CRYPTREC Report 2007

平成 20 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 2007 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。

2002 年度末に公表された電子政府推奨暗号リストは、2007 年度末で 5 年が経過し、その間、暗号技術を取り巻く状況は大きく変化してきた。これに対応していくためにも、一定期間毎に電子政府推奨暗号リストを見直していくことが望ましい。そのため、今年度は、内閣官房情報セキュリティセンター、総務省、経済産業省と連携を取り、電子政府推奨暗号リストの改訂に向けての準備を開始した。さらに、電子政府推奨暗号リストだけでは電子政府システムの構築時において暗号技術の選択基準が明確でないことから、利用の際の指針となるリストガイドを作成した。また、仕様書の参照先の変更を行うため、電子政府推奨暗号リストに掲載されている一部の暗号技術について安全性を検討した。

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章は今年度の監視活動、調査等の活動概要の報告である。第3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。

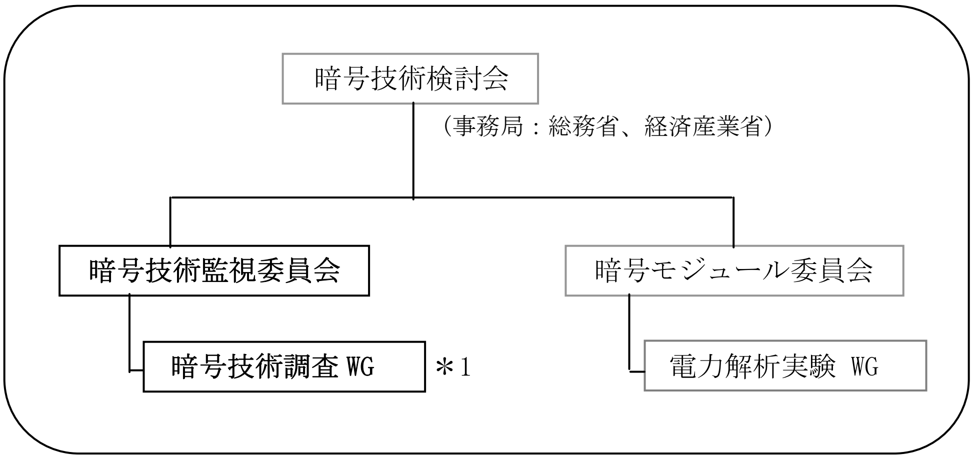
【問合せ先】　info@cryptrec.go.jp

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 19 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、「公開鍵暗号技術に関する安全性」及び「電子政府推奨暗号リストに関するガイドの作成」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) 公開鍵暗号技術に関する安全性の調査

2) 電子政府推奨暗号リストに関するガイドの作成

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	中央大学理工学部電気電子情報通信工学科教授
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	電気通信大学電気通信学部情報通信工学科教授
委員	金子 敏信	東京理科大学理工学部電気電子情報通信工学科教授
委員	佐々木 良一	東京電機大学未来科学部情報メディア学科教授
委員	松本 勉	横浜国立大学大学院環境情報研究院教授
委員	大塚 玲	(独)情報処理推進機構セキュリティセンター主任研究員
委員	田中 秀磨	(独)情報通信研究機構情報通信セキュリティ研究センター研究員
委員	山村 明弘	(独)情報通信研究機構情報通信セキュリティ研究センターグループリーダ
委員	渡辺 創	(独)産業技術総合研究所情報セキュリティ研究センター副研究センター長

暗号技術調査ワーキンググループ

委員	荒木 純道	東京工業大学大学院理工学研究科教授
委員	有田 正剛	情報セキュリティ大学院大学情報セキュリティ研究科教授
委員	小暮 淳	(株)富士通研究所 IT コア研究所主任研究員
委員	酒井 康行	三菱電機(株)情報技術総合研究所チームリーダ
委員	四方 順司	横浜国立大学大学院環境情報研究院准教授
委員	駒野 雄一	(株)東芝研究開発センター
委員	洲崎 誠一	(株)日立製作所システム開発研究所主任研究員
委員	藤岡 淳	日本電信電話(株)情報流通プラットフォーム研究所主幹研究員
委員	松崎 なつめ	松下電器産業(株)ネットワーク開発センターチームリーダ
委員	青木 和麻呂	日本電信電話(株)情報流通プラットフォーム研究所研究主任
委員	川村 信一	(株)東芝研究開発センター研究主幹
委員	香田 徹	九州大学大学院システム情報科学研究院教授
委員	古原 和邦	(独)産業技術総合研究所情報セキュリティ研究センター主幹研究員
委員	下山 武司	(株)富士通研究所 IT コア研究所研究員
委員	角尾 幸保	日本電気(株)インターネットシステム研究所主席研究員
委員	時田 俊雄	三菱電機(株)情報技術総合研究所チームリーダー
委員	古屋 聡一	(株)日立製作所システム開発研究所研究員
委員	森井 昌克	神戸大学大学院工学研究科教授
委員	廣瀬 勝一	福井大学大学院工学研究科准教授
委員	盛合 志帆	ソニー(株)情報技術研究所シニアリサーチャー
委員	内山 成憲	首都大学東京理工学研究科准教授
委員	宇根 正志	日本銀行金融研究所情報技術研究センター企画役

委員　　村上 哲　　　富士通(株)ソフトウェア事業本部
委員　　谷川 嘉伸　　(株)日立製作所システム開発研究所主任研究員
委員　　高橋 芳夫　　(株)NTT データ SI アーキテクチャ開発センタシニアエキスパート
委員　　國廣 昇　　　電気通信大学電気通信学部情報通信工学科准教授

オブザーバー

山田 繁夫　　内閣官房 情報セキュリティセンター
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
吉田 和彦　　警察庁 情報通信局
小松 聖　　　総務省 行政管理局
田中 敦仁　　総務省 自治行政局
中小路 昌弘　総務省 自治行政局
藤田 和重　　総務省 情報通信政策局[2007 年 7 月まで]
能登 治　　　総務省 情報通信政策局[2007 年 7 月まで]
網野 尚子　　総務省 情報通信政策局[2007 年 7 月まで]
荻原 直彦　　総務省 情報通信政策局[2007 年 7 月より]
川崎 光博　　総務省 情報通信政策局[2007 年 12 月まで]
増子 喬紀　　総務省 情報通信政策局[2007 年 12 月より]
山崎 浩史　　総務省 情報通信政策局[2007 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
太田 保光　　経済産業省 商務情報政策局[2007 年 5 月まで]
花田 高広　　経済産業省 商務情報政策局[2007 年 5 月より]
齊藤 文信　　防衛省 運用企画局
神藤 守　　　防衛省 陸上幕僚監部
滝澤 修　　　(独)情報通信研究機構
大蒔 和仁　　(独)産業技術総合研究所

事務局

(独)情報通信研究機構（篠田陽一、山村明弘、黒川貴司、松尾真一郎、松尾俊彦、中里純二、田村仁、金森祥子、村瀬一郎、中村豪一、牧野京子、赤井健一郎）
(独)情報処理推進機構（三角育生[2007 年 6 月まで]、山田安秀[2007 年 6 月から]、山岸篤弘、大熊建司、大久保美也子、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きたが、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認識されるようになってきた。

