CRYPTREC Report 2012

平成 25 年 3 月

独立行政法人情報通信研究機構
独立行政法人情報処理推進機構

「暗号方式委員会報告」

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方式委員会の 2012 年度活動報告である。

2012 年度活動において、特筆すべきは、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として、CRYPTREC 暗号リストが公表されたことである。CRYPTREC 暗号リストは、暗号技術に対する解析・攻撃技術の高度化や、新たな暗号技術の研究開発が進展している状況を踏まえ、安全性だけではなく、調達容易性、国産暗号の普及促進といった様々な視点で検討されたリストであり、「電子政府推奨暗号リスト」、「推奨候補暗号リスト」、「運用監視暗号リスト」から構成される。本リストは、2003 年に公表された「電子政府推奨暗号リスト」を改定したものである。

2003 年のリストは、策定時点において、10 年間は安心して利用できるという観点で選定された暗号が掲載されているが、暗号をとりまく状況の変化に対応するため、5 年後には見直しを行い、10 年後には改定を行うことが想定されていた。このため、2008 年度から準備を始め、2009 年度に、「電子政府推奨暗号リスト改訂のための暗号技術公募」を実施し、「暗号方式委員会」、「暗号実装委員会」、「暗号運用委員会」の 3 委員会体制により、2012 年度のリスト改定に向けて検討を行ってきた。

暗号方式委員会は、独立行政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おり、暗号技術の安全性及び信頼性確保の観点から、電子政府推奨暗号の監視を行い、リスト改定に向けた安全性評価を行った。2012 年度の活動としては、リスト改定に向けて、推奨候補暗号リストを選定するための安全性評価、総合評価、及び注釈の整理を担当し、さらに、電子政府推奨暗号の監視と、暗号技術調査ワーキンググループにおける以下の二つの検討を行った。リストガイドワーキンググループで行った、一般的な暗号プロトコルにおける暗号技術の利用方法についての調査と、計算機能力評価ワーキンググループで行った、離散対数問題の困難性の見積もりの検討及び素因数分解問題や離散対数問題以外の暗号技術で利用される数学的な問題に関する検討である。

改定された CRYPTREC 暗号リストの監視は、暗号が使われ続ける限り、電子政府の安全性確保のためにも、またネットワークセキュリティ全般の維持のためにも、継続していかねばならない活動である。来年度 CRYPTREC は、新たな委員会体制で活動を継続するが、暗号方式委員会後継の暗号技術評価委員会は、この監視活動を担っていくことになる。また、暗号運用委員会後継の暗号技術活用委員会との連携を保ちつつ、暗号技術の適切な利用の普及にも貢献していくことが求められる。このような CRYPTREC の活動は、これまでも、これからも、暗号技術やその実装及び運用に係る研究者及び技術者等の多くの関係者の協力を得て成り立つものであることを改めて強調しておきたい。

末筆ではあるが、本活動に様々な形でご協力下さった関係者の皆様に深甚な謝意を表する次第である。

暗号方式委員会　委員長　今井 秀樹

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章は暗号方式委員会及び監視活動等について説明してある。第2章は電子政府推奨暗号リスト改訂に係る暗号技術評価に関する報告である。第3章は今年度の監視活動、調査等の活動概要の報告である。第4章は暗号方式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「暗号方式委員会」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、電子政府推奨暗号の仕様書は、CRYPTREC事務局（総務省、経済産業省、独立行政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。

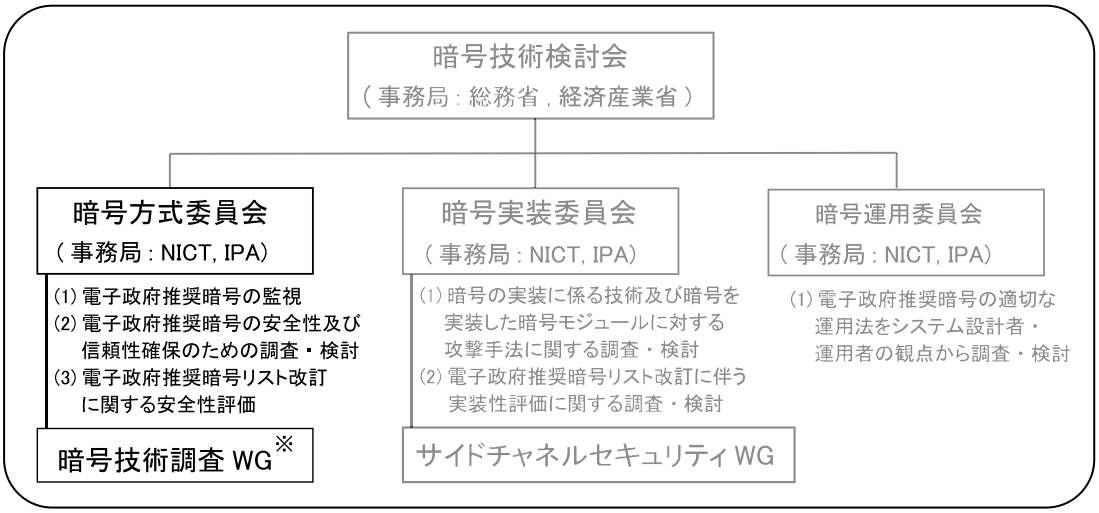
【問合せ先】　info@cryptrec.go.jp

委員会構成

暗号方式委員会(以下「方式委員会」)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、独立行政法人情報通信研究機構(NICT)と独立行政法人情報処理推進機構(IPA)が共同で運営する。方式委員会は、暗号技術の安全性及び信頼性確保の観点から、電子政府推奨暗号の監視、電子政府推奨暗号に関する暗号アルゴリズムを主な対象とする調査・検討を適宜行う等、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、将来的には、電子政府推奨暗号リストの改定に関する調査・検討を行う予定であり、暗号技術関連学会や国際会議等を通じての暗号技術に関する情報収集、関係団体の Web サイトの監視等を行う。

暗号技術調査ワーキンググループ(以下「調査 WG」)は、方式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、方式委員会活動に関連して必要な項目について、方式委員会の指示のもとに調査・検討活動を担当する作業グループである。方式委員会の委員長は、実施する調査・検討項目に適する主査及びメンバーを、方式委員会及び調査 WG の委員の中から選出し、調査・検討活動を指示する。主査は、その調査・検討結果を方式委員会に報告する。平成 21 年度、方式委員会の指示に基づき実施されている調査項目は、「電子政府推奨暗号リストに関するガイドの作成」である。

方式委員会と連携して活動する「暗号実装委員会」及び「暗号運用委員会」も、方式委員会と同様、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:

・電子政府推奨暗号リストに関するガイドの作成

・素因数分解問題及び離散対数問題等の困難性に関する調査・研究

図 1:CRYPTREC 体制図

委員名簿

暗号方式委員会

委員長	今井 秀樹	中央大学 教授
顧問	辻井 重男	中央大学研究開発機構　教授
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	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	盛合 志帆	独立行政法人情報通信研究機構 研究室長
委員	松本 勉	国立大学法人横浜国立大学 大学院 教授
委員	山村 明弘	国立大学法人秋田大学 大学院 教授
委員	渡辺 創	独立行政法人産業技術総合研究所 研究グループ長

暗号技術調査ワーキンググループ(リストガイド)

主査	手塚 悟	東京工科大学　教授
委員	岡崎 博之	日本電気株式会社　事業部長代理
委員	菅野 哲	ＮＴＴソフトウェア　主任エンジニア補
委員	清本 晋作	株式会社ＫＤＤＩ研究所　主任研究員
委員	佐野 文彦	東芝ソリューション株式会社　研究主務
委員	花岡 悟一郎	独立行政法人産業技術総合研究所　研究チーム長
委員	藤城 孝宏	株式会社日立製作所　部長
委員	松尾 真一郎	独立行政法人情報通信研究機構　研究室長
委員	民田 雅人	株式会社日本レジストリサービス　主任研究員
委員	渡辺 大	株式会社日立製作所　主任研究員

暗号技術調査ワーキンググループ(計算機能力評価)

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	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 主任研究員

オブザーバー

福永 利徳	内閣官房情報セキュリティセンター
中山 慎一	内閣官房情報セキュリティセンター
今福 健太郎	内閣官房情報セキュリティセンター

杉浦 幹人	内閣官房情報セキュリティセンター
根木 まろか	警察庁 情報通信局
大平 利幸	総務省 行政管理局
林 俊子	総務省 自治行政局 住民制度課[2012 年 7 月まで]
野村 知宏	総務省 自治行政局 住民制度課[2012 年 7 月から]
浦船 利幸	総務省 自治行政局 地域情報政策室[2012 年 6 月まで]
須藤 正喜	総務省 自治行政局 地域情報政策室[2012 年 6 月から]
飯田 恭弘	総務省 情報流通行政局
鮫島 清豪	総務省 情報流通行政局[2012 年 8 月まで]
樋口 有二	総務省 情報流通行政局[2012 年 8 月まで]
上原 哲太郎	総務省 情報流通行政局[2012 年 8 月から]
吉田 丈夫	総務省 情報流通行政局[2012 年 8 月から]
橋本 直樹	総務省 情報流通行政局[2012 年 10 月から]
佐久間 明彦	外務省 大臣官房
山中 豊	経済産業省 産業技術環境局[2012 年 7 月まで]
岩永 敏明	経済産業省 産業技術環境局[2012 年 7 月から]
森川 淳	経済産業省 商務情報政策局[2012 年 10 月まで]
中谷 順一	経済産業省 商務情報政策局[2012 年 10 月から]
守山 速飛	経済産業省 商務情報政策局
坂下 圭一	防衛省 運用企画局[2012 年 5 月まで]
古市 洋希	防衛省 陸上自衛隊 通信団[2012 年 5 月より]
岡野 孝子	警察大学校
滝澤 修	独立行政法人情報通信研究機構
花岡 悟一郎	独立行政法人産業技術総合研究所

事務局

独立行政法人 情報通信研究機構 （高橋幸雄[9 月まで]、平和昌[10 月から]、沼田文彦、松尾真一郎、盛合志帆、野島良、大久保美也子[9 月まで]、蓑輪正[1 月まで]、江村恵太[8 月から]、黒川貴司、金森祥子、多賀文吾、側髙幸治、八代祐子、笠井祥、大川晋司、赤井健一郎[11 月まで]、村野正泰[12 月から]、持永大）

独立行政法人 情報処理推進機構（笹岡賢二郎、近澤武、小暮淳、大熊建司、神田雅透、鈴木幸子）

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、暗号技術は情報セキュリティシステム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。

高度情報通信ネットワーク社会形成基本法（IT 基本法）が策定された 2000 年以降、行政の情報化及び公共分野における情報通信技術の活用に関する様々な取り組みが実施されてくるにつれて、情報セキュリティ問題への取組みを抜本的に強化する必要性がますます認識されるようになってきた。

2006 年 2 月、内閣官房情報セキュリティセンター(NISC)の情報セキュリティ政策会議(議長：内閣官房長官)において、我が国の情報セキュリティ問題全般に関する中長期計画(2006～2008 年度の 3 ケ年計画)として「第 1 次情報セキュリティ基本計画」（第 1 次基本計画）が決定され、同計画において、暗号技術に関して今後取り組むべき重点政策として、「電子政府の安全性及び信頼性を確保するため、電子政府で使われている推奨暗号について、その安全性を継続的に監視・調査するとともに、技術動向及び国際的な取組みを踏まえ、暗号の適切な利用方策について検討を進める」こととされた。

CRYPTREC では、2005 年度にハッシュ関数の安全性評価を実施し、2006 年 6 月に SHA-1 の安全性に関する見解を公表した。これに基づき、上述の第 1 次基本計画の年度計画である「セキュア・ジャパン 2007」では、「電子政府推奨暗号について、その危殆化が発生した際の取扱い手順及び実施体制の検討を進める」こととされ、NISC をはじめとする政府機関において、暗号の危殆化に備えた対応体制等を整備することが喫緊の課題であることが認識された。そして、2006 年度には素因数分解問題の困難性に関する評価を実施し、RSA1024 の安全性の評価を公表した。これらの SHA-1 及び RSA1024 に関する安全性に関する CRYPTREC からの見解に基づき、NISC の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」[1]が 2008 年度に決定されるに至った。

2010年度から2013年度の4年間を対象とした施策である「国民を守る情報セキュリティ戦

[1] 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）

略」[2]の年度計画である「情報セキュリティ2011」[3]においても、「政府機関における安全な暗号利用の推進」として、

a. 総務省及び経済産業省は、電子政府推奨暗号の監視、電子政府推奨暗号の安全性及び信頼性の確保のための調査、研究、基準の作成等を2011 年度も引き続き行う。
b. 総務省及び経済産業省は、「電子政府推奨暗号リスト」の改訂に向けた取組を着実に実施する。
c. 総務省及び経済産業省は、必要に応じて、電子政府推奨暗号の監視により得られた情報を内閣官房に提供し、内閣官房は、必要な情報を速やかに各府省庁に提供するなど、「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」に従った取組を推進する。
d. 内閣官房及び各府省庁は、暗号技術検討会における議論等を参考に、急激な安全性の低下に備え、緊急避難的な対応（コンティンジェンシープラン）に係る発動要件について検討を行い、CISO 等連絡会議において当該要件の決定を行う。
e. 各府省庁は、2011 年度も引き続き、同移行指針に基づき、それぞれで保有する情報システムについてより安全な暗号アルゴリズムへの移行を着実に実施する。
a. 内閣官房は、各府省庁における同移行指針への対応状況を把握して、新たな暗号アルゴリズムへの切替え開始時期までに、各情報システムが同移行指針の規定する要件に適合させるよう促す。

の通り、暗号技術の安全性に関する重要な施策が取りまとめられている。

このように、電子政府推奨暗号の安全性及び信頼性確保のための活動等の機能は非常に重要であり、暗号技術の危殆化を予見し、電子政府システムで利用される暗号技術の安全性を確保するためには、最新の暗号理論の研究動向を専門家が十分に情報収集・分析することが必要であることはもちろんのこと、今後も、CRYPTREC が発信する情報を踏まえ、各政府機関が連係して情報通信システムをより安全なものに移行するための取り組みを実施していくことが必要不可欠である。

1.2 暗号方式委員会

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（CRYPTREC: Cryptography Research and Evaluation Committees）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（付録５）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。

[2] http://www.nisc.go.jp/active/kihon/pdf/senryaku.pdf （2010 年５月 11 日情報セキュリティ政策会議決定）
[3] http://www.nisc.go.jp/active/kihon/pdf/js2011.pdf （2011 年７月８ 日情報セキュリティ政策会議決定）

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。暗号技術監視委員会の責務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である。さらに、暗号技術監視委員会は電子政府推奨暗号の監視活動のほかにも、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を委ねられている。

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た。その概要については、第 2 章を参照のこと。

また、引き続き、暗号技術調査ワーキンググループ（リストガイド）において、暗号技術に詳しくない情報システム調達担当者及び運用担当者を対象とした、電子政府推奨暗号リストの適切な利用のため技術的解説書の作成を継続して行っている。詳細については、第 4 章を参照こと。

1.3 電子政府推奨暗号リストとその改定

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」（付録５）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[4]を行い、「電子政府における調達のために参照すべき暗号のリスト（ＣＲＹＰＴＲＥＣ暗号リスト）」(付録１)が決定された。

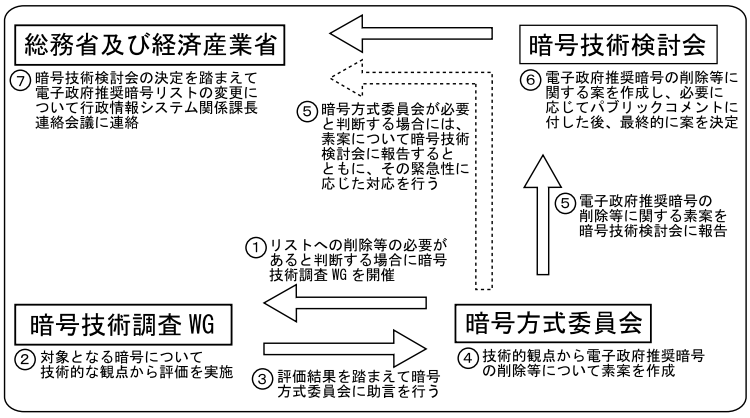
1.4 活動の方針

電子政府推奨暗号リスト[5]掲載の暗号に関する研究動向を把握して、暗号技術の安全性について監視を行い、必要に応じて電子政府システムにおける暗号技術の情報収集と電子政府推奨暗号リストの改訂について暗号技術検討会(総務省・経済産業省)に対して助言を行う。また、暗号理論全体の技術動向を把握して、最新技術との比較を行い、電子政府システムにおける暗号技術の陳腐化を避けるため、将来の電子政府推奨暗号リストの改正を考慮して、電子政府推奨暗号に関する調査・検討を行う。監視活動は、情報収集、情報分析、審議及び決定の３つのフェーズからなる。

暗号技術検討会における電子政府推奨暗号の監視に関する基本的考え方は以下の通りである。

(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。

電子政府推奨暗号の削除等の手順



[4] http://www.cryptrec.go.jp/topics/cryptrec_201212_listpc.html
[5] 2003 年 2 月 20 日に策定されたものを指す。

第２章 電子政府推奨暗号リストの改定[1]について

2.1. 改定の背景

CRYPTREC は、客観的な評価により安全性及び実装性に優れると判断される暗号技術をリストアップすることを目的に、2000 年度に暗号技術の公募・評価活動を開始し、2002 年度末に電子政府推奨暗号リスト（以下、「リスト(2002 年度版)」）を発表した。

その後、各府省に対してその利用を推奨することにより、電子政府の高度な安全性と信頼性を確保することを目指して、2003 年度から監視活動及び安全性評価を継続して行ってきた。これにより、リスト(2002 年度版)の信頼性は高められ、また、それらの活動に基づいた暗号の危殆化への対応・提言は電子政府において広く認知されてきた。

リスト(2002 年度版)には、策定時点において、今後 10 年間は安心して利用できるという観点で選定された暗号が掲載されている。しかし、策定から 5 年余りが経過し、暗号技術に対する解析・攻撃技術の高度化や、新たな暗号技術の開発が進展している状況にある。

また、今日では CRYPTREC への要望が、暗号技術に対する安全性評価とその周知のみならず、安心・安全な情報通信システムを構築する上で、暗号技術の危殆化及び移行対策等を含めた、適切な暗号技術の選択を支援するものへと変化しつつある。

さらに、暗号技術の評価の面において、政府調達等における入手し易さや導入コスト、相互運用性と普及度合いの観点も取り入れる必要性が指摘されているところである。

これらの状況を踏まえ、2012 年度、リスト(2002 年度版)を改定することが必要である。

2.2　リスト(2002 年度)の改定の目的

今回の改定においては、第一に、電子政府において暗号技術を利用する際に安全な暗号技術を選択するための指針を与えること、第二に、暗号を利用した技術をシステムのセキュリティ要件に合わせて正しく組み込むための指針を与えることを目的とする。次期リストは、内閣官房情報セキュリティセンター（NISC）の調整により、情報セキュリティ政策会議で決定された「政府機関の情報セキュリティ対策のための統一基準」等から参照されることを想定している。

このため、今回の改定にあたっては、新たに暗号技術の公募を行うとともに、リスト(2002 年度版)に掲載されている暗号技術の見直しを行い、リスト(2002 年度版)の全体の構成を改めることとする。

---

[1] 2011 年度までの暗号方式委員会報告書では、「改訂」を用いていたが、2012 年度から「改定」に改めた。

2.3　電子政府推奨暗号リスト改定のための暗号技術の公募（2009 年度）

2.3.1.　公募の概要

CRYPTREC は評価対象暗号技術を公募し、暗号技術評価を実施する。特に、安全性及び実装性で、リスト(2002 年度版)に記載されている暗号アルゴリズムよりも優位な点を持ち、国際学会で注目されている新技術が提案されている暗号技術カテゴリであること、及び、リスト(2002 年度)に掲載されている暗号技術と同カテゴリに属する暗号技術については、それらの暗号技術よりも、安全性もしくは実装性において優れた暗号技術であることを指針としている。

暗号技術評価の実施にあたっては、暗号技術評価に実績のある国内及び国外の専門家に委託した評価や学会及び論文誌等で発表された評価を踏まえ、各暗号技術の安全性及び実装性等の特徴を整理する。その結果は、事務局が開催するシンポジウムや報告書等を通じて、一般に公表することを予定している。

2009 年度から 2010 年度にかけては、主に応募された暗号技術の評価を実施する。また、2011 年度には、応募された暗号技術の評価を継続するほか、リスト(2002 年度)に掲載されている暗号技術の再評価も行う。

暗号方式委員会、暗号実装委員会及び暗号運用委員会が、評価結果に基づき、次期リストへの暗号技術の記載について判定し、暗号技術検討会に報告する。報告された暗号技術の次期リストへの記載については、暗号技術検討会での検討を経た後、最終的に総務省及び経済産業省において決定される。

2.3.2.　公募の対象

2009 年度公募対象の暗号技術の種別は、以下のとおり（表 2.1）である。ただし、主な留意事項としては、

- 応募される暗号技術は、2010 年 9 月末までに、査読付きの国際会議、または、査読付きの国際論文誌で発表されているか、あるいは、採録が決定されているもの。
- 評価する際に知的財産の利用が無償で行えるもの。
- 公募する暗号技術、またはそれを実装した製品が、電子政府等の利用に際し、次期リスト策定後 3 年以内までに調達可能なもの。

等を挙げていた。

表 2.1 2009 年度公募対象の暗号技術の種別

暗号技術の種別	仕様の概要
ブロック暗号	平文及び暗号文ブロックサイズが 128 ビットであり、鍵長が 128 ビット、192 ビットまたは 256 ビットであるブロック暗号で、リスト(2002 年度)に掲載されている暗号技術と同等以上の特長（安全性または実装性）を持つもの。
暗号利用モード	秘匿に関する 128 ビットブロック暗号及び 64 ビットブロック暗号を対象にした利用モード。
メッセージ認証コード	鍵長が 128 ビットである 128 ビットブロック暗号及び 64 ビットブロック暗号を利用したメッセージ認証コード。
ストリーム暗号	鍵長が 128 ビット以上であり、平文をビット単位もしくはバイト単位で暗号化するストリーム暗号。
エンティティ認証	リスト(2002 年度)に掲載された共通鍵暗号、公開鍵暗号、ハッシュ関数、メッセージ認証コードの組み合わせによって実現されるエンティティ認証、あるいは、安全性を計算量的な困難さに帰着できるエンティティ認証を公募します。エンティティ認証を構成する要素技術は、リスト(2002 年度)に掲載されている暗号技術を用いることを原則とします。要素技術として、リスト(2002 年度)に掲載されていない共通鍵暗号、メッセージ認証コードを用いる場合は、これらの要素技術を同時に応募する必要があります。また、上記以外の要素技術を用いたエンティティ認証技術の応募も可能。

