撃を採用しており、GGH に対するより影響が大きい。GGH の場合、ペアリングベース暗号からの Decision Linear 問題と部分集合メンバーシップ問題の一般化を解くが、CLT の場合は完全解読となる。

2.3. Eurocrypt 2015 の発表(4 日目)

Cube Attacks and Cube-attack-like Cryptanalysis on the Round-reduced Keccak Sponge Function [Eurocrypt 2015]

Itai Dinur, Pawel Morawiecki, Josef Pieprzyk, Marian Srebrny, Michal Straus

SHA-3(Keccak)の鍵バリアントの代数攻撃に対する耐性を包括的に調べる。鍵回復、MAC 偽造等広範囲の攻撃をカバーし Keccak 内部置換を 9 段(full は 24 段)まで、全数探索より高速に解読した。そのうちのいくつかは、6 段ならば完全に実際的な攻撃となり、PC 上で検証した。本攻撃は Cube 攻撃と Keccak 置換の構造解析に関連する代数的テクニックを組み合わせたものである。Keyak(Keccak ベースの認証暗号)に対する攻撃では 12 段まで可能となり、セキュリティマージンはより小さい。いずれにしてもマージンはまだ大きいが、これらのテクニックは Keccak や同様の設計の暗号解析に将来役に立つであろう。

Twisted Polynomials and Forgery Attacks on GCM [Eurocrypt 2015]

Mohamed Ahmed Abdelraheem, Peter Beelen, Andrey Bogdanov, Elmar Tischhauser

デンマークの Abdelraheem らが、認証暗号に対する偽造攻撃を発表した。多項式ハッシュを用いる方式に対し、偽造多項式を構成することによる攻撃が知られていたが、偽造多項式の構成法は見つかっていなかった。今回の発表では、偽造多項式の構成法を提案し、CRYPTREC 暗号リストに掲載されている認証つき秘匿モード GCM(Galois Counter Mode)を、弱鍵モデル（弱鍵を持つという条件）のもとで、ナンスを再利用せずに偽造する攻撃に初めて成功した。攻撃の成功する条件等の現実性について詳細に評価する必要がある。

3. LIGHTWEIGHT CRYPTOGRAPHY WORKSHOP 2015 の発表

3.1. LIGHTWEIGHT CRYPTOGRAPHY WORKSHOP 2015 の発表(2 日目)

Some Observations on ACORN v1 and Trivia-SC [Lightweight Cryptography Workshop 2015]

Rebhu Johymalyo Josh, Santanu Sarkar

CAESAR 候補の ACORN に対し、鍵、初期値、関連データ長を固定し、全関連データについて出力を XOR すると最初のうち 0 が続く現象を発見した。10 から 18 ビットの間で関連データ長を変えながら出力の XOR が何ビットまで 0 になるか実験し、その結果を利用して XOR 値の連続が 512 ビットに到達する関連データ長を外挿したところ、37 から 45 ビットという

値を得た。筆者らはこの結果を踏まえ、状態更新回数を現状の「関連データ長＋512」回から「関連データ長＋1024」回に増やすことを提案している。

CAESAR 候補の TriviA-ck-v1 は部品としてストリーム暗号 Trivia-SC を利用している。Trivia-SC はパディングが対称であるため、スライド攻撃によって容易に攻撃できることが指摘されており、攻撃者はパディングを非対称にすることを提案している。本論文ではパディングを非対称化した改良版 Trivia-SC に対し、スライド攻撃に必要な slid ペアの探索を試み、256 変数 128 の連立方程式を SAT solver を利用して解くことによって、初期状態から 280 ビットシフトした際の slid ペアを約 407 秒で見つけた。

A New Distinguisher on Grain v1 for 106 rounds [Lightweight Cryptography Workshop 2015]

Santanu Sarkar

Grain v1 は eStream プロジェクトに選定されたストリーム暗号である。Asiacrypt 2010 では鍵スケジュール部を 97 ラウンドに減らした Grain v1 に対し、Knellwolf らが 2^{27} の選択した IV を用いて識別攻撃を行った。また、104 ラウンドに減らしたものに対し、2^{35} の選択した IV を利用して攻撃を行った。その後、Banik は同様の手法を用いて、105 ラウンドの新たな distinguisher を見つけた。本論文では、代数的条件を課したうえで探索空間を 64 分割してすべての IV ビットに 1 階差分を適用することで、63%の確率で新しい 106 ラウンドにおける distinguisher を得られることを示した。

Differential Cryptanalysis of the BSPN Block Cipher Structure [Lightweight Cryptography Workshop 2015]

Liam Keliher

BSPN(byte-oriented SPN)は SAC ’96 で Youssef らに提案された一般的なブロック暗号の構造であり、差分解析及び線形解析に耐性があると主張されている。本論文では、BSPN の線形変換の特性を考慮することで、たとえ AES のような s-box を用いたとしても差分解析を用いた攻撃を許すような高い確率の差分が存在することを示した。特に、ブロック長 64 ビットでは 9 ラウンドまで攻撃でき、ブロック長 128 ビットでは 18 ラウンドまで攻撃できることを示した。

4. Crypto 2015 の発表

4.1. Crypto 2015 の発表(1 日目)

On Reverse-Engineering S-Boxes with Hidden Design Criteria or Structure [Crypto 2015]

Alex Biryukov, Léo Perrin

S-box のリバースエンジニアリングに使うことのできるテクニックを調べ、設計プロセスがこれまで秘密にされている Skipjack 暗号の S-box F を例にとってその方法を記述する。初めに F の線型性質はランダムでないことを示し、設計クライテリアを提案する。次に S-box 分解の新しい方法を与える。最後に DDT エントリの多くを設計者の選んだ値に直すことのできる S-box 生成アルゴリズムを開発した。

4.2. Crypto 2015 の発表(3 日目)

Integral Cryptanalysis on Full MISTY1 [Crypto 2015]

Yosuke Todo

64 ビットブロック暗号 MISTY1 に対する暗号解読を発表した。Eurocrypt 2015 で発表した一般的な攻撃法を MISTY1 に適用した結果、1997 年の MISTY1 発表から 18 年目にして、解読計算量が初めて総当たり法を下回った。選択平文 $2^{63.58}$ の場合、時間計算量は 2^{121} であり、選択平文 $2^{63.994}$ の場合、時間計算量は $2^{107.9}$ である。本結果により、藤堂氏は、最優秀論文賞および最優秀若手研究者賞をダブル受賞した。藤堂氏の結果をイスラエルの Bar-On 氏がさらに改良した結果が Crypto 2015 のランプセッションで発表され、解読計算量は $2^{69.5}$ にまで下がっているが、解読に必要なデータ量は 2^{64} であり、まだ現実的な脅威とは言えない。

