CRYPTREC Report 2008

平成 21 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

「暗号技術監視委員会報告」

目次

はじめに

本報告書は、総務省及び経済産業省が主催している暗号技術検討会の下に設置されている暗号技術監視委員会の 2008 年度活動報告である。

電子政府(e-Government)での利用に資する暗号技術のリストアップを目的として、暗号技術監視委員会の前身とも言える暗号技術評価委員会では、2000 年度から 2002 年度の 3 年間をかけて、暗号技術評価活動(暗号アルゴリズムの安全性評価)を推進してきた。その結果、2003 年 2 月に、暗号技術検討会を主催する総務省、経済産業省が電子政府推奨暗号リストを公表する運びとなり、暗号技術評価活動も一区切りを迎えた。

現在、CRYPTREC 活動は 2003 年度に発足した「暗号技術監視委員会」と「暗号モジュール委員会」を中心に行われている。両委員会とも総務省及び経済産業省が主催している暗号技術検討会の下で活動をしており、前者は電子政府推奨暗号の安全性の監視等、後者は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っている。

暗号技術監視委員会は、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、技術面を中心とした活動を担当している。一方、ユーザの立場でかつ政策的な判断を加えて結論を出しているのが暗号技術検討会であり、相互に協調して電子政府の安全性及び信頼性を確保する活動を推進している。

2008 年度は、2013 年度に行われる電子政府推奨暗号リスト改訂に向けての第一歩を踏み出した年であった。8 月に実施した「電子政推奨暗号リストの改訂に関する骨子（案)」に対する意見募集の結果を受けて、暗号技術監視委員会では、公募要項（案）の内容を審議し、2 月には、「CRYPTREC シンポジウム 2009～電子政府推奨暗号リスト改訂に向けて～」を開催した。参加者は約 230 名に及び、パネルディスカッションでは、今後の日本の暗号技術に関する活発な議論が交わされた。2009 年 10 月からは、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，暗号利用モード，エンティティ認証の 5 つのカテゴリにおいて、実際の公募が始まるため、2009 年度の暗号技術監視委員会では、公募やリスト改訂に関する事項を審議していく。

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、暗号モジュール委員会との連携を保ちつつ、暗号技術やその実装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。

暗号技術監視委員会　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章は暗号技術監視委員会及び監視活動等について説明してある。第2章は今年度の検討してきた電子政府推奨暗号リスト改訂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章は暗号技術監視委員会の下で活動している暗号技術調査ワーキンググループの活動報告である。

本報告書の内容は、我が国最高水準の暗号専門家で構成される「暗号技術監視委員会」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。

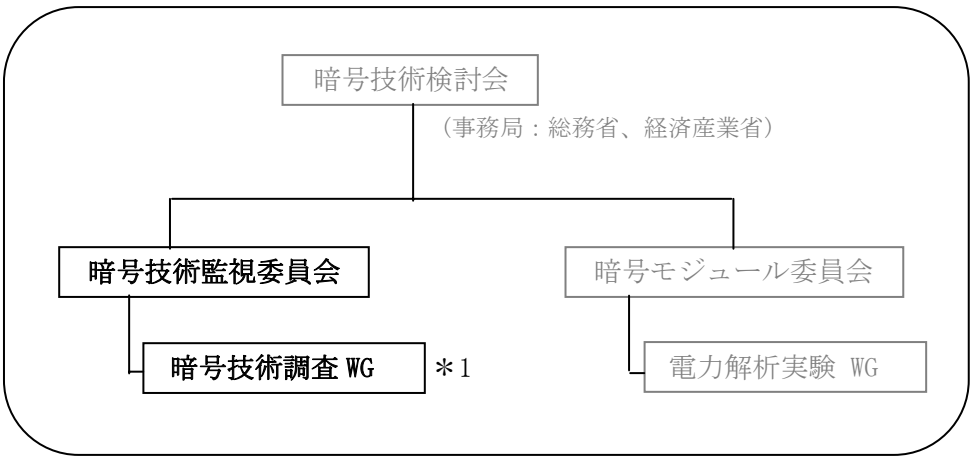
【問合せ先】　info@cryptrec.go.jp

委員会構成

暗号技術監視委員会(以下「監視委員会」)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。監視委員会は、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、監視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、監視委員会活動に関連して必要な項目について、監視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。監視委員会の委員長は、実施する調査・検討項目に適する主査及びメンバーを、監視委員会及び調査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・検討結果を監視委員会に報告する。平成20年度、監視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」及び「IDベース暗号に関する調査」である。

監視委員会と連携して活動する「暗号モジュール委員会」も、監視委員会と同様、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

1) 電子政府推奨暗号リストに関するガイドの作成

2) IDベース暗号に関する調査

図1　CRYPTREC体制図

委員名簿

暗号技術監視委員会

委員長	今井 秀樹	中央大学 教授
顧問	辻井 重男	情報セキュリティ大学院大学 学長
委員	太田 和夫	国立大学法人電気通信大学 教授
委員	金子 敏信	東京理科大学 教授
委員	佐々木 良一	東京電機大学 教授
委員	田中 秀磨	独立行政法人情報通信研究機構 主任研究員
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　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

委員	荒木 純道	国立大学法人東京工業大学 大学院 教授
委員	有田 正剛	情報セキュリティ大学院大学 教授
委員	酒井 康行	三菱電機株式会社 チームリーダ
委員	四方 順司	国立大学法人横浜国立大学 大学院　准教授
委員	洲崎 誠一	株式会社日立製作所 部長
委員	藤岡 淳	日本電信電話株式会社 主幹研究員
委員	松崎 なつめ	パナソニック株式会社　チームリーダ
委員	青木 和麻呂	日本電信電話株式会社 主任研究員
委員	川村 信一	株式会社東芝 研究主幹
委員	香田 徹	国立大学法人九州大学　大学院　教授
委員	古原 和邦	独立行政法人産業技術総合研究所　主幹研究員
委員	下山 武司	株式会社富士通研究所 主任研究員
委員	角尾 幸保	日本電気株式会社 主席研究員
委員	時田 俊雄	三菱電機株式会社 チームリーダー
委員	古屋 聡一	株式会社日立製作所 主任研究員
委員	森井 昌克	国立大学法人神戸大学 教授
委員	廣瀬 勝一	国立大学法人福井大学 大学院　准教授
委員	盛合 志帆	ソニー株式会社 主任研究員
委員	内山 成憲	公立大学法人首都大学東京 准教授
委員	駒野 雄一	株式会社東芝 研究員
委員	宇根 正志	日本銀行　金融研究所　企画役
委員	國廣 昇	国立大学法人東京大学　大学院 准教授
委員	田村 裕子	日本銀行　金融研究所

委員	高木 剛	公立大学法人公立はこだて未来大学 教授
委員	伊豆 哲也	株式会社富士通研究所　研究員
委員	岡本 健	国立大学法人筑波技術大学　准教授
委員	小林 鉄太郎	日本電信電話株式会社　研究主任
委員	境 隆一	大阪電気通信大学　講師
委員	高島 克幸	三菱電機株式会社　主席研究員
委員	花岡 悟一郎	独立行政法人産業技術総合研究所　研究員

オブザーバー

椿井 隆志	内閣官房 情報セキュリティセンター[2008 年 12 月まで]
山下 博道	内閣官房 情報セキュリティセンター[2008 年 12 月より]
栢沼 伸芳	内閣官房 情報セキュリティセンター
繁富 利恵	内閣官房 情報セキュリティセンター
本多 祐樹	内閣官房 情報セキュリティセンター
大橋 一夫	警察庁 情報通信局
小松 聖	総務省 行政管理局[2008 年 7 月まで]
松本 和人	総務省 行政管理局[2008 年 7 月より]
藤井 信英	総務省 地域力創造グループ
中小路 昌弘	総務省 自治行政局[2008 年 7 月まで]
山﨑 敏明	総務省 自治行政局[2008 年 7 月より]
荻原 直彦	総務省 情報通信国際戦略局
増子 喬紀	総務省 情報通信国際戦略局[2008 年 7 月まで]
山崎 浩史	総務省 情報通信国際戦略局[2008 年 7 月まで]
梶原 亮	総務省 情報通信国際戦略局[2008 年 7 月より]
齊藤 修啓	総務省 情報通信国際戦略局[2008 年 7 月より]
東山 誠	外務省 大臣官房
森田 信輝	経済産業省 産業技術環境局
小野塚 直人	経済産業省 商務情報政策局[2008 年 5 月まで]
下里 圭司	経済産業省 商務情報政策局[2008 年 5 月より]
花田 高広	経済産業省 商務情報政策局
齊藤 文信	防衛省 運用企画局
神藤 守	防衛省 陸上幕僚監部[2008 年 7 月まで]
千葉 修治	防衛省 陸上幕僚監部[2008 年 7 月より]
滝澤 修	独立行政法人 情報通信研究機構
大蒔 和仁	独立行政法人 産業技術総合研究所[2008 年 12 月まで]
大塚 怜	独立行政法人 産業技術総合研究所[2008 年 12 月より]

事務局

独立行政法人 情報通信研究機構 （篠田陽一、山村明弘[2008 年 4 月まで]、田中秀磨、黒川貴司、中里純二「2008 年 11 月まで]、王立華[2008 年 9 月より]、金森祥子、松尾真一郎、中村豪一、赤井健一郎）

独立行政法人 情報処理推進機構（山田安秀、山岸篤弘、星野文学、大熊建司、小暮淳、伊東徹、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、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 が事務局を務める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」が決定されるに至った。

第 1 次基本計画に引き続いて、中長期計画(2009～2011 年度の 3 ケ年計画)として「第 2 次情報セキュリティ基本計画」が NISC の情報セキュリティ政策会議において 2009 年 2 月に決定され、同計画において、「「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」の策定時の経験を適切に継承し、安全性が低

下した暗号について速やかに安全な暗号への移行を進める」こととされた。

このように、電子政府推奨暗号の監視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 暗号技術監視委員会

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。

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。

平成２０年度において、暗号技術監視委員会は、「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)」の策定に大いに寄与した。また、平成１９年度に引き続き、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、電子政府推奨暗号リストの適切な利用のために、アウトリーチ活動として、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、リストに係る技術的解説書として、電子政府推奨暗号リストガイドの作成を継続して行った。さらに、ＩＤベース暗号の技術動向を調査するため、暗号技術調査ワーキンググループ(ＩＤベース暗号)を開催した。

これらの詳細については、それぞれ、第 2 章及び第 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

平成 20 年度は、暗号技術監視委員会を中心に、電子政府推奨暗号リストの改訂に関する検討が行われた。詳しくは、第 2 章を参照のこと。

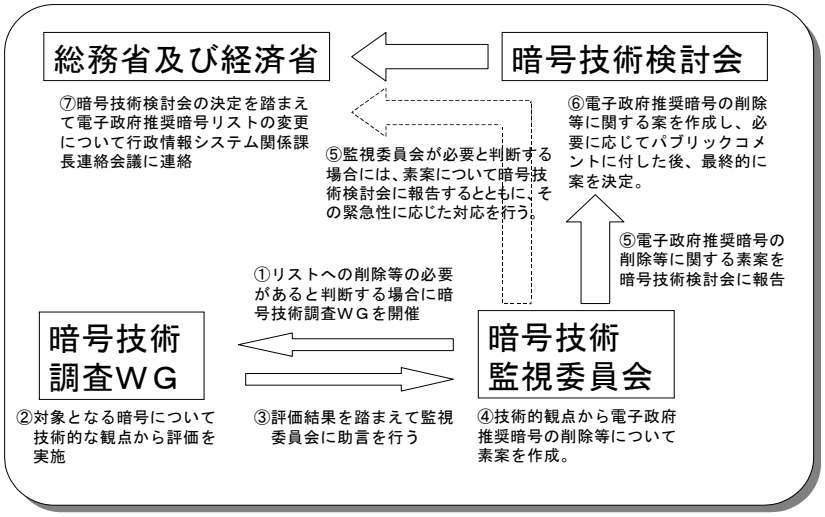
1.4 活動の方針

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の改訂に関する骨子

以上の考え方のもと、CRYPTREC では「電子政府推奨暗号リストの改訂に関する骨子（案）」

（以下、骨子案という。）を作成し、総務省及び経済産業省において、2008 年 8 月 6 日から 9 月 5 日にかけてパブリックコメント[1]を行った。その結果[2]、全部で個人・企業から合計 7 件の意見があった。2.3.1 節～2.3.4 節では、骨子案の概要について報告する。

2.3.1. 現リストの構成の見直し

現時点で CRYPTREC が公開している暗号リストは現行の電子政府推奨暗号リストのみであるが、下記の（1）～（3）の各リスト及び(4)リストガイドをまとめて「CRYPTREC 暗号リスト（仮称)」（以下、「次期リスト」）として、計画では 2012 年度までに公開することを予定している。

（1） 電子政府推奨暗号リスト（仮称）
（2） 推奨暗号候補リスト（仮称）
（3） 互換性維持暗号リスト（仮称）
（4） リストガイド

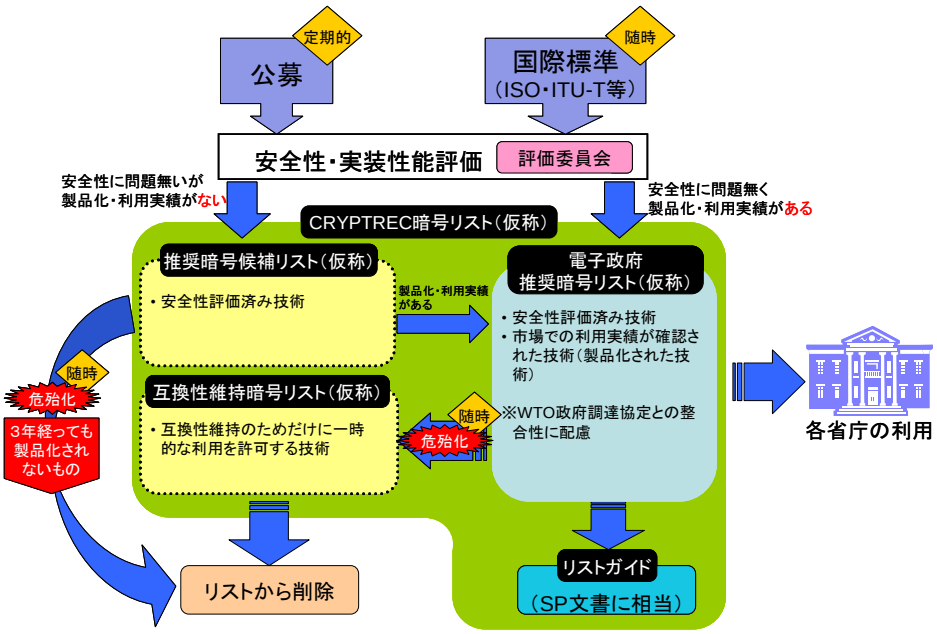


図 2.1. リスト改訂概念図（案）

CRYPTREC により安全性が確認された暗号技術は、（1）～（3）の 3 つのリストのいずれかに登録される。各リストへの登録は、WTO 政府調達協定[3]との整合性に配慮しつつ、安全性や市場動向により決定される。登録の見直しは一定の間隔で行う。

[1] http://search.e-gov.go.jp/servlet/Public?CLASSNAME=Pcm1010&BID=145207347
[2] http://search.e-gov.go.jp/servlet/Public?ANKEN_TYPE=3&CLASSNAME=Pcm1090&KID=145207347
[3] http://www.mofa.go.jp/mofaj/gaiko/wto/chotatu.html

現リストに掲載されている暗号技術については、安全性の再評価を行った上で 2013 年の次期リスト運用開始前に推奨暗号候補リスト（仮称）へ登録されていたものとして扱う。2013 年の次期リスト運用開始時には、新たに応募された技術と共に製品化の状況・技術の利用状況により電子政府推奨暗号リスト（仮称）へ登録するかの決定を行う。

次期リストにおける各（部分）リストの役割は以下の通りである。

(1)　電子政府推奨暗号リスト（仮称）

CRYPTREC により安全性が確認され、かつ市場において利用実績が十分である技術リスト。電子政府構築（政府調達）の際には当該技術を推奨する（現リストと同等の位置づけ）。ここに登録される技術は国際標準化機関等により、標準化されていることが望ましい。電子政府推奨暗号リスト（仮称）に登録されるカテゴリ別の暗号数はいたずらに多くならないことを基本とする。

(2)　推奨暗号候補リスト（仮称）

CRYPTREC により安全性が確認されているが、市場において利用実績が十分でない普及段階にある暗号技術が登録されているリスト。今後、利用が期待される新規技術等はここに分類される。電子政府構築（政府調達）の際には当該技術を調達しても良い。

一定期間ごとに普及の度合いの調査を行い、利用実績が十分であると認められれば電子政府推奨暗号リスト（仮称）に登録される。また、利用実績が十分であると認められなかった場合にはここから削除される。そして、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は随時削除される。

(3)　互換性維持暗号リスト（仮称）

電子政府推奨暗号リスト（仮称）に登録されていたが、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もののうち、互換性維持のために継続利用を容認するもののリスト。暗号解読のリスクと、電子政府システムにおける移行コスト等を勘案して、定期的に掲載継続の可否を判断する。CRYPTREC として新規調達を推奨しない。

(4)　リストガイド

電子政府で利用されている、あるいは利用する可能性のある技術について、その技術概要と、推奨する利用方法を記述する。また、次期リストに記載された技術の中で、安全性を維持するため正しいパラメータの設定が要求される技術における具体的なパラメータ設定方法の記述を行う。さらに、将来必要になると予想されるセキュリティ技術については、その開発状況や利用可能性について記載する。リストガイドは、システム運用者や設計者の利用や、システム利用者への啓発を目的とする。

2.3.2. 暗号技術公募の基本方針

原則として、一定期間ごとにリストを見直し、必要があれば公募を行う。公募を行う際の基本方針は以下の通りである。

(1) 公募対象のカテゴリは、下記の(1a)～(1c)のいずれかの条件を満たすものとする。

(1a) 現リストに含まれていないが、電子政府システムの構築において安全性及び実装性の高い技術仕様の推奨が必要とされている暗号技術カテゴリであること。

(1b) 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。

(1c) 普及・標準化が見込まれる暗号技術カテゴリであること。

(2) 応募可能な暗号技術は、下記の(2a)～(2e)のすべての条件を満たすものとする。

(2a) 十分な安全性を有する暗号技術であること。ただし、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。

(2b) 個別のシステムやアプリケーションの仕様に依存しない、汎用的な暗号技術であること。

(2c) 当該技術を利用した製品が販売済みであるか又は、販売の予定があること。

(2d) 安全性評価及び、実装性能評価に足る技術仕様が公表されていること。

(2e) 暗号技術に関する基本特許については、製造、販売、使用に対して、無償(Royalty Free) 又は、妥当かつ非差別的 (Reasonable And Non-Discriminatory) な条件で、暗号技術の実施許諾権が与えられること。

2.3.3. 2009 年度公募カテゴリ

2009 年度は、2.3.2. (1) (1a) に該当するものとして暗号利用モード、メッセージ認証コード及びエンティティ認証、2.3.2. (1) (1b) に該当するものとしてブロック暗号及びストリーム暗号を公募対象のカテゴリとする。

なお、現リストにおいて例示的に技術名の記載があるカテゴリである、擬似乱数生成系については、公開鍵暗号技術等で利用される要素技術であり、相互接続性に影響を与えないこと、安全性要件として満たすべき乱数検定法が示されていることから、リストガイド

にて参照することが適当であると考えられる。よって、電子政府推奨暗号リスト（仮称）及び推奨暗号候補リスト（仮称）から外し、2009 年度公募カテゴリには入れないこととする。

以上のことから、次期リストの技術カテゴリは表 2.1 のようになる。

表 2.1 次期 CRYPTREC 暗号リスト（仮称）カテゴリ（現リストとの比較）

電子政府推奨暗号リスト （現リスト）	CRYPTREC 暗号リスト(仮称) （次期リスト）
署名	署名
守秘	守秘
鍵共有	鍵共有
64 ビットブロック暗号	ブロック暗号
128 ビットブロック暗号	
ストリーム暗号	ストリーム暗号
	メッセージ認証コード
	暗号利用モード
ハッシュ関数	ハッシュ関数
疑似乱数生成系	
	エンティティ認証

2.3.4. 今後のスケジュール

2009 年度　第 3 四半期　公募書類受付開始（提出書類の審査を実施。）
2009 年度　第 4 四半期　公募〆切
2010 年度　第 1 次評価期間（主に、応募暗号技術の評価を実施。）
2011 年度　第 2 次評価期間（応募暗号技術の継続評価の他、現リストに登録されている暗号技術の再評価等も実施。）
2012 年度　第 1 四半期～第 3 四半期　次期リスト（案）の策定
2012 年度　第 4 四半期　次期リストの発表
2013 年度　第 1 四半期　次期リストの運用開始

2.4. 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）

骨子案に対するパブリックコメントの結果を踏まえ、CRYPTREC では、「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）」（付録 3）を策定した。

2.4.1 節～2.4.7 節では、この公募要項の概要について報告する。

2.4.1. 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。

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、事務局が開催するワークショップ（2.4.7 節を参照のこと。）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、現リストに登録されている暗号技術の再評価も行う。

CRYPTREC 内に設置された「評価委員会（仮称)」が、評価結果に基づき、「CRYPTREC 暗号リスト（仮称)」（以下、「次期リスト」という。）への暗号技術の記載について判定し、暗号技術検討会に答申する。答申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。

2.4.2. 2009 年度公募カテゴリ

骨子で策定されたとおり、2009 年度公募カテゴリは、下記の表の通りとなった。

表 2.2. 2009 年度公募カテゴリの概要

2009 年度公募カテゴリ	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 ビット又は 256 ビットであるブロック暗号。
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	共通鍵暗号技術、公開鍵暗号技術、MAC によるチャレンジ・レスポンスを用いたエンティティ認証。

主な採用理由としては、ブロック暗号及びストリーム暗号については、最新の研究動向

や国際標準化動向の進展に追従するためであり、メッセージ認証コード及び暗号利用モードについては、現リストにないが、情報通信システムの構築にはなくてはならない技術であるからである。なお、エンティティ認証については、前回公募時に現リスト掲載に資する技術がなかったため、今回追加した。

2.4.3. 提出書類

今回の応募に際して必要な提出書類は以下のとおり。

(1) 暗号技術応募書
(2) 暗号技術仕様書
(3) 自己評価書
(4) テストベクトル、テストベクトル生成ソースコード及びその仕様書
(5) 参照ソースコード及びその仕様書
(6) 参照ハードウェア設計記述及びその仕様書
(7) 誓約書
(8) 公開の状況等に関する情報
(9) 応募暗号説明会発表資料
(10) 自己チェックリスト

詳細については、「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）」（付録 3）を参照のこと。

2.4.4. 評価スケジュール（予定）

2000 年度から 2002 年度まで実施された評価スケジュールを参考にして以下のように定めた。

応募暗号説明会開催：	2010 年 3 月頃
第 1 次評価実施：	2010 年 4 月～2011 年 3 月
第 1 回ワークショップ開催：	2011 年 2 月頃
第 2 次評価実施：	2011 年 4 月～2012 年 3 月
第 2 回ワークショップ開催：	2012 年 2 月頃
2012 年度シンポジウム：	2013 年 2 月頃

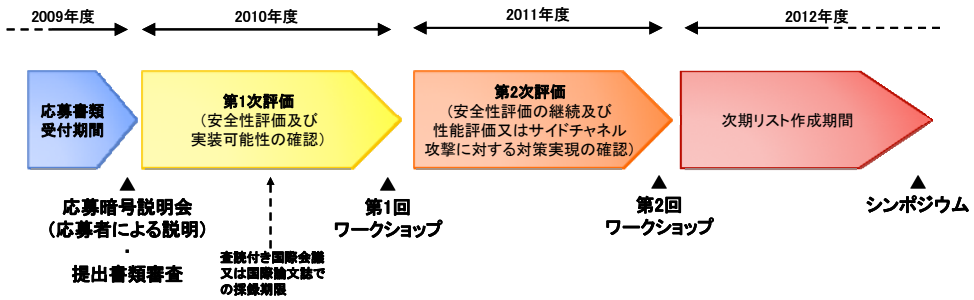


図 2.2. 評価スケジュール（予定）

なお、暗号技術公募の基本方針において、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、を指針として採用したことから、提案する技術については、査読付きの国際会議または国際論文誌で論文として採録されていることを必須としている。また、評価及び実施方法等において未確定な部分がある実装性評価については、2009 年度以降において検討を行う予定である。

2.4.5. 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います。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[4]、ASIC[5]等）別に性能（処理速度、使用セル数又はゲート数等）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、今回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るので、次年度以降に詳細を検討する必要がある。その結果は、CRYPTREC 統一 Web サイト

[4] FPGA：Field Programmable Gate Array
[5] ASIC：Application Specific Integrated Circuit

（http://www.cryptrec.go.jp/）などを通じてアナウンスする予定である。詳細については、「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）」（付録 3）を参照のこと。

2.4.6. 応募暗号説明会の開催

応募された暗号技術の評価を開始するにあたり、応募者自ら公の場で、応募暗号技術の技術仕様、安全性、実装性、公開状況、及びライセンス等について説明する機会を設ける予定である。正式日程などの詳細については、2009 年 10 月頃に CRYPTREC 統一 Web サイト（http://www.cryptrec.go.jp/）などを通じてアナウンスする予定である。

2.4.7. ワークショップの開催

開催時点までの評価委員会（仮称）における最新の評価結果を公表し、それらを検討する場を設ける予定である。この機会を利用して、応募者が自らの意見を述べることもできる。

第 1 次評価実施期間（2010 年 4 月～2011 年 3 月）の後に開催予定の第 1 回ワークショップでは、応募暗号技術の安全性評価及び実現可能性の確認結果を公表する予定である。また、第 2 次評価実施期間（2011 年 4 月～2012 年 3 月）の後に開催予定の第 2 回ワークショップでは、第 1 次評価実施期間後に継続して実施された安全性評価、性能の評価及びサイドチャネル攻撃に対する対策実現の確認結果を公表する予定である。また、現リストに掲載されている暗号技術に関する再評価の結果も公表する予定である。詳細については、各年度の 10 月頃に正式日程を CRYPTREC 統一 Web サイト（http://www.cryptrec.go.jp/）などを通じてアナウンスする予定である。

2.5. CRYPTREC シンポジウム 2009 について

2.5.1. 開催目的

2009 年度から 2012 年度にかけて実施する、電子政府推奨暗号リストの改訂の背景や目的及び、暗号技術公募とその評価等について広く一般に周知するために、シンポジウムを開催することとした。

また、それに加えて、公募カテゴリを中心とした暗号技術の最新動向を一般に周知するため、また、今後の暗号研究の方向性についてより大局的な議論を行うために、パネルディスカッションを併設した。

2.5.2. プログラムの概要

日時：2 月 18 日（水）13：00～16：30　主催：NICT・IPA　共催：総務省・経済産業省
場所：虎ノ門パストラルホテル　本館 1 階　葵の間
参加人数：約 230 名

表 2.3　プログラム

時間		目的
13:00	開会の挨拶	総務省/経済産業省
13:05	講演 1「電子政府推奨暗号リストについて」（今井委員長）	・電子政府推奨暗号リストの重要性について ・電子政府推奨暗号リスト改訂の理由および目的について
13:15	講演 2「リスト改訂スキームについて」(山村委員)	・今後の電子政府推奨暗号リストの改訂スキームについての説明、特に、リスト間遷移条件を中心にスキームの詳細についての説明 ・質疑応答によって得られた有意義な意見はスキームを最終決定する際の参考とする
13:40	講演 3「暗号技術の公募について」CRYPTREC 事務局	・今回の暗号技術の公募について、公募要項を基に説明
14:00	休憩	
14:10	パネル 1 「公募対象カテゴリを中心とした暗号技術の動向について」 モデレータ：高木剛(公立はこだて未来大学) パネリスト：大塚玲(産業技術総合研究所)、下山武司(富士通研究所)、盛合志帆(ソニー)、吉田博隆(日立製作所)	・公募を行うカテゴリの最新技術動向と、電子政府にとってどのようなアルゴリズムが求められるかを中心にパネルを行い、評価基準を決定する際の参考とする ・将来的にリストに掲載する可能性のある暗号について、パネルを行い、将来のリスト掲載の可能性について周知をしておく
15:00	休憩	
15:15	パネル 2 「日本の暗号研究と電子政府推奨暗号の今後について」 モデレータ：佐々木良一(東京電機大学) パネリスト：岩下直行(日本銀行)、辻井重男(情報セキュリティ大学院大学)、苗村憲司(SC27/WG2 コンビーナ)、松本勉(横浜国立大学)、伊藤毅志（内閣官房情報セキュリティセンター)	・現行の電子政府推奨暗号リストやその(2001 年当時の)選定方法について、問題点や反省点を明示する ・今後の電子政府推奨暗号リスト、CRYPTREC、および、日本の暗号研究の方向性についてより大局的な観点から議論を行う
16:25	閉会の挨拶	NICT/IPA

2.5.3. 意見・コメントの概要

パネル 1 及びパネル 2 では、パネリスト他から、これから実施される電子政府推奨暗号リストの改訂や暗号技術公募に対する意見・コメントが寄せられた。ここではそれらの概要を記しておく。

(1) 暗号技術公募について

- 実装プラットフォームや実装方法に強く依存するサイドチャネル攻撃に対する耐性をどのように評価・比較していくのか。
- サイドチャネル攻撃に対する耐性という評価項目が挙がっているが、どこまで厳密に行うつもりなのか、応募する側にも評価する側にもコストがかかることが懸念させる。
- 暗号アルゴリズムの評価ならCall for attackというような手段もあるが、サイドチャネル攻撃の場合には、例えば、応募者が攻撃対象の実装をサンプルとして提供して、call for attackをする方法を思い付くが、この場合にはその経費をCRYPTRECが負担することになるのか？ CRYPTRECとして、サイドチャネル攻撃に対する評価方法をどのように考えているか、お聞きしたい。
- Call for attackの実施に必要な予算の確保は難しいので、今回のリスト改訂では、ある実装に対して安全性が示されることが必要という趣旨で評価を実施する予定である。コストをかけた特別な実装方法などではなく、通常で利用できる範囲でサイドチャネル攻撃に対する耐性を確認する予定である。
- 公募カテゴリにはモードとMACがあるが、対象としている分類を明確にすべきである。
- 客観的な安全性評価の行われたエンティティ認証に基づくシステムが構築されていくことを期待している。
- 将来CRYPTRECでハッシュ関数を公募する際には、汎用のハッシュ関数の他にも、特殊用途やハッシュ関数関連のモードについても検討するべきである。
- IDベース暗号を調達する際には、主に、数学的基盤、ペアリングアルゴリズム、プロトコル、運用の4つの点が定まっている必要があるが、CRYPTRECとして扱うべき領域について検討する必要がある。

(2) 電子政府推奨暗号リストの今後について

- 評価し尽くされ、長持ちする汎用の実用的な暗号アルゴリズムを厳選すべきである。競争力の点で少数であることが本質的であり、同じカテゴリなら高々2 個。また、専任の機関が自分のものとして責任をもって維持管理していくことが必要である。
- 政府等の大口ユーザーの意思の表明がはっきりしていないので、制度的な裏づけの下で

利用していくべきである。

- 安全性に問題がある場合には国際標準技術を使わないことに問題はないだろうが、それ以外の場合は WTO 政府調達協定では問題になるだろう。WTO 協定の恩恵をうけているのは実は日本であり、ISO/IEC 規格との整合性の確保をお願いしたい。
- 今後は、専門家側は評価にあたって実務上の影響を分析して考慮し、ユーザー側は評価結果を実務によりきちんと反映していくことが必要である。
- 政府機関では危殆化対策としてこれから数年程度かけてシステム移行を行っていく予定である。CRYPTREC には今後もリアルタイムでの情報提供をお願いしたい。
- 電子署名を認証に利用することは多いが、電子政府推奨暗号リストでは認証に利用できるかどうかははっきりしないところがある。
- 電子政府推奨暗号リストを参考にしているという結果も出てきているが、電子政府推奨暗号リストは民間での利用が低いことが問題である。
- 暗号危殆化における世代交代については幅を持たせて進めていくことが必要である。
- 企業において暗号研究者の数を減らす傾向が出てきている。セキュリティ技術に携わる人口を維持するための強化が必要である。CRYPTREC は人材育成という面でも重要な活動であるので、今度も維持していく体制作りが必要である。

第３章 監視活動

3.1. 監視活動報告

3.1.1. 共通鍵暗号に関する安全性評価について

2008 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。

具体的な動きとしては、SAC 2008 において、FL 関数を除いた縮小版のブロック暗号 Camellia に対し、128 ビット鍵で 12 段（フルラウンド 18 段）まで、256 ビット鍵で 16 段（フルラウンド 24 段）までという不能差分攻撃が報告されている。また、ASIACRYPT 2008 において、縮小版のブロック暗号 MISTY1（フルラウンド 8 段）に対し、FL 関数付きで 6 段まで、FL 関数なしで 7 段までという不能差分攻撃が報告されている。なお、この攻撃手法は 2003 年度に学会発表がなされており、監視活動において既知のものである。さらに、SCIS 2009 において、データ量 $2^{54.1}$ 及び計算量 $2^{120.8}$ で 7 段という高階差分攻撃が報告されている。また、CRYPTO 2008 において、ストリーム暗号 RC4 に対し、計算量 2^{579}（現実的な仮定のものでは計算量 2^{241}）という内部状態回復攻撃が示されている。

3.1.2. ハッシュ関数に関する安全性評価について

2008 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。

具体的な動きとしては、CRYPTO 2008 において、縮小版の SHA-1（フルラウンド 80 段）に対し、44 段で計算量 2^{157} という原像攻撃が報告されている。また、SAC 2008 において、縮小版の SHA-256（フルラウンド 64 段）に対し、23 段で計算量 $2^{44.9}$、24 段で計算量 $2^{53.0}$ の、縮小版の SHA-512（フルラウンド 80 段）に対し、23 段で計算量 2^{18}、24 段で計算量 $2^{28.5}$ の衝突発見攻撃が報告されている。さらに、FSE 2009 において、24 段に縮小した SHA-256 に対し、計算量 2^{240} の原像攻撃と第 2 原像攻撃、24 段に縮小した SHA-512 に対し、計算量 2^{480} の原像攻撃と第 2 原像攻撃が報告されている。

3.1.3. 公開鍵暗号に関する安全性評価について

2008 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。

具体的な動きとしては、ANTS-VIII において、Certicom 社の ECC Challenge[1]でまだ解かれていない楕円曲線 ECC2K-130 に関する離散対数問題の計算量について報告があり、2 万台の計算機を使用すれば 2 年で解けると見積もられている。また、ASIACRYPT 2008 において、素体上の離散対数問題に対する Pollard の ρ 法の高速化手法が提案され、1024 ビットのランダムな素体では従来よりも 10 倍程速くなると報告されている。

3.1.4. その他の暗号技術に関する安全性評価について

2008 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。

リストには含まれていないが、Eurocrypt 2008 において、大手自動車メーカの多くで採用されているキーレスエントリー・システムで使われるブロック暗号 KeeLoq に対し、攻撃可能な条件が 2^{16} 個の既知平文と暗号化 $2^{44.5}$ 回分の計算量にまで削減され、初めて現実的な脅威となっている。また、ASIACRYPT 2008 において、欧州で実施されているプロジェクトである eSTREAM の最終選考まで残っていたストリーム暗号 F－FCSR-H に対する現実的な攻撃が報告され、その結果により最終選考から急遽、外されている。また、MD5 に対して Eurocrypt 2007 において発表されていた衝突発見攻撃の一種（Chosen-prefix Collision）[2]を電子証明書に関する署名の偽造に応用して、現実的な計算量で中間 CA 証明書の偽造に成功したことが 2008 年の暮れに報告されている[3]。そして、PKC 2007 で提案されていた多変数公開鍵暗号系である ℓIC を用いた署名方式 ℓIC⁻に対して、署名偽造や秘密鍵の解読が可能なことが報告されている。

3.2. 暗号技術標準化動向

3.2.1. 米国 NIST による次世代ハッシュ関数 SHA-3 の公募

National Institute of Standard and Technology (NIST)は 2009 年 2 月 25 日～2 月 28 日の日程で、次世代ハッシュ関数 SHA-3 の選考のための第 1 回会合(The First SHA-3 Candidate Conference)をルーベン・カトリック大学（ベルギー）にて開催した。参加者は

[1] http://www.certicom.com/index.php/the-certicom-ecc-challenge/

[2] 最近の研究結果では計算量が 2^{41} と報告されている。SHA-1 に関する Chosen-prefix Collision の計算量について 2^{80} 弱という見積が出されているので、今後注意が必要である。詳しくは、http://eprint.iacr.org/2009/111/ または、http://www.win.tue.nl/hashclash/rogue-ca/を参照のこと。

[3] JVNVU#836068、MD5 アルゴリズムへの攻撃を利用した X.509 証明書の偽造、http://jvn.jp/cert/JVNVU836068/

約 220 名であった。

ハッシュ関数の説明を行うセッションでは、2008 年 10 月までに応募のあった 64 件のうち、書類審査を通過した 51 件で、この会議までに脆弱性が発見され、提案の取り下げがあった 10 件と今回の会議に参加したかったもの 5 件を除く、36 件のプレゼンテーションが行われた。

NIST による評価観点の説明と議論を行うセッションでは、今後のハッシュ関数の評価において、重要なポイントとなる部分について現時点での NIST の見解を紹介するとともに、参加者からの意見を聴取するセッションが 4 件行われた。各セッションのテーマは以下の通りであった。

(a) System Properties：SHA-3選定にあたって対象とすべきシステム要件

少なくとも電子署名、鍵導出関数、HMAC、擬似乱数生成をサポートすることが示された。処理性能と実装性のトレードオフの観点としては、ゲート数、ハードウェアのハッシュ性能への依存度、メモリサイズ、並列性等が挙げられた。議論を受けて、NISTは、最小限の要求事項と優先順位の低い評価軸を今後提示することを表明した。

(b) System Evaluation：安全性評価の方法

安全性評価のためのモデル設定について現状の案が紹介され、その後参加者から意見が聴取された。アルゴリズムの安全性を示す状態として、

- Completely breaks： 現実的な攻撃が存在する
- Wounds： 原像(preimage)が2^nより少ない計算量で計算できる等の、安全性要件を満たさない
- Undermines confidence： 近似衝突(near collision)、擬似衝突(pseudo collision)等、内部にいくつかの脆弱性が存在するが、第2原像(second preimage)や衝突(collision)等は発見されていない
- Little to no concern： 衝突(collision)、第2原像(second preimage)等が発見されており考慮の対象外

という4つの定義が提示された。

(c) System-Performance Tradeoff：安全性と性能のトレードオフ

幅広いアプリケーションに柔軟に対応するために、ブロック長やラウンド数等のパラメータを可変とすることが想定されている。第2ラウンドに向けて、パラメータの仕様の修正の他に、エディトリアルな変更、安全性評価の記述、評価例の追加等を行うことが認められた。さらに、第2ラウンドに選ばれた候補に対しては、変更の理由を示すことを条件にア

ルゴリズムの微修正を行うことも認められた。また、参照プラットフォームであるIntel IA-32及びAMD64上でSHA-256、SHA-512と同等の性能を実現するパラメータにおいて安全でない場合は、選考の優先順位が下がることが示された。一方で、第2ラウンドへの選考においては性能を特に重視する意図はないことが表明された。また、演算に必要なリソースの観点では、第1ラウンドではソフトウェア実装におけるリソースに注目するとともに、スマートカードのような制約された環境での実装性についても評価を行い、ハードウェア実装については、第1ラウンドでは概要的な評価を行い、第2ラウンドにおいてゲート数を含めた詳細な評価を行うことを表明した。その他、並列実装、アルゴリズム解析の容易性、複数の組み込みシステムへの適正等も評価項目として挙げられた。

(d) The Way Forward：今後の評価の進め方

SHA-3への要件がさまざまであることからパラメータの選択設計が重要であること、また、安全性の評価に加え、性能評価も考慮していることが表明された。今後、第1ラウンドでは特に安全性の評価を重視する形で評価を行い、2009年8月に開催されるCRYPTO 2009の前までに約15件の候補に絞ることが宣言された。この際、異なる設計思想のものをバランス良く残す方針が示された。さらに、研究者に対しては2009年の6月1日までに第1ラウンドの候補に対して、安全性評価結果やコメントを提示するように求めた。なお、次回の会議はCRYPTO 2010辺りに実施される予定である。

その他のセッションでは、提案されているハッシュ関数の分析や比較状況に関する発表や、最新の研究成果に関する発表があった。

3.2.2. ECRYPT の動向

欧州では ECRYPT（以下、「ECRYPT I」という。）[4]に引き続き、ECRYPT II[5]が 2008 年 8 月から開始されている。ECRYPT II は、

- Symmetric techniques virtual lab (SymLab) … 共通鍵暗号系に関する研究
- Multi-party and asymmetric algorithms virtual lab virtual lab (MAYA)… 公開鍵暗号系に関する研究
- Secure and efficient implementations virtual lab (VAMPIRE) … 暗号技術の実装に関する研究

の 3 つの活動に分かれている。

[4] http://www.ecrypt.eu.org/ecrypt1/
[5] http://www.ecrypt.eu.org/

なお、前回の ECRYPT Ⅰ では、優れたストリーム暗号を選定するためのプロジェクト eSTREAM[6]を実施していたが、最終的に下記のように選定されている[7]。

表 3.1　eSTREAM 最終選考結果

Profile 1 (Software-oriented)	Profile 2 (Hardware-oriented)
HC-128	Grain v1
Rabbit	MICKEY v2
Salsa20/12	Trivium
SOSEMANUK	

3.3. 公的個人認証サービスにおける暗号方式等の移行に関する検討会への技術的意見の提出について

総務省 自治行政局 地域情報政策室を事務局とする「公的個人認証サービスにおける暗号方式等の移行に関する検討会」(座長：辻井 重男　情報セキュリティ大学院大学 学長)[8]では、公的個人認証サービスの信頼性を今後も継続的に確保するため、暗号方式等の移行について検討を行っており、報告書を作成している。CRYPTRECに対して、RSA-1024bit及びSHA-1の暗号危殆化の見通しについて技術的意見を求められていたので、第1回検討会において回答した。

3.4. 学会等参加記録

2008年度は、国内・国外の学会に参加し、暗号解読技術に関する情報収集を実施した。監視要員等を派遣した国際会議は、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
PKC 2008	11th International Workshop on Practice and Theory in Public Key Cryptography	バルセロナ (スペイン)	3 月 9 日～ 3 月 12 日
TCC 2008	Fifth Theory of Cryptography Conference	ニューヨーク (米国)	3 月 19 日～ 3 月 21 日
ANTS-Ⅷ	Eighth Algorithmic Number Theory Symposium	バンフ (カナダ)	5 月 18 日～ 5 月 22 日

[6] http://www.ecrypt.eu.org/stream/
[7] http://www.ecrypt.eu.org/stream/announcements.html
[8] http://www.soumu.go.jp/menu_03/shingi_kenkyu/kenkyu/kouteki_kojin/

FDTC 2008	Workshop on Fault Diagnosis and Tolerance in Cryptography	ワシントン (米国)	8月10日～ 8月10日
CHES 2008	Workshop on Cryptographic Hardware and Embedded Systems	ワシントン (米国)	8月10日～ 8月13日
SAC 2008	Workshop on Selected Areas in Cryptography	サックヴィル (カナダ)	8月13日～ 8月15日
CRYPTO 2008	International Cryptology Conference	サンタバーバラ (米国)	8月17日～ 8月21日
ECC 2008	Workshop on Elliptic Curve Cryptography	ユトレヒト (オランダ)	9月22日～ 9月24日
PQCrypto 2008	International Workshop on Post-Quantum Cryptography	シンシナティ (米国)	10月17日～ 10月19日
ASIACRYPT 2008	International Conference on the Theory and Application of Cryptology & Information Security	メルボルン (オーストラリア)	12月7日～ 12月11日
SCIS 2009	2009年暗号と情報セキュリティシンポジウム	大津 (日本)	1月20日～ 1月23日
FSE 2009	Workshop on Fast Software Encryption	ルーベン (ベルギー)	2月22日～ 2月25日
SHA-3 Candidate Conference	SHA-3 Candidate Conference	ルーベン (ベルギー)	2月25日～ 2月28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について述べる。

3.4.1. ブロック暗号の解読技術

従来からの代数的攻撃の研究が着実に進んでいる。MISTY1 に対して高階差分攻撃を適用することで、8段中7段まで攻撃可能になった[高階差分攻撃に関する7ラウンドMISTY1の安全性、齊藤 照夫、茂 真紀、川幡 剛嗣、角尾 幸保、SCIS 2009]。

また、代数攻撃に差分解読法のような確率的法を組み合わせる方式が開発され、軽量暗号として注目されるPRESENTに適用したところ、31段中17段まで解読可能という評価が出ている[Algebraic Techniques in Differential Cryptanalysis、Martin Albrecht and Carlos Cid、FSE 2009]。

3.4.2. ストリーム暗号の解読技術

暗号研究プロジェクト eSTREAM で採用された暗号 F-FCSR-H と Sosemanuk、国際標準(ISO/IEC 18033-4)に採用された SNOW 2.0 に対する解読が示された[Breaking the F-FCSR-H Stream Cipher in Real Time、Martin Hell and Thomas Johansson、ASIACRYPT 2008]。特に、F-FCSR-H に対する攻撃は現実的な時間で実際に鍵の復元が可能であることを実証したものである。この攻撃の発表を受け、eSTREAM の終了時にハードウェア向け暗号としてポートフォリオに掲載されていたのが、削除された。

Sosemanuk と SNOW 2.0 に対する攻撃は、全数探索よりも少ない計算量で高い確率で鍵が復元できると評価したものである[Cryptanalysis of Sosemanuk and SNOW 2.0 Using Linear Masks、Jung-Keun Lee、Dong Hoon Lee、Sangwoo Park、ASIACRYPT 2008]。

製品に対する現実的な攻撃も幾つか報告されている。第 3 世代携帯電話の規格 GSM で利用されているストリーム暗号である A5/1 への攻撃の実装報告が行われた。解読可能であるとする理論解析結果は既知であった。Xilinx 社製 Spartan3-XC3S1000 FPGA 120 個を使った高性能低コストの暗号解読専用機 COPACOBANA 上に実装し、予備的な実装でフル実装した場合の性能を外挿したところ、最適化したデザインで全探索をすると 11.78 時間、鍵発見の平均時間は 5.89 時間という見積もりを得た[A Real-World Attack Breaking A5/1 within Hours、Timo Gendrullis、Martin Novotny、Andy Rupp、CHES2008]。