2.3.3. 公募期間

2009 年 10 月 1 日～2010 年 2 月 4 日 17 時

2.3.4. 応募暗号技術

2009 年度において、下記のとおり（表 2.2)、6 件の暗号技術について応募があった。

表 3.2 2009 年度応募暗号技術一覧

暗号種別	暗号技術名	応募者
128 ビットブロック暗号	CLEFIA	ソニー株式会社
	HyRAL	株式会社ローレルインテリジェントシステムズ
ストリーム暗号	Enocoro-128v2	株式会社日立製作所
	KCipher-2	KDDI 株式会社
メッセージ認証コード	PC-MAC-AES	日本電気株式会社
エンティティ認証	無限ワンタイムパスワード認証方式（Infinite One-Time Password)	日本ユニシス株式会社

※暗号利用モードについては応募なし。

2.3.5.　事務局選出暗号技術

CRYPTREC におけるリストガイド策定時の検討結果などを参考に、国際標準化等の実績がある以下の暗号技術について、CRYPTREC 事務局より選出した。

表 2.3　2009 年度事務局選出暗号技術一覧

暗号種別	暗号技術名	評価仕様
メッセージ認証コード	CBC-MAC	ISO/IEC 9797-1
	CMAC	NIST SP 800-38B
	HMAC	NIST FIPS 198-1
暗号利用モード	CBC モード	NIST SP 800-38A
	CFB モード	NIST SP 800-38A
	OFB モード	NIST SP 800-38A
	CTR モード	NIST SP 800-38A
	GCM モード	NIST SP 800-38C
	CCM モード	NIST SP 800-38C
エンティティ認証	共通鍵暗号利用による認証プロトコル	ISO/IEC 9798-2、対称暗号化アルゴリズムを使用する機構
	電子署名利用による認証プロトコル	ISO/IEC 9798-3、デジタル署名技術を使用する機構
	検査関数（MAC）による認証プロトコル	ISO/IEC 9798-4、暗号検査機能を使用する機構

※128 ビットブロック暗号及びストリーム暗号については選出なし。

2.4.　応募暗号の評価スケジュール

2009 年度から 2012 年度までの電子政府推奨暗号リストの改定に向けた応募暗号の評価スケジュールをまとめると以下のとおり。

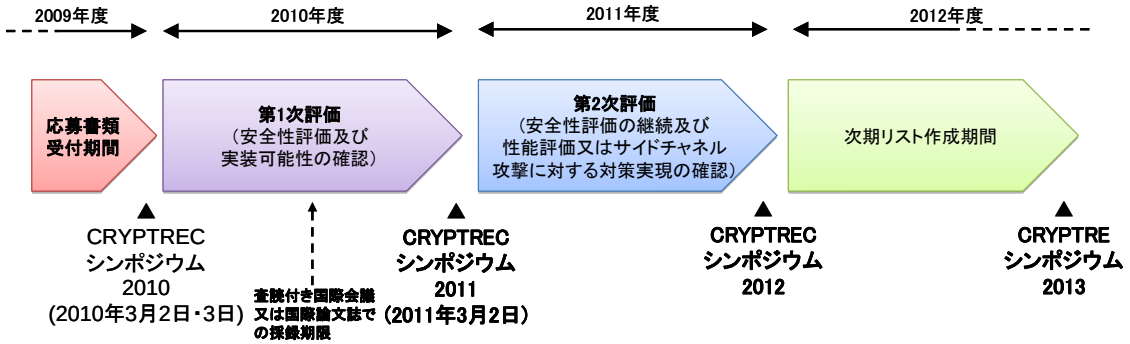


図 3.4 評価スケジュール

CRYPTREC シンポジウム 2010 開催： 2010 年 3 月 2 日・3 日
第 1 次評価実施： 2010 年 4 月～2011 年 3 月
CRYPTREC ジンポジウム 2011 開催： 2011 年 3 月 2 日
第 2 次評価実施： 2011 年 4 月～
CRYPTREC シンポジウム 2012： 2012 年 3 月 9 日
CRYPTREC シンポジウム 2013： 2013 年 3 月 26 日

2.5. 応募暗号の評価項目

安全性評価項目と実装性評価項目の 2 つに大別される。

(1) 安全性評価項目

既知の一般的な攻撃法に対する耐性を評価する。また、その暗号に特化した攻撃法や、ヒューリスティックな安全性の根拠も評価の対象とすることがある。

(2) 実装性評価項目

提出資料に基づいて、実現可能性の確認を行う。性能の評価に関して、ソフトウェア実装では、標準的なプラットフォーム上での性能（処理速度、メモリ使用量等）を評価する。また、ハードウェア実装（エンティティ認証を除く）では、使用するプロセス（FPGA[2]、ASIC[3]等）別に性能（処理速度、使用セル数またはゲート数等）を評価する。また、一部の暗号技術に対しては、サイドチャネル攻撃に対する対策実現の確認も行う。

なお、2009 年度公表した公募要項では、実装性評価の実施に際して、明確でない部分があったため、暗号実装委員会において詳細を検討し、その結果を応募者にアナウンスした。

詳細については、「暗号実装委員会報告」を参照のこと。

[2] FPGA：Field Programmable Gate Array
[3] ASIC：Application Specific Integrated Circuit

2.6. 第 1 次評価の進捗状況

2010 年度における応募暗号技術及び事務局選定暗号技術に関する第 1 次評価の進捗状況は以下のとおりである。

2.6.1. 応募暗号技術の評価状況

表 3.5 応募暗号技術の第 1 次評価結果(2010 年度実施)

暗号種別	暗号技術名	提案者	評価継続の要否
128 ビットブロック暗号	CLEFIA	ソニー株式会社	引き続き第 2 次評価を行う。
	HyRAL	株式会社ローレルインテリジェントシステムズ	128 ビット鍵長から 255 ビット鍵長においては、現在のところ問題点は見つかっていないが、256 ビット鍵長の場合、極小的な数であるが等価鍵の発見及び現実的な計算量での導出法が示された。よって、リスト(2002 年度)に掲載されている暗号技術と同等以上の安全性を持たないと判断し、第 1 次評価までで評価終了とし、次期リストには掲載しない。
ストリーム暗号	Enocoro-128v2	株式会社日立製作所	引き続き第 2 次評価を行う。
	KCipher-2	KDDI 株式会社	引き続き第 2 次評価を行う。
メッセージ認証コード	PC-MAC-AES	日本電気株式会社	引き続き第 2 次評価を行う。

※ 暗号利用モードについては応募なし。

※ エンティティ認証に応募された無限ワンタイムパスワード認証方式については、2010 年 9 月末までに、査読付きの国際会議または査読付きの国際論文誌で発表されなかったことにより、応募資格を喪失した。

2.6.2. 事務局選出暗号技術の評価状況

表 3.6 応募暗号技術の第 1 次評価結果(2010 年度実施)

暗号種別	暗号技術名	評価仕様	評価継続の要否
メッセージ認証コード	CBC-MAC	ISO/IEC 9797-1	今後、注意すべき利用方法や利用方法に関する注釈等について検討した上で、次期リストに掲載する。
	CMAC	NIST SP 800-38B	
	HMAC	NIST FIPS 198-1	
暗号利用モード	CBC モード	NIST SP 800-38A	
	CFB モード	NIST SP 800-38A	
	OFB モード	NIST SP 800-38A	
	CTR モード	NIST SP 800-38A	
	GCM モード	NIST SP 800-38C	
	CCM モード	NIST SP 800-38C	

エンティティ証	共通鍵暗号利用による認証プロトコル	ISO/IEC 9798-2、対称暗号化アルゴリズムを使用する機構	一部のタイプに脆弱性を発見したので、それらについては利用しないよう注釈を付けた上で、次期リストに掲載する。ただし、脆弱性の発見されたタイプに関しては、修正方法が存在するので、ISO/IECに対して修正を求め、修正が完了し次第、注釈に関して再検討を行う。
	電子署名利用による認証プロトコル	ISO/IEC 9798-3、デジタル署名技術を使用する機構	
	検査関数（MAC）による認証プロトコル	ISO/IEC 9798-4、暗号検査機能を使用する機構	

※128ビットブロック暗号及びストリーム暗号については選出なし。

2.7. 2011 年度における安全性評価について

2011 年度における応募暗号技術に関する第 2 次評価及び現在、リストリスト(2002 年度)に掲載された暗号技術の安全性に関する再評価の状況は以下のとおりである。

2.7.1. 128 ビットブロック暗号の鍵拡大関数の安全性

関連鍵攻撃[4]に対する安全性評価を目的として鍵拡大関数の差分特性確率[5]の上界を評価した。差分特性確率は、秘密鍵を操作したときに拡大鍵を制御できる確率の上界を示しており、関連鍵攻撃についての安全性の指標になると考えられる。本評価において排他的論理和、定数加乗算に関しては全て攻撃者に都合の良い差分伝播が確率 1 で生じるとし、攻撃者有利に評価をしている。

表 3.7 鍵拡大関数の差分特性確率の上界

鍵長 / アルゴリズム	差分特性確率の上界		
	128 ビット	192 ビット	256 ビット
AES	2^{-24}	2^{-6}	2^{-6}
Camellia	2^{-30}	2^{-18}	2^{-18}
CIPHERUNICORN-A	2^{-259}	2^{-175}	2^{-133}
Hierocrypt-3	2^{-36}	2^{-36}	2^{-36}
SC2000	2^{-48}	2^{-24}	2^{-24}

この結果から、AES と比較した場合、Camellia、CIPHERUNICORN-A、Hierocrypt-3 及び SC2000 は関連鍵攻撃に対して、より耐性があると見積もられる。関連鍵攻撃は、192/256

[4] 関連鍵攻撃とは、攻撃者が秘密鍵を操作できるという仮定の下での攻撃である。
[5] 鍵拡大関数にはデータ撹拌部における拡大鍵挿入に相当するものがないため、単に active s-box について最大差分確率の積を取ることにより上界を算出している。

ビット鍵の AES に対して解読可能であることが示されているが、特殊な攻撃条件のため現実的な脅威には至っていないと考えられる。関連鍵攻撃に対して安全であることの必要性については今後検討が必要である。

等価鍵存在[6]に関しては、AES、Camellia、CIPHERUNICORN-A 及び Hierocrypt-3 については鍵拡大関数が全単射であることから等価鍵が存在しない。SC2000 については、拡大鍵計算の途中で生成される中間鍵には衝突がないことが確認されているが、拡大鍵については未確認であった。

2.7.2. 128 ビットブロック暗号の 192/256 ビット鍵の場合の安全性

192/256 ビット鍵の場合の計算量的安全性を関連鍵攻撃まで想定して概算で見積もるため、差分/線形特性確率の上界を評価した。本評価においてはデータ撹拌部のみを考え、データ撹拌部全ラウンドの丸め差分／線形パスを探索することによりその特性確率の上界を評価している。ただし、排他的論理和やビットシフトなどの線形演算に関しては確率 1 で、算術加乗算や s-box などの非線形演算に関しては最大差分確率で、それぞれ攻撃者に都合の良い差分伝播が生じるとし、攻撃者有利の評価を行った。

(a) 差分攻撃

表 3.8 データ撹拌部の差分特性確率の上界

アルゴリズム＼鍵長	差分特性確率の上界		
	128 ビット	192 ビット	256 ビット
AES	2^{-336}	2^{-456}	2^{-486}
Camellia	2^{-216}	2^{-288}	192 ビット鍵と同じ
CIPHERUNICORN-A	2^{-190}[1][7]	128 ビット鍵と同じ	128 ビット鍵と同じ
Hierocrypt-3	2^{-450}	2^{-480}	2^{-600}
SC2000	(2^{-187}[2] [8])	(2^{-215}[2])	192 ビット鍵と同じ

[6] 等価鍵とは、任意の平文の暗号化において同じ暗号文を出力する秘密鍵の組をいう。

[7] [1] 角尾幸保、久保博靖、茂真紀、洲崎智保、宮内宏, “CIPHERUNICORN-Aの差分解読／線形解読に対する安全性について (II) ”、SCIS 2003, 5D-1, 2003.

[8] [2] H.Yanami, T.Shimoyama, and O.Dunkelman, Differential and Linear Cryptanalysis of a Reduced-Round SC2000, FSE 2002, LNCS 2365: 34-48

表 3.9　攻撃計算量が鍵全数探索を上回るラウンド数／暗号化ラウンド数

アルゴリズム＼鍵長	攻撃計算量が鍵全数探索を上回るラウンド数／暗号化ラウンド数		
	128 ビット	192 ビット	256 ビット
AES	4/10	7/12	8/14
Camellia	12/18	17/24	22/24
CIPHERUNICORN-A	12/16[1]	-	-
Hierocrypt-3	2/6	4/7	4/8
SC2000	(13/19[2])	(21/22[2])	-

※ -は 1 を超えた場合である。

ア） AES、Camellia 及び Hierocrypt-3

全てのアルゴリズムについて修正を行うことなしに評価を行った。Camellia のデータ撹拌部は 192 及び 256 ビット鍵において同じ構造であるため差分特性確率は等しい値となる。

イ） CIPHERUNICORN-A

データ撹拌部はすべての鍵長において同じ構造であるため、差分特性確率は鍵長に依らず一定である。ラウンド関数の構造が複雑であり拡大鍵入力の独立性を考慮した差分特性確率の見積もりが難しいことから、参考文献[1]の結果を事務局の評価とした。この結果から示される差分特性確率の上界は、全鍵長において、2^{-190} である。

ウ） SC2000

丸め差分評価では 2^{128} 以上の計算量的安全性を確認できなかったため、参考文献[2]の結果を全ラウンドに適用した。表中の()内の値は、[2]の繰り返しパスを全ラウンドにそのまま適用した値である。128 ビット鍵では 2^{-187}、192/256 ビット鍵では 2^{-215} の差分パスが存在する。

(b) 線形攻撃

表 3.10　データ撹拌部の線形特性確率の上界

アルゴリズム＼鍵長	線形特性確率の上界		
	128 ビット	192 ビット	256 ビット
AES	2^{-330}	2^{-450}	2^{-480}
Camellia	2^{-228}	2^{-324}	192 ビット鍵と同じ
CIPHERUNICORN-A	2^{-171}	128 ビット鍵と同じ	128 ビット鍵と同じ
Hierocrypt-3	2^{-450}	2^{-480}	2^{-600}
SC2000	(2^{-176}[2])	(2^{-204}[2])	192 ビット鍵と同じ

表 3.11　攻撃計算量が鍵全数探索を上回るラウンド数／暗号化ラウンド数

アルゴリズム＼鍵長	攻撃計算量が鍵全数探索を上回るラウンド数／暗号化ラウンド数		
	128 ビット	192 ビット	256 ビット
AES	4/10*	7/12	8/14
Camellia	11/18	15/24	21/24
CIPHERUNICORN-A	12/16	-	-
Hierocrypt-3	2/6	4/7	4/8
SC2000	(15/19[2])	(21/22[2])	-

※ -は 1 を超えた場合である。

ア） AES、Camellia 及び Hierocrypt-3

Camellia の評価は、FL 関数無しで行った。AES、Hierocrypt-3 に対しては、アルゴリズムを修正することなしに評価を行った。

イ） CIPHERUNICORN-A

データ撹拌部はすべての鍵長において同じ構造であるため、線形特性確率は鍵長に依らず一定である。ラウンド関数の構造が複雑であり、簡易な構造に変形した mF 関数を用いて評価した。参考文献[1][3]と異なり、定数乗算及び、A3 関数に関し、bit 単位の接続可能性に極力配慮した再評価を行った。しかし、拡大鍵入力の独立性を考慮した評価結果は[1][3][9]と、同じである。この結果から示される線形特性確率の上界は、全鍵長において、2^{-171} である。

ウ） SC2000

S-box として、4,5,6 ビット幅の物 3 種類が混在する事及びビットスライス構造を持つ為、トランケート評価では、大幅に緩い上界しか得られない。表中の()内の値は、参考文献[2]の繰り返しパスを全ラウンドに適用した値である。

192/256 ビット鍵の場合の安全性に関する取扱いについては 2012 年度に検討を行った。

2.7.3.　MULTI-S01 の MAC 機能について

MULTI-S01 はストリーム暗号としてリスト(2002 年度)に掲載されているが、 提案者は MAC 機能も謳っている。次期リストの暗号種別において新たに MAC を追加したので、その取り扱いについては 2012 年度に再度検討を行った。

[9] [3]　金子敏信, “共通鍵ブロック暗号CIPHERUNICORN-Aの安全性に関する詳細調査報告書”, http://www.cryptrec.go.jp/estimation/rep_ID0027.pdf, 2001

2.8. 2012 年度における安全性評価について

電子政府推奨暗号リストの改定を控えて、最近の暗号解読技術の進歩を踏まえた 128 ビットブロック暗号の安全性評価及び SSL/TLS で利用する際のストリーム暗号 128-bit RC4 の安全性評価を実施したので報告する。

2.8.1. 128 ビットブロック暗号

128 ビットブロック暗号（第 2 次評価までに特段問題点が指摘されなった 2009 年度応募暗号の CLEFIA 及び現行の電子政府推奨暗号である AES、CIPHERUNICORN-A、Camellia、Hierocrypt-3、SC2000）を評価対象とし、関連鍵攻撃及び中間一致攻撃(Biclique 攻撃を含む)に関して評価を行った。

(1) 関連鍵攻撃

全段で関連鍵攻撃が理論上可能なアルゴリズムは 192 及び 256 ビット鍵の AES のみであり、その他のアルゴリズムには関連鍵攻撃は見つかっていない。CIPHERUNICORN-A 及び 128 ビット鍵の Hierocrypt-3 については関連鍵攻撃の適用は困難であると報告されている。関連鍵攻撃の評価結果を表 3.12 に示す。

なお、256 ビット鍵の SC2000 に関して等価鍵[10]の存在が報告され、例示されている鍵の組が実際に等価鍵となっていることを事務局にて確認した。報告書で提示されている方法を用いた場合、等価鍵の組を見つけるための計算量は 2^{39} とのことである。取り扱いについては次年度以降に検討することとなった。

表 3.12　AES、CIPHERUNICORN-A 及び Hierocrypt-3 の関連鍵攻撃評価結果

アルゴリズム-鍵長	攻撃法	攻撃段数	計算量
AES-128	ブーメラン攻撃	7 段　(全 10 段)	2^{97}
AES-192	差分攻撃	11 段　(全 12 段)	2^{186}
	ブーメラン攻撃	12 段　(全 12 段)	2^{189}
AES-256	識別攻撃	14 段　(全 14 段)	2^{67} と 2^{37}
	ブーメラン攻撃	13 段　(全 14 段)	2^{76}
	ブーメラン攻撃	14 段　(全 14 段)	2^{99}
	差分攻撃	14 段　(全 14 段)	2^{131}
CIPHERUNICORN-A	適用不能	－　(全 16 段)	－
Hierocrypt-3-128	適用不能	－　(全 6 段)	－
Hierocrypt-3-192	差分攻撃	1 段　(全 7 段)	2^{144}
Hierocrypt-3-256	ブーメラン攻撃	2 段　(全 8 段)	2^{208}

[10]等価鍵とは、任意の平文の暗号化において同じ暗号文を出力する秘密鍵の組をいう。

表 3.13　128 ビットブロック暗号の中間一致攻撃（biclique 攻撃含む）評価結果

アルゴリズム-鍵長	データ量*	メモリ†	計算量‡	備考
AES-128	2^{64}	2^{8}	$2^{126.16}$	biclique 攻撃を適用
	2^{128}	2^{8}	$2^{125.6}$	biclique 攻撃を適用
AES-192	2^{80}	2^{8}	$2^{189.74}$	biclique 攻撃を適用
AES-256	2^{40}	2^{8}	$2^{254.42}$	biclique 攻撃を適用
Camellia-128	2^{128}	小	$2^{127.6}$	biclique 攻撃を適用
Camellia-192	2^{128}	小	$2^{191.7}$	biclique 攻撃を適用
Camellia-256	2^{128}	小	$2^{255.7}$	biclique 攻撃を適用
CIPHERUNICORN-A-128	2^{120}	2^{8}	$2^{127.6}$	biclique 攻撃を適用
CIPHERUNICORN-A-192	－	－	－	
CIPHERUNICORN-A-256	2^{112}	2^{8}	$2^{255.4}$	biclique 攻撃を適用
CLEFIA-128	2^{64}	小	$2^{127.7}$	biclique 攻撃を適用
CLEFIA-192	2	小	$2^{191.5}$	
CLEFIA-256	2^{64}	小	$2^{255.5}$	biclique 攻撃を適用
Hierocrypt-3-128	2^{96}	2^{8}	$2^{127.2}$	biclique 攻撃を適用
Hierocrypt-3-192	－	－	－	
Hierocrypt-3-256	2^{112}	2^{8}	$2^{255.5}$	biclique 攻撃を適用
SC2000-128	2	小	$2^{126.5}$	
SC2000-192	2	小	$2^{190.6}$	
SC2000-256	3	小	$2^{254.5}$	

＊ 攻撃に必要な平文-暗号文対の数
†攻撃の際に確保する必要があるメモリ上のデータの大きさ（ブロック長を単位としている）
‡攻撃に要する時間（暗号化 1 回を単位としている）

(2)中間一致攻撃（biclique 攻撃を含む）

現時点では、192 ビット鍵の CIPHERUNICORN-A 及び Hierocrypt-3 を除き、中間一致攻撃（biclique 攻撃含む）を適用できており、全数探索より小さい計算量で鍵を導出できると報告されている。特に、CLEFIA-192 と SC2000 については、biclique 攻撃を適用しない中間一致攻撃で、わずかな平文-暗号文対を用いて攻撃が可能であることが示されている。しかしながら、いずれについても必要な計算量は全数探索と比較してわずかに小さいだけであり、中間一致攻撃に対して十分な安全性を持っていると報告されている。中間一致攻撃の評価結果を表 3.13 に示す。

(3)その他（ゼロ相関線形攻撃）

Camellia 及び CLEFIA についてゼロ相関線形攻撃の解析を行い、192 ビット鍵の Camellia については（24 段中）11 段、256 ビット鍵の Camellia については（24 段中）12 段、192 ビット鍵の CLEFIA については（22 段中）13 段、256 ビット鍵の CLEFIA については（26 段中）14 段まで攻撃できることが報告されている。表 3.14 に

ゼロ相関線形攻撃の評価結果を示す。

表 3.14　Camellia 及び CLEFIA のゼロ相関線形攻撃評価結果

アルゴリズム-鍵長	攻撃段数	データ量	メモリ	計算量
Camellia-192	11 段（全 24 段）	$2^{125.1}$	2^{101}	$2^{157.79}$
Camellia-256	12 段（全 24 段）	$2^{125.9}$	2^{165}	$2^{234.31}$
CLEFIA-192	13 段（全 22 段）	$2^{125.8}$	2^{104}	$2^{159.56}$
CLEFIA-256	14 段（全 26 段）	2^{128}	2^{136}	2^{222}