New Attacks on Feistel Structures with Improved Memory Complexities [Crypto 2015]

Itai Dinur, Orr Dunkelman, Nathan Keller, Adi Shamir

4 段以上の Feistel 構造に対する改良攻撃を述べる。中間一致攻撃の利点と dissection 攻撃とを組合せた新しい攻撃により本結果を達成した。例えば、n ビット入力、n/2 ビット 7 独立段鍵の 7 段 Feistel 構造に対し、中間一致攻撃は$(2^{1.5n}, 2^{1.5n})$時間、メモリを使うが、dessection 攻撃は、$(2^{2n}, 2^{n})$時間、メモリを使う。新しい攻撃では、少しの平文・暗号文ペアと、$(2^{1.5n}, 2^{n})$時間、メモリで済む。理論だけでなく、縮約 CAST-128(メモリ計算量を 2^{111} から 2^{64} に) 、full DEAL-256(メモリ計算量 2^{200} を 2^{144} に)に対し時間・データ計算量に影響を与えることなくメモリ計算量を削減した。

Last Fall Degree, HFE, and Weil Descent Attacks on ECDLP [Crypto 2015]

Ming-Deh A. Huang, Michiel Kosters, Sze Ling Yeo

Asiacrypt 2012 において Petit らは、ある仮定(「First Fall Degree」仮定と呼ばれる)の元に、楕円曲線暗号の解読計算量が準指数時間オーダーになることを示した。これに対し、アメリカ・南カリフォルニア大学の Huang 教授らは、この仮定の正当性に疑問を投げかけるデータを示し、解読計算量評価はより慎重に行うべきであると主張した。本論文の結果が正しいとすると、楕円曲線暗号は Petit らによる評価結果より安全であると考えられる。

4.3. Crypto 2015 の発表(4 日目)

Practical Free-Start Collision Attacks on 76-Step SHA-1 [Crypto 2015]

Pierre Karpman, Thomas Peyrin, Marc Stevens

フランスの Karpman らが SHA-1 圧縮関数の衝突攻撃評価を行った。GPU による実装を行い、76 段(フルは 80 段)を約 5 日で攻撃できることを示し、SHA-1 の使用を速やかに止めるように注意喚起を行った。なお、Free-Start とは仕様で固定されている初期ベクターを可変とすることで難度を下げた攻撃法であり、これが 80 段まで伸ばしただけでは SHA-1 の衝突発見には至らない。しかし、Free-Start による解析結果を利用して、仕様通りのハッシュ関数の衝突発見に導くことは可能であり、今後の進展を注視していく必要がある。

Fast Correlation Attacks over Extension Fields, Large-unit Linear Approximation and Cryptanalysis of SNOW 2.0 [Crypto 2015]

Bin Zhang, Chao Xu, Willi Meier

拡大体上の Fast Correlation 攻撃のフォーマルなフレームワークを与える。本方式を ISO/IEC 18033-4 標準である SNOW 2.0 ストリーム暗号に適用することにより、データ計算量 $2^{163.59}$、時間計算量 $2^{164.15}$ に削減することができる。Asiacrypt 2008 で発表されたこれまでの最良計算量よりも 2^{49} 倍良い結果である。

Cryptanalysis of Full Sprout [Crypto 2015]

Virginie Lallemand, María Naya-Plasencia

FSE 2015 においてストリーム暗号レジスタの内部状態サイズを削減する新しい手法が提案され、ハードウェア実装のエリア削減が可能となり、実装例として Sprout 暗号が提案された。本論文では Sprout のセキュリティを解析し、全数探索攻撃より 2^{10} 倍高速で、データ計算量が非常に小さい鍵回復攻撃を提案する。

Higher-Order Differential Meet-in-The-Middle Preimage Attacks on SHA-1 and BLAKE [Crypto 2015]

Thomas Espitau, Pierre-Alain Fouque, Pierre Karpman

高階差分をハッシュ関数の中間一致原像攻撃に初めて適用した。SHA-1 の攻撃段数を、パディングなし 1 ブロック原像の場合 62 段、パディングあり 1 ブロック原像の場合 56 段、パディングなし 2 ブロック原像の場合 62 段に改良した。更に SHA-3 ファイナリストである BLAKE およびその新版 BLAKE2 に対し、パディングあり 2.75 段原像、圧縮関数の 7.5 段擬原像攻撃を与えた。

5. FDTC 2015 の発表

Fault Attacks at the System Level-The Challenge of Securing Application Software [FDTC 2015]

Stefan Mangard

暗号実装攻撃の研究者はハードウェアに関心が集中している現状に対し、ソフトウェアを介した攻撃にも注意する必要性を指摘し、具体的例として“Row Hammer”を紹介した。“Row Hammer”とは、DRAM の行(Row)領域を高い頻度でアクセスすると隣の行の内容が書き換わる現象で、DRAM の信頼性に関わる問題として知られていたが、最近、サイドチャネル攻撃への利用が試みられている。これを利用したデータを書き換えにより、Linux kernel の権限昇格に成功した例も報告されている。対策として、Control-Flow Integrity(制御フロー完全性)を維持する方法を示した。

EM Injection: Fault Model and Locality [FDTC 2015]

Sebastien Ordas, Ludovic Guillaume-Sage and Philippe Maurine

故障利用攻撃の研究において、電磁妨害(EM injection)の利用が増えている。この論文では、電磁妨害によって引き起こされるのは、ビット設定に対するものでも、クロック動作が引き起こすタイミング故障でもなく、D-type Flip-Flop のサンプリング・プロセスに

おける擾乱によって引き起こされることを示した。さらに、電磁妨害は今まで考えられていたより局所的であることを明らかにした。

On the Complexity Reduction of Laser Fault Injection Campaigns using OBIC Measurements [FDTC 2015]

Falk Schellenberg, Markus Finkeldey, Bastian Richter, Maximilian Schaepers, Nils Gerhardt, Martin Hofmann and Christof Paar