2006 年 2 月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」が決定された。同計画においては、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」こととされており、電子政府推奨暗号の監視等の機能は更に重要性を増している。

また、「第 1 次情報セキュリティ基本計画」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」こととされており、内閣官房情報セキュリティセンター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となっている。

CRYPTREC では、2005 年度には SHA-1 について、2006 年度には RSA の安全性に密接に関係する素因数分解問題についての安全性評価を行ったが、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、SHA-1 や RSA-1024 ビットについての安全性に関する見解等、CRYPTREC が発信する情報を踏まえて、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・選択する活動が平成１２年度から平成１４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。

そのため平成１５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研究動向を把握し、将来の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。

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１２年度版）は、次のURLから入手できる。

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

1.4 活動の方針

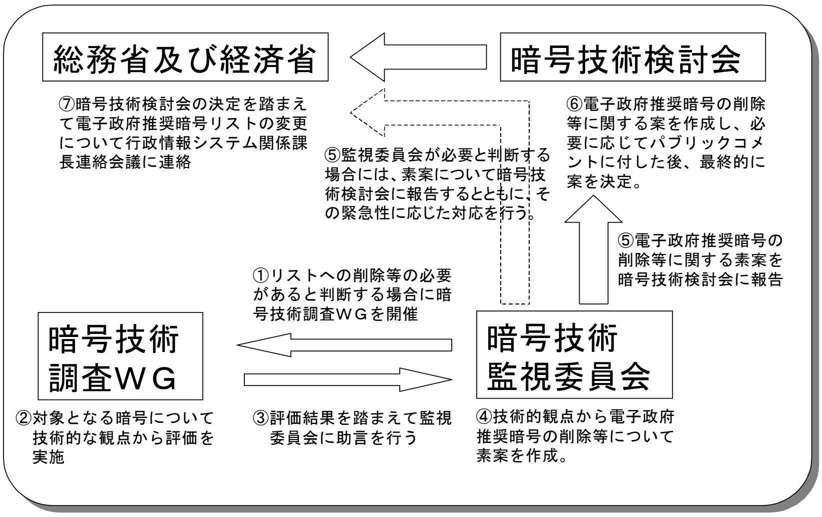
電子政府推奨暗号リスト掲載の暗号に関する研究動向を把握して、暗号技術の安全性について監視を行い、必要に応じて電子政府システムにおける暗号技術の情報収集と電子政府推奨暗号リストの改訂について暗号技術検討会(総務省・経済産業省)に対して助言を行

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



平成１９年度は、暗号モジュール試験及び認証制度（以下、JCMVP）の事務局から、電子政府推奨暗号リスト（以下、リスト）記載の暗号技術とJCMVPにおいて承認されたセキュリティ機能との間のうち、いくつかの差異についてJCMVPの要望を認めるよう検討依頼があったため、JCMVPの要請等に基づいて検討が必要となった暗号技術に関して、技術的検討を行った。

また、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[1]を作成した。

[1] 別冊の「電子政府推奨暗号の利用方法に関するガイドブック」を参照のこと。

第２章 監視活動

2.1.概要

平成 19 年度は、現在広く利用されているセキュリティに関する標準技術について、安全に利用するための指針を示すため、新規にリストガイドワーキンググループを組織した。また、平成 18 年度から組織されている公開鍵暗号ワーキンググループでは、暗号モジュール試験及び認証制度（以下、JCMVP）からの要請により、検討が必要となった暗号技術に関して安全性評価を実施した。各ワーキンググループ（WG）が活動した主要活動項目は、表 2.1 の通りである。

表 2.1　平成 19 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 技術対象となる標準技術についての調査・検討 ② 暗号アルゴリズムの選択についての検討 ③ セキュリティパラメータについての検討
公開鍵暗号 WG	太田和夫	① NIST SP 800-56A に関する DH 及び ECDH の安全性についての調査・検討 ② SECG SEC1 及び ANS X9.62 に関する ECDSA の安全性についての調査・検討 ③ PSEC-KEM に関する安全性についての調査・検討

2.2.監視活動報告

2.2.1. ハッシュ関数に関する安全性評価について

平成 19 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、ECRYPT Hash Workshop 2007 において、C. Canniere(グラーツ工科大)らが２ブロックメッセージに対して、SHA-1 の 70 段縮小版の衝突発見を発表している。また、Crypto 2007 において、A. Joux(DGA and Versailles University)らも、共通鍵暗号

への攻撃手法の一つであるブーメラン攻撃を応用し SHA-1 の 70 段縮小版の衝突発見を発表している。

また、Eurocrypt 2007 において、A.Lenstra らが、MD5 の衝突探索攻撃を応用して、X.509 の署名偽造に成功した事例を発表している。

さらに、メールなどの受信時の認証などとして用いられている、チャレンジレスポンス型で MD5 を利用した暗号プロトコル APOP に関しての解析結果が示された。理論的には 79 文字までは総当り攻撃よりも有効な解析が実行可能となることが示されている。

2.2.2. その他の暗号技術に関する安全性評価について

平成 19 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、Eurocrypt 2007 において、K. Aoki(NTT)らが特殊数体篩法(SNFS)を利用した、1039 ビットの合成数 $2^{1039}-1$ の素因数分解例を発表している。なお、特殊数体篩法は大部分の合成数に対して適用できないので、1024 ビット鍵の RSA 暗号の安全性が低下したわけではない。

2.2.3. 電子署名に関する技術的意見の提出について

2007 年度において、総務省、法務省及び経済産業省を事務局とする「電子署名及び認証業務に関する法律の施行状況に係る検討会」(以下「電子署名法検討会」という。)(座長：辻井　重男　情報セキュリティ大学院大学　学長）では、「電子署名に用いる暗号技術の安全性向上に係る方策」について検討を行っており、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、電子署名法検討会事務局に回答した。これらの報告等に基づき、電子署名及び認証業務に関する法律の施行状況に係る検討会報告書（案）に係る意見募集[1]が実施されている[注]。

2.2.4. 暗号技術標準化動向

NIST による次世代ハッシュ関数 SHA-3 の公募が 2007 年 11 月 2 日付けで開始された[2]。公募要領や安全性や実装性能で評価する方針が表明されている。