2.8.2.　ストリーム暗号 128 ビット鍵 RC4

128 ビット鍵 RC4 を SSL3.0/TLS1.0 以上で利用する際の安全性について評価を行った。

(1)ストリーム暗号 128 ビット鍵 RC4 の安全性評価

識別攻撃、内部状態復元攻撃、鍵回復攻撃及び予測攻撃については、現実的な脅威になるものは報告されなかった。しかしながら、擬似乱数との識別が容易で、全数探索より効率的に秘密鍵を導出可能であることから、厳密な意味で 128 ビット安全性を有していないと報告されている。

(2)SSL3.0/TLS1.0 以上で RC4 を利用する場合の安全性

RC4 の脆弱性を利用した攻撃が現実的になる場合として、Broadcast セッティング（同じ平文を多数の異なる鍵で暗号化して送信するような場合）が考えられる。このセッティングにおける攻撃に関して、既存の研究では、平文の 2 バイト目が 2^8 程度の異なる鍵で生成された暗号文により、平文の 3～255 バイト目が 2^{24} 程度の異なる鍵で生成された暗号文により、それぞれ特定できることが示されている。

今回は、さらに 1 バイト目と 256 バイト目以降の平文を求める方法について検討が行われている。表 3.15 に Broadcast セッティングにおける平文導出の評価結果を示す。

表 3.15　Broadcast セッティングでの平文導出の評価結果

求める平文バイト位置	必要な暗号文数	備考
1 バイト目	2^{17}	2 バイト目の偏りも利用
2 バイト目	2^8	
3～255 バイト目	2^{24}	
256,257 バイト目	2^{32}	255 バイト目までの偏りも利用
258 バイト目以降	2^{34}	直前のバイトまでの偏りも利用

1 バイト目の平文は、1 及び 2 バイト目の偏りを併せて利用することにより、2^{17} 程度の鍵で生成された暗号文から導出できることを示している。257 バイト目までの平文につい

ては、新たに発見された 3～257 バイト目の偏りを利用することにより、2^{32} 程度の異なる鍵で生成された暗号文から導出できることを示している。258 バイト目以降については、257 バイト目までの偏りを利用して、以降のバイトの平文を逐次的に導出する方法が示され、2^{34} 程度の異なる鍵で生成された暗号文から平文を導出できると報告されている。

以上のように、Broadcast セッティングで RC4 を用いる場合、全てのバイトの平文を導出する攻撃が報告され、現実的な脅威になり得ることが示された。

2.9. 次期電子政府推奨暗号選定のための「安全性評価」判定方法及び「評価 B」「総合評価」に関する評価項目・配点について

2.9.1. 選考基準に対する検討について

2012 年度暗号方式委員会では、2011 年度の暗号技術検討会において承認された「電子政府推奨暗号選定のための選考基準案の考え方」に基づき、暗号技術の評価を行う必要がある。

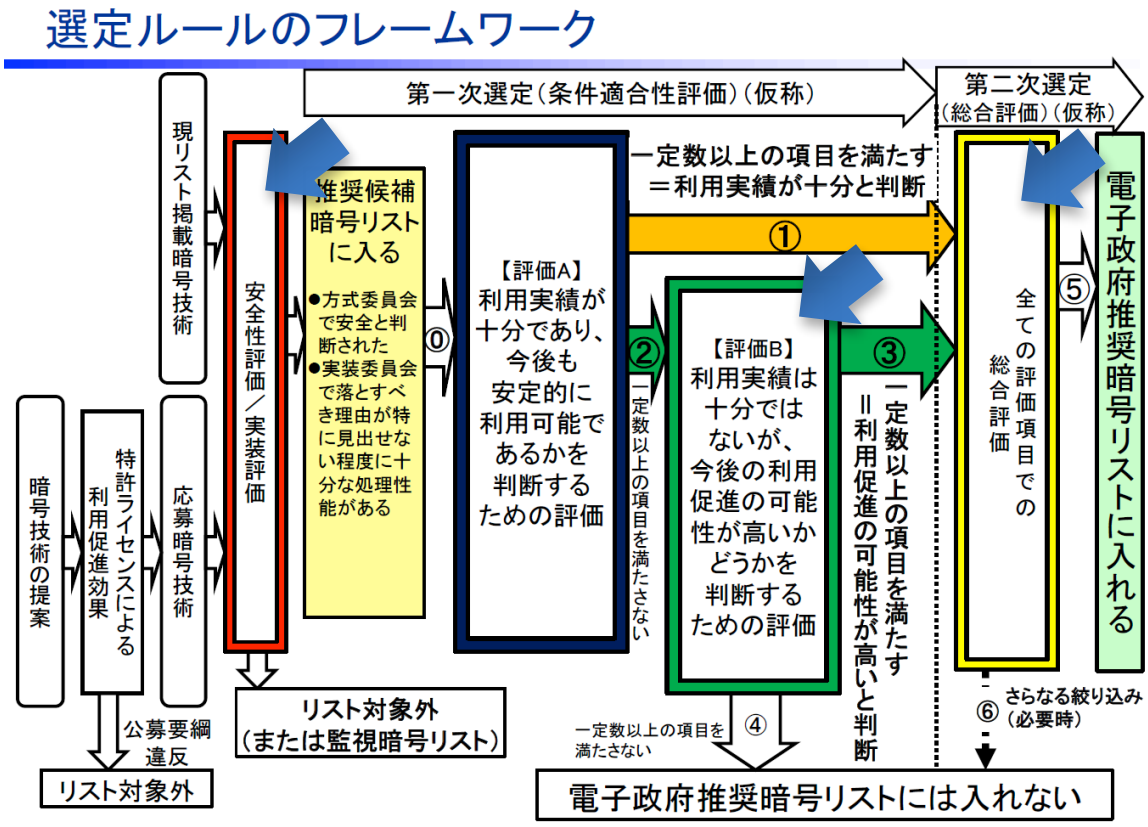


図 3.5 選定ルールのフレームワーク

承認された選定ルールのフレームワークにおいて、暗号方式委員会が実施する必要があるのは次の 3 点である（図 3.5 内の青矢印）。

1)「安全性評価」

評価対象の暗号技術が電子政府での利用において安全性上問題がないかを評価し、推奨候補暗号リストに入れるか、リスト対象外とするかを判定する。

2)「評価 B」

「評価 A」で利用実績が十分でないと判定された暗号技術について、今後の利用促進の可能性が高いかどうかを判定するための一項目として、「安全性」に関して「市場が認める程度の技術的アドバンテージがあるか」を判定する。

3)「総合評価」

評価項目の「技術的側面」の 2 項目「安全性についての仕様上のアドバンテージ」と「論文数の多寡によるアドバンテージ」の採点を行う。

本評価はさらなる絞り込みを行うためのものあるが、今回は、暗号技術検討会にて、安全性評価／実装評価／条件適合性評価の評価プロセスが十分に機能し、さらなる絞り込みは不要と判断されたため、実施されなかった。以下では「安全性評価」と「評価 B」の各々について説明する。

2.9.2. 「安全性評価」について

検討の対象となっている暗号技術には、

① リスト(2002 年度版)に記載されている暗号技術

② 2009 年度応募暗号技術（128 ビットブロック暗号／ストリーム暗号／メッセージ認証コードの 3 つの暗号カテゴリを含む)

③ 事務局選出暗号技術（メッセージ認証コード／暗号利用モード／エンティティ認証の 3 つの暗号カテゴリを含む)

の 3 つがあり、安全性に係る判定方針を下記の通り決定した。

① リスト(2002 年度版)に記載されている暗号技術に対する選定方針

(ア)監視結果等から判断して、リスト(2002 年度版)策定時における安全性評価結果が現在も妥当と判断されること。

ただし、新たな攻撃方法等が提案されている場合、それらに対しても安全性に関して問題がないと判断されること。

(イ)注釈が付いている場合、その内容が現在も妥当かどうかを検討した上で、安全性に問題がないと判断されること。

(ウ)(ア)及び(イ)を満たさない場合、原則として運用監視暗号リストに含める。

② 2009 年度応募暗号技術に対する選定方針

(ア)安全性評価結果(今年度に評価を実施する場合はそれも含む)に関して問題がないこと。

(イ) (ア)を満たさない場合、次期リストの選考外とする。

③ 事務局選出暗号技術に対する選定方針

(ア)安全性評価結果(今年度に評価を実施する場合はそれも含む)に関して問題がないこと。

(イ)(ア)を満たさない場合は、原則として次期リストの選考外とする。

なお、①・②・③に共通の方針として、同じ暗号カテゴリがある場合は、整合性のため、同じ評価基準を採用するものとする。

2.9.3.「評価 B」及び「総合評価」に関する評価項目・配点について

(1)「評価 B」に関する評価項目について

「評価 B」において、今後の利用促進の可能性が高いかどうかを判定するための一項目として「市場が認める程度の技術的アドバンテージがあるか」(以下、技術的アピールポイント)が設定されている。「技術的アピールポイント」は、安全性と実装性能の 2 つの観点から評価される[11]。暗号方式委員会では、「安全性」に関する技術的アピールポイントとして、以下の通り、評価方針(表 3.16)及び評価項目が了承された。

- 証明可能安全性の有無や安全性評価の容易性
- 安全性証明における仮定の妥当性
- 安全性証明の帰着効率
- 鍵の全数探索等よりも効率のよい攻撃の有無
- 安全性マージン(現時点での最長攻撃可能段数)
- 安全性に関連する利用上の制限の有無
- 提案論文が採録された国際会議・論文誌

表 3.16 「技術的アピールポイント」に係る評価方針

● 同じ暗号カテゴリにおける他の暗号アルゴリズムと比べて、安全性に関して事務局が指定する範囲のいずれかの評価項目において、技術的に優れている点が存在するかどうかの判定を行う。なお、応募者への問い合わせ内容において、事務局が指定する範囲外の評価項目が存在する場合は、暗号方式委員会にて承認があれば認めるものとする。 ● 応募暗号技術の場合は、応募者にその旨を問い合わせる。それ以外の場合は、事務局が調査する。 ● その内容の妥当性を暗号方式委員会が認めた場合、「技術的アピールポイント」があるものと判定する。

[11] 各々、暗号方式委員会と暗号実装委員会が評価し、少なくとも一方で「アドバンテージがある」と判断すれば、「技術的アピールポイント」があると判定される。

これらの評価項目について、応募暗号技術については応募者へ問い合わせ(付録 3 を参照のこと)、応募暗号でないものについては事務局にて作成し、その内容を暗号方式委員会にて検討する。

(2)「総合評価」に関する評価項目について

「総合評価」の評価項目「安全性についての仕様上のアドバンテージ」に関する評価方針は表 3.17 の通り了承された。

また、「総合評価」の評価項目「論文の多寡によるアドバンテージ」に関する評価方針は表 3.18 の通り了承された。なお、被引用数をポイントへ換算する方法としては、提案時から 2012 年 8 月末時点までの被引用数の値そのものを、配点（20 点）を上限としてポイントとすることとなった。

(3) 「総合評価」に関する配点について

「安全性についての仕様上のアドバンテージ」と「論文の多寡によるアドバンテージ」の配点については、「論文の多寡によるアドバンテージ」は「安全性についての仕様上のアドバンテージ」における各評価項目と同等の扱いとし、「安全性についての仕様上のアドバンテージ」における評価項目の総数が N 個の場合、当該比率を N 対 1 と決定した。

了承された配点にもとづき、「総合評価」の評価項目「安全性についての仕様上のアドバンテージ」「論文の多寡によるアドバンテージ」の配点は表 3.19 の通りとなった。

表 3.17 「安全性についての仕様上のアドバンテージ」に関する評価方針

- 各暗号カテゴリの評価項目数は同じにする。
- 各評価項目のポイントの比率は同じとする。
- 各暗号カテゴリの評価項目は下記の通りにする（評価項目数は 5)。

(a) 公開鍵暗号
  (1) 証明可能安全性の有無
  (2) 安全性証明における仮定の妥当性
  (3) 帰着効率の良し悪し
  (4) 利用上の制限の有無
  (5) 査読付きの国際会議・論文誌で提案論文が採録されたか否か

(b) 共通鍵暗号(64 ビット及び 128 ビットブロック暗号、ストリーム暗号)
  (1) 証明可能安全性の有無または安全性評価の容易性
  (2) 全数探索よりも効率の良い攻撃の有無
  (3) 安全性マージン(最長攻撃可能段数／仕様段数)
  (4) 利用上の制限の有無
  (5) 査読付きの国際会議・論文誌で提案論文が採録されたか否か

(c) ハッシュ関数
  (1) ハッシュ長（256 ビット以上か否か)
  (2) 衝突発見困難性に関する安全性マージン（最長攻撃可能段数／仕様段数)
  (3) 第二原像計算困難性に関する安全性マージン（最長攻撃可能段数／仕様段数)
  (4) 原像計算困難性に関する安全性マージン（最長攻撃可能段数／仕様段数)
  (5) 利用上の制限の有無

(d) メッセージ認証コード
  (1) 証明可能安全性の有無
  (2) 安全性証明における仮定の妥当性
  (3) 帰着効率の良し悪し
  (4) 利用上の制限の有無
  (5) 査読付きの国際会議・論文誌で提案論文が採録されたか否か

(e) 暗号利用モード
  (1) 証明可能安全性の有無
  (2) 安全性証明における仮定の妥当性
  (3) 帰着効率の良し悪し
  (4) 利用上の制限の有無
  (5) 査読付きの国際会議・論文誌で提案論文が採録されたか否か

(f) エンティティ認証
  (1) 証明可能安全性の有無
  (2) 安全性証明における仮定の妥当性
  (3) 帰着効率の良し悪し
  (4) 利用上の制限の有無
  (5) 査読付きの国際会議・論文誌で提案論文が採録されたか否か

表 3.18　「論文数の多寡によるアドバンテージ」に関する評価方針

● 暗号技術が提案された文献の被引用数の多い・少ないを判定する。 ● 調査対象となる暗号技術に対する安全性評価に関する論文のみを対象とする。安全性評価に関する論文に限定するため、被引用数が多い暗号技術に対しては、サンプリングより被引用数を推定する。 ● 引用論文の調査範囲は、論文誌または Springer LNCS[12]、IEEE[13]、ACM[14]で論文が出版されている査読付き国際会議とし、調査先は、検索サイト(例：GoogleScholar, http://scholar.google.co.jp/)または既存の学術データベースを利用する。 ● 引用元である暗号技術が提案された文献に関して複数の候補がある場合には、主要な 3 つの文献に基づいて調査する。また、重複は可能な限り除外する。 ● 暗号カテゴリ間のポイントのばらつきに起因する調整は行わない。

表 3.19 「総合評価」に関する配点

評価項目	配点
安全性についての仕様上のアドバンテージ　(各暗号カテゴリ 5 項目)	100
論文の多寡によるアドバンテージ	20

2.9.4.　「安全性評価」判定結果

リスト(2002 年度)、新規応募暗号、事務局選出暗号を、推奨候補暗号、または運用監視暗号に分類する必要がある。これら暗号技術を承認された方針に従い分類する。

表 3.20　第 2 回暗号方式委員会における検討対象暗号技術

技術分類	名称
署名	DSA、ECDSA、RSASSA-PKCS1-v1_5、RSA-PSS
守秘	RSA-OAEP、RSAES-PKCS1-v1_5*
鍵共有	DH、ECDH、PSEC-KEM*
ハッシュ関数	RIPEMD-160*、SHA-1*、SHA-256、SHA-384、SHA-512
暗号利用モード	CBC モード、CFB モード、OFB モード、CTR モード、CCM モード
メッセージ認証コード	CBC-MAC+、CMAC、HMAC
エンティティ認証	ISO/IEC 9798-2+、ISO/IEC 9798-3+、ISO/IEC 9798-4+

* は注釈が付いている技術

+ は監視活動等により安全性上の問題が報告されている技術

[12] Springer Lecture Notes in Computer Science (http://www.springer.com/lncs)
[13] The Institute of Electrical and Electronics Engineers (http://www.ieee.org/)
[14] Association for Computing Machinery (http://www.acm.org/)

表 3.21　第 3 回暗号方式委員会における検討対象暗号技術

技術分類	名称
64 ビットブロック暗号*	CIPHERUNICORN-E, Hierocrypt-L1, MISTY1, 3-key Triple DES*
128 ビットブロック暗号	AES+, Camellia, CIPHERUNICORN-A, Hierocrypt-3, SC2000, CLEFIA
ストリーム暗号	MUGI, MULTI-S01+, 128-bit RC4*+, Enocoro-128v2, KCipher-2
メッセージ認証コード	PC-MAC-AES, CBC-MAC+(再)
暗号利用モード	GCM+

＊ は注釈が付いている技術

+ は監視活動等により安全性上の問題が報告されている技術

(1)リスト(2002 年度版)に記載されている暗号技術

【公開鍵暗号】

・DSA／ECDSA／RSASSA-PKCS1-v1_5／RSA-PSS／RSA-OAEP／DH／ECDH の分類

*、+ 印が付いていない技術は、安全性上の問題が報告されておらず、また注釈もついていない。従って、これら暗号技術については、次期リストの推奨候補暗号とする。

・RSAES-PKCS1-v1_5 の分類

現在、注釈「SSL3.0/TLS1.0 で使用実績があることから当面の使用を認める」が付与されている。Bleichenbacher の攻撃[15]といった現実的な攻撃が起因となり付与された注釈であり、次期リストの運用監視暗号とする。　新たな注釈は「SSL3.0/TLS1.0, 1.1,1.2 で使用実績があることから当面の使用を認める」とする。

・PSEC-KEM の分類

現在、注釈「KEM(Key Encapsulating Mechanism)-DEM(Data Encapsulating Mechanism)構成における利用を前提とする」が付与されている。メッセージの秘匿化に使用する技術を DEM にすることを推奨しているものであり、鍵共有部である (PSEC-) KEM に、安全性に係わる問題は報告されていないため、次期リストの推奨候補暗号とする。　注釈は、引き続き同じものを使用する。

[15] D. Bleichenbacher: Chosen Ciphertext Attacks Against Protocols Based on the RSA Encryption Standard PKCS #1, CRYPTO 1998, pp.1-12, 1998.

【64 ビットブロック暗号】

・CIPHERUNICORN-E／Hierocrypt-L1／MISTY1 の分類

安全性に係る問題は報告されていないため、次期リストの推奨候補暗号とする。

注釈は、以前と同じもの[16]を使用する。

・3-key Triple DES の分類

安全性に係る問題は報告されていないため、次期リストの推奨候補暗号とする。

注釈は、以前と同じもの[17]を使用する。

【128 ビットブロック暗号】

・AES の分類

AES-192/AES-256 は関連鍵攻撃に対する脆弱性を有するが[18]、単一鍵の通常の利用に関しては安全性に問題はない。また、鍵の全数探索の効率性を高めた Biclique 攻撃は多くのブロック暗号に適用可能であるが、AES に対する Biclique 攻撃[19]は依然として計算量が大きいため、安全性に問題はない。よって AES を次期リストの推奨候補暗号とする。

・Camellia／CIPHERUNICORN-A／Hierocrypt-3／SC2000 の分類

安全性に係る問題が報告されていないため、次期リストの推奨候補暗号とする。

なお、SC2000 の等価鍵については次年度以降に検討を行う。

【ストリーム暗号】

・MUGI の分類

安全性に係る問題は報告されていないため、次期リストの推奨候補暗号とする。

・MULTI-S01 の分類

MULTI-S01 の認証部分の構造は GCM のそれと類似しており、FSE 2012 において報告された GCM の弱鍵発見手法[20]が適用可能であるが、その割合は非常に小さいため、安全性に問

---

[16] (注 3)新たな電子政府用システムを構築する場合、より長いブロック長の暗号が使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。

[17] (注 3)及び(注 4)3-key Triple DES は、以下の条件を考慮し、当面の使用を認める。
1)(NIST の)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。

[18] A. Biryukov and D. Khovratovich, Related-key Cryptanalysis of the Full AES-192 and AES-256, Asiacrypt 2009, LNCS 5912, p.1-18.

[19] A. Bogdanov, D. Khovratovich and C. Rechberger, Biclique Cryptanalysis of the Full AES, ASIACRYPT 2011, LNCS 7023, p.344-371.

[20] Saarinen, Cycling Attacks on GCM, GHASH and Other Polynomial MACs and Hashes, FSE 2012, LNCS 7549, p.216-225.

題はない。他に安全性に係わる問題は報告されていないため、次期リストの推奨暗号暗号とする。なお、パディング方法に問題があり、平文サイズが 64 ビットの倍数でなければ正常に復号できないため[21]、注釈は、「平文サイズは 64 ビットの倍数に限る。」とする。なお、ISO/IEC 18033-4 において同じ名称の暗号技術があるが、CRYPTREC に応募されたものとは異なる。

・128-bit RC4 の分類

同じ平文を各々別々の鍵で暗号化しブロードキャストするような場合において、安全性に係る問題が報告されているため、次期リストの運用監視暗号とする。

注釈は、引き続き同じもの[22]を使用する。

【ハッシュ関数】

・SHA-1／RIPEMD-160 の分類

現在、注釈「新たな電子政府用システムを構築する場合、より長いハッシュ値のものが使用できるのであれば、256 ビット以上のハッシュ関数を選択することが望ましい。ただし、公開鍵暗号での仕様上、利用すべきハッシュ関数が指定されている場合には、この限りではない。」が付与されている。本暗号技術のハッシュ長は 160 ビットであり、安全性の観点から 256 ビット以上のハッシュ関数を選択することが望ましいため、次期リストの運用監視暗号とする。注釈は、引き続き同じものを使用する。

(2) 2009 年度応募暗号技術

【128 ビットブロック暗号】

・CLEFIA の分類

安全性に係る問題は報告されていないため、次期リストの推奨候補暗号とする。

【ストリーム暗号】

・Enocoro-128v2／KCipher-2 の分類

安全性に係る問題は報告されていないため、次期リストの推奨候補暗号とする。

【メッセージ認証コード】

・PC-MAC-AES の分類

安全性に係る問題は報告されていないため、次期リストの推奨候補暗号とする。

---

[21] 古屋、渡辺、宝木、MULTI-S01 のパディングと安全性についての考察、信学技法、ISEC2000-68.