広く普及している、ストリーム暗号 RC4 を使った無線通信プロトコル WEP に対し、104 ビット鍵の場合でも、40,000 パケット程度の受動的観測だけで破れることが示された。従来は、プロトコルの初期ベクトル IV に弱いものが選ばれる等の条件があったが、今回はそのような制約なしで適用できる[Breaking WEP with Any 104-bit Keys ―All WEP Keys Can Be Recovered Using IP Packets Only―、寺村 亮一、朝倉 康生、大東 俊博、桑門 秀典、森井 昌克、SCIS2009]。

3.4.3. ハッシュ関数の解読技術

衝突発見では、SHA-1 の攻撃段数が 80 段中 70 段のままで大きな進展が無かったものの、より大規模な方式に対する解析が進んだ。SHA-256 の衝突は、64 段中 24 段まで発見できた[Collisions and other Non-Random Properties for Step-Reduced SHA-256、Sebastiaan Indesteege、Florian Mendel、Bart Preneel and Christian Rechberger、SAC 2008]。また、国際標準(ISO/IEC 10118-3)に採用されている Whirlpool の衝突は、10 段中 4.5 段まで計算可能になった[The Rebound Attack: Cryptanalysis of Reduced Whirlpool and Grøstl、Florian Mendel、Christian Rechberger、Martin Schläffer and Søren S. Thomsen、FSE 2009]。

原像計算や第 2 原像計算では、中間データの一部について誕生日攻撃を適用する攻撃手

法が開発され、攻撃が進展した。原像攻撃では、SHA-1 が 80 段中 44 段まで[Preimages for Reduced SHA-0 and SHA-1、Christophe De Canniere、Christian Rechberger、CRYPTO 2008]、SHA-256 が 64 段中 36 段まで[Preimage Attacks on MD, HAVAL, SHA, and Others、Yu Sasaki and Kazumaro Aoki、CRYPTO 2008 Rump]、SHA-512 が 64 段中 24 段まで[FSE 2009]可能となった。第 2 原像攻撃では、SHA-256 が 64 段中 24 段まで、SHA-512 が 64 段中 24 段まで可能となった[Preimage Attacks on Reduced Tiger and SHA-2、Takanori Isobe、Kyoji Shibutani、FSE 2009]。

3.4.4. 公開鍵暗号の解読技術

素因数分解に関しては、数体篩法の内部で利用される楕円曲線法(ECM)などの高速化が進展している。モンゴメリ型楕円曲線の代わりに、効率的な演算規則を持つエドワーズ型楕円曲線を GMP-ECM に組み込み 7% の高速化に成功したことが報告された[Edwards Curves and the ECM Factorisation Method、Peter Birkner、ECC 2008]。

離散対数問題に関しては、素体上の離散対数問題に対する ρ 法を高速化する方法の提案が行われ、1024 bit のランダム素体の離散対数問題に対する ρ 法が従来より 10 倍以上高速化された[Speeding up the Pollard Rho Method on Prime Fields、Jung Hee Cheon、Jin Hong and Minkyu Kim、ASIACRYPT 2008]。

楕円曲線上の離散対数問題に関しては、Certicom 社の ECC challenge（楕円曲線に関する暗号解読コンテスト）でまだ解けていない ECC2K-130 の攻撃計算量について、2 万台のマシンを 2 年稼動させれば解読可能との見積もりが報告された[Implementing a Feasible Attack against ECC2K-130 Certicom Challenge、Ahmad Lavasani、Reza Mohammadi、ANTS-VIII poster]。また、ある条件を満たす拡大体上に定義された楕円曲線の定義体上有理点に関する離散対数問題を解く準指数時間アルゴリズムの報告が行われた。Weil Descent Attack の一種と見られる。しばしば利用される 2 の拡大体にはこの条件は適用できないとのこと。以前から指摘されている事ではあるが、こうした曲線を使用する場合は注意してパラメータを選ぶ必要がある。[An update on ECDLP over extension fields、Claus Diem、ECC 2008 rump]。

その他、PKC 2007 で提案されていた多変数公開鍵暗号系である ℓIC を用いた署名方式 ℓIC ーに対して、署名偽造や秘密鍵の解読が可能なことが報告されている[Total Break of the ℓ-IC Signature Scheme、P.A. Fouque、G. Macariorat、L. Perret and J. Stern、PKC2008]

3.4.5. その他の解読技術

多くの車のドアロックシステム、また欧米のほとんどのガレージ開閉システムに採用されている KeeLoq システムに対する現実的な攻撃が報告された。KeeLoq システムでは

Manufacturer 鍵は一意で、それとシリアル番号とから、各コントローラーのデバイス鍵が作られる。システムのすべてのレシーバーには、Manufacturer 鍵が埋め込まれており、送られてくるシリアル番号とからデバイス鍵を認証する。電力解析により、実際の製品から、Manufacturer 鍵やデバイス鍵を取り出すことに成功し、鍵の複製や本物の鍵を無効にすることができた。ECC 2008 では公演中の実製品攻撃デモンストレーションに成功した[On the Power of Power Analysis in the Real World: A complete Break of the KEELOQ Code Hopping Scheme、Thomas Eisenbarth、Timo Kasper、Amir Moradi、Christof Paar、CRYPTO 2008] [On the Power of Power Analysis in the Real World、Timo Kasper、ECC 2008]。

CRYPTO 2008 の招待講演にて Adi Shamir からブロック暗号、ストリーム暗号、MAC など広範囲の暗号に適用することができる非常に強力な代数的攻撃手法である CUBE attack が紹介された[How to Solve it: New Techniques in Algebraic Cryptanalysis、Adi Shamir、CRYPTO 2008]。

3.5. 暗号調査ワーキンググループ開催状況

2008 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 3.3 の通りである。

表 3.3　2008 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	佐々木 良一	１．CRYPTREC が今年度策定した電子政府推奨暗号リストの改訂に関する骨子に基づき、リストガイドで取り扱う対象技術の体系化やロードマップについて検討。 ２．対象仕様の明確化。
ID ベース暗号 WG	高木 剛	１．ID ベース暗号、ペアリング利用技術の安全性評価手法の調査 ２．ID ベース暗号、ペアリング関連技術の実用化に関する動向調査 ３．ID ベース暗号、ペアリング関連技術の標準化に向けた検討

3.6. 委員会開催記録

2008 年度、暗号技術監視委員会は、表 3.4 の通り 4 回開催された。暗号技術調査ワーキンググループは、表 3.5 及び表 3.6 の通り計 8 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) 暗号技術監視委員会

表 3.4　暗号技術監視委員会の開催

回	年月日	議題
第 1 回	2008 年 7 月 28 日	活動方針、リスト改訂及び公募要項の検討、監視状況の報告
第 2 回	2008 年 10 月 28 日	WG 活動の中間報告、公募要項の検討、監視状況の報告
第 3 回	2008 年 12 月 19 日	WG 活動の中間報告、公募要項の検討、シンポジウム開催準備及び監視状況の報告
第 4 回	2009 年 3 月 4 日	WG の報告書案の検討、シンポジウムの開催報告、CRYPTREC Report 2008 の検討

(2) 暗号技術調査ワーキンググループ

表 3.5　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	2008 年 9 月 2 日	活動目的と報告内容の確認、作業の割り振り
第 2 回	2008 年 11 月 28 日	調査内容の中間報告とその検討
第 3 回	2009 年 1 月 9 日	調査内容の中間報告とその検討
第 4 回	2009 年 3 月 3 日	報告書案の検討

表 3.6　暗号技術調査ワーキンググループ(ID ベース暗号)の開催

回	年月日	議題
第 1 回	2008 年 9 月 11 日	活動目的と報告内容の確認、作業の割り振り
第 2 回	2008 年 11 月 20 日	調査内容の中間報告とその検討
第 3 回	2008 年 12 月 18 日	調査内容の報告とその検討、特徴の調査とその検討
第 4 回	2009 年 2 月 17 日	報告書案の検討、標準化に向けた課題の検討

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

本ワーキンググループの 2008 年度の活動目的は、2007 年度のリストガイド策定の目的である、「電子政府推奨暗号の適切な利用のために、CRYPTREC のアウトリーチ活動として、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に係る技術的解説書」という位置づけを踏襲しつつ、2013 年に予定されている電子政府推奨暗号リストの体系の見直しを視野に入れて、リストガイドについてもその位置づけを整理した上で、優先度を考慮した改版を行い、これを暗号技術監視委員会に報告することである。

4.1.2. 委員構成（敬称略、五十音順）

主査： 佐々木 良一 （東京電機大学）
委員： 駒野 雄一 （株式会社東芝）
委員： 田中 秀磨 （独立行政法人情報通信研究機構）
委員： 田村 裕子 （日本銀行）
委員： 古屋 聡一 （株式会社日立製作所）
委員： 盛合 志帆 （ソニー株式会社）
委員： 渡辺 創 （産業技術総合研究所）

4.1.3. 活動方針

2007 年度に策定したリストガイドにおいては、標準的なセキュリティ技術において電子政府推奨暗号リストに掲載されている暗号アルゴリズムの利用形態を分析し、それぞれの利用形態について、推奨される暗号アルゴリズム、および推奨されるセキュリティパラメータを示した。2007 年度のリストガイドでは、標準的な利用方法に関する網羅性は確保できたが、一方で電子政府における調達元と調達先にとって一意に参照できる形態が望ましいこと、また策定する利用方法や仕様は暗号モジュール評価に対して曖昧さを残さないことが求められること、暗号技術の実際の利用状況から次期リスト策定前に推奨となる実装を示す技術が存在すること、などの課題が存在した。

そこで、2008 年度のリストガイド WG においては、上記の課題に対応するために、以下の活動方針のもと、活動を行った。

- リストガイドを、電子政府における利用形態ごとの暗号技術仕様と位置づけて体系化し、識別子を付与することにより、調達の際に識別子によって一意に調達仕様が示すことができるようにする。
- 体系におけるリストガイドを 2013 年までに整備することを念頭に、優先順位の高い利用形態と技術から、推奨される利用方法や技術仕様をまとめる。
- 暗号モジュール評価における評価対象の仕様での曖昧さを解消するため、モジュール評価における評価者にとって曖昧でない利用方法を提示すること。
- 現在、広く使われているが電子政府推奨暗号リストにおいて標準化されていない技術について、2013 年より前にも推奨される使われ方を示す必要があるため、リストガイドの中で推奨を示す。

本 WG の 2008 年度の活動では上記の方針に沿って、

- 優先順位の高い「PKI 向け電子署名」
- 現在電子政府推奨暗号リストに存在しない、メッセージ認証子と暗号利用モードについて、仕様の策定を行った。

4.1.4. リストガイドの位置付け

2008 年度のリストガイドは、暗号技術を利用したシステムの調達を行う調達元とシステムの構築を行う調達先が、暗号技術の実装に関する仕様の共通の参照先として使われると同時に、暗号モジュール評価においても参照されることを想定している。仕様策定にあたっては、2007 年度版リストガイドと同様、作成完了後 3 年間程度において有効な内容として執筆を行った。

4.1.5. 活動概要

2008 年度は、PKI 向け電子署名、メッセージ認証子、暗号利用モードについて、リストガイドの検討を行った。

まず、最初の検討として、各技術について電子政府における利用形態の調査を行った。その上で、ISO、IETF などの国際標準規格において、既に規格化されている内容について調査を行い、それらの標準の内容について、我が国の電子政府における利用に問題がない場合にはその内容に沿った執筆内容とし、不足点、問題点がある場合にはその不足点を補う検討を行い追加の記述を行った。

リストガイドの構成は、それぞれの技術が分冊的に参照されることを考慮し、共通的に以下の通りとすることとした。

(ア) 本文書の位置づけ

文書の目的、Introduction など

(イ) 定義

用語および記号などの定義

(ウ) 技術概要

基本的なセキュリティ機能、利用のモデル、技術の構成要素、主要技術の仕様、比較

(エ) 実装仕様

各技術の実装仕様

(オ) テストベクトル

実装評価などに用いるテストベクトル

その上で、リストガイドを記述する上で以下の議論を行った。

(1) PKI 向け電子署名

- 記述の対象を DSA、ECDSA、RSASSA-PKCS1-v1_5, RSASSA-PSS とした。
- DSA、ECDSA については、ドラフトであるが、FIPS-186-3 draft をベースに記載を行い、その他の標準については参考情報として記載した。
- 安全性については、SP 800-57 を基本に進め、CRYPTREC の監視状況に基づく見解も含めることとした。

(2) メッセージ認証子

- 記述の対象を、HMAC、CBCMAC、CMAC とした。
- HMAC については、FIPS198 をベースとし、CMAC については NIST SP 800-38B をベースとして記述した。
- CBC-MAC は、金融業界で利用されているため、互換性維持の観点から基本的にはリストガイドとして作成するが、強いて利用する必要がない場合には推奨しないことを明示した。
- HMAC における SHA-1 の利用等、アプリケーションごとに要求条件が異なる場合には、それに関連する事項を参考情報として可能な限り掲載した。
- 内部で利用されている暗号プリミティブについては、現在の電子政府推奨暗号リスト（以下、現リスト）に記載される暗号プリミティブをベースに進めた。
- 現在使われていないと考えられる暗号プリミティブについては、国際標準に関する参考情報として記載した。
- MAC の出力の truncated output は、FIPS-198 を引用し、参考情報として提示した。

(3) 暗号利用モード

- 記述の対象を、ECB、CBC、CFB、OFB、CTR の各モードとした。
- 技術的詳細に関しては、SP800-38A をベースに記載した。
- CBC モードを長く続ける場合には誤りが発生しやすくなる等、利用するパラメータについて、標準仕様に記載されていない場合でも、アドバイス可能な事項は極力記載した。
- 細かいパラメータの推奨方法については、明確なものについては記述した。
- パディングの誤った利用方法については、注意を記述した。
- 各モードの特徴について、安全性、処理速度、並列処理、自己同期性、エラー伝播、パディングの必要性、初期ベクトルなどについて比較を行うとともに、簡潔な根拠を追記することとした。

また、活動においては、ISO などの国際標準との整合性、金融分野などの業界標準の動向を参考にし、記述内容の精査も合わせて行った。

上記の検討を行い、最終的に 2008 年度版リストガイドとしてとりまとめ、暗号技術監視委員会への報告を行った。

4.1.6. まとめ

本年度の活動では、国際標準との整合性を考慮しながら、PKI 向け電子署名、メッセージ認証子、暗号利用モードに関する推奨される利用方法、実装仕様をまとめた。今後の活動としては、本年度の策定内容について、CRYPTREC における監視活動の結果に基づいて、適宜維持管理を行うとともに、次年度以降、仕様策定の優先順位に応じてリストガイドの残りの項目について整備を進めることが必要である。活動の結果をまとめた報告書を別冊「2008 年度版リストガイド」として公表しているので、詳細はそちらを参照して欲しい。

4.2. IDベース暗号ワーキンググループ

4.2.1. 活動目的

2001年に利便性の高い公開鍵暗号としてペアリングという特別な数学的な性質を用いた「IDベース暗号」が提案されて以来、IDベース暗号、およびペアリングを利用した各種暗号技術の研究が活発に行われている。また、IEEEやIETFで標準化が行われるなど、実用化に近い段階に入っている。本技術分野は、近い将来電子政府での利用も見込まれ、その場合には、CRYPTRECにおける評価、および電子政府推奨暗号リストへの掲載を行うことも視野に入れる必要がある。

本ワーキンググループの活動目的は､将来IDベース暗号のCRYPTRECでの評価の実施や、電子政府推奨暗号リストにおける公募の実施の可能性の検討に向けた現状調査を行い、将来の検討に資する知見を取りまとめた調査報告書を作成し、これを暗号技術監視委員会に報告することである。

4.2.2. 委員構成（敬称略、五十音順）

主査：　高木　剛（公立はこだて未来大学）
委員：　伊豆　哲也　（株式会社富士通研究所）
委員：　岡本　健　　（国立大学法人筑波技術大学）
委員：　小林　鉄太郎（日本電信電話株式会社）
委員：　境　　隆一　（大阪電気通信大学）
委員：　高島　克幸　（三菱電機株式会社）
委員：　田中　秀磨　（独立行政法人情報通信研究機構）
委員：　花岡　悟一郎（独立行政法人産業技術総合研究所）

4.2.3. 活動方針

IDベース暗号、およびペアリング技術を将来CRYPTRECで評価、および公募するための事前調査として以下の観点での調査を行った。

- 技術の概要と想定されるアプリケーション
- 安全性評価手法と安全性評価の現状
- 実装アルゴリズムと実装の現状
- 国際会議における研究発表の動向、および標準化動向
- 製品動向、および知的財産権の動向

以上の調査から、安全性、実装性の面という理論的な成熟度と、アプリケーション、および製品動向という電子政府での利用方法という政府調達に関する成熟度の現状を把握した。その上で、上記の観点について、CRYPTREC での評価や公募に向けた今後の検討課題を洗い出し、次年度以降の検討に資することとした。

4.2.4. 活動概要

本ワーキンググループでは、4.2.3 に挙げた 5 つの面について調査を行い、以下のような動向を取りまとめた。

(1)技術の概要と想定されるアプリケーション

- ID ベース暗号技術の概要、および有用性について調査を行った。ID ベース暗号の有用な点として、PKI における認証局が不要となる点、新規ユーザへの対応が容易である点、未登録者への暗号データの送信が可能である点を挙げた。
- ID ベース暗号の課題としては、ID の信頼性の確保、鍵生成センタの信頼性の確保、鍵更新、ユーザ鍵の無効化といった運用面の課題を挙げた。
- ID ベース暗号を構成する基本的な構造を挙げた上で、既存の方式の分類を行った。
- ID ベース暗号から、放送暗号、属性暗号など多くのアプリケーションが発展していることを示した。
- 公開鍵インフラとして利用した場合のメリットとデメリットを深く考察し、特に公開鍵証明書が不要になるメリットがある一方、上記に挙げた鍵更新と無効化を考えた場合 PKI に対するメリットが少ないことも判明している。また、ID ベース署名自体には、PKI ベースの署名に対するメリットは認められない。一方で、基礎となるペアリングによって多くのアプリケーションが派生しており、その点における暗号学的メリットがあることを挙げている。

(2)安全性評価手法と安全性評価の現状

- ID ベース暗号における安全性は、既存の公開鍵暗号と同様に数学的に困難な問題への帰着によって行われることを示し、その上で ID ベース暗号の安全性レベルの定義と、数学的な仮定と、その強さの評価方法をまとめた。
- ペアリングを用いた暗号技術においては、新たな数学的仮定が数多く提案されている。まず、ベースとなる楕円曲線上における数学的に困難な問題について調査を行うとともに、ペアリング逆関数問題の困難性、および安全性証明に利用される問題に関する調査を行った。

(3)実装アルゴリズムと実装の現状

ここでは、特にペアリングに焦点を当て、ペアリングを実現する著名なアルゴリズムとして、Tate ペアリング、ηT ペアリング、Ate ペアリングについて、その実装アルゴリズムを示すとともに、PC、FPGA、スマートカード、組み込み用 CPU における楕円曲線、実行環境に応じた処理の実行時間をまとめた。

(4) 国際会議における研究発表の動向、および標準化動向

- ID ベース暗号、およびペアリング技術に関する国際会議における発表の動向の調査を行った。対象としては、IACR 主催の会議、IACR ePrint アーカイブ、その他の国際会議である。
- 発表論文は、基礎的な技術（主にペアリング計算の高速化やアルゴリズムの改良）と、応用技術、アプリケーションの提案の 2 種類に大別される。
- 国際標準化の動向を調査した。現状では、IETF、ISO/IEC、IEEE において標準化活動が認められるため、これらの内容を調査した。

(5) 製品動向、および知的財産権動向

- ID ベース暗号、およびペアリング技術を実装した製品について、製品のリスト、製品の概略、入手方法の調査を行った。16 の製品についての調査結果がまとまった。
- 「世界で少なくとも 600 万人が利用している」という報告もなされている。
- 知的財産権の調査として、日米の特許に関する状況の違いに触れながら、日本、および米国で出願されている特許の出願番号、出願日、出願人、出願の状態、特許の概要などについて調査結果をまとめた。

上記の調査内容をもとに、次年度以降の CRYPTREC における検討項目として以下の項目を指摘した。

- ID ベース暗号に関連する評価対象とする領域。ID ベース暗号を調達する際には、主に、数学的基盤、ペアリングアルゴリズム、プロトコル、運用の 4 つの点が定まっている必要があるが、CRYPTREC として扱うべき領域について検討する必要がある。
- ID ベース暗号を調達する際の課題。特に ID ベース暗号の利用に当たっては、鍵生成センタの運用などに条件があるほか、鍵更新、無効化、ID の信頼性など解決すべき課題があるため、これらの課題についての更なる検討が必要である。

上記の内容について、調査報告書としてとりまとめ、暗号技術監視委員会に報告した。

4.2.5. まとめ

本年度の活動では、IDベース暗号、およびペアリング技術に関する技術的成熟度、および政府調達に向けた標準化動向／製品動向などを導出した。今後は、前節の終わりに挙げた課題について重ねて検討を行う必要がある。活動の結果をまとめた報告書を、別冊「IDベース暗号に関する調査報告書」として公表しているので、詳細についてはそちらを参照して欲しい。

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/> 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	〒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 情報流通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.sw.nec.co.jp/middle/SecureWare/advancedpack/ http://www.nec.co.jp/access/prod/cipherunicorn.html
問い合わせ先	〒108-8558 東京都港区芝浦 4-14-22 日本電気株式会社　第一システムソフトウェア事業部 TEL：03-3456-3248, FAX：03-3456-7689 E-MAIL: info@mid.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/
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	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 情報セキュリティ推進センター　担当課長　畠山有子 TEL:03-3218-3406　FAX:03-3218-3638 E-MAIL:Hatakeyama.Yuko@aj.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.sw.nec.co.jp/middle/SecureWare/advancedpack/ http://www.nec.co.jp/access/prod/cipherunicorn.html
問い合わせ先	〒108-8558 東京都港区芝浦 4-14-22 日本電気株式会社　第一システムソフトウェア事業部 TEL：03-3456-3248, FAX：03-3456-7689 E-MAIL: info@mid.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/
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.sdl.hitachi.co.jp/crypto/mugi/ 英文： http://www.sdl.hitachi.co.jp/crypto/mugi/index-e.html
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) 日立製作所 ソフトウェア事業部 システム管理ソフトウェア本部　担当本部長　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.sdl.hitachi.co.jp/crypto/s01/index-j.html 英文： http://www.sdl.hitachi.co.jp/crypto/s01/index.html
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) 日立製作所 ソフトウェア事業部 システム管理ソフトウェア本部　担当本部長　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 RSA セキュリティ社(http://www.rsasecurity.co.jp/) ・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/cryptobytes/cryptobytes_v5n2.pdf>

3. ハッシュ関数

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

暗号名	SHA-1, 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

CRYPTREC

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）

CRYPTREC 事務局

2009 年 3 月 27 日

目次

＜添付資料＞

別紙 1 暗号技術応募書（提出資料 1）
別紙 2 誓約書（提出資料 6）
別紙 3 公開の状況等に関する情報（提出資料 7）
別紙 4 自己チェックリスト（提出資料 9）

1. 公募の概要

総務省及び経済産業省が開催している暗号技術検討会（座長：今井秀樹中央大学教授）では、電子政府利用等に資する暗号技術の評価等を行っており、2003年2月に発表した電子政府における調達のための推奨すべき暗号のリスト（以下、「電子政府推奨暗号リスト」又は「現リスト」という。）の改訂を行うことを目的として、「電子政府推奨暗号リストの改訂に関する骨子(案)」（以下、「骨子案」という。）を作成し、2008年8月6日から2008年9月5日までの間、当該骨子案について意見募集[1]を行いました。

意見募集の結果[2]を踏まえ、CRYPTRECでは、「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）」を策定しましたので、公表いたします。

（1） これを受けて、CRYPTREC は評価対象暗号技術を公募し、CRYPTREC 事務局の情報通信研究機構及び情報処理推進機構（以下、「事務局」という。）は、暗号技術評価を実施します。
（2） 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します。その結果は、事務局が開催するワークショップ(「9. ワークショップ」を参照のこと。)や報告書等を通じて、一般に公表することを予定しています。応募者にとって不利益と解される情報を含むこともあり得ます。
（3） 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します。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、現リストに登録されている暗号技術の再評価も行います。
（4） CRYPTREC 内に設置された「評価委員会(仮称)」が、評価結果に基づき、「CRYPTREC 暗号リスト（仮称)」（以下、「次期リスト」という。）への暗号技術の記載について判定し、暗号技術検討会に答申します。答申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ます。決定については、2012 年度実施を予定しています。なお、仮称付きの語句に関しては、「5. 公募の目的」又は骨子案をご覧下さい。

2. 公募の対象

2.1. 暗号技術の種別

（1） 共通鍵暗号技術
共通鍵暗号技術に関しては、以下の暗号技術の種別に属する方式を公募します。
a) 128bit ブロック暗号 （鍵長 128bit/192bit/256bit）
b) ストリーム暗号 （鍵長 128bit 以上）

[1] http://search.e-gov.go.jp/servlet/Public?CLASSNAME=Pcm1010&BID=145207347
[2] http://search.e-gov.go.jp/servlet/Public?ANKEN_TYPE=3&CLASSNAME=Pcm1090&KID=145207347

(2) メッセージ認証コード
鍵長が128bitである128bitブロック暗号及び64bitブロック暗号を利用したメッセージ認証コードを公募します。

(3) 暗号利用モード
秘匿に関する128bitブロック暗号及び64bitブロック暗号を対象とした利用モードを公募します。

(4) 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です。

2.2. 応募暗号に関する留意事項

(1) ブロック暗号及びストリーム暗号については、現リストに掲載されている暗号技術と同等以上の特長（安全性又は実装性）を持つ技術に限ります。
(2) 同一の技術的根拠を有する方式に関しては、最善な方式を選択して、1つの暗号技術の種別のみに応募して下さい。
(3) 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、又は、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に限ります。
(4) 国内及び国外において評価が可能であり、かつ、第三者が全ての機能を実装可能となる情報を開示してあるものに限ります。評価を依頼する際に必須なものです。したがって、応募書類受付締切までに公知であることを明確にして下さい。なお、万一応募書類締切時点までに公知にできない理由がある場合には、2009年9月末までに事務局へ相談して下さい。
(5) 評価する際に知的財産の利用が無償で行えるものに限ります。
(6) 公募する暗号技術、又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であることを条件とします。

3. 応募方法

(1) 提出期限
2009年10月1日から2010年2月4日17時（必着）までに情報通信研究機構・情報通信セキュリティ研究センター内 CRYPTREC事務局宛てに郵送又は宅配便にて提出

して下さい。また、書類提出は、郵送又は宅配便でのみ受付け、応募者持参による受付は行いません。なお、送料は発信元払いでお願いします。

（2） 提出物

提出書類（文書及び電子媒体）（「6. 提出書類」を参照のこと。）を1つの封筒に入れ、「暗号技術応募」と表に朱記の上、提出して下さい。1応募暗号技術につき1封筒での提出として下さい。

電子媒体については、全ての電子データをCD-R（ISO 9660 Level 1又はJoliet形式）にまとめて入れ、暗号技術名と応募者名を記入して下さい。なお、提出物については返却致しませんのでご了承下さい。

（3） 応募に関する問い合わせ及び提出先

情報通信研究機構　情報通信セキュリティ研究センター内　CRYPTREC事務局宛
〒184-8795　東京都小金井市貫井北町四丁目2番1号
e-mail：　info@cryptrec.go.jp
FAX：　042-327-5609
問い合わせの受付はe-mail又はFAXのみとします（電話での問い合わせは、ご遠慮下さい）。

4. 応募に際しての留意事項

（1） 応募に際しては、提出書類（「6. 提出書類」を参照のこと。）に漏れが無いことを確認の上、応募者側で自己チェックリストを記入し、提出書類に添えて提出して下さい。
（2） 別紙2（p.22参照）の誓約書を提出して下さい。
（3） 本公募の実施に際し、事務局と応募者との間での金銭の授受は行いません。暗号技術の開発、書類の作成、自己評価その他の応募に際して応募者側で発生する費用、及び追加資料等の作成及び提出、実装性評価時の立会い等に際して応募者側で発生する費用は、応募者が負担して下さい。評価の委託その他の事務局側で発生する費用は事務局が負担します。
（4） 評価者（外部評価者を含む）については、審査の公平性の観点から、応募者に対して開示しません。
（5） 応募担当者は、適時連絡が取れ、日本語が話せる方として下さい。特に、応募書類受付締切から応募暗号説明会までの期間は、常時連絡が取れるようにお願いします。また、応募担当者の連絡先等に変更が生じる場合は、速やかに事務局へ暗号技術応募書（電子データ含む）の更新版を送付願います。
（6） 提出資料の不備、暗号技術に関連する知的財産の実施・利用やライセンス上に問題がある等、評価の実施が困難であると事務局が判断した場合には、応募資格を喪失する場合がありますのでご了承下さい。

5.　公募の目的

5.1.　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」という。）を発表しました。

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ました。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ました。

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ます。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ります。

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ります。

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やすさや導入コスト、相互運用性、普及度合い等の観点も取り入れる必要性が指摘されているところです。

これらの状況を踏まえ、2013 年度以降の電子政府における暗号技術の利用に当たり、信頼性のある暗号技術のリストとして、現リストの改訂を行います。この結果は、電子政府において暗号技術を利用する際の参考として様々な形で利用されることが期待されます。

5.2.　新しい CRYPTREC 暗号リストの構成と本公募の位置づけ

先に述べた背景に従い、2013 年度から、推奨する暗号のリストのみから構成される現リストから、新たな推奨暗号の体系に移行する予定です。

今回の見直しに合わせて、下記の（1）～（3）の各リスト及び(4)リストガイドをまとめて「CRYPTREC 暗号リスト（仮称）」（以下、「次期リスト」という。）として公開します。

(1)　電子政府推奨暗号リスト（仮称）
(2)　推奨暗号候補リスト（仮称）
(3)　互換性維持暗号リスト（仮称）
(4)　リストガイド

CRYPTREC により安全性が確認された暗号技術は、（1）～（3）の 3 つのリストのいずれかに登録されます。各リストへの登録は、WTO 政府調達協定との整合性に配慮し

つつ、安全性や市場動向により決定されます。登録の見直しは一定の間隔で行います。
　現リストに掲載されている暗号技術については、安全性の再評価を行った上で次期リスト運用開始前に推奨暗号候補リスト（仮称）へ登録されていたものとして扱います。次期リスト運用開始時には、新たに応募された技術と共に製品化の状況・技術の利用状況等により電子政府推奨暗号リスト（仮称）へ登録するか否かの決定を行います。

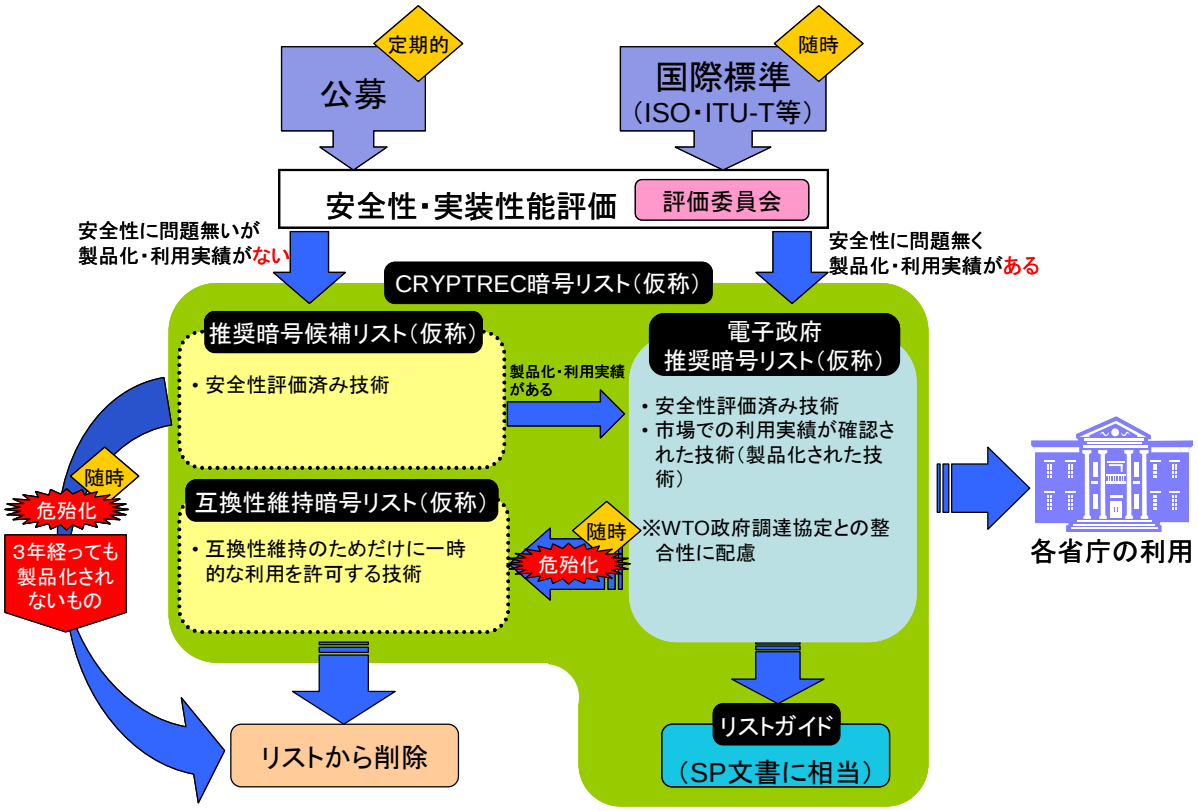


図 1.　リスト改訂概念（案）

次期リストにおけるそれぞれのリストの役割は以下のとおりです。

（1）電子政府推奨暗号リスト（仮称）

　CRYPTREC により安全性が確認され、かつ市場において利用実績が十分である暗号技術リスト。電子政府構築（政府調達）の際には当該技術の利用を推奨します（現リストと同等の位置づけ）。ここに登録される技術は国際標準化機関等により、標準化されていることが望まれます。

（2）推奨暗号候補リスト（仮称）

　CRYPTREC により安全性が確認されているが、市場において利用実績が十分でない普及段階にある暗号技術が登録されているリスト。今後、利用が期待される新規技術等はここに分類されます。電子政府構築（政府調達）の際には当該技術も利用することができます。

本リストに登録された技術は、一定期間ごとに普及の度合いの調査を行い、利用実績が十分であると認められれば電子政府推奨暗号リスト（仮称）に登録されます。また、利用実績が十分であると認められなかった場合にはここから削除されます。危殆化が生じた暗号技術については、随時ここから削除されます。

(3) 互換性維持暗号リスト（仮称）

電子政府推奨暗号リスト（仮称）に登録されていたが、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もののうち、互換性維持のために継続利用を容認するもののリスト。暗号解読のリスクと、電子政府システムにおける移行コスト等を勘案して、定期的に掲載継続の可否を判断します。CRYPTREC として互換性維持以外の目的では利用を推奨しません。

(4) リストガイド

電子政府で利用されている、あるいは利用する可能性のある暗号技術について、その技術概要と、推奨する利用方法を記述します。また、次期リストに記載された技術の中で、安全性を維持するため正しいパラメータの設定が要求される技術における具体的なパラメータ設定方法の記述を行います。さらに、将来必要になると予想されるセキュリティ技術については、その開発状況や利用可能性について記載します。リストガイドは、システム運用者及び設計者の利用や、システム利用者への啓発を目的とします。

今回の暗号技術の公募は、現リストにおいて早期にリストの改訂が必要である技術カテゴリを対象として、推奨暗号候補リスト（仮称）、あるいは電子政府推奨暗号リスト（仮称）へ登録するための、安全性及び実装性の評価を行うことを目的に行います。

6. 提出書類

今回の応募に際して必要な提出書類は以下のとおりです。なお、提出された情報については、CRYPTREC 統一 Web サイト（http://www.cryptrec.go.jp/）にて公開する予定です。

項番	提出書類	1.記述言語 2.提出形式	作成要領の書式	電子データのファイル名	参照ページ
6.1	暗号技術応募書	1.和文及び英文 2.文書及び電子データ	別紙 1	和文:09appl_j.pdf 英文:09appl_e.pdf	9
6.2	暗号技術仕様書	1.和文及び英文 2.文書及び電子データ	なし	和文:09spec_j.pdf 英文:09spec_e.pdf	9
6.3	自己評価書	1.和文及び英文 2.文書及び電子データ	なし	和文:09eval_j.pdf 英文:09eval_e.pdf	10
6.4	テストベクトル	2.電子データのみ	なし	半角英数で、任意	11
6.5	参照ソースコード	1.英文 2.電子データのみ	なし	半角英数で、任意	12
	参照ソースコード仕様書	1.和文及び英文 2.文書及び電子データ	なし	和文:09sref_j.pdf 英文:09sref_e.pdf	
	参照ハードウェア設計記述	1.英文 2.電子データのみ	なし	半角英数で、任意	
	参照ハードウェア設計記述仕様書	1.和文及び英文 2.文書及び電子データ	なし	和文:09href_j.pdf 英文:09href_e.pdf	
	テストベクトル生成ソースコード	1.英文 2.電子データのみ	なし	半角英数で、任意	
	テストベクトル生成ソースコード仕様書	1.和文及び英文 2.文書及び電子データ	なし	和文:09tvec_j.pdf 英文:09tvec_e.pdf	
6.6	誓約書	1.和文 2.文書の原本	別紙 2	なし	13
6.7	公開の状況等に関する情報	1.和文 2.文書及び電子データ	別紙 3	和文:09publ_j.pdf	13
6.8	応募暗号説明会発表資料	1.和文及び英文 2.文書及び電子データ	なし	和文:09brfg_j.pdf 英文:09brfg_e.pdf	14
6.9	自己チェックリスト	1.和文 2.文書の写し	別紙 4	なし	14

表 1. 提出書類一覧

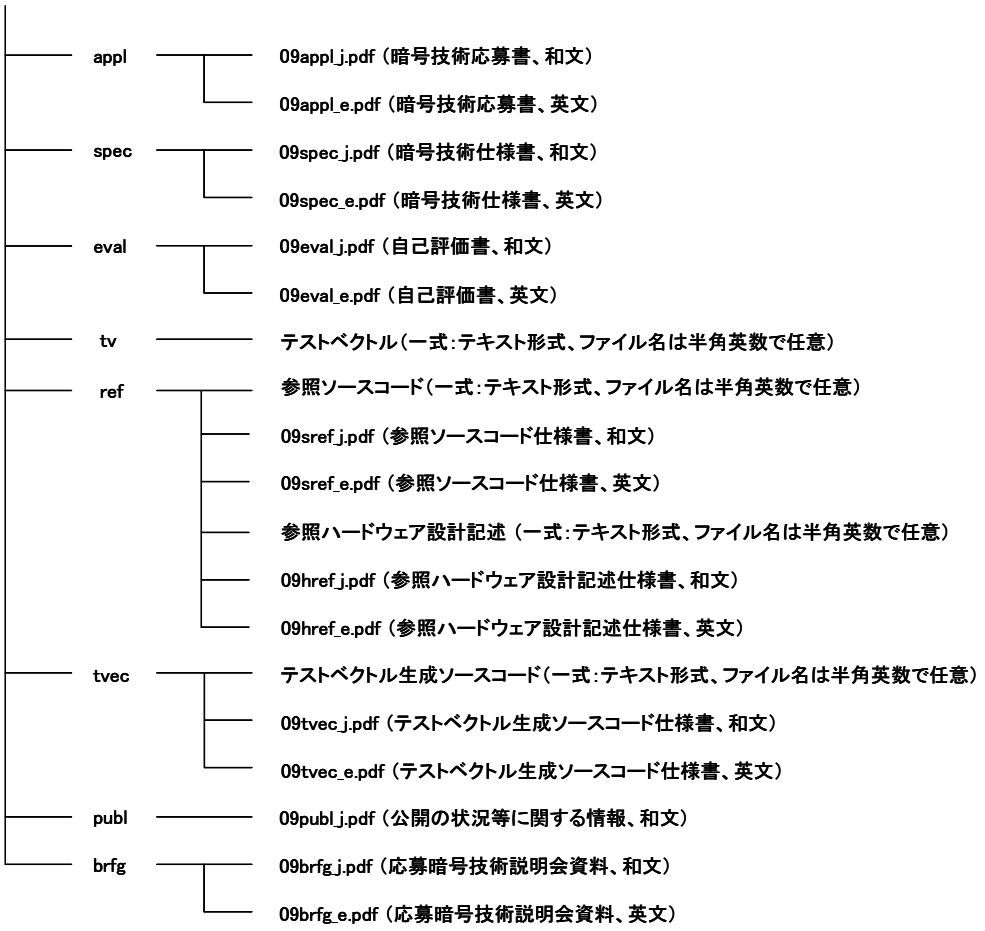


図 2. 提出書類（電子データ）の構成図

ⅰ）提出書類となる各種電子ファイルは、上に示すようなファイル名（半角英数）をつけて下さい。

ⅱ）電子ファイルは、それぞれ上に示すようなディレクトリを作成し、対応するディレクトリ直下に保存して下さい。（ディレクトリ名は半角英数）

注）

〇文書については、全て日本工業規格 A4 判として下さい。

〇6.1～6.3、6.5 及び6.8 は、和文・英文両方の提出が必要です。和文を正文とし、両者の内容に齟齬があった場合は和文を優先しますが、可能な限り同一の内容として下さい。評価の実施に関して支障が出る場合には応募資格を喪失することもあり得ます。

〇6.1～6.3、6.5、6.7 及び6.8 のファイル形式については、以下のものとし、表 2 に示したファイル名を使用して下さい。

・Adobe PDF 形式

日本語版：Adobe Acrobat 日本語フォントで読めるもの

英語版：Adobe Acrobat で読めるもの

〇6.4 及び6.5 のプログラムの電子データについては、テキスト形式として下さい。

〇評価においては国外における評価も想定していますので、提出書類のうち6.1～6.3、6.5 及び6.8 の電子媒体については、全ての電子データを CD-R(ISO 9660 Level 1 又

は Joliet 形式)にまとめて入れ、暗号技術名と応募者名を記入して下さい。

それぞれの提出書類について、以下に説明します。

6.1. 暗号技術応募書（別紙 1 の書式）

ⅰ）応募日
・応募書提出日を記入して下さい。

ⅱ）暗号技術名
・正式名称を読み方も含めて記述して下さい。また、正式名称が長い場合は、略称名を 5 文字程度のアルファベット表記で記述して下さい。

ⅲ）応募暗号技術公開ホームページ URL
・国内外の暗号技術者が、評価を行う際に必要となるデータを参照できるホームページ URL を記入して下さい（和文及び英文)。

ⅳ）応募暗号種別
・該当する項目を 1 つだけ選択して下さい。

ⅴ）応募責任者
・今回の応募に関する一切の責任を負う方とします。
・本応募に関する責任者の企業・団体名、所属・役職及び氏名を記入して下さい。

ⅵ）応募担当者
・今回の応募に関し、事務局との問い合わせ・連絡窓口となる方とします。
・本応募担当者は、日本語が話せる方として下さい。
・応募担当者の氏名、企業・団体名、所属・役職、所在地、電話番号（代表、直通を明記)、FAX 番号及び e-mail アドレスを記入して下さい。

ⅶ）開発者
・開発者の氏名及び企業・団体名を記入して下さい。

ⅷ)応募暗号調達窓口
・次期リスト策定後 3 年以内までに調達可能であることが応募条件であることから、応募暗号技術を調達する場合の窓口（連絡先）を記述して下さい。
・応募時点で正式な調達窓口が設置されていない場合においても、調達に関する問い合わせに答えられる仮窓口を記述して下さい。

ⅳ)応募暗号説明会
・応募暗号説明会における発表予定者名、参加人数を記述して下さい。

6.2. 暗号技術仕様書

ア　設計方針、設計基準
ⅰ)応募暗号技術についての設計方針及び設計基準を記述して下さい。
ⅱ)共通鍵暗号の場合は、現リストに記載された暗号技術と同等以上の特長(安全性又は実装性等）についても記述して下さい。

イ　暗号アルゴリズム（実装に必要な全情報）
第三者が評価・実装するために十分な仕様が完全に記述されていることが必

要です。記述が十分でない場合、応募資格を喪失することがあります。具体的には以下に従って下さい。

ⅰ）暗号アルゴリズムの完全な仕様を記述して下さい。アルゴリズムの実装に必要なすべての情報（数式、テーブル、アルゴリズム、図及びパラメータ）を記述して下さい。

ⅱ）暗号鍵等のパラメータの設定に条件がある場合には、パラメータの設定基準、推奨値も記述して下さい。

ⅲ）共通鍵暗号で複数の鍵長をサポートする場合には、互換性の有無に関しても明記して下さい。

ⅳ）応募技術の入出力は、ビット列レベルで記述して下さい。

ⅴ）入力が Z/nZ（Z は有理整数環）の元等、実装する上で実現法が一意に定まらない場合は、ビット列への変換法の推奨方式も同時に提示して下さい。

ⅵ）endian の種類を記述して下さい。

ⅶ）高速実装やコンパクト実装に関する方法等があれば記述して下さい。

ⅷ）実装方法についての説明

本応募暗号技術を実装するために必要な実装手順等の情報を記述して下さい。

情報が不十分であるために実装ができない場合には、応募資格を喪失することがあります。

また、評価に必要な情報の追加提出を求めることがあります。

ウ　バージョン情報

今回の応募以外に、同一若しくは類似した名称で他に発表又は応募した暗号技術、同一仕様で名称が異なった暗号技術等があれば列挙して下さい。

また、それぞれの相違点を明記して下さい。また、バージョン更新時に推奨パラメータが変更された場合には、変更した理由を明記して下さい。

バージョンの更新について、設計思想、安全性及び実装性の違いを明確に記述して下さい。また、バージョン更新をした理由についても明記して下さい。

異なるバージョン間における互換性の有無を完全に記述して下さい。バージョンが異なる場合に想定されるユーザー側のメリット及びデメリットについても記述して下さい。

エ　利用実績・推奨用途等

応募暗号技術に係る利用実績や推奨用途について記述して下さい。

6.3. 自己評価書

応募される暗号技術に対する応募者自身による自己評価情報を記述して下さい。自己評価が十分でないと判断される場合には、応募資格を喪失することがあります。

また、ウ・エ・オ・カの項目については詳細に記述して下さい。

ア　設計思想

他の著名な暗号技術との差別化、優位性等も含め記述して下さい（既存の技術と比べて優位性がある部分、提案技術が電子政府で使用するものとして妥当であると考えられる部分等）。