---

1 http://search.e-gov.go.jp/servlet/Public?BID=145207274

注 報告書の公表及び意見募集の結果については、
http://www.soumu.go.jp/s-news/2008/080530_4.html
を参照のこと。

2 http://csrc.nist.gov/groups/ST/hash/federal_register.html

2.3. 学会等参加記録

平成19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 2.11 に示す通りである。

表 2.11　国際会議への参加状況

学会名・会議名		開催国・都市	期間
TCC 2007	The fourth Theory of Cryptography Conference	アムステルダム（オランダ）	2 月 21 日～2 月 26 日
FSE 2007	The 14th Fast Software Encryption	ルクセンブルグ（ルクセンブルグ）	3 月 26 日～3 月 28 日
PKC 2007	The 10th International Workshop on Practice and Theory in Public Key Cryptography	北京（中国）	4 月 16 日～4 月 20 日
Eurocrypt 2007	26th International Conference on the Theory and Application of Cryptographic Techniques	バルセロナ（スペイン）	5 月 21 日～5 月 24 日
ECRYPT Hash Workshop 2007	ECRYPT Hash Workshop 2007	バルセロナ（スペイン）	5 月 24～5 月 25 日
SAC 2007	The 14th Annual Workshop on Selected Areas in Cryptography	オタワ（カナダ）	8 月 16～8 月 17 日
Crypto 2007	The 28th International Cryptology Conference	サンタバーバラ（米国）	8 月 19 日～8 月 23 日
ECRYPT / SHARCS 2007	Special-purpose Hardware for Attacking Cryptographic Systems	ウィーン（オーストリア）	9 月 9 日～9 月 10 日
FDTC 2007	4th Workshop on Fault Diagnosis and Tolerance in Cryptography	ウィーン（オーストリア）	9 月 10 日
CHES 2007	9th Workshop on Cryptographic Hardware and Embedded Systems	ウィーン（オーストリア）	9 月 11 日～9 月 13 日
ECRYPT / TFC	Tools for Cryptanalysis	クラクフ（ポーランド）	9 月 24 日～9 月 25 日
IEEE / FOCS 2007	48th Annual IEEE Symposium on Foundations Of Computer Science	プロヴィデンス（米国）	10 月 20 日～10 月 23 日

ProvSec 2007	International Conference on Provable Security 2007	ウロンゴン (オーストラリア)	11 月 1 日～ 11 月 2 日
Asiacrypt 2007	The 14th Annual International Conference on the Theory and Application of Cryptology & Information Security	クチン (マレーシア)	12 月 3 日～ 12 月 6 日
FSE 2008	The 15th Fast Software Encryption	ローザンヌ (スイス)	2 月 11 日～ 2 月 13 日
ECRYPT / SASC 2008	The State of the Art of Stream Ciphers IV	ローザンヌ (スイス)	2 月 13 日～ 2 月 14 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。

2.3.1. ハッシュ関数の解読技術

SHA-1 の衝突発見法の研究も段階的に進み、衝突発見可能段数はこれまでの 64 段から 70 段まで伸び、フルラウンド 80 段に近づいた。80 段に対する差分経路は分かっているので、グリッド計算機と分散 PC を合わせた衝突メッセージの発見プロジェクトも実施中である。[On the full cost collision search for SHA-1, C.De Canniere et al., ECRYPT Hash Workshop 2007;Dedicated Collision Search, C.Rechberger, SHARCS 2007] また、ブロック暗号用のブーメラン攻撃法を適用することで、70 段の衝突を発見している。この攻撃では差分経路は変えないものの、衝突発見の計算量を 1/30 に削減する方法も提案されている。[Hash Functions and the (Amplified) Boomerang Attack, A.Joux & T.Peyrin, Crypto 2007]

MD4 と MD5 に対しては衝突発見法の効率が非常に向上し、通常の PC でも短時間で実行可能となっている。第 2 原像計算も実行可能となり、それを利用した署名偽造も提案されている。[Full Key-Recovery Attacks on HMAC/NMAC-MD4 and NMAC-MD5, P.A.Fouque et al., Crypto 2007] さらに、MD4 では原像計算困難性も否定されるに至った。[MD4 is Not One-Way, G.Leurent, FSE 2008]

メールなどの受信時の認証などとして用いられている、チャレンジレスポンス型で MD5 を利用したプロトコル APOP に関しての解析結果が示された。G.Leurent らはプロトコルの中で用いているパスワードについて 3 文字まで現実的な時間内で推定可能であることを示した。更に、佐々木らは Chosen Challenge attack の環境下では 31 文字のパスワードは容易に解読可能であること、また現実的な環境下では約 1 時間に 1 文字の解読に成功、31 時間で 31 文字のパスワードの解読が可能であることを示している。この攻撃手法を用いる

と理論的には79文字までは総当り攻撃よりも有効な解析が実行可能となることを示した。[Message Freedom in MD4 and MD5 Collisions: Application to APOP, Gaetan Leurent, FSE 2007] [Extended APOP Password Recovery Attack, Yu Sasaki, Lei Wang, Kazuo Ohta and Noboru Kunihiro, FSE 2007 Rump session]

MD5の衝突耐性の不備を利用して、X.509に従った一対の署名が作れることを実例によって示した。2005年のACISPでLenstra-WagnerらによりMD5の脆弱性に起因するX.509で異なる署名が作成できることは示されていたが、当初は(結果として)同じユーザ(ID)に対して異なる公開鍵を持つような署名の生成に留まっていた為、実質的な脅威はそれほど大きくなかったが、本結果では異なるIDに対する署名が生成できることから実質的な脅威につながる結果であるといえる。技術的にはMD5への攻撃がより強力になり意図する任意の2つのIHVs(Intermediate Hash Values)に対する衝突発見が可能になったためである。この署名対を作るのに要する計算量はMD5の圧縮関数2^{52}回分であり、Eindhoven技術大学のクラスター計算機と分散PC(ボランティア1200名)を利用したHashClashプロジェクト(ピーク性能400GFlops)で合計6カ月掛かった。MD5の脆弱性を強く印象付ける結果である。[Chosen-prefix Collisions for MD5 and Colliding X.509 Certificates for Different Identities, Marc Stevens, Arjen Lenstra and Benne de Weger, Eurocrypt 2007]

2.3.2. ストリーム暗号の解読技術

GSMで利用されているA5/2に対する攻撃がいくつか提案されているが、実際に解こうとすると連立方程式解法のコストの大きさが問題になる。そこで0.18μロジックの専用ASICでGauss-Jordan法を実装したところ、事前計算無しで、約1秒で初期状態を復元することに成功した。[Hardware-Assisted Realtime Attack on A5/2 without Precomputations, A.Bogdanov et al., CHES 2007]

RC4は広く利用されているストリーム暗号の一つで、鍵セットアップ(KSA)の後、擬似乱数生成(PRGA)を行うという２段階の動作を行う。従来から、KSA後の状態に偏りがあることが知られ、それを利用した攻撃法が提案されてきたが、致命的ではないと考えられてきた。この発表では、鍵に関する情報に関わりなく、256番目及び257番目の出力バイトで、状態の偏りが最も大きくなる時刻を明らかにした。この偏りは、ランダムに選んだ1万個の暗号化鍵に対し、148個で現れる。[New Form of Permutation Bias and Secret Key Leakage in Keystream Bytesof RC4, S.Maitra & G.Paul, FSE 2008]

2.3.3. ブロック暗号の解読技術

AESに対するSQUARE攻撃の手法を応用して5段の識別子を作り、それを利用した中間一致攻撃が提案された。この攻撃によって、192ビット鍵AESで7段まで、256ビット鍵AES

で８段まで解読可能であることが示された。[A Meet-in-the-Middle Attack on 8-Round AES, H.Demirci & A.A.Selcuk, FSE 2008]

