CRYPTREC Report 2011

平成 24 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 2011 年度活動報告である。

暗号技術評価プロジェクト CRYPTREC は 2000 年に開始され、2003 年 2 月には、暗号技術検討会を主催する総務省及び経済産業省が電子政府推奨暗号リスト(現リスト)を公表した。その後 2003 年度からは、電子政府推奨暗号の安全性の監視等を行う「暗号技術監視委員会」と電子政府推奨暗号を実装する暗号モジュールの評価基準・試験基準の作成等を行う「暗号モジュール委員会」の 2 委員会の体制となった。

現リストは、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。しかし、策定から 5 年が経過し、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ったため、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」が実施された。そのため、2009 年度からは、「暗号方式委員会」、「暗号実装委員会」、「暗号運用委員会」の 3 委員会の体制により、2013 年のリスト改訂に向けて活動を開始した。

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、リスト改訂に向けた安全性評価を行っている。

2011 年度は、暗号技術の監視活動及び、応募暗号技術に関する第 2 次評価並びに現リスト掲載暗号技術の安全性に関する再評価を行った。2012 年度は、第 2 次評価を引き続き実施する予定であり、さらに電子政府推奨暗号リストの改訂に関する事項を審議していく予定である。暗号技術調査ワーキンググループでは、昨年度に引き続き、リストガイドワーキンググループを開催し、鍵共有技術及び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調査を行った。また、新たに計算機能力評価ワーキンググループを開催し、2006 年度に公表された「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」に関する図の更新に関して審議した。この予測図は、RSA-1024 を安全に使える期間の根拠となっており、「政府機関の情報システムにおいて使用されている暗号技術 SHA-1 及び RSA1024 に係る移行指針」等の策定にも活用されている。

電子政府推奨暗号の監視は、暗号が使われ続ける限り継続していかねばならない活動である。また、この活動は、暗号実装委員会及び暗号運用委員会との連携を保ちつつ、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っている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。

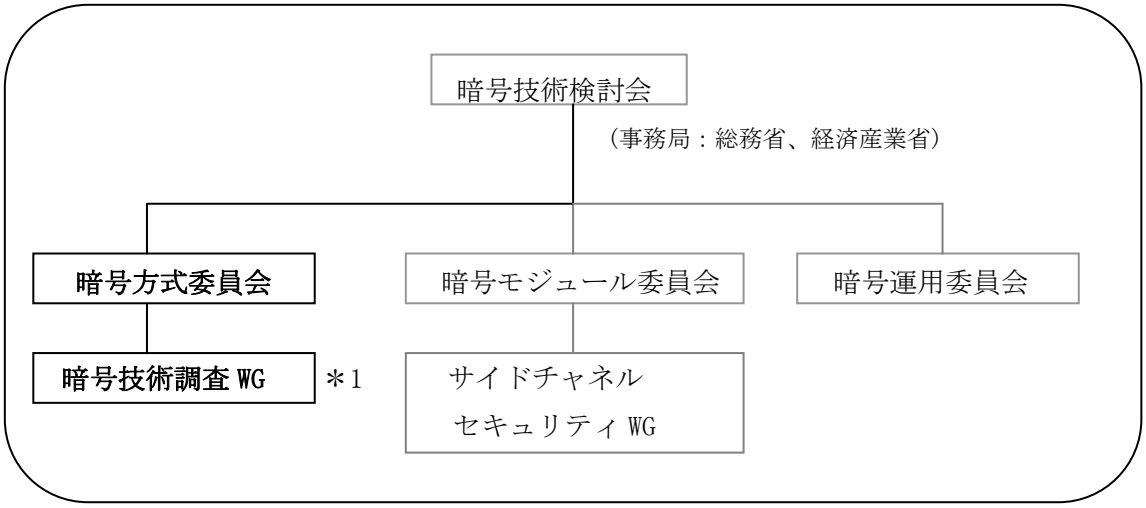
【問合せ先】　info@cryptrec.go.jp

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訂に関する調査・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。



＊1 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	田中 秀磨	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 副研究センター長

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
委員	菅野　哲	ＮＴＴソフトウェア　主任エンジニア補
委員	佐野　文彦	東芝ソリューション株式会社
委員	寺西　勇	日本電気株式会社　主任
委員	花岡　悟一郎	独立行政法人産業技術総合研究所
委員	藤崎　英一郎	日本電信電話株式会社　主幹研究員
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

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	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

中嶋　良彰	内閣官房情報セキュリティセンター［2011 年 6 月まで］
山口　利恵	内閣官房情報セキュリティセンター［2011 年 6 月まで］
根本　農史	内閣官房情報セキュリティセンター［2011 年 6 月まで］
福永　利徳	内閣官房情報セキュリティセンター［2011 年 7 月より］

中山　慎一	内閣官房情報セキュリティセンター［2011 年 7 月より］
今福　健太郎	内閣官房情報セキュリティセンター［2011 年 7 月より］
初川 泰介	警察庁 情報通信局[2011 年 7 月まで]
山城　瑞樹	警察庁 情報通信局[2012 年 3 月まで]
根木　まろか	警察庁 情報通信局[2012 年 3 月より]
松宮 志麻	総務省 行政管理局
浦上 哲郎	総務省 自治行政局 住民制度課[2011 年 7 月まで]
山﨑 敏明	総務省 自治行政局 住民制度課[2011 年 3 月まで]
林　俊子	総務省 自治行政局 住民制度課[2011 年 7 月より]
浦船 利幸	総務省 自治行政局 地域政策課
水野 伸太郎	総務省 情報流通行政局[2011 年 10 月まで]
佐々木 信行	総務省 情報流通行政局[2011 年 9 月まで]
谷岡 大祐	総務省 情報流通行政局[2011 年 7 月まで]
飯田 恭弘	総務省 情報流通行政局[2011 年 10 月より]
鮫島 清豪	総務省 情報流通行政局[2011 年 9 月より]
樋口 有二	総務省 情報流通行政局[2011 年 7 月より]
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
森川 淳	経済産業省 商務情報政策局
池西 淳	経済産業省 商務情報政策局[2011 年 5 月まで]
守山 速飛	経済産業省 商務情報政策局[2011 年 5 月より]
坂下 圭一	防衛省 運用企画局
石川 正興	防衛省 技術研究本部[2011 年 4 月まで]
佐藤 史生	防衛省 技術研究本部[2011 年 4 月より]
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、近藤玲子[7 月まで]、沼田文彦[9 月より]、松尾真一郎、野島良、大久保美也子、蓑輪正、黒川貴司、金森祥子、多賀文吾、笠井祥、赤井健一郎、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、山岸篤弘、大熊建司、神田雅透、小暮淳、恵本健亮、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１参照）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

平成１２年度から平成１４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、平成１４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１参照）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、平成２１年度は、平成２０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。

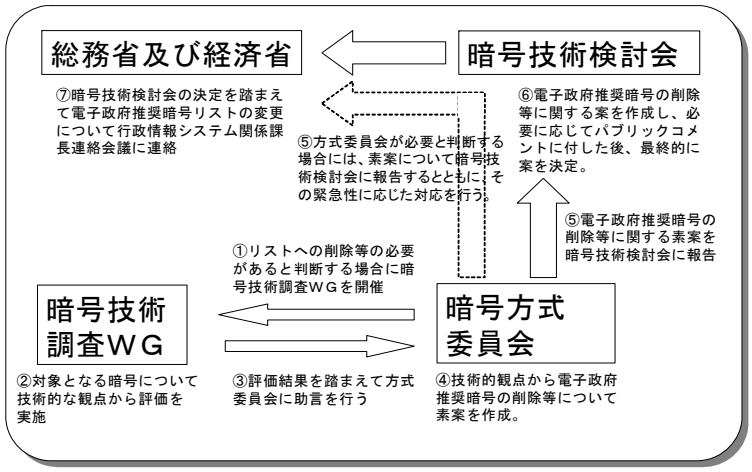
1.4 活動の方針

電子政府推奨暗号リスト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



第２章 電子政府推奨暗号リストの改訂について

2.1. 改訂の背景

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、「現リスト」）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、現リスト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。

現リストには、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、現リストを改訂することが必要である。

2.2　現リストの改訂の目的

今回の改訂においては、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、今回の改訂にあたっては、新たに暗号技術の公募を行うとともに、現リストに掲載されている暗号技術の見直しを行い、現リストの全体の構成を改めることとする。

2.3　電子政府推奨暗号リスト改訂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、現リスト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、現リスト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、現リスト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。決定については、2012 年度実施を予定している。

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、現リスト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	電子政府推奨暗号リスト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、現リスト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、現リスト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

2012 年度の電子政府推奨暗号リストの改訂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。

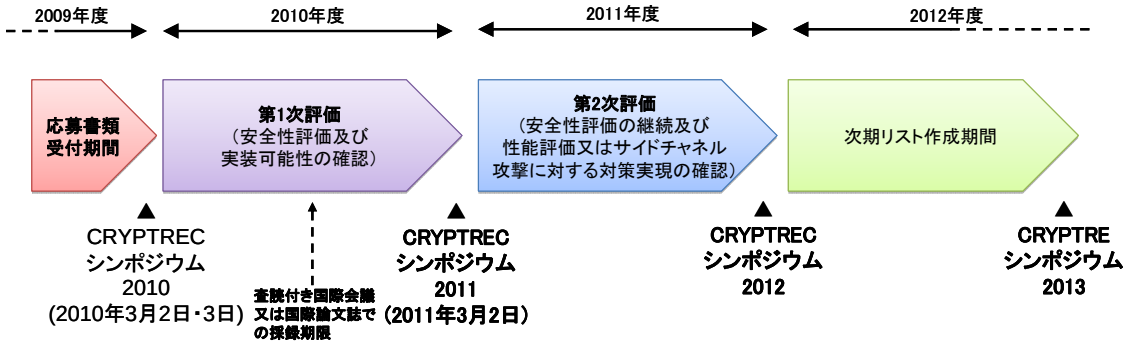


図 3.4 評価スケジュール

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 月頃

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[1]、ASIC[2]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。

[1] FPGA：Field Programmable Gate Array
[2] 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、現リスト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．第２次評価及び現リストに記載された暗号技術の再評価の進捗状況

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、電子政府推奨暗号リストに掲載された暗号技術の安全性に関する再評価の進捗状況は以下のとおりである。

２．７．１．安全性評価状況

(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[3]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[4]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、

[3] 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。
[4] 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。

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 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[5]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る。

(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評価

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][6]	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] [7])	(2^{-215}[2])	192 ビット鍵と同じ

[5] 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。

[6] [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.

[7] [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][8]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今後検討が必要である。

[8] [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

(3) MULTI-S01 の MAC 機能について

MULTI-S01 はストリーム暗号として現リスト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、MAC 機能に関する評価が必要である。

２．７．２．実装性評価状況

応募暗号技術及び現行の電子政府推奨暗号リスト掲載暗号技術に対するソフトウェア実装性能及びハードウェア実装性能の評価を実施した。評価対象の暗号技術と評価用実装の開発者を表 3.12 に示す。

表 3.12　評価対象の暗号技術と評価用実装の開発者

評価対象 アルゴリズム	実装評価		実装者
	ソフトウェア評価	ハードウェア評価	
CLEFIA	○	○	応募者
Enocoro-128v2	○	○	応募者
KCipher-2	○	○	応募者
PC-MAC-AES	○	○	応募者
AES	○	○	外部委託先
Camellia	○	○	外部委託先
CIPHERUNICORN-A	○	○	外部委託先
Hierocrypt-3	○	○	外部委託先
SC2000	○	○	外部委託先
MUGI	○	○	外部委託先
MULTI-S01	－	○	外部委託先
AES-CMAC	○	○	外部委託先

(1) ソフトウェア実装の性能評価

評価環境には、2009 年度に経済産業省による研究開発事業「クラウド環境における暗号技術評価」として開発された性能評価ツールを利用し、通常の PC 環境における処理速度、実装サイズ等を測定する方針に沿って実装評価を実施した。

現リスト掲載暗号の評価用実装は、性能評価ツールに添付の暗号ライブラリとして用意されているものを利用した。新規応募暗号については、実装開発に必要な情報をまとめた「応募暗号ソフトウェア実装性能評価要項」を応募者に配布し、評価用暗号モジュールの提出を依頼した。11 月内に全応募者から暗号モジュールが提出され、現リスト掲載暗号と合わせて、初期化、暗

号化(MAC 生成)、復号(MAC 検証)に掛かったクロック数、使用したメモリ量を測定し、ソフトウェア実装性能評価はほぼ終了した。評価の結果、いずれの暗号技術も十分な実装性能を有していることを確認した。

測定結果のまとめ方と公開方法については、さらに検討する必要があるため、2012 年度もソフトウェア実装評価活動は継続する。

(2) ハードウェア実装性能の評価

実装プラットフォームに、サイドチャネル攻撃用標準評価ボード SASEBO-GII(産業技術総合研究所と東北大学が開発)を、評価環境には CRYPTREC の依頼により産業技術総合研究所が開発したものを利用して、高速実装における処理性能の評価とサイドチャネル攻撃に対する対策可能性の確認を実施した。

現リスト掲載暗号については、サイドチャネル攻撃対策可能性の確認は実施せず、高速実装の開発及び性能評価を、一般競争入札で選考した業者に委託した。実装情報とその評価結果は 2 月末に納入され、現在その内容を確認中である。

新規応募暗号については、応募者に実装開発に必要な情報をまとめた「応募暗号ハードウェア実装性能評価要項」配布し、次の３種類の実装を提出するように依頼した。

評価用実装 1 (高速実装)
評価用実装 2 (対策実装)
評価用実装 3 (素朴実装)

これらの実装は 1 月内に提出され、高速実装については、動作周波数、暗号化・復号のサイクル数、実装サイズなどの測定がほぼ終了した。いずれの新規応募暗号技術も十分な実装性能を有していることを確認した。サイドチャネル攻撃対策可能性については、有効性を確認するための測定を準備中である。

２．８．CRYPTREC シンポジウム 2012 の開催

2011 年度は、電子政府推奨暗号リストの改訂のために応募暗号技術の第 2 次評価及び現リスト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。

２．８．１．プログラムの概要

日時：2012 年 3 月 9 日（金）10：00～15：45

場所：秋葉原 UDX

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：205 名

表 3.13　プログラム

3 月 9 日(金)		
時間	内容	
10:00	開会挨拶	
10:10	暗号方式委員会報告	応募暗号技術や現リストに掲載されている暗号技術に対する安全性評価の進行状況についての説明
10:40	暗号実装委員会報告	応募暗号技術と現リストに掲載されている暗号技術に対する実装性能評価の進行状況についての説明
11:40	昼休み	
12:40	暗号運用委員会報告	次期電子政府推奨暗号選定にあたっての考え方、並びに選定基準の検討状況についての説明
13:55	休憩	
14:10	ネットワークセキュリティについて 篠田陽一教授（北陸先端科学技術大学院大学）	
14:55	情報セキュリティ人材育成について 今井秀樹教授（中央大学）	
15:40	閉会挨拶	

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 2010 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 の全鍵サイズに対する単一鍵攻撃 ［理論的攻撃、Asiacrypt 2011, Crypto 2011 rump］

電子政府推奨暗号の一つである共通鍵ブロック暗号 AES に対する最初の単一鍵攻撃が Crypto 2011 のランプセッションで公表され、正式な国際発表論文としては Asiacrypt 2011 で発表された。本攻撃では、以前よりハッシュ関数に適用されていた Meet-in-the-Middle 攻撃を改良してブロック暗号に適用した Biclique Attack が利用されている。基本的には鍵回復における総当たり攻撃において、その効率性を高めたものであり、論文では AES 128 に対して $2^{126.1}$、AES 192 に対して $2^{189.7}$、AES 256 に対して $2^{254.4}$ の計算量で鍵回復ができるとしている。AES については、これまで関連鍵攻撃についての報告がなされていたが、関連鍵を必要としない攻撃が発見されたという意味では大きな報告である。一方で、この攻撃による計算量の減少は約 2 ビット分と非常に少ない。会議に参加していた暗号研究者の議論によると、この手法をより発展させて効率的な攻撃に結びつけることは難しく、AES の安全自体への影響はほとんどないと考えられる。Biclique Attack は他のブロック暗号にも適用可能ということであり、今後の動向には注意する必要がある。