イ　ベースとして用いる理論（数学的仮定）・技術

応募される暗号に、ベースとして用いられている理論（数学的仮定）や技術について記述して下さい。

ウ　安全性に対する評価

応募される暗号の安全性に関する根拠及び通常想定される汎用的な攻撃法に対する対抗策を具体的に示して下さい。

想定する攻撃法に関しては、「7. 評価項目」を参考にして下さい。なお、評価項目に例示されている攻撃法が適用できない場合には、評価は必要ありませんが、その攻撃法が適用できないと判断した理由を明示して下さい。但し、全く自己評価がなされていない場合は、応募資格を喪失する場合があります。

応募暗号に固有の特殊な攻撃法が想定される場合には、その攻撃法に対し施した対抗策についても具体的に提出して下さい。

提案方式に対する既知の攻撃論文の有無や学会(ASIACRYPT、CRYPTO、EUROCRYPT、FSE、ISEC、PKC、SCIS 等)等で攻撃や問題点が指摘されている場合には、その攻撃論文を引用し、これに対する技術的コメントを記述して下さい。

証明可能安全性を主張する場合にはそのレベルを記述し、その論証を行うか、学会等で発表されているならその論文等について記述して下さい。

エ　ソフトウェアの実装性評価

速度評価、リソース使用量（コード量・ワークエリア)、記述言語、評価プラットホーム等を記述して下さい。また、実際に速度計測を行った場合には、計測法を詳細に記述して下さい。

※ブロック暗号に関しては、鍵スケジュール部単独の速度評価結果も記述して下さい。

オ　ハードウェアの実装性評価

使用したプロセス（Field Programmable Gate-Array、Gate-Array 等)、速度評価、設計環境、リソース使用量（Field Programmable Gate-Array の場合は使用セル量、Gate-Array 等の場合はゲート数）等を記述して下さい。

※ エンティティ認証は対象外です。

カ　サイドチャネル攻撃に対する評価

本項目は、自己評価書の提出に当たっては必須ではありませんが、サイドチャネル攻撃に対する耐性を主張する場合には、攻撃法、施した対抗策及び動作環境等についてできるだけ詳しく記述して下さい。学会等で発表されているならその論文等について記述して下さい。

キ　第三者評価実績

既に第三者評価を受けた実績がある場合には、評価者名及び評価結果を記述して下さい。開示可能であれば、報告書のコピーもあわせて（できるだけ電子データで）添付して下さい。

6.4. テストベクトル

実装性確認のために十分な量のテストベクトルを記述して下さい。十分な量のテストベクトルが提出されないときには応募資格を喪失することがあります。テストベクトルは暗号処理途中の中間結果と、暗号全体をブラックボックスと見な

したときの入出力対の 2 種類を提出して下さい。どちらのファイルもテキスト形式で生成し、キャラクタセットとしては ASCII のみを使って下さい。改行コードは MS-DOS 形式(CR+LF)とします。

暗号処理途中の中間結果については、応募暗号技術を第三者が実装する上でデバッグの役に立つ情報について、少なくとも入出力 1 対に対応するデータをなるべく詳しく記述して下さい。例えば、共通鍵暗号については繰り返し処理ごとの入出力等を記述して下さい。

暗号全体をブラックボックスと見たときの入出力対については、以下に示す応募する暗号技術ごとの方針に従って下さい。どの暗号技術についても、テストベクトルには endian の間違い等ビット列表記が反転した場合等を検出できるデータを含む等、テストベクトルとして相応しい入出力を選んで下さい。

乱数を用いる場合は、再度検証可能なように、擬似乱数生成系を用い、種(Seed)を明示して下さい。

ア　共通鍵暗号技術

ⅰ)ストリーム暗号

10 例以上の鍵に対し、8192bit 以上の処理例

ⅱ)ブロック暗号

10 例以上の鍵に対し、128 ブロック以上の処理例

イ　メッセージ認証コード

3 例以上の鍵に対し、3 例以上の処理例

ウ　暗号利用モード

3 例以上の鍵に対し、3 例以上の処理例

エ　エンティティ認証

共通鍵暗号を利用する場合には、3 例以上の鍵に対し、3 例以上の処理例。テストベクトルには、ランダムに生成されたデータを含んで下さい。

公開鍵暗号を利用する場合には、3 例以上の鍵に対し、3 例以上の処理例。テストベクトルには、ランダムに生成されたデータを含んで下さい。また、ベキ乗剰余等の数学的構造を含む場合は、境界条件となるデータを含んで下さい。

なお、再度検証可能なように、擬似乱数生成系を用い、種（Seed）を明示して下さい。

6.5. 参照ソースコード

ⅰ） 応募暗号技術の実装が実際に可能であることを確認するため、また応募暗号技術に関連する各種データの正当性の効率的な検証を可能とするために参照ソースコードとその仕様書を提出して下さい。

参照ソースコードは、ソフトウェアの実装性評価向けには ANSI C で、ハードウェアの実装性評価向けには Verilog-HDL で記述して下さい。なお、この目的を達成するため、参照ソースコードを見難くするような、処理中の機微データをゼロクリアする等の安全性を高めるような部分を記述する必要はありません。

ⅱ） 参照ソースコードでは、推奨パラメータを含む応募暗号技術の全ての機能を

実現して下さい。さらに、参照ソースコードの可読性を落とさない範囲で移植性の高いものとして下さい。例えば、ソフトウェア評価の場合には、endian 非依存とし、最低限 int、long、pointer の長さが 32bit の処理系で動くように作成して下さい。多倍長整数を利用する場合は GNU MP ライブラリなどの利用を推奨します。

iii） テストベクトル生成ソースコードとその仕様書も提出して下さい。テストベクトル生成プログラムは参照ソースコード中の関数を呼び出すものとします。

6.6. 誓約書（別紙 2 の書式）

本項目に関しては、別紙 2 の書式に従って記述して下さい。提出がない場合には、応募資格を喪失しますのでご留意下さい。

6.7. 公開の状況等に関する情報（別紙 3 の書式）

本項目に関しては、別紙 3 の書式に従い下記ア～ウの内容について記述して下さい。

ア 応募暗号技術の公開時期とその学会名

本公募では、仕様等が公開されている暗号技術を評価対象としていますので、仕様等の公開の状況を確認するために必要な情報（応募暗号技術が公開された時期、学会名、あるいは掲載文献名等）を提出して下さい。なお、応募時点で仕様等の公開がなされていない場合には、その時点での状況とともに、2010 年 9 月末までの公開スケジュールを提出し、応募暗号技術に関する論文発表や仕様書等の公開された際には、その状況を確認するために必要な情報を提出して下さい。

イ 輸出規制問題を解決していることの宣誓書とその証拠

応募された暗号技術の評価については、事務局より評価の一部を海外を含めた評価者に外部委託することを予定しており、提出された情報を我が国の非居住者である委託者に提供すること等も予想されます。このため、「6. 提出書類」の6.1～6.5 及び6.7 の情報のそれぞれについて、非居住者への提供等に際して輸出管理上許可が不要であると考える場合には、その根拠及び確認のための文書を提出して下さい（例えば、学会誌、雑誌、論文集等で既に公開されており不特定多数の方が自由に入手できる情報であるため許可不要と考える場合には、当該学会誌、雑誌、論文誌等の関連部分等を提出するとともに、公開形態についての説明を加えて下さい）。

ウ 知的財産権とライセンス

応募された暗号技術に関して取得あるいは出願中の特許、著作権、ライセンス方針等の知的財産に関する状況を応募書類の「自社特許とその扱い」の中で記述して下さい。

応募された暗号技術に関連し、他社が特許権、著作権等の知的財産を保有する場合、それらの権利関係についても、応募書類の「関連する他社の特許」の

中で可能な範囲で記述して下さい。

事務局及び評価者が評価の実施に際して必要となる知的財産の利用（特許法上の発明の実施、著作権法上の著作物（全ての応募書類）の複製・領布等、事務局が評価を委託する第三者による利用を含む）を無償で行えることを明記して下さい。知的財産上の制限により評価の実施が妨げられる場合は、応募資格を喪失することがあります。

また、政府機関で使用する場合のライセンス方針を記述して下さい（無償又は、妥当かつ非差別的な条件に限ります）。

なお、評価のために、事務局及び評価者が応募者と、秘密保持契約等の特別な契約を結ぶことはいたしません。

6.8. 応募暗号説明会資料

応募される暗号技術についての説明資料を作成し、Adobe PDF 形式にて提出して下さい。資料構成としては、以下を参考にし、説明内容は 15 分程度のもので作成して下さい。なお、白黒のハードコピーが配布資料となることにご留意下さい。

〈資料構成〉

１．表紙（応募暗号名、発表者名を記載）
２．技術仕様について
３．安全性に関する自己評価について
４．実装性に関する自己評価について
５．公開状況、ライセンス等について

6.9. 自己チェックリスト（別紙 4 の書式）

「自己チェックリスト」に従って内容を確認して下さい。このチェック結果を記入した「自己チェックリスト」の写しを、提出物と同じく封筒に入れて提出して下さい。

7.　評価項目

7.1.　評価スケジュール（予定）

応募暗号説明会開催：	2010 年 3 月頃
第 1 次評価実施：	2010 年 4 月～2011 年 3 月
第 1 回ワークショップ開催：	2011 年 2 月頃
第 2 次評価実施：	2011 年 4 月～2012 年 3 月
第 2 回ワークショップ開催：	2012 年 2 月頃
2012 年度シンポジウム：	2013 年 2 月頃

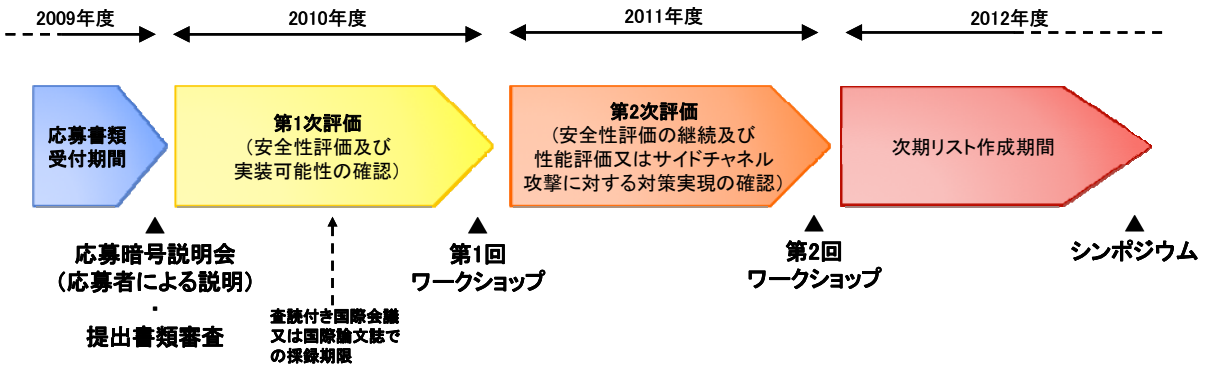


図 3.　評価スケジュール（予定）

7.2.　共通鍵暗号技術

共通鍵暗号については、現リストに掲載されている暗号技術と比較して安全性又は実装性において優れた暗号技術を公募します。そのため、評価においても現リストに掲載された暗号に対する優位点の評価を行います。

（１）安全性評価項目

暗号は守秘目的以外にも利用されるので、いわゆる暗号文単独攻撃以外の既知平文攻撃、(適応的)選択平文・暗号文攻撃、関連鍵攻撃、選択IV攻撃等、攻撃者にとって非常に都合のよい環境での耐性も評価します。

ア　ブロック暗号に関する評価項目

差分攻撃法や線形攻撃法等の既知の一般的な攻撃法に対する耐性を評価します。また、応募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ります。その他、サイドチャネル攻撃等に対する耐性についても評価します。

イ　ストリーム暗号に関する評価項目

time/memory/data-tradeoffや分割統治攻撃、相関攻撃、またGroebner基底計算アルゴリズムを元にした代数攻撃等の既知の攻撃法に対する耐性を評価しま

す。また、応募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ります。その他、サイドチャネル攻撃等に対する耐性についても評価します。

（２）実装性評価項目

ア　共通条件

「7.6 実装性評価について」を参照して下さい。

イ　ソフトウェア実装による評価項目

ソフトウェア実装に関しては、次の項目について評価します。

ｉ）標準的なプラットホーム上での処理速度、リソースの使用量（コード量、作業領域等）等を評価します。

ii）鍵スケジュール個別の処理速度も評価します。

ウ　ハードウェア実装による評価項目

使用するプロセス（Field Programmable Gate-Array、Gate-Array 等）別に、処理速度評価及びリソースの使用状況（Field Programmable Gate-Array の場合には使用セル数、Gate-Array 等の場合には使用ゲート数等）を評価します。

7.3. メッセージ認証コード

（１）安全性評価項目

利用ブロック暗号をもとにした証明可能安全性、特に適応的選択文書攻撃や、検証オラクルを多数回呼び出したときの識別不能性について評価します。また、nonce や乱数要素の有無についても評価します。さらに利用ブロック暗号に対する仮定の強さ(ideal cipher model や関連鍵攻撃耐性)についても評価します。さらに、利用ブロック暗号に特定の方式を適用した場合の安全性についても評価の対象とすることがあります。

（２）実装性評価項目

ア　共通条件

「7.6 実装性評価について」を参照して下さい。

イ　ソフトウェア実装による評価項目

ソフトウェア実装に関しては、次の項目について評価します。

ｉ）標準的なプラットホーム上での処理速度、リソースの使用状況（コード量、作業領域等）等を評価します。

ii）鍵スケジュール個別の処理速度も評価します。

ウ　ハードウェア実装による評価項目

使用するプロセス（Field Programmable Gate-Array、Gate-Array 等）別に、処理速度評価及びリソース使用量（Field Programmable Gate-Array の場合には使用セル数、Gate-Array 等の場合には使用ゲート数等）を評価します。

7.4. 暗号利用モード

（１）安全性評価項目

利用ブロック暗号をもとにした証明可能安全性、特に適応的選択平文・暗号文攻撃に対する識別不能性について評価します。また、nonceや乱数要素の有無についても評価します。さらに利用ブロック暗号に対する仮定の強さ(ideal cipher model や関連鍵攻撃耐性)についても評価します。さらに、利用ブロック暗号に特定の方式を適用した場合の安全性についても評価の対象とすることがあります。

（２）実装性評価項目

ア　共通条件

「7.6 実装性評価について」を参照して下さい。

イ　ソフトウェア実装による評価項目

ソフトウェア実装に関しては、次の項目について評価します。

ｉ）標準的なプラットホーム上での処理速度、リソースの使用状況（コード量、作業領域等）等を評価します。

ii）鍵スケジュール個別の処理速度も評価します。

ウ　ハードウェア実装による評価項目

使用するプロセス（Field Programmable Gate-Array、Gate-Array 等）別に、処理速度評価及びリソース使用量（Field Programmable Gate-Array の場合には使用セル数、Gate-Array 等の場合には使用ゲート数等）を評価します。

7.5. エンティティ認証

（１）安全性評価項目

安全性の評価は、エンティティ認証としてのセキュリティに問題が生じないことを、形式的な手法を用いて行います。安全性を脅かす状態としては、なりすましの成功、セッションの取り換え等を想定します。

暗号プリミティブとして、電子政府推奨暗号リストに掲載されている、あるいは応募中の共通鍵暗号、公開鍵暗号、ハッシュ関数、メッセージ認証コードのみを利用している場合には、暗号プリミティブを理想的に安全なものとして安全性の評価を行います。その他の暗号プリミティブを用いる場合には、暗号プリミティブを理想化せずに安全性の検証を行います。

上記のいずれの場合も、提案者はプロトコルの安全性を示す情報を提出し、本公募における安全性評価では、これらの正当性を検証します。

（２）実装性評価項目

エンティティ認証プロトコルの実装性能評価として、ソフトウェアによる実装性評価を行います。標準的なプラットホーム上での処理速度、リソースの使用状況（コード量、作業領域等）等を評価します。通信時間は考慮しません。

ア　共通条件

「7.6 実装性評価について」を参照して下さい。

7.6. 実装性評価について

実装性評価について共通的な条件を記述します。実装性評価を行う目的は、

- 実現可能性の確認、
- 性能の評価
- サイドチャネル攻撃に対する対策実現の確認

の 3 つです。

（１）実現可能性の確認

- 提案された暗号アルゴリズムが、事務局が指定した動作環境において実装可能であり、かつ、動作可能であることを確認することが目的です。応募時に提出されたテストベクトルを処理できることを確認します。第 1 次評価期間内に実施します。
- 実現可能性の確認で用いた参照ソースコード及び参照ハードウェア設計記述は、性能の評価には利用しませんが、第三者が実装する場合の参考として公開する予定です。想定している動作環境は、以下のとおりです。
- 暗号利用モード及びメッセージ認証コードの実装性評価では､128bit ブロック暗号及び 64bit ブロック暗号を使用するものとします。ここで用いるブロック暗号は、事務局から提供します。

(i) ソフトウェアでの実現可能性の確認のための動作環境

- CPU: Intel x86 アーキテクチャ互換のプロセッサ
- Memory: 2GB 以上
- OS: Microsoft Windows のいずれかのエディション

(ii) ハードウェアでの実現可能性の確認のための動作環境

- FPGA : Xilinx FPGA XC5VLX30、もしくは、XC5VLX50

また、設計環境としては以下のとおりです。

(i) ソフトウェアでの実現可能性の確認のための設計環境

- 記述言語 : ANSI-C 言語
- Compiler: Microsoft Visual Studio

(ii) ハードウェアでの実現可能性の確認のための動作環境

- 設計記述言語 : Verilog-HDL
- 論理合成 : Xilinx ISE Foundation
- 配置配線 : Xilinx ISE Foundation
- 論理シミュレーション : Mentor Graphics ModelSim

（２）性能の評価

- 性能の評価は、安全性評価及び実現可能性の確認を通過し、次期リストへの掲載が可能と判断された暗号技術に対して第 2 次評価期間内に実施します。
- 性能の評価を行う動作環境については、実現可能性の確認で使用する動作環境に準じるものを想定していますが、性能の評価を実施する上で必要となる情報は、安全性評価及び実現可能性の確認の段階（2010 年 10 月頃）で、公開する予定です。
- 性能の評価で使用する実装については、事務局からソースコードの提出を要求しませんが、事務局が指定する動作環境にて実行可能なロードモジュールを応募者側で実装して頂き、事務局立会いにて実地で測定を行うことを想定しています。詳細については、2010 年度末までに CRYPTREC 統一 Web サイト（http://www.cryptrec.go.jp/）などを通じてアナウンスする予定です。
- ソフトウェアの性能の評価に関しては、通常の PC 環境における性能を測定します。各暗号技術の種別毎の評価項目については、7.2 から7.5 の該当する評価項目を参照して下さい。処理速度のほか、リソース使用量（静的メモリ量、動的メモリ量）の評価を想定しています。
- ハードウェアの性能の評価に関しては、FPGA 環境における性能をシミュレーションにより測定します。回路規模、クリティカルパス遅延及びスループットの測定を想定しています。

（３）サイドチャネル攻撃に対する対策実現の確認

- サイドチャネル攻撃に対する対策を実装アルゴリズムで実現できることを確認することが目的です。ソフトウェア実装及びハードウェア実装の両方を対象とします。第 2 次評価期間内に実施します。
- 原則として、提出された自己評価書に記述された対策技術を確認の対象としますが、応募書類提出後に学会又は論文誌に採録された応募暗号に関する対策についても、脅威の重要度・実現性等を考慮して、評価委員会（仮称）が別途認めたものを確認の対象とすることがあります。
- サイドチャネル攻撃に対する対策実現の確認で使用する実装については、事務局からソースコードの提出を要求しませんが、事務局が指定する動作環境にて実行可能なロードモジュールを応募者側で実装して頂き、事務局立会いにて実地で測定を行うことも想定しています。詳細については、2010 年度末までに CRYPTREC 統一 Web サイト（http://www.cryptrec.go.jp/）などを通じてアナウンスする予定です。

8. 応募暗号説明会について

応募された暗号技術の評価を開始するにあたり、応募者自ら公の場で、応募暗号技術の技術仕様、安全性、実装性、公開状況、及びライセンス等について説明する機会を設けます。本説明会は一般公開とし、全応募者が説明することを原則とします。

説明時間を 15 分程度、質疑応答時間を 10 分程度取ることを予定していますが、応募者数が多い場合には短くなることがあります。

正式日程などの詳細については、2009 年 10 月頃に CRYPTREC 統一 Web サイト（http://www.cryptrec.go.jp/）などを通じてアナウンスする予定です。

9. ワークショップについて

ワークショップ（「7.1 評価スケジュール（予定）」を参照のこと。）は、開催時点までの評価委員会（仮称）における最新の評価結果を公表し、それらを検討する場を設けるために開催されます。この機会を利用して、応募者が自らの意見を述べることもできます。

第 1 次評価実施期間（2010 年 4 月～2011 年 3 月）の後に開催予定の第 1 回ワークショップでは、応募暗号技術の安全性評価及び実現可能性の確認結果を公表する予定です。

第 2 次評価実施期間（2011 年 4 月～2012 年 3 月）の後に開催予定の第 2 回ワークショップでは、第 1 次評価実施期間後に継続して実施された安全性評価、性能の評価及びサイドチャネル攻撃に対する対策実現の確認結果を公表する予定です。また、現リストに掲載されている暗号技術に関する再評価の結果も公表する予定です。

詳細については、各年度の 10 月頃に正式日程を CRYPTREC 統一 Web サイト（http://www.cryptrec.go.jp/）などを通じてアナウンスする予定です。

10. シンポジウムについて

シンポジウム（「7.1 評価スケジュール（予定）」を参照のこと。）は、それまでに実施されてきた電子政府推奨暗号リストの改訂、暗号技術公募と評価活動及び次期リスト策定に関して、広く一般に報告するために開催することを想定しています。詳細については、確定し次第、CRYPTREC 統一 Web サイト（http://www.cryptrec.go.jp/）などを通じてアナウンスする予定です。

以 上

（別紙 1）

受付番号	

応募日　20　　年　　月　　日

CRYPTREC 事務局　御中

暗号技術応募書（提出資料 1）

暗号技術名：			略称名：
応募暗号技術公開ホームページURL：			
応募暗号種別			
１．共通暗号技術	a)128bitブロック暗号　b)ストリーム暗号		
２．メッセージ認証コード			
３．暗号利用モード			
４．エンティティ認証			
応募責任者			
企業・団体名：			
責任者氏名：	印	所属・役職：	
応募担当者			
企業・団体名：			
担当者氏名：		所属・役職：	
所在地：〒			
TEL：（代表）		（直通）	
FAX:		e-mail:	
開発者			
開発者名：		企業・団体名：	
応募暗号調達窓口			
担当者氏名：		所属・役職：	
企業・団体名：		所在地：〒	
TEL:	FAX:	e-mail:	
応募暗号説明会			
発表者氏名：		参加人数：	
TEL:	FAX:	e-mail:	

（別紙 2）

CRYPTREC 事務局宛

誓約書（提出資料 6）

このたび、「電子政府推奨暗号リスト改訂のための暗号技術公募」への応募にあたり、以下の事項について、ここに誓います。

記

1. 応募暗号技術〇〇〇〇〇〇〇〇に関するすべての技術は公知であり、提出書類を国外の評価者等に提供することは輸出管理上の許可が不要であること
2. 応募暗号技術〇〇〇〇〇〇〇〇の評価において、事務局との間において金銭等の授受を行わないこと
3. 応募暗号技術〇〇〇〇〇〇〇〇に係る評価を行う際に、当該暗号技術に関連する特許権、著作権等の知的財産の実施・利用について、CRYPTREC 検討会事務局（外部評価者を含む）に対して、無償で通常実施権や利用許諾等を与えること。
4. 応募暗号技術〇〇〇〇〇〇〇〇に関する特許権、著作権等の知的財産については、それを利用する製品等に対して、無償又は妥当かつ非差別的な条件で、通常実施権、利用許諾等を与えること
5. 応募暗号技術〇〇〇〇〇〇〇〇の評価において、不利益と解される情報を含むことがあっても異議を申し立てないこと
6. 応募暗号技術〇〇〇〇〇〇〇〇が、2010 年 9 月末までに、査読付きの国際会議又は査読付きの国際論文誌で発表されない場合には、応募資格を喪失することに異議を申し立てないこと
7. 応募暗号技術〇〇〇〇〇〇〇〇を使用する製品は、{既に製品化され調達可能になっている／CRYPTREC 暗号リスト（仮称）策定後 3 年以内に製品化がなされるよう鋭意努力する} こと
8. 応募暗号技術〇〇〇〇〇〇〇〇の評価結果の如何に関わらず、CRYPTREC 暗号リスト（仮称）に掲載されなくても異議を申し立てないこと

20〇〇年〇月〇日

応募暗号責任者
会社名・部署名　〇〇〇〇〇〇〇
住　所　〇〇〇〇〇〇〇〇丁目〇番〇号
氏　名　〇〇〇〇〇〇　　印

以　上

（別紙 3）

各項目の記入スペースの配分は応募者の任意とします。1 ページに収める必要はありません。

公開の状況等に関する情報（提出資料 7）

暗号技術名：
応募責任者名： 印
ⅰ)応募暗号技術を発表した国際会議又は国際論文誌に関する情報を列挙して下さい： 発表期日： 発表者： 会議名又は論文誌名：
ⅱ)輸出管理 輸出管理上の許可が不要であることを示す根拠に関する情報を列挙して下さい：
ⅲ）知的財産とライセンス方針： 応募暗号技術に関連する知財権などに関する情報を明記して下さい。また、電子政府で使用する際のライセンス方針を明記して下さい：
ⅳ)調達可能性について 応募暗号技術が既に製品等で利用されている場合には、その製品名に関する情報を列挙して下さい：
その他関連事項等あれば記載して下さい。

（別紙 4）

自己チェックリスト （提出書類 9）

暗号技術名＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

本チェックリストは、あくまでも事務手続き上のチェックリストです。
下記内容が確認できたら、□部分を黒く(■)塗りつぶして使用します。

＜チェック項目＞

□ 1.応募暗号技術は、次期リスト策定後、3 年以内に製品化がなされ、調達可能ですか？
□ 2.応募暗号技術は、応募書類受付締切までに公知となっていますか？
□ 3.応募暗号技術は、査読付きの国際会議、国際論文誌に採録されていますか？
□ 4.一つの暗号技術の種別のみに応募していますか？
□ 5.応募暗号技術は、今回公募する暗号技術の種別に該当しますか？
□ 6.応募に必要な以下の提出物（文書・電子データ）が揃っていますか？
［暗号技術応募書、暗号技術仕様書、自己評価書、テストベクトル、参照ソースコード、誓約書、公開状況等に関する情報、応募暗号説明会資料、自己チェックリスト］
□ 7.以下の内容が網羅されていますか？

●暗号技術応募書 (P. 9)
□ 8.応募暗号技術公開ホームページ URL が記載されていますか？
□ 9.応募担当者は、適時連絡が取れ、日本語が話せる方ですか？
□10.応募担当者の電話番号（代表、直通を明記)、FAX 番号、e-mail アドレスをもれなく記入していますか？

●暗号技術仕様書 (P. 9)
□11.応募暗号が現リストに掲載されている暗号技術と同等以上の特長を持つ点について記述していますか？
□12.実装に必要な全情報を記載していますか？
□13.応募暗号技術は第三者が全ての機能を実装可能ですか？
□14.今回の応募以外に、同じような名称で他に発表又は応募した暗号技術があれば列挙していますか？

●自己評価書 (P. 10)
□15.十分な自己評価が記載されていますか？

●テストベクトル (P. 11)
□16.公募要項に示された要求件数以上のテストベクトルが提出されていますか？

●参照ソースコード (P. 12)
□17.実装動作確認済ですか？
□18.テストベクトル生成ソースコードは添付されていますか？

●誓約書(P. 13)
□19. 提出資料に誓約書は含まれていますか？

●公開の状況等に関する情報 (P. 13)
□20.応募暗号技術の公開時期とその学会名は記述されていますか？
□21.輸出規制問題を解決していることの証拠について記載及び資料添付されていますか？
□22.知財権とライセンスについて記載されていますか？
□23.ライセンス方針は、電子政府における利用において無償か、あるいは、妥当かつ非差別的な条件となっていますか？

●応募暗号説明会発表資料 (P. 14)
□24.提出資料に応募暗号説明会発表資料は含まれていますか？

付録 4　　学会等での主要論文発表等一覧

目次

1. ハッシュ関数

1.1. ハッシュ関数 解析

Preimage Attacks on Reduced Tiger and SHA-2 [FSE 2009]

Takanori Isobe and Kyoji Shibutani

3 種のハッシュ関数 Tiger, SHA-256, SHA-512 に対し、鍵スケジュール関数における独立なワードの存在と、中間一致攻撃を利用することで、原像攻撃と第 2 原像攻撃を行った。両攻撃に対する攻撃効率は等しく、Tiger は計算量 2^{161} で 24 段中 16 段、SHA-256 は計算量 2^{240} で 64 段中 24 段、SHA-512 は計算量 2^{480} で 80 段中 24 段で攻撃できると評価した。SHA-256 に対する原像攻撃では、NTT の佐々木・青木が出した 36 段まで攻撃可能という結果があり、及んでいないが、それ以外は新記録となっている。Tiger は FSE '96 で Anderson と Biham が提案した 192 ビット・ハッシュ関数であり、従来の攻撃記録は、原像攻撃では計算量 $2^{128.5}$ で 13 段まで、第 2 原像攻撃では計算量 $2^{127.5}$ で 13 段までだった。

Preimage Attacks on One-Block MD4, 63-Step MD5 and More [SAC 2008]

Kazumaro Aoki, Yu Sasaki

1 ブロックの MD4 と 64 ステップ中 63 ステップに縮小した縮小版 MD5 の原像攻撃を示した．中間一致攻撃をベースとして，さまざまな改良の追加によって，ブルートフォース攻撃（2^{128} 回のハッシュ計算）より高速な原像計算が可能となった．1 ブロック MD4 の原像は 2^{107} 回の MD4 圧縮関数，縮小版 MD5 の原像は 2^{121} 回の MD5 圧縮関数の計算量にてそれぞれ計算可能となった．さらに（フルステップの）MD5 のブルートフォース攻撃の計算順序を最適化することによって MD5 の原像は 2^{127} 回の MD5 圧縮関数の計算量で計算できる事を示した．他のハッシュの結果が CRYPTO 2008 の Rump セッションにて速報された．詳細は Asiacrypt 2008 にて発表予定とのこと．

http://rump2008.cr.yp.to/efa237568f229268803b82ed02e217ca.pdf

The Rebound Attack: Cryptanalysis of Reduced Whirlpool and Grøstl [FSE 2009]

Florian Mendel, Christian Rechberger, Martin Schläffer and Søren S. Thomsen

リバウンド攻撃はブロック暗号ベースのハッシュ関数の衝突探索用の攻撃である。ブロック暗号の攻撃法である truncated 差分攻撃を応用した攻撃法で、S-box 活性・非活性パターンを利用し、中間段内部における効率的中間一致攻撃と、truncated 差分を利用した外向きの経路探索を組み合わせることから rebound と名づけられている。
Whirlpool と Grøstl はハッシュ関数であり、Whirlpool は国際標準 ISO/IEC 10118-3 に記載され、Grostl は SHA-3 候補である。ともに、AES の SPN 構造をベースとした S-box が全部活性となる S-box 層での中間一致探索と、外側（両側）への特定の truncated 差分パターンに限定した経路探索を組み合わせる。全活性の S-box 層が連続する段数の増減で攻撃可能段数が調整できる。
リバウンド攻撃により、Whirlpool の衝突は、10 段中 4.5 段まで計算可能で、計算複雑度は 2^{120}、必要メモリは 2^{16} である。また、連鎖値を自由に選べる semi-free-start 衝突探索だと、Whirlpool は、計算複雑度 2^{120}、必要メモリ 2^{16} で、10 段中 5.5 段まで計算可能、Grøstl は、計算複雑度 2^{120}、必要メモリ 2^{70} で、10 段中 6 段まで計算可能である。

Practical collisions for EnRUPT [FSE 2009]

Sebastiaan Indesteege and Bart Preneel

EnRUPT は SHA-3 候補のハッシュ関数で、7 種類のハッシュ長をサポートする。EnRUPT には、2つを除く他の全処理が線形、各メッセージ・ワードが1回ずつしか使われないという特徴がある。これらの特徴を利用して次の手順による攻撃戦略を実行した。
(1)圧縮関数の線形近似を見つける

(2)差分特性を見つける
(3)適合するペアを見つける
探索において、Viterbi アルゴリズムを使うことによって、7 種類のハッシュ長全部に対する衝突を具体的に発見した。EnRUPT-128 でメッセージ長が 6 ブロック、計算複雑度が $2^{36.04}$ 回、EnRUPT-384 でメッセージ長が 8 ブロック、計算複雑度が $2^{39.63}$ 回。

Meet-in-the-Middle Attacks on SHA-3 Candidates [FSE 2009]

Dmitry Khovratovich, Ivica Nikolic and Ralf-Philipp Weinmann

原像攻撃を SHA-3 候補である Boole、Edon-R、EnRUPT、Sarmal に対して適用し、安全性を評価した。ここの原像攻撃ではメッセージを2ブロックとし、メッセージからの順方向の中間出力と、ハッシュ値からの逆方向の中間出力を各々多数用意し、誕生日攻撃を行う。解読効率の向上のため、中間出力の一部ビットは期待する固定値となるよう、少ない計算量で調整するが、そこでは Floyd cycle を利用する。攻撃の結果は次の通りである。

・Boole (ストリーム暗号ベース)
　Bool3-384/512 が対象
　計算複雑度: 2^{288} 回分(圧縮関数計算)
　必要メモリ量: 2^{64} ブロック
　状況: 辞退
・Edon-R (Merkle-Damgard 型)
　Edon-R-n が対象(全ハッシュ値長)
　計算複雑度: $\max(2^{n-s},2^{n/2+s})$回分(圧縮関数計算)
　必要メモリ量: 2^{s} ブロック
　状況: 辞退せず
・EnRUPT (ストリーム暗号ベース)
　EnRUPT-512 が対象
　計算複雑度: 2^{480} 回分(圧縮関数計算)
　必要メモリ量: 2^{384} ブロック
　状況: 辞退せず
　　＊ EnRUPT-256 の具体的衝突は前項の発表を参照
・Sarmal (HAIFA 型)
　Sarmal-512 が対象
　計算複雑度: $\max(2^{512-s},2^{256+s})$回分(圧縮関数計算)
　必要メモリ量: 2^{s} ブロック
　状況: 辞退せず

Cube Testers and Key Recovery Attacks On Reduced-Round MD6 and Trivium [FSE 2009]

Jean-Philippe Aumasson, Willi Meier, Itai Dinur and Adi Shamir

Cube とは GF(2)上の多項式において、選択した入力ビットについて、取り得る全組合せについて足し合わす操作を言う。この操作を利用した Cube 攻撃が CRYPTO 2008 で Shamir によって提案され、暗号の多項式次数が低い場合、暗号化鍵の導出に有効であることが示されている。今回の発表では鍵導出でなく、暗号系の入出力関係が乱数と区別できるか否かを判定する Cube テスターを提案し、SHA-3 候補の MD6 と eSTREAM でハードウェア向けストリーム暗号として選ばれた Trivium に対して適用した。
MD6 に適用した結果、128 ビット鍵は 14 段まで計算量 2^{22} で攻撃可能であった。これに対し、Cube テスターでは、18 段では計算量 2^{17} で識別でき、段点数が $S_i=0$ の条件を付けると、66 段が計算量 2^{24} で識別可能であった。
また、Trivium に適用した結果、1152 段の初期化に対し、Cube 攻撃で 771 段まで攻撃可能であるのに対し、Cube テスターでは、初期ベクトルを選ぶとき、計算量 2^{24} で 772 段まで、計算量 2^{30} で 790 段まで識別可能であることが分かった。

Indifferentiability of Permutation-Based Compression Functions and Tree-Based Modes of Operation, with Applications to MD6 [FSE 2009]

Yevgeniy Dodis, Leonid Reyzin, Ronald L. Rivest and Emily Shen

MD6 はメッセージブロック長が 512 バイトであり、512 バイト入力・128 バイト出力の圧縮関数を使い、4 ブロック分の圧縮関数出力を上位階層での圧縮関数入力とする 4 分岐の階層型動作モードを持つハッシュ関数である。圧縮関数は、89 ワードの内部状態を持つ非線形シフトレジスタで構成される。この発表では、次の 2 つの indifferentiability を証明した。
圧縮関数がランダムであるとき、4 分岐構造とランダム関数の差を観測する際の advantage が $2q^2/2^{1024}$ 以下(q は圧縮関数の呼び出し回数)である。
シフトレジスタを更新規則がランダムであるとき、それを使った圧縮関数とランダム関数の差を観測する際の advantage が $q/2^{1024}+2q^2/2^{4672}$ 以下である。

Preimage Attacks on 3, 4, and 5-Pass HAVAL [ASIACRYPT 2008]
Yu Sasaki, Kazumaro Aoki

出力長 256 bit の HAVAL の原像攻撃の提案. 以下の 3 つの主結果

- 3-pass HAVAL のベストアタックの更新（計算量 $2^{230} \rightarrow 2^{225}$）
- 4-pass HAVAL に対する初めての攻撃（計算量 2^{241}）
- 5-pass Reduced round HAVAL(151steps)への攻撃（計算量 2^{241}）

および、その他の結果として

- 5-pass HAVAL へのブルートフォース攻撃の最適化（計算量 $2^{254.89}$）

を主張している. 中間一致攻撃と局所衝突 (local-collision) の手法を組み合わせて pseudo-preimage を見つけ, それを preimage に変換する generic なアルゴリズムを使用しているとのこと.

Preimage Attacks on 3-Pass HAVAL and Step-Reduced MD5 [SAC 2008]
Jean-Philippe Aumasson, Willi Meier, Florian Mendel

3-pass HAVAL (出力 256 bit) と ステップ縮小版 MD5 (出力 128 bit) の原像攻撃を示した. これらのハッシュ関数に対して衝突攻撃の研究はいくつか発表されているが, 原像攻撃は今まで無かった. 本論文では 3-pass HAVAL の圧縮関数に関する 2 つの原像攻撃を記述する.本原像攻撃は圧縮関数 2^{224} 回分の計算量を持つ. それから MD5 に対して いろいろな原像攻撃を示した. 2^{96} 回の試行で 47 段まで逆像計算できる. これらの攻撃は現実的な脅威ではないが, こうした事実は 3-pass HAVALと MD5 のセキュリティマージンが逆像攻撃の観点では期待されるほど大きくない事を示している.

Cryptanalysis of Tweaked Version of SMASH and Reparation [SAC 2008]
Pierre-Alain Fouque, Jacques Stern, Sébastien Zimmer

本論文では固定鍵ブロック暗号に基づくハッシュ関数のような置換に基づくハッシュ関数の安全性を研究している. SMASH は 2005 年に Knudsen が提案した置換に基づくハッシュ関数で, 同年に Pramstaller らによって破られた. その直後に この攻撃を回避するため Knudsen によって提案された 2 つの修正版が, やはり O(n 2^(n/3)) の時間で衝突攻撃が可能であることを本論文で示す.この計算量は最初の修正版に対しては O(2^(2√(n))) まで削減できる.この事実は c＊2^(32) (c は小さい係数) の SMASH-256 に対する攻撃が存在する事を意味する. さらに, 本論文では置換を 1 回ではなく 2 回使う事で, Ω(2^(n/4)) 回の置換へのクエリに対し, イデアルサイファーモデルで衝突安全性が証明可能な SMASH の効率的な一般化を示す. それから 本証明の tight さを解析するため, O(2^(3n/8))の非自明な攻撃を提案する. 最後に本構成が Ω(2^(n/2)) 回のクエリにて原像困難であることを証明する. それは 2-置換に基づくハッシュ関数が達成できる最高の安全性レベルである ([12] で証明されている).

Analysis of the Collision Resistance of RadioGatún using Algebraic Techniques [SAC 2008]
Charles Bouillaguet and Pierre-Alain Fouque

ハッシュ関数 RadioGatún の解析を行い、提案者より低い複雑度の衝突探索に成功した。RadioGatu'n は 2nd NIST Hash Workshop で提案されたハッシュ関数で、独自の belt-and-mill 構造を持っている。設計者は、AES の開発者の一人である J.Daemen を含む STMicroelectronics の研究者である。構造の特徴は内部状態が 59 ワードであり、1 ワードは 1～64 ビットである。 この発表では、1 ワードを 1 ビットとして、代数攻撃の一種である backtracking 攻撃を適用したところ、段関数の約 $2^{24.5}$ 回分の計算量で衝突が発見できた。これは提案者たちの攻撃より 32 倍効率が良い。

Cryptanalysis of RadioGatún [FSE 2009]
Thomas Fuhr and Thomas Peyrin

RadioGatún は 2006 年に Bertoni らが提案したストリーム暗号をベースとするハッシュ関数であり、belt-and-mill 構造を採用している。スポンジ関数に似ているが、要件を全部満たしていない。動作は3つの段階、メッセージ入力、ブランク(入出力無し)、ダイジェスト出力で構成される。
この論文では、メッセージ入力の段階で状態が一致するような衝突を探索し、状態更新 2^{11w} 回分(w はワード長で、メッセージ・ブロック長は 3w)の計算量で 148 ブロックの衝突が見つかることを示した。
攻撃法は、対称差分解読による差分経路探索と中間一致攻撃を組み合わせたもので、エントロピーを使って時間が掛る複雑な経路の探索を避けることで効率化した。探索で見つかった 143 ブロックの線形経路を使って、攻撃に必要な計算量を評価した。

Collisions of the LAKE Hash Family [FSE 2009]
Alex Biryukov, Praveen Gauravaram, Jian Guo, Dmitry Khovratovich, San Ling, Krystian Matusiewicz, Ivica Nikolic, Josef Pieprzyk and Huaxiong Wang

LAKE は Aumasson らが FSE 2008 で提案したハッシュ関数で、ハッシュ値のサイズが異なる LAKE-256 と LAKE-512 の2種類がある。HAIFA 構造が特徴で、圧縮関数の入力は、連鎖値、メッセージ・ブロック、ソルト(salt)、ブロック指数の4種類である。ソルトを使って連鎖値の幅を2倍にし、圧縮関数処理を 8 段(LAKE-256)/10 段(LAKE-512)行なった後、データの幅を半分にして次のブロック用の連鎖値とする。
この論文では、連鎖値とブロック指数に対する衝突を 2^{33} 回分の計算量で具体的に発見することに成功した。なお、この攻撃法は、類似の構造を持ち SHA-3 候補である BLAKE に対しては有効でない。

Collisions and other Non-Random Properties for Step-Reduced SHA-256 [SAC 2008]
Sebastiaan Indesteege and Florian Mendel and Bart Preneel and Christian Rechberger

ハッシュ関数 SHA-256 の縮小版に対する攻撃探索を行った他、ランダム性から離れた性質を発見した。SHA-256 は NIST が FIPS 180-2 で SHA-1 とともに採用され、電子政府推奨暗号にも選ばれているハッシュ関数である。SHA-1 の衝突発見が現実味を帯び来たことから、SHA-1 から SHA-256 を含む SHA-2 ファミリーへ移行する動きが強まっている。SHA-2 はフルスペックでは 64 段であるが、従来の結果では、Sanadhya と Sarkar による 22 段縮小版に対する攻撃が最高だった。また、本来固定である初段入力値を部分的に自由にした変形版に対して、Nikolic-Viryukov は 23 段と 24 段の衝突を発見している。
この発表では、Nikolic-Viryukov の方法を若干変更し、23 段及び 24 段の初段入力値の固定部分を増やしたモデルに対する衝突を発見した後、8 段の差分経路を選びなおすことで固定の初期値に戻し、23 段及び 24 段での完全な衝突の発見に成功した。フルラウンドの 64 段まで十分な段数があり、差し迫った脅威とはなっていない。

Cryptnalysis of the GOST Hash Function [CRYPTO 2008]
Florian Mendel(Graz Univ. of Tech.), Marcin Kontak and Janusz Szmidt(Military Univ. of Tech. Warsaw)

GOST ハッシュ関数は、ロシア標準 GOST 34.11-94 で定義された、256-bit ハッシュ値を生成する関数である。圧縮関数の衝突を用いることにより、2^{105} 回の圧縮関数評価でハッシュ関数の衝突を生成できることを示した。また、preimage 攻撃に関しては、2^{192} 回の圧縮関数評価および 2^{70} バイトメモリにより、preimage を構成できることを示した(これまでは 2^{225} の計算量を必要としていた(Mendel et al. FSE 2008))。メモリは本来 2^{133} バイト必要であるが、Quisquater/Delescaile らの手法により大幅に削減できる。

Preimages for Reduced SHA-0 and SHA-1 [CRYPTO 2008]

Christophe De Canniere(ENS/Kathoieke Univ. Leuven) and Christian Rechberger(Graz Univ. of Tech.)