レーザによって誤作動を起こす故障利用攻撃において、効果的なレーザ照射位置の特定が重要であり、従来その探索に必要な時間をいかに短縮するかの研究が行われてきた。フリップフロップ回路の位置は有効であり、走査型電子顕微鏡(SEM)画像による探索は有効であるが、時間と費用が掛かる。本論文では、光起電流(OBIC)を利用することによって、フリップフロップの位置を低コストで容易に高精度で特定できることが示された。

Improved Differential Fault Attack on the Block Cipher SPECK [FDTC 2015]

Yuming Huo, Fan Zhang, Xiutao Feng and Li-Ping Wang

米国 NSA はソフトウェア向けの軽量ブロック暗号 SPECK を提案しており、10 種類のパラメータ設定で、異なるブロック長・鍵サイズ、段数の組み合わせが利用できる。SPECK に対する故障利用攻撃の研究としては Tupsamudre らが FDTC 2014 で発表したものがあり、鍵の導出に平均でブロック長の 1/6 回のビット誤りが必要という結果が得られている。本論文では、法 2^n のモジュロ演算を 2 次以下の代数方程式に変換し、グレブナー基底の計算システム Singular を利用する方法を用いて、必要なビット誤り回数を下表のように削減した。

ブロック長	必要な誤り回数
32	5
48	5
64	6
96	7
128	8

J-DFA: A Novel Approach for Robust Differential Fault Analysis [FDTC 2015]

Luca Magri, Silvia Mella, Filippo Melzani, Pasqualina Fragneto and Beatrice Rossi

故障利用攻撃において、故障の起こり方を予め想定しておく。しかし、この想定から外れたデータが出力されると正しい鍵候補が捨てられる可能性がある。本論文では、そのような可能性をなくすため、クラスタリング手法 J-Linkage を応用した攻撃法 J-DFA を開発し、計算機実験でその有効性を確認した。

Lost in Translation: Fault Analysis of Infective Security Proofs [FDTC 2015]

Alberto Battistello and Christophe Giraudy

FDTC 2014 で Rauzy と Guilley が提案した CRT-RSA に対する高次故障利用攻撃への対策が、論文中に書かれた仮定の下で安全でなく、攻撃できることを示した。

An Efficient One-Bit Model for Differential Fault Analysis on Simon Family [FDTC

2015]

Juan Grados, Fabio Borges, Renato Portugal and Pedro Lara

NSA が設計した軽量ブロック暗号 Simon に対する故障利用攻撃としては、FDTC 2014 で Tupsamudre らが提案した 1 ビット・フリップ・モデルとランダム 1 バイト・モデルの２種類があり、それらを改良した高橋らのランダム n ビット・モデルが ICISC 2014 で提案されている。本論文では、故障を起こす位置を 1 段入力寄りにすることにより、全鍵導出に必要な故障の位置を半減することに成功した。ただし、故障を起こす回数は増加する。

Singular Curve Point Decompression Attack [FDTC 2015]

Johannes Blömer and Peter Günther

安全性の高い楕円曲線暗号の実装に対し、故障を利用して point decompression をスキップすることで、解くべき問題を弱い特異曲線上の離散対数問題に変換する攻撃法を提案した。その有効性は、AVR Xmega A1 上に実装されたペアリング・ベースの Boneh-Lynn-Shacham short signature scheme に対する攻撃で実証された。この攻撃が特に有効な楕円曲線は、j-invariant が 0 のものである。

Improving Fault Attacks on Embedded Software using RISC Pipeline Characterization [FDTC 2015]

Bilgiday Yuce, Nahid Farhady Ghalaty and Patrick Schaumont

パイプライン・アーキテクチャの RISC プロセッサの構造を解析することによって、暗号計算のソフトウェアにおいて最も故障を起こしやすい箇所をピンポイントで特定する方法論を示した。その有効性を、Spartan6 FPGA でマップされた 7-stage pipeline LEON3 プロセッサに適用することで実証した。

6. CHES 2015 の発表

6.1. CHES 2015 の発表(1 日目)

Robust Profiling for DPA-Style Attacks [CHES 2015]

Carolyn Whitnall, Elisabeth Oswald

計測波形の歪みに強い DPA 攻撃の識別子(distinguisher)を設計し、幅広い歪みに対して非常に有効であることを確認した。識別子の設計には、平均トレース、主成分分析と教師なし機械学習が利用される。

Less is More -- Dimensionality Reduction, from a Theoretical Perspective [CHES 2015]

Nicolas Bruneau, Sylvain Guilley, Annelie Heuser, Damien Marion, Olivier Rioul

サイドチャネル攻撃を実施する際に直面することの一つにデータの次元が大きいため、計算量が膨大になることがある。本論文では、攻撃成功率の低下を起こさない次元圧縮方法を線形結合を利用して構成した。さらに、この次元圧縮が線形判別分析(linear discriminant analysis)に漸近的に一致することを理論的に示した。また、主成分分析よりも成功率が高い。

Blind Source Separation from Single Measurements using Singular Spectrum Analysis [CHES 2015]

Santos Merino Del Pozo, François-Xavier Standaert

サイドチャネル攻撃で使用する測定波形のノイズ除去に特異スペクトル分析(SSA)を導入した。SSA の長所は、主成分分析(PDA)や独立成分分析(LDA)のように成分を固有値でランキングできることと、サンプリングレートが低くても利用できることの２点である。有効性確認のため、ブロック暗号 PRESENT を３つの環境（対策なしソフトウェア、マスクで対策を施したソフトウェア、対策なしのハードウェア）で実験したところ、いずれも SN 比の向上が見られた。

6.2. CHES 2015 の発表(2 日目)

Stealing Keys from PCs using a Radio: Cheap Electromagnetic Attacks on Windowed Exponentiation [CHES 2015]

Daniel Genkin, Lev Pachmanov, Itamar Pipman, Eran Tromer

Genkin らは Crypto 2014 と CHES 2014 において、RSA と ElGamal が動作している PC が放出する電波を測定することで鍵を導出する２種類の攻撃を提案した。１つは長波／超長波(15-40kHz)を用いた非適応的選択暗号文攻撃で、測定は数秒で済むものの高価な低ノイズの測定器が必要である。もう一つは中波(2MHz)を用いた適応的選択暗号文攻撃で、通常の測定機器で済むものの 1 時間程度の測定が必要である。さらに両者は最近の windowed exponentiation を利用した実装には適用できない。本論文では、復号の際に中間データが特定の構造を持ち、電磁波に揺らぎを起こすようにすることで、ポータブルラジオやループアンテナなど安価な機器でも数秒の測定で済む改良攻撃を示した。