SQUARE 攻撃を一般化した Integral 攻撃は AES のような SPN 型に対して有効であることが知られているが、S-box のサイズを単位とするのが基本となっている。しかし、ビット・パターンに着目したビット単位の積分攻撃も可能である。ビット単位の Integral 攻撃をブロック暗号に適用したところ、AES の設計者が設計した Noekeon で５段まで、AES 最終５候補の一つの Serpent で５段まで、CHES 2007 で小型実装用に提案された PRESENT で７段まで解読可能であることが分かった。[Bit-Pattern Based Integral Attack, M.R.Zaba et al., FSE 2008]

自動車のキーレス・エントリで実際に使われている 64 ビット・ブロック暗号 KeeLoq は、非線形 FSR を利用した設計で、既に攻撃法がいくつか発表されていたが、既知平文が 2^{32} 個も必要である点で現実的でなかった。スライド攻撃と代数攻撃を組み合わせることで、既知平文 2^{16} 個で解読できた。現実的な脅威につながる可能性が高まった。[Algebraic and Slide Attacks on KeeLoq, N.T.Courtois et al., FSE 2008]

非対称 Feistel 暗号に対する汎用の攻撃法として C.S.Jutla が Crypto 1998 で提案した一般化バースデイ攻撃があるが、Integral 攻撃の考え方を応用することでより効率の良い解読法が実現できた。[Generic Attacks on Unbalanced Feistel Schemes with Expanding Functions, J.Patarin, Asiacrypt 2007]

2.3.4. 公開鍵暗号の解読技術

SFLASH は、2003 年に NESSIE で選ばれた多変数２次連立方程式に基づくディジタル署名方式で、スマートカードのような低リソースの環境での利用に向いている。Eurocrypt 2007 で、SFLASHv2 のパラメータを変更すると攻撃できる公開鍵の差分を利用した攻撃法が発表され、更に Crypto 2007 では極座標形式(polar form)を利用することで連立方程式の線形化を行い、SFLASHv2, SFLASHv3 共に破れることが示された。これらは A.Shamir 氏・J.Stern 氏およびその研究室からの示された一連の結果である。[Cryptanalysis of SFLASH with Slightly Modified Parameters, Vivien Dubois, Pierre-Alain Fouque and Jacques Stern, Eurocrypt 2007] [Practical Cryptanalysis of SFLASH, Vivien Dubois, Pierre-Alain Fouque, Adi Shamir and Jacques Stern, Crypto 2007]

数体篩法専用ハードウェアを作成し、ふるい部分の高速化を図ったハードウェアを利用した解析には TWIRL (a wafer-scale design) があるが、TWIRL に比べ 2～3.5 倍程度遅いが、メモリ量を削減していており TWIRL に比べ安価で構成可能な方法が発表された。[Non-Wafer-Scale Sieving Hardware for the NFS: Another Attempt to Cope with 1024-bit, Willi Geiselmann and Rainer Steinwandt, Eurocrypt 2007]

1039 ビットの合成数 $2^{1039}-1$ の素因数分解が特殊数体篩法(SNFS)を利用して実現された。

既にこの合成数が 5080711 という素因数を持つことは分かっていたので、ここではこれで割った 1017 ビット数の素因数分解ができることを示した。また、本実験は遠隔地を結び分散処理を実施し得られた結果である。なお、特殊数体篩法は大部分の合成数に対して適用できないので、1024 ビット鍵の RSA 暗号の安全性が決定的に低下したというわけではない。[A Kilobit Special Number Field Sieve Factorization, Kazumaro Aoki, Jens Franke, Thorsten Kleinjung, Arjen K. Lenstra, and Dag Arne Osvik, Eurocrypt 2007]

2.3.5. その他

NIST の提唱している NIST SP 800-90 の楕円曲線を利用した random number generator に関する解析結果においては、楕円曲線上での DH 問題の困難性、2 つの新たな問題に対する困難性(x-アルゴリズム問題、truncated point problem) を満たすときは ECRNG (Elliptic curve random number generator)は安全であるとしている。truncated problem に関して、NIST が規定している範囲内でごく小さなビット数が truncate されている場合であっても、解けてしまうことがあることを示した。これは、ストリーム暗号に用いられているような場合その安全性を保障できない場合があることを意味する。一方、nonce としての使用や鍵生成などの場合には無害である。[A Security Analysis of the NIST SP 800-90 Elliptic Curve Random Number Generator, Daniel R.L. Brown and Kristian Gjøsteen, Crypto 2007]

RFID のタグの認証に注目し、満たされるべき安全性の要求条件を提示し、8 つ安全性レベルを定義し、それら定義間の帰着関係を示した。(但し、タグ認証にのみ言及しており、リーダ認証は含まれていない) ここ 2～3 年の間、RFID の認証関係の論文は数多く出ているが安全性に関してきちんと議論されているものはあまり多くない。本結果は、今後の RFID の認証方式を提案していく上でも一つの指標になると考えられる。[On Privacy Models for RFID, Serge Vaudenay, Asiacrypt 2007]

2.4.委員会開催記録

平成 19 年度、暗号技術監視委員会は、表 2.12 の通り 3 回開催された。暗号技術調査ワーキンググループは、表 2.13 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 2.12 暗号技術監視委員会の開催

回	年月日	議題
第 1 回	平成 19 年 6 月 5 日	活動方針確認、監視状況報告
第 2 回	平成 19 年 11 月 13 日	技術調査 WG 中間報告、リスト改訂のための勉強会検討状況報告
第 3 回	平成 20 年 3 月 3 日	監視状況報告、CRYPTREC Report 2007 審議

(2) 暗号技術調査ワーキンググループ

表 2.13 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	平成 19 年 8 月 7 日	第 1 回リストガイド WG（活動計画の審議）
第 2 回	平成 19 年 10 月 17 日	第 2 回リストガイド WG（リストガイド対象技術の審議）
第 3 回	平成 20 年 1 月 16 日	第 3 回リストガイド WG（リストガイド 0 次案の審議）
第 4 回	平成 20 年 2 月 25 日	第 4 回リストガイド WG（リストガイド 1 次案の審議）

表 2.14 暗号技術調査ワーキンググループ(公開鍵)の開催

回	年月日	議題
第 1 回	平成 19 年 5 月 16 日	第 1 回公開鍵暗号 WG（活動計画の審議）
第 2 回	平成 19 年 12 月 18 日	第 2 回公開鍵暗号 WG（活動計画修正の審議）
第 3 回	平成 20 年 2 月 8 日	第 3 回公開鍵暗号 WG（暗号技術仕様、仕様参照先変更の審議）
第 4 回	平成 20 年 2 月 22 日	第 4 回公開鍵暗号 WG（2007 年報告書審議）

第３章 暗号技術調査ワーキンググループ

3.1. リストガイドワーキンググループ

3.1.1. 調査背景

電子政府システムにおいて、安全な暗号技術を利用することを目的に、総務省および経済産業省が共同で開催する暗号技術検討会のもと、電子政府推奨暗号リストが 2003 年 2 月 20 日に公表された。また、2003 年 2 月 28 日に行政情報システム関係課長連絡会議において、各府省が情報システムの構築にあたり暗号を利用する場合には、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旨の「各府省の情報システム調達における暗号の利用方針」が了承された。