ハッシュ関数 SHA-0 および SHA-1 に対する新たな preimage 攻撃を開発し、49-step の SHA-0 に対しては 2^{159} の計算量、44-step の SHA-1 に対しては 2^{157} の計算量で preimage を構成することができることを示した。新たな手法として、「圧縮関数の反転」および「P3(Partial-Pseudo-Preimages)グラフ」を導入した。コンセプトの正しさを示すために、33-step SHA-0 圧縮関数の preimage と 31-step SHA-0 ハッシュ関数の preimage を付録に付けた。

Slide Attacks on a Class of Hash Functions [ASIACRYPT 2008]

Michael Gorski (Bauhaus-University of Weimar), Stefan Lucks (Bauhaus-University of Weimar) and Thomas Peyrin (Orange Labs and University of Versailles)

本論文ではハッシュ関数へのスライド攻撃の適用を研究している．スライド攻撃は大抵はブロック暗号の解析に用いられる．しかし本論文で示す通り，ハッシュ関数，即ちスポンジ関数構造への潜在的脅威になりうる．あるハッシュ関数に基づくメッセージ認証コードの構成は偽造不可能性に関して，あるいは鍵回復不可能性に関してさえ脆弱性をもつ．そうでない場合でも,少なくともハッシュ関数とランダムオラクルとの識別不可能性を破ることが出来る.この結果の実例として本論文では GRINDAHL-256 および GRINDAHL-512 への攻撃を記述している．GRINDAHL-512 への攻撃は初めてとのこと．さらに modified RADIOGATUN へのスライド攻撃に基づく識別攻撃を示し，最後にスライド攻撃に対する簡単な対策技術を論じている．

Enhanced Target Collision Resistant Hash Functions Revisited [FSE 2009]

Mohammad Reza Reyhanitabar, Willy Susilo and Yi Mu

eTCR(enhanced Target Collision Resistance)とは、鍵付きハッシュ関数 H_K の安全性に関する概念で、固定したメッセージと鍵の組(M,K)に対し、これとは異なる組(M',K')で H(M,K)=H(M',K')を満たすものを見つけるのが困難である性質である。eTCR は明らかに原像計算困難(TCR)より強い概念であるが、TCR より強いもう一つの概念である衝突発見困難性(CR)とどちらが強い概念であるかは今まで明らかでなかった。この発表では、eTCR と CR の強度についての関係を明らかにし、各種領域拡張法が eTCR を満たすか否かを評価した。
eTCR と CR の強度を調べた結果、どちらが強いとも言えず、eTCR は成立・CR は不成立の例も、その逆の例も存在することが示された。
領域拡張法として、Merkle-Damgard, Randomized Hashing, Shoup, Enveloped Shoup, XOR Linear Hash, Linear Hashing、及びこれらの強化・変形版について解析した。これらの領域拡張法の基本形は、使用する鍵とその挿入位置だけが異なる。解析の結果、Linear Hashing(LH)でメッセージにパディングを連接した入れ子型 LH だけが領域拡張に対して eTCR が保持されることが分かった。

1.2. ハッシュ関数 設計

Multi-Property Preserving Combiners for Hash Functions [TCC 2008]

Marc Fischlin and Anja Lehmann

robust hash combiner は、2 つのハッシュ関数を組合せて、1 つのハッシュ関数を作り、用いた元の 2 つのハッシュ関数の少なくともひとつが安全性の要求条件を満たせば、組合せて作ったハッシュ関数もその性質を満たすようなハッシュ関数を構成する 本発表では、満たすべき安全性に関する要求条件が一つでなく複数ある場合にその要求条件を満たすようなハッシュ関数を構成できる hash combiner に注目し、collision resistance, pseudo-randomness, random-oracle-ness, target collision resistance, message authenticating などを満たすハッシュ関数を構成できる hash combiner の構成を提案。

Hash Functions and RFID Tags: Mind The Gap [CHES 2008]

Andrey Bogdanov, Gregor Leander, Christof Paar, Axel Poschmann, Matt J.B. Robshaw, Yannick Seurin

リソースの限られた RFID に向いたハッシュ関数を検討した。RFID のプロトコルで使われるハッシュ関数

には小型である程度処理速度が速いという条件がある一方、要求される安全性の条件は、通常の利用におけるものより低くても構わないものがある。この論文では、低コストの RFID を仮定して、通常より、安全性に関する要求を下げ、逆に実装性能に関する要求をきつくした。具体的には、サイズが十分小さく、入力データは 256 ビット以下、衝突発見困難性は要求せず、80 ビットの安全性で十分とし、ピークと平均での電力消費が小さいとする。以上の要件を基に、既存の専用アルゴリズムとブロック暗号を利用した設計を対象に検討した。既存の専用ハッシュ関数を使わない理由は、それらが通常のブロック暗号と比べて内部状態が大きく、安全性も確かでないためである。著者らが開発したブロック暗号 PRESENT を利用したハッシュ関数が望ましい性質を満たすと結論した。具体的には、64 ビット・ハッシュでは DM-PRESENT-80 と DM-PRESENT-128 が、128 ビット・ハッシュの小型実装としては H-PRESENT-128 が良いとした。

A Three-Property-Preserving Hash Function [SAC 2008]
Elena Andreeva and Bart Preneel

衝突探索困難性(Coll)、第2原像発見困難性(Sec)、現像発見困難性(Pre)の3つを満足するハッシュ関数を構成した。広く使われているハッシュ関数のうち、MD4 と MD5 の衝突は容易に発見され、SHA-1 の衝突発見も現実的になりつつあり、安全性が理論的に保証できる現実的なハッシュ関数が求められている。この発表ではこの条件を満たすハッシュ関数の候補として、上構造を Merkle-Damgard(MD)型とし、圧縮関数に、メッセージと鍵の与え方を改良した backwards chaning mode(BCM)のブロック暗号を利用する方式を提案した。この方式は、メッセージが一様分布と仮定すると、BCM が、スタンダード・モデルで Coll と Sec が保証でき、ランダムオラクル・モデルで Pre が保証できることが証明された。

A Scheme to base a Hash Function on a Block Cipher [SAC 2008]
Shoichi Hirose and Hidenori Kuwakado

ブロック暗号を利用したあるハッシュ関数の構成(MDP-MMO)が、理想暗号におけるランダムオラクルと indiffirentiable であることを示した。最近、暗号内部の構成要素の入出力関係の問い合わせを許したとき、2つの関数形が区別できるかどうかに注目した indifferentiablity が提案され、共通鍵暗号系の安全性評価に応用されるようになっている。
この発表では、Matyas-Meyer-Oseas(MMO)スキームで構成されたブロック暗号を使い置換付きの Merkle-Damgard 型(MDP)の領域拡張を適用したハッシュ関数を対象とする。これを理想暗号(ICM)における、入力サイズが可変のランダムオラクル(RO)と比較した。その結果、MDP-MMO 構成が ICM における RO と indifferentiable であることが証明できた。また、MDP-MMO を使った HMAC が次の条件で擬似ランダム関数となることが示された。その条件とは、MDP で使う置換が関連鍵攻撃の下でベースとなるブロック暗号がランダム置換となることである。

The MD6 hash function [CRYPTO 2008]
Ronald L. Rivest

NIST SHA-3 competition 応募ハッシュの MD6 に関する暗号学的な全容の紹介が行われた．大きいメッセージブロック長、単純な圧縮関数、演算量は比較的大きいが並列化可能などの特徴を備える．(4096 bit メッセージブロック長は，この大きさの RSA コプロを意識したアーキテクチャか？)

http://people.csail.mit.edu/rivest/Rivest-TheMD6HashFunction.ppt
http://groups.csail.mit.edu/cis/theses/crutchfield-masters-thesis.pdf

Beyond Uniformity: Better Security/Efficiency Tradeoffs for Compression Functions [CRYPTO 2008]
Martijn Stam

n+c-to-n bit の完璧な圧縮関数 f が与えられたとして より大きい m+s-to-s bit の圧縮関数 H を構成したいとする．H が f を r 回呼び出すとして，H から どんなレベルの安全性が（特に衝突困難性に関して）期待できるだろうか? 典型的な衝突は 2^(nr+cr-m)/(r+1) 個のクエリ中に見つけられると著者は予想している．この上界は 鍵長 k ブロック長 n のブロック暗号に基づいて m+s-to-s bit の圧縮関数を構成する場合にも関係がある．(単純に c = k あるいは固定鍵の場合は c = 0 とせよ)．また衝

突困難性がこの上界に近い幾つかの（概念的）圧縮関数を示した.
特に以下の 4 つのシナリオを研究した.

- n-to-n bit プリミティブ 2 call で構成され 2^{n/3}/n クエリまで衝突困難な 2n-to-n bit 圧縮関数.
  この結果は，あらゆる rate-1/2 の圧縮関数の衝突を見つけるにはベースとなる n-to-n bit ランダム関数 2^{n/4}回のクエリで十分であるとする Rogaway と Steinberger による最近の結果に反しており,彼らの（c=0 に対する）2^{(nr-m-s/2)/r} 回のクエリという上界が決定的に一様性仮定に依存している事を示している: 任意の圧縮関数に拡大して一般化している部分が正しくないのであろう.
- 3n-to-n bit プリミティブ 1 call で構成され 2^n クエリまで衝突困難な 3n-to-2n bit 圧縮関数.
- 2n-to-n bit プリミティブ 2 call で構成され 2^n クエリまで衝突困難な 3n-to-2n bit 圧縮関数.
- m <= n+c, n <= s, c <= m を満たすプリミティブ 1 call で構成された圧縮関数.
  この結果は 1 call の n+c-to-n bit ランダム関数を想定した時の圧縮可能なビット数と達成できる安全性レベルとの間のトレードオフを与える.

Compression from Collisions, or Why CRHF Combiners Have a Long Output [CRYPTO 2008]
Krzysztof Pietrzak

衝突困難ハッシュ関数(CRHF)に対するブラックボックスコンバイナとは,その構成要素である二つのハッシュ関数へのブラックボックスアクセスを仮定して，少なくともその一つが衝突困難ならば，衝突困難であるようなハッシュの構成方法である．本論文では CRHF に対するブラックボックスコンバイナの出力長の下界を証明する．この下界は Canetti らの方法［Crypto 2007］によって既に達成されており基本的にタイトである．従来の最良の下界は，非常に強い安全性の帰着を持った極めて限定されたクラスのコンバイナしか制限しない: すなわち この帰着は，コンバイナの一つの衝突に対して，それを構成する全てのハッシュの衝突を出力することが要求される．(Boneh-Boyen［Crypto 2006］および Pietrzak［Eurocrypt 2007］に基づく Canetti ら［Crypto 2007］による構成)
本論文の証明では，一方向でないあらゆる関数は圧縮可能（従って一様ランダム関数は必ず一方向）なる Gennaro-Trevisan［FOCS'00］のエレガントな ″reconstruction lemma″ と類似の補題を用いる．本論文では衝突困難でないあらゆる関数は圧縮可能である事を示す.
それから，なんらかの非常に強力なオラクル（本論文の場合は指数時間衝突発見オラクルに相当）に対して ″reconstruction lemma″ が やはり証明可能である事を示した Haitner ら［FOCS'07］の仕事からもアイディアを借用している.

Constructing Cryptographic Hash Functions from Fixed-Key Blockciphers [CRYPTO 2008]
Phillip Rogaway, John Steinberger

固定鍵ブロック暗号から構成される圧縮関数の族を提案しイデアルサイファーモデルで衝突および原像安全性を調べた．この構成は，著者らの以前の仕事[24] で見つかった安全性の上界に迫る安全性をもち，多くの場合には一致する．特に n-bit 置換 3 call (呼び出し) を用い N = 2^n のとき 衝突安全性 N^{0.5} を持つ 2n-to-n bit 圧縮関数 および置換 5 call および 6 call を用い それぞれ衝突安全性 N^{0.55} および N^{0.63} を持つ 3n-to-2n bit 圧縮関数を記述する.

Elliptic Curve Hash (and Sign) [ECC 2008]
Daniel Brown (Certicom, Canada)

Bellare と Micciancio の MuHASH に触発された，楕円曲線演算を用いたハッシュ関数(ECOH)の提案．このハッシュ関数は通常のハッシュ関数と比較すると低速であるとは思われるが，並列化可能で差分更新可能(incremental)である．(差分更新可能とはメッセージの大部分が同じならハッシュ関数の再計算が高速であるということ)．そのセキュリティは大体は MuHASH のセキュリティに基づいているが，MuHASH と違ってランダムオラクルあるいは衝突困難関数として用意されたハッシュ関数に依存しない．ジェネリックモデルにてこのハッシュの衝突困難性を示唆する根拠が存在する（ Semaev : Summation polynomial の低次の解が見つかるなら ECDLP が解ける．→ ECDLP が困難なら低次の解は見つからない → ECOH の次数は Summation polynomial の次数よりずっと高いので安全 ）．第二のトピックとして，ECDSA の安全性がベースとなる楕円曲線に関する 2 つの異なる問題，有名な離散対数問題と無名な ″one-up″ 問題 に依存している事を示す.

http://www.hyperelliptic.org/tanja/conf/ECC08/slides/Dan-Brown.pdf
http://eprint.iacr.org/2008/012.pdf
http://eprint.iacr.org/2008/286.ps

Hash Functions – Much ado about something [ECC 2008]
Orr Dunkelman

ハッシュ関数に関するサーベイ。collision resistance/preimage/2nd preimage などの性質、pseudorandomness、universal oneway、Merkle-Dangard、Davies-Meyer などの概念や各種攻撃が紹介された。 AHS に関しては、less secure であってはならない、SHA-1 より遅くてはならないなどの基準予想、性能に関しては、ASIC で 5Gbps、32 ビットで 35-40cpb、64 ビットで 25-30cpb くらいが目安になり、RFID への適用は重要な基準とはならないであろうなどの予想が示された。自らが Eli Biham と提唱する HAIFA(HAsh Iterative FrAmework)の宣伝もあった。

Syndrome Based Collision Resistant Hashing [PQCrypto 2008]
Matthieu Finiasz

Fast Syndrome Based ハッシュ関数ファミリーは、Syndrome Decoding 問題ベースの Collision Resistance ハッシュ関数である。即ち、コリジョンを見つけるためには、Syndrome Decoding 問題を解く必要がある。FSB におけるオリジナルの行列を Quasi-Cyclic とするバリアントを考え、既存攻撃を分析することにより、あるレベルのセキュリティと処理性能を持つパラメータを示す。

Hash Functions from Sigma Protocols and Improvements to VSH [ASIACRYPT 2008]
Mihir Bellare and Todor Ristov (UCSD)

本論文はあらゆるΣ-プロトコルから証明可能衝突困難ハッシュ関数を得る普遍的な方法を示した．この結果を用いてFiat-Shamir プロトコルの改良版を使って標準的な素因数分解仮定に基づき衝突困難性を証明可能な既知のどのハッシュ関数よりも高速なハッシュ関数を得ることが出来た．さらに短いメッセージをハッシュするとき高速である VSH の修正版である VSH* を提案した．またΣ-ハッシュ関数はカメレオン(トラップドアを用いると衝突を生成できること)であることを示す．そのため，オンラインあるいはオフラインの署名，カメレオン署名，検証者指定署名への応用を持つ効率的な新しいカメレオンハッシュ関数を得ることが出来た．

How to Fill Up Merkle-Damgard Hash Functions [ASIACRYPT 2008]
Kan Yasuda

Merkle-Damgard 型ハッシュ関数は、圧縮関数が Collision Resistant でなければ、第二原像攻撃耐性があるかどうか、また一方向性であるかどうかがわからなくなっている。``split padding''という手法を導入することにより、Merkle-Damgard 型ハッシュ関数を新しいハッシュ関数に変換する。これにより、圧縮関数が第二原像攻撃耐性に似た性質を持つならば新しいハッシュ関数は第二原像攻撃耐性を持ち、圧縮関数が一方向性に似た性質を持つならば新しいハッシュ関数は一方向性を持つことが示される。これらの性質は通常のセキュリティ概念との関係が明確であり単純に定義され、パッチのコストも小さい。

Limits of Constructive Security Proofs [ASIACRYPT 2008]
Michael Backes, Dominique Unruh

Rogaway の構成的セキュリティは、プロトコルを破る攻撃者は存在しない(存在的セキュリティ)ことを求める代わりに、プロトコルを破る攻撃者が存在した場合に、明に与えられた帰着を用いてハッシュ関数の衝突を効率的に構成できることを求める。存在的安全ではあるが、構成的セキュリティを用いては安全と証明できないプロトコルを示すことにより、Rogaway の構成的セキュリティのアプローチの限界を示す。

Blockcipher Based Hashing Revisited [FSE 2009]
Martijn Stam

ブロック長と鍵長が等しいランダムなブロック暗号1個(rate-1)と排他的論理和(XOR)を使って構成した、ハッシュ関数用の圧縮関数の安全性を解析した。その結果、初期ベクタ(IV)を自由に選べるときに衝突耐性が証明できるのが 12 方式、固定の IV で衝突耐性が証明できるのが 8 方式あることが示せた。
次にXORを全単射や単射の補助関数に一般化したモデルに拡張し、補助入出力サイズの大小関係による4分類、Classical，Chopped，Overloaded，Supercharged の各々について安全性を解析した。Classical には PGV と BRS が属し、Chopped には Grindahl が属し、Overloaded にはスポンジ型が属し、Suprecharged は新規の構成である。これら全部で、IV 自由での衝突耐性が証明でき、特に Supercharged では、birthday bound を超える安全性が実現することが証明された。
さらに、鍵長がブロック長の 2 倍となるブロック暗号を使い、連鎖値長がメッセージ・ブロック長の 2 倍となる rate-1 の圧縮関数の新規構成を提案し、IV 自由の衝突耐性を証明した。
この論文は、FSE 2009 のベスト・ペーパーに選ばれている。

On the Security of Tandem-DM [FSE 2009]
Ewan Fleischmann, Michael Gorski and Stefan Lucks

Tandem-DM は、鍵長がブロック長の2倍のブロック暗号2個を使ったハッシュ関数用圧縮関数の構成であり、EUROCRYPT '92 で提案された。メッセージブロック長が連鎖ブロック長の 1/2 であるが、同じスペックの圧縮関数に廣瀬が FSE 2006 で提案した DBL がある。DBL は提案時に衝突耐性が証明されていたが、Tandem-DM の衝突耐性は今回の発表で 15 年ぶりに証明された。

eBASH: ECRYPT Benchmarking of All Submitted Hashes [ASIACRYPT 2008 RUMP]
Daniel J. Bernstein, Tanja Lange

SHA-3 候補のベンチマークプロジェクトの紹介。SHA-3 への提案者は、ベンチマークプログラムの結果を送るよう依頼。

2. ストリーム暗号

2.1. ストリーム暗号 解析

A Real-World Attack Breaking A5/1 within Hours [CHES 2008]

Timo Gendrullis, Martin Novotny, Andy Rupp

ストリーム暗号 A5/1 に対する解読アルゴリズムを暗号解読専用ハードウェア COPACOBANA に実装し、予備評価を行ったところ、高速最適化実装により平均 6 時間程度で解けるとの評価が得られた。A5/1 は第3世代携帯電話の規格 GSM で利用されているストリーム暗号である。A5/1 に対する攻撃はいくつか提案されていて、解読可能であるとする理論解析結果は出されているが、実際に実装して解読した例はなかった。この論文では、2001 年に Keller らが提案したハードウェアを利用した guess-and-determine 法を基本に、探索規則を改良し、COPACOBANA 上に実装した結果が示されている。。COPACOBANA は 120 個の Xilinx 社製 Spartan3-XC3S1000 FPGA を使った高性能低コストの暗号解読専用機である。予備的な実装でフル実装した場合の性能を外挿したところ、最適化したデザインで全探索をすると 11.78 時間、鍵発見の平均時間は 5.89 時間という見積もりを得た。

Algebraic and Correlation Attacks against Linearly Filtered Non Linear Feedback Shift Registers [SAC 2008]

Côme Berbain, Henri Gilbert, Antoine Joux

filter generator はよく知られたストリーム暗号構成法の一つである．それは非線形ブール関数でフィルターされた一つの線形フィードバックシフトレジスタ (LFSR) からなる．本論文ではその双対的な構成，すなわち線形関数でフィルターされた非線形フィードバックシフトレジスタ (NFSR)，について焦点を当てる．本論文では，既存の filter generator に対する代数攻撃および相関攻撃を，その双対的な構成に対する代数攻撃および相関攻撃に翻訳できることを示す．さらに，そうした攻撃を研究し，線形関数でフィルターされた NFSR が 1 つかそれ以上の非線形関数でフィルターされた LFSR と線形に結合している場合へと拡張した．Grain-128 の修正版にこの代数攻撃を適用して，2^{105} の計算量と 2^{39} の鍵ストリームビットを要する攻撃を構成することができた．この攻撃はオリジナルの Grain-128 には適用できないが NFSR の使用が全ての代数攻撃を避けるのには十分ではないことを示している．

An Improved Fast Correlation Attack on Stream Ciphers [SAC 2008]

Bin Zhang, Dengguo Feng

Crypto 2000 で Johansson および Jonsson は Goldreich-Rubinfeld-Sudan アルゴリズムに基づくストリーム暗号の高速相関攻撃を提案した．本論文では，このアプローチを 鍵ストリームの置換およびパリティチェック評価のテクニックと 組み合わせることにより既知の最も効率的な高速相関攻撃が得られることを示す．新しいアルゴリズムを適用した結果 Krawczyk が 1994 年に提案したパラメタの shrinking generator に関する 初めての 近実用的な鍵回復攻撃が得られた．そして，識別攻撃しか知られていなかった 40-bit data LFSR の場合で本攻撃を実証した．

New State Recovery Attack on RC4 [CRYPTO 2008]

Alexander Maximov and Dmitry Khovratovich(Univ. of Luxembourg)

ストリーム暗号 RC4 の RC4-N ファミリーに対する新しい攻撃により解読計算量を大幅に引き下げた。RC4 の初期化プロセスに関しては多くの解析研究が行われている．一方，内部状態回復攻撃に関しては 1998 年 ASIACRYPT における Knudsen らの攻撃があるが計算量は 2^{779} であり、その後の改良でも 2^{700} に届いていなかった。本研究では RC4-256 に対する攻撃計算量は 2^{579} 以下であり、現実的な仮定により 2^{241} まで引き下げることができる。

How to Solve it: New Techniques in Algebraic Cryptanalysis [CRYPTO 2008]

Adi Shamir(Weizmann Inst. of Science)

*Itai Dinur*と共同で開発した、代数的手法を用いた新しい暗号解析の手法CUBE attackに関する講演。多くの暗号スキームは、秘密/公開変数による GF(2)上の多項式として記述することができるが、公開変数を選ぶことにより多項式方程式を解くことに帰着される。一つの方法としてグレブナ基底を用いた方法があるが、ブラックボックス多項式には適用できない double exponential である変数の数が数十となるGF(2)上では全数探索の方が速いなどの欠点がある。提案する CUBE attack はブラックボックス多項式に適用することができ、provable successful(次数 d の n 変数ランダム多項式に適用した場合、公開変数の個数が $d+\log_d n$ を超えるならば $n2^{d-1}+n^2$ の計算量で解くことができる)となる手法である。この結果、ブロック暗号、ストリーム暗号、MAC など広範囲の暗号に適用することができ、例えば Trivium(672 初期化ラウンド)に対する最良の攻撃計算量は 2^{55} であったところを、2^{19} に下げることができた。

Cube Attack に関して (2008/09/18)

Shamir が CRYPTO 2008 の招待講演で発表した Cube attack に関しては Michael Vielhaber が以下の主張を行っている.

Shamir's Cube attack == My AIDA attack !
Posted by: Vielhaber (IP Logged)

The so-called "Cube attack"

http://eprint.iacr.org/2008/385

is (in my personal, thus heavily partial, opinion) precisely the AIDA attack presented by myself in 2007 at

http://eprint.iacr.org/2007/413

([27] in Dinur/Shamir)

http://eprint.iacr.org/forum/read.php?8,59

Shamir らの論文は Eurocrypt 2009 に accept された.

Cryptanalysis of Sosemanuk and SNOW 2.0 Using Linear Masks [ASIACRYPT 2008]

Jung-Keun Lee, Dong Hoon Lee, Sangwoo Park (ETRI Network & Communication Security Division, Korea)

Sosemanuk は Berbain らによって提案され eSTREAM の最終選考に合格したソフトウェア向けストリーム暗号である. 本論文は Sosemanuk に対する相関攻撃を提案している. Sosemanuk は 10 個の 32-bit 語長の線形フィードバックシフトレジスタ(LFSR) と 2 個の 32-bit 語長の有限状態機械(FSM)から構成されているが, FSM 更新関数を考慮した線形近似関係, FSM 出力関数および鍵ストリーム出力関数の組み合わせにより, 鍵ストリームワードと LFSR の初期状態に関する相関 $-2^{-21.41}$ の線形近似関係を導くことが出来, 著者らはそれを用いて $2^{147.12}$ の計算量 $2^{147.00}$ bit のメモリ $2^{145.00}$ bit のデータで 384 bit の初期状態を 99% の成功確率で復元できる相関攻撃を構成している. また事前計算を 2^{150} より幾らか大きくして良いならさらに計算量を削減可能とのこと. さらに著者らは国際規格 ISO/IEC 18033-4 に記載されている SNOW 2.0 に関しても $2^{204.38}$ の計算量, $2^{202.83}$ bit のメモリ, $2^{198.77}$ bit のデータで相関攻撃を構成している.

A New Attack on the LEX Stream Cipher [ASIACRYPT 2008]

Orr Dunkelman (ENS, France) and Nathan Keller (Hebrew University, Israel)

LEX ストリーム暗号は Biryukov によって AES に基づき設計された eSTREAM 応募暗号で, その単

純な構造から暗号学者の注目を集め，高速性(AES の 2.5 倍)と期待された安全性（AES の安全性）により eSTREAM の最終選考においてもかなり有力な候補であった．本研究の前身となる研究において，eSTREAM の最終選考決定のわずか数日前に単一鍵，2^{64} byte の鍵ストリームでの鍵回復攻撃が発見され LEX ストリーム暗号は eSTREAM の最終選考から外れることとなった．必要な鍵ストリームは最終選考決定 2 日前には 2^{48} byte，4 日後には $2^{36.3}$ byte になったとのこと．

The eSTREAM Portfolio (rev. 1) (2008/09/08)

F-FCSR-H v2 に対する［3］の解析結果に従って eSTREAM Portfolio が revision 1 に改訂され F-FCSR-H v2 ストリーム暗号が削除された（2008/09/08）．CRYPTREC でも 2009 年度にストリーム暗号の公募を行う予定なので，eSTREAM の動向は何らかの参考になるであろう．［3］は Asiacrypt（2008 年 12 月 7 日～11 日）にて発表されるとのこと．

http://www.ecrypt.eu.org/stream/portfolio_revision1.pdf

[3]. M. Hell and T. Johansson. Breaking the F-FCSR-H stream cipher in Real Time. In J. Pieprzyk, editor, Proceedings of Asiacrypt 2008, Lecture Notes in Computer Science, to appear.

Breaking the F-FCSR-H Stream Cipher in Real Time [ASIACRYPT 2008]
Martin Hell and Thomas Johansson (Lund University, Sweden)

F-FCSR ストリーム暗号ファミリーは F.Arnault らにより提案され，そのハードウェア向けバージョンの F-FCSR-H v2 は eSTREAM の最終選考に合格している．本論文では F-FCSR ストリーム暗号ファミリーに関する深刻な暗号解析結果を発表している．本研究成果に基づいて eSTREAM portfolio は F-FCSR-H v2 を除外した revision 1 に改訂された．なお，前日のランプセッションにて B.Pousee がパッチを発表している（F-FCSR v3 ファミリー）．この論文は Asiacrypt 2008 の 3 つのベストペーパーの内の 1 つに選ばれた．

An Efficient State Recovery Attack on X-FCSR-256 [FSE 2009]
Paul Stankovski, Martin Hell and Thomas Johansson

X-FCSR-256 は、キャリー付きシフトバック・レジスタ(FCSR)2個と、AES に似た 256 ビット SPN 処理を組み合わせた高速ストリーム暗号であり、INDOCRYPT 2007 で提案された。Hell と Johannson が発見した中間出力に関する線形関係を、ブロック出力の組み合わせに適用し、バイト単位の式を立て、総当たり的に解く攻撃によって、$2^{49.3}$ 個の出力ブロック、$2^{57.6}$ 回のテーブル参照、テーブル 2^{33} 枚分のメモリ、で攻撃できることが示された。

Key Collisions of the RC4 Stream Cipher [FSE 2009]
Mitsuru Matsui

ストリーム暗号 RC4 では、擬似乱数の生成に先立ち、鍵スケジュール計算(KSA)によって初期状態が設定される。初期状態は高々256!(≒2^{1684})通りしかない。RC4 の鍵長は 1～256 バイトから選べるが、鍵が 210 バイトだと初期状態の総数より多くなるので、必ず同じ初期状態が生じる。つまり、鍵は異なるが生成される擬似乱数（鍵ストリーム）は同じになる場合が存在する。これを衝突と呼ぶ。
この論文では KSA の動作を解析し、衝突が起きる条件を求め、衝突が予想外に高い割合で存在することを発見し、具体的に 24 バイト鍵の衝突を示した。

2.2. ストリーム暗号 設計

Counting Functions for the k-Error Linear Complexity of 2^n-Periodic Binary Sequences [SAC 2008]
R. Kavuluru, A. Klapper

線形複雑度はストリーム暗号における鍵ストリームの暗号学的強度に関する重要な尺度である．(シンボル)列の線形複雑度は，数個のシンボルが変化するだけで劇的に減少しうる．従って，線形複雑度におけるこの不安定さを測る k-誤り線形複雑度に大きな関心が寄せられている．2^n 周期列に対しては k-誤り線形複雑度が線形複雑度を下回る周期あたり誤り数 k の最小値は，同じ線形複雑度を持つ列に対しては等しいことが知られている．(Kurosawa et al.[3])
本論文では 2^n 周期バイナリ列に対し線形複雑度 L を固定して k が上記の最小値と一致するときに k-誤り線形複雑度のあらゆる可能な値を数え上げる表現を導く.それらの値のいくつかに対して，L および k-線形複雑度を固定した時対応する 2^n-周期バイナリ列の個数の表現を導いた．これらの結果は 2^n-周期バイナリ列の線形複雑度の安定性に関するいくつかの統計的性質を計算するために重要となる．Games-Chan アルゴリズムの厳密解析によるもので，このアプローチは Meidl [4] → Meidl and Venkateswarlu [5] → Fengxiang and Wenfeng [1] → 本論文とのこと.

An infinite class of balanced functions with optimum algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity [ASIACRYPT 2008]
Claude Carlet, Keqin Feng

Courtois/Meier のストリーム暗号に対する代数的攻撃と代数的 immunity という概念の導入後、最適な代数的immunityを持つBoolean関数のクラスがいくつか提案されているが、これらは代数次数が十分に高くBerlekamp-Massey攻撃やRonjom-Helleseth攻撃に耐性を持つが、よい代数的immunityとよい非線型性を兼ね備えたものはなく、correlation 攻撃に対する耐性がない。標数 2 の有限体上の Boolean 関数でサポートが原始元のべき乗に一致するものは、代数的 immunity と非線型性とにおいて良いものを与えることを示す。

F-FCSRs are still alive [ASIACRYPT 2008 RUMP]
Francois Arnault, Thierry Berger, Cedric Lauradoux, Marine Minier, Benjamin Pousee

F-FCSR-H v2 は、本会議において解読が発表されたが、修正を施した F-FCSR-H v3 を発表する。v2 の解読者らの方法は v3 には適用できないと攻撃者も認めている。

3. ブロック暗号

3.1. ブロック暗号 解析

Improved Cryptanalysis of Reduced-Round SMS4 [SAC 2008]

Jonathan Etrog, Matt Robshaw

ブロック暗号 SMS4 は構成がシンプルではあるが，中国のワイヤレスネットワークで用いられていることから，近年注目を集めている．差分攻撃のバリエーションによって既に 32 ラウンド中 21 ラウンドまでは破られている．本論文では，この暗号に線形解読を適用し，22 ラウンドのシンプルな攻撃を示している．さらに攻撃可能ラウンド数を伸ばすのに使えそうなテクニックをいくつか検討している．

New Linear Cryptanalytic Results of Reduced-Round of CAST-128 and CAST-256 [SAC 2008]

Meiqin Wang and Xiaoyun Wang and Changhui Hu

CAST-128とCAST-256に対する線形解読を行い、選択平文攻撃で各々、4段、36段まで攻撃できた。CAST-128はGPGとPGPのいくつかのバージョンでデフォルトで使用され、国際規格ISO/IEC 18033-3に採用された 64 ビット暗号である。鍵サイズは 128 ビットで、16 段繰り返し構造である。CAST-256 はAES 公募での 15 候補に含まれた 128 ビット暗号で、鍵サイズは 128/192/256 ビットの3種類、段数は48 段で共通である。CAST-128 と CAST-256 に対する従来の最も有効な攻撃は線形解読法であり、各々、4 段と 12 段の縮小版に対する既知平文攻撃が提案されている。
この発表では、剰余加算におけるキャリーの影響を考察することで、3 段に対する従来より高い確率の線形近似を導き、線形解読法に利用した結果、次の評価が理論的に導かれた。

- 6 段 CAST-128 に対する線形解読で、既知平文 $2^{53.96}$ と暗号化 $2^{88.51}$ 回分の計算。
- 24 段 CAST-256(192/256 ビット鍵)に対する線形解読で、既知平文 $2^{124.10}$ と暗号化 $2^{156.20}$ 回分の計算。
- 4 段 CAST-128 に対する線形解読で、単独暗号文 $2^{33.38}$ と暗号化 $2^{68.38}$ 回分の計算。
- 21 段 CAST-256(192/256 ビット鍵)に対する線形解読で、単独暗号文 $2^{111.08}$ と暗号化 $2^{143.50}$ 回分の計算。

Improved Impossible Differential Cryptanalysis of Reduced-Round Camellia [SAC 2008]

Wenling Wu and Lei Zhang and Wentao Zhang

FL 関数を取り除いたCamelliaに対する不能差分攻撃を行い、128ビット鍵(Camellia-128)で12段まで、256ビット鍵(Camellia-256)で16段まで攻撃できるという見積もりを得た。Camelliaは NTTと三菱電機が設計した 128 ビット・ブロック暗号で、国際規格 ISO/IEC 18033-3、日本の電子政府推奨暗号、NESSIEのポートフォリオなどに採用されている。3種類の鍵長 128/192/256 ビットが利用でき、各々の段数は18/24/24 段である。今まで多くの攻撃が試みられたが、その大多数は攻撃を簡単にするため簡易な非線形関数 FL/FL^{-1} 関数と初期/最終 XOR(排他的論理和)を取り除いた簡略版を対象にしている。中でも最も成功しているのは不能差分解析であり、簡略版の128ビット鍵Camellia(Camellia-128)に対して11段まで、簡略版 192/256 ビット鍵 Camellia (Camellia-192/Camellia-256) に対して 13 段まで攻撃が可能であった。しかし、鍵スケジュールの性質を考慮した攻撃は今まで無かった。 この発表でも、FL/FL^{-1} 関数等を除いた簡略版 Camellia を対象としており、Camellia-128 に対し、8 段の不能差分を用い、平文側と暗号文側に段を伸ばし、伸ばした部分の拡大鍵を推定した。その結果、両側に2段ずつ伸ばすことで 12 段まで攻撃でき、必要な選択平文は 2^{65}、計算量は暗号化 $2^{111.5}$ 回分以下だった。FL/FL^{-1} 関数を除いた Camellia-256 では、両側に 4 段ずつ伸ばすことで 16 段まで撃でき、必要な選択平文は 2^{89}、計算量は暗号化 $2^{222.1}$ 回分以下だった。 なお、Camellia-128とCamellia-256に対するフルスペックの段数18 段と 24 段までにはまだ差があり、正式版では FL/FL^{-1} 関数等が使われているので、現状では、安全性に問題はない。

An Improved Impossible Differential Attack on MISTY1 [ASIACRYPT 2008]

Orr Dunkelman, Nathan Keller

本研究では 5 段 Feistel に対する generic な不能差分攻撃と MISTY1 専用の slicing 攻撃を組み合わせ, FL 関数付き 6 段、および FL 関数なし 7 段の MISTY1 の攻撃に成功した. 以下の文献にて, 同様の手法により同様の結果が報告されている.

保田康平, 秦野康夫, 金子敏信, :"MISTY1 の不能差分利用攻撃に関する一考察," 信学技法, ISEC2003-56, pp.39-42, (2003-9)

Y.Hatano, K.Yasuda, and T. Kaneko,:"A Study on Impossible Differential Cryptanalysis of MISTY1", Proc. of the 2nd Int'l Conf. on Information Technology for Application (ICITA 2004), (2004.1)

なお MISTY1 に関しては SCIS 2009 にて NEC 角尾氏らのグループから、データ量 $2^{54.1}$, 計算量 $2^{120.8}$ の 7 段の高階差分攻撃が報告されている.

New Cryptanalysis of Block Cipher with Low Algebraic Degree [FSE 2009]

Bing Sun, Longjiang Qu and Chao Li

PURE 暗号は、Feistel 型で段関数が入力に対する有限体上の 3 乗とするブロック暗号であり、差分／線形解読に対する証明可能安全性がある。しかし、代数攻撃の一種の補間攻撃によって、32 段まで攻撃可能であることが分かっている。ただし、全数探索よりも少ない計算量という条件であり、実際の計算機実験で敗れるのは 6 段程度であった。
この論文では、PURE の段関数を多項式に一般化した場合の代数的特性を解析し、それに基づいて代数攻撃と積分攻撃を改良した。PURE 暗号に適用したところ、改良型補間攻撃で 10 段まで実際に解読でき、平文・暗号文組数とメモリの必要量ははともに 3^9+1 個で、PC(Pentium 4, 3.06 GHz)で 1.5 分掛った。さらに、積分攻撃において、従来は最終段出力の右半分 C_R(x)に対する和を取るところを $x^iC_R(x)$とすることで、実際に 22 段まで破れた。必要な平文・暗号文組数は $3*2^{32}$ でメモリは無視できる程度しか使用せず、PC(Pentium 4, 3.06 GHz)で 148 時間掛った。

Algebraic Techniques in Differential Cryptanalysis [FSE 2009]

Martin Albrecht and Carlos Cid

ブロック暗号 PRESENT は、ブロック長 80 ビット、フルスペックで 31 段の SPN 型暗号で、鍵長は 80 ビットと 128 ビットの2種類がある。この論文の対象である 80 ビット鍵では、4172 変数、13642 個の連立多項式で表せる。
想定した差分経路を実現する入力ペアを正しいペアと呼ぶことにすると、上記 13464 個の方程式に、正しいペアで成立する方程式群を合わせた方程式群を実際に計算機で解くことを試みる。解く過程で矛盾が生じるじれば、正しいペアでないことが分かる。攻撃を効率化するため、方程式群は最後まで解かず、適切に設定した時間内に矛盾が見つからなければ正しいペアと判断する計算の時間の上限は計算機実験で経験的に決める。正しいペアと判断したら、具体的に鍵を計算する。
80 ビット鍵の縮小 PRESENT に対してこの攻撃を適用したところ、14 段で確率 2^{-62} の差分経路を用いて 17 段まで攻撃できると評価。ここで、PolyBoRi による計算時間は 9.03～16.93 秒であった。よって、鍵の全数探索より計算時間は多く掛かると思われるが、新しい発想の攻撃手あり、今後の進展が期待できる。

Multidimensional Extension of Matsui's Algorithm 2 [FSE 2009]

Miia Hermelin, Joo Yeon Cho and Kaisa Nyberg

通常の線形解読法では、1つの線形近似式を利用するが、この発表では、複数の線形近似式を利用し、各々から得られる鍵に関する情報を統合して鍵推定を行う。鍵推定の際、個々の線形近似式による鍵推定の独立性を仮定せず、鍵に関するエントロピーに基づく鍵推定法を構成した。鍵推定では、仮定する鍵が正しいときと正しくないときの分布の区別がポイントとなるが、この発表では、χ^2 法と対数尤度比(Log-Likelihood Ratio)を使った方法の2つを試し、推定効率を比較した。
ブロック暗号 Serpent について、7 次元の線形解読で 12 ビット分の advantage を得るのに必要な平文数を実験的に評価したところ、χ^2 法では 2^{28} 個だったのに対し、LLR を使った方法では $2^{27.5}$ 個と少なく、後

者の効率の高さが実証された。

Cryptanalysis of the ISDB Scrambling Algorithm (MULTI2) [FSE 2009]
Jean-Philippe Aumasson, Jorge Nakahara Jr. and Pouyan Sepehrdad

MULTI2 は、ブロックサイズ 64 ビット、鍵長 256 ビットのブロック暗号で、Feistel 型に似た 32 段構造で構成されている。MULTI2 に対する既存の攻撃には、Aoki-Kurokawa(SCIS1995)の線形解読法によって 12 段縮小モデルまで現実的な計算時間で攻撃可能という結果がある。
今発表の成果は次の3つである。
(1)Aoki-Kurokawa の線形解読法を 20 段まで拡張
(2)推定決定型攻撃で任意の段数に拡張
(3)関連鍵スライド攻撃で 8 の倍数の段数(r)へ拡張
(1)の線形解読法に必要な平文数は $2^{39.2}$ 個、計算量は暗号化 $2^{93.4}$ 回分、メモリは $2^{39.2}$(32-bit words)である。(2)と(3)は等価鍵の解析に基づくもので、(2)に必要な平文数は 3 個、計算量は暗号化 $2^{185.4}$ 回分、メモリは 2^{31}(32-bit words)である。また、(3)に必要な平文数は 2^{33} 個、計算量は暗号化 $2^{128}/r$ 回分、メモリは 2^{33}(32-bit words)である。

3.2. ブロック暗号 設計

Building Secure Block Ciphers on Generic Attacks Assumptions [SAC 2008]
Jacques Patarin, Yannick Seurin

従来のブロック暗号のデザインは，主に発見的な議論によって行われ，そのアーキテクチャ開発の良いガイドラインとなるような理論はほとんど知られていない．こういう状況を改善するため，高い自己相似性を持った新しいタイプの対称鍵暗号プリミティブのデザイン方法を導入する．(″Russian Dolls″(マトリョーシカ) Construction と称する Feistel の再帰) このデザイン戦略は，ランダム Feistel スキームと理想的構成とを識別する最良の攻撃計算量に関する尤もらしい仮定に基づく帰着安全性証明を，暗号プリミティブに対し与えることができる．こうした仮定の下では，本結果の暗号プリミティブは，計算資源がある与えられた限界より少ないあらゆる攻撃者に対して完全に安全である．一方，例えば C[3] や KFC[4] のような情報理論的結果を用いてデザインされた他の証明可能安全対称鍵プリミティブは (重要ではあるが) 限定的な範囲の攻撃への耐性しか証明されてない．このデザイン戦略は大きな拡大鍵サイズを必要とするが，なんとか実使用可能であろう (およそ 1 MB のオーダー).