Exclusive Exponent Blinding May Not Suffice to Prevent Timing Attacks on RSA [CHES 2015]

Werner Schindler

RSA の CRT とモンゴメリ乗算を利用した実装において、指数マスクはタイミング攻撃対策として有効と考えられてきた。本論文では新規の識別子(distinguisher)を利用することで、鍵が導出できることを示した。ただし、攻撃の計算量は対策なしのときと比べ非常に大きくなる。

Who Watches the Watchmen?：Utilizing Performance Monitors for Compromising Keys of RSA on Intel Platforms [CHES 2015]

Sarani Bhattacharya, Debdeep Mukhopadhyay

Hardware performance counter (HPC)は、マイクロプロセッサ内の活動に関するカウントを行う特殊用途のレジスタである。本論文では RSA の計算における分岐に着目し、HPC の出力を利用して秘密鍵の導出に成功した。

Improved Cryptanalysis of the DECT Standard Cipher [CHES 2015]

Iwen Coisel, Ignacio Sanchez

コードレス電話の秘匿通信規格 DECT では、64 ビット鍵のストリーム暗号 DST が利用され

ている。DST のアルゴリズムは非公開であったが、FSE 2010 で Nohl らはリバースエンジニアリングした結果を公開した。同論文には暗号解析の結果も書かれており、最良の環境では 10 分程度の通信傍受で既知平文攻撃が成功することを示した。本論文では攻撃を改良し、通信傍受の時間を 3 分に短縮した。攻撃では 2^{13} 個の鍵ストリームを解析し、2^{31} 回の鍵探索によって 50%の成功率で鍵の導出に成功した。

Practical Key Recovery for Discrete-Logarithm Based Authentication Schemes from Random Nonce Bits [CHES 2015]

Aurélie Bauer, Damien Vergnaud

RSA 暗号については、秘密鍵の一部ビットが与えられた条件下での鍵復元が研究されている。本論文では、Schnorr の同定スキームや Girault-Poupard-Stern(GPS)の同定・署名スキームのような離散対数問題ベースの認証スキームに対する統計的攻撃を示した。nonce の与え方について２つの攻撃シナリオが提示されている。一つは nonce の 1 ビットだけが正確に分かっているとするもの、もう一つは全ビットが示されているが独立に小さな確率で反転しているとするもの。前者のシナリオで、GPS スキームが 710 個の署名生成で攻撃できる。

Improved Side-Channel Analysis of Finite-Field Multiplication [CHES 2015]

Sonia Belaïd, Jean-Sébastien Coron, Pierre-Alain Fouque, Benoît Gérard, Jean-Gabriel Kammerer, Emmanuel Prouff

AES の GCM モードに対する攻撃に、128 ビット有限体の乗算に着目する方法がある。Belaid らは Asiacrypt 2014 において、最下位ビットを利用する方法を提案した。しかし、最下位ビットはノイズの影響を受けやすいので、本論文では代りに最上位ビットを利用する方法により、ノイズ耐性が格段に向上することを確認した。GF(2^{128})上の乗算に適用した例では、SN 比が 8 でも、2^{20} 個の消費波形、時間複雑度 $2^{51.68}$、計算複雑度 2^{36} で攻撃できる。

Evaluation and Improvement of Generic-Emulating DPA Attacks [CHES 2015]

Weijia Wang, Yu Yu, Junrong Liu, Zheng Guo, François-Xavier Standaert, Dawu Gu, Sen Xu, Rong Fu

Whitnall らは CT-RSA 2014 において、相互情報量解析(MIA)や線形回帰(LR)ベースの解析などのデバイス固有の性質を仮定しない汎用 DPA は、単射関数を利用した暗号実装に対して有効でないことの証明を示した。さらに、条件をわずかに緩めることで、汎用 DPA を有効にした generic-emulating DPA を提案した。本論文では、generic-emulating DPA の２つの欠点、ノイズに弱いことと効率の悪さ(スマートカードにおいて顕著)を解決する方法を提案した。提案手法では、回帰分析に基づく２種類の識別子と、cross-validation が利用されている。

Transient-Steady Effect Attack on Block Ciphers [CHES 2015]

Yanting Ren, An Wang, Liji Wu

回路のゲート出力は、計算途中の一時的な値をしばらく保持した後、最終的な出力結果に切り替わる。この現象は transient-steady effect(TSE)と呼ばれる。本論文が提案する TSE 攻撃では、クロック・グリッチを注入することで、この一時的な値を取り出すことで鍵を導出する。TSE 攻撃の有効性を確認するため、Altera Cyclone IV チップを搭載した DE2-115

FPGA ボードに実装したマスク有り無し両方の AES に対して実験した。その結果、マスク無しでは暗号化１回、マスク有りでは暗号化 20 回で鍵の導出に成功した。

6.3. CHES 2015 の発表(3 日目)

Assessment of Hiding the Higher-Order Leakages in Hardware, What Are the Achievements Versus Overheads? [CHES 2015]

Amir Moradi, Alexander Wild

DPA 対策として対策の次数を上げるのではなく、次の２つを組み合わせる方法を提案した。

(1) １次の対策: threshold implementation (TI)

(2) 電力の平準化: glitch-free duplication (GliFreD)

有効性確認するため、Spartan-6 FPGA 上での実装により、次の２種類と比較し、有効性を確認した。

(a) １次 TI で、電力平準化 GliFreD はなし

(b) ２次 TI で、電力平準化 GliFreD はなし

Multi-variate High-Order Attacks of Shuffled Tables Recomputation [CHES 2015]

Nicolas Bruneau, Sylvain Guilley, Zakaria Najm, Yannick Teglia

サイドチャネル攻撃対策のパーツに、データを d 個のシェアに分けるマスク法があるが、d 次のサイドチャネル攻撃で破れることが知られている。本論文では、次数を d より大きくすることで、攻撃効率が向上することを理論的に示した。

DPA, Bitslicing and Masking at 1 GHz [CHES 2015]