[22] 128-bit RC4 は、SSL(TLS1.0 以上)に限定して利用することを想定している。

(3)事務局選出暗号技術

【メッセージ認証コード】

・CMAC／HMAC の分類

*、+ 印が付いていない技術は、安全性上の問題が報告されておらず、また注釈もついていない。従って、これら暗号技術については、次期リストの推奨候補暗号とする。

・CBC-MAC の分類

メッセージ長が固定の場合、MAC として安全であるが、メッセージ長が可変の場合、容易に MAC の偽造が出来る[23]。安全性に問題があるため、次期リストの運用監視暗号にする。注釈は、「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。」とする。

・GCM の分類

FSE 2012 において弱鍵の存在が報告されたが、その割合は非常に小さいため、安全性に問題はない。CRYPTO 2012 において、安全性証明に問題が見つかったが、新たに証明が修正された[24]。他に安全性に係る問題は報告されていないため、次期リストの推奨候補暗号とする。注釈は、「初期化ベクトルは 96 ビット長を推奨する。」とする。

【暗号利用モード】

CBC／CFB／OFB／CTR／CCM モードの分類

*、+ 印が付いていない技術は、安全性上の問題が報告されておらず、また注釈もついていない。従って、これら暗号技術については、次期リストの推奨候補暗号とする。

【エンティティ認証】

・ISO/IEC 9798-2／ISO/IEC 9798-3／ISO/IEC 9798-4 の分類

第 1 次評価において一部のタイプに脆弱性が発見されたが、ISO/IEC にて規格修正され、安全性上の問題が取り除かれたため、次期リストの推奨候補暗号とする。　注釈は付与しない。

---

[23] A.J. Menezes, P.C. van Oorschot, and S.A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.

[24] T. Iwata, K. Ohashi and K. Minematsu, Breaking and Repairing GCM Security Proofs, CRYPTO 2012, LNCS 7417, p.31-49.

2.9.5. 「評価 B（技術的アピールポイント）」に係る判定結果

比較対象としては、市場において比較的多く使われている暗号技術を比較対象として選択した。なお、判定の根拠については、委員会が主体的に優位点の有無を判定したため、必ずしも応募者からの回答と必ずしも一致していない。

技術分類	暗号技術名	回答	比較対象	判定の根拠	判定
署名	DSA				
	ECDSA	有	RSASSA-PKCS1-v1_5	Index calculus 法は楕円曲線上の離散対数問題を解くには現時点ではまだ効率的であるとは言えない。	有
	RSA-PSS	－	RSASSA-PKCS1-v1_5	証明可能安全性(適応的選択文書攻撃に対して存在的偽造不可)がランダムオラクルモデルのもとで RSA 問題の困難性に帰着される。	有
	RSASSA-PKCS1-v1_5				
守秘	RSAES-PKCS1-v1_5				
	RSA-OAEP	－	RSAES-PKCS1-v1_5	証明可能安全性(適応的選択暗号文攻撃に対して強秘匿)がランダムオラクルモデルのもとで RSA 問題の困難性に帰着される。	有
鍵共有	DH				
	ECDH	有	DH	Index calculus 法は楕円曲線上の離散対数問題を解くには現時点ではまだ効率的であるとは言えない。	有
	PSEC-KEM	有	DH	KEM 技術に関する証明可能安全性がランダムオラクルモデルのもとで楕円曲線 DH 計算問題に帰着され、KEM(Key Encapsulation Mechanism)-DEM(Data Encapsulation Mechanism)構成に利用することは安全であることが示されている。	有
64 ビットブロック暗号	CIPHERUNICORN-E	有	3-key Triple DES	解析が困難な構造が採用されており、有効な攻撃法は見つかっていない。	有
	Hierocrypt-L1	有	3-key Triple DES	多くの攻撃手法に対する安全性評価がなされており、鍵の全数探索よりも効率の良い攻撃手法が知られていない。	有
	MISTY1	－	3-key Triple DES	差分攻撃および線形攻撃に対する証明可能安全性を有し、多くの攻撃手法に対する安全性評価がなされている。	有
	3-key Triple DES				

128 ビットブロック暗号	AES				
	Camellia	有	AES	多くの攻撃手法に対する安全性評価がなされており、特に AES に適用されているような関連鍵攻撃は見つかっていない。	有
	CIPHERUNICORN-A	有	AES	解析が困難な構造が採用されており、関連鍵攻撃をはじめ有効な攻撃法は見つかっていない。	有
	CLEFIA	有	AES	多くの攻撃手法に対する安全性評価がなされており、特に AES に適用されているような関連鍵攻撃は見つかっていない。	有
	Hierocrypt-3	有	AES	多くの攻撃手法に対する安全性評価がなされており、特に AES に適用されているような関連鍵攻撃は見つかっていない。	有
	SC2000	有	AES	多くの攻撃手法に対する安全性評価がなされており、特に AES に適用されているような関連鍵攻撃は見つかっていない。	有
ストリーム暗号	Enocoro-128v2	有	RC4	現時点において鍵の全数探索よりも効率の良い攻撃手法が知られていない。	有
	KCipher-2	有	RC4	現時点において鍵の全数探索よりも効率の良い攻撃手法が知られていない。	有
	MUGI	有	RC4	現時点において鍵の全数探索よりも効率の良い攻撃手法が知られていない。	有
	MULTI-S01	有	RC4	現時点において鍵の全数探索よりも効率の良い攻撃手法が知られていない。	有
	RC4				
ハッシュ関数	RIPEMD-160				
	SHA-1				
	SHA-256		SHA-1	Preimage attack、2nd-Preimage attack、Collision attack において、generic attack よりも効率の良い攻撃は知られていない。	有
	SHA-384		SHA-1	Preimage attack、2nd-Preimage attack、Collision attack において、generic attack よりも効率の良い攻撃は知られていない。	有
	SHA-512		SHA-1	Preimage attack、2nd-Preimage attack、Collision attack において、generic attack よりも効率の良い攻撃は知られていない。	有
メッセージ認証	CBC-MAC				
	CMAC		CBC-MAC	メッセージ空間に関する制約(prefix-free)のない安全性モデルにおいて証明可能安全性を有する。	有

コード	HMAC				
	PC-MAC-AES	有	CBC-MAC	メッセージ空間に関する制約(prefix-free)のない安全性モデルにおいて証明可能安全性を有する。	有
暗号利用モード	CBC				
	CFB		CBC	選択平文攻撃に対して、CBC と同程度の安全性である。	無
	OFB		CBC	選択平文攻撃に対して、CBC と同程度の安全性である。	無
	CTR		CBC	選択平文攻撃に対して、CBC と同程度の安全性である。	無
	GCM		CBC	適応的選択暗号文攻撃に対する証明可能安全性を有する。	有
	CCM		CBC	仕様変更した場合(守秘用と認証用で独立な個別の鍵を用いた場合)、適応的選択暗号文攻撃に対する証明可能安全性を有する。	有
エンティティ認証	ISO/IEC 9798-2		N/A	ISO/IEC 29128 PAL3 レベルに沿った形式検証において安全性検証済みである。他の方式には同等のプロセスによる検証結果はない。	有
	ISO/IEC 9798-3		N/A	ISO/IEC 29128 PAL3 レベルに沿った形式検証において安全性検証済みである。他の方式には同等のプロセスによる検証結果はない。	有
	ISO/IEC 9798-4		N/A	ISO/IEC 29128 PAL3 レベルに沿った形式検証において安全性検証済みである。他の方式には同等のプロセスによる検証結果はない。	有

2.10. CRYPTREC シンポジウム 2013 の開催

2012 年度は、電子政府推奨暗号リストの改定のために応募暗号技術の第 2 次評価及びリスト(2002 年度版)に掲載された暗号技術の再評価を実施し、次期リスト選定基準の検討を行った。本シンポジウムにおいて、最新の評価結果を公表し、それらについて検討した。

2.10.1 プログラムの概要

日時：2013 年 3 月 26 日（火）10：00～16：00
場所：コクヨホール
主催：独立行政法人情報通信研究機構、独立行政法人情報処理推進機構
共催：総務省、経済産業省
参加人数：238 名

表 3.22 プログラム

時間	内容	
10:00	開会挨拶	情報処理推進機構　理事　仲田雄作
10:05	総務省挨拶 経済産業省挨拶	政統括官（情報通信担当）　阪本泰男 商務情報政策局担当審議官　中山亨
10:15	CRYPTREC 暗号リストについて	暗号技術検討会事務局　総務省　上原哲太郎
10:40	暗号方式委員会報告	今井秀樹教授（中央大学）
10:45	暗号実装委員会報告	本間尚文准教授（東北大学）
11:05	暗号運用委員会報告	松本勉教授（横浜国立大学）
11:45	昼休み	
12:40	パネルディスカッション 「CRYPTREC 暗号リストの活用と日本の暗号・情報セキュリティ技術の競争力向上に向けて」	（パネリスト） 岡本龍明様（NTT/京都大学） 岩下直行様(日立製作所) 伊豆哲也様(富士通研究所) 三角育生参事官(NICT) 澤田稔一室長（総務省） 山碕良志室長（総務省） 上村昌博室長（経済産業省） （コーディネータ） 盛合志帆（NICT）
14:40	休憩	
15:00	リストガイド WG 報告	手塚悟教授（東京工科大学）
15:30	計算機能力評価 WG 報告	高木剛教授（九州大学）
16:00	閉会挨拶	情報通信研究機構　理事　榎並和雅

第３章 監視活動

3.1.監視活動報告

電子政府推奨暗号の安全性評価について2012年度の報告時点では収集した全ての情報が「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。

3.1.1.共通鍵暗号に関する安全性評価について

AES に対する攻撃には目立った進展はなく、関連鍵攻撃及び単一鍵攻撃で最も成功した攻撃は次の通りである。

・AES-128: 選択平文2^{88}個、計算量 $2^{126.2}$で攻撃可能 [1]

・AES-192: 選択平文2^{116}個、計算量2^{169} で攻撃可能 [2]

・AES-256: 選択平文2^{140}個、計算量$2^{254.4}$で攻撃可能[1]

AESの単一鍵攻撃について、最も成功した攻撃は次の通りである。

・AES-128:7段(10段中)を選択平文$2^{112.2}$個、メモリ量 $2^{117.2}$、計算量 2^{172}で攻撃可能 [3]

・AES-192: 8段(12段中)を選択平文2^{113}個、メモリ量 2^{129}、 計算量 2^{172}で攻撃可能 [4]

・AES-256: 8段(14段中)を選択平文2^{113}個、 メモリ量 2^{129}、 計算量 2^{196}で攻撃可能[3]

3.1.2.公開鍵暗号に関する安全性評価について

A.K. Lenstra らが Crypto 2012 で、実社会に公開されている RSA 公開鍵証明書(X.509)を6,582,851件収集して解析したところ、66,729個(約4%)で同じmodulusが使われ、12,934個(約0.2%)のmodulusが素因数分解できた。素因数分解が出来たのは、素因数の片方を共有するmodulusが存在するためで、共通の素因数が生じる原因は、鍵生成で利用される乱数生成でのエントロピーが小さいためと考えられ、N.HeningerらはUSENIX Security 2012において、分析と対策を示した。

---

[1] A. Bogdanov, D. Khovratovich, and C. Rechberger, *Biclique Cryptanalysis of the Full AES*, ASIACRYPT 2011, LNCS 7073, pp. 344-371. Springer, 2011.

[2] A. Biryukov and I. Nikolic, *Automatic Search for Related-Key Differential Characteristics in Byte-Oriented Block Ciphers: Application to AES, Camellia, Khazad and Others*, EUROCRYPT 2010. LNCS 6110, pp.322-344. Springer, 2010

[3] J. Lu, O. Dunkelman, N. Keller, and J. Kim, *New impossible differential attacks on AES*, INDOCRYPT 2008, LNCS 5365, pp. 279-293. Springer 2008

[4] O. Dunkelman, N. Keller, and A. Shamir, *Improved Single-Key Attacks on 8-Round AES-192 and AES-256*, ASIACRYPT 2010, LNCS 6477, pp.158-176. Springer, 2010

3.1.3. ハッシュ関数に関する安全性評価について

Crypto 2012 において、S.Knellwolf と D.Khovratovich が SHA-1 に対する原像攻撃が可能な段数を従来の48段(仕様は80段)から57段に伸ばしたと発表した。従来の攻撃はCrypto 2009 で発表され、48 段に対する 2 ブロックの原像を圧縮関数計算 $2^{159.3}$ 回分で求めるものだったが、パディングは不正確なものだった。今回は、1 ブロック原像と 2 ブロック原像の両方を計算量 $2^{150.6}$ で求めることができ、パディングも正しいものである。

NIST は 2012 年 10 月 2 日付けで最終 5 候補の一つ Keccak を SHA-3 に選んだことを発表した。選考理由としては安全性マージンの大きさと、唯一ハードウェア実装性能で SHA-2 を上回ったことなどとしている。なお、パラメータの設定を変更するなどの修正が行われる可能性があり、SHA-3 としての最終的な仕様は確定していない。最終 5 候補に対する評価結果は、NIST が「Third-Round Report of the SHA-3 Cryptographic Hash Algorithm Competition」[5]として公表している。

3.2. 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3.2に示す通りである。

表 3.2 国際会議への参加状況

学会名・会議名		開催国・都市	期間
Eurocrypt 2012	International Conference on the Theory and Applications of Cryptographic Techniques	英国・ケンブリッジ	2012 年 4 月 15 日～4 月 19 日
PKC 2012	International Conference on Practice and Theory of Public-Key Cryptography	ドイツ・ダルムシュタット	2012 年 5 月 21-5 月 23 日
SAC 2012	Conference on Selected Areas in Cryptography	カナダ・ウィンザー	2012 年 8 月 16 日～8 月 17 日
Crypto 2012	International Cryptology Conference	米国・サンタバーバラ	2012 年 8 月 19 日～8 月 23 日
CHES 2012	Workshop on Cryptographic Hardware and Embedded Systems	ベルギー・ルーベン	2012 年 9 月 9 日～9 月 12 日

[5] http://nvlpubs.nist.gov/nistpubs/ir/2012/NIST.IR.7896.pdf

Asiacrypt 2012	International Conference on the Theory and Application of Cryptology and Information Security	中国・北京	2012 年 12 月 3 日～12 月 6 日
PKC 2013	International Conference on Practice and Theory in Public-Key Cryptography	日本・奈良	2013 年 2 月 27 日～3 月 1 日
TCC 2013	Theory of Cryptography Conference	日本・東京	2013 年 3 月 3 日～3 月 6 日
FSE 2013	International Workshop on Fast Software Encryption	シンガポール	2013 年 3 月 11 日～3 月 13 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 3 を参照のこと。

3.2.1.ブロック暗号の解読技術

・An All-In-One Approach to Differential Cryptanalysis [SAC 2012]

差分解読法には、標準型の他、高階差分、不能差分、improvable 差分など、多様なバリエーションがあるので、これらから得られるゲインを多次元ベクトルとして扱うことによって、解読効率を改善することを提案した。このアプローチは、具体的な経路探索が可能なブロック長が小さい暗号に対して有効である。CHES 2009 で提案された 32 ビット暗号の KATAN-32 に適用したところ、差分に関する分布の偏りを従来より 20 段多い 91 段へ伸ばし、それを利用して 115 段縮小版の攻撃に成功した。この他、PRESENT のブロック長を 16 ビットに縮小した PRESENT-[4]について、差分経路を網羅的に調べ、従来法では 7 段までしか攻撃できなかったものを 9 段まで攻撃可能にした。なお、この攻撃に必要なメモリはブロック長の増加に対して急激に増加し、KATAN の 48 ビット版の KATAN-48 では $O(2^{48})$オーダとなり、現実的ではなくなる。

・Meet-in-the-Middle Technique for Integral Attacks against Feistel Ciphers [SAC 2012]

積分攻撃では特定の入力バイトは全値、他の入力バイトを固定して得られる識別子(distinguisher)を利用して鍵探索を行う。本発表では、識別子を利用した鍵探索において、異なるブランチに属する拡大鍵に共通して存在する鍵ビットを見つけることによって、攻撃の計算量が削減することを提案した。この方法により、HIGHT の 22 段縮小版に対する計算量を従来の $2^{118.71}$ から $2^{102.35}$ へ、CLEFIA(128 ビット鍵)の 12 段縮小版に対する計算量を従来の $2^{116.7}$ から $2^{103.1}$ へ削減できることを示した。また、LBlock の 20 段縮小版に対する Khovaratovich らの攻撃(FSE 2010)の誤りを指摘し、新たに選択

平文数 $2^{63.6}$、計算量 $2^{39.6}$ で攻撃できることを示した。

・Improved Cryptanalysis of the Block Cipher KASUMI [SAC 2012]

KASUMI は ETSI SAGE が設計した 64 ビットブロック暗号である。Asiacrypt 2012 で Dunkelman らが 8 段のフルバージョンを関連鍵攻撃(関連鍵 4 個)で破れることを示したが、単一鍵では破れていない。今回の発表では、FI 関数を鍵依存の 16 ビット S-box と見なして、鍵ごとの差分分布テーブルを作ることによって、不能差分解読法を改良し、7 段縮小版の不能差分攻撃を示した。縮小の仕方は、後 7 段(初段を削除)と前 7 段(最終段を削除)の 2 種類があり、前者で選択平文 $2^{52.5}$ 組、暗号化 $2^{114.3}$ 回分の計算量、後者で既知平文 2^{62} 組、暗号化 $2^{115.8}$ 回分の計算量で攻撃可能であることを示した。

3.2.2.ストリーム暗号の解読技術

・Cryptanalysis of the ‘Kindle’ Cipher [SAC 2012]

Amazon の電子書籍リーダ Kindle では、著作兼管理用にストリーム暗号 PC1 が利用されている。PC1 は 1991 年に Pukall が設計した自己同期型ストリーム暗号で、鍵は 128 ビットで、16 ビットの add, mult, xor 演算を利用し、IV は無く、8 ビットずつ鍵ストリームを出力する。内部状態が小さいので、頻繁に起こる内部状態での衝突を利用した攻撃が有効で非常に弱く、次の攻撃が示された。

・既知平文攻撃　計算量: 2^{31}, 平文数: 2^{20}

・暗号文単独攻撃　計算量 2^{35}, 平文数: 2^{17}

また、PC1 を利用したハッシュ関数 PSCHF も提案されており、計算複雑度 2^{24} で、意味のあるメッセージをターゲットとする第２原像攻撃が成功することが示されている。

3.2.3.ハッシュ関数の解読技術

・New Preimage Attacks Against Reduced SHA-1 [Crypto 2012]

本論文では、57 段まで縮退した SHA-1 に対する原像攻撃を示す。これまでの最良の攻撃は、Crypto 2009 で示された 48 段に対するもので、$2^{159.3}$ の圧縮関数評価コストで不正確なパディングの 2 つのブロック原像を見つけるものであった。同様の版に対して、我々の攻撃は $2^{150.6}$ の圧縮関数評価コストで 1 ブロック原像を、また $2^{150.6}$ の圧縮関数評価コストで正しくパディングされた 2 ブロック原像を見出すことができる。青木-佐々木らにより開発された中間一致テクニックを差分的見地で見ることにより本改良結果が得られる。この新しいフレームワークは中間一致攻撃を差分解析に近く関係づけるものであり、線型メッセージ拡大と弱い拡散性を持ったハッシュ関数には特に有効である。

・Boomerang and Slide-Rotational Analysis of the SM3 Hash Function [SAC 2012]

SM3 は中国の国内標準のハッシュ関数で、SHA-1 に対する差分解読で有名な Xiaoyun Wang(清華大学)らが設計した。中国は 2007 年 12 月に TPM の中国版ともいえる TCM を発表し、その中で、ブロック暗号 SMS4、公開鍵暗号 SM2、ハッシュ関数 SM3 を採用している。MD 構造で、内部状態 256 ビット、メッセージブロックサイズ 512 ビット、ハッシュサイズ 256 ビット、64 ステップとなっている。本発表では次のブーメラン識別子が発表された。

・33 ステップ、確率 $2^{-32.4}$

・34 ステップ、確率 $2^{-53.1}$

・35 ステップ、確率 $2^{-117.1}$

SHA-2 に対しては、Asiacrypt 2011 で 64 ステップ中 47 ステップのブーメラン識別子が発表されているので、この点に関しては SHA-2 より安全性は高い。SHA2 と異なり、SM3 には単純なスライド回転の性質があるが、具体的な攻撃には繋がっておらず、現在のところ安全性上の脅威はない。

3.2.4.公開鍵暗号の解読技術

・Public Keys [Crypto 2012]

実社会に公開されている RSA 公開鍵証明書を 6,582,851 件収集し、その内の 266,729 個(約 4%)は同じ modulus が使われており、12,934 個(約 0.2%)の modulus は、同じ素因子が存在するため素因数分解することができた。公開鍵情報である合成数 N は、2 つの素数の積 N=pq の形をしており、N を素因数分解することは困難であることが公開鍵暗号の安全性の根拠となっている。公開鍵の modulus が一致する場合、互いの秘密鍵を求めることができる。2 つの合成数 $N_1=pq_1$、$N_2=pq_2$ がたまたま素数 p を共通因子として持った場合、それらの最大公約数(GCD)は第三者が高速に計算することができ、秘密の素数 p を出力してしまう。原因は、鍵生成の際の乱数生成のエントロピーが小さい場合、たまたま同じ乱数を生成してしまうことにあると考えられる。N.Heninger らがランプセッションおよび 8 月 8 日～8 月 10 日に開催された USENIX Security 2012 において、エントロピーが低くなる原因について分析を行い、チェックツールを公開している[6]。既に秘密鍵が見つかってしまった公開鍵証明書に関しては再発行するしかなく、今後の対策としては、鍵生成時のエントロピーを十分大きくする手段を講ずる必要がある。

[6] https://factorable.net/

・Efficient Dissection of Composite Problems, with Applications to Cryptanalysis, Knapsacks, and Combinatorial Search Problems (Best Paper Award) [Crypto 2012]

本論文において、大きなクラスの様々な問題が、複数の合成された構造を持ち、そのことによって既知のアルゴリズムよりも良い時間／メモリトレードオフを持つ、新しいタイプの「分解(dissection)」攻撃が可能となることを示す。典型的な例は、r 個の独立した n ビット鍵を持つ、複数回暗号化スキームの鍵を求める問題である。エラーのない既知攻撃は、すべて $TM=2^{rn}$ を満たす時間 T およびメモリ M を必要とし、「誤り」を許容した場合でも、$TM < 2^{3rn/4}$ を満たす攻撃はなかった。我々の新しい攻撃は、誤ることはなく、より小さな TM の積で、可能性のある鍵をすべて見出す初めてのアルゴリズムとなる。例えば、r=7 のブロック暗号の連続実行を解読するのに、$T=2^{4n}$ および $M=2^{n}$ しか必要としない。改良の割合は、r が増加するにつれて上限なく大きくなり、時々誤った解を求めるアルゴリズムを許したときには、我々の分解テクニックと並行衝突探索とを組み合わせることにより、より良いトレードオフを得ることができる。新しい分解テクニックの汎用性を示すために、以下の問題における一般的な使い方を与える：ハッシュ関数をリバウンド攻撃で攻撃する場合、困難なナップサック問題を解く場合、一般化されたルービック・キューブに対する最短解を既知の最良アルゴリズムよりも良い時間計算量(小さなメモリ計算量の場合)で求める問題など。