Beyond-Birthday-Bound Security Based on Tweakable Block Ciphers [FSE 2009]
Kazuhiko Minematsu

n ビットのブロック暗号を利用して、2n ビットのブロック暗号を作ったとき、通常の構成では、$2^{n/2}$ 回程度の query でランダム置換と区別できる birthday-bound が存在する。この発表では、2段 Feistel 構造の中間に、tweakable ブロック暗号を2つ挿入することによって、birthday-bound を超えることが可能であることを証明した。さらに、そのような tweakable ブロック暗号の構成法について検討した。ここで使われる tweakable 暗号に対する tweak 入力としては、暗号化における中間データまたはその truncate した値を用いており、tweakable 暗号の新しい利用法といえる。

A Very Compact Hardware Implementation of the MISTY1 Block Cipher [CHES 2008]
Dai Yamamoto, Jun Yajima, Kouichi Itoh

MISTY1 の FO/FI 関数の実装を最適化することにより、コンパクトなハードウェア実装を実現した。FO 関数の一時的なレジスタを削減し、また FI 関数のクリティカルパスを短くすることにより、0.18 μ m CMOS でゲートサイズを世界最小の 3.95K ゲートとすることができた。

4. 公開鍵暗号

4.1. 公開鍵暗号 プリミティブ

4.1.1. 公開鍵暗号 プリミティブ 解析

4.1.1.1. 公開鍵暗号 プリミティブ 解析 素因数分解問題

4.1.1.1.1. 公開鍵暗号 プリミティブ 解析 素因数分解問題 実装

Improved stage 2 to P±1 factoring algorithms [ANTS-VIII]
Alexander Kruppa(フランス)

PARI-GCM は、P±1 法および ECM において使われる Stage 2 を統一しており、これは、1992 年の Montgomery 学位論文を基にした Zimmerman-Dodson 2006 を実装したものである。factor set を分割することにより高速化を図り、P+1 法で 60 桁の分解に成功し、記録を立てた。新しい GMP-ECM リリースに入っている。

Edwards Curves and the ECM Factorisation Method [ECC 2008]
Peter Birkner (Technische Universiteit Eindhoven, Netherlands)

楕円曲線法は およそ 20 年ほど前に Lenstra によって導入された素因数分解アルゴリズムのひとつである．この方法は，与えられた整数の素因子を見つける為に（通常はモンゴメリ型の）楕円曲線を用いる．最近導入されたエドワーズ型およびツイステッド・エドワーズ型曲線は非常に効率的な演算規則を持っており，楕円曲線法の速度を改善できる可能性がある．本発表では楕円曲線法とエドワーズ曲線の簡単な概要をおさらいし，楕円曲線法に適した，即ちQ上で大きいねじれ部分群と正のランクを持つ，エドワーズ曲線の構成法を示す．GMP-ECM に組み込んで 7% の高速化に成功とのこと．

http://www.hyperelliptic.org/tanja/conf/ECC08/slides/Peter-Birkner.pdf
http://eprint.iacr.org/2008/016.pdf

ECM on graphics cards [ASIACRYPT 2008 RUMP]
Daniel J. Bernstein, Tien-Ren Chen, Chen-Mou Cheng, Tanja Lange, Bo-Yin Yang

素因数分解の楕円曲線法において、1秒間に何本の曲線を扱えるかの数値を紹介。詳細はePrintを参照。

4.1.1.1.2. 公開鍵暗号 プリミティブ 解析 素因数分解問題 予測

Running time predictions for square products and large prime variation [ANTS-VIII]
Andrew Granville(カナダ、モントリオール大学)

招待論文
素因数分解の様々な手法において、以下の処理が使われる。
・Pseudo-random な整数 $a_1,a_2,\ldots$を生成する
・$y^2=a_{i1}\times\cdots\times a_{ik}$となるような y を見つける
Pomerance の問題は、$a_i<x$としたときに、上記のような y が見つかるまでの時間を求める問題である。これに対し、以下の conjecture を提起し、ある程度証明した。
予想:
$(e^{-\gamma}-\varepsilon)J_0(x)<T<(e^{-\gamma}+\varepsilon)J_0(x)$ $(x\to\infty$のとき確率$\to 1)$
定理:

$\pi/4(e^{-\gamma}-o(1))J_0(x)<T<(3/4)J_0(x)$ （$x\rightarrow\infty$のとき確率→1）
large prime variation の個数を増やしたときの、高速化係数因子理論値および実験値、Husimi Graph との関係を述べた。
素因数分解アルゴリズム(の一部分)の理論的時間計算量評価。Large Prime Variation を増やして高速化する示唆など実用的な見地も考慮している。LPV を多用するのは最近の素因数分解高速化のトレンドであろうか？

Predicting the sieving effort for the Number Field Sieve [ANTS-VIII]
Willemien Ekkelkamp(オランダ、CWI/ライデン大学)

数体篩法に必要な関係式の数を予測することが目標である。以下の段階を踏む。
・短い篩テストを行う。
・その結果を分析し simulation を行う。
・Stop Criteria を決める(#relation>#different primes)
これにより、実データと simulation との違いは、2%以内であった。
　より大きな simulation data を考えると、RSA 暗号のより精密な安全性評価ができるかもしれない。

Quantum Computer. [PQCrypto 2008]
Graeme Smith,

　理論モデルとしての量子計算は素因数分解などの高速アルゴリズムを実現し得るが、物理的な実現に関しては様々な困難があり、NMR、Ion Traps、Josephson Junctions 等いくつかの実装アプローチが提案されている。IBM 研究所では、このうちでも Ion Traps が有望であると考え、研究を進めている。質疑においては、暗号学者の関心の高さから、実現の可能性・時期に質問が集中し、初めは明確な言及を避けていたが、最終的には聴衆の欲求不満を察したのか、10 年以内は無理との見解を述べた。

Q：量子計算機の実現時期はいつになると思うか？
A：どれだけの予算をかけるかの問題だ。
Q：年間 100 億ドルをかければ、いつになるか？
A：何ともいえない。例えば、明日、新しいコスト削減の方法をたまたま思いつけば、答えは全然変わってくる。
Q：15 の素因数分解のニュースがあって以来、それより大きな素因数分解のニュースは聞かない。今日の話では進歩しているとのことだが、より大きな素因数分解はできるようになっているのか？
A：量子計算機の研究者は、素因数分解を高速に行うことに焦点をおいている人はあまりいない。評価の観点が違う。
Q：高速に素因数分解できるのはいつになると思うか？
A：高速とはどういう意味か？
Q：2048 ビットの素因数分解はいつできるのか？
A：10 年以内には無理であろう。

4.1.1.1.3. 公開鍵暗号 プリミティブ 解析 素因数分解問題 より易しい問題

Solving Systems of Modular Equations in One Variable: How Many RSA-Encrypted Messages Does Eve Need to Know? [PKC2008]
Alexander May and Maike Ritzenhofen

RSA を利用した放送暗号化の攻撃に利用できる一変数剰余多項式方程式系に対する解読効率を従来より高めた。一変数剰余多項式方程式系(SMUPE)の解法としては、Coopersmith が提案した格子を利用する方法が今まで最も効率が良かった。今回、異なる公開鍵(e_i,N_i)に対する連立剰余多項式を一つの式にまとめた式を利用して、解法の効率を高めることに成功し、攻撃に必要な公開鍵情報の量を評価した。

A Variant of Wiener's Attack on RSA with Small Secret Exponent [ANTS-VIII poster]

Andrej Dujella (クロアチア、ザグレフ大学)

Wiener の攻撃の改良。時間計算量 O(N^2)のところを、時間計算量 O(NlogN)、空間計算量 O(N)とした。Graz 大学で 7 月に行われる central european シンポジウムに投稿予定。

E-th roots and static Diffie-Hellman attacks using index calculus [ECC 2008]
Antoine Joux

指数計算法(index calculus)は、素因数分解/離散対数問題を解く場合に用いられる手法であるが、それをモジュラーe 乗根問題や static Diffie-Hellman 問題を解くことに応用する。c+x(c:fixed,x:small)の e べきを求めるオラクルを仮定すると、素因数分解よりも効率的に解ける。また、オラクルを仮定した場合の static DH 問題も、DLP よりも効率的に解ける。

On the Validity of the ϕ-Hiding Assumption in Cryptographic Protocols [ASIACRYPT 2008]
Christian Schridde, Bernd Freisleben

モジュラス N がある特定の条件を満たすときに、ϕ-Hiding 仮定が成り立たないことを示した。$N=PQ^{2e}$(ただし、P,Q は 2 より大きい素数、e は正の整数)であり、P が問題の素数を隠しているときには、3/4 の確率で隠された素数を選ぶことができ、ϕ-Hiding 仮定は成立しない。従って ϕ-Hiding 仮定を使うときには、N がこのような条件を満たすかどうか注意する必要がある。

Solving Linear Equations Modulo Divisors: On Factoring Given Any Bits [ASIACRYPT 2008]
Mathias Herrmann, Alexander May

合成数 N の未知因子 p を法とした線型方程式の解を求める問題は、p の一部のビットが与えられたときに N の素因数分解に応用することができる。P の高々半分のビットが未知であり、かつ連続したブロックに存在する場合に、この問題は多項式時間で解かれることが知られている。未知ビットの存在するブロックが n 個ある場合に問題を拡張したとき、ヒューリスティックなアルゴリズムを導入し、p の約 70%のビットがわかれば任意の n に対し p を求めることができることを示した。ただし、アルゴリズムは n に関して指数時間であるため、n=O(loglogN)ブロックの場合に、N に関して多項式時間となる。

4.1.1.2. 公開鍵 プリミティブ 解析 (楕円)離散対数問題

Implementing a Feasible Attack against ECC2K-130 Certicom Challenge [ANTS-VIII poster]
Ahmad Lavasani(Concordia Univ.), Reza Mohammadi(Sharif Univ. of Technology)

Harley らが解いた ECCK-109 のプログラムを基にしている。問題は 1000 倍難しくなっているが、
・トータルマシン数:約 10 倍:2 万台×2 年(1 万台×6 ヶ月)
・CPU 性能向上:約 10 倍
・実装・アルゴリズム向上:約 10 倍
を見込んでいる。CPU は、SSE2 の 128-bit レジスタを使用。アルゴリズムは、distinguished point の代わりに distinguished class を導入し、Frobenius map を 131 回行って代表元を探すオーバーヘッドを削減。Berkley の BOINC という並列システムを使用。2 万台も集まっていないためプロジェクト参加者を募集中。

An update on ECDLP over extension fields [ECC 2008 rump]
Claus Diem

E を拡大体 F_{q^n}上の楕円曲線とし、a<b とする。 an^2 <= logq <= bn^2 のとき、 ECDLP を解く計算量 exp{O(logq^n)^{2/3}}(以下)のアルゴリズムが存在する (explicit なアルゴリズムである。証明は 50 ページくらい). その後、Diem から入手した preprint(2008 年 9 月 13 日版)によると、以下の statement となっている。

Cor.

Let ε > 0, and let a > 2+ ε. Then the discrete logarithm problem in the groups of rational points of elliptic curves over finite fields F_{q^n} with

(2 + ε) · n^2 ≤ log_2(q) ≤ a · n^2

can be solved in an expected time of e^O(log(q^n)^{2/3}).

証明の正しさ及び本攻撃が適用できる場合の検証が今後の課題であると考えられる。

Speeding up the Pollard Rho Method on Prime Fields [ASIACRYPT 2008]

Jung Hee Cheon, Jin Hong and Minkyu Kim (Seoul National University)

Pollard の ρ 法は素因数分解, 離散対数問題, 楕円離散対数問題など, 広いクラスの暗号プリミティブの攻撃に適用可能な攻撃アルゴリズムである. この論文は特に素体の乗法群上の離散対数問題に対する ρ 法を高速化する方法を論じたものであり, そこで利用される r-adding walk を高速化する方法を提案している. r-adding walk とは ρ アルゴリズムに用いられる反復関数で, 衝突に到達するまでの反復回数がオリジナルの ρ 法の反復関数よりも少ない事が知られている. 主要なアイディアは r-adding walk の大部分のステップで次のステップを決めるための演算は到達したノードの部分情報のみを使って決定できるので, 演算を完全には行う必要がないということである. この方法で通過するステップは普通の r-adding walk と同じであるが, 各ステップに必要な実行時間は大幅に削減できる.普通の F_p 上の r-adding walk で 1 ステップには log p サイズの 2 つの整数の乗算が必要であるが, 提案法なら $O((\log p)^{r+1} \log\log p)$ サイズの事前演算テーブルを使えば log p に関する線形の演算量しか必要としない. 著者らの実装では 1024 bit のランダム素体 p の離散対数問題に対して r-adding walk を使った ρ 法を 10 倍以上高速化できたとしている. 実装はあまりチューニングしてないとの事. 対策としては乗法群の部分群の群位数サイズを log log p 程度大きくすれば十分と考えられる. (漸近的な意味では log log log p, その大きさの部分群が取れれば p の大きさは変更する必要は無い). 楕円離散対数問題への適用は未解決問題である. この論文は Asiacrypt 2008 の 3 つのベストペーパーの内の 1 つに選ばれた.

Subset-Restricted Random Walks for the Pollard Rho Method [ASIACRYPT 2008 RUMP]

Minkyu Kim, Jung Hee Cheon, Jin Hong

本会議で素体上の ρ 法高速化で Best Paper Award を受賞した著者らによる、拡大体上での高速化へのアプローチ。詳細は PKC2009 にて発表予定。

Birthday paradox for Markov chains, with an optimal bound for collision in the Pollard rho algorithm for discrete logarithm [ANTS-VIII]

Jeong Han Kim, Ravi Montenegro, Yuval Peres and Prasad Tetali

巡回群における DLP を解く Pollard の ρ 法は、分割関数がランダムオラクルで与えられれば、$\Theta(|G|^{1/2})$ ステップで高い確率で衝突する (初めての証明)。Pollard の ρ 法は、楕円曲線暗号解読やハッシュ関数の衝突探索に応用でき、指数時間ではあるが適用範囲が広い。

A Parameterized Splitting System and its Application to the Discrete Logarithm Problem with Low Hamming Weight Product Exponents [PKC2008]

Sungwook Kim and Jung Hee Cheon

ハミング重みの積が小さな(LHWP)指数を利用した離散対数問題(DLP)ベースの暗号系に対して、パラメータ化分割システムを適用し、従来より効率の良い攻撃を実現した。DLP ベースの暗号系において、計算効率を高めるため、ハミング重みの積が小さい(LHWP)指数をがしばしば利用されている。このような暗号系に対して Coppersmith らは Splitting system(分割システム)を利用した攻撃法を提案している。ここでいう分割システムとは、与えられた $y=g^x$ に対し、x をある条件を満たすように $x=x_1+x_2$ と分割して得られる式、$yg^{-x1}=g^{x2}$ を利用する方法である。この発表では、Coppersmith を一般化してパラメータ化することで探索効率を高めた。CHES 2005 で Coron らが提案した GPS 同定スキームの変形版に適用したところ、攻撃の時間複雑が従来評価の 2^{78} から $2^{61.6}$ に改善した。また、Hoffstein と Silverman が提案した LHWP 指数を持つ離散対数問題に適用したところ、時間複雑度で従来評価の 2^{59} を上回る $2^{54.51}$ という評価を

得た。

The Discrete Logarithm Problem on Elliptic Curves Defined Over Q [ANTS-VIII poster]
安田雅哉(富士通研究所)

有理数体上の楕円曲線離散対数問題の解法を与える。p 進体にも適用可能。暗号解読に適用するには有限体からの持ち上げが必要。

Lifting and the Elliptic Curve Discrete Logarithm Problem [SAC 2008]
Joseph H. Silverman

指数計算法は古典的な有限体の離散対数問題を準指数時間で解く持ち上げアルゴリズムであるが，一般的な楕円曲線に対してはそのようなアルゴリズムは見つかっていない．一方，ECDLP を解くのに使えそうな 4 つの異なる持ち上げシナリオが存在する．つまり，持ち上げ先の群が local field であるか global field であるか，そして持ち上げ先の点がねじれ点であるか否かの選択肢がある．これらの選択肢は 持ち上げを使った ECDLP の(準指数時間)解法に対する 4 つの異なるアプローチを導くが，どのアプローチも ECDLP の(準指数時間)解法を導きはしない．それぞれにうまく働かない理由がある．本発表ではこの 4 つの方法をサーベイし，それぞれの類似点と違いを説明し，それぞれの場合に発生する障害を説明する．(ECC 2007 等で発表されたものと同じ内容)

http://mathsci.ucd.ie/~gmg/ECC2007Talks/ECC4FacesOfLifts.pdf
http://www.math.brown.edu/~jhs/Presentations/ECC4FacesOfLifts.pdf

4.1.1.3. 公開鍵 プリミティブ 解析 その他の問題

4.1.1.3.1. 公開鍵暗号 プリミティブ 解析 その他の問題 多変数多項式

Total Break of the *l*-IC Signature Scheme [PKC2008]
P.A. Fouque and G. Macariorat and L. Perret and J. Stern

l-IC 署名スキームに対し、署名偽造攻撃に成功した。l-IC 署名スキームは PKC 2007 で提案された署名方式で、多変数連立方程式の解法が NP 困難であることに基づいて設計されている。多変数連立方程式に基づく署名方式には、NESSIE 推奨暗号の SFLASH があるが、l-IC 署名スキームはより計算効率が高い。最近、SFLASH は公開鍵の差分解析を利用して完全に解読された。SFLASH で利用された差分解析にグレブナー基底アルゴリズムを組み合わせることで秘密鍵を復元し、署名の偽造に成功した。

Cryptanalysis of Rational Multivariate Public Key Cryptosystems [PQCrypto 2008]
Jintai Ding and John Wagner.

辻井、藤岡、平山らの 4 次多変数有理関数を公開鍵とする暗号(1989)ファミリーへの暗号解析を行う。攻撃のキーポイントは、2 つの有理マップの decomposition の問題を、2 つの多項式マップの decomposition の問題に変換することである。同値な秘密鍵を PC 上で数秒で得ることができ、システムを完全に破ることができる。

MXL2: Solving polynomial equations using an improved mutant strategy [PQCrypto 2008]
Johannes Buchmann, Mohamed Saied Emam Mohamed and Wael Said Abdel Mageed Mohamed

SCC2008 において提案された MutantXL アルゴリズムを改良した MXL2 アルゴリズムを提案する。実験により XL や mutantXL に比べて行列サイズを大きく削減できることを確認した。

Fast Implementation of XL [PQCrypto 2008]
Bo-yin Yang,

XL 攻撃の実装およびその QUAD および Rainbow への適用 に関して述べられた。F4/F5 ではなく XL

を使う理由は、F4/F5 の行列は dense になりメモリ不足になりがちであるため。QUAD 攻撃 15 変数の場合には、F4 では 7 次元までであったが、XL では 8 次元まで届いた。実装では Lanczos よりプログラムがよりやさしい Wiedeman アルゴリズムを用いた。行列が正方でない場合には、行をランダムに削除する手法をとり、これがなぜかうまく動くところが面白い。

Nonlinear Piece In Hand Perturbation Vector Method for Enhancing Security of Multivariate Public Key Cryptosystems [PQCrypto 2008]
Ryou Fujita, Kohtaro Tadaki and Shigeo Tsujii

多変数多項式ベース暗号のセキュリティを向上させる新しいタイプの持ち駒スキームである、非線形持ち駒撹乱ベクトルの提案。既存の方式よりも効率的なことを示し、オリジナルスキームの安全性が向上していることを実験的に示した。

4.1.1.3.2. 公開鍵暗号 プリミティブ 解析 その他の問題 格子

Recovering NTRU Secret Key From Inversion Oracles [PKC2008]
Petros Mol and Moti Yung

暗号方式NTRUの逆算オラクルを利用して、秘密鍵が復元できることを示した。NTRUは国際規格IEEE P1363.1 で採用されている公開鍵暗号方式で、安全性は格子における最短ベクトル発見の困難さに基づいている。秘密鍵を求める選択暗号文攻撃(CCA)は提案されているが、不正な暗号文または復号誤りのどちらかは必要であり、暗号文に対する平文だけで解読することは出来ていなかった。鍵生成方程式を変形して、暗号化の逆算に帰着させることにより、秘密鍵を計算することに成功した。攻撃の効率はパラメータの選び方に依存する。

Explicit hard instances of the shortest vector problem [PQCrypto 2008]
Johannes Buchmann, Richard Lindner and Markus Rückert.

格子縮小の統一的な比較はこれまでになく、NTRU/GGH などのチャレンジ 問題は、特有の暗号に基づいているものであった。Ajtai の結果に基づき、SVP の hard instance と考えられる一連の次数が大きくなっていくチャレンジ問題を公開する。これにより格子縮小アルゴリズムの統一的なベンチマークを行うことができ、暗号パラメータの設計にも役立つであろう。公開アドレスは、
http://www.latticechallenge.org
であり、与えられたノルムバウンド以下の格子のベクトルを見つければよい。

Rigorous and Efficient Short Lattice Vectors Enumeration [ASIACRYPT 2008]
Xavier Pujol, Damien Stehle

格子の最短/最近接ベクトルを問題を解く際に、Kannan-Fincke-Pohst の数え上げアルゴリズムは、格子縮小アルゴリズムの根本原理であり、格子問題に根拠を置く暗号のセキュリティを評価する際に、これらのアルゴリズムの浮動小数点実装の有効性が重要となってくる。浮動小数点 KFP アルゴリズムによって返される解のノルムの大きさ等を評価した。

4.1.1.3.3. 公開鍵暗号 プリミティブ 解析 その他の問題 その他

An Improved multi-set algorithm for the dense subset sum problem [ANTS-VIII]
Andrew Shallue(カナダ、カルガリー大学)

モジュラー部分和問題に関し、k-set バースデイ問題を解くアルゴリズムを与えそれが高い確率で解けることを示した。部分和問題の困難性は、ナップサック暗号の根拠となっており、密度が低い場合には、Lagarias-Odlyzko により SVP-oracle を仮定すれば高い確率で解ける。この結果は、モジュラー部分和/k-set バースデイという設定のため、直接暗号に適用できるのかどうか明らかではないと思うが、密度は限定していないため、ナップサック暗号の安全性を考えるには、より詳細な分析が必要である。

Cryptanalysis of MinRank [CRYPTO 2008]
Jean-Charles Faugere(Univ Paris), Francoise Levy-dit-Vehel(ENSTA), and Ludovic Perret(Univ Paris)

MinRank 問題は、HFE、TTMなどの多変数公開鍵暗号やゼロ知識認証スキームと関連を持つ問題である。Schnorr の攻撃の拡張と見ることができる、グレブナ基底を用いた新しい攻撃を提案し、ASIACRYPT2001 の Courtois による MR ゼロ知識認証スキームを破った。

Attacking and defending the McEliece cryptosystem [PQCrypto 2008]
Daniel J. Bernstein, Tanja Lange and Christiane Peters

McEliece 暗号に対する Stern の攻撃を改良することにより、2.4GHz Core 2 Quad CPU により 1400 日で解読することができる。対策としては、符号長を長くする、list decoding の使用により w を大きくする、パラメータの最適化等が考えられる。

4.1.1.4. 公開鍵 プリミティブ 解析 安全性の帰着

Bits Security of Elliptic Curve Diffie-Hellman Secret Keys [CRYPTO 2008]
Dimitar Jetchev(UCB) and Ramarathnam Venkatesan(Microsoft Research)

ECDH 秘密鍵における LSB はハードコアであることを示した。即ち、有限体 Fp 上の楕円曲線に対し、ECDH 秘密鍵の LSB を無視できない advantage で効率的に予測することができれば、ECDH 秘密鍵全体を予測することができる。

An analysis of the vector decomposition problem [PKC2008]
Steven D. Galbraith and Eric R. Verheul

通常利用される超特異楕円曲線上では、ベクトル分解問題(VDP)を解くのは巡回群上の計算DH(CDH)問題を解くのと難しさが等価であることを示した。吉田らは SCIS2003 において、VDP を解くのが困難なことに基づく暗号を提案した。VDP とは、有限体上の 2 次元空間 G で(P1,P2)のペアを基底としたとき、与えられた元 Q∈G に対し、R∈$\langle P_1 \rangle$かつ Q-R∈$\langle P_2 \rangle$を満たす R を見つける問題である。ここで、$\langle P_i \rangle$は P_i が生成する G の部分群である。VDP を解く困難度を精密に評価する研究は今まで無かった。この発表では、G が distortion ベクトル基底を持つか否かに着目した結果、通常利用される超特異楕円曲線上の VDP では、distortion ベクトル基底が存在し、VDP と巡回群上の CDH 問題の困難度の等価性が示せた。また、Duursma と Kiyavash が提案した種数 2 の非特異楕円曲線でも同じ等価性が成立する。

The Role of Discrete Logarithms in Designing Secure CryptoSystems [PKC2008]
Victor Shoup

Diffie-Hellman 鍵共有方式の安全性を高めるため、片方の秘密鍵を 1 個から 2 個
に増やした Twin DH 方式を提案し、DH 問題との関係やその多様な応用例を紹介した。応用例として、Elgamal 暗号化方式、非対話鍵共有(NIKE:Non-Interactive Key Exchange)、DH self corrector、ランダムオラクルモデルを用いずに安全性証明可能な CCA 安全な暗号化方式、PAKE(Password Authentication Key Exchange)、IBE(ID-Based Encryption)などが挙げられた。

The Elliptic Curve Discrete Logarithm Problem and Equivalent Hard Problems for Elliptic Divisibility Sequences [SAC 2008]
Kristin E. Lauter and Katherine E. Stange

楕円曲線上の離散対数問題と等価な3種類の楕円分割可能列(EDS)に関連した問題を定義し、既存の暗号方式の安全性との関連性を調べた。楕円分割可能列とは次の関係式を満たす列 W(n)である。
$W(n+m)W(n-m) = W(n+1)W(n-1)W(m)^2-W(m+1)W(m-1)W(n)^2$
EDS に関する3種類の問題、EDS 結合問題、EDS 剰余問題、EDS 離散対数問題を定義し、

3種類のEDSに関する問題の困難度を検討した。その結果、楕円曲線上の離散対数問題を解く困難度が準指数時間であるとき、同じ困難度を持つことが証明できた。また、EDS結合問題とTateペアリングやMOV/Frey Rueck攻撃との関係を論じた。

Lattice Based Cryptography. [PQCrypto 2008]
Daniele Micciancio.

ラティスベースハッシュ関数・署名・暗号の最近の結果について述べられた。Ajitai のハッシュ関数 fA(x)=Ax mod q に関し、l∞-SVP がほとんどのΛ(A)に対して困難であれば collision resistant であることなどが知られているが、2002 年に fA が oneway となるための仮定を明確にした。Cyclic lattice を使うのは NTRU と似た idea である。署名に関しては、Lyubashevsky-Micciancio の one time signature scheme がある種の approximate SVP/SIVP の worst case hardness に基づいていえること、暗号に関しては、GGH/NTRU(1997)は証明がなく、AD(1997)/Regev(2005)の安全性などが紹介された。最後に、Open Problem として、
－Regev 暗号を cyclic lattice を用いて instantiate すること(効率的だが証明は破綻する)
－署名を cyclic lattice を用いて instantiate すること(証明は成立する)
－ラティスベース関数の具体的なセキュリティ評価
－実用に耐えうる実用的な instantiations
などが挙げられた。

4.1.2. 公開鍵暗号 プリミティブ 高速化・実装

4.1.2.1. 公開鍵暗号 プリミティブ 高速化・実装 楕円

Ultra High Performance ECC over NIST Primes on Commercial FPGAs [CHES2008]
Tim Güneysu, Christof Paar

商用の FPGA を利用して、NIST が指定した素数で超高速で動作する楕円曲線暗号の実装を行った。楕円曲線暗号は同等の安全性なら、RSA より鍵サイズは小さくて済み、計算も簡単である。しかし、その実装は、最近の高速 FPGA の能力を十分発揮できるほどには極まっていない。
この論文では、Xilinx の Virtex-4 SX55 FPGA 上で計算のコアになる部分を Digital Signal Processing(DSP)ブロックで処理する方法を試みた。その結果、NIST の指定した素数 P-224 と P-256 に対し、毎秒 37,000 回以上の楕円スカラー倍演算を達成した。

High Performance ECC over NIST Primes on Commercial FPGAs [ECC 2008]
Tim Güneysu (Ruhr-University Bochum, Germany)

FPGA の DSP ブロックを使って NIST Prime (P-224,P-256) の楕円を実装する話題. 楕円スカラー倍演算が small インプリで 360 μsec, large インプリで 26 μsec で比較的高速な実装. CHES 2008 で発表された

Ultra High Performance ECC over NIST Primes on Commercial FPGAs

と基本的には同じ内容.

Exploiting the Power of GPUs for Asymmetric Cryptography [CHES2008]
Robert Szerwinski, Tim Güneysu

画像用プロセッサ(GPU)の並列処理性能を活かした公開鍵実装を行った。性能とゲート数に関し、最近の GPU の性能は CPU を大きく凌駕している。しかし、多くの計算機でほとんどの時間、GPU はアイドル状態にあるので、汎用のコプロセッサとして利用することが可能である。この論文では、Nvida 8800GTS

Graphic card 上にモンゴメリ乗算、剰余数表現(RNS)、混合 Radix システム(MRS)などを実装して利用する方法を試みた。その結果、1024 ビットの RSA/DSA ベースのべき乗剰余計算 毎秒 813 回、NIST 推奨曲線 P-224 上の楕円スカラー倍 毎秒 1412 回を達成した。

Elliptic Curve on GPU [ECC 2008 rump]
Chen-Mou Cheng, Tanja Lange

GPU を使った ECM の実装により、New Speed Record を作った。

ECC is Ready for RFID – A Proof in Silicon [SAC 2008]
Daniel Hein and Johannes Wolkerstorfer and Norbert Felber

RFID に楕円曲線暗号が実装できるとを実証した。商品の偽造を防ぐ手段として RFID が期待されているが、ID の真正性を検証するためにはチャレンジ・レスポンスが有効である。これは、共通鍵暗号で実現でき、AES による実装が可能であることが分かっているが、鍵の運用に関する条件がきついため実用的でない。そこで、公開鍵暗号が必要になるが、実装サイズと計算時間の制約から、楕円曲線暗号(ECC)が最有力候補となる。
この発表では、RFID の電力供給は受動型とし、163 ビットの楕円曲線を使い、単位時間当たりの電力消費を抑えるため、実際に計算する際のワード長は 16 ビットに設定した構成を採用した。UMC L180 GII 1P/6M 1.8V/3.3V CMOS technology で実装したところ、面積は 128,098 μm^2、13,250 GE、最大周波数は 46 MHz、電力消費は 10.8 μW@ 106 KHz だった。1 回の ECC 計算に約 300,000 クロック掛り、ディジタル通信の国際規格 ISO/IEC 18000-3 に従ったとき、電力消費は 10.8 μW だった。これらは実測値であり、実際に利用できる。

Faster ECC using an efficient endomorphism for general curves [ANTS-VIII poster]
Steven Galbraith, Renate Scheidler (Univ. London)

詳細は、2 週間以内に ePrint archive に置く。この分野は日本の研究が多く、refer された 4 論文は、すべて日本人(趙先生、松尾先生、野上先生ら)によるものであった。

New record breaking implementations of ECC on quadratic extensions using endomorphisms [ECC 2008]
Mike Scott (Dublin City University, Ireland)

素体上の標準的な方法より高速だと思われる高速な自己準同型を利用した 2 次拡大上の楕円スカラー倍の新しい方法が最近(再)提案されている．ここでは（何人かの日本の研究者による先駆的な仕事の上に打ち立てられた）新しい方法について説明し，8-ビットマイクロプロセッサー上および標準的な 64-ビットワークステーション上での実装について報告する．特に実装上の問題と挑戦に関して取り上げ，いくつかの可能な拡張についても説明する．ANTS VIII の Last Minute research announcement などでも紹介された内容．

http://www.hyperelliptic.org/tanja/conf/ECC08/slides/Mike-Scott.pdf
http://eprint.iacr.org/2008/194.pdf

Double-Base Number System and Applications [ECC 2008]
Christophe Doche

楕円曲線の n 倍算を計算する手法の一つに、n を $2^{ai} \times 3^{bi}$ の和の形に展開することにより高速化するものがある。greedy なアルゴリズムでは、まず n を $2^a \times 3^b$ の形で最も良く近似し、その近似との差についての近似を繰り返す。係数を 6 と互いに素なものに拡張することにより、greedy アルゴリズムより鎖の長さを 10%短くすることに成功した。また、Koblitz 曲線の τ とその conjugate に関して同様な展開を行うことにより、8-9%の高速化に成功した。

New Composite Operations and Precomputation Scheme for Elliptic Curve Cryptosystems over Prime

Fields [PKC2008]
Patrick Longa and Ali Miri

楕円曲線暗号の高速化のために dP+Q の形の計算を高速化した。楕円曲線暗号における計算ではスカラ倍演算の時間が大きな割合を占め、高速化における最も重要な検討対象となっている。特に、dを2以上の小さな整数としたとき、dP+Q の形の計算がしばしば現れる。この発表では、dP+Q = P+P+…+P+(P+Q)の形に展開し、変形することで、従来より高い実装性能を実現した。d=2 の例では、計算時間が 6.2%の削減できた。

4.1.2.2. 公開鍵暗号 プリミティブ 高速化・実装 Edwards 型楕円曲線

The elliptic curve zoo: a study of curve shapes [ANTS-VIII poster]
D.Bernstein, Tanja Lange

Edwards 型楕円曲線と Weierstrass 型との比較。ここ 1 年ほどの間に Edwards 型は、Weierstrass 型を追い抜いたと主張。char 2 の場合、任意の ordinary EC は、complete binary Edwards 曲線と双有理同値。奇標数の場合は、2007 年 1 月から 3 月の間に(自分達が)完成した。標数 2 の場合は、2008 年 2/13-2/29 の間に(自分達が)完成した。詳細は、hyperelliptic.org/EFD または ePrint 2008/171
Q:higher genus の場合に似たようなことはできるのか？
A: Working on it.

Binary Edwards Curves [CHES2008]
Daniel J. Bernstein, Tanja Lange, Reza Rezaeian Farashahi

標数 2 の Edwards 型楕円曲線における例外のない加算と2倍算の項式を導いた。素体上の Edwards 型の楕円曲線では加算と2倍算の公式が同じになり、サイドチャネル攻撃耐性と計算効率が高いことが示されているが、素体上の Edwards 型楕円曲線の式はそのままでは、標数 2 の楕円曲線にならなかった。この論文では、標数 2 の Edwards 型楕円曲線が $d_1(x+y)+d_2(x^2+y^2)=xy+xy(x+y)+x^2y^2$ であることを示した。ここで、k を体としたとき、d_1,d_2 は k の元で、$d_1 \neq 0$, $d_2 \neq d_1^2+d_1$ を満たす。また、例外のない加算と2倍算の公式を導いた。2倍算専用公式の計算コストは 2M+6S+3D になった。ここで、M, S, D は各々、k 上での乗算、2乗算、曲線パラメータとの乗算を表す。

Binary Edwards Curves [ECC 2008]
Reza Rezaeian Farashahi (Technische Universiteit Eindhoven, Netherlands)

エドワーズ曲線は点の座標に関して強い対称性を持った加法則を与える，新しい対称的な楕円曲線の型である．本講演では標数 2 の ordinary 楕円曲線に対する新しい型である ″バイナリ エドワーズ曲線″ を提案する．この新しい型を用いて標数 2 の楕円曲線に対して，初めての完全加法公式を提案する．（“完全”とは単位元(無限遠点)も含めた全ての点をサポートするという意味）この完全バイナリエドワーズ曲線は n>2 なる F_{2^n}上の ordinary 楕円曲線の全ての同型類をカバーする．また，バイナリエドワーズ曲線に対する非常に高速な2倍算公式を提案する．それは、はじめての完全2倍算(専用)公式でもある．最後に差分加算(differential-addition)の完全公式を示す．この公式は非常に高速な差分加算を標数 2 の楕円曲線に対して提供する．CHES 2008 で発表された

Binary Edwards Curves [CHES 2008]

の詳細版で，ニュートンダイアグラムを用いた曲線のデザイン，ワイヤストラスフォームとの双方向の変換，超特異な楕円には行けない事などが紹介された．

http://www.hyperelliptic.org/tanja/conf/ECC08/slides/Reza-Rezaeian-Farashahi.pdf
http://eprint.iacr.org/2008/171.pdf

Twisted Edwards Curves Revisited [ASIACRYPT 2008]
Huseyin Hisil, Kenneth Koon-Ho Wong, Gary Carter and Ed Dawson

Edwards 曲線の導入により楕円曲線暗号の高速化が図られているが、twisted Edwards 曲線に拡張座標系を導入することにより、演算量の削減に成功した。これまで加算には最速でも 9M+1S の演算量がかかっていたところを、曲線の係数を適切に選ぶことにより 8M にまで削減できることを示した。並列計算にも向いており、4 プロセッサで実装することにより実際のコストを 2M に下げることができる。スカラー倍算の高速化も可能であり、更には SPA 攻撃に対する自然な対策となっている。

4.1.2.3. 公開鍵暗号 プリミティブ 高速化・実装 超楕円

Efficient hyperelliptic arithmetic using balanced representation for divisors [ANTS-VIII]
Steven D. Galbraith(イギリス、ロイヤル・ホロウェイ大学)

超楕円曲線の演算において、imaginary/balanced/non-balanced representation の各場合の演算速度比較。

Faster Halvings in Genus 2 [SAC 2008]
Peter Birkner, Nicolas Thériault

2 の拡大体上の種数 2 の超楕円の diviser class の 1/2 倍算の研究. 暗号学的に興味ある曲線および群位数が 4 で割れない曲線に対する explicit halving formulas を示した. その他 h(x) の型によっていろいろな結果を示した.

HECC Goes Embedded: An Area-efficient Implementation of HECC [SAC 2008]
Junfeng Fan and Lejla Batina and Ingrid Verbauwhede

超楕円曲線暗号(HECC)が組み込み系で使えるよう、小型実装を実現した。楕円曲線暗号(ECC)と超楕円曲線暗号(HECC)はともに、RSA 暗号より短い鍵サイズで同等の安全性が実現できる。1024 ビット RSA と同等の安全性を持つ ECC の定義体長は 163 ビット、HECC の定義体長は 83 ビットと見積もられている。しかし、射影座標を使ったとき、EC 上の点加算に GF(2^{163})上の乗算 15 回と自乗算 3 回が必要なのに対し、HEC 上の点加算では GF(2^{83})上の乗算 49 回と自乗算 4 回が必要となり、ビット長が半分なのを考慮しても計算コストはずっと大きい。高速化のために並列化を行うと面積が大きくなってしまう。
この発表では、乗算と逆元計算を一体化し、Xilinx ISE8.1i を使い、Virtex-II FPGA(XC2V 4000)上のコプロセッサを合成した。その結果、HECC のスカラー積が、2316 スライス、2016 ビット・メモリを使うと、311 μ sec で実行できた。これは今までの HECC の FPGA 実装で最も高速である。

4.1.2.4. 公開鍵暗号 プリミティブ 高速化・実装 ペアリング

On Software Parallel Implementation of Cryptographic Pairings [SAC 2008]
Philipp Grabher, Johann Großschädl, Dan Page

ペアリングの効率を高めるための膨大な研究がある.ペアリングを計算するハードウェアアクセラレーターは大抵高速化の為に拡大体演算内で並列演算を用いるが, ソフトウェアでは並列化はあまり強調されていない. この論文ではペアリング内部(intra-pairing)での並列演算および複数のペアリングを同時に計算する際の(inter-pairing)並列演算に焦点を当てている. BN 曲線 (埋め込み次数 12) での Ate-pairing, で、いわゆる SIMD を使った結果.

Efficient Pairing Computation on Genus 2 Curves in Projective Coordinates [SAC 2008]
Xinxin Fan, Guang Gong, David Jao

種数 2 の素体超楕円上のペアリングで射影座標の使用を検討した. [Chatterjee-Sarkar- Barua(2004)] のアイディアを一般化し射影座標と新しく導入した座標に適用した. 種数 2 の超特異と非超特異の両方に適用.

- F_p 上の種数 2、超特異、埋め込み次数 4 で最速 (I/M > 14.65 の場合)、

- F_p 上の種数 2、非超特異、埋め込み次数 2 で初めてのペアリングの効率的実装

なる結果を得た．特殊な種数 2 の非超特異曲線を使ってさらに高速化できるとのこと．

Efficient and Generalized Pairing Computation on Abelian Varieties [ECC 2008]
Hyang-Sook Lee (Ewha Womans University, Seoul, Korea)

本発表では，ペアリング計算を効率化するテイトペアリングのバリエーションを簡単に概観する．特に，発表者らは R-ate ペアリングと呼ぶ，(超)楕円曲線上に双線形ペアリングを構築する新しい方法を提案している．このペアリングは Ate ペアリングおよび Ate_i ペアリングの一般化であり，ペアリング計算の効率を向上する．従来ミラーのアルゴリズムにおけるループ長が log(r^{1/φ(k)}) の下界に達してなかった幾つかのペアリング用楕円曲線に対して，R-ate ペアリングを用いて この下界を達成できる．種数 2 の超特異超楕円曲線上では，このアプローチのミラーのアルゴリズムにおけるループ長が Ate ペアリングの場合より短いことを示す．R-ate ペアリングに関するこの結果は Runjeong Lee (KIAS) および Cheol-Min Park (Ewha Womans University) との共同研究によるものである．

http://www.hyperelliptic.org/tanja/conf/ECC08/slides/Hyang-Sook-Lee.pdf
http://eprint.iacr.org/2008/040.pdf

4.1.2.5. 公開鍵暗号 プリミティブ 高速化・実装 低レイヤプリミティブ

An Optimized Hardware Architecture for the Montgomery Multiplication Algorithm [PKC2008]
Miaoqing Huang and Kris Gaj and Soonhak Kwon and Tarek El-Ghazawi

モンゴメリ法の計算速度を改善するハードウェア構成を実現した。RSA 暗号を初めとする剰余乗算を高速化する方法として、モンゴメリ法が知られているが、桁上がりの有無を待つため並列化ができないという問題のため、さらなる高速化が出来なかった。今回、二つの可能な選択肢の両方を計算し、桁上がりの有無が判明した段階で片方だけを利用することにより、計算を高速化を試みた。2種類のアルゴリズム MWR2MM と MWR4MM を Xilinx Virtex-II 6000 FPGA で実装したところ、対面積性能で従来より約 30%の高速化を達成した。

A New Bit-Serial Architecture for Field Multiplication Using Polynomial Bases [CHES 2008]
Arash Reyhani-Masoleh

多項式基底を用いた標数 2 の拡大体上の、新しいシリアル出力ビットシリアル乗算器を提案する。各クロックサイクルで積演算結果の 1 ビットを 1 サイクルのレイテンシーで出力する。一般の規約多項式に関するこのタイプの乗算器としては初めてのものである。

Trinomial bases and Chinese remaindering for modular polynomial multiplication [SAC 2008]
Eric Schost and Arash Hariri

標数 2 の 3 項式を既約多項式とする有限体上の乗算にモンゴメリ法を適用する際に、剰余数セット(RNS)を使って高速化した。標数 2 の有限体上での乗算を高速化するのにモンゴメリ法が利用されるが、Cook らは乗算モジュロ R として x^m を選んだ。計算コストの点では m が大きいほど良いが、計算速度は m が中程度(例えば、1000 以下)が望ましい。乗算モジュロ R を互いに素となる n 個の多項式 r_i の積、つまり、$R=r_1 \cdots r_n$ として、剰余数セット(RNS)の手法を利用する。ここで、r_i の最大次数は等しく d とし、3 項式としたところ、元の有限体上の乗算が RNS 上の乗算 $7nd^2$ 回と加算 $7nd^2+8n^2d-2nd\log_2(n)+6nd-2n^2-10n$ 回で実行できた。

Faster multiplication in GF(2)[x] [ANTS-VIII]
Emmanuel Thome(フランス)

GF(2)[x]の計算は、暗号を含め応用が広い。多くのソフトウェア実装があるが、以下の機能を持ったものはまれである。
・CPU 固有命令を利用したもの

・Toom-Cook multiplication
・FFT
64 次以下のもの(SIMD)、中くらいのサイズのもの(Toom-3)、大きいサイズの場合(FFT:additive/tenary 両方実装)に分け、それぞれ高速化を図った。
暗号処理高速化への影響がどの程度あるか、より詳細な分析が必要であろう。

4.1.2.6. 公開鍵暗号 プリミティブ 高速化・実装 その他の暗号

Time-Area Optimized Public-Key Engines: MQ-Cryptosystems as Replacement for Elliptic Curves ? [CHES2008]
Andrey Bogdanov, Thomas Eisenbarth, Andy Rupp, Christopher Wolf

多変数2次多項式公開鍵暗号の実装を時間・領域に関して最適化した。楕円曲線暗号は RSA 暗号と比べ、短い鍵で高い安全性が達成されるため、盛んに研究されているが、量子計算機が実用化されると、効率的に解けることが分かっている。これに対し、多変数2次多項式(MQ)暗号は、量子計算機でも効率的には解けないと予想されている。そこで、MQ 暗号の署名法を効率的に実装することを目指し、amended Tame Transformation Signatures(amTTS)を使いし、FPGA 実装において、シストリック・アレイを利用した線形連立方程式の解法回路を設計する方法を試みた。その結果、時間・領域効率で、楕円曲線暗号を利用した署名より 50 倍も効率が高かった。

Practical-Sized Instances of Multivariate PKCs: Rainbow, and ℓIC-derivatives [PQCrypto 2008]
Anna Inn-Tung Chen, Chia-Hsin Owen Chen, Ming-Shing Chen, Chen-Mou Cheng and Bo-Yin Yang

Rainbow, TTS, lIC を実装し、処理速度を測定し、既存の RSA/ECC 等と比較することによってトラディショナルな暗号に対して数倍～数百倍のアドバンテージがあることを検証した。また、各スキームに対し、具体的なインスタンスを挙げた。

McElice cryptosystem implementation: theory and practice [PQCrypto 2008]
Bhaskar Biswas and Nicolas Sendrier

McEliece 暗号の実装において、Generator matrix を row echelon form とするなどにより、鍵サイズを減らし、information rate を上げ、暗号化を高速化した。Intel Core 2 プロセッサにより実装を行い、88 ビットセキュリティ(パラメータ(m,t)=(11,32),(12,21))において、暗号化で 178/126 cycles/byte、復号で 1848/573 cycles/byte を達成した。鍵サイズは 73/118kB。EBATS における RSA1024(暗号化 800 cycles/byte、復号 23100 cycles/byte)、NTRU787(暗号化 4753 cycles/byte、復号 8445 cycles/byte)と比較すると、5 倍～数 10 倍有利である。

SQUARE-VINEGAR SIGNATURE SCHEME [PQCrypto 2008]
John Baena, Crystal Clough and Jintai Ding

HFEv-署名スキームの改良提案。標数を奇素数とし、次数を 2 の secret map により、HFE タイプの弱点である署名処理速度の高速化を図り、署名、鍵生成とも、数十倍の改善となった。また、F4 による解読実験により、推奨パラメータを提示した。

4.1.3. 公開鍵暗号 プリミティブ 楕円・超楕円・代数曲線

Computing Zeta functions in families of $C_{a,b}$ curves using deformation [ANTS-VIII]
Wouter Castryck(ベルギー、ルーベン大学)

$C_{a,b}$ 曲線のゼータ関数を計算する手法の改良。現在の state of art は、直接法に関しては、Kedlaya のアルゴリズムを一般化した Denef-Vercauterer の方法($F_{2^{60}}$ 上の $C_{3,4}$)が 1.5 時間程度、間接法に関しては、

数日かかる。改良により暗号に適した(位数がほとんど素数な Jacobian を持つ $C_{a,b}$)曲線の生成は、genus=3,4 で、数分でできるようになった。

Computing L-series of Hyperelliptic curves [ANTS-VIII]
Andrew V. Sutherland(アメリカ、MIT 大学)

genus 3 以下の超楕円曲線を対象とした L-series の計算。はじめに Frobenius Trace の分布をデモで表示し、理論どおりになるケースとならないケースがあることがよくわかる（グラフは、math.mit.edu/drew で入手可能）。ゼータ関数の分子に興味があり、good reduction を持つすべての p<N に対して $L_p(T)$を計算することが目標。アルゴリズムをどうするべきか、N をどの程度大きくできるか？genus により使うアルゴリズムを変えるストラテジー等により、PARI、Magma をしのぐ性能を達成した。プログラム smalljac v2 は、GPL のもとで、ソースコードを無料公開している。(drew@math.mit.edu)

A survey on algorithms for computing isogenies on low genus curves [ANTS-VIII]
Francois Morain(フランス)

招待講演
研究のモチベーションは、数論・計算・暗号応用などがある。はじめに isogeny の理論、次にモジュラー多項式の計算、最後に isogeny の計算に関してサーベイが述べられた。結論としては genus が 1 のケースは、ほとんどできているが、genus が 1 より大きい場合は、バラバラな成果があるのみである。genus が大きくなると、対象が指数的に大きくなるため、簡単ではない。

Efficiently computable distortion maps for supersingular curves [ANTS-VIII]
Katsuyuki Takashima(日本、三菱電機)

distortion map はペアリング暗号で使用される重要な技術である。Galbraith らの超特異曲線における d.m.に関する結果において未解決であった問題を解決した。$y^2=x^w+1$,$y^2+y=x^5+x^3+b$ の形の各々の曲線に関し、ある条件(gcd(r,2gw)=1,r<19)のもと、直接構成するアプローチにより効率的に計算できる d.m.の存在を示した。
Q:19 は optimal か？(Galbraith)
A:わからない。もっと小さいかもしれない。

On prime-order elliptic curves with embedding degrees k=3,4,6 [ANTS-VIII]
Koray Karabina(カナダ、Waterloo 大学)

MNT(Miyaji-Nakabayashi-Takano)曲線はペアリング暗号で使用される曲線であるが、まれな曲線である(Luca-Shperlinski 2006)。それに付随する MNT equation をより深く分析し、より効率的に曲線パラメータを明確にするアルゴリズムを提示する。

Almost prime orders of CM elliptic curves modulo p [ANTS-VIII]
Jorge Jumenez Urroz(カナダ、モントリオール大学)

位数がほぼ素数になるような曲線の数の評価(の向上)。

Point counting in genus 2: reaching 128 bits [ECC 2008]
Eric Schost (University of Western Ontario, Canada)

種数 2 の暗号系は今や同じ安全性レベルの楕円曲線暗号と同等かそれ以上に高速である．この暗号系に関する残された課題は 例えば 2^128 くらいの大きさの素体上で安全で適当な曲線パラメータを決定する事くらいである．Pierrick Gaudry と発表者との共同研究の結果，最近このサイズの位数計算が出来るようになった．高次拡大での素因子分解からホモトピー連続変形までの基礎となるアルゴリズムの検討など詳細を報告する．

http://www.hyperelliptic.org/tanja/conf/ECC08/slides/Eric-Schost.pdf

Constructing abelian varieties for cryptographic use [ECC 2008]
Peter Stevenhagen (Universiteit Leiden, Netherlands)