Josep Balasch, Benedikt Gierlichs, Oscar Reparaz and Ingrid Verbauwhede

スマートフォンやタブレットで利用されるハイエンドのプロセッサである Sitara ARM Cortex-A8 32-bit RISC processor(1GHz)に実装された AES に対する DPA に成功するとともに、この攻撃に対するゲートレベルの対策を実施して有効性を確認した。攻撃対象はタイミング攻撃が無効な AES のビットスライス実装であり、数千波形の観測で鍵の導出に成功した。ゲートレベルの対策では、中間データをマスクで防御するもので、DPA に必要な波形数は約２桁に増加した。

SoC it to EM: ElectroMagnetic Side-Channel Attacks on a Complex System-on-Chip [CHES 2015]

Jake Longo, Elke De Mulder, Dan Page, Michael Tunstall

サイドチャネル攻撃の対象として、新しく複雑な Texas Instruments AM335x SoC 上に実装された AES に対する電磁波解析に成功した。攻撃対象の AES 実装は次の３種。

(1) ARM core 上の OpenSSL Server の実装

(2) proprietary AES co-processor

(3) ビットスライス AES を含んだ NEON core

Finding the AES Bits in the Haystack: Reverse Engineering and SCA Using Voltage Contrast [CHES 2015]

Christian Kison, Jürgen Frinken, Christof Paar

電磁波解析において、暗号処理が実行される Region of Interest (ROI)の特定が重要で時間が掛かる作業となっている。従来、近接場測定や光子検出などが利用されてきたが、本論文では走査型電子顕微鏡(SEM)を利用する方法を提案している。攻撃対象は XMEGA microprocessor 上の AES 実装であり、電位コントラスト(VC)を利用して ROI を特定し、テンプレート攻撃と単純電磁波解析で各々、全鍵の導出に成功している。

7. PROOFS 2015 の発表

Buffer Overflow Attack with Multiple Fault Injection and a Proven Countermeasure [PROOFS 2015]

Shoei Nashimoto, Naofumi Homma, Yu-ichi Hayashi, Takafumi Aoki

C 言語を利用したソフトウェア実装に対するバッファ・オーバーフロー(BOF)攻撃対策の一つにメモリコピーのサイズを制限する方法がある。これを無効化するために多重故障を注入して命令をスキップさせる方法を提案し、SASEBO-W に設置された AVR ATmega163(8 bit)上への実装に適用して有効性を確認した。さらに分岐命令を置き、ループカウンタを置くことで異常を検知する対策を提案し、可能な攻撃パターンの全てが失敗することを示し安全性を証明した。

8. Asiacrypt 2015 の発表

8.1. Asiacrypt 2015 の発表(1 日目)

Tradeoff Cryptanalysis of Memory-Hard Functions [Asiacrypt 2015]

Alex Biryukov, Dmitry Khovratovich

意図している量よりも少ないメモリが使われる場合に、大きな計算量／時間のデメリットが生じる「メモリ hard 関数」に対し、タイム・メモリ等のトレードオフを研究した。本研究では、パスワード・ハッシュ・コンペティションのファイナリストのうち Catena、yescrypt、Lyra2 の 3 つを対象として解析した。設計者らは本研究における解析を踏まえて、Catena, Lyra2 について新しいモードの追加を行った。

Computing Individual Discrete Logarithms Faster in GF(pn) with the NFS-DL Algorithm [Asiacrypt 2015]

Aurore Guillevic

離散対数問題を解く数体篩法は、多項式選択、関係収集、線型代数、離散対数計算の 4 つのステップからなる。最終ステップの離散対数計算は、素体および 2 次拡大体の場合に比べて、中程度の標数および大標数で拡大次数が 3 以上の場合の方が、遅くなる。本論文では、離散対数計算の最初のステップ(booting step)を、原像ノルムのサイズを劇的に削減することにより最適化した。拡大次数が 2～6 の場合に非常に有効であり、中程度もしくは大標数の任意の拡大体に対して適用できる。

Multiple Discrete Logarithm Problem with Auxiliary Inputs [Asiacrypt 2015]

Taechan Kim

補助的な入力のある、複数 DLP 問題に対する解法を与える。g を素数位数 p の有限体の元とし、α_1、・・・α_Lを Z/pZ の元とする。g、g^{α_i} 、・・・、$g^{\alpha_i d}$ (i=1～L)が、ある d|p-1 に対して与えられたとき、またすべての d に対して与えられたときの、α i に関する離散対数を求めるアルゴリズムおよび計算量を示した。

Solving Linear Equations Modulo Unknown Divisors: Revisted [Asiacrypt 2015]

Yao Lu, Rui Zhang, Liqiang Peng, Dongdai Lin

既知の合成数 N の未知因子 p を法とする線型方程式群の小さい解を求める問題を再訪する。複数のパラメータを導入することにより、方程式の一般化をいくつか提案する。変形 RSA に対するいくつかの攻撃はこれらの一般系に帰着されるが既知のアルゴリズムは適用できなかった。今回アルゴリズムにより、以下のケースで最良の解析/実験結果を得た。

－$N=p^rq$(r：2 以上)の場合の May(PKC2004)の小さな秘密指数攻撃に関する結果の改良

－$N=p^rq$(r:2 以上)で既知ビットのある素因数分解に関する Boneh らのアルゴリズム(Crypto 1998)を実験的に改良

－共通素因子 RSA 問題(p-1 と q-1 が大きな共通素因子を持つ場合)に対する Jochemsz-May の攻撃(Asiacrypt 2006)を大幅に改良

－RSA/CRT-RSA の弱い暗号化指数に関する Nitaj の結果(Africacrypt 2012)の拡張

8.2. Asiacrypt 2015 の発表(2 日目)

Key-Recovery Attacks on ASASA [Asiacrypt 2015]

Brice Minaud, Patrick Derbez, Pierre-Alain Fouque, Pierre Karpman

ASASA 構成は Asiacrypt2014 において Biruykov らにより導入された新しい暗号設計スキームであり、2 つの公開鍵スキーム、1 つの秘密鍵スキーム、ホワイトボックススキームの super S-box 等の構成に利用されているが、CRYPTO 2015 において Gilbert らにより 1 つの公開鍵スキームが解読された。本論文により提案された新しい代数的鍵回復攻撃により、秘密鍵スキームおよび残りの公開鍵スキームは各々2^{63}、2^{39}の時間計算量で解読された(セキュリティパラメータはどちらの場合も 128 ビット)。更に、公開鍵スキームの方は、別の攻撃によりヒューリスティックではあるが解読可能なパラメータの LPN 問題に帰着される。また、ホワイトボックススキームに対する非常に効率的なヒューリスティック攻撃により 64 ビットセキュリティが主張されていたインスタンスがデスクトップ PC1 台で 1 分以下で解読された。