3.2 学会等参加記録

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3.1に示す通りである。

表 3.1 国際会議への参加状況

学会名・会議名		開催国・都市	期間
FSE 2011	International Workshop on Fast Software Encryption	デンマーク・コンゲンスリンビー	2/14～2/16
ECRYPTⅡ SKEW 2011	Symmetric Key Encryption Workshop	デンマーク・コンゲンスリンビー	2/16～2/17
PKC 2011	International Conference on Practice and Theory in Public Key Cryptography	イタリア・タオルミナ	3/7～3/9
Eurocrypt 2011	International Conference on the Theory and Applications	エストニア・タリン	5/16～5/19

	of Cryptographic Techniques		
ECRYPTⅡ Hash Workshop	Hash Workshop	エストニア・タリン	5/19～5/20
SAC 2011	Selected Areas in Cryptography	カナダ・トロント	8/11～8/12
Crypto 2011	International Cryptology Conference	米国・サンタバーバラ	8/14～8/18
NIAT 2011	Non-Invasive Attack Testing Workshop	日本・奈良	9/26～9/27
FDTC 2011	Fault Diagnosis and Tolerance in Cryptography	日本・奈良	9/28
CHES 2011	Workshop on Cryptographic Hardware and Embedded Systems	日本・奈良	9/29～10/1
Asiacrypt 2011	International Conference on the Theory and Application of Cryptology and Information Security	韓国・ソウル	12/5～12/8

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について述べる。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

・A Single-Key Attack on the Full GOST Block Cipher [FSE 2011]
ロシア連邦標準 GOST 28147-89 に規定されたブロック暗号に対するフルスペック 32 段に対する単一鍵攻撃に成功した。GOST ブロック暗号は、ブロック長 64 ビット、鍵長 256 ビットて、攻撃コストは 2^{32} 個の既知平文と暗号化 2^{225} 回分の計算量。提案攻撃は、反射(Reflection)攻撃と中間一致攻撃を組み合わせたものである。8 種類の同じ段鍵を 4 回使い回す単純な鍵スケジュールと Feistel 型のデータ攪拌部の組み合わせが攻撃を効率的にしており、2^{-32} の確率で真ん中(16 段目出力)が暗号文と一致する性質が利用されている。GOST ブロック暗号はロシアの他、カザフスタンやウクライナなど旧ソ連数カ国で利用されており、現在、ブロック暗号の国際規格 ISO/IEC 18033-3 への採用が検討されている。

・AES の全鍵サイズに対する単一鍵攻撃 ［理論的攻撃、Asiacrypt 2011, Crypto 2011 rump］
電子政府推奨暗号の一つである共通鍵ブロック暗号 AES に対する最初の単一鍵攻撃が Crypto 2011 のランプセッションで公表され、正式な国際発表論文としては Asiacrypt 2011 で発表された。本攻撃では、以前よりハッシュ関数に適用されていた Meet-in-the-Middle 攻撃を改良してブロック暗号に適用した Biclique Attack が利用されている。基本的には鍵回復における総当たり攻撃において、その効率性を高めたものであり、論文では AES 128 に対して $2^{126.1}$、AES 192 に対して $2^{189.7}$、AES 256 に対して $2^{254.4}$ の計算量で鍵回復ができるとしている。AES については、これまで関連鍵攻撃についての報告がなされていたが、関連鍵を必要としない攻撃が発見されたという意味では大きな報告である。一方で、この攻撃による計算量の減少は約 2 ビット分と非常に少ない。会議に参加していた暗号研究者の議論によると、この手法をより発展させて効率的な攻撃に結びつけることは難しく、AES の安全自体への影響はほとんどないと考えられる。Biclique Attack は他のブロック暗号にも適用可能ということであり、今後の動向には注意する必要がある。

・Automatic Search of Attacks on Round-Reduced AES and Applications [Crypto 2011]
AES に対して、使用できる平文・暗号文組が少数(1 個または 2 個)の現実的な条件で有効な攻撃を自動的に探索する方法を提案し、これを単体の AES の他、AES を使った MAC や故障利用攻撃に適用

し、有効性を示した。探索における入力は、平文と暗号文が満たすべき制約条件から導かれる連立方程式であり、guess-and-determine 攻撃と中間一致攻撃のクラスの中から有効なものを選択する。この方法はバイト単位構造のブロック暗号一般に有効である。AES に対する攻撃では、4 段縮小版に対する選択平文 2 個の攻撃では、従来の記録では、計算複雑度と必要メモリ(単位は、ブロック長=128 ビット)が各々、2^{140} と 1 だったのに対し、今回の自動探索では、各々2^{80} と 2^{80} とメモリを多く消費する分、計算量を削減する結果が得られている。この結果は、AES を使った MAC である、Pelican-MAC、Alpha-MAC、LEX に対する攻撃や、AES に対する故障利用攻撃に適用され、有効性を示している。

3.2.2 ストリーム暗号の解読技術

・Analysis of the Initial and Modified Versions of the Candidate 3GPP Integrity Algorithm 128-EIA3 [SAC 2011]

第 3 世代携帯電話プロジェクト 3GPP の通信規格である LTE では、暗号化アルゴリズム 128-EEA3 と完全性検証アルゴリズム 128-EIA3 が採用されるが、これら 2 つは中国科学院で開発されたストリーム暗号型 ZUC をベースとしている。本論文では、128-EIA3 の最新版の一つ前のバージョンである 2010 年 6 月版に対する偽造攻撃の詳細を初めて明らかにした。この攻撃に対応して改訂された 2011 年 1 月版ではこの攻撃は無効であるものの、初期ベクタ(IV)の再利用には注意を要することが指摘された。

3.2.3 公開鍵暗号の解読技術

・Cryptanalysis of the RSA Subgroup Assumption from TCC 2005 [PKC 2011]

TCC 2005 において提案された、特殊な型の RSA モジュラスを使う暗号プリミティブに対する効率的な攻撃方法が発表された。N=pq=(2p'r+1)(2q's+1)、p,p',q,q'は素数、r,s はランダムの場合、最良の攻撃法の計算量は、O(p')と見積もられていたが、今回の攻撃の計算量は O(√p')となる。この型の RSA モジュラスを使用する場合は、p',q'のビット長に注意しなければならない。

・ On the Correct Use of the Negation Map in the Pollard Rho Method [PKC 2011]

電子署名技術 ECDSA および鍵共有技術 ECDH は、いずれも電子政府推奨暗号リストに掲載されている、楕円曲線を使用した暗号技術である。これらの技術の安全性は ECDLP 問題[1]が解決されれば破綻する（解読される)。ECDLP を最も効率的に解く手法はρ法[2]と呼ばれる解読法であり、有理点群の位数を n とすると√n の計算量オーダーとなることが知られている。イリノイ大学のバーンスタイン教授らは、マイナス写像を利用して、ρ法の実行をこれまでより√2 倍高速化することに成功したと発表した。楕円曲線の有理点のうち、x 座標が等しいものを同一視することにより、有理点群の位数は 1/2 となり、計算量は 1/√2 となることが理論的には知られていたが、実際にはフルーツレスサイクル[3]という問題が起こり、実現することは困難であった。今回の発表はこの問題を解消し、√2 倍の高速化に成功したというものである。この解読法の高速化により、ECDSA および ECDH の安全性をこれまでと同程度に保つためには、鍵長を 1 ビット増やさなければならないこととなる。ただし、現在の解読計算量は、通常用いられる 160 ビット鍵長の場合、2^{80} のオーダーであり、それが $2^{79.5}$ になったとしても、まだ現実的に解読できる計算量ではないため、緊急に対処が必要となるわけではない。

・準同型暗号

CRYPTO 2011 で IBM の Shai Halevi により、準同型暗号のチュートリアルが行われた。例年自由時間となる 2 日目の午後に行われたが、レギュラーセッションと同程度の参加者があり関心の高さをうかがわせた。完全準同型暗号を構成するには、(完全でない) 準同型暗号と再暗号化を用いている。暗号化の際にノイズ情報を付加するが、暗号文の準同型操作によりノイズが大きくなり、ある閾値を超えると復号に失敗するため、完全準同型性を実現するためには、途中で暗号文をリフレッ

---

[1] ECDLP 問題：Elliptic Curve Discrete Logarithm Problem：楕円曲線離散対数問題。有限体上に定義された楕円曲線上の有理点 P および生成元 G が与えられたとき、P=αG を満たす整数αを求める問題。

[2] ρ法：一般の有限群の離散対数問題を解く汎用的な手法。群の位数の√オーダーの計算量となることが知られている。ランダムな点列を生成し衝突が起こることを利用するが、それを図式的に書くとρの形になることに由来する。

[3]フルーツレスサイクル：実の成らない輪。ρ法で衝突が起こっても、解を得ることができない現象の一つ。

シュする必要がある。その際、別の鍵で暗号化し、暗号化したまま復号処理を行う（再暗号化）ため、処理時間が膨大なものとなってしまう。そこで、再暗号化を用いずに完全準同型暗号を構成する研究を進めており、数年後にはアプリケーションによるが実用的になるであろうとの見通しが述べられた。アプリケーションによるとのことであり、どの程度実用的になるかは未知数であるが、数年内に斬新な技術的進歩があることが予想されるため、引き続き動向を注目する必要がある。

3.3 暗号調査ワーキンググループ開催状況

2011 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　2011 年度の主要活動項目

ワーキンググループ名	主査	主要活動項目
リストガイド WG	手塚 悟	暗号技術の専門家並びに暗号実装・運用等に関わる専門家の知見を集約し、鍵共有技術、及び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、情報提供並びに推奨事項を取り纏めて、リストガイドを作成。
計算機性能評価 WG	高木 剛	・2006 年度から現在までに新規のスーパーコンピュータが開発されており、それらをプロットする。 ・予測図によれば、RSA-1024 は世界最速のスーパーコンピュータを占有して計算すると、1 年間で解読される状況に到達したと読める。この解釈で問題がないか、または必要に応じて補足すべき資料を作成すべきかを検討する。 ・予測図の更新に関して、年度単位もしくは新しいスーパーコンピュータの誕生を目途にするなど、更新する機会について検討する。さらに公開の方法についても検討する。

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	2011 年 8 月 5 日	暗号方式委員会活動方針の検討、暗号技術調査ワーキンググループ活動方針の検討、暗号技術評価方法の検討、監視状況報告。
第 2 回	2012 年 2 月 24 日	暗号技術評価結果（案）に係る検討、WG 活動報告、監視情報報告。

(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	2011 年 11 月 14 日	リストガイドの構成、執筆内容、作業方針の検討
第 2 回	2012 年 1 月 24 日	各検討項目に関する検討を元にした議論と執筆内容の確定 今年度作業から判明した課題についての整理

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	2011 年 10 月 6 日	活動計画や作業内容についての審議と了承
第 2 回	2011 年 12 月 21 日	報告内容についての審議と了承

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

2010 年度リストガイド WG の活動を通して抽出された 6 つの課題の中で、特に重要性が高いと考えられる「暗号プロトコルの利用方法に関するリストガイドの作成」を行うこととした。

4.1.2.　委員構成（敬称略、五十音順）

主　査：	手塚 悟	東京工科大学コンピュータサイエンス学科教授
委　員：	岡崎 博之	日本電気株式会社
委　員：	佐野 文彦	東芝ソリューション株式会社
委　員：	寺西 勇	日本電気株式会社
委　員：	花岡 悟一郎	独立行政法人産業技術総合研究所
委　員：	藤崎 英一郎	日本電信電話株式会社
委　員：	藤城 孝宏	株式会社日立製作所横浜研究所
委　員：	松尾 真一郎	独立行政法人情報通信研究機構
委　員：	民田 雅人	株式会社日本レジストリサービス

4.1.3.　活動方針

2011 年度は、暗号プロトコルの利用方法に関するリストガイドの作成を中心に検討を行った。具体的な検討対象技術は以下である。

(1)　電子政府推奨暗号における鍵共有

DH(ANSI X9.42-2003、NIST SP 800-56A)、ECDH(SEC1, NIST SP800-56A)、PSEC-KEM

(2)　一般的な暗号プロトコル

SSL3.0、TLS 1.0/1.1/1.2、IPsec、DNSSEC

4.1.4.　活動概要

2011 年度は 2 回の WG を開催し、活動項目(1)については、各暗号技術の仕様およびセキュリティパラメータについて、暗号監視報告並びに国内外の暗号鍵管理等に関連する標準文書を基に、暗号技術の専門家の知見を集約した。活動項目(2)については、RFC 等で規定

される選択可能な暗号スイートの中から、推奨する暗号スイートについて検討を行う。以上を取り纏めてリストガイドを作成した。

なお、DNSSEC については、RFC 等で規定される仕様や米国 NIST SP 等の文章を調査し、リストガイドへの記載の可否も含めて検討した。

第 1 回リストガイド WG(2011 年 11 月 14 日)では、今年度作成するリストガイドの構成、執筆内容、作業方針について議論を行った。今年度作成するリストガイドは、電子政府推奨暗号の鍵共有（DH、ECDH、PSEC-KEM)、SSL/TLS、IPsec、DNSSEC の 4 つに分けて構成することとした。それぞれの項目に係る執筆内容について、下表に示す。

表 2.1　2011 年度リストガイド執筆内容・検討項目

リストガイド	執筆内容・検討項目
電子政府推奨暗号：鍵共有	・ DH,ECDH のスキーム・アルゴリズムの整理・記載 ・ PSEC-KEM のスキームの追記及びアルゴリズムの記載 ・ FFC/ECC セキュリティパラメータの推奨 ・ FFC/ECC ドメインパラメータの整理 ・ KDF に関する整理
SSL/TLS	・ SSL/TLS の実行環境の整理 ・ 推奨暗号スイート一覧作成 ・ PSK、SRP の取扱い ・ DES/3DES/RC4 に関する取扱い
IPsec	・ 推奨暗号スイートの一覧作成 ・ HMAC-SHA1-96 の取扱い
DNSSEC	・ DNSSEC ソフトウェアの整理 ・ 推奨暗号スイートの一覧作成 ・ ZSK、KSK に係る鍵長の推奨

推奨暗号スイート一覧の作成においては CRYPTREC として推奨していない暗号スイートを除いた一覧を作成することを大方針とし、具体的には以下の場合を除いた暗号スイート一覧を作成することとした。

- 電子政府推奨暗号して指定された暗号プリミティブを用いているが、鍵長等について安全性上問題がある場合
- 電子政府推奨暗号して指定された技術カテゴリであるが、推奨されていない暗号プリミティブを用いている場合
- 電子政府推奨暗号として指定されていない技術カテゴリであり、かつ、安全性に問題がある場合

作業方針として、検討項目について事務局で検討を進めるとともに、執筆内容に沿って

各リストガイドの素案の作成を行い、適時委員のレビュー及び検討・作業を行いながら作業を進めることとなった。

この他、JCMVP 櫻井様より鍵共有に係る暗号モジュール試験方法及び動向について講演いただくとともに、DNSSEC の仕組み及び動向について民田委員より講演をいただいた。

第 2 回リストガイド WG(2012 年 01 月 24 日)では、各検討項目に関する検討結果を示し、議論を行い執筆内容の確定を行った。また、併せて、2011 年度作業から判明した課題について整理・議論を行った（4 節参照)。具体的な議論の内容と結果について以下に示す。

- FFC/ECC　セキュリティパラメータについて
  - 新規システムでの導入も含め、暗号強度 128 ビット相当以上への切り替えを推奨する
    - FFC：|p|=2048、|q|=224
    - ECC：f=224 以上
  - 暗号強度 80 ビット相当については当面（2～3 年）程度の利用を認める
    - FFC：|p|=1024、|q|=160
    - ECC：f=160-223
- FFC/ECC　ドメインパラメータについて
  - FFC のドメインパラメータについては、SP 800-56A、FIPS 180-3 に記載される L=|p|,N=|q|の組を記載する
  - ECC については、NIST が指定する曲線(FIPS 180-3)及び SEC2 で指定される曲線を明示し、情報提供を行う
- SSL/TLS　実行環境について
  - クライアントサイドの実行環境について、OS とブラウザのペアを整理し、SSL/TLS の各バージョンの利用可能性を調査した
  - 結果、TLS 1.1/1.2 を利用できるのは Microsoft 社の Windows 7 + SP 1 環境における Internet Explorer 9 のみであることが判明した
  - OpenSSL 等での TLS 1.1/1.2 対応が進み始めた状況を踏まえ、今後円滑に TLS 1.1/1.2 が利用できるように環境を整備することを付言することとした
- IPsec　HMAC-SHA-1-96 の取扱いについて
  - HMAC-SHA-1-96 については 96 ビット程度の安全性を有していることを確認した
  - 一方で、IPsec においては HMAC-SHA-1-96 をはずして推奨暗号スイート一覧を作成することは、実用上困難であることから、安全性については 96 ビット相当であることを付言することとした
- DNSSEC 推奨鍵長
  - 比較的長期間(13 ヶ月程度)利用する KSK については 2048 ビット相当以上を推奨することとした