この電子政府推奨暗号リストは、安全性が確認された暗号アルゴリズムが列挙されている。一方、安全な電子政府システムを構築する際には、暗号アルゴリズムが組み合わされて使われているセキュリティの標準技術が調達の際の選択基準となる。そのため、構築する電子政府システムの安全性を確認するためには、暗号アルゴリズムの安全性とセキュリティの標準技術の関係を理解したうえで、推奨される標準技術を利用することが必要となる。

上記の課題を解決するために、リストガイドワーキンググループを今年度新たに組織して、電子政府推奨暗号リストガイド（以下「リストガイド」という。）を作成した。リストガイドは、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を利用したセキュリティ技術の安全性と暗号アルゴリズムの安全性の関係を示した上で、標準技術の中で選択することが望ましい暗号アルゴリズムとそのセキュリティパラメータを示したものである。

リストガイドの想定読者は、電子政府システムの調達者、およびシステム構築を行うベンダである。

システム調達者は、電子政府システムの調達を行う際に、その調達仕様の中にセキュリティに関する要件を盛り込む。調達に際し、システムベンダは提案書類の中に、暗号技術を用いたセキュリティ技術の利用を盛り込む。リストガイドは、システム調達者が提案されたセキュリティ技術が本当に安全であるかどうかを確認する際に参照する。

一方、システムベンダは、調達の際の安全性のガイドラインとして、本リストガイドの情報を参照して仕様の策定、および設計を行うことで、調達要件に沿った安全なシステム構築を容易に行うことができる。

3.1.2. 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：	宇根　正志	（日本銀行金融研究所）
委員：	國廣　昇	（電気通信大学）
委員：	高橋　芳夫	（NTT データ）
委員：	谷川　嘉伸	（日立製作所）
委員：	角尾　幸保	（日本電気）
委員：	村上　哲	（富士通）
委員：	山村　明弘	（情報通信研究機構）
委員：	渡辺　創	（産業技術総合研究所）

3.1.3. 活動内容

リストガイドワーキンググループでは、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を利用したセキュリティ技術について、その技術概要と、推奨する利用方法を導出することを目的として、検討を行った。

【検討方針】
リストガイドにおいて、推奨される利用方法を選ぶ際の選択基準は以下の通りである。

・基本的な考え方として、使ってはいけない暗号技術を除外することを目標とする。
・標準規格の中に定められている暗号アルゴリズムの中に、電子政府推奨暗号リストに含まれる暗号アルゴリズムがある場合、当該アルゴリズムを推奨とする。
・標準規格の中で、特に暗号アルゴリズムが定められていない場合には、電子政府推奨暗号リストの暗号アルゴリズムを適用する。
・電子政府推奨暗号リストで注釈がついているアルゴリズムについては、標準規格の中で他に選択肢がない場合を除いては、リストガイド内では推奨しない。
・電子政府推奨暗号リストにない暗号技術（MAC など）については、標準で規定されている技術などで問題があるかどうかを確認する。
・セキュリティパラメータは、該当する利用方法に必要な保証期間を念頭に、過去の CRYPTREC レポートでの監視結果に基づいて選択する。
・公開鍵暗号の鍵長については、2048 ビット以上を基本とする。ただし、規格や実装上の制約により 2048 ビット以上の鍵長を利用することが困難であることが想定される場合には、必要な有効期間に応じて、注釈つきで短い鍵長について別途、記載をする。

・DSA については、2048 ビットの仕様が策定されつつあるが、ドラフト版であるため、参考として掲載している。仕様と評価が固まり次第、推奨とする。
・パディングの方式が複数定義されている暗号技術の場合、過去の CRYPTREC Report での安全性評価に従い、最も安全な方式について推奨とする。

【記述対象技術】
記述対象のセキュリティ技術は、
・認証技術
・PKI 関連技術
・通信路の暗号化技術
・蓄積データの暗号化技術
・改ざん検知、時刻認証技術
・鍵管理
・MAC、KDF
である。その中で、ISO、IEC、ITU、IETF、NIST などの標準化機関で定められた標準技術について記述を行っている。

【記述項目】
リストガイドには、電子政府システムで利用することが想定される、上記の標準的なセキュリティ技術について、
・技術の概要
・想定される脅威
・脅威に対する対策方針
・技術が備えるべき要件
・標準化動向
・技術の安全性と、暗号アルゴリズムの安全性の関係
・推奨される利用方法（暗号アルゴリズム、セキュリティパラメータ）
を記述している。

3.1.4. 調査結果の概要

【推奨される利用方法】
① エンティティ認証
エンティティ認証においては、SSL、SSH のような相手認証の技術と、ワンタイムパスワード、認証付き鍵交換、公開鍵暗号や共通鍵暗号を用いる認証プロトコル、IC カードや TPM を利用した認証方式についての検討を行った。

SSL の証明書の認証においては、2048 ビット以上の電子署名アルゴリズム、鍵交換においても 2048 ビット以上の公開鍵技術（楕円の場合は 224 ビット以上）の利用、完全性の保証においては HMAC-SHA1、暗号通信においては AES、Camellia の 128 ビット以上を推奨とした。また、ハッシュ関数については SHA-1 が RFC で規定されているため、注釈つきで掲載している。SSH においても、SSL と同様の推奨アルゴリズムとした。

ワンタイムパスワードにおいては、ハッシュ関数を利用した技術を取り上げ、SHA-256/384/512 と CRYPTREC で例示した擬似乱数生成系を利用することを推奨した。

認証つき鍵交換については、共通鍵を用いる場合リスト掲載の 128 ビットブロック暗号と、CRYPTREC Report 2005 において安全性が確かめられた MAC を推奨とすることにした。公開鍵を用いる場合、2048 ビット以上の公開鍵技術（楕円の場合 224 ビット以上）、ハッシュ関数として SHA-256/384/512、MAC として CRYPTREC Report 2005 において安全性が確かめられた MAC を推奨とすることにした。

IC カードを利用した認証技術、共通鍵暗号、公開鍵暗号、MAC を利用した認証技術についても、同様の推奨とした。

② PKI

証明書の発行、CRL の発行、OCSP プロトコルについての検討を行った。

証明書の発行においては、SHA-256/384/512 と、2048 ビット以上の電子署名技術を推奨とした。また、CRL の発行、OCSP における電子署名も同様の推奨とした。

③ 通信路の暗号化

通信路における暗号化方式として、PIN の暗号化、SSL-VPN、IPsec-VPN、無線 LAN、鍵共有方式について検討を行った。

PIN の暗号化については、共通鍵暗号を用いる場合にはリストに掲載された 128 ビット以上のブロック暗号を、公開鍵アルゴリズムの場合には RSA-OAEP 2048 ビット以上を、MAC として CRYPREC Report 2005 において安全性が確かめられた MAC を推奨とすることにした。