・Breaking Pairing-Based Cryptosystems Using η_T Pairing over GF(3^{97}) [Asiacrypt 2012]

GF(3^n) 上の η_T ペアリングを用いたペアリング暗号はその安全性を GF(3^n) 上の ECDLP と GF(3^{6n}) 上の DLP を解くことの困難性に依存する。拡大次数 n = 97 は η_T ペアリングの実装実験で実際に採用され、注目されている拡大次数である。本発表では、小さい標数の拡大体上の DLP を効率よく解く関数体篩法に、格子篩などの高速アルゴリズムを改良して導入し、関数体篩法の最適なパラメータ値を採用することで、923 bit 長である GF($3^{6\cdot 97}$) 上の DLP を 148.2 日で解いたことを報告している。この成果は GF(3^{6n}) の形の拡大体上の DLP を解くことにおいて世界記録を達成したことを意味している。

・Efficient Padding Oracle Attacks on Cryptographic Hardware [Crypto 2012]

様々な暗号機器の暗号化された鍵を取り入れる機能を利用して、取り入れた鍵を暴く方法を示す。攻撃はパディングオラクル攻撃であり、不正にパディングされた平文に対するエラーメッセージをサイドチャネル情報として使用する。非対称暗号の場合、Bleichenbacher の RSA PKCS#1 v1.5 に対するパディングを改良し、「百万メッセージ攻撃」を平均 49,000 回(中間値 14500 回)のオラクル呼び出しで実現し、1,024 ビット鍵

による未知の正当な暗号文を解読した。元のアルゴリズムでは平均 215,000 回(中間値 163,000 回)のオラクル呼び出しが必要であった。ある特定の機器の場合には、平均 9,400 回(中間値 3,800 回)の操作しか必要としない実装の詳細を示す。対称鍵暗号の場合には、既に非常に効率的である Vaudenay の CBC 攻撃を取り上げる。セキュリティトークン、スマートカード、エストニア電子 ID カード等を含む多くの商用暗号機器の脆弱性を示す。攻撃は十分に効率的であり、実際に行うことができる。脆弱であるとわかったすべての機器に対する実行時間を与え、我々の最適化によってどの程度現実的になるかを示す。また、攻撃の有効性の数学的解析、広範囲にわたる実験結果、対策に関する議論も示す。

・Improving the Complexity of Index Calculus Algorithms in Elliptic Curves over Binary Fields [Eurocrypt 2012]

標数 2 の拡大体上の楕円曲線離散対数問題に対する decomposition 攻撃法の改良。Semaev とそれに続く Gaudry, Diem らの方法に更なる制約条件を付加し、多変数多項式系に問題を帰着し、グレブナ基底を求めることにより問題を解く。あるヒューリスティックを仮定すれば、計算量は $O(2^{\omega n/2})$ と見積もられる。

講演中、準指数時間解読の噂に触れ、まだ指数時間であり、結論を急ぐべきではないと釘を刺す見解が述べられた。

3.2.5.その他の解読技術

・Cryptanalyses on a Merkle-Damgard Based MAC --- Almost Universal Forgery and Distinguishing-H Attacks [Eurocrypt 2012]

本論文は、Merkle-Damgard ハッシュに基づいたメッセージ認証子(MAC: Message Authentication Code)に対する 2 種類の解析を示す。Merkle-Damgard MAC とは、メッセージを M、メッセージ長を l、共有鍵を K としたときに、Hash(K||l||M)により MAC 値を計算するものである。この構成は、しばしば、LPMAC と呼ばれる。

初めに、任意の狭いパイプの Merkle-Damgard ハッシュに基づいた LPMAC に対する $O((2^{n/2})$問合せの H-識別攻撃を示す。このことは安全なハッシュ関数による LPMAC は H-識別攻撃に対して、2^n問合せまで耐性を持つという広く信じられている仮説が正しくないことを示している。実際、既存のすべての H-識別攻撃は、基づくハッシュアルゴリズムに対する専用攻撃を考えており、ほとんどの場合において、縮退段数で $2^{n/2}$ から 2^nの間の計算量で攻撃されていた。我々の攻撃は、一般的に機能するため、これらの結果を更新するものである。即ち、完全な段数が $O((2^{n/2})$で攻撃される。

次に、LPMAC に対してより強力な攻撃、即ち、ほぼ万能な偽造攻撃(almost universal forgery attack)の強い形の攻撃が実行可能であることを示す。この設定では、攻撃者

は与えられたメッセージの初めのいくつかのメッセージブロックを変更することができ、内部状態を解読し、MAC 値を偽造しようとする。任意の狭いパイプの Merkle-Damgard ハッシュ関数に対し、$O(2^{n/2})$回の問合せで攻撃を実行できる。

これらの結果は、安全な MAC を実現するには、長さを前に追加するスキームは十分でないことを示している。

3.3 暗号技術調査ワーキンググループ開催状況

2012 年度は、各ワーキンググループ（WG）が活動した主要活動項目は、表 3.2 の通りである。

表 3.2　2012 年度の主要活動項目

WG 名	主査	主要活動項目
リストガイド WG	手塚 悟	2011 年度リストガイド WG の活動を通して抽出された課題の中から，導出関数（KDF）に関する安全性の検討、一般的な暗号プロトコルに関する調査及びリストガイドの利用促進に係る検討を行った。
計算機能力評価 WG	高木 剛	2011 年度に調査を行った素因数分解問題の困難性に加え、離散対数問題の困難性の見積りについても同様な予測が可能かどうかの検討を行った。また、素因数分解問題や離散対数問題の他にも、暗号技術で利用される数学的な問題に関しても同様な検討を行った。

3.4. 委員会開催記録

2011 年度、暗号方式委員会は、表 3.3 の通り 2 回開催された。暗号技術調査ワーキンググループは、表 3.4 及び表 3.5 の通り計 4 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。

(1)　暗号方式委員会

表 3.3　暗号方式委員会の開催

回	年月日	議題
第 1 回	2012 年 6 月 8 日	暗号方式委員会活動計画の検討、暗号技術調査ワーキンググループ活動計画の検討、安全性に関する次期リスト作成方針の検討、外部評価についての検討、監視状況報告
第 2 回	2012 年 7 月 24 日	技術的アピールポイントについての検討、評価 B 及び総合評価についての検討、安全性に関する推奨候補暗号と運用監視暗号の分類についての検討

第 3 回	2012 年 10 月 9 日	推奨候補暗号と運用監視暗号の分類についての検討、評価 B 対象アルゴリズムの判定についての検討、安全性に関する仕様上のアドバンテージについての検討
第 4 回	2013 年 3 月 5 日	外部評価報告、暗号技術調査 WG に関する活動報告、監視状況報告、次年度の課題についての検討

(2) 暗号技術調査ワーキンググループ

表 3.4　暗号技術調査ワーキンググループ(リストガイド)の開催

回	年月日	議題
第 1 回	2012 年 8 月 29 日	・リストガイド WG 2012 年度活動方針について ・暗号技術調査 WG の運営等 ・リストガイド WG の進め方について ・IETF における暗号関連動向
第 2 回	2012 年 12 月 20 日	・KDF に関する調査 - ISO における KDF の検討状況について - KDF の分類・安全性について ・一般的な暗号プロトコルに関する調査 - SRP の安全性について - DNSSEC の鍵管理にかかわる課題について ・リストガイドの利用促進にかかわる検討
第 3 回	2013 年 2 月 25 日	・一般的な暗号プロトコルに関する調査 - PSK の安全性について ・リストガイド WG 活動報告（案）について

表 3.5　暗号技術調査ワーキンググループ(計算機能力評価)の開催

回	年月日	議題
第 1 回	2012 年 12 月 21 日	活動計画や作業内容についての審議と了承 -離散対数問題の困難性に関する調査 -格子問題の困難性に関する調査
第 2 回	2013 年 2 月 22 日	報告内容についての審議と了承 -2012 年度の予測図の更新 -離散対数問題の困難性に関する調査 -素因数分解・離散対数問題以外の数学的問題の困難性を利用した暗号技術の調査

第4章 暗号技術調査ワーキンググループ

4.1.リストガイドワーキンググループ

4.1.1.活動目的

2011 年度リストガイド WG の活動を通して抽出された課題の中から，導出関数（KDF）に関する安全性の検討、一般的な暗号プロトコルに関する調査及びリストガイドの利用促進に係る検討を行った。

4.1.2.委員構成(敬称略，五十音順)

主査：手塚 悟（東京工科大学　教授）
委員：岡崎 博之（日本電気株式会社　事業部長代理）
委員：菅野 哲（NTT ソフトウェア株式会社　主任エンジニア補）
委員：清本 晋作（株式会社 KDDI 研究所　主任研究員）
委員：佐野 文彦（東芝ソリューション株式会社　研究主務）
委員：花岡 悟一郎（独立行政法人産業技術総合研究所　研究チーム長）
委員：藤城 孝宏（株式会社日立製作所　部長）
委員：松尾 真一郎（独立行政法人情報通信研究機構　研究室長）
委員：民田 雅人（株式会社日本レジストリサービス　主任研究員）
委員：渡辺 大（株式会社日立製作所　主任研究員）

4.1.3.活動方針

本年度は、鍵導出関数（KDF）に関する安全性の検討、一般的な暗号プロトコルに関する調査及びリストガイドの利用促進に係る検討を行った。具体的な検討項目は以下である。

(1)　鍵導出関数（KDF）に関する調査

平成 23 年度に作成したリストガイド「電子政府推奨暗号:鍵共有」の検討過程において、補助関数として利用する鍵導出関数(KDF)が未検討となっていた。KDF については 2007 年度に暗号技術調査 WG において検討を行っているが、検討後 4 年が経過したことから、安全性評価に関する現状の調査として安全性要件の検討及び能動的攻撃に対する評価を行う。

(2)一般的な暗号プロトコルに関する調査

IETF (Internet Engineering Task Force)において「SSL/TLS」及び「IPsec」に関連したRFC (Request For Comments)の追加が検討されており、その動向を踏まえ適宜リストガイドに反映していく必要があることから標準化動向の調査を行う。「DNSSEC」については、鍵更新を含む鍵管理の検討を行うための事前調査として、実運用面からの課題の整理を行う。

(3)リストガイドの利用促進に係る検討

リストガイドについては、これまで複数年にわたる活動を通してコンテンツが作成されているが、利用促進に課題が残ることから、その利用促進策について検討を行う。

4.1.4.活動概要

本年度は3回のWGを開催した。

第1回WG（2012年8月29日）では、 2012年度活動方針について議論を行った。今年度のWGでは、(1) KDFに関する調査、(2) 一般的な暗号プロトコルに関する調査、(3)リストガイドの利用促進に係る検討を実施することとした。

表 1　2012年度暗号技術調査WG（リストガイド）検討項目

検討項目	検討項目
KDFに関する調査	・　電子政府推奨暗号として指定される仕様書に記載されるKDFを中心に、将来に安全性評価を行うための調査・検討を行う ・　今後CRYPTRECにおける評価上の課題について検討する
一般的な暗号プロトコルに関する調査	・　IETFにおいて、SSL/TLS、IPsecの暗号スイートの標準化動向の調査と昨年度残課題の検討を行う ・　DNSSECにおける運用面での鍵管理の課題整理を行う
リストガイドの利用促進に係る検討	・　利用者視点からリストガイドに記載すべきコンテンツや記載レベル、公開形態について検討を行う

(1) KDFに関する調査

- KDFに関する安全性要件の検討：2008年度以降に発行されたNIST SP800の追加文書に関する調査を実施し、KDFの安全性要件を検討した。その結果、基本的にKDFの出力生成にはハッシュ関数もしくはMACが用いられているため、KDFの安全性として独自に検討すべき事項はないこと及び暗号アルゴリズムが危殆化した場合に、影

響を受ける可能性があるとの結論に達した。また、ハッシュ関数を直接用いる場合、ハッシュ関数に求められる安全性要件は一方向性と出力の一様ランダム性であり、衝突困難性は不要であることが指摘されていることを確認した。

- 能動的攻撃に対する KDF の評価を行い、下表に示す結果を得た。

表 2　能動的攻撃に対する KDF の評価

仕様	評価結果
NIST SP800 56A, 56B, 56C	Other Info の各フィールドが固定長であれば問題ない
NIST SP800 108	同上
NIST SP800 132	基本的に問題はないが、Salt の作り方において、任意入力を許容（S=purpose||rv）しており、注意が必要（KDF の仕様対象外の可能性あり）
NIST SP800 135rev1	SRTP の仕様に問題あり
SEC1	問題なし
ANSI X9.42-2003	問題なし
PSEC-KEM	問題なし

(2)一般的な暗号プロトコルに関する調査

一般的な暗号プロトコルに関する調査として，IETF のセキュアプロトコル（tls、ipsecme 等）における暗号技術及び電子政府推奨暗号リストに掲載されている暗号技術の標準化動向等，SRP，DNSSEC，PSK について調査を行った。具体的には以下の通りである。

- IETF のセキュアプロトコル（tls、ipsecme 等）における暗号技術及び電子政府推奨暗号リストに掲載されている暗号技術の標準化動向等についての調査：
  - セキュアプロトコル関係：この数年以内に RFC 化され，暗号利用に影響を与えそうな仕様の確認を行い、暗号技術が利用される分野が広がりつつあり、監視が必要になる可能性もあるとの結論に達した。
  - 調査した I-D(インターネットドラフト)は以下の通り
    - tls：Secure Password Ciphersuites for Transport Layer Security (TLS), Standards Track 等、3 トラック
    - ipsecme： More Raw Public Keys for IKEv2, Informational 等、2 トラック
    - その他：kerberos、jose、dnsext、sidr、karp 等
  - 電子政府推奨暗号関係：現在，標準化が行われているドラフト文書に関する状況について確認を行った。また、大半のドラフト文書は提案者によって執筆さ

れており、米国系暗号アルゴリズム以外の標準化活動が困難な状況になりつつあるなどの状況が明らかになった。

- 調査した I-D(インターネットドラフト)は以下の通り
  - Camellia：Camellia Encryption for Kerberos 5, Standards Track 等、8 トラック
  - CLEFIA：CLEFIA Cipher Suites for Transport Layer Security (TLS), Informational 等、3 トラック
  - KCipher-2：Use of KCipher-2 in Transport Layer Security, Standard 等、3 トラック

■ SRP に関する調査：

- SRP の標準化動向：IETF における SRP の位置づけについて、以下の RFC について調査を実施。
  - RFC2944 Telnet Authentication: SRP
  - RFC2945 The SRP Authentication and Key Exchange System (SRP-3)
  - RFC3720 Internet Small Computer Systems Interface (iSCSI)
  - RFC3723 Securing Block Storage Protocols over IP
  - RFC3669 Guidelines for Working Groups on Intellectual Property Issues
  - RFC5054 Using the Secure Remote Password (SRP) Protocol for TLS Authentication
- SRP の安全性：SRP の安全性について評価を実施し以下の結果を得た。
  - 証明可能安全性のフレームワークにおける安全性証明はない
  - RFC における Security Consideration の記述
    - 鍵確認は必須である
    - セキュリティパラメータは十分に大きくする
    - パスワード推測を防ぐため、試行回数を制限する
    - SHA-1 の現状の衝突はプロトコル安全性への影響は少ないが、他の脆弱性が出てきたときには使わないようにすべき
  - SRP 自体のセキュリティについては、継続調査が必要
  - TLS の Cipher Suite において、暗号化部分で電子政府推奨暗号リストに掲載されていないアルゴリズムの扱いを検証する必要がある

■ DNSSEC に関する調査：

- DNSSEC の普及状況：79 の TLD(Top Level Domain)で DNSSEC 運用(DS レコードをルートゾーンに登録済)が行われている。

- DNSSEC 運用におけるリスク：
  - 鍵や署名、手順を誤れば、正規のリソースレコードであっても署名検証に失敗し、不正な情報として扱われる。
  - DNSSEC の運用において、「失敗が許されない運用」が要求される。

■ PSK に関する調査：

- TLS-PSK の利用状況：ほとんど利用されていない状況
  - RFC 4279 における利用用途の記載
    - PKI を使用したくない場合に適用可能
    - 省リソースであることが利点
  - OpenSSL 1.0.1 では，normal PSK のみ実装されている（現在は TLS と DTLS でサポート）
  - GnuTLS では、normal PSK / DHE_PSK / ECDHE_PSK が実装されている（RSA_PSK が未実装）
- TLS-PSK の鍵共有方式に関する安全性:PSK の安全性について評価を実施し以下の結果を得た。
  - 安全と考えられる方式（事前共有鍵が十分に大きい前提）
    - normal PSK：適切な暗号アルゴリズムとの組み合わせを用いる場合
    - RSA_PSK：適切な暗号アルゴリズムとの組み合わせを用いる場合。ただし、公開鍵証明書を参照するため、PSK の利点が小さいこともあり、openssl や GnuTLS では実装されていない
  - 取り扱いを検討すべき方式
    - DHE_PSK および ECDHE_PSK：ephemeral な DH および ECDH パラメータを署名なしに使用しており、中間者攻撃が可能であるため

(3)リストガイドの利用促進に関わる検討

(a)リストガイドに関するニーズと課題の整理

利用者視点からリストガイドに関する意見を収集するとともに、次年度以降の CRYPTREC におけるガイド文書の作成及び運営の指針を策定する上での提言をまとめた。具体的には以下の通り。

■ ニーズ調査：委員へのヒアリングを行い、以下のような意見を得た。

- 内容が専門的すぎるため、想定読者を明確化するとともに一般的な用語の整理を行い、平易な内容・構成とすることが望ましい。
- 技術解説よりも、電子政府で利用可能な暗号スイートやパラメータ等を一覧化して提示することが望ましい。
- SSL/TLS 等の代表的なソフトウェアについて、具体的な設定内容などを例示す

ることが望ましい。

■ CRYPTREC の情報提供体制に関する課題：注意喚起やリストガイドの内容や範囲を再検討するとともに、迅速に情報提供を行うことができる体制の構築について課題が提起された。

- ➢ 既存リストガイドの位置づけ
  - ✧ 現状のリストガイドには暗号実装、推奨セキュリティパラメータ、運用・鍵管理、テクニカルレポート等に関する内容が混在している
  - ✧ 想定読者がリストガイド毎に異なるため、読者がどのリストガイドを読むべきか分かりにくい
- ➢ リストガイドの情報提供体制
  - ✧ リストガイドの内容や範囲を再検討するとともに、迅速に情報提供を行うことができる体制の構築
- ➢ 情報提供機能の強化
  - ✧ リストガイドの認知度向上施策の検討

(b)将来に向けた展望

上記の課題に対して，リストガイドの利用促進への考えられる方策を，将来に向けた展望として提言した

■ リストガイドの名称変更

- ➢ リストガイドの名称：より広範な読者の獲得等を勘案し、文書のタイトルを以下の通り修正する。
  - ✧ CRYPTREC 暗号技術利用ガイド
- ➢ 目的の拡大：民間での利用を妨げない旨を追記する。具体的には以下の通りとする。
  - ✧ CRYPTREC 暗号技術利用ガイドは、電子政府のシステム調達者及び電子政府システムを構築する開発者に向けて、電子政府推奨暗号を利用する際に必要となる情報並びに推奨を示すものである。なお、電子政府以外の目的に用いることを妨げるものではない。

■ リストガイドの分類

- ➢ ニーズ調査を踏まえ、以下の三種類のドキュメントとして整理してはどうか
  - ✧ CRYPTREC 暗号技術利用ガイド
    - ● 従来のリストガイドのうち､暗号実装､推奨セキュリティパラメータ、運用・鍵管理について記述したもの
  - ✧ CRYPTREC テクニカルレポート
    - ● 利用ガイドの理論的・専門的な裏付けを述べたもの。

- 利用ガイドには掲載されない先進的な暗号技術等の動向や技術をとりまとめたもの。

✧ CRYPTREC 注意喚起レポート

- 暗号やプロトコルの監視活動において早急に対策を要する事項が発生した場合に、技術的な側面から妥当性を検討したもの。

■ CRYPTREC 暗号技術利用ガイドの分類

➢ CRYPTREC 暗号技術利用ガイドを以下の 3 つのカテゴリに分類し、記載内容を整理することで、想定読者に適合した内容としてはどうか

✧ カテゴリ A　暗号実装：実装仕様、耐サイドチャネル実装等について記述したもの。システム発注者・構築者を想定読者とする。

✧ カテゴリ B　推奨セキュリティパラメータ：暗号技術・プロトコルにおける、パラメータ、ドメインパラメータ等について記述したもの。システム発注者・構築者を想定読者とする。

✧ カテゴリ C　運用・鍵管理：運用・鍵管理他について記述したもの。システム運用者を想定読者とする。

■ 文書番号体系の確立

➢ リストガイドを参照しやすくするため、統一的な番号体系を採用し文書番号を付与する。

✧ ＜文書番号＞::=＜略称＞”-”＜カテゴリ＞”-”＜連番＞

✧ 例：「CUG-A-003」

➢ 一度付与された連番は，文書の改訂では変更しない

➢ 改訂における考え方

✧ 改訂年度などの情報を入れる（ISO 方式）⇒　例：CUG-A-003-2013

✧ バージョンを文書に付与する（NIST SP800 方式）⇒　例：CUG-A-003 Rev.1

■ CRYPTREC 暗号リスト改定に伴う修正

➢ CRYPTREC 暗号リストの改訂に伴い、これまでに作成したリストガイドを修正する

✧ 新しい体系（電子政府推奨暗号リスト、推奨候補暗号リスト、運用監視暗号リスト）に対応した内容の追記

■ 情報提供機能の強化

➢ リストガイドの利用促進のため、リストガイドを掲載する HP を再整理する必要がある

➢ リストガイド公開等のタイミングで、想定ユーザである各府省庁並びにベンダ等に向けて告知を行い、認知度を向上させる必要がある

4.2.計算機能力評価ワーキンググループ

4.2.1.活動目的

公開鍵暗号の安全性は、素因数分解問題の困難性や離散対数問題(有限体あるいは楕円曲線)等の困難性などさまざまな数学的問題に依存している。2011 年度までに行った素因数分解問題の困難性に関する調査研究に基づいて RSA1024 ビットの危殆化に関する見積りが作成された。離散対数問題の困難性の見積りについても同様な予測が可能かどうかの検討が必要である。
また、素因数分解問題や離散対数問題以外にも、暗号技術で利用される数学的な問題に関しても同様な検討を行う。

4.2.2.委員構成

主査：高木 剛(九州大学)
委員：青木 和麻呂(NTT)
委員：太田 和夫(電気通信大学)
委員：國廣 昇(東京大学)
委員：下山 武司(富士通研究所)

4.2.3.活動方針

(1)離散対数問題の困難性に関する調査

有限体上の離散対数問題、及び、楕円曲線上の離散対数問題の困難性に関する調査を行う。離散対数問題の困難性に関する見積りを作成できるかどうかの検討を行い、可能であれば作成する。

(2)格子問題の困難性に関する調査

暗号技術で利用される数学的な問題、特に今年度については、格子に係る数学的な問題の困難性について調査を行う。また、素因数分解問題や離散対数問題と同様な検討が可能かどうかの審議も行う。

4.2.4.活動概要

(1)スケジュール

第1回　2012年12月21日　　活動計画や作業内容についての審議と了承
第2回　2013年2月22日　　報告内容についての審議と了承

(2)素因数分解問題に関する予測図の更新

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[1]において、2012年6月・11月のベンチマーク結果が追加されたので、「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」に関する図を更新した。

(3)離散対数問題の困難性について

現在のところ、楕円曲線上の離散対数問題を解くための最速アルゴリズムは、ポラード(Pollard)のρ(ロー)法である。下山委員が論文[2]に従って、楕円曲線上の離散対数問題の計算量評価方法について解説を行った。

(4)格子問題の困難性について

格子問題の他にもよく利用されている問題として、NP 困難に係る問題、多変数多項式に係る問題、符号理論に係る問題なども調査する必要があるとの意見があったため、

① Learning with error (LWE)
② Learning parity with noise (LPN)
③ Approximate GCD(AGCD)
④ Subset-Sum (SS)
⑤ Multivariate Quadratic(MQ)問題

にまで対象を広げて、これらをベースとする公開鍵暗号（守秘）に関する論文をリストアップした。

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

[2] M. Yasuda, T. Shimoyama, J. Kogure, and T. Izu, “On the Strength Comparison of the ECDLP and the IFP,” SCN 2012, LNCS 7485, pp.302-325, Springer 2012.