- 比較的短期間(1ヶ月程度)利用するZSKについては、実用上の問題も加味し、1024ビット相当以上を推奨することとした。

詳細については、CRYPTREC Webサイト(http://www.cryptrec.go.jp/index.html)に別冊として公開予定である。

4.1.5. 課題等

2011年度の作業業過程において抽出された課題を以下に示す。

■ 電子政府推奨暗号：鍵共有

① 楕円曲線に係る検討
- NIST Curve, SEC2等、各種標準のコンフォーマンスの確認
- CRYPTRECとして推奨する楕円曲線パラメータの策定

② KDFに係る検討
- CRYPTRECとして推奨するKDF Setの策定

③ 素数判定に係る検討
- 素数判定アルゴリズムの利用方法の整理

■ SSL/TLS

④ RC4_128、3DES_EDEに関する取扱い

⑤ RFC等の策定状況に基づく、推奨暗号スイートの定期的なメンテナンス

⑥ サーバサイドTLSの対応状況及び設定方法についての整理・推奨

⑦ PSKに係る鍵管理、SRPの安全性に関する確認

■ IPsec

⑧ RFC等の策定状況に基づく、推奨暗号スイートの定期的なメンテナンス

■ DNSSEC

⑨ ZSK、KSKに係る鍵管理・鍵更新に関するリストガイドの作成

上記課題①～④については、暗号方式委員会において検討・議論頂きたい旨を報告した。その他の項目については、2012年度以降のリストガイドWGにおいて適宜検討を進めたい。

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

RSA-1024 を安全に使える期間の根拠となっている計算機能力進化の予測図は様々な機関において有効に活用されているが、作成が 2006 年度であり、更新が必要となっている。また、一定期間毎に更新されることも求められている。これらの状況を鑑みて、2006 年度に作成されたグラフの見直しと更新作業及び公開の方法について検討を行う。

4.2.2. 委員構成（敬称略、五十音順）

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：下山武司(富士通研究所)

4.2.3. 活動方針

(1) 予測図の見直し

2006 年度から現在までに新規のスーパーコンピュータが開発されており、それらをプロットする。

(2) 2011 年現在における状況の解説

予測図によれば、RSA-1024 は世界最速のスーパーコンピュータを占有して計算すると、1 年間で解読される状況に到達したと読める。この解釈で問題がないか、または必要に応じて補足すべき資料を作成すべきかを検討する。

(3) 更新作業のあり方について

予測図の更新に関して、年度単位もしくは新しいスーパーコンピュータの誕生を目途にするなど、更新する機会について検討する。さらに公開の方法(特に関係省庁などへの周知の仕方)についても検討する。

4.2.4. 活動概要

(1) スケジュール

第 1 回　2011 年 10 月 6 日　　活動計画や作業内容についての審議と了承

第 2 回　2011 年 12 月 21 日　　報告内容についての審議と了承

(2) 近年の研究動向について

2006 年度以降、768 ビット RSA の分解をはじめとして、多くの研究が発表されている。ここに記載した研究はその一部である。

・768 ビット RSA の分解(2009 年 12 月)

[1] T. Kleinjung, K. Aoki, Jens Franke, A. K. Lenstra, E. Thomé, J. W. Bos, P. Gaudry, A. Kruppa, P. L. Montgomery, D. A. Osvik, H. J. J. te Riele, A. Timofeev, P. Zimmermann: Factorization of a 768-Bit RSA Modulus. CRYPTO 2010: 333-350

・多項式選択ステップに関する改良の一例

[2] T. Prest, P. Zimmermann, Non-linear polynomial selection for the number field sieve, Journal of Symbolic Computaion, Vol. 47, Issue 4, 401-409.
http://www.loria.fr/~zimmerma/papers/polyselect.pdf

[3] J. Papadopoulos, High-performance optimization of GNFS polynomials, WCNT 2011.

・フィルタリングステップと線形代数ステップの評価

[4] T. Kleinjung Filtering and the matrix step in NFS, WCNT 2011.

・1024 ビット RSA と 160 ビット楕円曲線暗号の計算量の比較

[5] J. W. Bos, M. E. Kaihara, T. Kleinjung, A. K. Lenstra, P. L. Montgomery, On the Security of 1024-bit RSA and 160-bit Elliptic Curve Cryptography, Cryptology ePrint Archive: Report 2009/389.

・クラウド環境を考慮に入れた鍵長の選択

[6] T. Kleinjung, A.K. Lenstra, D. Page, N.P. Smart, Using the Cloud to Determine Key Strengths, Cryptology ePrint Archive: Report 2011/254.

・オープンソースな一般数体ふるい法の実装例

[7] GGNFS, http://www.math.ttu.edu/~cmonico/software/ggnfs/

(3) 予測図の見直し

CRYPTREC では、CRYPTREC Report 2006[1]において「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」に関する図を公表した。そこでは、計算機性能の将来予測に関して、スーパーコンピュータのベンチマーク結果の 1 位から 500 位を 1993 年から半年毎に集計している Web サイト TOP500.Org[2]に掲載されているデータを利用している。現在までに 2007 年 6 月から 2011 年 11 月までのベンチマーク結果が追加されているので、以前公表し

[1] http://www.cryptrec.go.jp/report/c06_wat_final.pdf
[2] http://www.top500.org/

た図についても下記の通り更新した。また、一般数体ふるい法が利用された過去の素因数分解記録についてもプロットした。

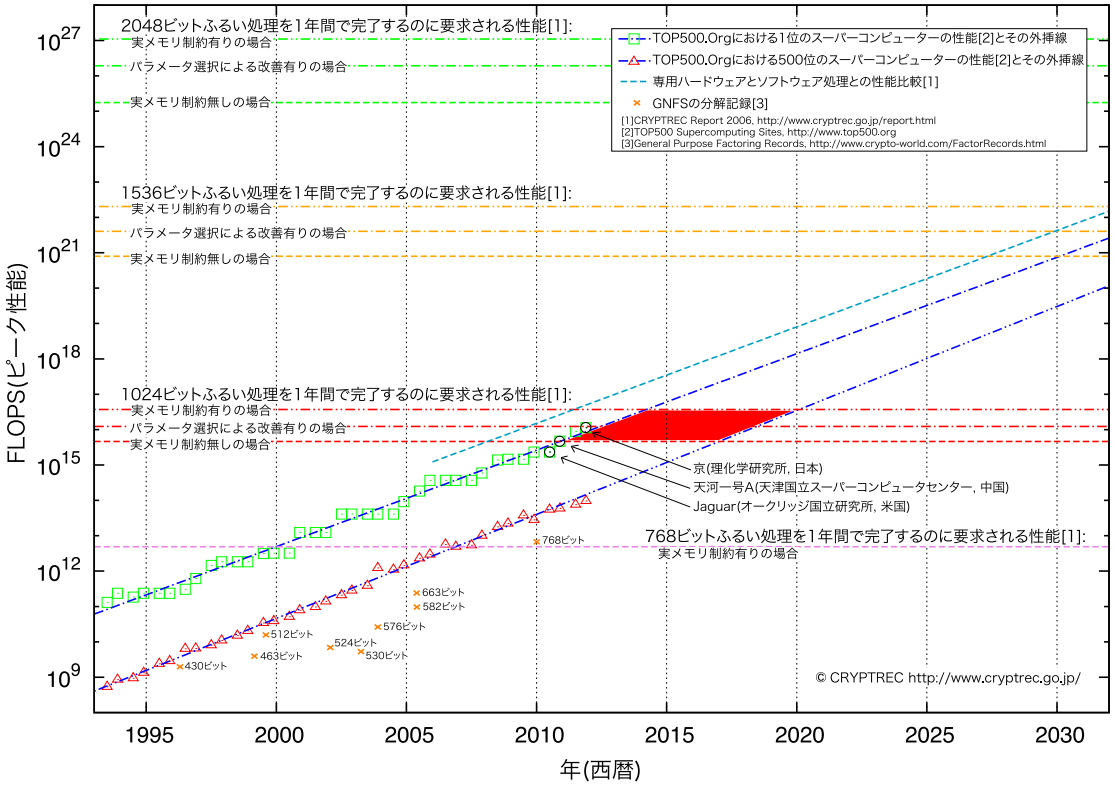


図 4.2：1 年間でふるい処理を完了するのに要求される処理能力の予測(2011 年 12 月更新)

(4) 2011 年現在における状況の解説

(a) ふるい処理の前段階の多項式選択ステップの改善により完了時期が若干前倒しされる可能性はあるものの、過去の予測を大きく変えるものではないため、ふるい処理に要する計算量の推定に関する情報の更新は行わなかった。つまり、図 4.2 の水平方向に描かれているすべての点線（ふるい処理を 1 年間で完了するのに要求される性能）の位置は以前と変わらない。

(b) 2011 年 11 月現在における top 1 のスーパーコンピュータの性能は、1024 ビットふるい処理を 1 年間で完了するのに要する性能における、「実メモリ制約無しの場合」を超え、「パラメータ選択による改善有りの場合」の水準まで近づいてきている。計算機能力の進展が現状の通り達成され続けている限りは、菱形領域内に入った計算機で当該処理を各々の制約条件[3]のもと 1 年間で完了できるとの予測は現在も妥当であると考えられる。つまり、

[3] 制約条件とは、実メモリ制約有り／パラメータ選択改善有り／実メモリ制約無し、のいずれかを指す。

RSA1024 の安全性評価は以前と変わらず、過去における、

CRYPTREC Report 2006 の 18 ページの上から 2 行目：

法パラメータのサイズが 1024 ビットの IFP(n=pq 型素因数分解問題)を 1 年間の計算によって完了させるためには、10^{15}FLOPS から 10^{17}FLOPS の処理能力を持つ計算機が要求され、高性能のスーパーコンピュータが過去の成長率を続けて成長した場合に、そのレベルに到達する時期は、図 2.2 に示すように 2010 年～2020 年の間と推定することができた。

電子署名及び認証業務に関する法律の施行状況に係る検討会報告書（平成 20 年 3 月）[4]の 18 ページの下から 6 行目：

二 RSA1024bit については、概ね 2015 年以降に、危殆化のおそれが高まってくること が示されている(図 2-4)こと。

という報告ついても特に変更を要するものではない。従って、2008 年 4 月に情報セキュリティ政策会議において決定されている「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」[5]は、その記載の通り対応していくことが望ましいと考えられる。

(c) 公表されているデータ[6]に基づいて、過去の RSA 分解記録をプロットした。なお、RSA768 の記録は、CRYPTREC Report 2006 に公表したデータ（参考資料 1 p.14 の表 2.4）における RSA768 に関する推定値（実メモリ制約有りの場合）とほぼ同じである。

(d)暗号の安全性の尺度としてコストが用いられることが多いが、電気代、場所のコストや並列処理に必要となる通信時間が考慮してされているとは限らないことなど、コスト換算に関して様々な前提条件があることに注意が必要である。費用対効果の観点から考えると、RSA-1024 解読のための最も現実的な選択肢は汎用計算機であり、4.2 節の参考文献[6,7]に基づく概算によれば、おおよそ 10 億ドル(以上)のコストが必要となる。独立行政法人理化学研究所と富士通株式会社が共同開発したスーパーコンピュータ「京」の総事業費が約 1120 億円であることを考慮に入れると、この概算はスーパーコンピュータを購入する経費に匹敵しており、「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」に関する図とほぼ整合性が取れていることがわかる。

[4] http://www.soumu.go.jp/menu_news/s-news/2008/080530_4.html
[5] http://www.nisc.go.jp/active/general/res_niscrypt.html
[6] http://www.crypto-world.com/FactorRecords.html

(5) 更新作業のあり方について

予測図に関して、最新のデータが欲しいという要望があるため、公開方法について WG にて検討し、下記の通りの結論を得た。

(1) 公開場所
  (a) CRYPTREC の Web サイト及び CRYPTREC Report に掲載する。
    ※CRYPTREC Report については、その年度の最新データのみ掲載する。
(2) 公開する内容
  「4.2.4. (3) 予測図の見直し」と「4.2.4.(4) 2011 年現在における状況の解説(a)～(c)」
(3) 更新頻度
  (a) TOP500.Org における更新頻度に合わせて、スーパーコンピュータのプロットに関しては原則年 2 回更新を行う。RSA 分解記録が出た場合は、その都度更新する。
  (b) 暗号方式委員会にてメール審議を行い、承認の後に公開／更新を行う。
(4) 予測図の取り扱い
  (a) 予測図は多目的に引用されてきていることから、予測図のみの引用は可能とし、公開の際は、予測図と安全性評価に関する文言とは切り離し可能とする。引用の際は、CRYPTREC 事務局(info@cryptrec.go.jp)への連絡を希望する。

4.2.5. 課題等

次期リスト作成に鑑み、素因数分解問題だけではなく、有限体上の離散対数問題や楕円曲線上の離散対数問題に関する鍵長の選択指針の作成が求められているので、今後検討が必要である。

付録 1

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		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

付録 2

電子政府推奨暗号リスト掲載暗号の問い合わせ先一覧

1. 公開鍵暗号技術

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/PubsFIPS.html>

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/>

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	〒100-0005 東京都千代田区丸の内 1-3-1 東京銀行協会ビルヂング 13F RSA セキュリティ株式会社 ソリューション営業本部 副本部長　齊藤賢一 TEL：03-5222-5210, FAX：03-5222-5270, E-MAIL：ksaito@rsasecurity.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	〒100-0005 東京都千代田区丸の内 1-3-1 東京銀行協会ビルヂング 13F RSA セキュリティ株式会社 ソリューション営業本部 副本部長　齊藤賢一 TEL：03-5222-5210, FAX：03-5222-5270, E-MAIL：ksaito@rsasecurity.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	〒100-0005 東京都千代田区丸の内 1-3-1 東京銀行協会ビルヂング 13F RSA セキュリティ株式会社 ソリューション営業本部 副本部長　齊藤賢一 TEL：03-5222-5210, FAX：03-5222-5270, E-MAIL：ksaito@rsasecurity.com

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	〒100-0005 東京都千代田区丸の内 1-3-1 東京銀行協会ビルヂング 13F RSA セキュリティ株式会社 ソリューション営業本部 副本部長　齊藤賢一 TEL：03-5222-5210, FAX：03-5222-5270, E-MAIL：ksaito@rsasecurity.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 (Revides) において、FCC DH プリミティブとして規定されたもの。 ・参照 URL <http://csrc.nist.gov/publications/PubsSPs.html>

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 (Revides) において、C(2,0,ECC CDH)として規定されたもの。 ・参照 URL <http://csrc.nist.gov/publications/PubsSPs.html>

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. 共通鍵暗号技術

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　第二 IT 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　第三グループマネージャー　吉良賢治 TEL：03-3218-3225　FAX：03-3218-3638 E-Mail：Kira.Kenji@ea.MitsubishiElectric.co.jp

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〈http://csrc.nist.gov/publications/nistpubs/800-67/SP800-67.pdf〉

暗号名	AES
関連情報	仕様 ・FIPS PUB 197, Advanced Encryption Standard (AES) ・参照 URL〈http://csrc.nist.gov/CryptoToolkit/tkencryption.html〉

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 情報流通プラットフォーム研究所 Camellia 問い合わせ窓口　担当 TEL: 0422-59-3456, FAX: 0422-59-4015 E-MAIL: camellia@lab.ntt.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　第二 IT 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-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) 東芝 研究開発センターコンピュータ・ネットワークラボラトリー 主任研究員 秋山浩一郎 TEL：044-549-2156, FAX：044-520-1841 E-MAIL:crypt-info@isl.rdc.toshiba.co.jp