SSL-VPN については、エンティティ認証における SSL と同様の推奨とした。IPsec-VPN については、IKE のための鍵共有においては 2048 ビット以上の鍵共有技術と 2048 ビット以上の電子署名技術、相手認証においては 2048 ビット以上の電子署名技術と 128 ビット以上の AES、Camellia、MAC として CRYPREC Report 2005 において安全性が確かめられた MAC を推奨とすることにした。

無線 LAN については、可能な限り WPA2 を利用すること、WEP を利用しないこととした。

鍵共有方式については、エンティティ認証における認証付き鍵交換と同様とした。

④ 蓄積データの暗号化

蓄積データの暗号化技術として、ファイル暗号化、DB の暗号化、OS による暗号化を対象に検討を行った。

ファイル暗号化では OpenPGP を対象として、乱数生成においてリストで例示されている擬似乱数生成系を、共通鍵暗号として AES128 ビット以上を、公開鍵暗号としては RFC4880 で規定されているため RSAES-PKCS-v1_5 2048 ビット以上を、ハッシュ関数として SHA-256/384/512 を、電子署名アルゴリズムにおいて RSASSA-PKCS-v1_5 あるいは DSA の 2048 ビット以上を掲載した。

DB による暗号化では Oracle における暗号化方式を例にとり、同様の暗号化方式を採用した場合にリストに掲載されている 128 ビット以上のブロック暗号を推奨とした。

OS による暗号化では、MS Windows 2000 以降に搭載されている EPS を例にとり、同様の暗号方式を採用した場合に、乱数生成としてリストで例示されている擬似乱数生成系を、共通鍵暗号としてリストに掲載されている 128 ビット以上のブロック暗号を、公開鍵暗号として RSA-OAEP 2048 ビット以上を、鍵共有として PSEC-KEM 224 ビット以上を、証明書向けハッシュ関数として SHA-256/384/512、電子署名アルゴリズムにおいて RSASSA-PKCS-v1_5、DSA の 2048 ビット以上、ECDSA 224 ビット以上を掲載した。

⑤ 改ざん検知・時刻保証

改ざん検知技術として、ハッシュ関数を用いた方法、MAC を用いた方法、電子署名を用いた方法、S/MIME、コード署名技術を、時刻保証技術として、電子署名を用いたタイムスタンプ方式について検討を行った。

ハッシュ関数を用いた改ざん検知では、SHA-256/384/512 を推奨とした。MAC を用いた方法では、CRYPREC Report 2005 において安全性が確かめられた MAC を推奨とした。電子署名を用いた方法では、RSASSA-PKCS-v1_5、DSA の 2048 ビット以上、ECDSA 224 ビット以上と SHA-256/384/512 ビットのハッシュ関数を掲載した。S/MIME においても、同様の推奨とした。コード署名技術においては、Microsoft 社の Authenticode、JAVA SDK のコード署名を対象に検討を行い、RSASSA-PKCS-v1_5、DSA の 2048 ビット以上、ECDSA 224 ビット以上と SHA-256/384/512 ビットのハッシュ関数を掲載した。

電子署名を用いたタイムスタンプ方式については、RSASSA-PKCS-v1_5、DSA の 2048 ビット以上、ECDSA 224 ビット以上と SHA-256/384/512 ビットのハッシュ関数を掲載した。

⑥ 鍵管理

暗号鍵管理に関する基本的な要件を示す。生成から破棄に至る暗号鍵のライフサイクルとその各段階における鍵管理上の機能と保護について、NIST SP 800-57 Part 1 および ISO 11568-1/2/4 を参考に記述した。また、利用場面における鍵管理を具体的に示すために、署名用途 PKI のプライベート鍵を例に、鍵ライフサイクル、鍵管理機能、保護

対策の方針について検討を示した。

⑦ 暗号利用モード及びMAC（メッセージ認証コード）

現状の電子政府推奨暗号リストでは、暗号利用モード及びMACに関する言及がないため、暗号利用モードに関しては、EBC、CBC、k-CFB、OFB、CTR の各モード、MAC に関しては、CBC-MAC、EMAC、XCBC、CMAC、HMAC の各 MAC について、その概要と安全性、性能などの評価を掲載した。

⑧ 鍵導出関数

現状の電子政府推奨暗号リストでは、暗号実装の評価に足る鍵導出関数に関する仕様の言及がないため、KDF 関数に関する概要、ハッシュ関数ベースの KDF、HAMC ベースの KDF 関数の概要と、安全性に関する評価を掲載した。評価結果としては、SHA-1/256/384/512 を利用する限り、NIST SP 800-56A、ANS X9.42、SECG SEC1 で使用される KDF 関数の安全性が直ちに脅かされる状態でないことを掲載した。

3.1.5. まとめ

本年度の活動では、標準的なセキュリティ技術について、リストやこれまでの監視結果、そして標準仕様の制約に基づき、推奨される利用方法を導出した。詳細な内容については、別冊の「電子政府推奨暗号の利用方法に関するガイドブック」を参照のこと。

今後は、暗号技術の進展、および暗号技術に対する攻撃の進展に伴い、対象となる技術を更新していくとともに、リストガイドを定期的に見直していくことが望まれる。また、標準的なセキュリティ技術、暗号アルゴリズムに対する攻撃が発生し、緊急の安全性に対する問題が発生した場合には、可能な限り修正情報を公開するとともに、リストガイドに反映の上、改版されたリストガイドを公開することが必要である。

3.2. 公開鍵暗号ワーキンググループ

3.2.1. 調査背景

暗号技術調査ワーキンググループ（公開鍵暗号）（以下、本 WG）の 2007 年度当初の活動目的は、NIST から提出されている Draft FIPS 186-3 に記載されている DSA について、1024 ビットより長い鍵サイズをサポートする変更部分を確認の上、その安全性の検討する計画であった。

その後、暗号モジュール試験及び認証制度（以下、JCMVP）の事務局から、電子政府推奨暗号リスト（以下、リスト）記載の暗号技術と JCMVP において承認されたセキュリティ機能との間のうち、いくつかの差異について JCMVP の要望を認めるよう検討依頼（資料 3-1 を参照のこと）があったため、事務局はその調整が付くまで本 WG の開催を見合わせていた。

暗号技術検討会（2007 年 11 月 20 日開催、第 2 回）において、上述の要望等に対応して電子政府推奨暗号の監視の具体的な内容の一部修正が認められた。従って、本 WG では JCMVP の要請等に基づいて検討が必要となった暗号技術に関して、技術的な部分に限定して検討を実施した。

本 WG が提出する結果に基づき、今後開催される暗号技術監視委員会及び暗号技術検討会において、電子政府推奨暗号の仕様書の参照先の変更（追加を含む）及び仕様の変更に関する結論が下されている。

3.2.2. 活動目的

公開鍵暗号ワーキンググループでは、暗号技術監視委員会及び暗号技術検討会において、検討対象の暗号技術における「仕様書の参照先の変更（追加を含む）または仕様書の変更」に関して、その妥当性を判断できる資料を作成するために、年度当初に計画された検討項目に優先して、次の各項目の安全性について調査・検討を行うこととした。