アーベル多様体(大抵は有限体上定義され群位数に好ましい性質を持ちそしてペアリングを持つ楕円曲線か超楕円曲線のヤコビアン)が暗号に利用されている．多くの場合，暗号に利用可能なアーベル多様体は虚数乗法を用いて適当なヴェイユ数から構築可能である．本発表では，低次元の状況における，そのようなヴェイユ数の見つけ方および使い方を説明する．

http://www.hyperelliptic.org/tanja/conf/ECC08/slides/Peter-Stevenhagen.pdf

Division Polynomials for Twisted Edwards Curves [ECC 2008 rump]
Richard Maloney

以下に論文が公開されている。
http://arxiv.org/abs/0809.2182

Computing Hilbert class polynomials with the CRT method [ECC 2008]
Andrew V. Sutherland

新しい技術であるペアリング暗号用の楕円曲線生成法の改良。曲線生成の過程において Hilbert class polynomial H_D(x)を計算するが、既存の方法には 3 種類(複素解析的方法、p 進法、CRT(中国人剰余)法)あり、最も速く多くの曲線を生成できるのは、複素解析的方法である。本研究では、H_D(x)modp を計算するアルゴリズムを導入し、CRT 法により、$|D|>10^{12}$(従来は 10^{10} 程度)、h(D)=400000 程度のペアリングに適した曲線を数多く生成することに成功した。

More Constructing Pairing-Friendly Elliptic Curves for Cryptography [ANTS-VIII poster]
田中悟、中村憲(首都大学東京)

ペアリング計算に適した楕円曲線の構成と具体例の提示。

Abel's Generalization of the Addition Operation on Elliptic Curves [ECC 2008]
Harold M. Edwards (Courant Institute of Mathematical Sciences, USA)

ニールス・ヘンリック アーベルの 1826 年の定理は 関数論，リーマン面，代数幾何などの分野における数学のその後の発展に重大な影響を与えた．さまざまな分野のさまざまな数学者たちがその定理をいろんな方法で定式化してきたので，「アーベルの定理とは何か？」という問いに答えるのは簡単ではない．この発表ではアーベル自身がおそらくそうしたであろう見方---即ち楕円曲線上の加法演算の自然な一般化としてこの定理を捉えることによってこの問いに取り組む．(数学史的な話題)

http://www.hyperelliptic.org/tanja/conf/ECC08/slides/Ed-Edwards.pdf

4.1.4. 公開鍵暗号 プリミティブ その他

RSA - Past, Present, Future [CHES2008]
Adi Shamir(Weizmann Inst. of Science)

RSA 暗号の歴史を紐解くことにより将来を占うことを目的とした講演であり、いくつかの興味深い示唆を含んでいた。
[RSA Past] 1979-1982
・今年は CHES10 周年であるとともに、RSA 暗号の 30 周年でもある。1981 に始まった CRYPTO、1999 に始まった CHES ともに大きく成功した会議であるが、これらの成功の共通要因をデータマイニングで調

べてみたところ、どちらも最初の talk は私であり、しかもプログラムに typo があることが共通点であることが判明した。
・1980 頃から、RSA の 3 人は別々の所に住んでおり、当時は電話・ネットによるコミュニケーションは難しく、テープに会話を録音・送付することによって、さまざまな議論を行った。当時 PC は Novelty であり、Shamir と Adleman は、CRYPTO82 において Apple II で 10 時間かけて knapsack 暗号を破った。1979 年当時、 RSA-512 の復号は Apple II で 2 分かかり、鍵生成は数時間かかっていた。このため、ハードウェアを作らざるを得ず、初めて自信を持って発表した$3000 の RSA ボードは、0.1sec で復号を行ったが、誰も興味を持たなかった。次に、当時 MIT で新設された VLSI システムのコースを利用して RSA チップを開発したが、LSI を作成するチャンスは 1 度だけであり、半年かけて設計・開発した LSI はショートして失敗に終わった。ただし、この頃の経験が元になって、来週の CRYPTO 学会で発表するバグ攻撃(LSI のバグを利用した攻撃)の着想を得た。
[RSA Present]
・RSA 暗号は数学的には成熟した技術であるが、サイドチャネル攻撃・故障攻撃・バグ攻撃などの新しい攻撃が問題となっている。バグ攻撃は来週の CRYPTO2008 で発表するが、誤った積となる一組の数を知っているだけで、RSA/DH/ECC を攻撃することができ、OAEP でさえ対策にはならない。
[RSA Future]
・今後の見通しでは、脅威として考えられるのは、計算機の性能が徐徐に上がっていくことと、アルゴリズムが飛躍的に進歩することである。30 年後には、RSA 暗号の現在使用されている鍵長は安全ではなくなっているであろうが、30 年後に安全であろう鍵長は現在は使用に耐えないであろう。ポスト RSA 暗号と目されている楕円曲線暗号は、30 年後には all or nothing であろう。即ち準指数時間解読アルゴリズムが発見されなければ、鍵長の伸びが小さくて済む利点を将来には十分活用できるであろうが、そうでなければ RSA 暗号に対するメリットは全くなくなる。

Post Quantum Cryptography. [PQCrypto 2008]
Johannes Buchmann,

Software Update、車の組込み機器、パスポートなど、日常生活においても意識しないところで公開鍵暗号やそれによる認証 が必要となってきている。1978 年に発表された RSA 暗号は当時 RSA200 を推奨したが、27 年後の 2005 年には RSA200 は解読された。暗号の寿命は 13 年～27 年程度であり、将来に備えなければならない。Post-Quantum Cryptography の現在における候補としては以下のものがある。
－格子ベース
－符号ベース
－多変数ベース
－ハッシュベース
－量子暗号
また、扱うテーマとしては以下が考えられる。
－モデル
－困難なインスタンス
－アルゴリズム
－証明
－実装
－標準

Lattices in cryptography [ANTS-VIII]
Johannes Buchmann(ドイツ、ダルムシュタット大学), 招待講演

暗号に疎い聴衆もいるため、基礎的な話題から入る。電子社会においては、偽のウェブ記事、フィッシング詐欺、偽の update プログラムなどの危険性があり、真の情報であることの認証が必要であり、そのために電子署名が実際に使われている。20 年前は理論のみの感があったが、現在では重要な社会インフラであることを強調したい。
Peter Shor のアルゴリズム(1994)により暗号は解読されるため、量子計算機にも強い署名が求められている。宣伝:PQCrypt 2008 10/17-19 Cincinatti で開催。格子の CVP 問題は、NP 困難であり、候補の一つである。GGH 署名、NTRU 署名などがあったが、2006 年に Nguyen、Regev らにより完全に破られた。NTRU251 は 400 個の署名により、GGH-400 は、16 万個の署名により解読された。署名を集めて、基本

領域を求める方法である。
Dahmen,Schneider らは 2008 年に Winterritz の OTS ベースの署名 GMSS を作ったが、署名サイズが大きすぎる欠点があった。Lyubashevsky,Micciancio は 2008 年に署名サイズ削減の改良を行ったが、その後、新しい攻撃を発見してしまい、実用にはいたっていない。
Linder,Ruckert らは 2008 年に NTRU-based Lattice OTS を提示した。NTRU-lattce の SVP に根拠を置いている。www.LatticeChallenge.org にチャレンジ問題がある。

4.2. 公開鍵暗号 鍵共有・秘匿

SAS-Based Group Authentication and Key Agreement Protocols [PKC2008]
Sven Laur and Sylvain Pasini

従来の一般的な鍵共有方式の多くは能動攻撃に対して安全でなく、メッセージの送受信における本格的なメッセージ認証が不可欠だった。これに対し、CRYPTO2005 で Vaudenay 氏により提案された SAS (Secure Authentication String, 信頼できる通信路で共有された20ビット程度の情報) を利用した能動的攻撃者に対して安全なメッセージ認証方式が Pasino と Vaudenay によって CT-RSA 2006 で提案されている。本発表では、この提案方式を複数人プロトコルに展開し、従来の認証された通信路数が限定されている場合に適用可能なグループメッセージ認証方式を提案。提案方式によりグループ鍵共有プロトコルを構成することが出来る。

Certificateless Encryption Schemes Strongly Secure in the Standard Model [PKC2008]
Alexander W Dent and Benoit Libert and Kenneth G. Paterson

署名なしの暗号スキーム(CLE)は、署名付き公開鍵方式とIDベース暗号の中間に位置する有益な方式であるが、安全性の証明には困難が伴っていた。この発表では、任意の受動的攻撃者に対して安全な方式をからスタンダードモデルにおける強い攻撃者に対しても安全なCLEを構成する方法を提示。また強い攻撃者に対して安全な方式の具体的構成法として、Water が提案した IBE 方式をベースにした構成方法を提案した。

Unidirectional Chosen-Ciphertext Secure Proxy Re-Encryption [PKC2008]
Benoit Libert and Damien Vergnaud

代理者による再暗号化とは、代理者がある公開鍵で暗号化された暗号文を同じ平文の別の公開鍵で暗号化した暗号文に、元の平文を知ることなく変換することである。従来の再暗号化方式では、公開鍵の置き換えは双方向で出来たため、利用法によっては安全性に問題が生じた。この発表では、公開鍵の置き換えが一方向に限られる方式が報告された。方式の構成には 2005 年/2006 年に Ateniese らにより提案された方式を基に第3者によりその暗号文の正しさが検証可能な再暗号化方式を組込んだ。スタンダードモデルでの安全性証明可能な方式となっている。

Public Key Broadcast Encryption with Low Number of Keys and Constant Decryption Time [PKC2008]
Yi-Ru Liu and Wen-Guey Tzeng

放送暗号とは、正当な権利を持つユーザがメッセージ(コンテンツ)を受け取れ、権利を持たないユーザが利用できなくする方式である。この発表では、双線形 Diffie-Hellman 問題の困難性に基づいた安全性を持ち、計算効率の良い3種類の放送暗号が提案された。1 つ目は、Bilinear map を利用した基本方式、2 つ目は Naor らにより Crypto 2001 で提案された SD 方式の中で用いられている subset cover method を応用した方式、3 つ目は SD method を更に展開した LSD method を応用した方式である。

Faster and Shorter Password-Authenticated Key Exchange [TCC2008]
Rosario Gennaro

CRF モデル(common reference model)で効率的な PAKE(password authenticated key exchange)の構成方法を提案。既存結果としてGennaroらに折提案されているGLフレームワークをベースにしている。GLプロトコルでは MIT(man-in-the-middle atack)を防ぐ為の non-malliability を実現する為に ワンタイム署名を用いていた。提案方式ではワンタイム書名の代わりに短い MAC(message authentication codes：メッセージ認証子)を利用する。プロトコルの中の暗号化アルゴリズムの non-malliability を活かし、暗号文に何かラベルとなるような値を入れ込む。また、MAC に用いる鍵を生成するのに使うハッシュ関数に smooth progective hash function を利用する。

Circular-Secure Encryption from Decision Diffie-Hellman [CRYPTO 2008]

Dan Boneh, Shai Halevi, Mike Hamburg, Rafail Ostrovsky

秘密鍵に依存するメッセージを暗号化しても安全な公開鍵暗号システムを構築する。特に、公開鍵・秘密鍵ペア(pki, ski),i=1,2,…,n において書く ski を pk(i mod n +1)で暗号化する安全な鍵サイクルを使用しても安全である。鍵サイクルは、鍵管理システムや匿名信用証明の文脈で登場する。DDH 仮定のもと選択平文攻撃に対して circular 安全な暗号システムをランダムオラクルによらずに構成した。

Public Key Locally Decodable Codes [CRYPTO 2008]

Brett Hemenway, Rafail Ostrovsky

局所的に復号可能な誤り訂正符号でもある公開鍵暗号スキーム(PKLDC)の概念を導入する。特に、多項式時間の攻撃者に、すべての暗号文を読み一定割合のビットを破壊することを許したとしても、復号アルゴリズムは暗号文の sublinear 数のビットを読むだけで、無視できる確率を除き平文のどのビットも復元することができる。Semantically 安全な公開鍵暗号とプライベート情報回復(PIR)プロトコルからPKLDCを構成する方法を与える。準同型暗号は PIR を意味するため、準同型暗号から PKLDC への帰着も示す。Gentry/Ramzan の PIR プロトコルに適用することにより、メッセージサイズ n、セキュリティパラメータ k に対し、暗号文サイズ O(n)、公開鍵サイズ O(n+k)、サイズ $O(k^2)$の局所性を持つ PKLDC を得る。

A modular security analysis of the TLS handshake protocol [ASIACRYPT 2008]

P. Morrissey, N.P. Smart and B. Warinschi (University of Bristol)

本研究は，TLS で使用されているプロトコルのモジュール化手法を解析したものである．TLS プロトコルの鍵共有ハンドシェイクは3つのレイヤから構成されている．上位アプリケーションに提供されるアプリケーション鍵はマスター鍵から対話プロトコル AK_{SSL} によって導出され，マスター鍵はプリマスター鍵から，対話プロトコル MKD_{SSL} によって導出される．プリマスター鍵は Signed DH や RSA 鍵配送を使って鍵共有が行われる．この研究では次の事を証明している．

- 定理：Πを OW-PMS 安全なプリマスター鍵共有プロトコルとし，Mac を安全なメッセージ認証コードとし，G をランダムオラクルとすると（Π;MKD_{SSL}(Mac,G)）は OW-MS 安全なマスター鍵共有プロトコルとなる．
- 定理：Πを OW-MS 安全なマスター鍵共有プロトコルとし，H をランダムオラクルとすると（Π;AK_{SSL}(H)）は IND-AK 安全なアプリケーション鍵共有プロトコルとなる．

上記の定理により，Mac，G，H，をそれぞれ安全であるとするなら TLS のアプリケーション鍵共有の IND-AK 安全はプリマスター鍵共有の OW-PMS 安全から導くことが出来る．この論文は Asiacrypt 2008 の 3 つのベストペーパーの内の 1 つに選ばれた．

OAEP is Secure under Key-Dependent Messages [ASIACRYPT 2008]

Michael Backes, Markus Durmuth and Dominique Unruh (Saarland University)

鍵依存メッセージ安全性（KDM 安全性）は鍵サイクルが暗号の中に現れる場合(例えば鍵自体がその鍵で暗号化されている場合など)を取り扱う為に Black，Rogaway，Shrimpton によって導入された．この論文では，適応的懐柔(adaptive corruption)および任意の動的攻撃を含むよう KDM 安全性の定義を

拡張した adKDM 安全性について論じ，OAEP 暗号スキームがランダムオラクルモデルにおいて adKDM 安全性を満たすことを示している.

Efficient Chosen Ciphertext Secure Public Key Encryption under the Computational Diffie-Hellman Assumption [ASIACRYPT 2008]

Goichiro Hanaoka, Kaoru Kurosawa

CDH 仮定のもとで CCA 安全となる公開鍵暗号スキームを示す。Cash-Kiltz-Shoup らによるスキームでは暗号文サイズのオーバーヘッドは DDH 仮定に基づく Cramer-Shoup スキームに対して、k をセキュリティパラメータとしたときに、k/logk+2 個の群要素分だけ増加したが、本スキームでは 3 個の群要素分ですむ。また、DDH 仮定よりも弱い HDH(hashed Diffie-Hellman)仮定に基づくより効率的な CCA 安全な公開鍵暗号スキームを示す。これらのスキームは Naor-Pinkas のブロードキャスト暗号(BE)に基づいているが、任意の selectively CPA 安全な verifiable BE スキームを CCA 安全な KEM に変換する方法を示す。更に、任意の CPA 安全な verifiable BE スキームを CCA 安全な BE にほとんどコストなしに変換することができる。

Chosen Ciphertext Security with Optimal Ciphertext Overhead [ASIACRYPT 2008]

Masayuki Abe, Eike Kiltz, Tatsuaki Okamoto

公開鍵暗号が CCA 攻撃に対して安全であるためには、暗号文にある程度のランダム性を取り入れなければならない。2^t ステップの総当り攻撃者に対してアドバンテージが $2^{-\varepsilon}$ 以下になるためには、暗号文オーバーヘッドの下限は一般に $t+\varepsilon$ であるが、これまでの IND-CCA スキームは、2t ビット以上の暗号文オーバーヘッドを必要としていた。4 ラウンド Feistel ネットワークを用いることにより、ランダムオラクルモデルの下で IND-CCA 安全な最適な暗号文オーバーヘッドを持つ公開鍵暗号スキームを示した。

4.3. 公開鍵暗号 署名・認証

Off-Line/On-Line Signatures: Theoretical aspects and Experimental Results [PKC2008]

Dario Catalano and Mario Di Raimondo and Dario Fiore and Rosario Gennaro

オフライン／オンライン署名方式とは、オフラインで事前の計算をしておき、メッセージを受け取ってからオンラインでは低コストで署名を作成する方式である。この発表では、この署名方式で既存に示されている2つの方式 Shamir-Tauman 方式と Even らの方式の安全性を解析し、カメレオンハッシュが弱い意味でのワンタイム署名として用いることが出来ることを示すことで、2 つの方式は概念的には大きな違いがないことを示した。またその考察の過程で、two-trapdoor chameleon hash を用いると強い意味でのワンタイム署名を構成できることも示している。また、実際に SSH のライブラリで効率的に実装できることを実証した。

Construction of Universal Designated-Verifier Signatures and Identity-Based Signatures from Standard Signatures [PKC2008]

Siamak F Shahandashti and Reihaneh Safavi-Naini

汎用検証者指定署名(universal designated-verifier signature)とは、署名を持つものなら誰でもその署名を望みの検証者への検証者指定署名に変換でき、さらに指定された検証者はその検証者指定署名の正しさを検証できるが、他者にその正しさを確信させることができないような署名方式である。この発表では、効率的で安全性証明可能な方式を提案。方式の構成には ID-based 署名を利用しており、また、証明には完全な honest verifier zero-knowledge(HVZK) を用いるのではなく、方式に十分なややリラクスさせた証明手法を用いて、ランダムオラクルモデルで示されている。
最新版は、IACR/e-print の 2007/462 に公開されている。

Proxy Signatures Secure Against Proxy Key Exposure [PKC2008]

Jacob C. N. Schuldt and Kanta Matsuura and Kenneth G. Paterson

代理人署名方式とは、代表者が必要に応じて代理人に署名する権限を与える署名方式である。この発表では、より現実の利用方法にマッチした安全性証明モデルを提示し、1 階層で
なく複数階層であることを想定し、また、代理人の鍵が公開されても署名の安全性が保証される構成方法を示した。更に ID-base の構成も可能であるとしている

Lattice-Based Identification Schemes Secure Under Active Attacks [PKC2008]
Vadim Lyubashevsky

同定(ID)スキームは利用者を特定する方式で、従来示されている結果のほとんどは数論の問題の困難性に基づくものであった。本発表では格子問題の困難性に基づくチャレンジレスポンス方式の同定スキームを提案。安全性の証明として、能動的攻撃者に対して方式の安全性をランダムインスタンスの解法問題(FOCS2002 で Micciancio により提示されている)に帰着させている。この問題は、worst case で 格子問題と等価の解法困難性を持つことが示されている。正当なユーザが常に検証者からのレスポンスに対して返答する場合、受動的攻撃者に対してすら秘密鍵に関する情報が漏れるが、ユーザが時折レスポンスを返さない場合は並列攻撃に対しても witness-indistinguishable であるとしている。

Online Untransferable Signatures [PKC2008]
Moses Liskov and Silvio Micali

オンラインの電子署名において、署名検証の権利を移行できないようにする機能が必要となる。従来の署名方式では、オフラインではこの性質の安全性が保たれるものの、プロトコルが終了していないオンライン上での攻撃法が存在した。この発表では、オンライン上の攻撃を想定したとしても安全で効率も従来法に比べて同等程度となるプロトコルを提案。モデルとして PKI を前提としており、構成にはランダムオラクルやゼロ知識証明を用いない Designated Confirmer 署名方式に似た構成をとっている。

Security of Digital Signature Schemes in Weakened Random Oracle Models [PKC2008]
Akira Numayama and Toshiyuki Isshiki and Keisuke Tanaka

電子署名スキームの安全性を証明するのに、ハッシュ関数をランダム・オラクル(RO)だと仮定することが多いが、RO の条件を必ずしも全部満たす必要はない。この発表では、衝突発見困難性などの条件を外した弱められた RO モデルを使った電子署名の安全性を解析し、各条件の意義を明らかにした。弱められた RO モデルを具現化するために証明の中で攻撃者に通常のリソースの他、collision oracle が与えられている。

A Digital Signature Scheme based on CVP_∞[PKC2008]
Thomas Plantard and Willy Susilo and Khin Than Win

格子における最短ベクトル問題(CVP)の困難性を利用した電子署名方式である GGH スキームは、距離として l_2 ノルムを使っているために攻撃が存在することが知られている。この発表では、l_∞ノルムを使うことによって、安全性と計算速度の両方を改善できることが示された。更にパラメータを変化させた場合の処理効率と署名空間の解析結果を示した。

Equivocal Blind Signatures and Adaptive UC-Security [TCC2008]
Aggelos Kiayias and Hong-Sheng Zhou

lite プラインド署名という攻撃者に条件をつけたモデルで安全性証明可能な方式を構成。(攻撃者は、corrupt しているユーザのランダムテープを要求されたら示さないといけない)を提案。目的は安全なブラインド署名に求められる要求条件の中で zero-knowledge に関連する要求条件を切り離して取り扱うこと

を意図し、single-prover ZK と single-verifier ZK[1] を用いて 2-move equivocal lite blind signature を構成している。その構成には TCC 2006 で NTT 岡本(龍明)氏により提案された方式が利用されている。この署名を用いて adaptive な攻撃者に対して安全性証明可能な方式を構成している。

Improved Bounds on Security Reductions for Discrete Log Based Signatures [CRYPTO 2008]

Sanjam Garg (IIT) ,Raghav Bhaskar, and Satyanarayana V. Lokam(Microsoft Research India)

Schnorr 署名スキームの偽造攻撃を DLP を解くアルゴリズムに帰着するときの loss 因子下限を $q^{1/2}$ から、$q^{2/3}$ に下げた。すなわち、以前と同レベルのセキュリティを実現するためには、より大きなパラメータを採用しなければならない。

DNSCurves [ECC 2008 rump]

Dan Bernstein

DNS のセキュリティを保つために、DNSSEC という米国政府プロジェクトが 15 年間 1000 万ドルをかけて行われたが、ユーザー数は 100 人にも達していない。DNSSEC では 1024 ビット RSA 署名を使っていたが、ECDH で行う DNSCurve というプロジェクトが始まっていることの紹介。

A New Efficient Threshold Ring Signature Scheme based on Coding Theory [PQCrypto 2008]

Carlos Aguilar Melchor, Pierre-Louis Cayrel and philippe gaborit

Stern の認証/署名を拡張することにより、初めての効率的な符号ベースリング署名スキームおよび符号ベース閾値リング署名スキームを示した。t-out-of-N 閾値に関し、署名サイズは O(N)であり t によらない。プロトコルは anonymous でありランダムオラクルモデルで安全であり、計算量は O(N)である。

Merkle tree traversal revisited [PQCrypto 2008]

Johannes Buchmann, Erik Dahmen and Michael Schneider

Merkle 木における認証パスの計算において、これまでの best algorithm である Szydlo のアルゴリズムを上回るアルゴリズムを提案する。Merkle 木における内部ノードと葉とを区別することにより、各ステップにおける葉の数のバランスをとることにより、例えば木の高さ H=20 において 15%の高速化を達成した。

Digital Signatures out of Second-Preimage Resistant Hash Functions [PQCrypto 2008]

Erik Dahmen, Katsuyuki Okeya, Tsuyoshi Takagi and Camille Vuillaume.

Merkle 署名スキームのバリアントとして、より弱いセキュリティ仮定を用いた SPR-MSS を提案する。ハッシュ関数の 2nd preimage/preimage resistance を仮定すれば、適応的選択メッセージ攻撃に対して、存在的偽造が不可能となる。

Concurrently Secure Identification Schemes Based on the Worst-Case Hardness of Lattice Problems [ASIACRYPT 2008]

Akinori Kawachi, Keisuke Tanaka, Keita Xagawa

Stern の Identification スキームは、符号理論におけるあるデコード問題の平均的困難性と衝突困難なハッシュ関数を仮定して、受動攻撃に対して安全である。Stern のスキームのバリアントとして、ラティス問題の最悪ケース困難性を仮定して、並列攻撃に対して安全な 2 つのスキームを提案する。更に、これらのバリアントは、効率的な匿名 Identification スキームも構成できることを示す。

---

[1] ZK : Zero-Knowledge : ゼロ知識証明の略。相手に秘密の知識を与えることなく、秘密の知識を保有していることを示す手法。

5. その他

5.1. その他 解析

On the Power of Power Analysis in the Real World: A complete Break of the $K_{EE}L_{OQ}$ Code Hopping Scheme [CRYPTO 2008]

Thomas Eisenbarth, Timo Kasper(Ruhr Univ. Bochum), Amir Moradi(Sharif Univ. of Tech.), Christof Paar(Ruhr Univ. Bochum)

多くの車のドアロックシステム、また欧米のほとんどのガレージ開閉システムには、1980 年代に南アフリカで開発された $K_{EE}L_{OQ}$ 暗号が採用されている。Manufacturer 鍵は一意で、それとシリアル番号とから、各コントローラーのデバイス鍵が作られる。システムのすべての受信機には、Manufacturer 鍵が埋め込まれており、送られてくるシリアル番号とからデバイス鍵を認証する。電力解析攻撃により、実際の製品から、Manufacturer 鍵やデバイス鍵を取り出すことに成功し、鍵の複製や本物の鍵を無効にすることができた。

無線傍受により平文で送られているシリアル番号を入手し既にわかっている Manufacturer 鍵とからデバイス鍵を割り出し、鍵の複製による(すなわち本物の鍵を使わない)ガレージ開閉を行うことができる。更には、カウンタの操作をPCで行い、カウンタを大幅に増加させることにより本物の鍵はその増加回数だけ押さないと機能しないが、PCからは自由に開閉できる。実製品の攻撃に成功した点においてインパクトの強い発表であった。ただし、講演中のデモは残念ながら失敗に終わった。

On the Power of Power Analysis in the Real World [ECC 2008]

Timo Kasper

多くの車のドアロックシステム、また欧米のほとんどのガレージ開閉システムには、1980 年代に南アフリカで開発された $K_{EE}L_{OQ}$ 暗号が採用されている。Manufacturer 鍵は一意で、それとシリアル番号とから、各コントローラーのデバイス鍵が作られる。システムのすべてのレシーバーには、Manufacturer 鍵が埋め込まれており、送られてくるシリアル番号とからデバイス鍵を認証する。電力解析により、実際の製品から、Manufacturer 鍵やデバイス鍵を取り出すことに成功し、鍵の複製や本物の鍵を無効にすることができた。デモでは、無線傍受により平文で送られているシリアル番号を入手し既にわかっている Manufacturer 鍵とからデバイス鍵を割り出し、鍵の複製すなわち本物の鍵を使わないガレージ開閉を行った。更には、カウンタの操作を PC で行い、本来のカウンタを 5 インクリメントすることにより、本物の鍵を 5 回押さないとガレージが開かないようにすることもできた。更には、カウンタを 3000 増加させることにより本物の鍵は 3000 回押さないと機能しないが、PC からは自由に開閉できることを示した。実製品の攻撃に成功した点においてインパクトの強い発表であった

ePassport の複製ツール (2008/09/29)

The Hackers Choice なるグループにより ePassport を複製したり修正したりできるツールが公開された. 下記の URL にて，詳細およびデモ動画などが公開されている. self-signed certificate が問題になっているとのこと. 当面の旅券業務に関しては物理的なセキュリティ手段により運用可能であろうとのこと. 将来的にはより本格的な暗号学的ケアが必要とされるであろう.

THC-ePassports
http://freeworld.thc.org/thc-epassport/
The Risk of ePassports and RFID
http://blog.thc.org/index.php?/archives/4-The-Risk-of-ePassports-and-RFID.html

Practical attacks against WEP and WPA

Martin Beck (TU-Dresden, Germany), Erik Tews (TU-Darmstadt, Germany)

WEP の脆弱性については、以前から様々な現実的攻撃が指摘されていたが、本論文では新たに WPA TKIP に対する現実的な攻撃が発表された.

http://dl.aircrack-ng.org/breakingwepandwpa.pdf

SSH 通信において一部データが漏えいする可能性 (2008/11/17)
CPNI-957037

概要
SSH(Secure Shell)は、ネットワークを介してインターネット上に置かれているサーバにログインしたり、コマンドを実行したりするためのプログラムおよび通信プロトコルで、データは暗号化された状態で通信が行なわれます。SSH で使用される通信方式の一部に対する攻撃方法が報告されています。
影響を受けるシステム
SSH を実装する製品が影響を受ける可能性があります。
詳細情報
報告された攻撃方法では、SSH がデフォルトで使用する通信方式において、ひとつの暗号化ブロックから 32 ビットの平文を取り出すことができるとされています。この攻撃が行なわれると、SSH セッションが切れることがあります。RFC 4251 では、通信エラーが発生した際再接続すべきとされているため、自動的に再接続する実装の場合、攻撃による影響が大きくなる可能性があります。
想定される影響
攻撃が成立する可能性は低いとされていますが、攻撃が成立した場合、ひとつの暗号化ブロックから 32 ビットの平文を取り出すことが可能です。
対策方法
CTR モードを使用する。CBC(Cipher Block Chaining)モードではなく CTR(CounTR)モードを使用する。RFC 4344 において、SSH で使用する CTR モードに関する記述がされています。また、OpenSSH 3.7 以降では CTR モードの使用がサポートされています。

http://jvn.jp/niscc/CPNI-957037/
http://www.cpni.gov.uk/Docs/Vulnerability_Advisory_SSH.txt

Extracting RSA Private Keys from a Particular TPM [ASIACRYPT 2008 RUMP]
Tsutomu Matsumoto, Yoshio Takahashi

ある特定の TPM(Trusted Platform Module)チップにおける素数生成処理の SPA 攻撃により RSA 暗号の秘密鍵を求めることに成功した。

On the Security of HB# Against a Man-in-the-Middle Attack [ASIACRYPT 2008]
Khaled Ouafi, Raphael Overbeck and Serge Vaudenay

RFID 用認証プロトコル HB#の安全性は、ある特定のクラスの man-in-the-middle 攻撃者に対してしか証明されておらず、一般の場合には安全と予想されているのみであったが、本論文では、HB#および RANDOM- HB#に対する一般的な攻撃を示す。HB#の場合には、パラメーター集合により 2^{25} もしくは 2^{20} 認証ラウンドで、RANDOM- HB#の場合には、2^{34} もしくは 2^{28} 認証ラウンドで、共有秘密を復元できる。更にある条件の下では、計算量は漸近的に多項式時間となることを示す。

Key-Recovery Attacks on Universal Hash Function Based MAC Algorithm [CRYPTO 2008]
Helena Handschuh(Spansion) and Bart Preneel(Katholieke Univ. Leuven)

汎用ハッシュ関数に基づくMACアルゴリズムに対するいくつかの攻撃を提案しその有効性を評価した。攻撃の対象となるアルゴリズムは、Polynomial ハッシュ(GF(2n)、GF(p))、MMH、Square ハッシュ、NMH、NH、WH、Bucket ハッシュ(短い鍵)である。各々に対し、弱鍵の存在、鍵の漏洩、誕生日攻撃の拡張を示した。ISO/IEC JTC1/SC27 において汎用ハッシュ関数に基づく MAC アルゴリズムの標準 9797-3 を作成中であるため、本研究内容を参考とすべきである。

MAC Reforgeability [FSE 2009]
John Black and Martin Cochran

MAC において衝突を1回起こせたとき、次の衝突を起こすのに要する計算量がそれより小さくなるかどうかが安全性の基準として重要になる場合がある。この発表では、2回目の衝突の起こしやすさをreforgeability として定義した。次に、既存の各種 MAC について reforgeability を評価したところ、パディング攻撃やその他の攻撃によって全部、破れることが分かった。より詳しく言うと、パディング攻撃で状態なしの全部及び状態有りのほとんどが破れ、状態有りでも nonce を再利用するという誤った利用法をすると破れることが分かった。
次に reforgeability のない MAC が構成できないか検討し、Carter-Wegman-Shoup MAC をベースとしたWMAC を導入した。WMAC は最も効率的な攻撃法に対する安全性を達成し、安全性・速度・タグ長・状態利用の有無に関するトレードオフを調整できる。ただし、他の Wegman-Carter 型 MAC よりも計算量は多くなる。

Short chosen-prefix collisions for MD5 and the creation of a rogue CA certificate
Marc Stevens and Alex Sotirov and Jake Appelbaum and Arjen Lenstra and David Molnar and Dag Arne Osvik and Benne de Weger

MD5 に対して Eurocrypt 2007 において発表されていた衝突発見攻撃(Chosen-prefix Collision)を電子証明書に関する署名の偽造に応用して、SSL 用の中間 CA 証明書の作成に成功した.

http://eprint.iacr.org/2009/111.pdf

2008 年暮れに 25th Chaos Communication Congress で報告された以下の発表の詳細版.

MD5 Considered Harmful Today Creating a rogue CA certificate
http://events.ccc.de/congress/2008/Fahrplan/attachments/1251_md5-collisions-1.0.pdf

5.2. その他 暗号理論

Relations Among Notions of Plaintext Awareness [PKC2008]
James Birkett and Alexander W. Dent

与えられた暗号文に対する平文の回答が正しいか否かを判断できるを平文認知(PA: plaintext awareness)と言う。この発表では、平文認知バリエーションとそれらの安全性に関する関係を解析した結果を示した。より強い概念として PA2 が示されているが、本発表では、PA2I という概念を提示し、それらが IND-CPA および OW-CPA の条件化で帰着関係・separation の関係を示した。

Completely Non-Malleable Encryption Revisited [PKC2008]
Carmine Ventre and Ivan Visconti

頑強性(non-malleability)とは公開鍵暗号で、秘密鍵を知らない攻撃者が与えられた暗号文を、対応する平文が何らかの関係を持つ別の暗号文に変形できない性質のことであり、完全頑強性(completely non-malleability)とは攻撃者が出力暗号文用の公開鍵を自分で選べる場合にも頑強性が保たれる性質を言う。この発表では、game-base で示される定義を示し、それらの定義からこれまで示されている simulation-base の定義への帰着関係を示している。interactive non-black-box 技術などを用いて上記の定義を満たす暗号方式の構成方法を示している。

Incrementally Verifiable Computation or Knowledge Implies Time/Space Efficiency [TCC2008]
Paul Valiant

非対話証明を行う際に必要となる時間および領域(メモリ量)を改善した方式の提案。証明者は従来手法の証明者が使う領域に多項式程度の領域を利用し、また線形程度の時間を使う。一方検証者の使う時間および領域は非常に小さく従来手法の検証者の用いる定数倍程度である。構成にはCS-proof(computationally sound proof)を利用する。知識に関するCS proof が存在すると仮定すると複数の CS proof をマージしても証明の長さが変わらない証明を構成でき、これを用いることによりincrementally verifiable computation が構成できる。この発表は本会議の最優秀論文賞に選ばれた。

On Seed-Incompressible Functions [TCC2008]

Shai Halevi, Steven Myers, and Charles Rackoff

SI(seed ncompressibility)という概念を提示し、暗号プロトコルやアプリケーションではランダムオラクルほど強い要求条件は必要なくSIを満たすことで安全に構成できると主張。n ビット seed の関数 f_s(・) がseed incompressible であるとは、 n/2 ビットの(seed s に依存するものも含め)アドバイスが攻撃者に与えられ、f_s(・)へのオラクルアクセスが攻撃者に許されるような環境下であっても、その攻撃者は、アドバイスを一切与えられずに f_s(・)へのオラクルアクセスのみが許される環境下よりも効率的に f_s(・)を breakすることが出来ないような場合にその関数 f_s(・)は SI であるという。SI な PRF(Pseudo-random functions)は存在しないことを示し、SI よりやや弱い概念 SI correlation interactability という概念を提示。この存在も否定できる場合もあるが、完全にないとは否定しきれない。SI correlation interactable function があれば CRHF(collision resistant hash functions) の構成や Σ-プロトコルから NIZK(non-interactive zero-knowledge)を構成するのには十分であることも示された。

Basing weak public-key cryptography on strong one-way functions [TCC2008]

Eli Biham, Yaron Goren and Yuval Ishai

共通鍵暗号を用いた鍵共有プロトコルに関しては、Ralph と Merkle により提案された結果がある。この結果では攻撃者の run time と正当なユーザの run time とのギャップがせいぜい quadratic 程度あれば、共通鍵暗号を用いて安全な鍵共有プロトコルを構成することが示されている。この結果に起因し、exponentially strong な一方向関数を用いると上記の攻撃者に対して安全な鍵共有プロトコルを構成できることを示した。このプロトコルの安全性強度は Yao の XOR lemma のバリエーションで記されるより強い意味での hard-core predicate を満たす一方向性関数を用いると強化することが出来ることを示した一方、そのような一方向性関数は、black box モデルでは構成できないことも示している。さらにこれらの結果と bounded storage モデルで安全性証明可能なプロトコルのランダムオラクルモデルで安性性証明可能なプロトコルへの変換に変換手法に関する考察を行った。

Which Languages have 4-Round Zero-Knowledge Proofs? [TCC2008]

Jonathan Katz

言語 L で 4 ラウンドの black-box で computational zero-knowledge proof が存在する場合、言語 $\overline{L}$は MA に含まれることを示した。この結果は多項式階層が崩れないことを仮定した場合 NP 完全問題の言語は(少なくとも black-box では) 4 ラウンドの Computational Zero-Knowledge proof を持たないことを意味する。本結果は proof にのみ適用される結果であり argument の場合には NP[2]完全な言語であっても 4 ラウンドの Computational Zero-Knowledge が存在することは従来結果で示されている。

Layered Specifications, Design and Analysis of Security Protocols [TCC2008]

Amir Herzberg and Igal Yoffe

新しいモデルの提案。基本コンセプトは解析の対象となるプロトコルや方式を層ごとにゲームベースのフレームワークで捉え、下位層から順に積み上げる。上位層の攻撃者は下位層にアクセス可能な条件化でその挙動を識別不可能であることを安全性の根拠とするモデルである。質疑の時間には、すべての方式をこのモデルで捉えることはできないのではないか、これは(UC[3]モデルでの)限定した

---

[2] 計算複雑性理論における問題の複雑性クラスで、Non-deterministic Polynomial time(非決定性多項式時間)の略。

[3] Universal Composebility. 安全性が確認されている構成要素を用いて、別の安全なシステムを構築しようとする概念。

environment のみを捉えているのではないか、などの意見が出ており、懐疑的に思う聴講者もいたようである。

Invited talk : A Survey of Game-Theoretic Approaches for the Design and Analysis of Protocols [TCC2008]

Jonathan Katz

最近注目を集めている game 理論の暗号分野への導入について。試みとしては 2 方向。geme 理論の中に暗号的概念を持ち込むか、game 理論を暗号のフレームワークに載せるか。前者は game 理論で一般的に用いられる trusted mediator を如何にして distributed cryptographic protocol で構成するかが問題となり、後者の場合 game 理論で想定されるユーザ(rational adversary として)を暗号のフレームワークでの捉え方が課題となる。

Verifiably Secure Devices [TCC2008]

Sergei Izmalkov, Matt Lepinski and Silvio Micali

Verifiably secure device というコンセプトを提案。これは secure computing の概念を強めたような概念。ballet box モデルで実現できる。game 理論の中に暗号の概念を取込むアプローチ。2 種類提案されており、一つは GMW を若干改変して用いた.実際に実装もなされており、詳細は MIT-CSAIL-TR-2007-040 に掲載。もう一つの方法では、各プレイヤは全く独立に処理を進めることが出来る。後者は前者より強い安全性を持つ。後者をベースに Permutation inverse, Permutation Product, Permutation Clone などを示した。

Cryptography and Game Theory: Designing Protocols for Exchanging Information [TCC2008]

Gillat Kol and Moni Naor

game 理論で捉えられる rational user を想定し暗号プロトコルの安全性の中で取り扱う試み。Fair protocol で rational user 取り扱う為に問題となるのは rational user は最終ラウンドで送信するのをやめてしまう挙動である。この問題を解決する為にまず SBC(simultaneous broad cast channel)を想定し、rushing が起きない状況で、fair, coalition-resilient rational secret sharing scheme を構成し、これを利用して rational MPC(multiparty computation) を構成。更に NSBC(Non-simultaneous broadcast channel)の場合で送信者が 1 人である場合に展開した。提案方式では backward induction を必要としない。

An Equivalence between Zero Knowledge and Commitments [TCC2008]

Shien Jin Ong and Salil Vadhan

zero-knowledge が(sender は efficient であり non standard な 1-out-of-2 binding な) instance-dependent コミットメントと等価であることを示した。全ての promis problem Π について、$\Pi \in SZKP$[4]は Π が YES instance に関して statistically hiding であり NO instance に関して statistically binding であり、public coin をもつ constant ラウンドな instance-depend commitment を持つことと等価である。NP 問題に属する問題 について $\Pi \in CZKP$[5]は Π が YES instance に関して computationally hiding であり NO instance に関して statistically binding であり、public coin をもち、constant ラウンドな instance-depend commitment を持つことと等価である。$\Pi \in SZKA$ は Π が YES instance に関して statistically hiding であり NO instance に関して computationally binding であり、public coin をもつ instance-depend commitment を持つことと等価である。$\Pi \in CZKA$ は Π が YES instance に関して computationally hiding であり NO instance に関して computationally binding であり、public coin をもつ instance-depend commitment を持つことと等価である。

The Round-Complexity of Black-Box Zero-Knowledge: A Combinatorial Characterization [TCC2008]

---

[4] SZKP:Statistical Zero Knowledge Interactive Proof.

[5] CZKP:Computational Zero Knowledge Interactive Proof.