暗号名	SC2000
関連情報	公開ホームページ 和文： http://jp.fujitsu.com/group/labs/techinfo/technote/crypto/sc2000.html 英文: http://jp.fujitsu.com/group/labs/en/techinfo/technote/crypto/sc2000.html
問い合わせ先	富士通株式会社 電子政府推奨暗号 問い合わせ窓口 E-MAIL：crypto-ml@ml.soft.fujitsu.com

暗号名	MUGI
関連情報	公開ホームページ 和文：http://www.hitachi.co.jp/rd/yrl/crypto/mugi/ 英文：http://www.hitachi.com/rd/yrl/crypto/mugi/
問い合わせ先	〒244-8555 神奈川県横浜市戸塚区戸塚町 5030 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： 045-865-9055 E-MAIL： kazuo_matsun.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	〒244-8555 神奈川県横浜市戸塚区戸塚町 5030 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： 045-865-9055 E-MAIL： kazuo_matsun.bz@hitachi.com

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://www.esat.kuleuven.ac.be/~bosselae/ripemd160.html>

暗号名	SHA-1, SHA-256, SHA-384, SHA-512
関連情報	仕様 ・FIPS PUB 186-2, Secure Hash Standard (SHS) ・参照 URL <http://csrc.nist.gov/CryptoToolkit/tkhash.html>

4. 擬似乱数生成系

暗号名	PRNG in ANSI
関連情報	仕様 ・ANSI X9.42-2001, Public Key Cryptography for The Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography ・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	PRNG in ANSI X9.62-1998 Annex A.4
関連情報	仕様 ・ANSI X9.62-1998, Public Key Cryptography for The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA) ・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	PRNG in ANSI X9.63-2001 Annex A.4
関連情報	仕様 ・ANSI X9.63-2001, Public Key Cryptography for The Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography ・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	PRNG for DSA in FIPS PUB 186-2 Appendix 3
関連情報	仕様 ・FIPS PUB 186-2, Digital Signature Standard (DSS) ・参照 URL <http://csrc.nist.gov/CryptoToolkit/tkrng.html>

暗号名	PRNG for general purpose in FIPS PUB 186-2 (+ change notice 1) Appendix 3.1
関連情報	仕様 ・FIPS PUB 186-2, Digital Signature Standard (DSS) ・参照 URL <http://csrc.nist.gov/CryptoToolkit/tkrng.html>

暗号名	**PRNG in FIPS PUB 186-2 (+ change notice 1) revised Appendix 3.1/3.2**
関連情報	仕様 ・FIPS PUB 186-2, Digital Signature Standard (DSS) ・参照 URL <http://csrc.nist.gov/CryptoToolkit/tkrng.html>

付録３　　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
★	On the Correct Use of the Negation Map in the Pollard Rho Method [PKC 2011]	56
☆	Cryptanalysis of the RSA Subgroup Assumption from TCC 2005 [PKC 2011]	56
	Cryptanalysis of Multivariate and Odd-Characteristic HFE Variants [PKC 2011]	57
	Cryptanalysis of Cryptosystems Based on Non-Commutative Skew Polynomials [PKC 2011]	57
	Practical Cryptanalysis of the Identification Scheme Based on the Isomorphism of Polynomial with One Secret Problem [PKC 2011]	57
	Improved Generic Algorithms for Hard Knapsacks [Eurocrypt 2011]	60
★	A Unified Framework for Small Secret Exponent Attack on RSA [SAC 2011]	66
	Analyzing Blockwise Lattice Algorithms using Dynamical Systems [Crypto 2011]	68
☆	Smaller Decoding Exponents: Ball-Collision Decoding [Crypto 2011]	69
	Decoding Random Linear Codes in O(2^{0.054n}) [Asiacrypt 2011]	71
	Lower and Upper Bounds for Deniable Public-Key Encryption [Asiacrypt 2011]	71
★	On the strength comparison of ECC and RSA [SHARCS 2012]	79
	A flexible hardware ECDLP engine in Bluespec [SHARCS 2012]	79
	Solving discrete logarithms in smooth-order groups with CUDA [SHARCS 2012]	79
	Solving quadratic equations with XL on parallel architectures [SHARCS 2012]	80
	ハッシュ関数	**頁**
	Iterative Differentials, Symmetries, and Message Modification in BLAKE-256 [Hash Workshop 2011]	62
	On alignment in Keccak [Hash Workshop 2011]	63
	Recent Advances in MITM Preimage Attacks [Hash Workshop 2011]	63
	Near-Collision Attack on the Step-Reduced Compression of Skein-256 [Hash Workshop 2011]	62
	Boomerang Distinguishers on MD4-Based Hash Functions: First Practical Results on Full 5-Pass HAVAL [SAC 2011]	64
	Improved Analysis of ECHO-256 [SAC 2011]	64
	Provable Chosen-Target-Forced-Midfix Preimage Resistance [SAC 2011]	64
	Cryptographic Analysis of All 4 X 4 - Bit S-Boxes [SAC 2011]	64
	How to Improve Rebound Attacks [Crypto 2011]	67
	The preimage security of double-block-length compression functions [Asiacrypt 2011]	73
☆	Rebound Attack on JH42 [Asiacrypt 2011]	73
☆	Second-Order Differential Collisions for Reduced SHA-256 [Asiacrypt 2011]	73
★	Finding SHA-2 Characteristics: Searching Through a Minefield of Contradictions [Asiacrypt 2011]	73
	Cryptanalysis of ARMADILLO2 [Asiacrypt 2011]	73
	Practical Collisions in Bound-Reduced Keccak [Asiacrypt 2011 rump]	76

1.2. PKC 2011 の発表

1.2.1. PKC 2011 の発表(1 日目)

On the Correct Use of the Negation Map in the Pollard Rho Method [PKC 2011]
Daniel J. Bernstein, Tanja Lange, Peter Schwabe

電子署名技術 ECDSA および鍵共有技術 ECDH は、いずれも電子政府推奨暗号リストに掲載されている、楕円曲線を使用した暗号技術である。これらの技術の安全性は ECDLP[1]問題が解決されれば破綻する(解読される)。ECDLP を最も効率的に解く手法はρ法[2]と呼ばれる解読法であり、有理点群の位数をｎとすると√ｎの計算量オーダーとなることが知られている。イリノイ大学のバーンスタイン教授らは、マイナス写像を利用して、ρ法の実行をこれまでより√2 倍高速化することに成功したと発表した。楕円曲線の有理点のうち、x 座標が等しいものを同一視することにより、有理点群の位数は 1/2 となり、計算量は 1/√2 となることが理論的には知られていたが、実際にはフルーツレスサイクル[3]という問題が起こり、実現することは困難であった。今回の発表はこの問題を解消し、√2 倍の高速化に成功したというものである。この解読法の高速化により、ECDSA および ECDH の安全性をこれまでと同程度に保つためには、鍵長を 1 ビット増やさなければならないこととなる。ただし、現在の解読計算量は、通常用いられる 160 ビット鍵長の場合、2^{80} のオーダーであり、それが $2^{79.5}$ になったとしても、まだ現実的に解読できる計算量ではないため、緊急に対処が必要となるわけではない。

Cryptanalysis of the RSA Subgroup Assumption from TCC 2005 [PKC 2011]
Jean-Sebastien Coron, Antoine Joux, Avradip Mandal, David Naccache, Mehdi Tibouchi

TCC 2005 において提案された、特殊な型の RSA モジュラスを使う暗号プリミティブに対する効率的な攻撃方法が発表された。N=pq=(2p'r+1)(2q's+1)、p,p',q,q'は素数、r,s はランダムの場合、最良の攻撃法の計算量は、O(p')と見積もられていたが、今回の攻撃の計算量は O(√p')となる。この型の RSA モジュラスを使用する場合は、p',q'のビット長に注意しなければならない。

---

[1] ECDLP：Elliptic Curve Discrete Logarithm Problem：楕円曲線離散対数問題。有限体上に定義された楕円曲線上の有理点 P および生成元 G が与えられたとき、P=αG を満たす整数αを求める問題。

[2] ρ法：一般の有限群の離散対数問題を解く汎用的な手法。群の位数の√オーダーの計算量となることが知られている。ランダムな点列を生成し衝突が起こることを利用するが、それを図式的に書くとρの形になることに由来する。

[3] フルーツレスサイクル：実の成らない輪。ρ法で衝突が起こっても、解を得ることができない現象の一つ。

1.2.2. PKC 2011 の発表（3 日目）

Cryptanalysis of Multivariate and Odd-Characteristic HFE Variants [PKC 2011]
Luk Bettale, Jean-Charles Faugre, Ludovic Perret

HFEの変形(多変数・奇標数)の安全性を解析する。Kipnis-Shamir鍵回復攻撃の改良を示し、更に多重HFEへの攻撃に拡張する。公開鍵に関する直接的なMiniRank問題を解くことに帰着し、Chen, Chen, Ding, Werner, Yang による256ビット安全性を持つとされるパラメーターを9日で解読した。

Cryptanalysis of Cryptosystems Based on Non-Commutative Skew Polynomials [PKC 2011]
Vivien Dubois, Jean-Gabriel Kammerer 非可換なねじれ多項式に基づいた暗号の安全性解析を行う。本論文では、ねじれ多項式に基づいたDiffie-Hellman問題に対しては、非常に効率的な攻撃が存在することを示す。

Practical Cryptanalysis of the Identification Scheme Based on the Isomorphism of Polynomial with One Secret Problem [PKC 2011]
Charles Bouillaguet, Jean-Charles Faugre, Pierre-Alain Fouque, Ludovic Perret

CRYPTO 1996でPatarinにより提案された認証スキームに対する解読を示す。このスキームは、1つの秘密を持つ多項式の同型問題(IP1S: Isomorphism of Polynomial with One Secret)の困難性に基づく。2つの決定的な攻撃アルゴリズムを示し、2次のインスタンスの大部分を多項式時間で解読できることを示す。Patarinによる2次のパラメータはすべて数秒で解読され、3次のパラメータもCPU-月以内に解読された。

1.3. Eurocrypt 2011 の発表

1.3.1. Eurocrypt 2011 の発表(1 日目)

On Ideal Lattices and Learning with Errors over Rings [Eurocrypt 2011]
V. Lyubashevsky, C. Peikert, and O. Regev

LWE(Learning With Errors)問題とは、小さなノイズにより摂動を与えられたランダムな線型方程式を、真に一様ランダムなものと見分ける問題であるが、最悪ケースの格子問題と同程度に困難であることが示されており、多くの暗号応用の基礎となっている。しかしながらこれらの応用は、LWE を用いる際の 2 次のオーバーヘッドのために効率的ではなく、更なる代数的構造を利用することにより効率的にできるかどうかは未解決問題であった。本論文では、R-LWE(Ring-LWE)という新たな代数的問題を導入することにより、この問題を肯定的に解決した。特に、R-LWE 分布は、イデアル格子の最悪ケース問題が多項式量子アルゴリズムに対して困難であると仮定すれば、擬ランダムであることを示した。これにより、効率的な帰着を持つ初めての実用的な公開鍵格子暗号を提示し、他の LWE を用いる暗号も効率的にすることができ、LWE ベースとしては知られていなかった R-LWE の代数構造に基づく新たな暗号応用も期待できる。

1.3.2. Eurocrypt 2011 の発表(2 日目)

New Generic Algorithms for Hard Knapsacks [Eurocrypt 2011]
N. Howgrave-Graham and A. Joux(米国、フランス)

ナップザック問題では、密度が低いとき、格子ベースの低密度攻撃法という効率的な解法が存在する。この低密度攻撃を避けるために、密度を 1 に近く設定したものに対しては、31 年前に提案されたSchroeppelとShamirのアルゴリズムがある。要素数をnとすると、このアルゴリズムの計算量は$O^{\sim}(2^{n}/2)$、必要なメモリは $O^{\sim}(2^{n}/4)$であった。本論文では、このアルゴリズムを改良した2種類のアルゴリズムを提案し、各々の計算量が $O^{\sim}(2^{0.385n})$と $O^{\sim}(2^{0.3113n})$になることを示し、さらに新規の攻撃法を実装してその有効性を実証した。

1.3.3. Eurocrypt 2011 の発表(3 日目)

On Linear Hulls, Statistical Saturation Attacks, PRESENT and a Cryptanalysis of PUFFIN [Eurocrypt 2011]
Gregor Leander

linear hull は、線形解読法に対する安全性評価の尺度の一つであるが、その値は鍵に依存し、安全性はその平均値によって議論される。本論文では、平均値はしばしば無限大になるので安全性指標と適切でなく、median を利用することを提案している。
128 ビット鍵のブロック暗号 PUFFIN(フルラウンド)に提案の評価法を適用したところ、少なくとも鍵空間の 1/4 に対し、最終段の段鍵の 4 ビットが計算複雑度 2^{58} で求めることが可能であることを示した。
同じ解析法をブロック暗号 PRESENT に適用したところ、PRESENT の仕様に従う S-box と拡散層(線形変換)を使った場合の、線形解読に対する安全性が証明できた。

Statistical Attacks on RC4: Distinguishing WPA [Eurocrypt 2011]
Pouyan Sepehrdad, Serge Vaudenay and Martin Vuagnoux

RC4 の解析によって得られた偏り(biases)の集合を利用して、ツールをいくつか構成し、WEP と WPA に対する攻撃に適用した。WEP に対する最善の戦略では、最初の平文バイトが既知の 4000 パケットで破れることを示した。WPA に対する攻撃では、最初に 2^{40} 個のパケットを使って、計算複雑度 2^{43} で利得(advantage)が 0.5 の識別子(distinguisher)を構成した。さらに、この識別子を利用して、必要パケット数 2^{38}、計算複雑度 2^{96} で 128 ビットの一次鍵を復元できることを理論的に示した。

Improved Generic Algorithms for Hard Knapsacks [Eurocrypt 2011]
Anja Becker, Jean-Sebastien Coron and Antoine Joux

Eurocrypt 2010 において、Howhgrave-Graham と Joux は、密度が 1 に近い場合のハード・ナップザック問題を時間複雑度 $O\tilde{}(2^{0.337n})$、$O\tilde{}(2^{0.256n})$で解く方法を示した。これは、1981 年に Shamir-Schroeppel が示した解法の記録を 30 年ぶりに更新するものであった。本論文では、計算複雑度とメモリ複雑度の各々に最適化した 2 種類の攻撃を示した。計算複雑度を最小化した攻撃では、計算複雑度・メモリ複雑度ともに $O\tilde{}(2^{0.291n})$を実現した。メモリ複雑度を最小化した攻撃では、計算複雑度 $O\tilde{}(1)$、メモリ複雑度 $O\tilde{}(2^{0.72n})$を実現した。さらに、小型の数値実験によって提案方式の有効性を確認した。

1.3.4. Eurocrypt 2011 の発表(4 日目)

Multi-Property-Preserving Domain Extension using Polynomial-Based Modes of Operation [Eurocrypt 2011]
J. Lee and J. Steinberger(韓国、中国)

MD 型変換は使用する圧縮関数の衝突発券困難性が毀損すると、長メッセージに対する第2原像攻撃耐性などが有効になるなどの欠点がある。この欠点を解消するために、S.Lucks は Asiacrypt 2005 で、内部状態のサイズを大きくする方法を提案した。Yasuda は Eurocrypt 2009 で Lucks が提案した二重パイプ構造の安全性を厳密に評価し、O(n5/6)回までの質問に対して偽造不可能性が保てることを証明した。
本論文では、複数の性質を維持する領域拡張を多項式を利用した効率のよい新規の二重パイプの動作モードで実現した。この領域拡張は、MAC、擬似ランダム関数、擬似ランダム・オラクルとして使用できる。提案方式は、Stam が Crypto 2008, FSE 2009 で提案した多項式ベースの圧縮関数を使用しており、Lucks の方式より2倍高速で、安全性は同程度である。
圧縮関数とハッシュ値のサイズが n ビットとしたとき、提案法の圧縮関数は、2種類の 3n ビット入力、n ビット出力の関数 f_1、f_2を使い、$H[f_1,f_2]$と表される。f_1は繰り返し連鎖処理で使用し、f_2は終了処理に使用する。$H[f_1,f_2]$は、次の性質を持つ。