ASCA, SASCA and DPA with Enumeration: Which One Beats the Other and When? [Asiacrypt 2015]

Vincent Grosso, François-Xavier Standaert

Asiacrypt 2014 において導入された SASCA(Soft Analytical Side-Channel Attacks)に関する 3 点の貢献。

－代数的サイドチャネル攻撃(ASCA: Algebraic Side-Channel Attacks)と比較し、ノイズのないシミュレーション設定において SASCA の方においてより効率的な鍵回復が認められた。

－実際の AES 実装に対する初めての SASCA 実験。DPA に対する利点。

ー数え上げを実行する計算パワーを強化された場合の SASCA と DPA との距離を評価し、両攻撃のギャップは非常に削減されることを示した。

Counting Keys in Parallel After a Side Channel Attack [Asiacrypt 2015]
Daniel P. Martin, Jonathan F. O'Connell, Elisabeth Oswald, Martijn Stam
サイドチャネル攻撃により得られた情報が不十分である場合に、残りの手間を評価する手法を提案した。まず、あるサイドチャネル攻撃のスコアに従って順序づけられたすべての鍵リストにおけるある鍵のランクを正確に計算する非常に効率的なアルゴリズムの構成法を示した。次に、最も可能性の高い鍵を並行して数え上げるための改良を示した。

A Unified Metric for Quantifying Information Leakage of Cryptographic Devices under Power Analysis Attacks [Asiacrypt 2015]
Liwei Zhang, A. Adam Ding, Yunsi Fei, Pei Luo
サイドチャネル電力解析攻撃に対する有効な対策を設計するためには、システム漏洩の評価は軽くなければならず、また暗号アルゴリズムやソースコードなど早い段階において行わなければならない。従って、実装や電力漏洩測定が可能でない場合には、セキュリティ評価はアルゴリズムの情報漏洩を測定する基準に従って行われなければならない。本論文では、このような一般的かつ統一的な測定基準 ILA(Information Leakage Amount)が提案された。様々な種類の攻撃(1 階/高階の DPA/CPA)に対する情報漏洩測定を統一的に行い、マスク防御のないアルゴリズムにも部分/完全マスク防御を持つアルゴリズムにも機能し、物理的な実装における攻撃成功率と関連するものであり、早い段階での対策設計に役立つものである。

How Secure is AES under Leakage [Asiacrypt 2015]
Andrey Bogdanov, Takanori Isobe
明確な漏洩が存在する場合の AES のセキュリティを研究する。即ち、各操作において内部秘密状態の一部が漏洩するものとする。また、限られたコントロールしか持たない攻撃者からより多くの計算基盤の知識を持ったより強力な攻撃まで、かなり広い範囲の設定を考慮する。漏洩から鍵回復を行うため、偏向差分攻撃等の新しい暗号解析技術を開発した。更に、これらの攻撃の元で、不確定要素および実装対策(ブラックボックスラウンド、空間ランダム化、時間ランダム化、ダミー操作)の影響を評価した。特に、不確定要素および基礎的な対策が取られているときには、AES のセキュリティマージンはかなり十分なものであることが見て取れた。

8.3. Asiacrypt 2015 の発表(3 日目)

The Tower Number Field Sieve [Asiacrypt 2015]
Razvan Barbulescu, Pierrick Gaudry, Thorsten Kleinjung
ペアリングベース暗号の安全性は GF(p^n)(n: n>1 なる小さな整数)の離散対数を計算する困難性に依拠している。現状最速のアルゴリズムは数体篩法(NFS: Number Field Sieve)であるが、p が特殊な形の場合(SNFS: Special NFS)は、Joux-Pierrot による高速版がある。本論文では、Shirokauer による tower 拡大に基づく TNFS(Tower NFS)は、Joux-Pierrot より高速になり得ることを、効率はスムーステストをされる要素のノルムの積のサイズに関

連するというモデルを基に示した。

Heuristic Tool for Linear Cryptanalysis with Applications to CAESAR Candidates [Asiacrypt 2015]

Christoph Dobraunig, Maria Eichlseder, Florian Mende

近年、暗号解析を自動的に行うツールが導入されているが、これらの多くは差分特性のみを扱うものであった。本論文では線型特性を見つけ出すためのヒューリスティックな探索ツールを示し、CAESAR 第一ラウンド候補 ASCON、ICEPOLE、KEYAK、Minalpher、PROST の置換に適用した。ASCON、ICEPOLE、KEYAK に関しては、縮退版の鍵回復または識別攻撃に将来つながるかもしれない差分特性を発見した。

Collision Attacks against CAESAR Candidates Forgery and Key-Recovery against AEZ and Marble [Asiacrypt 2015]

Thomas Fuhr, Gaëtan Leurent, Valentin Suder

本論文では、Marble、AEZ、COPA のような OCB モードにより喚起された認証暗号を解析した。Ferguson の攻撃は、これらのアルゴリズムに適用できないが、誕生日計算量により秘密マスクを復元できることを示した。秘密マスクの復元は簡単に偽造攻撃につながるが、Marble と AEZ v2/v3 に関しては、より破壊的な鍵復元攻撃につながる。Marble に関しては n ビット安全性主張に反し、AEZ に関しては安全性証明に適合するが、衝突攻撃によるマスター鍵復元を許す望ましくない性質であると主張された。

Optimized Interpolation Attacks on LowMC [Asiacrypt 2015]

Itai Dinur, Yunwen Liu, Willi Meier, Qingju Wang

LowMC は Eurocrypt 2015 において Albrecht らにより導入されたブロック暗号ファミリーの集まりであり、マルチパーティ計算、完全準同型暗号、ゼロ知識証明のインスタンスに最適化される。LowMC の独特の特徴は内部アフィン層はランダムに選択される点であり各ブロック暗号ファミリーは多くのインスタンスを持つ。本論文では補間攻撃(Jackobsen、Knudsen により導入された代数攻撃)を LowMC に対して行い、80 ビット鍵のインスタンスにおいて全体のインスタンスは全数探索よりも倍高速に破られ、128 ビット安全性は約 1000 倍高速に破られることを示した。

Another Tradoff Attack on Sprout-like Stream Ciphers [Asiacrypt 2015]