Daniele Micciancio and Scott Yilek

任意の semantically secure な暗号化アルゴリズムから non-malleable なものの black-box を用いての構成方法を示した。Pass らにより Crypto 2006 で non-black-box での構成方法は示されており、それを更に発展させた結果。提案方式は更に Cramer らにより示されている結果とあわせると black-box で bounded storage モデルでの bounded-CCA attack に対して non-malliable な方式にも展開できる。構成にはローカルにチェックし自己修正可能なメッセージエンコーディング technique が使われている。

On Constant-Round Concurrent Zero-Knowledge [TCC2008]

Rafael Pass and Muthuramakrishnan Venkitasubramaniam

PQT(quasi-polynomial time machine)を用いて constant-round concurrent zero-knowledge の構成を示す。PQT に対して CFP (clow-free permutation)を仮定すると全ての NP 言語について PQT に対して O(1)[6]-ラウンドの perfect conccurent black-box ZK argument が構成できる。 同様に OWF(one-way function) と CRHF (collision-resistant hash function) を仮定すると、O(1)-ラウンドの concurrent computational black-box ZK proof が構成できる。OWF[7]を仮定すると、O(1)-ラウンドの concurrent computationa black-box ZK argument が構成できる。また、特に GNI(Graph Non-Isomorphism) と ANR(Quadratic Non-Residuosity) については、上記のような仮定無しに O(1)-ラウンド concurrent perfect ZK proof が存在する。

Concurrent Non-Malleable Commitments from One-way Functions [TCC2008]

Huijia Lin, Rafael Pass and Muthuramakrishnan Venkitasubramaniam

OWF(one-way function)から concurrent non-malleable コミットメントの構成方法を提案。black-box を用いている。提案プロトコルは Dolev らにより提案されている方式の構成に用いていたのと同様の scheduler technique を用いている。Dolev らの方式では O(log n)ラウンド (ここで n は party identifiers の長さ) の interaction が必要であったのに対し、本結果では O(n)程度のラウンド数で実現できる。更に数論的仮定を置くと Cook の reduction technique を利用せずに実装可能なものがえられる。

The "Coefficients H" Technique [SAC 2008]

Jacques Patarin

係数 H の定義と、それが満たす5つの基本定理を示し、それらを使って関数の擬似ランダム性を証明したり、設計された暗号に対する攻撃見つけたりする手法を紹介した。係数 H 手法は 1990 に、Patarin、Gilbert、Vaudenay らによって導入され、擬似ランダム関数や擬似ランダム置換に関する証明に使われた。しかし、この手法を紹介する英語の文献はなかったので今回、自己完結的な論文として紹介する。m 個の平文・暗号文組$(a_i,b_i)(i=1,\ldots,m)$を全部満たす鍵の個数を H と定義し、H が満たす5個の不等式を導入する。これらの不等式を使い、Feistel 型暗号の各種攻撃に対する安全性を係数 H 手法で導いた。各種攻撃とは、既知平文攻撃、非適応的選択平文攻撃、適応的選択平文攻撃、選択平文・選択暗号文攻撃などである。

On Notions of Security for Deterministic Encryption, and Efficient Constructions without Random Oracles [CRYPTO 2008]

Alexandra Boldyreva, Serge Fehr, Adam O'Neill

確定暗号 (deterministic encryption) とは暗号化アルゴリズムが決定的 (deterministic) な公開鍵暗号のことである. 平文に対して暗号文が一意に決定されるので、暗号文をインデックスとするデータベースの中から、ある平文に対応するエントリーを高速に検索するような場合に使用する事ができる. Bellare ら(CRYPTO'07) は 確定公開鍵暗号 に対して, (PRIV と呼ばれる) "可能な最強の" 安全性概念を導

---

[6] 計算量の表記法。O(1)であれば、一定の計算量であることを意味し、O(n)であれば、パラメーターn に比例した計算量であることを表す。

[7] One-Way Function. ハッシュ関数のような一方向性関数。

入し，ランダムオラクル(RO)モデルで PRIV を満たす確定公開鍵暗号を構成した．本論文では効率的な確定暗号スキームをランダムオラクル無しで構成することに焦点を当てる．そのために，少し弱い安全性概念を考察した．この PRIV のバリエーションは 弱い定義ではあるものの，多くの現実的応用により適していると考えられる．それから，この定義と，より取扱いの易しい 単一メッセージで識別不可能性に基づいた（PRIV のバリエーションの）定義との等価性を示す．さらに CPA と CCA 安全な確定暗号スキームの両方の一般的な構成方法を示し，標準的な数論的仮定の下でのそれらの効率的な実現方法を示す．この構成方法は CCA-安全な確率暗号スキームを構成する為に最近導入された Peikert と Waters（STOC'08)のフレームワークに基づいており，それを確定暗号のセッティングに拡張したものである．

Deterministic Encryption: Definitional Equivalences and Constructions without Random Oracles [CRYPTO 2008]
Mihir Bellare, Marc Fischlin, Adam O'Neill, Thomas Ristenpart

本論文は確定公開鍵暗号に関する基礎的な研究に関するものであり，定義の等価性および一般的仮定に基づくスタンダードモデルでの構成を報告している．特に 強秘匿（semantic security）の 6 つの形式 および 1 つの識別不可能性（indistinguishability）の概念からなる 確定暗号に対する 7 つのプライバシー概念を調べ，すべて等価であることを示した．そして 落し戸付き一方向置換の存在のみに基づく（つまりスタンダードモデルで）一様で独立に分布したメッセージの安全な暗号化に対する確定スキームを提案する．さらに（必ずしも一様ではない）独立な高エントロピーのメッセージの安全な確定暗号を可能とする構成法の一般化を示す．最後に確定暗号と標準的な（ランダム化された)暗号の関係を示す．

Communication Complexity in Algebraic Two-Party Protocols [CRYPTO 2008]
Rafail Ostrovsky, William E. Skeith III

暗号学においては 強秘匿準同型暗号スキームからその準同型性をブラックボックス的に用いて 小さい通信量でいろいろな 2 パーティプロトコルを構成する膨大な研究成果がある．そうしたプリミティブの注目すべき例は単一データベースの Private Information Retrival（PIR）[15] や小さい通信量での private database update [5] が挙げられる．本論文では準同型暗号をブラックボックス的に用いてどのようなタイプのプロトコルが小さい通信量で実現可能かあるいは不可能かを決定する一般的方法論を説明する．この仕事は，少ない通信量で新しいプロトコルを開発しようとしている暗号研究者が既知の準同型暗号スキームのブラックボックス的利用による実現可能性を測る簡単な"リトマス試験"となる事を目論んでいる．さらに，本研究では そうした問題について推論するための厳密な数学的言語を開発した．本論文で通信量の下界を証明した代数構造のクラスは大きく，そして（双線形写像に基づくものを含む）実用的な全ての知られている強秘匿な準同型暗号系をカバーしている事を強調しておく．最後に群準同型暗号と、いわゆる完全準同型暗号系の設計に関する主要なオープン問題を関係づける次の等価性を示した．

> 「あらゆる有限非アーベル単純群上に準同型暗号が存在する時 および その時に限り(非零環上の)完全準同型暗号スキームが存在する.」

この結果は(有限非アーベル単純群を含むあらゆる群への）Barrington の結果[1] および Maurer と Rhodes の結果 [18] をいくらか一般化しており，そして Werner の 1974 年の結果[28] の構成的証明を実際に与えている．(また 2004 年に Rappe により提案され（その特殊な場合は証明され）たオープン問題 [23] への回答となっている)

Efficient Constructions of Composable Commitments and Zero-Knowledge Proofs [CRYPTO 2008]
Yevgeniy Dodis, Victor Shoup, Shabsi Walfish

Canetti ら [7] は最近 大域的セットアップの存在の元での 暗号プロトコルの並列実行を 適切に解析するために Generalized Universal Composability（GUC）と呼ばれる新しいフレームワークを提案した．そして，幾つかの自然なセットアップの元で，任意の 2 パーティまたはマルチパーティの 関数 を実現するのに十分な最初の GUC-安全なコミットメント（GUCC）および零知識証明（GUC ZK）の実現方

法を示した．しかしながらこのプロトコルは，任意の関数の実現可能性を示す為に設計されたものであり，その構成方法はかなり非効率的であった．
本論文では，データの消去を許す仮定の下で（適応的安全な）GUCC および GUC ZK の効率を劇的に改善した．すなわち，[7]と同じ最小のセットアップの仮定の元で，以下を行った．

- (NP 関係) R に対する直接的で効率的な定数ラウンドの GUC ZK を R に対する あらゆる"密な" Ω-プロトコル[21] から構築した．
- 系として，あらゆる R に対するΣ-プロトコルから（Cook-Levin 帰着を介さない）準-効率的な (GUC ZK の) 構成，および離散対数表現の知識証明の為の非常に効率的な GUC ZK を得た．
- 初めての定数レート(定数ラウンド) の GUCC スキームを構築した．

さらに，本論文はランダムオラクルを GUC フレームワークの魅力的な特徴である否認性(deniabilty) を失わずに GUC フレームワークの中で正しくモデル化する方法を示した．特に，ランダムオラクルを [7] で使われていたセットアップの仮定に付加することで初めての 2-ラウンド（最適ラウンド），否認可能，直接的 extract 可能およびシミュレーション可能な，あらゆる NP 関係 R に対する零知識証明を構成した．

A Framework for Efficient and Composable Oblivious Transfer [CRYPTO 2008]
Chris Peikert, Vinod Vaikuntanathan, Brent Waters

効率的で Universal Composable で DDH 仮定，平方剰余仮定，合成数剰余判定仮定，および 最悪ケース格子仮定を含むあらゆる標準的な数論的仮定の元で一般的に実現可能な紛失通信路(OT)を構成するための単純で一般的なフレームワークを提案する．この OT プロトコルはラウンド数最適（どちら向きも 1 メッセージ）で，計算量および通信量において極めて効率的で，同じ送信者および受信者間の無制限回の実行に対して 単一の共有文字列 (common string) が使用可能である．このプロトコルは単に共有文字列の分布を変えるだけで送信者または受信者のどちらかに統計的安全性を提供できる．具体的なプロトコルを得るには，一様ランダムな共有文字列で十分である．
本論文の鍵となる技術的貢献は，本論文でデュアルモード暗号系と呼ぶ抽象化である．さらに本論文で呼ぶところの"messy" public keys（"散らかった"公開鍵）を持ついくつかの暗号系を統一的に見ることによってデュアルモード暗号系を実現している．"messy" public keys とは，そういう公開鍵で暗号化された暗号文が平文に関する一切の情報を（統計的に）持たないということである．
また上記とは別の貢献として，時間および空間計算量がセキュリティパラメタ n の 1 次因子に比例する Regev らの格子に基づく暗号系(STOC 2005) を拡張して，複数ビットに分割された (amortized) バージョンを提供した．出来上がった 分割暗号化 (amortized encryption) および復号の時間はメッセージビット(1 ビット)につき たったの ¥tilde{O}(n) ビット演算のみで，暗号文長の増加は定数程度である．公開鍵の大きさと，それが基づく格子仮定は本質的に同じ大きさのままでよい．

Founding Cryptography on Oblivious Transfer -- Efficiently [CRYPTO 2008]
Yuval Ishai, Manoj Prabhankaran, Amit Sahai

本論文では，OT(紛失通信路)ハイブリッドモデルに於いて honest majority 下で安全な MPC (マルチパーティ計算)プロトコルをこの仮定が無くても安全なプロトコルに変換する単純で効率的な翻訳系を提案する．このテクニックは，honest majority で安全なプロトコル を この仮定無しで semi-honest な攻撃者にのみ安全なプロトコルと組み合わせる事によって機能する．いろいろなプロトコルのバリエーションに，この翻訳系を適用すると honest majority がなくとも安全な 2 パーティ計算や MPC に関する様々なアプリケーションが得られる．例えば

- OT ハイブリッドモデルでの 定数レート 2 パーティ 計算，
- OT の malicious model への拡張，
- honest majority が無い 定数ラウンド MPC のブラックボックス的構成

The Random Oracle Model and the Ideal Cipher Model are Equivalent [CRYPTO 2008]
Jean-Sébastien Coron, Jacques Patarin, Yannick Seurin

本論文は、Random Oracle Model と Ideal Cipher Model との等価性を証明し、Best Paper Award を受賞した。CRYPTO 2005 において、Coron らは、ランダムオラクルモデルで安全なスキームにおいてランダムオラクルをブロック暗号ベースの構成に置き換えてなお Ideal Cipher モデルで安全なスキームを得ることができることを示した。本論文では、Ideal Cipher モデルで安全なスキームにおいて Ideal Cipher を 6 段の Ruby-Rackoff 構成の関数に置き換え、その関数をランダムオラクルと見た場合に安全なスキームを得ることを示した。更に、5 段の場合に攻撃が存在することを示すことにより、6 段が最適であることを示した。

Programmable Hash Functions and Their Applications [CRYPTO 2008]

Dennis Hofheinz, Eike Kiltz

新たな情報理論プリミティブとして、programmable hash function(PHF)という概念を導入する。PHF は、ハッシュ関数の出力を離散対数問題のインスタンスをある確率で含むようにプログラムするのに使われる。ランダムオラクルモデルのセキュリティ証明に用いられるテクニックであるが、PHF のスタンダードモデルの実現を与える。PHF はそのプログラム可能性により、adaptive 攻撃を考慮したときに、暗号プロトコルのブラックボックス証明を与えるツールとなる。

One-Time Programs [CRYPTO 2008]

Shafi Goldwasser, Yael Tauman Kalai, Guy Rothblum

セキュリティアプリケーション向けに One-time プログラムという新たな計算パラダイムとなる概念を導入する。One-time プログラムは、実行時に値を指定できる単一の入力により実行され、入力に対する計算結果以外にはプログラムの情報は何も漏れないため、One-time プログラムは、一度だけ評価され自動的に破壊されるブラックボックス関数と見られる。One-time プログラムは、ソフトウェア保護など、プログラム obfuscation と同様の目的で用いられるが、更に一度しか実行できないという特性により、電子現金やトークンスキームに使うことができ、更に one-time 証明という新たな概念を生む。

Adaptive One-way Functions and Applications [CRYPTO 2008]

Omkant Pandey, Rafael Pass, and Vinod Vaikuntanathan

新しいクラスの計算量理論的困難仮定である Adaptive Hardness 仮定を導入する。これらの仮定はランダムオラクルの具体的な性質の抽象化であり、ここでの結果は、ランダムオラクルを必ずしも必要としない。Adaptive 一方向置換の族を仮定して、ブラックボックスセキュリティ証明を持つ、非対話 concurrently nonmalleable ストリングコミットメントを構成できることなどを示すことができる。

Metareduction Calculus : Intutionistic Tautologies and the Gap Diffie-Hellman Gap [ECC 2008 rump]

Dan Brown

(CDH⇒DDH)⇒(((DDH⇒CDH)⇒CDH)⇒DDH)
Reductionist の tautology かどうか教えて欲しいとのことである。

Basing PRFs on Constant-Query Weak PRFs: Minimizing Assumptions for Efficient Symmetric Cryptography [ASIACRYPT 2008]

Ueli Maurer and Stefano Tessaro (ETH Zurich, Switzerland)

あらゆる基本的秘密鍵暗号プリミティブが一方向関数(PRF)から導けることはよく知られている．そうしたプリミティブを構成できるより弱い仮定を見つける事は暗号学的に興味のある仕事である．この目的の為に，本論文では定数クエリ弱一方向関数(constant-query weak PRF) すなわち 秘密鍵を持ち，s が 2,3,4,… くらい小さいとし,既知ランダム入力が定数 s 回しか評価されないとき計算量的にランダム関数と区別がつかない関数の概念を導入する．そして constant-query weak PRF から (任意入力長) PRF を反復構成する方法を示す．この構成法はより強い仮定の弱一方向関数(多項式回の評価が許される)を用いる従来の構成方法よりも効率が良い．本論文の結果により IND-CPA 対称鍵暗号に対する効率的なモード (modes of operation)，反復 PRF，MAC，鍵固定のハッシュ関数に対する効率的なモード等が導かれる．

Sufficient Conditions for Intractability over Black-Box Groups: Generic Lower Bounds for Generalized DL and DH Problems [ASIACRYPT 2008]
Andy Rupp (Ruhr-University Bochum), Gregor Leander (Ruhr-University Bochum and Technical University of Denmark), Endre Bangerter (Bern University of Applied Sciences), Ahmad-Reza Sadeghi (Ruhr-University Bochum), and Alexander W. Dent (Royal Holloway, University of London)

generic group モデルは暗号学における数論的問題の計算量的困難さを解析するのに有用な方法論である．普遍的(generic)な困難性の証明は，多くの群に共通の性質を明らかにするが，未だにあらゆる新しい問題の計算量的困難性は一から証明されなくてはならず，その厳密解析はすぐに煩雑な仕事になってしまう．本論文は多項式関数によって表現できるあらゆる操作が攻撃者に許される拡張されたgeneric model の問題の困難性を保証する判定基準を与えることによって，この問題を克服するための最初のステップを構築する．

Towards Robust Computation on Encrypted data [ASIACRYPT 2008]
Manoj Prabhakaran, Mike Rosulek

暗号化されたデータに対する計算のセキュリティは、CPA 攻撃に対して安全であることしか示されていないなど限られたものが多い。本論文では、non-malleable 準同型暗号に関する最近の結果を適用することにより、active corruption に対して UC 安全な新しいプロトコルを構築する。更には、複数の暗号文を結合するオペレーションを扱えるように non-malleable 準同型暗号を拡張する。

5.3. その他 プロトコル

5.3.1. その他 プロトコル マルチパーティ

MPC vs. SFE: Perfect Security in a Unified Corruption Model [TCC2008]
Zuzana Beerliova-Trubiniova,Matthias Fitzi, Martin Hirt, Ueli Maurer and Vassilis Zikas

既存結果として、Crypto 2006 で Ishai らにより、active corrupt ion と passive corruption が混在するような閾値つき攻撃者が存在するようなプレイヤの集合に対して、SFE(Secure function evaluation，参加者が任意の合意された関数の下、それぞれの入力を用いて正しい出力が得られる一方、攻撃者は何の情報も得ることが出来ない)は構成可能であるが MPC(Multi-Party Computation)の構成は不可能であることが示されている。本発表では、上記の結果は perfect security の場合には成立しないことを示した。ここでは最も general に攻撃者を捉えた場合は、perfectly secure MPC は perfectly secure SFE から separate できることを示した。

MPC vs. SFE: Unconditional and Computational Security [ASIACRYPT 2008]
Martin Hirt, Ueli Maurer, and Vassilis Zikas (ETH Zurich, Switzerland)

インターネットのように多数の利害関係者が参加するようなネットワーク上で安全な対話計算を実行するには，参加者の何人かが攻撃者によって懐柔(corrupt)されているような状況を想定する必要がある．一般に，懐柔は，能動的懐柔(active)，受動的懐柔(passive)，不能的懐柔(fail)の 3 つに分類することができる．A,E,F をそれぞれ参加者集合の部分集合とし，A に含まれる参加者は能動的懐柔可能，E に含まれる参加者は受動的懐柔可能，F に含まれる参加者は不能的懐柔可能とし，3 つ組 (A,E,F) を懐柔の選択肢とすると，攻撃者の能力は懐柔の選択肢を列挙した，いわゆる攻撃構造によって特徴付けられる．本論文は，様々なモデルにおいて，一般の安全な関数評価(SFE)および安全な(動的)マルチパーティー計算(MPC)が，どの攻撃構造に対し可能であるかを論じ，SFE と MPC のセパレーションを与えている．

Scalable Multiparty Computation with Nearly Optimal Work and Resilience [CRYPTO 2008]

Ivan Damgård, Yuval Ishai, Mikkel Krøigaard, Jesper Buus Nielsen, Adam Smith

n プレイヤーが関数 f を計算するのに必要な計算量が、n に依存するが f の計算量には依存しない加算項を無視すれば n に関し対数多項式でしか増加しない、安全なマルチパーティ計算プロトコルを初めて示す。プロトコルは resilience の点においてほぼ最適であり、プレイヤーの(1/2- ε)と結託する active/adaptive な攻撃者に対して計算量的に安全である。

Cryptographic Complexity of Multi-party Computation Problems: Classifications and Separations [CRYPTO 2008]

Manoj Prabhakaran, Mike Rosulek

Universal Composition(UC)フレームワークにおける安全なマルチパーティ計算の計算量を研究する新しいツールを与える。一つは splittability という概念を導入し、通信チャネル機能の大きなクラスに関する UC フレームワークにおける実現性の特徴づけを行う。今一つは、制限された corruption 設定から標準的な悪意 corruption 設定へ実現可能性のセパレーションを持ち上げる効率的なテクニックである。これにより、splittability は比較的低い計算量機能のセパレーションを行うのに対し、後者のツールではより高い計算量機能のセパレーションが可能となる。

Efficient Secure Linear Algebra in the Presence of Covert or Computationally Unbounded Adversaries [CRYPTO 2008]

Payman Mohassel, Enav Weinreb

線形代数の問題に特化した安全なマルチパーティプロトコルの設計に関する研究．従来の方法は通信量が非効率であったか，攻撃者が semi-honest である仮定が必要であったが，本研究ではより現実的な 2 種類の攻撃者のセッティングに対し，それぞれプロトコルを設計している．1 つは，[Aumann and Lindell, TCC 2007] で導入された，covert adversary (潜伏攻撃者) のセッティングに対して安全性を達成するプロトコルである．covert とは要するに，不正を行おうとしてプロトコルを逸脱した者が、ある適当な確率でしか honest party に識別されないという事である．もう 1 つは，パーティの 1/3 以下をコントロールできる計算能力無制限の攻撃者の存在の下で，任意の悪意ある行動に対し安全性を達成するプロトコルである．(情報理論的なセッティング)．
本論文の主な結果は，上記の両方のセッティングにおいて t を定数として，分散共有された n×n 行列の正則性を判定する定数ラウンド (O(t)ラウンド) のプロトコルに対し，O(n^{2+1/t}) なる通信量の新しい上界を与えたことである (Theorem 5)．この正則性判定プロトコルを用いると，同じくらいの効率で 他の線形代数の問題，例えば分散共有された行列のランク計算や線形方程式系の求解などに関する安全なマルチパーティプロトコルを設計することができる．正則性判定問題を，行列の積の安全な計算に帰着させるため [Cramer, Kiltz, Padro, CRYPTO 2007] のアイディアと計算機代数の特異なテクニック (Toeplitz 行列) を使用している．
それから上記の両方のセッティングに対して行列の積を安全に計算する新しい効率的なプロトコルを設計した．two-party のセッティングでは，シミュレーションに基づく安全性を達成するため入力のランダム加法分解に関する cut-and-choose を準同型暗号スキームのランダムストリングの注意深い使用と組み合わせている．ジェネリックな零知識証明を避け，準同型暗号スキームをブラックボックス的に使用するだけでプロトコルを構成している．
スキームの構成はだいたい次の通り．線形代数の問題 → 一般行列の正則性判定 → Toeplitz 行列の正則性判定 → 行列の積の問題 → 行列の積のマルチパーティプロトコル．但し，Theorem 1,2,4 の詳細は full version を待てとのこと

Graph Design for Secure Multiparty Computation over Non-Abelian Groups [ASIACRYPT 2008]

Xiaoming Sun, Andrew Chi-Chih Yao and Christophe Tartary (Tsinghua University,China -all authors, Nanyang Technological University,Singapore-last author)

アーベル群を使った暗号プリミティブは量子計算機を用いると簡単に攻撃可能である．非アーベル群研究の暗号学的意義は量子計算機に対する耐性が期待できることであり，近年，非アーベル群を使った暗号研究が少しずつ増加してきている．Desmedt らは最近 非アーベル群上の安全なマルチパーティ計算を研究している．彼らは受動的攻撃者モデルを考え，参加者は有限群 G に関してブラックボッ

クス演算のみ許されると仮定し，参加者の入力の積を評価するマルチパーティ計算に関して，幾つかの結果を示した．本論文では，Desmedt らの結果を以下の2つの方向に拡張した．

- 浸透理論(percolation theory)を使って $\varepsilon > 0$ として任意の閾値 $t \leqq n/(2+\varepsilon)$ となる $O(n^3)$ の通信量を使う randomized algorithm を示した．マルチパーティ計算の分野で浸透理論が使われたのはこれが初めてとのこと．
- 多項式通信量，閾値 $O(n^{1-\varepsilon})$ の確定的構成法を明らかにした．さらに，各参加者が一個以上の入力を持つ場合のへ拡張．

5.3.2. その他 プロトコル 秘密分散

Public Verifiability from Pairings in Secret Sharing Schemes [SAC 2008]
Somayeh Heidarvand and Jorge L. Villar

ペアリングを利用して公開検証可能な秘密分散スキームを実現した。近年開発された暗号ツールは閾値暗号化や閾値署名など使われているが、秘密分散スキームには適用されてこなかった。この発表では、ペアリングを利用して秘密分散スキームを構成し、安全性評価のため、秘密情報の識別不可能性概念を定式化した。その結果、決定双線形自乗(DBS)仮定の下で、秘密情報識別不可能性が達成された。DBS は決定双線形 Diffie-Hellman 仮定の自然な変形の一つである。

Strongly Multiplicative and 3-Multiplicative Linear Secret Sharing Schemes [ASIACRYPT 2008]
Zhifang Zhang, Mulan Liu, Yeow Meng Chee, San Ling, Huaxiong Wang (Key Laboratory of Mathematics Mechanization, AMSS, CAS, China and Nanyang Technological University, Singapore)

線形秘密分散(LSSS)とは Shamir の秘密分散のように 2 つの分散値(share)から簡単に和の share が作れるような秘密分散のことである．2 つの share から積の share を作ることは一般にはそれほど単純ではないが，Cramer, Damgard, Maurer によって 2000 年にアクセス構造に含まれる参加者集合に関しては 2 つの share の積の線形結合が真の値の積となるような LSSS,即ち乗法的線形秘密分散(multiplicative LSSS) の概念が与えられた.アクセス構造に含まれない参加者集合にも上記が成立するような multiplicative LSSS を強乗法的線形秘密分散(strongly multiplicative LSSS)と呼ぶ．strongly multiplicative LSSS があれば情報理論的なシナリオにおいて適応的動的攻撃者に対して安全なエラーフリーのマルチパーティー計算が可能であり，攻撃者に懐柔(または買収)された参加者の share が誤りを含んでいる場合でも効率的な 秘密回復アルゴリズムを構成できることが分かっている．一般の LSSS から strongly multiplicative LSSS を構成する効率的な方法が存在するか否かは未解決問題である．本論文では，この未解決問題への 1 ステップとして，3-multiplicative LSSS の概念を提案し，strongly multiplicative LSSS との関係を明らかにした．さらに 3-multiplicative LSSS の無制限入力乗算への応用を示し対話計算量(round complexity)を 4 に削減した（従来の multiplicative LSSS ベースの方法では 5 であった）．また Reed-Muller 符号および代数幾何符号に基づく 2 つの 3-multiplicative LSSS の具体的構成法を示した．

5.3.3. その他 プロトコル データベース

A Linear Lower Bound on the Communication Complexity of Single-Server Private Information Retrieval [TCC2008]
Iftach Haitner, Jonathan J. Hoch and Gil Segev

一方向性置換(OWP; one way permutation) を用いて black-box により構成できる PIR(Private Information Retrieval) の communication complexity の下限に関する研究。サーバのデータベースのサイズ n に対して、従来の結果([HHRS], FOCS 2007)では $\Omega(n/\log n)$ が示されていたが、本結果では $\Omega(n)$ となることを示した。技術的には trapdoor permutation から black-box で構成する

statistically-hiding ビットコミットメントの下限の解析 を Haitner らにより FOCS 2007 で示された結果を用いて行い、また statistically-hiding ビットコミットメントからシングルサーバの PIR への帰着を考察することにより本結果を導き出している。

Distributed Private Data Analysis: Simultaneously Solving How and What [CRYPTO 2008]
Amos Beimel, Kobbi Nissim, Eran Omri

プライバシに関する分散計算の 2 つの研究分野である

- secure function evaluation (SFE) および
- differential privacy

の組み合わせに関する研究. どちらも個別の入力の集合に対する何らかの関数値を (入力)非公開のまま評価することを目的としてるが, プライバシの要求条件が決定的に異なる. SFE が一般に実現可能であるという結果は differential privacy の分散計算による実現への自然なパラダイム, つまり, まず 何を計算するか (例えば differential privacy の計算対象など) を選び, その後で どうやってそれを計算するか (例えばその計算の SFE プロトコルなど) を決定するパラダイム を示唆している.
本論文では, 計算対象とプロトコルの両方が同時に決定されるパラダイムが有利であるか否か調べ, このパラダイムの方が効率的で簡単なプロトコルを導出するという結果を導いた. 特に Binary Sum, Gap Threshold, Approximate Median を含むある関数族の計算に対して, 近似精度が どのくらい であればこのパラダイムが有益となるのか調べた. この結果によりプライベートデータ解析計算の局所モデルと大域モデルの間の新たなセパレーションが導かれた.

New Efficient Attacks on Statistical Disclosure Control Mechanisms [CRYPTO 2008]
Cynthia Dwork, Sergey Yekhanin

statistical database の目的はデータベース内の個々のレコードのプライバシを守ると同時に母集団に関する統計を提供することである. statistical database のプライバシとユーザビリティとの綱引きは近年統計, 理論計算機科学, セキュリティ, および データベースのコミュニティで多くの注目を引きつけている. Dinur と Nissim が始めた一連の研究によって ある特別な型のクエリに対して, プライバシの大きな侵害を防ぐために必要な歪みの下界が調査された. 本論文の第一の結果(Fourier Attack) は Dinur と Nissim の結果を単純化して明確にした. Dinur-Nissim スタイルの結果は あらゆる低歪みプライバシメカニズムの危険性を示しており, 強力である. その攻撃には all-or-nothing といった性質がある: 即ち n をデータベースのサイズとして, 何も学習しないまま先ず Ω(n) 個のクエリが作られ, その後いっきに Θ(n) ビットの秘密が暴かれる.
一方, 攻撃対象を十分広くて現実的な, ある低歪みメカニズムの部分集合に限定すると本論文の第二の結果 (Interpolation Attack) はもっと激しい攻撃となる. この攻撃は秘密の各ビットに対して 1 ビットの暴露につき定数個のクエリしか必要としない.

5.3.4. その他 プロトコル 放送用暗号

Efficient Simultaneous Broadcast [PKC2008]
Sebastian Faust and Emilia Kasper and Stefan Lucks

既存の同時暗号放送方式では、計算効率が低いゼロ知識証明が使われていたり、ランダム・オラクルモデルを安全性の根拠としたりしていた。この発表では、ゼロ知識証明を使わず、決定 Diffie-Hellman 問題の困難性を利用したスタンダードモデルで安全性が保証される効率的な同時暗号放送方式を提案した。提案方式では参加者の半数より少ない数が不正者であったとしてもプロトコルを安全に実行することが出来る。技術的には Feldman の VSS(Verifiable Secret Sharing)を利用している。

Generalized Identify Based and Broadcast Encryption Schemes [ASIACRYPT 2008]
Dan Boneh and Mike Hamburg (Stanford University)

本論文は ID ベース暗号と同報用暗号(放送用暗号)を構成する普遍的なフレームワークを示す．特に様々なシステムに応用可能な空間暗号(spatial encryption)なる普遍的な暗号の構成を示す．本構成法を用いると，秘密鍵のサイズは系の複雑さに応じて大きくなるが，暗号文のサイズはユーザー数と独立で，たった3つの群要素のみで構成できるようになる．この結果の応用として，初めての固定暗号文長同報用階層型 ID ベース暗号を与える．同報用階層型 ID ベース暗号は，ID ベース暗号電子メールにて，送信相手がどんな PKG (private key generator) を使っているか分からない場合に，ありうるどの PKG を利用しても復号できる暗号文を構成するのに利用できる．従来，この用途では PKG の数に比例して暗号文が大きくなる問題があったが，今回の結果はこの問題を解決する．

5.3.5. その他 プロトコル その他

Cryptographic Test Correction [PKC2008]

David Naccache (ENS Paris)

大学における二者択一の期末試験を採点することになった講演者が、採点の負荷を受験生に分担させるという問題意識を持ち、暗号学的な手法を用いて、採点結果を補正する方法を実施したという内容。受験生が与えられた手順に従って、回答が作る 01 パターンから修正用の数値を計算して答案用紙に記入させる方式であり、半分冗談のような話だったが、展開されている議論は本格的なものだった。

Dynamic Threshold Public-Key Encryption [CRYPTO 2008]

Cécile Delerablée, David Pointcheval

本論文では，ある決められた数以上の特権メンバーが協力したときだけ暗号文を復号できる閾値付き公開鍵暗号の研究を行い，このプリミティブを動的なセッティングへと一般化している．すなわち，閾値付き公開鍵暗号を拡張して，あらゆるユーザーが動的に暗号文受信者候補としてシステムに参加でき，暗号文送信者は受信者の特権集合と閾値 t を,暗号文ごとに動的に設定できるようにした．まず，強頑健性 (strong robustness) の概念を含む形式的安全性モデルを与え，それから上記の動的性質をすべて達成し，双線形写像をもつ一般化 DH フレームワークに適した新しい非対話仮定の下 スタンダードモデルで強秘匿 (semantically secure) なスキームを提案する．このスキームは 特権集合および閾値が動的で暗号文がコンスタントサイズの初めての閾値付き公開鍵暗号であり，閾値付き放送用暗号などとも関連がある．

Collusion-Free Protocols in the Mediated Model [CRYPTO 2008]

Joël Alwen, Abhi Shelat, Ivan Visconti

無結託(collusion-free)プロトコルに対する従来のアプローチ [14,15] は特殊な物理的通信路を必要としていた．本論文では (通信路も懐柔(corrupt)可能な参加者と見なす) 概念的に新しいアプローチを取ることによって，よりディジタル通信向きな通信路を使う事ができるようになった．本論文では通信路上のメッセージをフィルタおよび再ランダム化出来る通信路を考え，この新しいセッティングにおいて無結託性の特徴を捉えた新しい安全性の定義を与えた．このセッティングでは仲介人 (通信路) が corrupt されることさえ許す．この安全性の定義によれば，そうした仲介人 (通信路) が corrupt されていくような場合には，標準的なプライバシや正当性は段階的に失われていくという事になる．このより強い概念は他のいろいろなセッティングにおいても有用であろう．任意の関数評価が実行可能であることを示すため，この定義に合うようなコミットメントスキームと知識の零知識証明を構成している．

Ambiguous Optimistic Fair Exchange [ASIACRYPT 2008]

Qiong Huang, Guomin Yang, Duncan S. Wong (City University of Hong Kong) and Willy Susilo (University of Wollongong, Australia)

Optimistic Fair Exchange (OFE)は 2 者間(すなわち署名者と検証者の間)で署名や契約を公平に交換する問題を解くプロトコルである．正常系では 2 者間の対話のみでプロトコルが完了し，署名の持ち逃

げ等が発生した場合には調停者とよばれる TTP の助けを借りて問題の解決を行うことができる．既存の OFE では，プロトコル実行中に対話履歴の一部分を提示することで，検証者は署名者の署名意思を第三者に示すことが出来る．いくつかのシナリオ(オークションなど)では検証者のこのような能力は署名者に害をもたらす．この問題を解決するため，本論文では Ambiguous Optimistic Fair Exchange (A-OFE) の概念を提案し，マルチユーザー設定かつ選択鍵モデルの元で A-OFE の形式的安全性のモデルを示し，ランダムオラクル仮定に依存せず証明可能安全な効率的構成法を示した．

Compact Proofs of Retrievability [ASIACRYPT 2008]

Hovav Shacham (University of California at San Diego) and Brent Waters (University of Texas at Austin)

復元可能性証明(proof-of-retrievability)システムにおいては，データストレージセンターは実際にクライアントのデータを確かに所有していることを検証者に確信させなくてはならない．
この分野では証明可能安全で効率的なシステムの構築が大きな課題である．証明可能安全とは検証を通過するあらゆる証明者からクライアントのデータが抽出可能であることを意味している．本論文は Juels と Kaliski の最も強いモデルにおいて任意の攻撃者に対して安全性の完全な証明をもつ初めての proof-of-retrievability スキームを与えたとのこと．

Universally Composable Adaptive Oblivious Transfer [ASIACRYPT 2008]

Matthew Green and Susan Hohenberger (Johns Hopkins University)

k out of N OT(Oblivious Transfer)とは，送信者が N 個のメッセージを送信し，受信者がその内 k 個を選んで受信できる二者間のプロトコルである．送信者は受信者がどのメッセージを選んだのか知ることが出来ない．また受信者は選ばなかったメッセージの内容を知ることが出来ない．適応的(adaptive) OT とは受信者がどのメッセージを受信するかを適応的に(選んだメッセージの内容を確認しながら)決定できる OT のことである．適応的 OT は，マルチパーティ計算や非公開データベース暗号などへ応用が可能である．本論文は UC セッティングでの初めての通信量が定数の適応的 OT プロトコルの提案とのこと．

Noninteractive Statistical Zero-Knowledge Proofs for Lattice Problems [CRYPTO 2008]

Chris Peikert, Vinod Vaikuntanathan

最短独立ベクトル問題あるいは最短ベクトル問題の補問題のような格子の標準的近似問題の変種に対して非対話統計的零知識(NISZK)証明系を構築した．従来の格子問題の証明系は対話的であるか知識を漏らしているかのどちらか（またはその両方)であった．
本論文の系は 初めての 素因数分解と関係ない暗号学的な問題の NISZK 証明系であり，さらに，知識の証明であり，妥当な計算量を持ち，(適切な補助入力の下) 効率的な証明者アルゴリズムを一般に許す．さらに，それは，幾つかの暗号学的に重要な格子問題に対しては，初めての統計的零知識対話証明を意味している．
また，最短ベクトル問題に関係した ある特殊な選言命題 (例えば OR ゲート) に対する NISZK を構成した．これは，格子仮定に基づく NP の非対話(計算量的)零知識証明を構成するのに使えるかもしれない．

A Linked-List Approach to Cryptographically Secure Elections Using Instant Runoff Voting [ASIACRYPT 2008]

Jason Keller, Joe Kilian

既存の投票システムよりも、投票者の候補者ランキングリストを明かさないという意味でプライバシーを向上した、linked-list ベースの投票スキームを提案する。所謂 instant runoff 投票に焦点を当て、候補者リストが大きい場合にも、漸近的に効率の良いプロトコルを示す。

Efficient Protocols for Set Membership and Range Proofs [ASIACRYPT 2008]

Jan Camenisch (IBM Zurich Research Laboratory), Rafik Chaabouni (EPFL), Abhi Shelat

匿名信用保証もしくは電子現金の文脈において、ある集合もしくは数の範囲に属することを証明するた

めのコミットメントスキームが必要となる場合がある。RSA のような仮定に基づくスキームとは異なり、双線型群仮定に基づくスキームでは、セキュリティパラメータ k に対して、O(k)の群要素を証明者と検証者間で交換する必要があった。本論文では、交換群要素が O(k/(logk-loglogk))で済む双線型群仮定に基づくコミットメントスキームを示す。

5.4. その他 メッセージ認証コード

Fast and Secure CBC Type MAC Algorithms [FSE 2009]
Mridul Nandi

CBC-MAC の変形である2種類の MAC、GCBC1 と GCBC2 を提案し、他の CBC-MAC と比較した。CBC-MAC で鍵が1個だけなのは、OMAC(FIPS では CMAC)、GCBC1、GCBC2 の3種類である。また、メッセージを s ブロックとすると、暗号化回数は、OMAC が必ず s+1 回必要なのに対し、GCBC1/2 では s≧2 のとき s 回、s=1 では 2 回以下で済む。GCBC1/2 の構造的特徴は、最後から2つ目の暗号化の直後に、メッセージ・サイズに応じて、0～2 ビットの左シフトを入れる点である。

HBS: A Single-Key Mode of Operation for Deterministic Authenticated Encryption [FSE 2009]
Tetsu Iwata and Kan Yasuda

通常の認証付暗号化(AE)では nonce が用いられるが、同じ値を2回以上使ってはいけないという制約があり、正しく運用されず、安全性を損なう恐れがあった。この問題は、Rogaway-Shrimpton が EUROCRYPT 2006 で提案した決定論的 AE(DAE)である、ブロック暗号の SIV モードによって解決された。SIV モードでは、ベクトル化した CMAC を認証用に、カウンタ・モードを暗号用に使っているが、2個の鍵が必要だった。この発表では、鍵が1個で済む HBS モードを提案した。この方式のポイントは、次の3点である。

・鍵を K、ブロック暗号を E_K としたとき、ハッシュ用の鍵を $L=E_K(0^n)$とする
・ハッシュ値 S を、L のべき乗、ヘッダー・ブロック、メッセージ・ブロックを使った有限体上の乗算と加算で作る
・ハッシュ値 S をカウンタ・モードの入力オフセットとする

ヘッダー・ブロック数を h、メッセージ・ブロック数を m として、計算量を比較すると次のようになる。
ブロック暗号の計算回数は、SIV で h+2m+2 であるのが HBS では m+2 に減り、一方、SIV で不要だった有限体上の乗算が HBS では h+m+2 回必要になる。一般に有限体上の乗算は暗号化より非常に軽いので、計算量では HBS が有利と考えられる。
また、安全性を評価するため、VI- ε -AXU ハッシュ関数の概念を導入した。これは、ランダムなハッシュ鍵 L についての確率に関する条件、Pr[Hash_L(H,M)](+)Pr[Hash_L(H',M')=Y] ≦ ε を満足するハッシュ関数であり、暗号化関数 E_K が十分ランダムであれば、有限体上の乗算・加算を使った構成はこの条件を満たすと期待できる。

5.5. その他 乱数・疑似乱数

A Design for a Physical RNG with Robust Entropy Estimators [CHES2008]
Wolfgang Killmann, Werner Schindler

物理乱数生成器(PRNG)が生成する乱数の品質を評価するための確率モデルを定式化し、雑音が多い2つのダイオードを乱数源とした効率の良い PRNG に適用して解析を行った。多くの暗号方式で質の高い乱数が必要とされるが、理想的な乱数は現実には存在せず、現実的な解としては決定論的及び非決定論的 RNG の混合系が利用される。非決定論的 RNG の一つに PRNG があるが、その利用において生成する乱数の質をエントロピーの測定で評価する必要がある。この論文では、効果的にエントロピーを測定するシステムの具体例として、雑音が多い2つのダイオードを乱数源とした効率の良い RNG を対象として、確率モデルを定式化し、それに対する解析を行った。その結果、生成された乱数から、それ

が持つエントロピーのタイトな下限を与える定理を導出した。これを利用してオンラインの評価が可能になった。

Fast Digital TRNG based on Metastable Ring Oscillator [CHES2008]
Ihor Vasyltsov, Eduard Hambardzumyan, Young-Sik Kim, Bohdan Karpinskyy

準安定なリング振動子を利用した高速の物理乱数生成器を構成した。ディジタル回路で設計された物理乱数生成器(ディジタル RNG)では、ランダム性の源としてジッタが利用された。しかし、生成される乱数の質を維持するためには、振動子間の同期設定などのための回路が必要だったり、生成に先立つエントロピー測定のためジッタを一定量収集する時間が必要であった。この論文では、CMOS 上に実装した準安定なリング振動子の利用を試みた。その結果、準安定状態に至る時間が短く、スループットの高いディジタル RNG が出来た。AIS.31 や FIPS 140-1/2 の統計試験により、乱数の品質の高さが確認できた。

Bounds on Fixed Input/Output Length Post-Processing Functions for Biased Physical Random Number Generators [SAC 2008]
Kyohei Suzuki and Tetsu Iwata

互いに独立で一定の偏り ε を持つ物理乱数(ビット)列に対する後処理法の性能を解析した。暗号方式では質の高い乱数を要求するものが多い。物理乱数は候補となるが、生の値は必ずしも一様でないので、後処理が必要である。実用上、後処理の入出力ビットのサイズが一定のものが望ましい。また、同じ入出力ビットのとき、出力ビットの偏りがどこまで下がるかを調べることが未解決の問題としてあった。
出力ビットの偏りの下限を次のように定式化する。互いに独立で一定の偏り ε を持つ物理乱数(ビット)列に対する後処理として、入出力サイズが固定で、各々、n ビット、m ビットのものを考える。出力ビットの偏りを ε で展開した時の最小次数は後処理に依存するが、可能な後処理に対する最大値を deg(n,m)とする。deg(n,m)を 1≦m≦n≦16 の範囲で調べ、deg(n,m)に関するいくつかの定理を導き、また具体的計算法も示した。

Secure PRNGs from Specialized Polynomial Maps over Any GF_q [PQCrypto 2008]
Feng-Hao Liu, Chi-Jen Lu and Bo-Yin Yang.