1. f_1とf_2が偽造不能なら、$O(2^n/n)$回までの質問に対し、偽造不能
2. f_1が偽造不能でf_2が擬似ランダムなら、$O(2^n/n)$回までの質問に対し、擬似ランダム
3. f_1とf_2が公開ランダム関数なら、$O(2^{2n/3})$回までの質問に対し、ランダム関数と識別不可能

1.4. Hash workshop の発表

1.4.1. Hash workshop の発表（1 日目）

Near-Collision Attack on the Step-Reduced Compression of Skein-256 [Hash Workshop 2011]
Hongbo Yu, Jiazhe Chen, Keting Jia and Xiaoyun Wang

SHA-3 最終候補の一つ Skein-256 の 32 段縮小版(仕様では 72 段)に対し、ハッシュ値 256 ビットのうち 51 ビット違いの近衝突(near-collision)を計算複雑度 2^{105} で発見する半自由スタートの攻撃法を示した。この攻撃では、ARX 型ハッシュ関数に対するリバウンド解析の手法を利用して、短い差分経路を2つ作り、これらを接続することで 32 段の差分経路を得た。

Iterative Differentials, Symmetries, and Message Modification in BLAKE-256 [Hash Workshop 2011]
Orr Dunkelman and Dmitry Khovratovich

SHA-3 最終候補の一つ BLAKE-256 の縮小版にリバウンド過程を含む差分解読を適用し、圧縮関数の衝突ペア発見と識別子生成を行った。圧縮関数の衝突ペア発見は 3 段縮小版に対するもので、計算複雑度は 2^{60}。識別子は 6 段まで全数探索より計算量が少なく、4 段縮小版で 2^{192}、6 段縮小版で 2^{456} である。なお、フルスペックの BLAKE-256 は 14 段。従来の BLAKE-256 に対する攻撃では、局所衝突やブーメラン攻撃が利用されているが、本論文では利用せず、オーソドックスな差分解読が利用されている。

1.4.2. Hash workshop の発表（2 日目）

On alignment in Keccak [Hash Workshop 2011]
Guido Bertoni, Joan Daemen, Michael Peeters and Gilles Van Assche

AES の truncated 差分では、S-box 1 個だけ活性(active)のパターンが、次の層で 4 個活性、次々層で 16 個全部活性となる。このように活性パターンが容易に予想できることを強い alignment とし、逆に活性パターンの伝搬が予測しづらいことを弱い alignment とすることを提案した。強い alignment はリバウンド攻撃の適用が容易となる目安となる。SHA-3 最終候補の一つ Keccak の alignment を調べたところ、弱いことが明らかになった。これはリバウンド攻撃の適用は容易でないことを意味するが、適用が不可能であることを証明しているわけではない。

Recent Advances in MITM Preimage Attacks [Hash Workshop 2011]
Yu Sasaki

中間一致を利用した原像攻撃に関する招待講演。中間一致攻撃はブロック暗号に対する攻撃法として以前から知られていたが、近年、ハッシュ関数の解析に適用され、目覚しい進展を見せている。講演は Triple DES による基本例の説明、MD5 や RIPEMD など広く利用されているハッシュ関数への攻撃例、近年新規提案が盛んな軽量ブロック暗号への攻撃例が紹介された。

1.5. SAC 2011 の発表

1.5.1. SAC 2011 の発表(1 日目)

Boomerang Distinguishers on MD4-Based Hash Functions: First Practical Results on Full 5-Pass HAVAL [SAC 2011]
Yu Sasaki

5-Pass HAVAL は MD4 構造に基づいて設計されたハッシュ関数で、連鎖変数とハッシュ値のサイズは 256 ビットであり、ステップ数は 96 である。圧縮関数計算 2^128 回分の計算で衝突攻撃が可能であることが理論的に示されている。本論文では、ブーメラン攻撃を利用して、4-sum の識別子(distinguisher)を構成し、計算量は圧縮関数計算で約 2^11 回分と評価し、計算機実験でその有効性を確認した。この結果は、フルスペックの 5-Pass HAVAL に対する攻撃であり、かつ、計算量が現実的なものとしては初めてのものである。

Improved Analysis of ECHO-256 [SAC 2011]
Jeremy Jean, Maria Naya-Plasencia, and Martin Schlaffer

ECHO-256 は AES に基づいて設計されたハッシュ関数で、SHA-3 コンペの第 2 ラウンド候補だった。本論文では、複数の inbound 経路を利用するリバウンド攻撃を改良することにより、利用可能な段数を衝突攻撃では 8 段中 4 段から 5 段に、また識別子(distinguisher)では 7 段まで伸ばした。5 段の衝突攻撃に必要な計算量は圧縮関数計算 2^{112} 回分、7 段の識別子では 2^{193} 回分である。

Provable Chosen-Target-Forced-Midfix Preimage Resistance [SAC 2011]
Elena Andreeva, and Bart Mennink

Kelsey-Kohno が Eurocrypt 2006 で発表した herding attack に関する安全性概念を一般化して、いくつかのハッシュ関数について、証明可能安全性を研究した。まず、オリジナルの chosen-target-forced-prefix では最初の部分を固定(prefix)していたのを一般化して、固定箇所を任意(midfix)とする chosen-target-forced-midfix (CTFM)とした。また、安全性を解析するハッシュ関数の入力には salt を含めることにした。以上の準備の後、narrow-pipe Merkle-Damgard 型や HAIFA 型に対する証明可能安全性と、Kelsey-Kohno attack が最善であることを証明した。ただし、salt をなくすと証明可能安全性は成立しなくなり、広いクラスの narrow-pipe MD 型ハッシュ関数にたいする herding attack が可能になる。

Cryptographic Analysis of All 4 X 4 - Bit S-Boxes [SAC 2011]
Markku-Juhani O. Saarinen

4 ビット入出力の S-box は全部で 16!個あり、WAIFI 2007 で Leander と Poschmann がアフィン同値クラス(線形同値クラス, LE)を調べ尽くしている。LE が同じだと、差分確率上限と線形確率上限は同じであるが、分岐数、代数的性質、回路での複雑度は必ずしも同じでない場合がある。本論文では、入出力ビットの置換と入出力ビットへの排他的論理和(XOR)関する同値類(置換同値クラス, PE)を導入し、PE が同じであれば、上記の性質も同じであることを示すとともに、暗号学的に最良である"golden" set of S-boxes を選別した。

Proof of Empirical RC4 Biases and New Key Correlations [SAC 2011]
Sourav Sen Gupta, Subhamoy Maitra, Goutam Paul, and Santanu Sarkar

RC4 が生成する鍵ストリームの初期において、大きな偏りが実験的に確認されていた。本論文では、この偏りが生じるメカニズムを初めて理論的に示すとともに、その理論に基づき新たな鍵ビット間に生じる高い相関を発見した。

Cryptanalysis of Reduced Versions of the Camellia Block Cipher [SAC 2011]

Jiqiang Lu, Yongzhuang Wei, Jongsung Kim, and Pierre-Alain Fouque

L.Duo らによる ICICS 2007 の論文では、SQUARE 型攻撃で Camellia-128 を 16 段中 9 段まで、FL/FL^{-1}関数なしの Camellia-256 を 24 段中 12 段まで攻撃可能と評価した。本論文では、L.Duo らの論文の攻撃における誤りを指摘するとともに、鍵候補を早期に棄却する方法と鍵スケジュールの観察に基づいた不能差分攻撃を適用することによって、FL/FL^-1 関数あり Camellia-128 の 10 段、FL/FL^{-1}関数あり Camellia-192 の 11 段、FL/FL^{-1}関数なし Camellia-192 の 14 段、FL/FL^{-1}関数なし Camellia-256 の 16 段が攻撃可能であることを理論的に示した。

Combined Differential and Linear Cryptanalysis of Reduced-Round PRINTcipher [SAC 2011]
Ferhat Karakoc, Huseyin Demirci, A. Emre Harmanci

PRINTcipher の差分特性確率の上限は設計者によって評価され、差分解読に対して十分安全としている。本論文では、一部の弱鍵に対してこの上限値を大きく上回る特性確率が存在する性質を利用し、PRINTcipher-48 について、48 段中 29 段まで 4.54%の弱鍵で攻撃可能、31 段まで 0.036%の弱鍵で攻撃可能であることを示した。本攻撃は differential-linear 攻撃ではなく、弱鍵に対する差分特性確率の大幅増加を評価するために線形解読を使用するものである。

Practical Attack on the Full MMB Block Cipher [SAC 2011]
Keting Jia, Jiazhe Chen, Meiqin Wang, and Xiaoyun Wang

MMB 暗号(Modular Multiplication based Block Cipher)は IDEA に代わるブロック暗号として設計されたもので、ブロック長と鍵長はともに 128 ビットである。本論文では、5 段のサンドイッチ識別子(distinguisher)を利用してフルラウンドの 6 段 MMB 暗号が確率 1 で攻撃可能であることを示した。平文と暗号文を適応的に選択できる場合、各々2^39 個ずつ利用すると MMD 暗号化 2^40 回分の計算で攻撃可能である。また、選択平文攻撃だと、2^66.5 個の平文・暗号文組、MMD 暗号化 2^66.5 回分の計算で攻撃可能である。サンドイッチ識別子はブーメラン識別子の拡張であり、ブーメラン識別子を構成する 2 つの部分暗号の間にもう一つ部分暗号を挿入することでサンドイッチ識別子を作る。

Conditional Differential Cryptanalysis of Trivium and KATAN [SAC 2011]
Simon Knellwolf, Willi Meier, and Maria Naya-Plasencia

ストリーム暗号 Trivium とブロック暗号 KATAN は、非線形フィードバックシフトレジスタ(NLFSR)に基づいて設計されている。本論文では、Knellwolf らが Asiacrypt 2010 で提案した条件付き差分解析攻撃を改良したもの適用した。Trivium では、弱鍵ならば 1152 段中 961 段までの識別攻撃が可能であることを示した。また、KATAN 暗号ファミリーはフルラウンドで 254 段だが、KATAN32 で 120 段まで、KATAN48 で 103 段まで、KATAN64 で 90 段まで、攻撃可能であることが示された。

1.5.2. SAC 2011 の発表(2 日目)

Some Instant- and Practical-Time Related-Key Attacks on KTANTAN32/48/64 [SAC 2011]
Martin Agren

KTANTAN 暗号ファミリーはハードウェア向けの軽量暗号として、KATAN 暗号ファミリーとともに CHES 2009 で発表された。Bogdanov と Rechberger は SAC 2010 で、鍵スケジュールの欠陥に着目した KATAN 暗号に対する match-in-the-middle 攻撃を提案した。本論文ではこの研究を踏まえた上で、最も弱い鍵ビットの絞り込み、いくつかの関連鍵攻撃を開発した。KTANTAN32 に対しては、関連鍵攻撃で 80 ビット鍵全部を暗号化 $2^{28.44}$ 回分の計算で求めることに成功した。

Analysis of the Initial and Modified Versions of the Candidate 3GPP Integrity Algorithm 128-EIA3 [SAC 2011]
Thomas Fuhr, Henri Gilbert, Jean-Rene Reinhard, Marion Videau

第 3 世代携帯電話プロジェクト 3GPP の通信規格である LTE では、暗号化アルゴリズム 128-EEA3 と完全性検証アルゴリズム 128-EIA3 が採用されるが、これら 2 つは中国科学院で開発されたストリーム暗号型 ZUC をベースとしている。本論文では、128-EIA3 の最新版の一つ前のバージョンである 2010 年 6 月版に対する偽造攻撃の詳細を初めて明らかにした。この攻撃に対応して改訂された 2011 年 1 月版ではこの攻撃は無効であるものの、初期ベクタ(IV)の再利用には注意を要することが指摘された。

New Insights on Impossible Differential Cryptanalysis [SAC 2011]
Charles Bouillaguet, Orr Dunkelman, Pierre-Alain Fouque, and Gaetan Leurent

不能差分攻撃によって、5 段の Feistel 暗号が攻撃可能であることが知られている。本論文では、一般化 Feistel 暗号に対する不能差分を設計する新しいアプローチを示し、それによって従来より 1 段またはそれ以上、適用可能段数を伸ばすことに成功した。さらに、ラウンド関数が全単射でなくても攻撃可能な例をいくつか示した。

A Unified Framework for Small Secret Exponent Attack on RSA [SAC 2011]
Noboru Kunihiro, Naoyuki Shinohara, and Tetsuya Izu

Boneh と Durfee は、RSA 暗号でモジュロを N、秘密鍵指数を d とすると、$d \leqq N^{0.292}$ が満たされるとき、格子に基づく攻撃が可能であることを示した。この方法では使われる格子がフルランクでないので、解析は難しかった。Bloemer と May は対案としてフルランクの格子を使った方法を提案したが、攻撃の適用可能範囲は $d \leqq N^{0.290}$ と悪くなり、証明も難しいものであった。本論文では、まず、unravelled linearization technique を使って、$d \leqq N^{0.290}$ の場合のより簡潔な証明を与えた。次に上記の 2 つの攻撃法を特殊な例として含む格子を設計する統一的な枠組みを作った。さらに、この統一的枠組の範囲内で、$d \leqq N^{0.292}$ が最適であることを証明した。

1.6. Crypto 2011 の発表

1.6.1. Crypto 2011 の発表(1 日目)

Automatic Search of Attacks on Round-Reduced AES and Applications [Crypto 2011]
Charles Bouillaguet, Patrick Derbez, and Pierre-Alain Fouque

AES に対して、使用できる平文・暗号文組が少数(1 個または 2 個)の現実的な条件で有効な攻撃を自動的に探索する方法を提案し、これを単体の AES の他、AES を使った MAC や故障利用攻撃に適用し、有効性を示した。探索における入力は、平文と暗号文が満たすべき制約条件から導かれる連立方程式であり、guess-and-determine 攻撃と中間一致攻撃のクラスの中から有効なものを選択する。この方法はバイト単位構造のブロック暗号一般に有効である。AES に対する攻撃では、4 段縮小版に対する選択平文 2 個の攻撃では、従来の記録では、計算複雑度と必要メモリ(単位は、ブロック長=128 ビット)が各々、2^{140} と 1 だったのに対し、今回の自動探索では、各々2^{80}と2^{80}とメモリを多く消費する分、計算量を削減する結果が得られている。この結果は、AES を使った MAC である、Pelican-MAC、Alpha-MAC、LEX に対する攻撃や、AES に対する故障利用攻撃に適用され、有効性を示している。

How to Improve Rebound Attacks [Crypto 2011]
Maria Naya-Plasencia

ハッシュ関数に対する有効な攻撃法であるリバウンド攻撃において、ほとんど攻撃で利用され、かつ、ボトルネックになっている操作の効率を改善する方法を開発し、いくつかのハッシュ関数について従来の適用段数を伸ばすことに成功した。ここで注目した操作は、大きなリストを結合するものである。SHA-3 の最終 5 候補に適用した所、段数と攻撃条件が同じ場合、計算量と必要メモリ量のどちらか一方または両方が、従来記録より少なくて済むという評価結果を得ている。

A Cryptanalysis of PRINTcipher: The Invariant Subspace Attack [Crypto 2011]
Gregor Leander, Mohamed Ahmed Abdelraheem, Hoda AlKhzaimi, and Erik Zenner

PRINTcipher は CHES 2010 で発表された SPN 型の軽量ブロック暗号であり、ブロック長、鍵長、段数が各々48 ビット、80 ビット、48 段の PRINTcipher-48 と、96 ビット、160 ビット、96 段の PRINTcipher-96 がある。軽量化のため各段の拡大鍵(段鍵)は同じであり、安全性向上のために段依存定数が加算される。本論文では、ある条件を満たす弱鍵では、データが属する剰余類が各段の変換に対して不変である性質を示し、これを利用することでフルスペックの PRINTcipher が攻撃できることを示した。弱鍵は PRINTcipher-48 と PRINTcipher-96 の各々に対し、2^{80}個中2^{52}個、2^{160}個中2^{104}個であり、5 個の選択平文・暗号文組で攻撃が可能である。既知平文攻撃で必要な平文・暗号文組数は、各々、$5*2^{16}$個と$5*2^{32}$個である。本論文のアイデアを利用して、truncated 差分攻撃を構成することも可能である。

1.6.2. Crypto 2011 の発表(3 日目)

Analyzing Blockwise Lattice Algorithms using Dynamical Systems [Crypto 2011]
Guillaume Hanrot, Xavier Pujol, and Damien Stehle