- （DH 及び ECDH に係る）鍵導出関数（KDF 関数、Key Derivation Function）
- （ECDSA 及び ECDH に係る）楕円曲線ドメインパラメータ（の生成・検証）
- （ISO 化に伴い生じた仕様変更に係る）PSEC-KEM

なお、NIST FIPS 186-2 (+ Change Notice 1)における DSA（鍵長が 1024 ビット）については、ANS X9.30:1-1997 と FIPS PUB 186-2 の仕様は基本的に同じであったが、FIPS PUB 186-2 は Change Notice 1 において鍵サイズ（1024 ビット未満は仕様外）と擬似乱数生成器に対して仕様変更があった。

擬似乱数生成系の問題点（DSA に関する Bleichenbacher の指摘[1]）は CRYPTREC では既に対応済みで、電子政府推奨暗号リストにおける例示において、指摘されていた問題点を有する擬似乱数生成器は除外されている[2]。このため、特に安全性には問題はないことが判明している。

よって、仕様書の参照先を変更する場合には、FIPS 186-2 (+ Change Notice 1)のみとするのは妥当であると考えられる。

3.2.3. 評価対象暗号技術

暗号技術名	主な検討対象
DH	NIST SP 800-56A, ANSI X9.42
ECDSA 及び ECDH	NIST SP 800-56A, ANSI X9.62 (ECDSA), SECG SEC 1
PSEC-KEM	提案者からの提出資料

3.2.4. 委員構成（敬称略、五十音順）

主査：　太田　和夫　　（電気通信大学）
委員：　内山成憲（首都大学東京）
委員：　小暮淳（富士通研究所）
委員：　駒野雄一（東芝）
委員：　洲崎誠一（日立製作所）
委員：　藤岡淳（日本電信電話株式会社）
委員：　松本勉（横浜国立大学）
委員：　渡辺創（産業技術総合研究所）

委員交代（１０月まで）：
　青木和麻呂（日本電信電話株式会社）、下山武司（富士通研究所）

[1] r を160 ビットの乱数、q を160 ビットの素数としたときに，r mod q の分布が偏ることを利用したもの。

[2] CRYPTREC Report 2002 第 5 章 擬似乱数生成系の評価, http://www2.nict.go.jp/y/y213/cryptrec_publicity/c02_report.pdf

3.2.5.活動概要

(1)DH に関する調査

現在の電子政府推奨暗号リストにおける DH の仕様参照先は ANS X9.42-2001 である。ANS X9.42 と SP800-56A の間に存在する技術仕様上の主な差異は、

（イ） 有限体ドメインパラメータについては、ANS X9.42 のものは、SP800-56A に適合しない場合があるが、NIST SP800-56A のものは ANS X9.42 に適合する。

（ロ） KDF 関数について差異が存在する。どちらもハッシュ関数を使用する KDF 関数としては同じタイプに属するので、安全なハッシュ関数を使用すれば、安全性上問題はない。

（ハ） その他、DH のスキームの種類、公開鍵の検証、鍵配送手法、鍵確立プロセスについて、SP800-56A の方がより強い制限を課している。

となっている。

よって、SP800-56A について安全性上の問題はない。なお、ANS X9.42-2003 という改訂版が発行されており、スキーム自体には変更はないものの、素数生成に関連する補助関数の記述に微修正があるため、ANS X9.42-2001 は ANS X9.42-2003 に変更すべきである。

仕様の参照先を変更する場合には、KDF 関数に関する差異による相互接続性を考慮すれば、NIST SP 800-56A を参照先として追加することが妥当であると考えられる。

詳細は、CRYPTREC Report 2007 付録 3 を参照のこと。

(2)ECDSA に関する調査

現在の電子政府推奨暗号リストにおける ECDSA の仕様参照先は SECG SEC 1 v1.0 である。SECG SEC 1 v1.0 と ANS X9.62-2005 の間に存在する技術仕様上の差異は、楕円曲線ドメインパラメータの選択方法にあり、以下が主なものです：

（イ） セキュリティレベル[3]の許容範囲：
ANS X9.62-2005はセキュリティレベルが80以上となっていて、SECG SEC 1 v1.0のようなセキュリティレベルが80未満のレベルは許容していない。

（ロ） 基礎体の標数が2の場合の、基礎体の基底を表す既約多項式の許容範囲：
SECG SEC 1 v1.0とANS X9.62-2005の間で、一方が許容するパラメータを他方が許容しない場合があるため、相互接続できない場合があり得る。

（ハ） コファクターの許容範囲：
ANS X9.62-2005はSECG SEC 1 v1.0よりも条件が緩和されているが、セキュリティレ

[3] セキュリティレベルについては、ANS X9.62-2005 の 6.1 節及び SECG SEC 1 v1.0 の 3.1 節を参照のこと。

ベルに依存して、ベースポイントの位数の下限が規定されているので、安全性が低下することはない。

（ニ） MOV条件

ANS X9.62-2005はSECG SEC 1 v1.0よりも条件が厳しくなっているので、安全性に問題はない。

（ホ） 擬似乱数生成器

SECG SEC 1 v1.0では、擬似乱数生成器について特に指定がない一方で、ANS X9.62-2005では、HMAC_DRBGというHMACベースの擬似乱数生成器が承認されたものとして利用できる。これは、JCMVPにおいて2007年度中に評価されており、安全性に問題はない。

したがって、（イ）～（ホ）の違いから、SECG SEC 1 Ver.1.0 と ANS X9.62-2005 のどちらを認証基準にするにしても、他方が認証されないことがあり得るので、仕様書の参照先を変更する場合には、ANS X9.62-2005 を追加するのが妥当であると考えられる。

詳細は、CRYPTREC Report 2007 付録 3 を参照のこと。

(3)ECDH に関する調査

現在の電子政府推奨暗号リストにおける ECDH の仕様参照先は SEC 1 Ver.1.0 である。SEC 1 Ver.1.0 と NIST SP800-56A の間に存在する技術仕様上の主な差異は、

（イ） 楕円曲線ドメインパラメータについて差異が存在する。安全性上の問題点はないものの、相互接続性に支障をきたす可能性がある。

（ロ） KDF 関数について差異が存在する。どちらもハッシュ関数を使用する KDF 関数としては同じタイプに属するので、安全なハッシュ関数を使用すれば、安全性上問題はない。

（ハ） security level、擬似乱数生成器、standard なプリミティブの使用について、NIST SP800-56A の方がより強い制限を課している。

また、NIST SP800-56A では key を次のように static key と ephemeral key とに区別している

- ephemeral key：トランザクション毎に変えること(を通常とする)key
- static key：鍵交換のエンティティや秘密鍵のオーナーの Identifier と結び付いた key であり、ephemeral key より長寿命な key

（ニ） NIST SP800-56A に規定されている 5 種類のスキームのうち、ephemeral key のみを使う最も構造の単純なスキームが、SECG SEC 1-v1.0 のスキーム(それにより強い制限を課したもの)に相当する。NIST SP800-56A のその他 4 種類のスキームは、static key の使用を伴うスキームである。