Eurocrypt 2006 において、Berbain, Gilbert, Patarin らは、F2 上の多変数 2 次多項式の一方向性に関する仮定に基づいた擬似乱数生成 QUAD を発表したが、我々は一般の Fq 上に拡張することにより、2 倍の効率を持ち、ストレージを 1/10 にできる擬似乱数生成器を得た。

On the power of quantum encryption keys [PQCrypto 2008]
Christopher Portmann and Akinori Kawachi

ワンタイムパッドの量子アナロジーである量子状態のランダム化は、通常、古典秘密鍵 k に条件づけられた量子メッセージの変換から成る。古典秘密鍵の代わりに量子鍵状態 ρk を使用した暗号スキームを考察し、対称鍵スキームを非対称鍵スキームに拡張し、メッセージサイズおよび鍵コピー数の上限を見出した。

5.6. その他 実装解析

How to Secretly Extract Hidden Secret Keys: A State of the Attacks [PKC2008]
Jean-Jacques Quisquater (Universite' Catholique de Louvain)

実装された暗号に対するサイドチャネル攻撃に関する歴史と現在の研究を系統的に紹介した。1980 年台から数多くの実装攻撃が行なわれていたが、研究は不十分であり、また攻撃成功の成果を公開しないように圧力を受けた話が興味深かった。また、PKI での利用は注意するようにと警告した。最後に AES の鍵スケジュールに対する故障攻撃の成果を紹介し、NTT による結果より優れていることをアピールし

た。

Silicon-Level Solutions to counteract Passive and Active Attacks – invited paper [FDTC 2008]

Sylvain Guilley, Laurent Sauvage, Jean-Luc Danger, Nidhal Selmane, Renaud Pacalet

独自に開発した評価環境SecMatを使って、攻撃法や対策の比較を行った。サイドチャネル攻撃の有効性は実装環境に依存するが、従来、各研究者がばらばらに用意したものを使っているため、結果の有効性を直接比較することはできなかった。そこで、標準的な評価環境が必要とされていた。そこで、4 種類の ASIC、1 種類の FPGA で実装した標準評価環境 SecMat を開発した。4 種類の ASIC は v1,v2,v3,v3/2 で、v1～3 の 3 種類はスマートカードの国際規格 ISO/IEC 7816 に従い、v3/2 はいくつかのロジック・スタイルでの情報漏洩を評価するためのものである。FPGA は v3 と同じ機能を持つ。SecMat には DES と AES が実装されており、電力解析、電磁波解析、故障攻撃を行って、その有効性を比較を行った。

Improved Differential Fault Analysis on CLEFIA [FDTC 2008]

Junko Takahashi, Toshinori Fukunaga

CLEFIA に対する従来の差分故障攻撃(DFA)を改良し、より少ないデータで鍵の復元を可能にした。CLEFIA は 2007 年にソニーと名古屋大学が共同で開発したブロック暗号である。ICICS 2007 で H.Chen らが最初の CLEFIA に対する DFA を発表し、故障が有るときと無いときの測定データを 18 個用いて、鍵の復元に成功している。この発表では、測定データ数を削減するため、128 ビット鍵の CLEFIA は 18 段であるが、15 段目の拡散行列の前の部分に故障を起こし、それに対する暗号文と故障がないときの暗号文から鍵を効率的に復元するアルゴリズムを開発した。その結果、2 組の故障有る無しの組を利用して、128 ビット鍵の復元することに高い確率で成功した。この確率は鍵推定アルゴリズムを動かした時間に依存し、Xeon 3.0GHz の PC を利用した場合、1 分で 74.1%、1 時間で 98.1%だった。

Masking does not protect against Differential Fault Attacks [FDTC 2008]

Helena Handschuh, Arnaud Boscher

AES を例に、S-box の入出力にマスクを掛けるサイドチャネル攻撃対策が故障攻撃に対して有効でないことを実証した。ブロック暗号の DPA 対策としては、S-box の入出力にマスクを掛ける方法がしばしば用いられる。この対策を施した実装に対する攻撃として、AES の最終段の S-box 入力の直前で故障を起こした時の暗号文を集め、鍵を推定した。その結果、マスクがプール型でも有限体上の乗算型でも、故障攻撃を適用したとき、故障が起きたときの暗号文を注意深く 32 個選ぶと、鍵が復元できた。

Comparative Analysis of Robust Fault Attack Resistant Architectures for Public and Private Cryptosystems [FDTC 2008]

Konrad J. Kulikowski, Zhen Wang, Mark G. Karpovsky

AES を例に、高い故障検知性能を得るにはより大きなオーバーヘッドを伴い、非線形の誤り訂正符号は線形のものより性能が良いことを明らかにした。動的で適応的な故障攻撃は予想が困難なので防御が困難である。対策として故障検知を使うこととし、故障検知法の性能とオーバーヘッドとの関係を調べた。調べたのは、3種類の符号、robust; partially robust; minimum distance partially robust に、著者のオリジナルである minimum distance robust 符号を加えたものである。高い故障検知の確率を得るにはオーバーヘッドも大きくなるが、非線形符号の一つである minimum distance robust 符号の効率が良いという結果を得た。

A Practical Attack on Square and Multiply [FDTC 2008]

Jorn-Marc Schmidt, Christoph Herbst

確率的にカウンタをスキップさせる故障攻撃によって鍵の復元に成功した。RSA 暗号に対する攻撃は、CRT や square and multiply といった高速化手法に固有の性質を利用するものだが、高い精度で故障を引き起こす必要がある。そこで、別の故障の起こし方として、カウンタをスキップさせて計算結果を変える方法を試した。この故障は毎回確実に起こる必要はなく、確率的に起れば良い。この方法により、カウン

タのスキップは低コストで実現でき、鍵の復元に成功した。また、様々なサイドチャネル対策を施した回路にも適用したところ、それらのほとんどに対し、鍵の推定ができた。

Exploiting Hardware Performance Counters [FDTC 2008]
Leif Uhsadel, Andy Georges, Ingrid Verbauwhede

hardware performance counter(HPC)の出力をサイドチャネル情報として利用する攻撃の有効性を確認した。キャッシュ・タイミング攻撃は、キャッシュ・メモリの動作特性に注目したサイドチャネル攻撃の一種だが、通常、命令(セット)に対する処理時間を測定してサイドチャネル情報として利用する。しかし、処理時間の測定が可能な状況は限られている。そこで、サイドチャネル情報として HPC の出力に注目し、命令セットの処理時間を推定する方法を試みた。HPC は最近の x86 CPU を始めとする CPU で使われている。AMD Athlon XP で実験したところ、HPC の出力はサイドチャネルとして大きな可能性があることが確認できた。

A Generic Fault Countermeasure providing Data and Program Flow Integrity [FDTC 2008]
Marcel Medwed, Jorn-Marc Schmidt

故障攻撃に対する汎用の対策として出力の完全性を代数的にチェックする誤り検出を利用する方法を提案し、有効性を理論的に検証した。故障攻撃に対する対策は数多く提案されているが、そのほとんどが個別の攻撃法に特化したものであり、汎用の対策はほとんど提案されていない。そこで、汎用の対策として、暗号処理の代数構造に注目した誤り検出を行う方法を試みた。具体的には、暗号で素体 GF(p)上の計算が使われるとき、p と異なる素数 z を用意し、環 Z_{zp}とそのイデアルを利用した冗長表現を導入し、それで書き換えた。さらに、一連の命令にフィンガープリントを付ける。その結果、許容できるオーバーヘッドで故障検出が可能になった。故障が検出できる確率は 1-1/z である。また、命令に付加したフィンガープリントはマスクとして使えるため、漏えいするサイドチャネル情報を低下できる。

Aspects of the Development of Fault Resistant Hardware – invited paper [FDTC 2008]
Wieland Fischer

近年、サイドチャネル攻撃(SCA)や故障攻撃(FIA)の研究が目覚ましく進展する中、安全なハードウェアを設計するには、サイズや処理時間などの制約があり、適切な防御を行うことは困難である。そこで、どのような攻撃法とハードウェアのどの部分が攻撃対象となり得るかを調査し、安全性と信頼性のバランスを取るため CC 評価を活用することの有効性を説明した。

Fault-Tolerant ECC Unit using Parity preserving Logic Gates [FDTC 2008]
Julien Francq, Jean-Baptiste Rigaud, Pascal Manet, Assia Tria

楕円曲線暗号(ECC)に対する差分故障攻撃(DFA)対策として、borrow-save-adder に基づくパリティ保存論理ゲートを利用する方法を提案し、実験で有効性を検証した。ECC に対する DFA は大きな脅威となっている。有効な対策の一つは、計算結果の完全性をチェックすることだが、ECC では RSA 暗号と違って、最終結果の完全性をチェックするには、暗号化を2回行うか、2並列で行う必要がある。そこで、部分的な計算の完全性をチェックする方法が好まれる。ここでは、borrow-save-adder を使って設計したパリティ保存論理ゲートを利用して、誤りを検出する方法を採用した。C35 CORELIB technology で Design Vision tool を使って合成して実験した結果、故障は高い精度で検出できた。対策による面積と処理時間の増加率は各々 1.38と2.38 であり、処理時間のオーバーヘッドは小さくないが、パリティ保存論理ゲートなどの最適化を行うことにより削減は可能である。

On the Security of a Unified Countermeasure [FDTC 2008]
Marc Joye

ISPEC 2007 で Baek と Vasyltsov が提案した楕円曲線に対する実装攻撃(差分電力
攻撃や故障攻撃など)に対する統合的な対策が期待したほどの効果がないことを示した。楕円曲線暗号の中心となる演算の点乗算に対する実装攻撃として、差分電力攻撃と故障攻撃などが提案され、有効性が確認されている。ISPEC 2007 で Baek と Vasyltsov は、これらの実装攻撃に対する統合的な対策

を示した。素体 p の例だと、小さな整数 r をランダムに選び、冗長表現 Z_{pr} 上で点乗算の計算を行い、Z_r 上で計算結果の正当性を確認する。
この対策に対する攻撃法として、ランダムな整数 r の最大の素因数を q としたとき、楕円曲線上の点で $(X_d:Y_d:Z_d)\equiv(0:0:0) \pmod q$を満たすものを利用した。その結果、点乗算における故障検出は $2^{-|r/q|2}$ の確率で失敗することが理論的に導かれた。ここで、|*|2 は*のビット長である。この結果は、NIST の推奨曲線での計算機実験で確認した。また、計算におけるオーバーヘッドは、モジュラスが平均10数ビット長くなることである。

Fault Attack on Elliptic Curve with Montgomery Ladder Implementation [FDTC 2008]
Pierre-Alain Fouque, Reynald Lercier, Denis Real, Frederic Valette

楕円曲線上スカラー倍算のサイドチャネル攻撃対策であるモンゴメリ・ラダー法が、攻撃可能であることを計算機実験で示した。楕円曲線暗号の中心的演算である楕円曲線上のスカラー倍算のサイドチャネル攻撃に対する対策はいくつか提案されたがほとんどは破られた。しかし、y 座標を使わない場合のモンゴメリ・ラダーを使った防御法は唯一破られていなかった。この発表では、楕円曲線の twist に注目して攻撃法を構成した。その結果、理論評価で、n=160 で確率 2^{-32} で成功すると評価された。NIST や SECG が推奨するパラメータのいくつかで計算機実験を行うことで有効性を確認した。

Security against Fault Injection Attacks for CRT-RSA Implementations [FDTC 2008]
Alexandre Berzati, Cecile Canovas, Louis Goubin

FDTC 2005 で Ciet と joye が提案した CRT-RSA 実装に対する故障攻撃対策が不完全であることを理論的に示した。RSA の高速化法として CRT がしばしば利用されるが、Eurocrypt 2007 で Boneh らが故障攻撃で鍵が復元できることを示した。その後、多くの対策法が提案されたがほとんどは攻撃され、FDTC 2005 で Ciet と joye が提案した対策はまだ破られていなかった。この発表では、平文のハッシュ値をべき乗する際に誤りを導入するが、それ以降にハッシュ値を呼び出すときは誤りがないというタイプの故障を利用することにした。その結果、1024 ビットの CRT-RSA 署名に対する理論評価では、13 個の誤った署名があれば 50%以上の確率で秘密鍵指数が復元できる。誤った署名を 83 個に増やすと確率は 99%に上がる。

Attacks on Authentication and Signature Schemes involving Corruption of Public Key (Modulus) [FDTC 2008]
Michael Kara-Ivanov, Eran Iceland, Aviad Kipnis

モジュラスに挿入した誤りを利用する故障攻撃を ECDSA に適用し、理論的な有効性を示した。同様の方法は Gullou-Quiscater 暗号にも同様に適用できるが、攻撃に対する対策が容易に行える。従来の公開鍵暗号系に対する故障攻撃は、秘密鍵指数に誤りを挿入する方法が研究されてきた。最近、公開鍵指数に誤りを挿入する方法も研究されるようになり、CHES 2006 で Brier らが RSA に対してモジュラス n を壊す攻撃法を提案している。この発表では、モジュラス n が壊れた後の値を n_i としたとき、n_i がある範囲で一様に分布すると仮定して攻撃を組み立て適用した。その結果、短い鍵に対して、秘密鍵の全ビットが復元できた。

Attack and Improvement of a Secure S-box Calculation Based on the Fourier Transform [CHES2008]
Jean-Se'bastien Coron, Christophe Giraud, Emmanuel Prouff, Matthieu Rivain

フーリエ変換を利用してサイドチャネル攻撃(SCA)耐性を高めた S-box に対する攻撃法とともに、その攻撃に対する対策を提案した。ブロック暗号の DPA に対する防御法として S-box 出力にフーリエ変換を適用する方法が CHES 2006 で提案された。この論文では、1次の欠陥 R1・(Z⊕R1⊕R2)が Z の情報を漏らすことを利用する。ここで、Z は S-box 入力の波数空間値、R1 と R2 は各々入力と出力のマスク値である。この性質を利用した DPA の有効性は理論と実験で確認できた。また、この攻撃を無効にする S-box の対策として、a・Z をランダム変数 b でマスクする方法を提案した。ここで、a は入力の実空間値である。

Collision-based Power Analysis of Modular Exponentiation Using Chosen-message Pairs [CHES2008]
Naofumi Homma, Atsushi Miyamoto, Takafumi Aoki, Akashi Satoh, Adi Shamir

剰余指数演算を使った公開鍵暗号系に対する単純電力解析(SPA)をより一般化した攻撃を構成し、有効性を計算機実験で確認した。剰余指数演算を使った公開鍵暗号系では演算の高速化法の特徴を利用して、2つの平文(入力指数)を使った攻撃法が知られている。入力指数の一つを N としたとき、他方を N-1 とする方法と 2*N とする方法の2つが提案されている。しかし、これらは left-to-right 法にしか適用できないという制約があった。そこで、2つのメッセージを Y、Z としたとき、$Y^{\alpha}=Z^{\beta}$の形に一般化し、適切な制約条件を導入する方法を開発した。その結果、left-to-right 法だけでなく、right-to-left 法や m-ary 法を使った実装に対しても攻撃が可能になった。

Multiple-Differential Side-Channel Collision Attacks on AES [CHES2008]

Andrey Bogdanov

サイドチャネル攻撃の一つである衝突攻撃の効率を向上する方法として、2者投票と3者投票を提案し、理論・計算機実験の両方で有効性を検証した。サイドチャネル攻撃の一種である、異なる2つの S-box 入力が同じ(衝突)か否かを利用する衝突攻撃が盛んに研究されている。ここでは、2つの S-box に対する波形を比較して異同を判断するが、ノイズの影響を除去するため、各々の波形を単純に平均化する方法が用いられてきた。
この論文では、2者投票と3者投票を利用して攻撃の効率を改善することを試みた。2者投票とは、個々の測定ごとに2つの S-box に対する波形の異同を判断し、多数派となった判断結果を採用する方法である。3者投票も個々の測定ごとに判断し、多数派の判断結果を採用する点は同じだが、2つの S-box に対する波形を直接比較するのではなく、予め用意した参照用の S-box 波形の集合と比較し、2者が参照用波形の一つと同時に同じと判断したときだけ衝突が起きたと判断する方法である。
実験の結果、2種類の提案法は単純な平均法より少ない測定で正しい判定ができることが確認できた。3者投票は事前測定などの手間はかかるが、最もより少ない測定数で正しく判断でき、従来 163 から 6912 回必要だったのが、6 回に削減できた。

High-performance Concurrent Error Detection Scheme for AES Hardware [CHES2008]

Akashi Satoh, Takeshi Sugawara, Naofumi Homma, Takafumi Aoki

AES の暗号化と同時に計算誤り検出を行う高効率の実装法を提案し、実験で有効性を確認した。故障注入攻撃対策として計算と同時に誤り検出を行う防御法があるが、ハードウェア性能の低下が極力小さい方式が望まれる。
この論文では、AES の段関数を2つに分割し、一方を暗号化用、他方を誤り検出用に利用する方法を試みた。90-nm CMOS で実装したところ、対策なしの小型と高速実装が各々 1.66 Gbps @ 12.9 Kgates、4.22 Gbps @ 30.7 Kgates なのに対し、対策を施した場合は各々、2.21 Gbps @ 16.1 Kgates、3.21 Gbps @ 24.1 Kgates だった。サイズと速度で最適化した場合、対策による性能の低下は最大で 14.5%となった。

A Lightweight Concurrent Fault Detection Scheme for the AES S-boxes Using Normal Basis [CHES2008]

Mehran Mozaffari-Kermani, Arash Reyhani-Masoleh

AES の暗号化と同時に計算誤り検出を行う高効率の実装法を提案し、実験で有効性を確認した。AES の計算で唯一の非線形要素は S-box である。S-box 計算の効率的計算法として、S-box の主要部である GF(2^8)上の逆元計算を代数的に表現する方法がある。この性質を利用して故障検出を行う方法を検討した。具体的には、S-box 計算に正規基底上の混合表現を利用する方法と多項式表現の2種類を試し、誤り検出にはパリティ・チェックを利用した。その結果、正規基底上の混合表現の効率が良く、誤り検出のオーバーヘッドは面積で約 35%だった。

RSA with CRT: A New Cost-Effective Solution to Thwart Fault Attacks [CHES2008]

David Vigilant

リソースの限られた組み込み系でも有効な、CRT を使った RSA 署名に対する故障攻撃への防御法を実現した。CRT を使った RSA に対する Bellcore 攻撃に対する防御法は提案されてきたが、組み込み系の

ようにリソースの制約を考えると実用的なものはなかった。
この論文では、モジュロ N のべき乗剰余計算をモジュロ NR の計算を使って実行する方法を試みた。ここで、RはNと互いに素となる整数で、ビット長を適切に設定した中でランダムに選ぶ。その結果、実行時間、メモリ消費、個人利用、コードサイズといった制約の下でも有効な、RSA-CRT 署名に対する防御法が実現できた。解析はしてないが、サイドチャネル対策としても有効なはずとしている。

The Carry Leakage on the Randomized Exponent Countermeasure [CHES2008]
Pierre-Alain Fouque, Denis Re'al, Fre'de'ric Valette, Mhamed Drissi

べき指数をランダム化する DPA 対策に対する、キャリーに注目した攻撃法を開発した。Coron らは CHES 1999 で、楕円曲線上演算の DPA 対策として、秘密のべき指数や秘密のスカラーにφ(N)の倍数を加えることでランダム化する防御法を提案した。CHES 2003 で Fouque らは、この対策に対する doubling 攻撃を提案したが、同じ平文を繰り返し入力できるといった条件を満たす必要があった。
この論文では、秘密指数をランダム化ために用いるl-ビット加算で生じるキャリーに注目した攻撃法を開発した。Actel の ProAsic3/E スタータ・キット(FPGA)上に 160-ビット・マスク対策した ECC に対し、電磁解析を用いて攻撃したところ、キャリーによる輻射が観測でき、秘密べき指数の復元には曲線 10,000 個で十分だった。

Recovering Secret Keys from Weak Side Channel Traces of Differing Lengths [CHES2008]
Colin D. Walter

べき指数をランダム化するサイドチャネル対策に対する隠れマルコフ・モデルを利用した効果的な攻撃法を提案した。RSA 暗号や楕円曲線暗号(ECC)のサイドチャネル攻撃対策にべき指数をランダム化する方法がある。この対策に対する攻撃法に、CHES 2003 で Karlov と Wagner が提案した隠れマルコフ・モデル(HMM)を利用する方法があるが、計算量が大きくなり、満足できるものでなかった。この論文では、トレース全体を計算するのではなく数ビットの区間に限った処理を行うとともに、いくつかの注目すべきビットを事前に固定する方法を試みた。計算機実験の結果、鍵推定の有効性を確認した。また、どの結果に数ビットの誤りが含まれるか、また、誤るとしたらどの位置かを推定することも可能になった。

Attacking State-of-the-Art Software Countermeasures – A Case Study for AES [CHES2008]
Stefan Tillich, Christoph Herbst

ソフトウェア実装におけるサイドチャネル対策に対する最近開発された DPA を、プログラム可能なスマートカードに実装した AES に適用し、有効性を確認した。暗号のソフトウェア実装におけるサイドチャネル攻撃対策として、全要素にマスクを掛け、最初と最後にだけ操作順序の入れ替えとダミー操作を行う防御法がしばしば利用される。このような防御法に対する攻撃法を ACNS 2007 で Tillich らが提案したが、実際の攻撃実験は行われていなかった。この論文では、次の3種類の攻撃法を適用した。(1)マスクのハミング重みに従って攻撃に使用するトレースを選択した後、1 次 DPA を適用; (2) 入力と各点の間の 2 次 DPA を行った後、足し合わせる(windowing); (3) (2)と逆に windowing の後に 2 次 DPA を行う。実験対象は、ATMega163 コアに実装された、上記対策を施した AES である。実験の結果、(1)で 300,000 トレース、(2)で 65,000 トレースで正しい鍵が推定できたが、(3)では正しい推定ができなかった。

Power and Fault Analysis Resistance in Hardware through Dynamic Reconfiguration. [CHES2008]
Nele Mentens, Benedikt Gierlichs, Ingrid Verbauwhede(Katholieke Univ. Leuven)

動的再配置により物理的な攻撃に対する暗号システムのセキュリティを高めることができる。動的再配置により、ソフトウェアで実装では実現されている一連の物理攻撃対策をハードウェアにおいても実現できることを示し、更に、実行時に機能ブロックの物理的位置をランダムに変えることにより特に故障解析に耐性のある新たな種類の対策を導入する。また、またビットストリームの一部を再配置エリアから読み戻し、ブロック RAM に保存されたリファレンスコピーと比較することにより、故障を発見する対策を実現できる。

RFID and its Vulnerability to Faults. [CHES2008]
Michael Hutter, Jörn-Marc Schmidt, Thomas Plos(Graz 大学)

RFID タグに対する物理攻撃の実験を行った。HF 帯/UHF 帯で動作する複数ベンダの passive RFID タグに対して種々の物理攻撃実験を行った。アンテナ tearing、電磁波干渉、レーザーによる故障誘発実験を行い、特に内部メモリにデータを書き込む際の故障に弱いことが判明した。実験では、データを書かせないことや、誤った値を書き込ませることが可能であった。

Perturbating RSA Public Keys: an Improved Attack. [CHES2008]

Alexandre Berzati, Cecile Canovas(CEA-LETI/MINATEC), Louis Goubin(Versailles Saint-Quentin-en-Yvelines Univ.)

RSA 署名に対する新しい差分故障解析法を Right-To-Left アルゴリズムにおける 2 乗演算中に故障を起こすことにより、秘密鍵を取り出すことができる。l をウィンドウサイズ、n を公開鍵のビット長とすると、攻撃の計算量は、$O(n^2 2^l (2^8-1)/8l)$となり、Bellcore 研究者らの EUROCRYPT97 の攻撃よりも小さく、l のサイズが十分に小さければ(例えば 1024 ビット RSA の場合 20 ビット以下)、Brier らの CHES2006 における攻撃の計算量よりも小さい。また、必要な故障の数は O(n/l)となり、これも Bellcore/Brier らよりも小さい。

Divided Backend Duplication Methodology for Balanced Dual Rail Routing [CHES2008]

Karthik Baddam and Mark Zwolinski(Univ. of Southampton)

DPA 対策のうちロジックレベルの対策として、各クロックにおける消費電力を一定にすることにより情報漏えいをなくす DRP(Dual Rail Precharge)スタイルがあるが、differntial ネットのルーティングバランスが取れていれば、DPA を防ぐことが示されている。ルーティングバランスを取るために、Divided Backend Duplication という手法を新たに導入し、ASIC および FPGA への実装により、その効果を確かめた。

Using Subspace-Based Template Attacks to Compare and Combine Power and Electromagnetic Information Leakages [CHES2008]

F.-X. Standaert(Univ. catholique de Louvain) and C. Archambeau(Univ. College London)

電力解析攻撃および電磁波解析攻撃の比較により、暗号チップの近接領域による測定が可能な場合には、電磁波解析攻撃の方が遥かに高い情報漏洩があることを示した。更にテンプレート攻撃における漏洩とレースの中から意味あるサンプルを取り出す良い手法として、LDA(Linear Discriminant Analysis)および PCA(Principal Component Analysis)を提案する。また、Hamming weight モデルなどの理想モデルにより電力/電磁波チャネルの情報漏洩を比較した。

Mutual Information Analysis A Generic Side-Channel Distinguisher [CHES2008]

Benedikt Gierlichs, Lejla Batina, Pim Tuyls, Bart Preneel(K.U.Leuven)

Standaert らのサイドチャネル漏洩モデルの refinement として、サイドチャネル攻撃における情報理論的 distinguisher のモデルを提案する。このモデルを用いることにより、新しいサイドチャネル攻撃を開発し、実験により効果を確かめた。

On the Exact Success Rate of Side Channel Analysis in the Gaussian Model [SAC 2008]

Matthieu Rivain

今日，サイドチャンネル攻撃はスマートカードのようなポータブルデバイスに組み込まれた暗号システムに対する最も強力な暗号解析技術の一つである．このような脅威に直面し，サイドチャンネル攻撃者とサイドチャンネル漏洩を与えた時，暗号システムに対して何が達成できるかを正確に決定する事が非常に重要となる．攻撃者の能力と漏洩の性質に従って，攻撃の成功確率を評価することにより，この問題に答えることができる．本論文では広く認められているガウシアン漏洩モデルの下でサイドチャンネル攻撃の成功確率を評価する問題を研究した．そして，このモデルで攻撃の成功確率を効率的に計算できる新しいアプローチを紹介し，それを 2 つの代表的なサイドチャンネル解析のファミリー（すなわち差分サイドチャンネル解析およびプロファイリングサイドチャンネル解析）に適用した．

Distinguishing Multiplication and Squaring Operations [SAC 2008]

Fre'de'ric Amiel and Benoi^t Feix and Michael Tunstall and Claire Whelan and William P. Marnane

べき乗剰余算に対するサイドチャネル攻撃として、乗算と自乗算を電力消費波形の違いから識別した。RSA のようなべき乗剰余算を利用する暗号では、乗算と自乗算を識別することで秘密鍵情報を推定するサイドチャネル攻撃がある。2004 年に Chevallier らは、この攻撃に対する防御法として side channel atomicity という防御法を提案した。この発表では、乗算と自乗算ではハミング重みの統計的性質が異なり、電力波形に現れる性質を利用し、side channel atomicity で防御した実装に対しても乗算と自乗算を識別し、平文なしで鍵を推定することができた。

A Cache Timing Analysis of HC-256 [SAC 2008]
Erik Zenner

本論文では eStream winner のストリーム暗号 HC-128 の強化版である HC-256 へのキャッシュタイミング攻撃を示す．この攻撃はキャッシュタイミング攻撃のある抽象的なモデルに基づいている．このモデルはストリーム暗号のデザインにも利用することもできる．本研究では，この解析に対する観察から，キャッシュタイミング攻撃を困難にする暗号のデザイン原理を いくつか 導く．

Bug Attacks [CRYPTO 2008]
Eli Biham, Yaniv Carmeli(Technion), and Adi Shamir(Weizmann Inst. of Science)

LSI のバグを利用した攻撃の提案。RSA 暗号発明当時は遅くて誰も使ってくれず、ハードウェア化をせざるを得なかったが、自ら開発した LSI はバグがあって動かなかった経験から着想したもの。
例えば、答えが正しくない掛け算を一組知っているだけで大きなセキュリティ脅威となり得る。CRT を使った RSA 暗号において、C mod q のべき乗が正しくないとする。このときに得られる平文を m'、正しい平文を m とすれば、m=m'(mod p)、m!=m'(mod q)となり、gcd(m'-m,n)を計算することにより、p が求まる。これ以外にも、Pohlig-Hellman スキーム、CRT を使わない RSA、RSA-OAEP、楕円曲線暗号、Symmetric Primitive(IDEA,MARS,DFC,MultiSwap,Nimbus,RC6,Rabbit,UMAC)などに適用可能である。

Advances in Power Analysis Attacks [ECC 2008]
Elisabeth Oswald

電力解析攻撃に関するサーベイ。攻撃に必要な power trace が少なくてすむか多いか、また characterization が必要か否かにより、4 つのカテゴリーに分類・整理した。また、この分野の研究は広範囲にわたり、ばらばらに行われている傾向があるため、協力/競争のための試み 2 件を紹介し、参加を呼びかけた。1 件はサイドチャネル対策 chip 評価・作成プロジェクト SCARD、もう一件は、ECRYPT の VAMPIRE WG であり、日本の SASEBO ボード、文献整理 www.dpabook.org、ツールボックス OpenSCA、DPA contest(次回の CHES)などを紹介した。

Side Channels in the McEliece PKC [PQCrypto 2008]
Falko Strenzke, H. Gregor Molter, Raphael Overbeck, Abdulhadi Shoufan and Erik Tews.

McEliece 暗号に対して、タイミング攻撃の実験を行った。N=2、セキュリティパラメータ(m,t)=(11,50)において、48%の確率で、エラーベクトル e を特定することができた。対策としては、error locator polynomial の次数を t まで上げることが考えられる。

Cryptanalysis of a Generic Class of White-Box Implementations [SAC 2008]
Wil Michiels and Paul Gorissen and Henk D.L. Hollmann

substitution linear-transformation(SLT)暗号の white-box 実装に対する攻撃を検討した結果、線形変換がある種の条件を満たすとき、攻撃が成功することが分かった。white-box 実装とは、鍵情報を推定できないように工夫した暗号のソフトウェア実装であり、SAC 2002 などで Chow らが white-box 実装の手法を提案し、DES と AES の実装例を提示した。それらの実装は破られたが、DES と AES の特徴を利用しているため、Chow らの実装手法が安全な white-box 実装となる SLT 暗号が実際に存在するかどうかは不明であった。

Chow らの方法を SLT 暗号に適用した実装に対し、拡散行列である線形変換行列が disjoint spanning block sets を持つ(MDS 行列はこの条件を満たす)と仮定して、攻撃を試みた。その結果、拡散行列が disjoint spanning block sets を持つとき、SLT 暗号を Chow らの手法による white-box 実装から鍵を推定することが可能であった。実際に、AES と Serpent に対する攻撃を試みることで有効性を確認した。

A white box implementation of ECC [ECC 2008 rump]
Arthur Jackson

Key decomposition に関する話題。

5.7. その他 その他

Efficient Helper Data Key Extractor on FPGAs [CHES2008]
Christoph Boesch, Jorge Guajardo, Ahmad-Reza Sadeghi, Jamshid Shokrollahi, Pim Tuyls

物理的に複製できない関数(PUF)を実装することにより、FPGA IP 保護に必要な要素を実現した。PUF はセキュリティの応用上魅力的であり、FPGA の IP 保護に重大な役割を果たすと考えられている。PUF を利用する上で不可欠なのは、ノイズが多く一様でない応答から大きいエントロピーを持つ鍵を生成する fuzzy extractor である。fuzzy extractor の実現法として BCH 符号のような誤り訂正符号を単純に適用する方法が提案されているが計算コストが大きくなる問題点があった。この論文では、複数の誤り訂正符号を連接することによって効率的に長い符号を作る方法を試みた。その結果、実用的な fuzzy extractor が設計でき、FPGA IP 保護に必要でありながら今まで欠けていた機能が実現できた。

A Vision for Platform Security [CHES2008]
Ernie Brickell (Intel Corporation)

インテルが最近開発したセキュリティ・プラットホームを紹介した。不正なソフトウェアから PC を守るために CPU 内に信頼できる領域を設ける方法が近年広まってきたが、計算コストの増加を抑えるため、仮想化技術を利用して領域を極力小さくするという方針を示し、具体的構成例を示した。

Light-Weight Instruction Set Extensions for Bit-Sliced Cryptography [CHES 2008]
Philipp Grabher, Johann Großschädl, Dan Page

ビットスライス法実装の有利な点をすべて保ちつつ、かつ性能を向上できる軽量の、6 アドレス命令フォーマットを持つ 32 ビット RISC プロセッサの命令セット拡張(ISEs：Instruction Set Extensions)を記述する。DES、Serpent、AES、PRESENT、SHA-1、標数 3 有限体係数多項式の積などへの適用により、有効性を示した。

【Birds-of-a-Feather】セッション [CRYPTO 2008]

以下の2セッションが行われた。
- e-Voting
  IACR の理事投票を電子投票で行おうという動きがあり、システム提案などの議論が活発に行われる。
- IEEE P1619
  セキュアストレージ(ディスクの暗号化など)に関する規格の議論。

【ランプ】セッション [CRYPTO 2008]

・Awards
－フェロー：Ueli Maurer, Ralph Merkle, Moni Naor ら 3 氏が新たに IACR フェローとして選出された。
－Best Paper Award

``The Random Oracle Model and the Ideal Cipher Model are Equivalent"
Jean-Sebastien Coron, Jacques Patarin, Yannick Seurin
－T-shirt prize
T-shirt に印刷された暗号文を解読するパズルにおいて、正解者 5 名が発表された。
－ランプセッションチェア：Dan Bernstein(シカゴ Illinois 大学)
・Voting(4 件)
IACR のボード選挙を e-voting で行う計画があり、David Chaum、Ben Adida(Helios システム)、Yvo Desmedt らにより、システム提案等が行われた。
・Encryption Hardware(5 件)
普段は成功するはずの KeeLoq デモは再び失敗に終わった。その他 www.lightweightcrypto.org、MQQ(Multivariate Quadratic Quasigroups)公開鍵の紹介等が行われた。
・Foundations(3 件)
・公開鍵(5 件)
NTRUEncrypt 等の紹介が行われた。
・ 共通鍵(5 件)
暗号化ウィルス Gpcode のリバースエンジニアリングを行い、RSA と RC4 を使用して暗号化していることを確認した(Tromer)。ハッシュ関数の preimage 攻撃を行っており、SHA-3 コンテストの要件には preimage 攻撃耐性も含まれているので十分注意されたい(Sasaki)。COPACOBANA の紹介。
・公開鍵 proofs(7 件)
・上位レベルプロトコル(5 件)

Vingt-cinq ans après, with apologies to Alexandre Dumas [CRYPTO 2008]
Gilles Brassard

量子鍵配送プロトコル BB84 の発明者の一人である Brassard による情報理論的見地による一般的な解説が行われた。量子通信の利点・特徴もしくは研究の動機として、無条件安全であること、現在のテクノロジーで実現可能であること、商用利用も可能であること、活発に研究が行われている分野であること、そして何より楽しいことが挙げられた。

ECRYPT2 の開始 (2008/10/17)

欧州で2004年から4年間に渡って暗号研究プロジェクト"ECRYPT"が実施され、ストリーム暗号の公募・評価やハッシュ関数に対する攻撃などで大きな成果を上げた．この後継プロジェクトとして"ECRYPT2"が開始されるという情報が ISO/IEC SC27/WG 会合の第2日目に報告された．SC27/WG2 としては、直ちに行動は取らず、今後の推移を見守る方針で合意された。Alex Dent によればプロモーターは Bart Preneel で，コンタクト先も Preneel で良いとのこと．その他の情報は以下の通り．

Web 上で近いうちに情報が公開される
プロジェクトの期間は3年から5年で詳細は未定
ECRYPT の共通鍵、公開鍵、プロトコル、実装、電子透かしの5つの仮想ラボのうち、電子透かしを除く4つが継続の見込み
実装の仮想ラボでは、サイドチャネル攻撃もおそらくスコープに入る
Competition は行わない．
CRYPTREC からのコンタクトを歓迎する

P1363.3/D1 の Proxy Re-encryption に関して (2008/09/15)

IACR の ePrint に

On the Insecurity of Proxy Re-encryption from IBE to IBE in P1363.3/D1

なるタイトルの論文が発表され著者が

In this paper, we show that their proxy re-encryption scheme from IBE to IBE is not secure.

と主張し IEEE P1363 ML で物議を醸したが，安全性証明の問題ではなく，proxy re-encryption の定義が気に入らないという話の模様．Insecurity は明らかに大げさな言い方．定義の妥当性については専門家が議論し，新しい定義ができたら，proxy re-encryption とは別の名前をつけるのが良いとのこと．

http://eprint.iacr.org/2008/387

(追記: 上記論文は 2009/02/13 に withdraw された)

SHA-3 competition に関して (2008/10/31)

Federal Register / Vol. 72, No. 212 / Friday, November 2, 2007 / Notices によれば NIST の SHA-3 competition の submission deadline は 2008 年 10 月 31 日とのこと．詳細は以下を参照．

http://csrc.nist.gov/groups/ST/hash/documents/FR_Notice_Nov07.pdf

(追記: その後 64 件の応募があり，書類審査等を経て 51 件が受理された)

http://csrc.nist.gov/groups/ST/hash/sha-3/Round1/submissions_rnd1.html

A brief survey of Post-Quantum Cryptography. [PQCrypto 2008]
Daniel Bernstein,

量子計算機に耐性を持つ各暗号技術候補の先端動向。
－ハッシュベース署名
公開鍵、秘密署名鍵、署名等の基本形。Lamport-Diffie スキーム、Merkle 署名。
－符号ベース
基本スキームの例示による解説、1986 年の Niederreiter による McEliece オリジナル改良による鍵スペースの削減。
－多変数2次署名スキーム
基本スキームの解説、Patarin の HFE^{v-}(Hidden Field Equation, v:vinegar variables, -:publish する方程式数を 450 から 300 に削減)を絶賛。
－格子ベース
明日の Micciancio の講演に譲る。
耐量子計算暗号は現在でも使うことができるにもかかわらず、ただちに移行しない理由としては、以下のものが考えられる。これらに向けて研究を進めることが必要である。
－効率を改善する
－信頼性を確立する
－使い勝手を改善する
ベンチマークに関しては、以下のページが参考となる。
eBATS: ECRYPT benchmark of Asymmetric systems
eBACS: ECRYPT benchmark of Cryptographic Systems //bench.cr.yp.to

Computer Algebra and Cryptography [ASIACRYPT 2008]
John Cannon

講演者はシドニー大学教授であり数式処理システム Magma の開発者。計算機代数と暗号との密接な関係を示すテーマとして、有限体、格子、連立方程式、曲線の4つを取り上げた。
有限体については、$GF(p^k)$の演算、線型代数、多項式の因数分解、応用例として APN 関数の delta 2-rank の決定などの紹介があった。格子に関しては、LLL から L^2 にいたるまでの歴史や HKZ 間との階層、最近の Stehle の結果などが紹介された。方程式解法に関しては、Grobner 基底、Buchberger アルゴリズム、F4/F5、暗号への代数攻撃の話題が紹介された。曲線に関しては、楕円・超楕円曲線の位数計算のいくつかのアルゴリズムに関して言及された。
アルゴリズムを理論的に注意深く分析することがとても重要であり、アルゴリズムの振る舞いを深く把握し、

大きな進歩をもたらす。実際のところ数学アルゴリズムに関して多くのことはわかっていない。

6. ランプセッション等一覧

8th Algorithmic Number Theory Symposium ANTS-VIII
Monday, May 19, 2008

Last minute research announcements

Authors	Title
Steven Galbraith	*Faster ECC using an efficient endomorphism for general curves*
Daniel J. Bernstein and Tanja Lange	*The elliptic curve zoo: a study of curve shapes*
Igor Shparlinski	*Fermat quotients*
Henri Cohen	*Counting cubic extensions with given quadratic resolvent*
Noam Elkies	*The smallest "congruent number" curves of rank* 5

Posters

Authors	Title
Andrew Arnold and Michael Monagan, Simon Fraser University	*Calculating Really Big Cyclotomic Polynomials*
Kevin Doerksen, Simon Fraser University * * * Winner of the ANTS-VIII Best Poster Award * * *	*Genus 2 Curves With Split Jacobians*
Andrej Dujella, University of Zagreb	*A Variant of Wiener's Attack on RSA with Small Secret Exponent*
Frederic Edoukou, Institut de Mathématiques de Luminy	*Computing the 2-Distribution of Points on Hermitian Surfaces*
Noam Elkies, Harvard University	*Curves of Genus 2 With Many Rational Points Via K3 Surfaces*
Felix Fontein, University of Zürich	*Abstract Infrastructures of Unit Rank Two*
Sonal Jain, Courant Institute of Mathematical Sciences, New York University	*Minimal Heights and Regulators for Elliptic Surfaces*
Ahmad Lavasani and Reza Mohammadi Concordia University and Sharif University of Technology	*Implementing a Feasible Attack against ECC2K-130 Certicom Challenge*
Nathaniel W. Lindle and Joshua Holden Rose-Hulman Institute of Technology	*A Statistical Look at Maps of the Discrete Logarithm*
Richard Pinch, HMG	*The Carmichael Numbers up to* 10^{21}
Raminder Ruprai and Steven Galbraith	*Computing L-polynomials of Non-Hyperelliptic Genus 4 and 5 Curves*

Royal Holloway University of London	
Tanaka Satoru and Ken Nakamula, Tokyo Metropolitan University	*More Constructing Pairing-Friendly Elliptic Curves for Cryptography*
Sidi Mohamed Sedjelmaci, University of Paris-North	*A Straight Line Program Computing the Integer Greatest Common Divisor*
Masaya Yasuba, Fujitsu Laboratories Ltd.	*The Discrete Logarithm Problem on Elliptic Curves Defined Over* $\boldsymbol{Q}$

CHES 2008 Rump Session

A pousse-café of crypto,fun,URLs,RNGs,GPUs,and PUFs
Tuesday 12 August 21:30

Author	Affiliation	Title
Stefan Tillich	IAIK/TUGraz	10 Years of CHES – a not so serious review of some technical highlights
Ghaith Hammouri	CRIS/WPI	A PUF-based stream cipher
Laszlo Hars	Seagate Research	Notes on Metastable Random Number Generators
Jean-Jaques Quisquater	DICE/UCL	Why the Bellcore Attack is not working against an ENIGMA machine – part 1
Axel Poschmann	COSY/U Bochum	lightweightcrypto.org
Daniel J. Bernstein	CS/UIC	Latest GPU News
Tien-Ren Chen	Taiwan Nat'IU	
Chen-Mou Cheng		
Tanja Lange	EIPSI/TUE	
Bo-yin Yang	Academia Sinica	
Johann Grosschadl	CS/U Bristol	Micro-architectural countermeasures against side-channel attacks
Berk Sunar	CRIS/WPI	RNG FUD
Martin Novotny	COSY/U Bochum	Al Gore and NSA: A meeting in Heaven thanks to COPACOBANA
Fan Zhang	U Conn	Power Analysis Attacks on Hash Functions?
Jerry Shi	U Conn	
Sylvain Guilley	ENST/COMELEC	Side-channel Emanations Database
David Hwang	ECE/GMU	SHA-FPGA
Patrick Schaumont	ECE/VT	

Crypto 2008 rump session, Tuesday 19 August 2008

Awards

19:30 Bart Preneel (IACR Big Kahuna): New IACR Fellows Induction Ceremony
19:45 Daniel J. Bernstein (chair): Welcome to the rump session
19:46 David Wagner (chair of something else): CRYPTO 2008 Best Paper Award
19:49 Tony Stieber: A Modest Drawing of Chance
19:52 Susan Langford: Crypto 2008 t-shirt prize

Voting

19:55 John Kelsey, David Chaum, Tal Moran, Andrew Regenscheid: Scratch off attacks on end-to-end voting systems
20:01 David Chaum, Richard Carback, Jeremy Clark, Aleksander Essex, Stefan Popoveniuc, Ronald L. Rivest, Peter Y.A. Ryan, Emily Shen, Alan T. Sherman: Scantegrity II
20:06 Ben Adida Helios: web-based cryptographic voting
20:10 Jon Callas and Yvo Desmedt: A privacy preserving electronic submission process

Encryption hardware

20:15 Timo Kasper, Christof Paar: KeeLoq attack demo that usually work (or: Murphy's Law also holds at CRYPTO)
20:20 Krzysztof Pietrzak: How to do it right
20:24 Axel Poschmann: www.lightweightcrypto.org
20:25 Danilo Gligoroski, Smile Markovski, Svein Johan Knapskog: MQQ - A Public Key Block Cipher
20:30 Jean-Jacques Quisquater: Why the Bellcore attack is not working against an ENIGMA machine. Parts 1 and 2
20:35 Break

Foundations

20:55 Michael Backes, Markus Duermuth, and Dominique Unruh: Polynomially-secure crypto
20:59 Ueli Maurer and Stefano Tessaro: Efficient PRFs from Very Weak Assumptions
21:02 Jon Callas and Yvo Desmedt: Assumptions, assumptions(?), assumptions (??), ...

Stellar examples of public-key cryptography

21:07 Brandon Enright, Eric Rescorla, Stefan Savage, Hovav Shacham, Scott Yilek: insecure.iacr.org
21:14 Hal Finney: Looking Over Virtual Shoulders
21:18 Yanbin Pan, Yingpu Deng: Cryptanalysis of the Cai-Cusick Lattice-based Public-key Cryptosystem
21:23 Eric Rescorla, Stefan Savage, Hovav Shacham, Terence Spies: Paper Cryptography

Stellar examples of secret-key cryptography

21:30 Eran Tromer: Cryptanalysis of the Gpcode.ak ransomware virus
21:35 Yu Sasaki, Kazumaro Aoki: Attacks on MD, HAVAL, SHA, and Others
21:40 Elena Andreeva, Charles Bouillaguet, Orr Dunkelmann, Pierre-Alain Fouque, Jonathan J. Hoch, John Kelsey Adi Shamir, and Sebastien Zimmer: Trojan Message Attacks
21:47 Timo Kasper: Breaking Ciphers with Special Purpose Hardware
21:50 Break

Public-key proofs

22:10 Divesh Aggarwal and Ueli Maurer: Breaking RSA Generically is Equivalent to Factoring
22:15 Chris Peikert: Public-Key Encryption from the Worst-Case Shortest Vector Problem
22:20 Eike Kiltz, Krzysztof Pietrzak, Martijn Stam, Moti Yung: Randomness-Extractor Key-Derivation Approach to CCA2-Secure Hybrid Encryption
22:24 Peeter Laud: Computational soundness of formal encryption in the presence of key cycles, in the plain model
22:28 Alexandra Boldyreva, Vipul Goyal, Virendra Kumar: Identity-based Encryption with Efficient Revocation
22:31 Ali Bagherzandi, Jung-Hee Cheon, Stanislaw Jarecki: Multisignatures based on DL assumption
22:35 Michael Backes, Matthias Berg, Dominique Unruh: Formal Modelling of Cryptographic Games
Higher-level protocols
22:39 Tal Moran, Moni Naor and Gil Segev: An Optimally Fair Coin Toss
22:44 Manoj Prabhakaran & Mike Rosulek: Robust Protocols from Homomorphic-CCA Encryption
22:47 Juan Garay and Daniel Wichs and Hong-Sheng Zhou: Somewhat Non-committing Encryption and Adaptively Secure OT
22:51 Mira Belenkiy, Melissa Chase, Chris Erway, John Jannotti, Alptekin Küpçü, Anna Lysyanskaya: Incentivizing Outsourced Computation
22:55 Huijia Lin, Rafael Pass, Muthu Venkitasubramaniam: Unified Framework for Secure Multiparty Computation
23:00 Fin!

The 12th Workshop on Elliptic Curve Cryptography (ECC 2008)

Rump Session
Monday, September 22, 2008, Utrecht, The Netherlands

Authors	Title
Claus Diem	An update on ECDLP over extension fields
Dan Brown	Metareduction Calculus : Intutionistic Tautologies and the Gap Diffie-Hellman Gap
Richard Maloney	Division Polynomials for Twisted Edwards Curves
Dan Bernstein	DNSCurves
Chen-Mou Cheng, Tanja Lange	Elliptic Curve on GPU
Arthur Jackson	A white box implementation of ECC

Asiacrypt 2008 Rump Session Tuesday 9 December 2008

Time	Authors	Speaker	Title
7:30	Ed Dawson	Ed Dawson	Welcome from the chair
7:34	Xun Yi, Raylin Tso and Eiji Okamoto	Xun Yi	ID-Based Group Password-Authenticated Key Exchange
7:40	Tsutomu Matsumoto and Yoshio Takahashi	Tsutomu Matsumoto	Extracting RSA Private Keys from a Particular TPM Chip
7:46	Winfried B. Müller	Winfried B. Müller	Some Algebraic Properties of the RSA-Permutation Group
7:52	Francois Arnault, Thierry Berger, Cedric Lauradoux, Marine Minier, Benjamin Pousse	Benjamin Pousse	F-FCSRs are still alive
7:58	Damien Stehlé and Ron Steinfeld	Ron Steinfeld	Provable Trapdoor Signatures from Ideal Lattices (Work in Progress)
8:04	Adem Atalay, Orhun Kara and Ferhat Karakoc	Adem Atalay	Improved Cryptanalysis of SHAMATA-BC
8:10	George Lippold and James Birket	George Lippold	Key Agreement Protocols: in theory and practice
8:16	San Ling, Huaxiong Wang	San Ling	Asiacrypt 2010
8:18	Kaoru Kurosawa	Kaoru Kurosawa	ICITS 2009
8:20	Eiji Okamoto	Eiji Okamoto	Announcement of Asiacrypt 2009
8:22	Mathias Herrmann	Mathias Herrmann	Eurocrypt 2009
8:24	Juan Gonzalez	Juan Gonzalez	ACISP 2009
8:26	BREAK		
8:45	Daniel J. Bernstein and Tien-Ren Chen and Chen-Mou Cheng and Tanja Lange and Bo-Yin Yang	Chen-Mou Cheng	ECM on graphics cards
8:51	Daniel J. Bernstein and Tanja Lange	D. Bernstein	eBASH: ECRYPT Benchmarking of All Submitted Hashes
8:57	Minkyu Kim, Jung Hee Cheon, and Jin Hong	Minkyu Kim	Subset-Restricted Random Walks for the Pollard Rho Method
9:03	J Hughes	J Hughes	Massively Parallel General Purpose Machines
9:09	Bernard Colbert	Bernard Colbert	Cryptoiad
9:15	Ed Dawson	Ed Dawson	Closing remarks

FSE 2008 rump session, Tuesday 24 March 2009

Authors: Title

Sax and salsa

16:15 Bart Preneel: The International Association for Cryptologic Research

16:22 Orr Dunkelman: Presentation of Best Paper Award

Implementors

16:25 Emilia Käsper, Peter Schwabe: Fast Software Encryption: How Fast is AES?

Attackers

16:33 Sebastiaan Indesteege: Practical Preimages for Maraca

16:35 Jean-Philippe Aumasson, Willi Meier, Raphael Phan: Improved analysis of Threefish

16:39 Ralf-Philipp Weinmann: The ARX challenge

16:44 Dmitry Khovratovich: Nonrandomness of the 33-round MD6

16:49 Christophe De Cannière, Itai Dinur, and Adi Shamir: New Generic Attacks which are Faster than Exhaustive Search

16:54 Julia Borghoff, Gregor Leander, Lars R. Knudsen and Krystian Matusiewicz: Reducing 2^1740 to 2^54 or how to break C2

16:59 Sebastiaan Indesteege, Florian Mendel, Christian Rechberger, Martin Schlaeffer: Hullaballoo

Conference organizers

17:05 Marcelo Kaihara: CHES 2009

17:07 Mario Lamberger and Christian Rechberger: WEWoRC 2009

Defenders

17:08 Carmi Gressel, Nicolas T. Courtois, Avi Hecht & Gregory V. Bard: Hybrid Filter Diffuses 11 Disparate State Variables into 1 Binary State Variable in 1 Clock

17:14 Alla Levina: Block ciphers based on wavelet decomposition of splines

17:21 Carmi Gressel, Avi Hecht & Gregory V. Bard: Whitening 2 Last Hash Message with HAIFA Inspired Mersenne Prime LFSR Counters

17:26 Marina Pudovkina: On Impossible Truncated Differentials of Generalized Feistel and Skipjack Ciphers

17:31 Carmi Gressel and Avi Hecht: Precluding Message Modification with 2 32 Bit Orthogonal Feedback Streams

17:38 Fin!

詳細目次

発行日　2009年5月14日　第1版　第1刷
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
（情報通信セキュリティ研究センター セキュリティ基盤グループ）
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