格子基底縮小(lattice reduction)は、格子暗号に対する重要な要素であり、最強であるものの実用的でないHKZ縮小と弱いものの計算が速いLLL縮小という両極端の２種類が知られている。両者の中間に位置し、適切なトレードオフを実現するアルゴリズム候補として、FCT '91 で Schnorr と Euchner が導入した BKZ が、時間と品質のバランスが取れた最良のものに見える。しかしながら、今まで BKZ の計算複雑度の上限は知られておらず、Gama と Nguyen は Eurocrypt 2008 で計算機実験で、格子次元数に対し指数関数的に増加することを観察している。本論文では、優れた品質を保ったまま、アルゴリズムの完了よりかなり手前で終了することが可能であることを示した。

1.6.3. Crypto 2011 の発表(4 日目)

Smaller Decoding Exponents: Ball-Collision Decoding [Crypto 2011]
Daniel J. Bernstein, Tanja Lange, and Christiane Peters

セキュリティ・レベルが 2^b と想定され(conjectured)、暗号化・復号の計算時間が $b^{2+o(1)}$ に抑えられる公開鍵暗号は少ないが、McEliece 符号ベース暗号はこの条件を満たす。既存の McEliece 暗号に対する最も効果的な攻撃法は、generic coding attack で、MacEliece の隠れバイナリ・ゴッパ符号をランダムな線型符号として扱った Stern のアルゴリズムである 。本論文では、ball-collision decoding を導入し、Stern のアルゴリズムと比較して n の指数倍の高速化を達成した。ここで、n はゴッパ符号の符号長である。

1.6.4. Crypto 2011 rump の発表

Biclique cryptanalysis of the full AES [Crypto 2011 rump session]
Andrey Bogdanov, Dmitry Khovratovich, and Christian Rechberger

フルスペックの AES に対する初の単一鍵攻撃の発表。使用した攻撃法である biclique は、ハッシュ関数用に開発された中間一致攻撃の一種である。3 種類の鍵長 128 ビット、192 ビット、256 ビットに対する攻撃の計算量が、各々鍵全数探索よりも約 2 ビット分少ないという見積もりを示した。本論文は e-Print の他、Asiacrypt 2011 で発表された。

1.7. Asiacrypt 2011 の発表

1.7.1. Asiacrypt 2011 の発表(1 日目)

BKZ 2.0 : Better Lattice Security Estimates [Asiacrypt 2011]
Yuanmi Chen and Pong Q. Nguyen

近年その応用が多数出てきている lattice ベースの方式などの安全性評価に用いられる高次元 lattice の帰着アルゴリズムとして実用的とされているものに Schnorr-Euchner の BKZ がある. 従来示されている lattice を用いた暗号システムの安全性評価には, この BKZ についての NTL の古くからの実装法に基づいている. しかし, 近年の lattice に関する実装技術の進展などにより, NTL の実装はもはやオプティマルなものではないと言わざるを得ない. この問題に対し, 近年示された Gama-Nguyen-Regev の BKZ2.0 の実装のように新たに推定する手段を持ち始めている. 本稿では, BKZ の(blocksize が 50 以上の)高次元での挙動をシミュレートできるシミュレーションアルゴリズムを提案した. 本アルゴリズムを用いることにより出力推定値の信頼性や running time をより正確に見積もることができる. 提案アルゴリズムが有効である一例として, NTRUSign を挙げ, NTRUSign では少なくとも 93 ビット security を提供するとされていたが, 実際には key-recovery lattice attacks に対して, せいぜい 65 ビット security しか提供しないことを示した.

Structure Preserving CCA Secure Encryption and Applications [Asiacrypt 2011]
Jan Camenisch, Kristiyan Hralambiev, Markulf Kohlweiss, Jorn Lapon, and Vincent Naessens

群構造維持可能な暗号アルゴリズムの提案. (Structure Preserving Encryption Alrotighm) 能動的選択暗号文攻撃に対して安全性を証明できる. 構成にはハッシュ関数やビット演算なども用いない. Algebraic 演算のみで構成出来る. このような群構造維持が可能な暗号プリミティブは, より複雑な暗号プロトコルのモジュール的構成に有効である. 本提案方式の具体的なアプリケーションとして, two party protocol や Oblivious TTP(Trusted Third parties) などを示した.

Decoding Random Linear Codes in O(2^{0.054n}) [Asiacrypt 2011]
Alexander May, Alexander Meurer, and Enrico Thomae

ランダム線型符号を復号するアルゴリズムで漸近的振舞いが最良のアルゴリズムは長い間、Stern による情報セット復号の変形版の一つが達成した $\tilde{O}(2^{0.05563n})$であった。本論文では、これを上回る $\tilde{O}(2^{0.05558n})$を達成した。利用した方法は球体衝突復号(Ball-collision deco)と呼ばれ、Eurocrypt 2010 で N.Howgrave-Graham と A.Joux が提案した部分集合和アルゴリズムで利用された表現技法に着想を得たとしている。

Lower and Upper Bounds for Deniable Public-Key Encryption [Asiacrypt 2011]
Rikke Bendlin, Jesper Buus Nielsen, Peter Sebastian Nordholt, and Claudio Orlandi

否認可能暗号は、攻撃者がパーティ参加者の内部状態をプロトコル実行後に明らかにしたとしても、内部状態を変更して、復号文が元の平文とは異なる文に復号するように見せかけることで安全性を維持するものである。本論文では、受け手が否認できるような否認可能暗号の安全性はは、非対話型(non-interactive)では高々多項式の安全性しか達成できないことと、双方向に否認可能な公開鍵暗号も非対話型では高々多項式の安全性しか達成できないこととを証明した。

Bridging Broadcast Encryption and Group Key Agreement [Asiacrypt 2011]
Qianhong Wu, Bo Qin, Lei Zhang, Josep Domingo-Ferrerm and Oriol Farras

ブロードキャスト暗号とグループ署名の概念をまたいだ contributory broadcaset encryption

となるフレームワークを提案．このフレームワークを満たす具体的な方式として，暗号文が小さな方式，通信量や計算量が小さくなる方式などを提案．また，提案方式の構成技術を利用して，aggregatable ブロードキャスト暗号

Noiseless Database Privacy [Asiacrypt 2011]
Raghav Bhaskar, Abhishek Bhowmick, Vipul Goyal, Srivatisan Laxman, and Abhradeep Thakurta

プライバシをデータベース上で確保するための手段として，Differential Privacy(DP) という概念が提示され形式化されている．一般にこの DP を満たすために，問い合わせに対して真のデータにノイズをのせて返信することになるが，このようにノイズが含まれてしまうと，多くの場合他のアプリケーションなどに適合しない．そこで本稿では，ノイズを乗せずに，データベース上のデータのプライバシを守る手法を提案．実現方法としては攻撃者に与える auxiliary information を限定的(という設定)とし，問い合わせは Boolean-function と linear Real-function に限定することにより，攻撃者にプライバシの識別が困難な環境を導いている．提案方式は，データ変更に伴う結合可能性の性質は満たすことができている．

1.7.2. Asiacrypt 2011 の発表(2 日目)

The preimage security of double-block-length compression functions [Asiacrypt 2011]
Frederik Armknecht, Ewan Fleischmann, Matthias Krause, Jooyoung Lee, Martijn Stam, and John Steinberger

ブロック暗号を使ったハッシュ関数のうち、圧縮関数の連鎖値サイズがブロック長の 2 倍で(double-block-length)、一回の圧縮関数計算でブロック関数を 2 回呼び出す(double-call)ものについて、原像攻撃に対する安全性の下限を評価する新方式を提案した。これを、double-block-length, double-call の圧縮関数の３方式、Abreast-DM、Tandem-DM、Hirose's scheme に適用した。その結果、確率 0.5 以上で原像を復元するのに最低限必要なブロック暗号呼び出しの回数は Hirose's scheme で 2^{2n-5} 回、Abreast-DM と Tandem-DM で 2^{2n-10} 回だった。

Rebound Attack on JH42 [Asiacrypt 2011]
Maria Naya-Plasencia, Deniz Toz, and Kerem Varici

JH42 は SHA-3 の最終５候補の一つであり、最終ラウンド(第３ラウンド)進出時に圧縮関数の段数を 35.5 段から 42 段に増やしている。この論文では、リバウンド攻撃を利用して発見した JH42 に対する 32 段の差分経路を与え、それを使った 37 段までの semi-free-start 内部衝突発見と 42 段(仕様通り)の内部置換に対する識別子設計が可能であることを示した。

Second-Order Differential Collisions for Reduced SHA-256 [Asiacrypt 2011]
Alex Biryukov, Mario Lamberger, Florian Mendel, and Ivica Nikoli?

SHA-256 の 47 段縮小版(仕様は 64 段)に対し、2 次高階差分値の衝突が圧縮関数 2^{46} 回分の計算量で発見できると評価し、実際に計算機実験で発見したその例を示した。今回の解析では、ブロック暗号に対する攻撃に利用される rectangle/ブーメラン攻撃をハッシュ関数用に変形したものが利用された。今回の攻撃に関しては、SHA-256 の安全性マージンは SHA-3 の最終５候補にと比べて特に小さいことが指摘されている。

Finding SHA-2 Characteristics: Searching Through a Minefield of Contradictions [Asiacrypt 2011]
Florian Mendel, Tomislav Nad, and Martin Schlaffer

SHA-2 の差分特性探索を自動化する方法を開発し、SHA-256 に適用したところ、semi-free-start 衝突の適用可能段数を従来の 24 段から 32 段(仕様は 64 段)に伸ばすとともに、27 段縮小版に対する衝突の具体例を示した。SHA-2 の構造は SHA-1 より複雑であるため、SHA-1 用に開発された差分特性の自動解析方法はそのままでは適用できない。具体的な問題は、探索における制約条件に互いに矛盾し合うものが出現するためであり、これを同調するメッセージ対を探索することによって解決した。

Cryptanalysis of ARMADILLO2 [Asiacrypt 2011]
Mohamed Ahmed Abdelraheem, Celine Blondeau, Maria Naya-Plasencia, Marion Videau, and Erik Zenner

ARMADILLO2 は多目的に利用できる暗号プリミティブ ARMADILLO の改良版として提案され、パラメータの設定にによって、固定長入力の MAC(FIL-MAC)、擬似乱数生成器・擬似ランダム関数(PRNG/PRF)、ハッシュ関数などに利用できる。この論文では、中間一致攻撃を適用することで、FIL-MAC モードに対する鍵回復攻撃、擬似乱数生成器モードで利用したストリーム暗号に対する攻撃が全てのパラメータ設定に対して可能であることと、ハッシュ関数モードに対する(第２)原像攻撃が有効であることを示した。本論文のアプローチはランダムな要素を含まないより広い問題に対しても有効である。

An Experimentally Verified Attack on Full Grain-128 Using Dedicated Reconfigurable Hardware [Asiacrypt 2011]
Itai Dinur, Tim Guneysu, Christof Paar, Adi Shamir, and Ralf Zimmermann

Grain v1 は欧州のストリーム暗号の暗号研究プロジェクト eSTREAM でハードウェア向けストリーム暗号の一つとして選ばれたもので、鍵長 128 ビットの Grain 128 と 80 ビットの Grain 80 の２種類がある。Grain 128 については、弱鍵に対する攻撃は提案されていたが、本論文では全鍵に対して有効な攻撃が初めて提案された。攻撃には cube tester が利用されているが、以前のバージョンと比べ、適用範囲と鍵探索効率が向上している。攻撃の有効性を数学的に解析することは困難なので、解析には FPGA を利用した暗号攻撃専用の超並列計算システム RIVYERA に攻撃を実装し、全鍵の約 7.5%に対する実験で cube tester に期待される振る舞いの偏りを確認した。著者らは、この成果は実用的な仕様通りの暗号に対する解析攻撃が、暗号攻撃専用計算機によって実現した最初の例であると主張している。

Biclique Cryptanalysis of the Full AES [Asiacrypt 2011]
Andrey Bogdanov, Dmitry Khovratovich, and Christian Rechberger

Crypto 2012 のランプセッションで発表された，AES に対する Biclique Attack に関する正式な国際発表論文．以前よりハッシュ関数に適用されていた Meet-in-the-Middle 攻撃を改良してブロック暗号に適用した Biclique Attack が利用されている．基本的には鍵回復における総当たり攻撃において，その効率性を高めたものであり，論文では AES 128 に対して $2^{126.1}$，AES 192 に対して $2^{189.7}$，AES 256 に対して $2^{254.4}$ の計算量で鍵回復ができるとしている．AES については，これまで関連鍵攻撃についての報告がなされていたが，関連鍵を必要としない攻撃が発見されたという意味では大きな報告である．一方で，この攻撃による計算量の減少は約 2 ビット分と非常に少ない．会議に参加していた暗号研究者の議論によると，この手法をより発展させて効率的な攻撃に結びつけることは難しく，AES の安全自体への影響はほとんどないと考えられる．

Tag Size Does Matter: Attacks and Proofs for the TLS Record Protocol [Asiacrypt 2011]
Kenneth G. Paterson, Thomas Ristenpart, and Thomas Shrimpton

インターネットにおいて安全な通信路を構築する技術として一般的に使われている TLS プロトコルについての安全性解析の報告．RFC6066 で規定されている TLS1.2 で使われている MAC-then-Encode-then-Encrypt (MEE) という手法において，データサイズが固定でないパディングと短く truncate された MAC を用いたときに，識別不可能性に関する安全性が損なわれることが示されている．また，このタグのサイズを長くすると，TLS Record Protocol は，Length-Hiding Ahthenticated Encryption の安全性を満たすことがきることが示されている．

1.7.3. Asiacrypt 2011 の発表(3 日目)

Cryptography Secure against Related-Key Attacks and Tampering [Asiacrypt 2011]
Mihir Bellare,David Cash,and Rachel Miller

Related-keyattack(RKA)の安全性に関するフレームワークの解析結果を示した．具体的に示された肯定的な結果として，RKA-secure IBE(Identity-based encryption)は RKA-secure IND-CCA PKE (CCA-secure public-key encryption)を imply することを示した．また，否定的な結果として RKA-secure signatures は RKA-secure PRFs(Pseudo Random Functions)を imply しないことも示した．その他，PRFs，wPRFs(weak PRFs)，IBE，Sig (Signatures)，SE-CCA (CCA-secure symmetric encryption),SE-CPA(CPA-secure symmetric encryption)，PKE-CCA 等について，RKA-secure についての関係性を明らかにした．詳細は，e-print Archive 2011/252.

Counting Points on Genus 2 Curves with Real Multiplication [Asiacrypt 2011]
Pierrick Gaudry, David Kohel, and Benjamin Smith

こちらも会議の最優秀論文に選ばれた．具体的な endomorphism の乗算計算を用いて genus 2 のカーブの Schoof タイプの point-counting のアルゴリズムを提案.
提案方式は，従来有限体 F_q 上の genus 2 の point counting に，O(log 8 q) 必要としていた計算量を O(log 5 q) まで減らすことができる．この提案アルゴリズムを用いて，256 ビットの 素数位数の Jacobian 演算，暗号アプリケーション，および 1024 ビット位数の Jacobian 演算などを示した.