Bin Zhang, Xinxin Gong

Sprout は FSE 2015 で提案された、より短い内部状態を持つ新しい軽量ストリーム暗号であり、鍵ストリーム生成フェーズにおいて更新される鍵に依存する状態を使っている。本論文では設計枠組みを拡張し Sprout 風の暗号の安全性を統一的に研究した。新しい洞察はプリミティブから派生するベクトルブール関数の k-正規性を調べることにあり、時間／空間／データトレードオフ攻撃を開発した。c を小さい定数、x/y を前進/後退ステップ数としたとき、Sprout は、$[c(2x+2y-58)2^{71-x-y}]$ビットメモリ、2^{9+x+y}ビット鍵ストリームが与えられた時、2^{79-x-y}時間で解読される。

Reverse-Engineering of the Cryptanalytic Atack Used in the Flame Super-Malware [Asiacrypt 2015]

Max Fillinger, Marc Steven

2012 年 5 月に中東を狙った Flame と呼ばれるスパイマルウェアが発見され、Windows Update に中間一致攻撃を行い、MD5 への選択プレフィックス攻撃で可能となる偽造署名を使うことにより Windows マシンに感染することがわかった。本論文では、ある弱い論理仮定を用いることにより衝突攻撃のかなりの部分を再構成した。実世界で利用されたアカデミックでない暗号解析攻撃のリバースエンジニアリングは前例がないと思われる。

Analysis of SHA-512/224 and SHA-512/256 [Asiacrypt 2015]

Christoph Dobraunig, Maria Eichlseder, Florian Mendel

オーストリアのグラーツ工科大学が SHA-512 に対する衝突攻撃を発表した。仕様で固定されている初期ベクターを可変とすることで攻撃難度を下げた攻撃法の場合、SHA-512/224 で 80 段中 43 段、SHA-512/256 で 80 段中 44 段、通常の衝突の場合 80 段中 27 段で構成できることを示した。新記録ではあるが段数のマージンはかなり残されている。

8.4. Asiacrypt 2015 の発表(4 日目)

On the Impact of Known-Key Attacks on Hash Functions [Asiacrypt 2015]

Bart Mennink, Bart Preneel

ASIACRYPT 2007 において、Knudsen と Rijmen はブロック暗号の既知鍵安全性を導入し、既存のブロック暗号構成に対する多くの識別攻撃につながった。本論文ではプリミティブベースのハッシュ関数に対するこの種の攻撃の影響を分析する。ブロック暗号がある弱点を持つがそれ以外は完全にランダムであるケースを捉える弱い暗号モデルを導入し定式化した。特定の実例を PGV 圧縮関数、Grostl、Shrimpton-Stam 圧縮関数に適用し、これらの設計は知られている差分既知鍵攻撃に対して重大な欠陥はないことを示した。

Property Preserving Symmetric Encryption Revisited [Asiacrypt 2015]

Sanjit Chatterjee, M. Prem Laxman Das

Eurocrypt 2012 において、Pandey と Rouselakis は、暗号文をテストすることにより平文の性質をチェックすることができる性質保存対称鍵暗号の概念を導入した。彼らの貢献は 2 つの安全性概念の分離および合成数位数の双線型群における安全な直交性テストの具体的な構成の 2 点である。本論文では、これらの観点から性質保存対称鍵暗号に関する包括的な解析を行った。直交性テストに関する暗号解析では、単純な識別攻撃により最も弱い安全性もなりたたないことを示した。

Refinements of the k-tree Algorithm for the Generalized Birthday Problem [Asiacrypt 2015]

Ivica Nikolić, Yu Sasaki

Wagner により一般化された誕生日問題の 2 つの未解決問題を研究した。K が 2 のべきでない場合に一般化誕生日問題を解く Wagner の k-木アルゴリズムをマルチ衝突を使って改良した。新しい 3-木アルゴリズムを CAESAR 提案の内 2 つに対し適用し、安全性を下げた。また、Hellman のテーブルを利用することにより、k-木の時間-空間トレードオフを改良し、新しい曲線 $T^2 M^{\lg k-1}=kN$ を得た。k=4 の場合には、$T^2 M=4N$ となる。

How to Sequentialize Independent Parallel Attacks? [Asiacrypt 2015]

Sonia M. Bogos, Serge Vaudenay

攻撃者が一つの CPU に対して複数の独立した攻撃を行うことができるシナリオを考える。各攻撃は独立して複数回行うことができ、与えられたステップ数の後、ある与えられた確率で成功するとした場合に、これらの攻撃を逐次的に行って最適にする戦略を研究した。最適の戦略が、ある攻撃を m ステップ実行し、次に別の攻撃を m ステップ実行し、ということを成功するまで続けるという戦略になるような、マジックナンバーm が存在することを示した。攻撃が鍵の全数探索のときの結果を LPN 問題とパスワード探索問題に適用した。

9. PKC 2016 の発表

9.1. PKC 2016 の発表(2 日目)

Algebraic Approaches for the Elliptic Curve Discrete Logarithm Problem over Prime Fields [PKC 2016]

Christophe Petit, Michiel Kosters, Ange Messeng

近年、拡大体上の ECDLP に対する指数計算法がいくつか提案されているが、実世界においてよく利用される素体上の ECDLP へは適用できないと考えられていた。本論文では、バイナリ曲線から素体上の曲線に攻撃を拡張する方法および実験による計算量評価が示された。現状は小さなパラメータの場合にしか有効とならず、漸近計算量評価もグレブナ基底のアルゴリズムを用いるために制限されるが、今後の進展に注意する必要がある。

Degenerate Curve Attacks: Extending Invalid Curve Attacks to Edwards Curves and Other Models [PKC 2016]

Samuel Neves, Mehdi Tibouchi

楕円曲線暗号に対する実装攻撃である不正曲線攻撃は、攻撃者が暗号デバイスが安全な曲線上ではない別の弱い曲線上でスカラー乗算を実行するように仕向ける攻撃である。従来、この攻撃は加算・倍算の実装に少なくとも曲線パラメータの一つと独立な公式を利用している実装に対して有効であり、Weierstrass 型の曲線には適用できたが、近年の Edwards 曲線には適用できなかった。本論文では、Edwards(捩れ)曲線、Jacobi 4 次曲線、Jacobi 交叉等に対する初めての攻撃を示す。不正曲線攻撃との違いは、暗号デバイスに対して、他の楕円曲線上の演算ではなく、基礎体の乗法群に同型な群の演算を行うように仕向けることである。