4.2.5. 検討内容

(1) 素因数分解問題に関する予測図の更新

「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 1 の通りとなる。

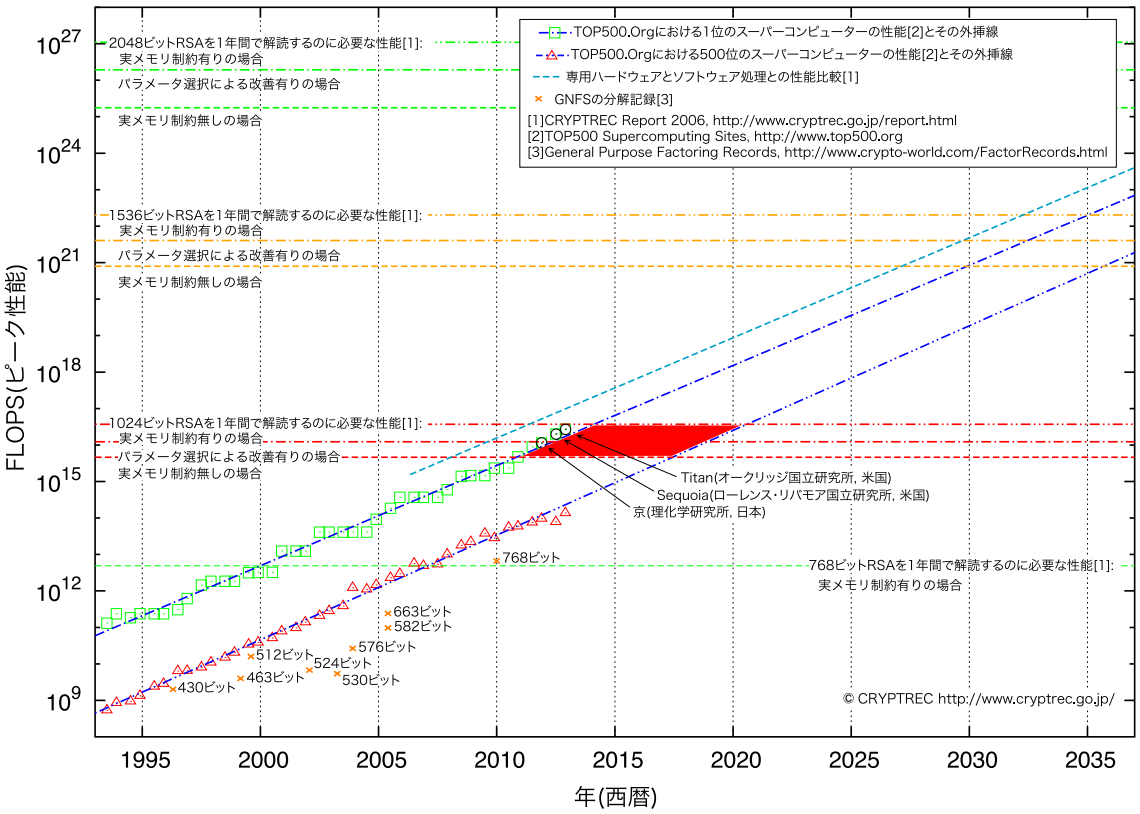


図 1：1 年間でふるい処理を完了するのに要求される処理能力の予測(2013 年 2 月更新)

(2) 離散対数問題の困難性について

上記の論文に記載された評価式

$$T_{ECDLP} = \begin{cases} 3\cdot\sqrt{\pi 2^N}/2 \times \dfrac{270.05}{4}\cdot\left(\left\lceil \dfrac{N}{64}\right\rceil\right)^2 \Big/ Y & (\text{prime field case}, 64 \le N \le 256), \\ 3\cdot\sqrt{\pi 2^N}/2 \times 388.48\cdot\left(N/131\right)^{1.585} / Y & (\text{binary field case}), \\ 3\cdot\sqrt{\pi 2^N/N}/2 \times 388.48\cdot\left(N/131\right)^{1.585} / Y & (\text{Koblitz curve case}), \end{cases}$$

where $Y = 365\cdot 24\cdot 60\cdot 60(\text{seconds})$ and $n = 2^N$ as the order of the point S.

から得られる数値を、素因数分解に関する予測図に倣って図に表すと図 2 の通りとなる。

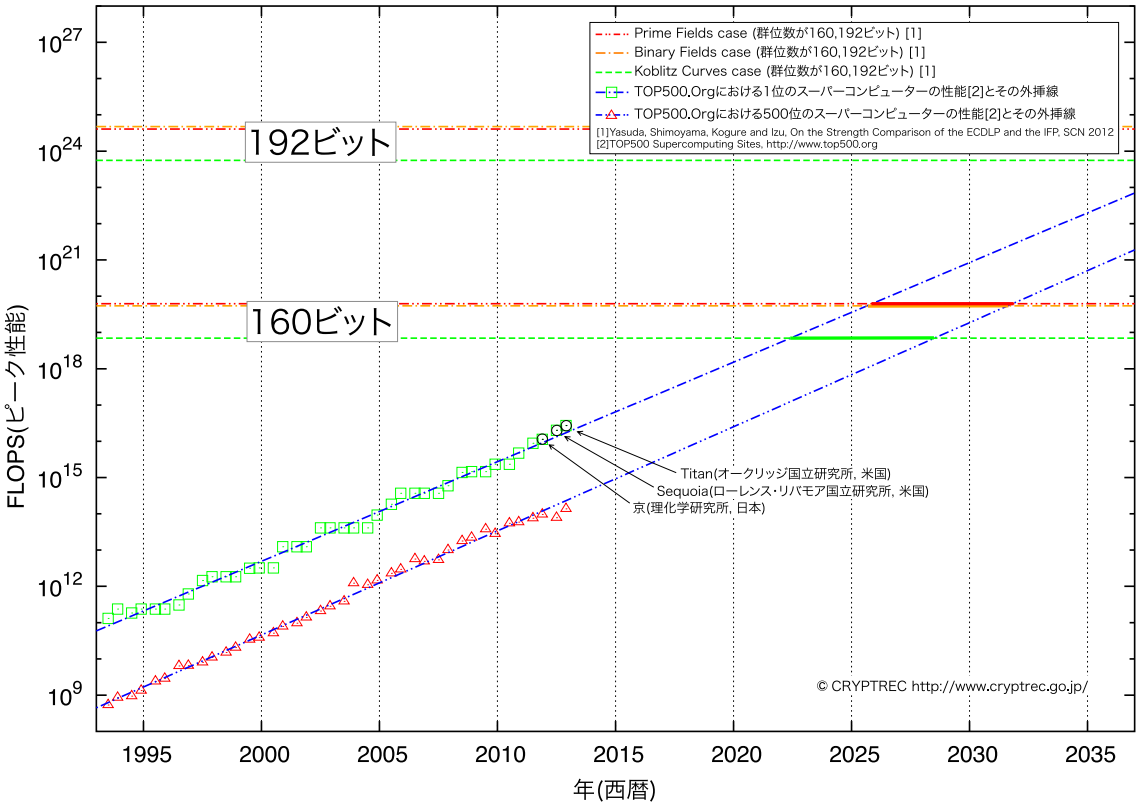


図 2： ρ 法で ECDLP を 1 年で解くのに要求される処理能力の予測(2013 年 2 月)

なお、今年度に入って、グレブナ基底を利用した ECDLP に対する指数計算法の高速化手法：

J. Faugère, L. Perret, C. Petit, and G. Renault,

“Improving the Complexity of Index Calculus Algorithms in Elliptic Curves over Binary Fields,” Eurocrypt 2012, LNCS 7237, pp. 27-44, Springer 2012.

や、ECDLP に対する指数計算法の新たな評価：

C. Petit and J. Quisquater

“On Polynomial Systems Arising from a Weil Descent,” Asiacrypt 2012, LNCS 7658, pp. 451-466, Springer 2012.

が提案され、新たな進展が見られる。今後、これらの研究動向には注意が必要である。

(3)格子問題の困難性について

①～⑤の数学的問題に係る公開鍵暗号(守秘)に関する代表的な論文をリストアップした。その結果は下記の参考文献の通りである。

① Learning with error (LWE)
② Learning parity with noise (LPN)
③ Approximate GCD(AGCD)
④ Subset-Sum (SS)
⑤ Multivariate Quadratic(MQ)問題

数学的問題	暗号技術
LWE 問題	[1][2][3][4]
LPN 問題	[5][6][7][8][9]
AGCD 問題	[10][11]
SS 問題	[12]
MQ 問題	[13]

下記に参考文献として例示する論文リストを記載する。CRYPTREC Report 2012 では各論文に対して簡単な概要を掲載する予定である。

今後は、これらの数学的問題におけるパラメータ選択とセキュリティレベルの関係に関する調査を行う予定である。

【調査対象予定の論文リスト】

[1]Oded Regev: New lattice-based cryptographic constructions. J. ACM 51(6): 899-942 (2004)

[2]Oded Regev: On lattices, learning with errors, random linear codes, and cryptography. STOC 2005: 84-93

[3]Zvika Brakerski, Vinod Vaikuntanathan: Efficient Fully Homomorphic Encryption from (Standard) LWE. FOCS 2011: 97-106

[4]Richard Lindner, Chris Peikert: Better Key Sizes (and Attacks) for LWE-Based Encryption. CT-RSA 2011: 319-339

[5]Ivan Damgård, *Sunoo Park:* Is Public-Key Encryption Based on LPN Practical?, Cryptology ePrint Archiveeprint 2012/699.

[6]Nico Döttling, Jörn Müller-Quade, Anderson C. A. Nascimento: IND-CCA Secure Cryptography Based on a Variant of the LPN Problem. ASIACRYPT 2012: 485-503

[7]Michael Alekhnovich: More on Average Case vs Approximation Complexity. FOCS 2003: 298-307

[8]McEliece R.J.: A public-key cryptosystem based on algebraic coding theory. Deep Space Network Prog. Rep. (1978).
[9] Nico Döttling, Rafael Dowsley, Jörn Müller-Quade, Anderson C. A. Nascimento: A CCA2 Secure Variant of the McEliece Cryptosystem. IEEE Transactions on Information Theory 58(10): 6672-6680 (2012)
[10]Jean-Sébastien Coron, Avradip Mandal, David Naccache, Mehdi Tibouchi: Fully Homomorphic Encryption over the Integers with Shorter Public Keys. CRYPTO 2011: 487-504
[11]Marten van Dijk, Craig Gentry, Shai Halevi, Vinod Vaikuntanathan: Fully Homomorphic Encryption over the Integers.
[12]Vadim Lyubashevsky, Adriana Palacio, Gil Segev: Public-Key Cryptographic Primitives Provably as Secure as Subset Sum. TCC 2010: 382-400
[13]Yun-Ju Huang, Feng-Hao Liu, Bo-Yin Yang: Public-Key Cryptography from New Multivariate Quadratic Assumptions. Public Key Cryptography 2012: 190-205
[14]Yuanmi Chen, Phong Q. Nguyen: Faster Algorithms for Approximate Common Divisors: Breaking Fully-Homomorphic-Encryption Challenges over the Integers. EUROCRYPT 2012: 502-519

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		該当なし
暗号利用モード	秘匿モード	該当なし
	認証付き秘匿モード	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。

[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） 128-bit RC4 は、SSL （TLS 1.0 以上）に限定して利用すること。

（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。

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 186-2 (+ Change Notice) (January 2000, Change Notice 1 は October 2001), Digital Signature Standard (DSS) で規定されたもの。 ・ 参照 URL <http://csrc.nist.gov/publications/fips/archive/fips186-2/fips186-2.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
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：soft-crypto-ml@ml.css.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/> 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	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.2.1) ・参照 URL <http://www.rsa.com/rsalabs/node.asp?id=2124> 和文： なし 英文： http://www.rsa.com/rsalabs/node.asp?id=2005
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 第二営業部 部長 齊藤 賢一 TEL：03-6830-3341, FAX：03-5308-8979, E-MAIL：kenichi.saito@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.2.1) ・参照 URL <http://www.rsa.com/rsalabs/node.asp?id=2124> 和文：　なし 英文：　http://www.rsa.com/rsalabs/node.asp?id=2125
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　第二営業部　部長　齊藤 賢一 TEL：03-6830-3341, FAX：03-5308-8979, E-MAIL：kenichi.saito@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.2.1) ・参照 URL <http://www.rsa.com/rsalabs/node.asp?id=2124> 和文：　なし 英文：　http://www.rsa.com/rsalabs/node.asp?id=2146
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　第二営業部　部長　齊藤 賢一 TEL：03-6830-3341, FAX：03-5308-8979, E-MAIL：kenichi.saito@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/>　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。
関連情報 2	仕様 ・NIST Special Publication 800-56A (March 2007), Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised) 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
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：soft-crypto-ml@ml.css.fujitsu.com
関連情報 2	仕様 ・NIST Special Publication SP 800-56A (March 2007), Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised) 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, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, May 2004. ・ 参照 URL[1] <http://csrc.nist.gov/publications/nistpubs/800-67/SP800-67.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:0422-59-3885 E-MAIL:camellia@lab.ntt.co.jp

[1] 付録 5 に記載の通り、2005 年度まで参照先として挙げていた仕様書は下記にある。
http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

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 研究マネージャー　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 180-2, Specifications for the Secure Hash Standard (SHS) ・　参照 URL <http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.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/publication/fips/fips198-1/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 signa- ture 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/advancedpack/
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　システムソフトウェア事業部 セキュリティ G E-MAIL:secsol@itpfs.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:044-549-2067, FAX:044-549-1841 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	〒100-8310 東京都千代田区丸の内 2-7-3（東京ビル） 三菱電機株式会社　インフォメーションシステム事業推進本部 連携事業推進センター　DIGUARD 事業グループマネージャー　米田 健 TEL：03-3218-3221　　FAX：03-3218-3638 E-MAIL：Yoneda.Takeshi@ak.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/advancedpack/
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　システムソフトウェア事業部 セキュリティ G E-MAIL: secsol@itpfs.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	〒141-8610 東京都品川区大崎 2-10-1 ソニーシティ大崎 ソニー株式会社 SSPF ソフトウェア設計技術センター セキュリティ＆テスト技術推進部 堅木 雅宣 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:044-549-2067, FAX:044-549-1841 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： soft-crypto-ml@ml.css.fujitsu.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　横浜研究所　エンタープライズシステム研究部 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	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　情報・通信システム社 IT プラットフォーム事業本部　開発統括本部 主管技師長　松永 和男 TEL：045-862-8498,　FAX：050-3139-8348 E-MAIL：kazuo.matsunaga.bz@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　情報・通信システム社 IT プラットフォーム事業本部　開発統括本部　主管技師長　松永 和男 TEL：045-862-8498,　FAX：050-3139-8348 E-MAIL： kazuo.matsunaga.bz@hitachi.com

3. メッセージ認証コード

暗号名	PC-MAC-AES
関連情報	公開ホームページ 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　クラウドシステム研究所　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

4. 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.2.1) ・参照 URL <http://www.rsa.com/rsalabs/node.asp?id=2125>
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　第二営業部　部長　齊藤 賢一 TEL：03-6830-3341, FAX：03-5308-8979, E-MAIL：kenichi.saito@rsa.com

2. 共通鍵暗号

暗号名	RC4
関連情報	仕様 ・問い合わせ先 EMC ジャパン株式会社 RSA 事業本部(http://japan.rsa.com) ・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.rsa.com/rsalabs/node.asp?id=2149>

3. ハッシュ関数

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

暗号名	SHA-1
関連情報	仕様 ・FIPS PUB 180-2, Specifications for the Secure Hash Standard (SHS) ・　参照 URL <http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.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

平成 24 年 7 月 26 日
CRYPTREC 暗号方式委員会委員長
CRYPTREC 暗号実装委員会委員長
CRYPTREC 暗号運用委員会委員長

CRYPTREC 暗号技術応募者 各位

日頃より CRYPTREC の活動にご理解とご協力を賜り、感謝申し上げます。

この度、CRYPTREC では、評価対象の暗号技術が安全性及び実装性能に関し、同じカテゴリの暗号技術等と比べてどのような技術的アドバンテージを持つかを評価することとなりました。
つきましては、各暗号技術の技術的アピールポイント及び論文リストを下記の通りご提出頂きたく、よろしくお願い申し上げます。ご提出いただいた回答を基に、評価をいたします。第 1 次選定を通過した暗号技術に関しては、総合評価でも技術的アピールポイントを使用いたします。必ず、ご提出ください。なお、回答の内容に関しては、CRYPTREC Report 等に記載することがあります。

安全性 （暗号方式委員会担当）

- 安全性に関する仕様上のアドバンテージ
  下記の該当するポイントを含めて A4 サイズ 1 枚以内にまとめてご提出下さい。
  - 証明可能安全性の有無や安全性評価の容易性
  - 安全性証明における仮定の妥当性
  - 安全性証明の帰着効率
  - 鍵の全数探索等よりも効率のよい攻撃の有無
  - 安全性マージン（現時点での最長攻撃可能段数）
  - 安全性に関連する利用上の制限の有無
  - 提案論文が採録された国際会議・論文誌
- 応募暗号技術の安全性評価に関して、これまで論文誌または査読付き国際会議で発表されている論文のリスト
  但し、対象は 2012 年 9 月 14 日時点で出版されている論文とします。
  なお、査読付き国際会議の論文については、Springer Lecture Notes in Computer Science, IEEE, ACM のいずれかから出版されている論文とします。

実装性能 （暗号実装委員会担当）

- 実装性能に関するアドバンテージ

ソフトウェア実装及びハードウェア実装の性能において、次に挙げる項目で標準的な暗号技術より優れている点があれば、A4 サイズ１枚以内にまとめるとともに、それを示す公知のデータ（文献等）のリストを作成し、ご提出下さい。なお、標準的な暗号技術とは、実際の利用において暗号技術を選択する際に競合する範囲にあり、かつ、最も広く使用されているものとします。競合する範囲としては、基本的には暗号技術の同じカテゴリ（64 ビットブロック暗号等）を想定していますが、同じカテゴリ内に標準的な暗号技術がないなどの場合は、適宜範囲を拡大して解釈して下さい。

比較対象として選択した暗号技術が標準的か否か、及び、ご提出頂いた公知のデータの信頼性については暗号実装委員会で判断致します。

- 初期化時間（鍵設定、IV 設定）
- スループット（暗号化、署名生成等）
- 実装サイズ（仕様リソース量、プログラムサイズ等）
- クリティカルパス遅延、消費電力、回路効率等（ハードウェア実装の場合）

提出期限：９月１４日(金)１６時

提出方法：本依頼状添付の回答フォーマットにご記入の上、電子メール添付にて
info@cryptrec.go.jp 宛にお送り下さい。

問い合わせ先：info@cryptrec.go.jp

短い実施期間となりますが、ご協力のほど、よろしくお願いいたします。

（参考）調査の背景

「暗号技術検討会 2011 年度報告書」
http://www.cryptrec.go.jp/report/c11_kentou_final_r2.pdf

2011 年度の暗号技術検討会において、「電子政府推奨暗号選定のための選考基準案の考え方」が承認されました。概要は、上記報告書 P20 の「図 4.1 選定ルールのフレームワーク」に示す通りで、４つの太枠（赤、紺、緑、黄）で囲まれた四角において暗号技術の評価が行われます。

「安全性評価／実装評価」(赤) の結果、推奨候補暗号リストに入った暗号技術のうち、【評価Ａ】（紺）で利用実績が十分でないと判定された暗号技術は、今後の利用促進の可能性が高いかどうかを判断する【評価Ｂ】（緑）の評価対象となります。今回調査する技術的アピールポイントは、【評価Ｂ】における選考基準の一つとなっています。すなわち、上記報告書 P22 の表 4.3 の「標準化・規格化の促進を図るハードルの低さ」を判定する際の項目の一つで、「安全性」または「実装性能」において、「市場が認める程度の技術的アドバンテージがある」かどうかを評価いたします。また、今回の調査内容は、「総合評価」（黄）でも利用する可能性があります。

暗号技術名：
安全性に関する仕様上のアドバンテージ（1 ページ以内で記載下さい）

暗号技術名：
安全性評価に関する論文リスト（紙面が足りない場合は追加して下さい） [1] … [2] …

暗号技術名：
実装性能に関するアドバンテージ(1 ページ以内で記載下さい)