1.7.4. Asiacrypt 2011 の発表(4 日目)

Computational Verifiable Secret Sharing Revisited [Asiacrypt 2011]
Charles Bouillaguet, Pierre-Alain Fouque, Gilles Macario-Rat

computational Verifiable Secret Sharing(VSS)について，同期通信路 での 1-round の構成が一般的な通信モデル上では不可能であることを示した．一方で，dealer が一人で，party のメンバが 4 名以上の場合について 1-round VSS の構成が可能であることを示した．また，computational VSS の構成には必ずしも準同形成の性質を必要としないことを示し，任意のコミットメント方式を用いて dealer のメンバ数 t 人，party のメンバ数 n 人について n が 2t +1 以上の場合に，2-round の構成が可能であることを示した．

Practical Key-Recovery for All Possible Parameters of SFLASH [Asiacrypt 2011]
Itai Dinur, Orr Dunkelman and Adi Shamir

SFLASH 署名方式は、多変数二次多項式の解法が困難(NP 完全)であることに基づいて設計された方式であり、双線形性を利用した攻撃を防ぐために、元となった松本-今井暗号の公開鍵(公開多項式)の一部を捨てることで安全性を高めてある。しかし、SFLASH 署名方式で定める全パラメータに対して有効な攻撃法が、Eurocrypt 2007 と Crypto 2007 で V.Dubois らによって発表された。しかしながら、この攻撃は公開鍵の捨てる割合が半分までしか有効でなく、実用性が落ちるので設定されたパラメータの範囲に入らないものの半分以上捨てることで攻撃を無効にすることは可能であった。本論文では、情報理論的に必要とされる情報が入手出来れば、任意の公開鍵廃棄の割合に対して有効になる攻撃法を示した。

1.7.5. Asiacrypt 2011 rump の発表

Practical Collisions in Bound-Reduced Keccak [Asiacrypt 2011 rump session]
Itai Dinur, Orr Dunkelman and Adi Shamir

SHA3 コンテストで最終ラウンドの候補に残っている Keccak の Reduced Round 版において衝突を発見する攻撃の発表．差分攻撃と Algebraic な解析を組み合わせ，メッセージペアの差分特性を見つける手法を利用している．結果としては，これまで 2 ラウンドの Keccak に対する攻撃が発見されていたが，この発表により 4 ラウンドまでその攻撃を拡張することができた．

1.8. SHARCS 2012 の発表

1.8.1. SHARCS 2012 の発表(1 日目)

CAESAR: cryptanalysis of the full AES using GPU-like hardware [SHARCS 2012]
Alex Biryukov and Johann Großschadl

GPU の構成を利用して、計算が実現可能な範囲に収まる AES 攻撃専用ハードウェアの設計が可能であることを示した。128 ビット鍵の AES (AES-128)に対しては、1 個の平文、2 の 32 乗個の鍵と対応する暗号文から、鍵の 1 個を特定する問題を設定。256 ビット鍵の AES (AES-256)に対しては、4 個の関連鍵を使った攻撃を設定した。攻撃専用ハードウェアのコアとなる AES 計算に関しては、GPU の 1 つである NVIDIA GT200b を使った設計によって、AES 計算を 1 秒間に 10 の 12 乗回計算するハードウェアが 30 米ドルで実現できるという見積もりを示した。これらによって、AES の攻撃は実現可能な規模に収まるという結果が導かれたが、使用電力量が世界全体の使用量と同程度あったり、開発費用が米国の財政赤字と同程度になるなど、攻撃成功によって得られる利益にはとても見合わない結果となっている。

Better than brute-force-optimized hardware architecture for efficient biclique attacks on AES-128 [SHARCS 2012]
Andrey Bogdanov, Elif Bilge Kavun, Christof Paar, Christian Rechberger, Tolga Yalcin

biclique 攻撃は、複数の関連鍵の利用を想定しない単一鍵攻撃として初めて仕様通りの AES に対する鍵特定を可能にした攻撃法である。しかしながら、攻撃の方法が複雑なことから実際に攻撃を実装した場合、鍵の総当たり攻撃より多くの計算量が必要となる可能性が指摘されていた。今回の発表では、FPGA 及び ASIC による最適実装を、biclique 攻撃と鍵総当たり攻撃の両方について開発して性能を比較した。その結果、FPGA 実装と ASIC 実装の両方で biclique 攻撃は鍵総当たり攻撃の半分程度の計算時間しか掛からず、優位性が確認された。

Speeding up GPU-based password cracking [SHARCS 2012]
Martijn Sprengers, Lejla Batina

UNIX 系 OS で広く使われているパスワードの認証方式では、ハッシュ関数 MD5 を使って固定長のハッシュ値をファイルに保存しておき、入力されたパスワードの正当性をハッシュ値が一致するか否かで判定することが行われている。この発表は、攻撃者がパスワードに対するハッシュ値ファイルを入手したとき、パスワードの総当り攻撃がどこまで可能か、専用ハードウェアを使った場合の性能を追求したもので、GPU の NVIDIA GT295 を使って MD5 の計算を毎秒 90 万回
実行可能であることを示し、文字種類数が 36(大文字小文字限定の英数字)の 8 文字パスワードでは総当りが 37 日で可能である等の評価結果が示された。

1.8.2. SHARCS 2012 の発表（2 日目）

On the strength comparison of ECC and RSA [SHARCS 2012]

Masaya Yasuda, Takeshi Shimoyama, Tetsuya Izu, Jun Kogure

1024 ビットの RSA 暗号の安全性は 160 ビットの楕円曲線暗号と同等と以前は信じられていた。しかし、両方式ともに攻撃法が進化しているので、最新の攻撃技術に基づく最適実装を行い、安全性が等価なのは何ビット対何ビットのときであるか調べた。楕円曲線としては素体上の曲線、2の拡大体上の曲線、Koblitz 曲線の3種類が利用され、各々安全性は異なるが、各々に対して攻撃に必要な計算量を評価する式を導出し、素因数分解に必要な計算量との比較を行った。結果は、768 ビットの RSA と同等の楕円曲線暗号は、素体版で 115 ビット、拡大体版で 112 ビット、Koblitz 版で 117 ビットだった。また、1024 ビットRSAと同等のものは、素体版で138ビット、拡大体版で136ビット、Koblitz版で141ビットであった。これは以前の評価と比べ、相対的に楕円曲線暗号の安全性が高くなったことを意味する。素因数分解に関する計算量の評価式は 2006 年度の CRYPTREC 報告書の評価と良く合っていることが紹介された。

A flexible hardware ECDLP engine in Bluespec [SHARCS 2012]

Lyndon Judge, Patrick Schaumont

楕円曲線暗号の安全性は楕円曲線上の離散対数問題の困難性によって評価する。一般に暗号方式に対する攻撃は、専用ハードウェアを使うことで最高の効率が達成される傾向にあるが、楕円離散対数問題では、ソフトウェア実装での結果が上位を占めている。これは、ハードウェア設計では、細かい内容の変更に容易に対応することができないためである。この講演では、ハードウェア実装設計を柔軟に行うことを可能にする電子システムレベル(ESL)ハードウェア合成ツールセット Bluespec を紹介し、それを使って高性能な実装記述言語 Verilog ソースが生成できることを楕円離散対数問題を解く Pallard の ρ 法を例に示した。具体的には、quadcore Xeon プロセッサ(E7310, 6.6GHz)と Virtex-5(xq5vsx240t) FPGA を使った Nallatech 計算プラットフォームを利用し、8 コアで毎秒 480 万回の点加算を実現した。残念ながらこの値は、Cell プロセッサを使って得られた毎秒 880 万回の記録には及ばないが、コア 1 個のサイクル数当たりの添加算数では同等と主張している。

Solving discrete logarithms in smooth-order groups with CUDA [SHARCS 2012]

Ryan Henry, Ian Goldberg

楕円離散対数問題を解く Pollard の ρ 法を効率的に実行する CUDA を使った実装を示した。CUDA は NVIDIA 製 GPU の GTX シリーズ用に開発された並列計算のフレームワークで、暗号攻撃用にしばしば利用されている。Nvidia Tesla M2050 GPU カード 1 枚で、768 ビットの剰余乗算を毎秒約 5190 万回を達成した。

Cryptanalysis of MD5 and SHA-1 [SHARCS 2012]

Marc Stevens

電子政府推奨暗号の一つでもあるハッシュ関数の SHA-1 とその原型となった MD5 に対する攻撃の発展についてのレビュー。ハッシュ関数の重要な安全性評価基準の一つである衝突発見攻撃の困難性とその変形である近衝突攻撃や擬似衝突攻撃の紹介から始め、攻撃可能な範囲がどのように広がってきたか、またその攻撃を高速実装するための並列化をどのように行うかを紹介した。

新規の結果は SHA-1 の衝突攻撃に関するもので、near-collision(近衝突)を 2^57.5 で発見できる方法を示した。

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

共通鍵暗号系に対する攻撃法の一つに、暗号化鍵に関する多変数二次連立方程式を立て、それを解く代数攻撃がある。この連立方程式を解く代表的な方法に XL 法(extended linearization)がある。この発表では、Wiedemann の方法を適用し、48 コアの NUMA システムと 4 ノードの Infiniband クラスターの組み合わせに実装した結果、GF(16)上の 30 変数 60 連立二次方程式を 2.5 日解くシステムが 6000 米ドルで実現できることを示した。

Experimentally verifying a complex algebraic attack on the Grain-128 cipher using dedicated reconfigurable hardware [SHARCS 2012]
Itai Dinur, Tim Guneysu, Christof Paar, Adi Shamir, Ralf Zimmermann

Grain-128 は欧州のストリーム暗号研究プロジェクト eSTREAM で最終的にハードウェア実装向け推奨暗号の一つに選ばれた方式であり、暗号化鍵の 1000 分の 1 が弱鍵であり、攻撃可能であることが示されている。この発表では、代数攻撃の一種である cube tester を使用することで、2 の 63 乗ビットのメモリがあれば、総当り法より 2 の 38 乗倍高速に暗号化鍵が求まるという評価結果が示された。これは、弱鍵に限らず一般の鍵に対して有効である。さらに、攻撃専用ハードウェア RIVIYERA に実装して実験したところ、この結果を裏付けるデータの偏りが観測された。

1.9. FSE 2012 の発表

1.9.1. FSE 2012 の発表(1 日目)

Improved Attacks on Full GOST [FSE 2012]
Itai Dinur, Orr Dunkelman and Adi Shamir

ロシア標準のブロック暗号 GOST 28148-89 に対し、本論文で新たに導入した Fixed Point Property と 2-dimensional meet-in-the-middle (2DMITM) という 2 つの性質を利用して、32 フルラウンドの GOST に対する単一鍵攻撃の複雑度を昨年提案されていた既存の攻撃方法による結果 2^{224} を 2^{192} に削減した。
GOST は同じ部分鍵の 8 ラウンドを 3 回繰り返した後、順番を反転させた部分鍵の 8 ラウンドを適用する構造をもつので、8 ラウンドへの攻撃が基本となる。前者の性質はまさにその特徴を利用している。また後者の性質も、8 ラウンド GOST を前後 4 ラウンドに分けて中間一致攻撃を行うところ、推測決定攻撃も組み合わせて行う。4 ラウンド GOST の部分鍵を推測と決定を繰り返して復元する(木のノードの枝刈りを行い可能性を排除していくような感じ)。鍵特定に必要な計算量を従来の 2^{224} 乗から 2^{192} 乗に削減した。
今回の攻撃では FSE 2011 で発表された中間一致攻撃のを改良することで攻撃に必要な計算量削減に成功した。
なお、前日開催された SHARCS 2012 で Courtois がこれを上回る 2^{178} という結果を出しており、同氏は質疑の際にそのことについてコメントしていた。

Zero Correlation Linear Cryptanalysis with Reduced Data Complexity [FSE 2012]
Andrey Bogdanov and Meiqin Wang

通常の線形解読法では、ビットマスクによる線形近似の成立確率の 1/2 からの差が大きくなものを利用する。これとは逆に、成立確率がちょうど 1/2 になるゼロ相関の線形経路を利用して正しい鍵を推定するのがゼロ相関線形解読法である。オリジナルのゼロ相関線形解読法は、全ての平文・暗号文ペアを必要としたが本論文では、この条件を緩和し、パラメータにより複雑度や成功確率を調整できるように改良した。
具体的には TEA と XTEA という通常の線形解読法に対する安全性が証明されているブロック暗号にこの手法を適用し、有効性を示した。

"Provable" security against differential and linear cryptanalysis [FSE 2012]
Kaisa Nyberg

差分解読法と線形解読法と、それらに対する安全性証明に関する研究を概観した招待講演。ブロック暗号の安全性において重要なテーマであり、研究の意義は大きい。一方、これらに対して安全性が証明できても、別の攻撃で簡単に破れた暗号の例など、これだけで万能ではないことが逆に強調されていた。一つ前のゼロ相関攻撃も線形解読法に対する安全性を逆手に取ったものであり、対照的であった。
最近は暗号に対して実装サイズの小ささに対する要求が強まっているが、安全性が証明可能な構成は計算コストが大きくなりがちであり、近年はあまり重視されていない。電子政府推奨暗号のブロック暗号のうち、この安全性証明を持つのは、AES と MISTY1 である。

A Model for Structure Attacks, with Applications to PRESENT and Serpent [FSE 2012]
Meiqin Wang, Yue Sun, Elmar Tischhauser and Bart Preneel

構造攻撃は差分解読法の変形である。差分解読法が一組の平文差分と暗号文差分を利用するのに対し、この攻撃では複数の平文差分と一個の暗号文差分の組み合わせを構造(structure)と呼び攻撃に利用する。これに似た攻撃として、平文差分・暗号文差分ともに複数にした多差分解読法があるが、必要なデータ量が大きくなりすぎるので改良案として今回の方法が開発された。提案法では多くのパラメータを使うので、差分の選択指針も示した。この攻撃法を ISO/IEC の軽量暗号に採用された PRESENT と AES の最終5候補の一つ Serpent に適用し、計算機実験の結果従来攻撃より複雑度が削減するのを確認した。

A Methodology for Differential-Linear Cryptanalysis and Its Applications [FSE 2012]
Jiqiang Lu

差分線形解読法は、差分解読法と線形解読法を組み合わせた攻撃法であり、差分を固定した平文ペアと対応する暗号文に対するマスク線形和を利用する。本発表では、平文差分に対して計算した中間状態の差分値の確率を利用した改良を行った。DES に対する解読実験では、従来の差分線形解読法では 16 段中 9 段までしか攻撃できなかったのを、13 段まで攻撃可能にした。なお、DES は基本的な差分解読法、及び、線形解読法で仕様通りの 16 段が破れている。

New Observations on Impossible Differential Cryptanalysis of Reduced-Round Camellia [FSE 2012]
Ya Liu, Leibo Li, Dawu Gu, Xiaoyun Wang, Zhiqiang Liu, Jiazhe Chen and Wei Li

電子政府推奨暗号のブロック暗号 Camellia に対する、不能差分解読法の改良には多くの研究があり、攻撃可能段数は増加している。今回の発表では、途中段に対する弱鍵の考察を利用し、一般の鍵に適用可能な攻撃法の改良を行った。その結果、適用可能な段数は、128 ビット鍵で従来の 18 段中 10 段から 11 段へ、192 ビット鍵で従来の 24 段中 11 段から 12 段へ、256 ビット鍵で従来の 24 段中 11 段から 13 段へ拡張した。まだ、仕様の段数までには差があり、当分は現実的な脅威となる可能性は低い。

Improved Rebound Attack on the Finalist Grøstl [FSE 2012]
Jeremy Jean, Maria Naya-Plasencia and Thomas Peyrin

Grøstl は SHA-3 の最終5候補の一つであるハッシュ関数である。この発表では中間一致攻撃の一種であるリバウンド攻撃の改良を行った。今回の改良は、中間の三段に対する差分特性を効率良く計算できるようにしたことである。改良によって、ハッシュ値が 256 ビットの Grøstl-256 に対しては従来からの改善が見られなかったものの、Grøstl-512 に対しては、置換の 10 段縮小版に対する識別子作成に成功した。なお、この結果はハッシュ関数 Gr φ stl 自体の安全性に対して、直接の影響はない。

(Pseudo) Preimage Attack on Reduced-Round Grøstl Hash Function and Others [FSE 2012]
Shuang Wu, Dengguo Feng, Wenling Wu, Jian Guo, Le Dong and Jian Zou

これもハッシュ関数 SHA-3 の最終5候補 Grøstl に関する発表。中間一致攻撃を利用して擬似原像を計算するという内容で、Grøstl-256 に対して 10 段中 5 段まで、Grøstl-512 に対して 14 段中 8 段まで、擬似原像の計算が可能であることを示した。

Practical Cryptanalysis of ARMADILLO2 [FSE 2012]
Maria Naya-Plasencia and Thomas Peyrin

ARMADILLO2 は、CHES 2010 で提案されたハードウェアの小型実装が可能な共通鍵暗号系用の構成要素であり、ブロック暗号やハッシュ関数の設計に利用できる。この発表では、拡散の制御のしやすさ、局所的線形化を利用した攻撃法を示し、ARMADILLO2 の安全性が高くないことを示した。具体的には、ストリーム暗号に利用した場合、真性乱数との違いが容易に検出でき、鍵を特定する関連鍵攻撃も可能であること、ハッシュ関数として利用した場合、半自由開始衝突が発見できることが示された。