Easing Coppersmith Methods Using Analytic Combinatorics: Applications to Public-Key Cryhptography with Weak Pseudorandomness [PKC 2016]

Fabrice Benhamouda, Celine Chevalier, Adrian Thillard, Damien Vergnaud

Coppersmith の方法は、多項式方程式の小さな整数解を求める格子理論に基づいた方法である。近年、変数の数と方程式の数が定数でない場合の応用が見られるが、このような場合、計算量と成功確率を求めるために必要な組合せ解析は非常に複雑になっている。本論文では、解析的組合せ論に基づいたツールボックスを提供し、数論的疑似乱数生成器に適用することにより、正確な解析を得た。また、RSA 鍵生成と暗号化のパディング関数で使わ

れる乱数生成への適用を示した。

How to Generalize RSA Cryptanalyses [PKC 2016]
Atsushi Takayasu, Noboru Kunihiro
標準的な RSA 暗号に対する攻撃テクニックを、$N=p^rq$ の形の変形 RSA に対する攻撃に拡張した。標準 RSA に対する攻撃の格子は、変形 RSA に対する攻撃では、(r+1)倍大きな格子に変換される。以下の適用結果を得た。
－Takagi RSA に対する小秘密指数攻撃の単純な証明
－Takagi RSA に対する部分鍵漏洩攻撃
－素数べき RSA に対する小秘密指数攻撃
－素数べき RSA に対する部分鍵漏洩攻撃

10. FSE 2016 の発表

10.1. FSE 2016 の発表(1 日目)

Cryptanalysis of the Full Spritz Stream Cipher [FSE 2016]
Subhadeep Banik, Takanori Isobe
RC4 の後継として Rivest と Schuldt により CRYPTO2014 rump session で発表されたストリーム暗号 Spritz (フルラウンド) の暗号解析。Distinguishing attack では、244.8 ペアの(鍵, IV)から生成された最初の 2 バイトの key stream データを用いて、Spritz の出力とランダム系列と識別することができることを示した。また、1 ペアの(鍵, IV)から生成された最初の 260.8 バイトの key stream データを用いて Spritz の出力とランダム系列と識別することができることを示した。また、後半では”weak state”に当たった場合の state recovery attack について述べている。

10.2. FSE 2016 の発表(2 日目)

MILP-Based Automatic Search Algorithms for Differential and Linear Trails for Speck [FSE 2016]
Kai Fu, Meiqin Wang, Yinghua Guo, Siwei Sun, Lei Hu
近年、ブロック暗号の差分特性や線形特性を探索するために混合整数線形計画法(Mixed Integer Linear Programming, MILP)を用いた手法が有効であるが、加算, Rotation, XOR をベースとした ARX タイプのブロック暗号への適用は困難であった。本論文では、Lipmaa-Moriai によって示された加算の差分特性や線形特性をオープンな MILP optimizer である Gurobi に組込み、NSA 設計の Simon に適用した。その結果、従来より長い段数の差分特性、および線形特性が見つかり、セキュリティマージンが減った。

パラメータ	攻撃可能段数/仕様段数	時間	データ量	メモリ量	攻撃法
Simon 48/72	15/22	2^{70}	2^{46}	2^{22}	差分攻撃

Simon 48/96	16/23	2^{94}	2^{46}	2^{22}	差分攻撃
Simon 64/96	19/26	2^{95}	2^{63}	2^{22}	差分攻撃
Simon 64/128	20/27	2^{127}	2^{63}	2^{22}	差分攻撃
Simon 96/96	19/28	2^{88}	2^{88}	2^{22}	差分攻撃
Simon 96/144	20/29	2^{136}	2^{88}	2^{22}	差分攻撃
Simon 128/128	22/32	2^{120}	2^{120}	2^{22}	差分攻撃
Simon 128/192	23/33	2^{184}	2^{120}	2^{22}	差分攻撃
Simon 128/256	24/34	2^{248}	2^{120}	2^{22}	差分攻撃

10.3. FSE 2016 の発表(3 日目)

Key Recovery Attack against 2.5-round π-Cipher [FSE 2016]

Christina Boura, Avik Chakraborti, Gaëtan Leurent, Goutam Paul, Dhiman Saha, Hadi Soleimany, Valentin Suder

認証暗号のコンペティション CAESAR の第 2 ラウンド候補となっている π-Cipher のバリアントに対する guess & determine 攻撃が示された。特に、2.5 ラウンドのπ16-Cipher096 が 2^{72} の計算量で鍵が導出されることが示された（設計者らは 3 ラウンドで 96 ビットセキュリティをもつと主張していた)。

Cryptanalysis of Reduced NORX [FSE 2016]

Nasour Bagheri, Tao Huang, Keting Jia, Florian Mendel, Yu Sasaki

認証暗号のコンペティション CAESAR の第 2 ラウンド候補となっている NORX のバリアントに対する鍵導出攻撃が示された。NORX は sponge 構造をもつ nonce ベースの認証暗号で、128 ビットセキュリティをもつ NORX32 と 256 ビットセキュリティをもつ NORX64 がある。ともに core permutation が 4 段の仕様のところを 2 段に削減したバリアントに対して、guess & determine 攻撃により NORX32 は時間計算量 2^{119}、データ量 2^{66} で、NORX64 は時間計算量 2^{234}、データ量 2^{132} で攻撃できることが示された。

Analysis of the Kupyna-256 Hash Function [FSE 2016]

Christoph Dobraunig, Maria Eichlseder, Florian Mendel

ウクライナ標準 DSTU 7564:2014 として公開されたハッシュ関数 Kupyna に対する解析が示された。Kupyna は SHA-3 最終候補であった Grostl に似た構造をしているが、ラウンド定数が XOR でなく、加算で加えられている点等が異なっており、rebound 攻撃等に対する耐性を高める効果があると考えられている。しかしながら、この論文では、このような対処を行っても rebound 攻撃を適用できることが示された。具体的には、10 段中 6 段に短縮した Kupyna-256 が 2^{70} の計算量で、7 段に短縮した Kupyna-256 が $2^{125.8}$ の計算量で圧縮関数の衝突を見つけられることが示された。さらに 10 段中 4 段に短縮した Kupyna-256 が 2^{67} の計算量で、5 段に短縮した Kupyna-256 が 2^{120} の計算量で、ハッシュ関数の衝突を見つけられることが示された。

発行日　2016年 6月 17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