暗号技術名：
実装性能に関する論文リスト（紙面が足りない場合は追加して下さい） [1] … [2] …

付録４

学会等での主要攻撃論文発表等一覧

目次

1.1. 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
☆	Cover and Decomposition Index Calculus on Elliptic Curves made practical. Application to a previously unreachable curve over Fp6 [Eurocrypt 2012]	86
☆	Improving the Complexity of Index Calculus Algorithms in Elliptic Curves over Binary Fields [Eurocrypt 2012]	86
	Faster Algorithms for Approximate Common Divisors: Breaking Fully-Homomorphic-Encryption Challenges over the Integers [Eurocrypt 2012]	87
	Decoding Random Binary Linear Codes in 2^(n/20): How 1+1=0 Improves Information Set Decoding [Eurocrypt 2012]	87
	Polly Cracker, revisited, revisited [PKC 2012]	88
	Solving Underdetermined Systems of Multivariate Quadratic Equations revisited [PKC 2012]	88
	Solving a Discrete Logarithm Problem with Auxiliary Input [PKC 2012]	88
☆	Attacking (EC)DSA Given Only an Implicit Hint [SAC 2012]	89
	Lattice Reduction for Modular Knapsack [SAC 2012]	91
☆	Efficient Padding Oracle Attacks on Cryptographic Hardware [Crypto 2012]	92
★	Public Keys [Crypto 2012]	93
	Efficient Dissection of Composite Problems, with Applications to Cryptanalysis, Knapsacks, and Combinatorial Search Problems (Best Paper Award) [Crypto 2012]	93
	Solving quadratic equations with XL on parallel architectures [CHES 2012]	95
☆	Breaking Pairing-Based Cryptosystems Using η_T Pairing over GF(3^{97}) [Asiacrypt 2012]	96
	A Coding-Theoretic Approach to Recovering Noisy RSA Keys [Asiacrypt 2012]	96
	Certifying RSA [Asiacrypt 2012]	96
	ストリーム暗号	
☆	Cryptanalysis of the ‘Kindle’ Cipher [SAC 2012]	89
	Cryptanalysis of the Loiss Stream Cipher [SAC 2012]	89
☆	Solving quadratic equations with XL on parallel architectures [CHES 2012]	95
	Smashing WEP in A Passive Attack [FSE 2013]	97
★	Full Plaintext Recovery Attack on Broadcast RC4 [FSE 2013]	98
	ブロック暗号	
	Narrow Bicliques: Cryptanalysis of Full IDEA [Eurocrypt 2012]	86
☆	An All-In-One Approach to Differential Cryptanalysis [SAC 2012]	89
	A New Method for Solving Polynomial Systems with Noise over F_2 and Its Applications in Cold Boot Key Recovery polynomial system with noise [SAC 2012]	89
	Cryptanalysis of the Xiao-Lai White-box AES Implementation [SAC 2012]	89
☆	All Subkeys Recovery Attack on Block Ciphers: Extending Meet-in-the-Middle Approach [SAC 2012]	90
☆	Improved Cryptanalysis of the Block Cipher KASUMI [SAC 2012]	90

1.2. Eurocrypt 2012 の発表

1.2.1. Eurocrypt 2012 の発表（1 日目）

Cover and Decomposition Index Calculus on Elliptic Curves made practical. Application to a previously unreachable curve over F_p^6 [Eurocrypt 2012]
Antoine Joux and Vanessa Vitse

合成数次拡大体上の楕円曲線離散対数問題に対する新しい攻撃法の提案。Weil Descent 攻撃と decomposition ベースの指数計算法を組み合わせた。例えば OEF (Optimal Extension Fields)では F_p^6 の形の有限体を使うが、このような場合に有効に働く。F_p^6- F_p^2- F_p という列の初めの拡大に Cover 攻撃を適用し、続く拡大では decomposition 攻撃(もしくはそれを改良した sieving 攻撃)を適用する。計算量見積もりは漸近的には $O\tilde{}(p^{5/3})$(decomposition)もしくは $O\tilde{}(p^{12/7})$(sieving)となっており、160 ビットセキュリティの場合は、それぞれ 750CPU 年もしくは 300CPU 年と見積もられている。

Improving the Complexity of Index Calculus Algorithms in Elliptic Curves over Binary Fields [Eurocrypt 2012]
Jean-Charles Faugere, Ludovic Perret, Christophe Petit, and Guenael Renault

標数 2 の拡大体上の楕円曲線離散対数問題に対する decomposition 攻撃法の改良。Semaev とそれに続く Gaudry, Diem らの方法に更なる制約条件を付加し、多変数多項式系に問題を帰着し、グレブナ基底を求めることにより問題を解く。あるヒューリスティックを仮定すれば、計算量は $O(2^{\omega n/2})$と見積もられる。
講演中、準指数時間解読の噂に触れ、まだ指数時間であり、結論を急ぐべきではないと釘を刺す見解が述べられた。

1.2.2. Eurocrypt 2012 の発表（2 日目）

Narrow Bicliques: Cryptanalysis of Full IDEA [Eurocrypt 2012]
Dmitry Khovratovich, Gaetan Leurent, and Christian Rechberger

最近導入された“biclique”フレームワークを IDEA に拡張／適用し、8.5 段の完全な IDEA に対する鍵解読を著しく高速化する初めてのアプローチを記す。
更に、ブロック暗号解析の biclique アプローチは、より多くの段数に対する結果を得られるだけではなく、既存攻撃の時間／データ計算量を改善することを示す。我々は IDEA のはじめの 7.5 段に対する攻撃を考え、実際的なデータ計算量で機能する変形アプローチを示す。
概念的な貢献は、「狭い biclique」テクニックである。即ち、最近導入された「独立」biclique アプローチを拡張し、他の条件は同じままで、データ計算量を著しく削減するものである。このために、ハッシュ関数解析において知られている、関連する差分経路を狭める自由度のテクニックを使用する。
我々の解析の計算量は大きく、IDEA の実用性を脅かすものではないが、これらのテクニックは実際に十分に有効性を確かめられるものである。

Cryptanalyses on a Merkle-Damgard Based MAC --- Almost Universal Forgery and Distinguishing-H Attacks [Eurocrypt 2012]
Yu Sasaki

本論文は、Merkle-Damgard ハッシュに基づいたメッセージ認証子(MAC: Message

Authentication Code)に対する 2 種類の解析を示す。Merkle-Damgard MAC とは、メッセージを M、メッセージ長を l、共有鍵を K としたときに、Hash(K||l||M)により MAC 値を計算するものである。この構成は、しばしば、LPMAC と呼ばれる。
初めに、任意の狭いパイプの Merkle-Damgard ハッシュに基づいた LPMAC に対する O((2^{n/2})問合せの H-識別攻撃を示す。このことは安全なハッシュ関数による LPMAC は H-識別攻撃に対して、2^n問合せまで耐性を持つという広く信じられている仮説が正しくないことを示している。実際、既存のすべての H-識別攻撃は、基づくハッシュアルゴリズムに対する専用攻撃を考えており、ほとんどの場合において、縮退段数で $2^{n/2}$ から 2^n の間の計算量で攻撃されていた。我々の攻撃は、一般的に機能するため、これらの結果を更新するものである。即ち、完全な段数が O($2^{n/2}$)回の問い合わせで攻撃される。
次に、LPMAC に対してより強力な攻撃、即ち、ほぼ万能な偽造攻撃(almost universal forgery attack)の強い形の攻撃が実行可能であることを示す。この設定では、攻撃者は与えられたメッセージの初めのいくつかのメッセージブロックを変更することができ、内部状態を解読し、MAC 値を偽造しようとする。任意の狭いパイプの Merkle-Damgard ハッシュ関数に対し、O($2^{n/2}$)回の問合せで攻撃を実行できる。
これらの結果は、安全な MAC を実現するには、長さを前に追加するスキームは十分でないことを示している。

1.2.3.Eurocrypt 2012 の発表（3 日目）

Faster Algorithms for Approximate Common Divisors: Breaking Fully-Homomorphic-Encryption Challenges over the Integers [Eurocrypt 2012]

Yuanmi Chen and Phong Q. Nguyen

Eurocrypt 2012 において、van Dijk らは、2001 年に Howgrave-Graham により導入された「近似整数共通因子問題(ACD: Approximate integer Common Divisors problem)」の困難性に基づく、単純な完全準同型暗号スキームを示した。ACD 問題には 2 種類ある。即ち、「部分的 ACD 問題(PACD: Partial ACD)」及び「一般的 ACD 問題(GACD: General ACD)」とである。一見してより簡単な PACD は、CRPTO 2011 において、van Dijk らの完全準同型暗号スキームよりも効率的な改良版を構成する際に、Coron らにより使われた。
我々は PACD の新しい解読アルゴリズムを示す。その実行時間は、本質的に総当たり法の「平方根」オーダーであり、実際の攻撃として最良のものである。この方法により、Coron らにより提案された完全準同型暗号のチャレンジ問題を実験で解くことができる。我々の PACD アルゴリズムは、新しい GACD 解読アルゴリズムに直結する。それは総当たり法よりも指数的に効率的である。興味深いことに、我々の主要なテクニックは、ノイズのある素因数分解や、小さい指数の RSA など、他の問題に適用することができる。

Decoding Random Binary Linear Codes in 2^(n/20): How 1+1=0 Improves Information Set Decoding [Eurocrypt 2012]

Anja Becker, Antoine Joux, Alexander May, and Alexander Meurer

ランダム線型符号の復号問題は、計算量理論と暗号において多くの応用を持ち、十分に研究されている問題である。符号及び LPN/LWE に基づくほとんどすべてのスキームの安全性は、ランダム線型符号を復号することは困難であるという仮定に基づく。
最近、2 新ランダム符号の復号アルゴリズムの実行時間を改良する進展があった。Bernstein、Lange、Peters の球衝突テクニックは、Stern らの情報集合復号アルゴリズムの計算量を $2^{0.0556n}$ に削減した。この境界は、「表現(representations)」テクニックを用いて、May、Meure、Thomae らにより $2^{0.0537n}$ に改善された。我々は更に、表現の数を増やす方法を示し、実行時間が $2^{0.0494n}$ となる新しい情報集合復号アルゴリズムを提案する。

1.3. PKC 2012 の発表

1.3.1.PKC 2012 の発表（1 日目）

Polly Cracker, revisited, revisited [PKC 2012]
Gottfried Herold

本論文では、Asiacrypt 2011 において、Albrecht、Farshim、Faugere、Perret により発表されたノイズのある Polly Cracker 暗号(PCN: Polly Cracker with Noise cryptosystem)を考える。PCN は、ノイズを持つランダム多変数方程式系のグレブナ基底を計算することの困難性に基づく公開鍵暗号である。我々は、0 次のノイズを持つ PCN 暗号が取りうるパラメーター範囲をすべてカバーする 4 種類の設定を調べる。初めの設定では、PCN 暗号は Regev の LWE に基づくスキームと等価であることが知られており、2 つ目の設定では、安全性は Regev のスキームと同等以下であることが知られている。
我々は、残り 2 つのうち 1 つの設定では、Regev の変形版と等価であるが効率は落ちることを示す。また、最後の 1 つの設定では、全く安全ではないことを示し、効率的な鍵回復攻撃を与える。攻撃とは関係ないが、PCN の安全性証明の誤りを修正する。

Solving Underdetermined Systems of Multivariate Quadratic Equations revisited [PKC 2012]
Enrico Thomae and Christopher Wolf

多変数(n 変数)の m 個の 2 次方程式系を解く問題(MQ: Multivariate Quadratic)は、代数的暗号解析における主要な課題の一つである。関連する MQ 問題は NP 完全であることが証明されているが、体の標数が偶数であるとき、m>=n(n-1)/2(過剰決定系)もしくは n>=m(m+1)(劣決定系)の場合には、多項式時間で解けることが知られている。m=n のときには、最悪計算量となることが広く信じられている。実際、過剰決定系においては、m=n から m>=n(n-1)/2 まで、より多くの方程式が利用可能となるため、計算量は次第に小さくなっていく。劣決定系の場合には、同様の現象は知られていなかった。これまで、m<n<m(m+1)の場合を扱うのに最善の方法は、m=n となるまでランダムに変数を推測することであった。
本論文は追加の変数をうまく使い、偶数標数で劣決定系の場合にも、次第に計算量を下げる方法を示す。即ち、変数の線型変換により、m 方程式(ただし、m=ωn、ω は 1 より大きい有理数)の MQ 系を解く計算量が(m-⌊ω⌋+1)個の方程式と変数を持つ MQ 系を解く計算量に削減されることを示す。我々のアルゴリズムは、既知の Kipnis-Patarin-Goubin(Eurocyrpt '99 の拡張版)の拡張と見ることができ、⌊$\log_2 \omega$⌋個の変数を消去する Courtois らのアルゴリズムを改良するものである。また、小さなωに対して我々のアルゴリズムを奇標数の場合にも適用する。我々の結果を、UOV(Unbalanced Oil and Vinegar)公開鍵署名スキームの現在の例(n=3m 即ちω=3 の場合)を破るために適用する。

1.3.2.PKC 2012 の発表（3 日目）

Solving a Discrete Logarithm Problem with Auxiliary Input [PKC 2012]
Yumi Sakemi and Goichiro Hanaoka and Tetsuya Izu and Masahiko Takenaka and Masaya Yasuda

160 ビット素体上の BN(Barreto-Naehrig)曲線上の補助情報つき離散対数問題解読実験。これまでの実験は 128 ビットであったが、今回は 160 ビットと現実に使用され得るパラメーター範囲となっている。ただし、パラメーターがある特殊な条件を満たさなければ、この解読手法は有効とならない。BGW(Boneh-Gentry-Waters)放送暗号、BB(Boneh-Boyen)ID ベース暗号、BB(Boneh-Boyen)署名スキーム等を利用する時には、この条件を満たさないようなパラメーターを選択するよう注意が必要である。

1.4. SAC 2012 の発表

1.4.1. SAC 2012 の発表（1 日目）

An All-In-One Approach to Differential Cryptanalysis [SAC 2012]

Martin Albrecht and Gregor Leande

差分解読法には、標準型の他、高階差分、不能差分、improvable 差分など、多様なバリエーションがあるので、これらから得られるゲインを多次元ベクトルとして扱うことによって、解読効率を改善することを提案した。このアプローチは、具体的な経路探索が可能なブロック長が小さい暗号に対して有効である。CHES 2009 で提案された 32 ビット暗号の KATAN-32 に適用したところ､差分に関する分布の偏りを従来より 20 段多い 91 段へ伸ばし、それを利用して 115 段縮小版の攻撃に成功した。この他、PRESENT のブロック長を 16 ビットに縮小した PRESENT-[4]について、差分経路を網羅的に調べ、従来法では 7 段までしか攻撃できなかったものを 9 段まで攻撃可能にした。なお、この攻撃に必要なメモリはブロック長の増加に対して急激に増加し、KATAN の 48 ビット版の KATAN-48 では O(2^{48})オーダとなり、現実的ではなくなる。

A New Method for Solving Polynomial Systems with Noise over F_2 and Its Applications in Cold Boot Key Recovery polynomial system with noise [SAC 2012]

Zhenyu Huang and Dongdai Lin

AES のようなブロック暗号の拡大鍵が展開されたメモリに対するコールドブート攻撃では、メモリ上のデータのノイズを、鍵ビットが満たす F_2 上の連立多項式を利用して除去することが必要となる。本発表では、F_2 上の max-PoSSo 問題を解く方法 ISBS (Incremental Solvingand Backtracking Search)を提案した。AES と Serpent の拡大鍵に対するコールドブート攻撃に適用したところ、従来からある SCIP 法よりも優れた鍵復元能力を示した。この比較において、時間を限定してノイズの除去能力を評価した。

Cryptanalysis of the Xiao-Lai White-box AES Implementation [SAC 2012]

Yoni De Mulder, Peter Roelse and Bart Preneel

White-box 実装では、信用できないエンドユーザを攻撃者みなし、鍵が引き出されないような対策が取られる。攻撃者は実装を完全に制御できることが仮定される。利用例としては携帯機器上のコンテンツの著作権管理がある。本発表では、Xiao と Lai が CSA 2009(IEEE)で提案した White-box 実装に対し、従来から利用された線形同値攻撃の改良版を用いて、より効率的な攻撃に成功した。

Cryptanalysis of the ‘Kindle’ Cipher [SAC 2012]

Alex Biryukov, Gaetan Leurent and Arnab Roy

Amazon の電子書籍リーダ Kindle では、著作兼管理用にストリーム暗号 PC1 が利用されている。PC1 は 1991 年に Pukall が設計した自己同期型ストリーム暗号で、鍵は 128 ビットで、16 ビットの add, mult, xor 演算を利用し、IV は無く、8 ビットずつ鍵ストリームを出力する。内部状態が小さいので、頻繁に起こる内部状態での衝突を利用した攻撃が有効で非常に弱く、次の攻撃が示された。

・既知平文攻撃　計算量: 2^{31}, 平文数: 2^{20}
・暗号文単独攻撃　計算量 2^{35}, 平文数: 2^{17}

また、PC1 を利用したハッシュ関数 PSCHF も提案されており、計算複雑度 2^{24} で、意味のあるメッセージをターゲットとする第２原像攻撃が成功することが示されている。

Cryptanalysis of the Loiss Stream Cipher [SAC 2012]
Alex Biryukov, Aleksandar Kircanski and Amr Youssef

Loiss Stream Cipher は IWCC 2011 で D.Feng らが発表した暗号で、SNOW ファミリーの設計を踏襲し、線形フィードバックシフトレジスタ(LFSR)と有限状態マシン(FSM)の組み合わせで構成されている。代数攻撃、線形識別子攻撃、高速相関攻撃などに対する耐性の向上を向上するため、FSM の出力先に独自の Byte-Oriented Mixer with Memory (BOMM)という構成要素を追加している。BOMM の主要部は RC4 と類似のバイトデータをスワップする仕組みである。本発表では、BOMM が確率$(15/16)^2$でしか拡散効果がないので、新規の構成要素に追加した意義は低いことを指摘した。実際、１バイトのみ異なる２個の関連鍵を利用した関連鍵攻撃を鍵の初期化に適用し、暗号化鍵 128 ビットのうち 92 ビットを Intel Pentium 4 プロセッサ(3GHz)搭載 PC で、１時間以内に特定することに成功した。

1.4.2.SAC 2012 の発表（2 日目）

All Subkeys Recovery Attack on Block Ciphers: Extending Meet-in-the-Middle Approach [SAC 2012]
Takanori Isobe and Kyoji Shibutani,

ブロック暗号に対する中間一致攻撃では、鍵スケジュールによる副鍵(拡大鍵)間の依存関係の扱いがポイントであり、GOST のように段鍵間の独立性が高い単純な鍵スケジュールでは有効性が高いが、複雑な鍵スケジュールでは攻撃の攻撃が下がる問題点があった。本発表では、中間一致攻撃において、各段の副鍵間の依存性を無視して探索することによって、任意の鍵スケジュールに対して有効な攻撃を示した。この方法により攻撃段数を、CAST-128 では従来の 6 段から 7 段へ、SHACAL-2 では 32 段から 41 段へ、KATAN32 では 78 段から 110 段に拡張した。

Improved Cryptanalysis of the Block Cipher KASUMI [SAC 2012]
Keting Jia, Leibo Li, Christian Rechberger, Jiazhe Chen and Xiaoyun Wang

KASUMI は ETSI SAGE が設計した 64 ビットブロック暗号である。Asiacrypt 2012 で Dunkelman らが 8 段のフルバージョンを関連鍵攻撃(関連鍵 4 個)で破れることを示したが、単一鍵では破れていない。今回の発表では、FI 関数を鍵依存の 16 ビット S-box と見なして、鍵ごとの差分分布テーブルを作ることによって、不能差分解読法を改良し、7 段縮小版の不能差分攻撃を示した。縮小の仕方は、後 7 段(初段を削除)と前 7 段(最終段を削除)の 2 種類があり、前者で選択平文$2^{52.5}$組、暗号化$2^{114.3}$回分の計算量、後者で既知平文2^{62}組、暗号化$2^{115.8}$回分の計算量で攻撃可能であることを示した。

Meet-in-the-Middle Technique for Integral Attacks against Feistel Ciphers [SAC 2012]
Yu Sasaki and Lei Wang

積分攻撃では特定の入力バイトは全値、他の入力バイトを固定して得られる識別子(distinguisher)を利用して鍵探索を行う。本発表では、識別子を利用した鍵探索において、異なるブランチに属する拡大鍵に共通して存在する鍵ビットを見つけることによって、攻撃の計算量が削減することを提案した。この方法により、HIGHT の 22 段縮小版に対する計算量を従来の$2^{118.71}$から$2^{102.35}$へ、CLEFIA(128 ビット鍵)の 12 段縮小版に対する計算量を従来の $2^{116.7}$ から $2^{103.1}$ へ削減できることを示した。また、LBlock の 20 段縮小版に対する Khovaratovich らの攻撃(FSE 2010)の誤りを指摘し、新たに選択平文数 $2^{63.6}$、計算量 $2^{39.6}$ で攻撃できることを示した。

Attacking (EC)DSA Given Only an Implicit Hint [SAC 2012]

Jean-Charles Faugere, Christopher Goyet and Guenael Renault

電子署名方式 DSA と ECDSA に対し、nonce に関する明示的でないヒントを利用することで、攻撃の効率が改善する方法を示した。ここで利用する明示的でないヒントとは、複数の nonce 間で最上位及び最下位の特定ビットを共有することであり、特定ビットの値自体は必要でない。このヒントを、格子の最小距離探索を探索する LLL アルゴリズムでこのヒントを利用することにより、DSA と ECDSA に対する攻撃の効率が改善することを理論と計算機実験の両方で示した。

Lattice Reduction for Modular Knapsack [SAC 2012]

Thomas Plantard, Willy Susilo and Zhenfei Zhang

LLL リダクションを利用したモジュラー型ナップザック問題の解法において、漸化式を改良することによって、計算効率が従来の $O(d^{3+\varepsilon}\beta^2+d^{4+\varepsilon}\beta)$ から $O(d^{2+\varepsilon}\beta^2+d^{4+\varepsilon}\beta)$ に改善した。ここで、d は格子の次元数、ベータは数値のビット長、ε は 1 以下のパラメータで基底に関する条件式を満足する値に設定される。

The Boomerang Attacks on the Round-Reduced Skein-512 [SAC 2012]

Hongbo Yu, Jiazhe Chen and Xiaoyun Wang

Skein-512 の 36 段縮小版に対して、最初の現実的なブーメラン識別子(practical boomenag distinguisher)を示した。既存の攻撃で利用されている互換性のない差分経路を正し、34 段縮小版の Threefish-512 に対する鍵復元攻撃を示した。

Boomerang and Slide-Rotational Analysis of the SM3 Hash Function [SAC 2012]

Aleksandar Kircanski, Yanzhao Shen, Gaoli Wang, Amr Youssef

SM3 は中国の国内標準のハッシュ関数で、SHA-1 に対する差分解読で有名な Xiaoyun Wang(清華大学)らが設計した。中国は 2007 年 12 月に TPM の中国版ともいえる TCM を発表し、その中で、ブロック暗号 SMS4、公開鍵暗号 SM2、ハッシュ関数 SM3 を採用している。MD 構造で、内部状態 256 ビット、メッセージブロックサイズ 512 ビット、ハッシュサイズ 256 ビット、64 ステップとなっている。本発表では次のブーメラン識別子が発表された。