On the (In)Security of IDEA in Various Hashing Modes [FSE 2012]
Lei Wei, Thomas Peyrin, Przemyslaw Sokolowski, San Ling, Josef Pieprzyk and Huaxiong Wang

PGP など古くから利用されている 64 ビット・ブロック暗号 IDEA を使ったハッシュ関数モードに安全性上の問題があることを指摘した。この研究では、鍵ビットを全部 0 にしたとき、確率 1 で成立する差分ペアが存在する性質を利用し、ブロック暗号を使った 6 種類のハッシュ関数モードに対する攻撃を試みた。その結果、6 種類のモード全部に対し、ハッシュ関数計算 2 の 25.5 回分の計算で、原像計算が可能であることなどが明らかになった。a

1.9.2. FSE 2012 の発表(2 日目)

The Security of Ciphertext Stealing [FSE 2012]
Phillip Rogaway, Mark Wooding and Haibin Zhang

Ciphertext Stealing は、ブロック暗号を利用したモードであり、NIST が Special Publication の 800-38A で、CBC-CS1, CBC-CS2, CBC-CS3 の三種類を規定している。このモードの特徴は、CBC モードにおいて、連鎖値の一部ビットを0にすることである。この発表では、この操作によって選択平文攻撃に対して新規に設定された ind$安全性が満たされることを証明した。

McOE: A Family of Almost Foolproof On-Line Authenticated Encryption Schemes [FSE 2012]
Ewan Fleischmann, Christian Forler and Stefan Lucks

認証付き暗号化方式(Authenticated Encryption)では、毎回異なる値を持つ nonce を利用することが必要であるが、実際には望ましくない nonce の再利用がしばしば行われる。nonce の再利用に対して安全性が保たれる方式は提案されているが off-line で利用し、安全性も攻撃者の能力に強い制約を課して達成されるものだった。今回の発表では、on-line に対応し、一般の攻撃者に対しても安全性が保証できる方式を提案した。なお、この発表に関し、ランプセッションで、誕生日攻撃が存在することが発表されたが、安全性証明と矛盾するものではない。

Cycling Attacks on GCM, GHASH and Other Polynomial MACs and Hashes [FSE 2012]
Markku-Juhani Olavi Saarinen

電子政府推奨暗号の改訂で、事務局選出暗号に含まれる使用モードの一つである GCM に対する攻撃の発表。GCM の構成要素である GHASH では、連鎖値を計算する際に AES の暗号文を GF(2^{128})上の固定値として乗算する。このため、GCM ではべき乗が1となる周期分だけ離れた中間データを入れ替える偽造攻撃が可能となる。この周期が短いものが弱い鍵であるが、GF(2^{128})では多数の弱い鍵の存在が、計算機実験で確認できた。この攻撃を避けるためには、GF(2^{128})以外の安全な有限体を使用することで防げる。

Collision Attacks on the Reduced Dual-Stream Hash Function RIPEMD-128 [FSE 2012]
Florian Mendel, Tomislav Nad and Martin Schlaffer

RIPEMD-128 は、国際規格 ISO/IEC 10118-3 に採用されているハッシュ関数である。従来最も成功した攻撃は 64 段中 33 段の縮小版に対する原像攻撃であった。今回の発表では、2並列の Chaining Value 計算において両方で高い確率で生じる差分を選択し、良い差分とメッセージモディフィケーションを自動的に探索する方法を開発し、38 段縮小版に対する衝突発見に成功するとともに、48 段縮小版の真性乱数からの違いが検出可能であることを示した。

Bicliques for Preimages: Attacks on Skein-512 and the SHA-2 family [FSE 2012]
Dmitry Khovratovich, Christian Rechberger and Alexandra Savelieva

biclique 攻撃は中間一致攻撃の一種で、2011 年 8 月に AES の攻撃に成功したことで注目されていた。今回の攻撃対象はブロック暗号ではなくハッシュ関数であり、SHA-3 最終5候補の一つ Skein と電子政府推奨暗号のハッシュ関数 SHA-256 と SHA-512 に対する攻撃に対して適用された。Skein-512 に対しては、第2原像攻撃が 72 段中 22 段まで成功した。SHA-256 に対しては、原像攻撃及び第2原像攻撃についての攻撃可能段数を従来の 64 段中 43 段から 45 段に拡張した。SHA-512 に対しては、原像攻撃及び第2原像攻撃についての攻撃可能段数を従来の 64 段中 46 段から 50 段に拡張した。

Converting Meet-in-the-Middle Preimage Attack into Pseudo Collision Attack: Application to SHA-2 [FSE 2012]
Ji Li, Takanori Isobe and Kyoji Shibutani

SHA-2 に対しては原像攻撃は中間一致攻撃の利用で 45 段(64 段中)まで可能である。一方、衝突攻撃は 32 段までしか成功していない。この研究は、中間一致攻撃の matching point を後ろにずらす partial target 原像攻撃を経由して、原像攻撃を衝突攻撃に変換することで、衝突攻撃の適用可能段数を伸ばすことを目的に行われた。結果は、擬似衝突攻撃ではあるものの、SHA-256 を 52 段まで、SHA-512 は 57 段まで攻撃可能段数を伸ばした。今回の攻撃法は、SHA-2 ファミリ以外にも Skein や BLAKE にも適用可能である。なお、今回の成果を擬似でない衝突攻撃に変換することは困難ということである。

UNAF: A Special Set of Additive Differences with Application to the Differential Analysis of ARX [FSE 2012]

Vesselin Velichkov, Nicky Mouha, Christophe De Canniere and Bart Preneel

剰余加算、ビット回転、排他的論理和を組み合わせた ARX は、軽量暗号の重要な設計要素として近年多用されている。しかし、安全性解析は S-box を使用した構成と比べて困難で、差分特性の解析も多くの場合分けを含む解析が必要である。本研究では、通常使われる排他的論理和や剰余加算の代わりに、UNAF を利用することによって、効果的に差分経路を探索することを提案する。ストリーム暗号の Salsa20 に適用した結果、従来記録を破る 5 段縮小版に対する攻撃を可能にした。

ElimLin Algorithm Revisited [FSE 2012]

Nicolas T. Courtois, Pouyan Sepehrdad, Petr Susil and Serge Vaudenay

多変数多項式に関する方程式系を解く手法である ElimLin について、単項式の異なる順序や変数の全単射なアフィン変換に対して結果が影響を受けないという、この種の方法として望ましい特徴付けがあることを示したという内容。具体的に CTC2 などのブロック暗号に対して、既存の代数攻撃手法などとの比較を行った。

The history of linear cryptanalysis [FSE 2012]

Mitsuru Matsui

線形解読法と関連する見解決問題等についての、開発者である三菱電機の松井氏による講演。DES の解読に使用する DES の S-box の線形近似式が Crypto '85 の Shmir の論文に載っているものの攻撃には結びつかなかったことや、1993 年に DES の解読実験に成功した際利用したワークステーションの CPU 速度が 99MHz と非常に遅かったことなど興味深い事実が紹介された。また、最近の話題として、Almost Perfect Nonlinear(APN)等に関する未解決話題が取り上げられた。

1.9.3. FSE 2012 の発表(3 日目)

Short-output universal hash functions and their use in fast and secure message authentication [FSE 2012]
Long Hoang Nguyen and Andrew William Roscoe

整数値の乗算をベースとして、処理速度の速さという点でコストが低く、出力長が短いユニバーサルハッシュ関数を提案し、メッセージ認証スキームを構成した。

Lapin: An Efficient Authentication Protocol Based on Ring-LPN [FSE 2012]
Stefan Heyse, Eike Kiltz, Vadim Lyubashevsky, Christof Paar and Krzysztof Pietrzak

有限体上の多項式環を(ある 1 つの)多項式から生成されるイデアルで割った環上で定義された LPN 問題ベースで、IC カードのようなリソースが限られた環境で効率的な実装が可能な認証プロトコルを HB(Hopper and Blum)風に作った。HB 系のスキームは中間者攻撃対策にも安全なスキームへの改良がなされているが、今回のスキームはまだそこまでの安全性は達成していない。共通鍵系のスキームとの比較において、安全性証明を考慮することの意図が Bernstein から質問された(。

Higher-Order Masking Schemes for S-Boxes [FSE 2012]
Claude Carlet, Louis Goubin, Emmanuel Prouff, Michael Quisquater and Matthieu Rivain

重要なデータを分割してから計算してサイドチャネル攻撃耐性を高める方法をマスキングというが、Sbox に対してソフトウェア実装での計算コストの増加を抑えたいくつかの手法が提案された。具体的には DES と PRESENT に対して適用した。

Recursive Diffusion Layers for Block Ciphers and Hash Functions [FSE 2012]
Mahdi Sajadieh, Mohammad Dakhilalian, Hamid Mala and Pouyan Sepehrdad

拡散層をベースとしてブロック暗号やハッシュ関数の構成する場合において、差分・線形攻撃耐性があり、軽量なものを代数的に構成した。具体的には、MMB の Binary matrix、AES・Hierocrypt の MDS_H 行列、PHOTON に適当し、処理コストを低減する改良案を示した。

Unaligned Rebound Attack: Application to Keccak [FSE 2012]
Alexandre Duc, Jian Guo, Thomas Peyrin and Lei Wei

Keccak の内部置換の差分パスを検索する新しい方法を提案して、5 ラウンドの縮小版 Keccak に対して適用して複雑度を低減した。また、Rebound Attack に対して今回の手法を適用したという内容。AES はもともと差分の伝播が良くなるように設計されていたのに対して、Keccak ではそうではところがあるので、それを weak alignment を言っている。

Differential propagation analysis of Keccak [FSE 2012]
Joan Daemen and Gilles Van Assche

差分伝播特性の一つである差分 trail を効率良く探索するために、新しく weight という指標を導入し、Keccak に適用し有効性を確認した。1 ラウンドの weight は差分確率の対数の符号を反転したものであり、複数ラウンドについては各ラウンドの独立性を仮定して再帰的に計算する。weight はラウンド数の増加に伴って増加するので、一定値を越した weight を枝刈りすることによって、探索が効率化できる。具体的には Keccak[1600]について、3 ラウンド縮小版の weight が 36 以下の全 trail を見つけるとともに、6 ラウンド縮小版の trail では weight の最小値が 74 以下と評価した。この結果は、Keccak には weight の小さな trail が存在にないことの確率的な証拠を与え、差分特性を利用した攻撃に対する安全性が高いことを示している。

New attacks on Keccak-224 and Keccak-256 [FSE 2012]
Itai Dinur, Orr Dunkelman and Adi Shamir

Keccak に対して新しい攻撃方法を提案し、Keccak-224 と Keccak-256 の縮小版に対し 1 台の PC による攻撃実験を行い、有効性を確認した。具体的には、両方式の 4 ラウンド縮小版に対する衝突を数分以内で発見した。また、5 ラウンド縮小版の Keccak-224 と Keccak-256 に対し、ハミング距離が各々5 ビットと 10 ビットの近似衝突を数日間の計算で発見した。提案方式では、差分解析手法と代数的手法を組み合わせ、Keccak のラウンド関数が二次写像であるという性質を使っている。

1.10. Third SHA-3 Candidate Conference の発表

1.10.1. Third SHA-3 Candidate Conference の発表(1 日目)

A Study of Practical-time Distinguishing Attacks Against Round-reduced Threefish-256 [3rd SHA-3]
Aron Gohr

Skein の構成要素となるブロック暗号 Threefish の縮小版に対する関連鍵ブーメラン攻撃の発表。Threefish は3種類のブロック長・鍵長(256 ビット、512 ビット、1024 ビット)と 128 ビットの tweak が使用でき、いずれも 72 段繰り返し構造である。この論文では、256 ビットの Threefish-256 に対し、次の2種類の攻撃が現実的な時間で実行可能であることを示した。・27 段縮小版に対する関連鍵攻撃・19 段縮小版に対する関連 tweak を使った単一鍵攻撃

ARXtools: A Toolkit for ARX Analysis [3rd SHA-3]
Pierre-Alain Fouque

ARX(Addition, Rotation, eXclusive-or)の差分特性の解析は困難である。解析のためのバックトラック法は計算量が指数関数的に増加し、現実的でない。本論文では解析のためにオートマトンを利用する解析法を開発し、それを利用して既存の解析結果を検証した結果、多くで解析に利用された仮定が正しくないことを発見した。この機能と GUI を備えた解析ツールが次の URL から入手可能である。
http://www.di.ens.fr/~leurent/arxtools.html

On the Algebraic Degree of some SHA-3 Candidates [3rd SHA-3]
Christina Boura

代数次数は代数攻撃に対する安全性を評価する際の重要な指標である。本論文では、構成要素(S-box 等)の次数が低い場合、通常考えられているものより代数次数の上限が低くなる場合があり、具体例として SHA-3 候補の Keccak, ECHO, JH に対する解析結果を示した。Keccak では Keccak-f 関数のフルスペック(24 段)に対する識別子の効率を改良するのに適用できた。また、JH については 16 段(仕様では 42 段)の次数が 1022 以下となり、飽和しないことが示された。

Side Channel Analysis of the SHA-3 Finalists [3rd SHA-3]
Michael Zohner

SHA-3 の最終5候補の特定の実装に対し、サイドチャネル攻撃(DPA とプロファイルベース攻撃)の安全性を解析。CHES 2010 で Benoit-Peyrin は、BLAKE と Grostl に対する DPA で MAC 偽造が可能と評価。本論文では、DPA によって Grostl に対する鍵回復攻撃、JH, Keccak, Skein に対する MAC 偽造攻撃が可能、プロファイルベース攻撃によって、Grostl に対するメッセージ復元が可能であることを示した。もちろん、サイドチャネル攻撃が可能か否かは実装の仕方に依存するので今回を解析は絶対でない。

Provable Security of BLAKE with Non-Ideal Compression Function [3rd SHA-3]
Bart Mennink

BLAKE は構成要素にブロック暗号を含んだ HAIFA 型の構造をしている。本論文では、BLAKE の圧縮関数が 2^n/4 回の query でランダムオラクルと強識別可能であること、しかし、ブロック暗号が理想的であれば、BLAKE 自体は 2^n/2 まで強識別不可能であることを証明した。

1.11. TCC 2012 の発表

1.11.1. TCC 2012 の発表（1 日目）

Simple and Efficient Public-Key Encryption from Computational Diffie-Hellman in the Standard Model [TCC 2012]

Kristiyan Haralambiev, Tibor Jager, Eike Kiltz, Victor Shoup

標準モデルにおいて計算量 Diffie-Hellman 仮定の下で、選択暗号文攻撃に対して安全であることが証明可能な、実用的な公開鍵暗号システムを提案する。本スキームは既存の構成よりも概念的により単純でありより効率的である。更に、nをセキュリティパラメーターとすると、双線型群において、公開鍵のサイズを群要素 n 個から $2\sqrt{n}$ 個に減らすことができることを示す。

1.11.2. TCC 2012 の発表（2 日目）

Secure Network Coding over the Integers [TCC 2012]
Rosario Gennaro, Jonathan Katz, Hugo Krawczyk, Tal Rabin

ネットワーク・コーディングへの汚染攻撃への対策として、準同型ハッシュと準同型署名を用いた、``ネットワーキング・コーディング署名''が近年開発されたが、本技術に関して以下の貢献を行う。
－ランダムオラクルモデルにおいて RSA 仮定に基づく初めての準同型署名を示す
－標準モデルにおいて素因数分解の困難性に基づく準同型署名を導く、既存のものよりも効率的な準同型ハッシュスキームを与える
－中規模ネットワークの通信オーバーヘッドを削減し、計算効率を改善する（中間ノードにおける署名生成が 20 倍高速になる場合もある）既存スキームの変形を示す

1.11.3. TCC 2012 の発表（3 日目）

Efficient Set Operations in the Presence of Malicious Adversaries [TCC 2012]
Carmit Hazay, Kobbi Nissim

共通集合および和集合を求める効率的で安全な2パーティプロトコルを構成する問題を、悪意ある攻撃者のモデルに焦点を当てて再考する。本プロトコルは定数ラウンドであり、シミュレーションベースの安全性を持ち、通信計算量およびべき乗計算数が線型となるものである。本構成の中心は、完全に隠蔽するコミットメントスキームと不記憶擬似ランダム関数評価プロトコルである。本プロトコルは、容易に、UC 安全なプロトコルに変換できる。

発行日　2011年 6月 8日　第2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
（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