- 33 ステップ、確率 $2^{-32.4}$
- 34 ステップ、確率 $2^{-53.1}$
- 35 ステップ、確率 $2^{-117.1}$

SHA-2 に対しては、Asiacrypt 2011 で 64 ステップ中 47 ステップのブーメラン識別子が発表されているので、この点に関しては SHA-2 より安全性は高い。SHA2 と異なり、SM3 には単純なスライド回転の性質があるが、具体的な攻撃には繋がっておらず、現在のところ安全性上の脅威はない。

1.5. Crypto 2012 の発表

1.5.1.Crypto 2012 の発表（1 日目）

Breaking and Repairing GCM Security Proofs [Crypto 2012]
Tetsu Iwata, Keisuke Ohashi, Kazuhiko Minematsu

GCM(Galois/Counter Mode of Operation)の設計者によるプライバシーと認証の安全性証明が基づいている、カウンター衝突確率の上限値に関する補題は、無効であることを示す。この考察から識別攻撃を導くことができ、プライバシーの証明は無効となる。我々は、新たな安全性境界値をプライバシーおよび認証に関して与えることにより安全性証明を修正した。結果として上限値は従来よりやや大きくなるが、GCM の証明可能安全性は保たれる。ただし、通常よく用いられる nonce が 96bit の場合には、よりよい上限値となる。

1.5.2.Crypto 2012 の発表（2 日目）

New Preimage Attacks Against Reduced SHA-1 [Crypto 2012]
Simon Knellwolf, Dmitry Khovratovich

本論文では、57 段まで縮退した SHA-1 に対する原像攻撃を示す。これまでの最良の攻撃は、Crypto 2009 で示された 48 段に対するもので、$2^{159.3}$の圧縮関数評価コストで不正確なパディングの 2 つのブロック原像を見つけるものであった。同様の版に対して、我々の攻撃は$2^{150.6}$の圧縮関数評価コストで 1 ブロック原像を、また$2^{150.6}$の圧縮関数評価コストで正しくパディングされた 2 ブロック原像を見出すことができる。青木-佐々木らにより開発された中間一致テクニックを差分的見地で見ることにより本改良結果が得られる。この新しいフレームワークは中間一致攻撃を差分解析に近く関係づけるものであり、線型メッセージ拡大と弱い拡散性を持ったハッシュ関数には特に有効である。

1.5.3.Crypto 2012 の発表（3 日目）

Efficient Padding Oracle Attacks on Cryptographic Hardware [Crypto 2012]
Romain Bardou, Riccardo Focardi, Yusuke Kawamoto, Graham Steel, Joe-Kai Tsay

様々な暗号機器の暗号化された鍵を取り入れる機能を利用して、取り入れた鍵を暴く方法を示す。攻撃はパディングオラクル攻撃であり、不正にパディングされた平文に対するエラーメッセージをサイドチャネル情報として使用する。非対称暗号の場合、Bleichenbacher の RSA PKCS#1 v1.5 に対するパディングを改良し、「百万メッセージ攻撃」を平均 49,000 回(中間値 14500 回)のオラクル呼び出しで実現し、1,024 ビット鍵による未知の正当な暗号文を解読した。元のアルゴリズムでは平均 215,000 回(中間値 163,000 回)のオラクル呼び出しが必要であった。ある特定の機器の場合には、平均 9,400 回(中間値 3,800 回)の操作しか必要としない実装の詳細を示す。対称鍵暗号の場合には、既に非常に効率的である Vaudenay の CBC 攻撃を取り上げる。セキュリティトークン、スマートカード、エストニア電子 ID カード等を含む多くの商用暗号機器の脆弱性を示す。攻撃は十分に効率的であり、実際に行うことができる。脆弱であるとわかったすべての機器に対する実行時間を与え、我々の最適化によってどの程度現実的になるかを示す。また、攻撃の有効性の数学的解析、広範囲にわたる実験結果、対策に関する議論も示す。

Public Keys [Crypto 2012]

Arjen K. Lenstra, James P. Hughes, Maxime Augier, Joppe W. Bos, Thorsten Kleinjung, Christophe Wachter

実社会に公開されている RSA 公開鍵証明書を 6,582,851 件収集し、その内の 266,729 個(約 4%)は同じ modulus が使われており、12,934 個(約 0.2%)の modulus は、同じ素因子が存在するため素因数分解することができた。公開鍵情報である合成数 N は、2 つの素数の積 N=pq の形をしており、N を素因数分解することは困難であることが公開鍵暗号の安全性の根拠となっている。公開鍵の modulus が一致する場合、互いの秘密鍵を求めることができる。2 つの合成数 $N_1=pq_1$、$N_2=pq_2$ がたまたま素数 p を共通因子として持った場合、それらの最大公約数(GCD)は第三者が高速に計算することができ、秘密の素数 p を出力してしまう。原因は、鍵生成の際の乱数生成のエントロピーが小さい場合、たまたま同じ乱数を生成してしまうことにあると考えられる。N.Heninger らがランプセッションおよび 8 月 8 日～8 月 10 日に開催された USENIX Security 2012 において、エントロピーが低くなる原因について分析を行い、チェックツールを公開している。既に秘密鍵が見つかってしまった公開鍵証明書に関しては再発行するしかなく、今後の対策としては、鍵生成時のエントロピーを十分大きくする手段を講ずる必要がある。

1.5.4.Crypto 2012 の発表 (4 日目)

Efficient Dissection of Composite Problems, with Applications to Cryptanalysis, Knapsacks, and Combinatorial Search Problems (Best Paper Award) [Crypto 2012]

Tung Chou, Chen-Mou Cheng, Ruben Niederhagen, Bo-Yin Yang

本論文において、大きなクラスの様々な問題が、複数の合成された構造を持ち、そのことによって既知のアルゴリズムよりも良い時間／メモリトレードオフを持つ、新しいタイプの「分解(dissection)」攻撃が可能となることを示す。典型的な例は、r 個の独立した n ビット鍵を持つ、複数回暗号化スキームの鍵を求める問題である。エラーのない既知攻撃は、すべて $TM=2^{rn}$ を満たす時間 T およびメモリ M を必要とし、「誤り」を許容した場合でも、$TM < 2^{3rn/4}$ を満たす攻撃はなかった。我々の新しい攻撃は、誤ることはなく、より小さな TM の積で、可能性のある鍵をすべて見出す初めてのアルゴリズムとなる。例えば、r=7 のブロック暗号の連続実行を解読するのに、$T=2^{4n}$ および $M=2^{n}$ しか必要としない。改良の割合は、r が増加するにつれて上限なく大きくなり、時々誤った解を求めるアルゴリズムを許したときには、我々の分解テクニックと並行衝突探索とを組み合わせることにより、より良いトレードオフを得ることができる。新しい分解テクニックの汎用性を示すために、以下の問題における一般的な使い方を与える：ハッシュ関数をリバウンド攻撃で攻撃する場合、困難なナップサック問題を解く場合、一般化されたルービック・キューブに対する最短解を既知の最良アルゴリズムよりも良い時間計算量(小さなメモリ計算量の場合)で求める問題など。

Resistance Against Iterated Attacks Revisited [Crypto 2012]

Asli Bay, Atefeh Mashatan, Serge Vaudenay

反復攻撃(iterated attack)は、d 回の平文問い合わせを行うことができ、各反復において 1 ビットを計算することができ、ランダムな暗号 C と理想的なランダム暗号 C*とをすべてのビットに基づいて区別しようとする反復攻撃者から成る。EUROCRYPT ’99 において、Vaudenay は、反復がほとんど共通の問い合わせを持たないときに、2d-非相関な暗号はオーダーd の反復攻撃に耐性があることを示した。そして彼は初めに、オーダーd の非適応的反復攻撃に耐性を持つための暗号の必要条件は何かを問いかけた。次に、彼は、異なる反復において平文の問い合わせを繰り返すことは、非適応的な区別者に何も有利にならないと推測した。我々は、これらの 2 つの長い間未解決であった問題に終止符を打つ。
オーダーd の非適応的反復攻撃に耐性を持つためには、オーダー2d-1 の非相関性は十分で

ないことを示す。我々は、このことを、オーダー2d-1 の非相関な暗号とそれに対して成功するオーダーd の非適応的反復攻撃からなる反例を挙げることにより示す。
更に我々は、上記の推測は誤りであることを示す。異なる反復において同じ問い合わせをより高い確率で行うことは、C と C*を区別することにおいて攻撃者にとってより有利になることを示す。我々は、同じ問い合わせを高い確率で行うオーダー1 の反復攻撃によって解読されるオーダー2d の非相関性を持つ暗号からなる直観に反する例を与える。

1.6. CHES 2012 の発表

1.6.1. CHES 2012 の発表（ランプセッション）

Solving quadratic equations with XL on parallel architectures [CHES 2012]
Tung Chou, Chen-Mou Cheng, Ruben Niederhagen, Bo-Yin Yang

ある種の暗号アルゴリズムは多変数の二次連立方程式を解くことによって攻撃可能である。この連立方程式を解く方法に XL アルゴリズムがある。この発表では、block Wiedemann アルゴリズムを適用し、それぞれ 8 個の CPU コアと 36GB の RAM を持つノード 8 個からなる小規模クラスタに実装したところ、GF(16)上の 32 変数 64 連立二次方程式を 5 日で解くことができた。ここで使用したソフトウェアは GF(2)や GF(31)にも適用でき、その他の小さな位数の有限体にも容易に適用可能である。

1.7. Asiacrypt 2012 の発表

1.7.1. Asiacrypt 2012 の発表（1 日目）

Breaking Pairing-Based Cryptosystems Using η_T Pairing over GF(3^{97}) [Asiacrypt 2012]
Takuya Hayashi, Takeshi Shimoyama, Naoyuki Shinohara, and Tsuyoshi Takagi

GF(3^n) 上の η_T ペアリングを用いたペアリング暗号はその安全性を GF(3^n) 上の ECDLP と GF(3^{6n}) 上の DLP を解くことの困難性に依存する。拡大次数 n = 97 は η_T ペアリングの実装実験で実際に採用され、注目されている拡大次数である。本発表では、小さい標数の拡大体上の DLP を効率よく解く関数体篩法に、格子篩などの高速アルゴリズムを改良して導入し、関数体篩法の最適なパラメータ値を採用することで、923 bit 長である GF($3^{6\cdot 97}$) 上の DLP を 148.2 日で解いたことを報告している。この成果は GF(3^{6n}) の形の拡大体上の DLP を解くことにおいて世界記録を達成したことを意味している。

1.7.2. Asiacrypt 2012 の発表（2 日目）

A Coding-Theoretic Approach to Recovering Noisy RSA Keys [Asiacrypt 2012]
Kenneth G. Paterson, Antigoni Polychroniadou, and Dale Sibborn

cold boot 攻撃を介して実際の(RSA)のオリジナルの秘密鍵を得る手法として従来提案されていた HS(Heninger & Shacham)法や HMM(Henecka & May & Meurer)法に比べ、より一般的な設定条件を想定したモデルについて取り扱っており、HS や HMM に比べ現実の cold boot の状況に適応し易い新たなアルゴリズムを提案した。技術的には、 cold boot problem を coding theory に結び付けノイズの乗った部分的な秘密鍵情報からオリジナルの秘密鍵を取り出すための(従来方法に比べ)より効率的なアルゴリズムの提案となっている。RSA に関わる攻撃手法の進展として継続監視が必要な技術である。

Certifying RSA [Asiacrypt 2012]
Saqib A. Kakvi, Eike Kiltz, and Alexander May

落とし戸付き置換は検証に必要となる overhead をつけることにより置換の検証可能性の性質を付加することができる。効率の観点から overhead はできるだけ小さなサイズに抑えられることが望ましい。落とし戸付き関数である RSA 関数は、入力-出力の関係が置換関数となっている場合に、検証可能な置換関数となり得る。
e>N の場合は、その条件を満たすことができる。この場合の overhead は大きく膨らんでしまう。一方で、e< $N^{1/4}$ の場合については、検証可能な置換関数の構成不可能性が示されている。$N^{1/4}$ < e < N の場合に関しては、構成可能/不可能については明らかにされていかなった。本発表では、この場合に関して、検証可能な置換関数が構成可能であることを示した。また、Coppersmith の方法を用いて具体的な検証可能な置換アルゴリズムの構成を示している。

1.8.PKC 2013 の発表

1.8.1. PKC 2013 の発表（2 日目）

Recovering RSA Secret Keys from Noisy Key Bits with Erasures and Errors [PKC 2013]

Noboru Kunihiro, Naoyuki Shinohara, Tetsuya Izu

RSA 秘密鍵ビットに紛失と誤りとがある場合に正しい秘密鍵を求める方法を議論している。既存アルゴリズムには 2 種類ある。Crypto 2009 において、Heninger と Shacham は紛失のみを含む秘密鍵から全体を求める方法を示している。その後、Henecka らは Crypto 2010 において、誤りのみを含む秘密鍵から正しい秘密鍵を求める方法を示した。サイドチャネル攻撃やコールドブート攻撃などの物理的攻撃においては、紛失も誤りも含む鍵から正しい鍵を求める必要がある。本論文では、紛失も誤りも含む秘密鍵から正しい秘密鍵を求める方法を提示し、多項式時間で求まるための条件を分析している。また、理論的限界を評価し、我々のアルゴリズムがどの程度まで達成するかを議論している。

Combined Attack on CRT-RSA -- Why Public Verification Must Not Be Public [PKC 2013]

Guillaume Barbu, Alberto Battistello, Guillaume Dabosville, Christophe Giraud, Guénaël Renault, Soline Renner, Rina Zeitoun

サイドチャネル解析および故障注入攻撃に耐性のある CRT-RSA 実装に対する、新しい結合攻撃を導入している。これらの実装は、計算中に故障が起こされた時に攻撃者が署名を得ることができないように対策されている。実際、このような値は、公開された法と誤った署名との最大公約数を計算することにより、攻撃者が RSA の秘密鍵を得ることを可能とする。攻撃の原理は、署名計算の最中に故障を注入し、故障注入対策が実行されている間にターゲットとする敏感な値に対しサイドチャネル分析解析を行うことにある。その結果得られる情報は、公開された法を素因数分解するのに使用され、RSA 秘密鍵全体を漏洩させることにつながる。本論文の攻撃は、格子縮小テクニックを使うことにより計算量を大幅に削減させている。攻撃が効率的であることを保証するシミュレーションを与えるとともに、アルゴリズムの性能に非常に小さな影響しか与えない 2 つの対策法も与えている。本論文の攻撃は、秘密の値を引き出すために、故障注入対策の最中にサイドチャネル解析を実行するため、本論文では、故障注入およびサイドチャネル解析に対する対策は一枚岩の実装である必要があることを注意喚起している。

1.9. FSE 2013 の発表

1.9.1. FSE 2013 の発表（1 日目）

Smashing WEP in A Passive Attack [FSE 2013]
Pouyan Sepehrdad, Petr Susil, Serge Vaudenay and Martin Vuagnoux

既知の偏りを改善することにより、WEP に対する能動的かつ受動的な攻撃に関して理論的にも実験的にも大幅な改善を行ったという発表。既知の攻撃用ソフトウェア Aircrack-ng に比べて、ARP インジェクションに基づく 104-bit WEP 鍵に対する能動的攻撃では必要パケット数を約 50%改善でき、受動的攻撃では約 28%改善されている。通常の PC 上では数秒で解読可能となっている。

Full Plaintext Recovery Attack on Broadcast RC4 [FSE 2013]
Takanori Isobe, Toshihiro Ohigashi, Yuhei Watanabe and Masakatu Morii

ブロードキャスト・シナリオにおける RC4 に対する攻撃についての発表。ブロードキャスト・シナリオとは同じ平文を異なる鍵で暗号化する際、元の平文復元する攻撃である。初めの 257 バイトにおいて攻撃に非常に有効な偏り(optimal bias set)を発見し、異なる鍵で暗号化された 2^{32} 個の暗号文があれば確率 0.8 以上で平文を復元することが可能となった。また 258 バイト目以降についても、既知の偏り(long-term bias)と組み合わせることにより、異なる鍵で暗号化された 2^{34} 個の暗号文さえあればほぼ確率 1 で平文を復号することが可能となった。

1.9.2. FSE 2013 の発表（2 日目）

Collision Attacks on Up to 5 Rounds of SHA-3 Using Generalized Internal Differentials [FSE 2013]
Itai Dinur, Orr Dunkelman and Adi Shamir

SHA-3 に選出された Keccak の縮小版に対する衝突発見攻撃についての発表。今まではハッシュサイズが 224 ビット及び 256 ビットに対する攻撃しか発表されていなかったが、ハッシュサイズが 384 ビット及び 512 ビットに対する攻撃が今回初めて発表されたことになる。Keccak-384 及び Keccak-512 ともに 24 ラウンド中 3 ラウンドまで実際の衝突が計算可能となり、Keccak-384 については、計算量 2^{147}(4 ラウンド)、Keccak-256 については、計算量 2^{115}(5 ラウンド)まで攻撃ラウンド数が拡張された。

Rotational cryptanalysis of round-reduced Keccak [FSE 2013]
Pawel Morawiecki, Josef Pieprzyk and Marian Srebrny

SHA-3 に選出された Keccak の縮小版に対する、原像計算攻撃及びラウンド関数とランダム置換を区別する識別攻撃についての発表。前者の攻撃に関しては、いずれも 4 ラウンドの縮小版 Keccak に対して計算量が 2^{221}(ハッシュサイズ 224)、2^{252}(ハッシュサイズ 256)、2^{378}(ハッシュサイズ 384)、2^{506}(ハッシュサイズ 512)となった。後者の攻撃に関しては、5 ラウンドまで攻撃ラウンド数が拡張された。

On Weak Keys and Forgery Attacks against Polynomial-based MAC Schemes (Best Paper Award) [FSE 2013]
Gordon Procter and Carlos Cid

米国NISTがSP 800-38Dで定めているGCMはブロック暗号の利用モードで、有限体上の多項式を用いてモード（の一部）を定義しているが（多項式ベースで定義されているこの種の技術は多い）、それに対する攻撃(弱鍵と偽造)に関する発表。有限体上の特定の元(複数の場合も含む)を根にもつ多項式を生成しそれを元の情報に加えることができれば、多項式に代入すると値がゼロになるためこの種の攻撃が可能になるという仕組みである。既知の攻撃ではメッセージサイズの長いことが適用条件としてあったが、今回の攻撃ではメッセージ長は小さいこと、弱鍵の範囲がより大きくなっていることが特徴となっている。
CRYPTRECでは注釈として、GCMにおけるパラメータにおいて多項式ベースにならない部分を推奨しているため、影響は限定的なものと考えられる。

1.9.3.FSE 2013 の発表（3 日目）

Exhausting Demirci-Selçuk Meet-in-the-Middle Attacks against Reduced-Round AES [FSE 2013]
Patrick Derbez and Pierre-Alain Fouque

既知の AES に対する中間一致攻撃を SPN 構造をもつ一般的なブロック暗号に適用可能なものに拡張し、計算量が小さくなる最適なパラメータを全数探索するアルゴリズムを開発したという発表。その結果、192 ビット鍵及び 256 ビット鍵の 8 ラウンド縮小版 AES に対する中間一致攻撃の計算量を改善している。

A Framework for Automated Independent-Biclique Cryptanalysis [FSE 2013]
Farzaneh Abed, Christian Forler, Eik List, Stefan Lucks and Jakob Wenzel

Biclique攻撃の解析を自動的に行うアルゴリズムを開発したという発表。AES、韓国で開発されたARIAやAESに似たBKSQ(設計者はRijndaelと同一)に対して同アルゴリズムを適用してBiclique攻撃を行い、既知の攻撃に比べて大幅な改善はなされていないものの、フルラウンドのAESに対しては、$2^{126.72}$(128ビット鍵)、$2^{190.28}$(192ビット鍵)、$2^{254.53}$(256ビット鍵)の計算量を有するパラメータを探索している。

付録５

電子政府推奨暗号リスト

平成15年2月20日
総務省
経済産業省

技術分類き		名称
公開鍵暗号	署名	DSA
		ECDSA
		RSASSA-PKCS1-v1_5
		RSA-PSS
	守秘	RSA-OAEP
		RSAES-PKCS1-v1_5(注1)
	鍵共有	DH
		ECDH
		PSEC-KEM(注2)
共通鍵暗号	64ビットブロック暗号(注3)	CIPHERUNICORN-E
		Hierocrypt-L1
		MISTY1
		3-key Triple DES(注4)
	128ビットブロック暗号	AES
		Camellia
		CIPHERUNICORN-A
		Hierocrypt-3
		SC2000
	ストリーム暗号	MUGI
		MULTI-S01
		128-bit RC4(注5)
その他	ハッシュ関数	RIPEMD-160(注6)
		SHA-1(注6)
		SHA-256
		SHA-384
		SHA-512
	擬似乱数生成系(注7)	PRNG based on SHA-1 in ANSI X9.42-2001 Annex C.1
		PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) Appendix 3.1
		PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) revised Appendix 3.1

注釈：

(注 1)　SSL3.0/TLS1.0 で使用実績があることから当面の使用を認める。

(注 2)　KEM (Key Encapsulation Mechanism) -DEM(Data Encapsulation Mechanism)構成における利用を前提とする。

(注 3)　新たな電子政府用システムを構築する場合、より長いブロック長の暗号が使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 4)　3-key Triple DES は、以下の条件を考慮し、当面の使用を認める。

1) FIPS46-3 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 5)　128-bit RC4 は、SSL3.0/TLS1.0 以上に限定して利用することを想定している。なお、リストに掲載されている別の暗号が利用できるのであれば、そちらを使用することが望ましい。

(注6)　新たな電子政府用システムを構築する場合､より長いハッシュ値のものが使用できるのであれば､256ビット以上のハッシュ関数を選択することが望ましい｡ただし、公開鍵暗号での仕様上、利用すべきハッシュ関数が指定されている場合には、この限りではない。

(注7)　擬似乱数生成系は、その利用特性上、インタオペラビリティを確保する必要性がないため、暗号学的に安全な擬似乱数生成アルゴリズムであれば、どれを利用しても基本的に問題が生じない。したがって、ここに掲載する擬似乱数生成アルゴリズムは「例示」である。

別添

電子政府推奨暗号リストに関する修正情報

修正日付	修正箇所	修正前	修正後	修正理由
平成 17 年 10 月 12 日	注釈の注 4)の 1)	FIPS46-3 として規定されていること	SP800-67 として規定されていること	仕様変更を伴わない､仕様書の指定先の変更

発行日　2013年 5月 31日　第1版
発行者
・〒184-8795
東京都小金井市貫井北四丁目2番1号
独立行政法人 情報通信研究機構
（ネットワークセキュリティ研究所 セキュリティ基盤研究室、
セキュリティアーキテクチャ研究室）
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