したがって、NIST SP800-56A の ephemeral key のみを使うスキーム C(2,0,ECC CDH)[4]はSECG SEC 1 v1.0 のスキームに相当し、安全性上の問題はないものの、NIST SP800-56A の static key を使う残りの 4 種類の ECDH スキームについては、SECG SEC 1 v1.0 で規定されているスキームの範囲を超えており、仕様書の参照先の変更先として結論付けるにはさらなる検討が必要であると考えられる。

詳細は、CRYPTREC Report 2007 付録 3 を参照のこと。

(4)PSEC-KEM に関する調査

現在の電子政府推奨暗号リストにおける仕様参照先は、2002 年度までに提案者から応募された提出書類に基づくものである[5]。

過去のCRYPTREC ReportにおいてPSEC-KEMは、「KEM 技術に関する証明可能安全性がランダムオラクルモデルのもとで楕円曲線DH計算問題に帰着されるように示されている。したがって、KEM(Key Encapsulation Mechanism)-DEM(Data Encapsulation Mechanism) 構成に利用することは安全である。」と評価されている。

ISO/IEC 18033-2の審議過程において、エディタ並びに各国からのコメント等を吸収する形で、提案された仕様に一部修正が加えられ、最終的に規格化されたものが電子政府推奨暗号リスト策定時のものと若干異なるものとなってしまった。そこで仕様書の変更の妥当性を判断できる資料を作成するために今年度評価が行われた。評価に当たっては、提案者に新たに資料の提出を求めた。

一部仕様変更により、証明可能安全性において証明の見直しが必要となるものの、ISO/IEC 18033-2:2006 の仕様そのままではなく、楕円曲線上の群に限定して議論することで、従来と同様の安全性を示すことができる。現仕様と比べて、安全性評価結果の帰着効率が 2 倍程度低下するが、安全性への影響は小さいといえる。

よって、ISO/IEC 18033-2:2006 における PSEC-KEM については楕円曲線上の群に限定することで安全性上の問題はないと考えられ、仕様の変更についても問題はない。

詳細は、CRYPTREC Report 2007 付録 3 を参照のこと。

---

[4] 記号 C については、NIST SP 800-56A の 6 節、Table 4 及び Table 5 (p.51)を参照のこと。

[5] PSEC-KEM 仕様書(2002 年 5 月 14 日)
http://cryptrec.nict.go.jp/cryptrec_03_spec_cypherlist_files/PDF/02_02jspec.pdf

3.2.5 まとめ

以上の検討結果により、電子政府推奨暗号リストに記載された一部の暗号技術において、仕様の変更、仕様書の参照先の変更または追加として修正情報を周知すべき内容は、以下の表の通りである。

表　修正情報を周知すべき内容

暗号技術名	仕様参照先（修正前）	仕様参照先（修正後）[6]
DSA	ANS X9.30:1-1997	NIST FIPS PUB 186-2（+ Change Notice 1）
DH	ANS X9.42-2001	ANS X9.42-2003 及び NIST SP 800-56A
ECDH	SECG SEC 1 v1.0	SECG SEC 1 v1.0 及び NIST SP 800-56A の C(2,0,ECC CDH)が定めるスキーム
ECDSA	SECG SEC 1 v1.0	SECG SEC 1 v1.0 及び ANS X9.62-2005
PSEC-KEM	PSEC-KEM 仕様書 2002 年 5 月 14 日版 (公募時の応募書類)	PSEC-KEM 仕様書 2008 年 1 月 18 日版[注]

[6] http://www.cryptrec.go.jp/method.html を参照のこと。

注： 第 3 回暗号技術検討会開催後、主に型変換関数に関する修正等が施された仕様書の再提出があった（2008 年 4 月 14 日）。それらの修正等は安全性には影響がないものと判断されたため、年度内での検討結果と併せ、最終的に 2008 年 4 月 14 日版である、
PSEC-KEM Specification version 2.2, NTT Information Sharing Platform Laboratories, NTT Corporation, April 14, 2008（及びその日本語版）
が仕様参照先として適当であると判断された。

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：crypto-ml@ml.soft.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：crypto-ml@ml.soft.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/
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　羽山哲雄 TEL:03-3218-4116　FAX:03-3218-3638 E-MAIL:Hayama.Tetsuo@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/
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 ネットワークソフトウェア本部　担当本部長　松永和男 TEL： 045-862-8498, FAX： 045-865-9055 E-MAIL： matsun_k@itg.hitachi.co.jp

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 ネットワークソフトウェア本部　担当本部長　松永和男 TEL：045-862-8498, FAX： 045-865-9055 E-MAIL： matsun_k@itg.hitachi.co.jp

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.rsasecurity.com/rsalabs/cryptobytes/index.html>

3. ハッシュ関数

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

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

4. 擬似乱数生成系

暗号名	PRNG in ANSI
関連情報	仕様 ・ANSI X9.42-2001, Public Key Cryptography for The Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography ・参照 URL <http://www.x9.org/> なお、同規格書は日本規格協会 (http://www.jsa.or.jp/) から入手可能である。

暗号名	PRNG in ANSI X9.62-1998 Annex A.4
関連情報	仕様 ・ANSI X9.62-1998, Public Key Cryptography for The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA) ・参照 URL <http://www.x9.org/> なお、同規格書は日本規格協会(http://www.jsa.or.jp/)から入手可能である。

暗号名	PRNG in ANSI X9.63-2001 Annex A.4
関連情報	仕様 ・ANSI X9.63-2001, Public Key Cryptography for The Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography ・参照 URL <http://www.x9.org/> なお、同規格書は日本規格協会(http://www.jsa.or.jp/)から入手可能である。

暗号名	PRNG for DSA in FIPS PUB 186-2 Appendix 3
関連情報	仕様 ・FIPS PUB 186-2, Digital Signature Standard (DSS) ・参照 URL <http://csrc.nist.gov/CryptoToolkit/tkrng.html>

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

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

付録 3

学会等での主要発表論文一覧

本付録では、情報収集を行なった学会等で発表された主要論文の要旨を、次の 6 つのカテゴリーに分類して記載する。

1. ハッシュ関数の脆弱性解析 / 新手法の提案
2. ストリーム暗号
3. ブロック暗号
4 公開鍵アルゴリズム
5. 暗号プロトコル
6. その他

1. ハッシュ関数の脆弱性解析 / 新手法の提案

New Message Difference for MD4 [FSE 2007]

Yu Sasaki, Lei Wang, Kazuo Ohta and Noboru Kunihiro

ハッシュ関数 MD4 について、局所衝突の解析を丁寧に行い、条件のよい衝突を絞り込み、従来提案されていた手法などの利点もうまく使った。結果として全体のかかる計算量を削減し、効率のよい衝突探索の手法を提案し、実装まで行った。MD4 の脆弱性をより強く印象付ける結果であると共に、これらの攻撃方針の MD5 や SHA-1 への適用可能性に関しては注目してゆく必要がある。

Gröbner Basis based Cryptanalysis of SHA-1 [FSE 2007]

Makoto Sugita, Mitsuru Kawazoe and Hideki Imai

58 段の SHA-1 の衝突発見、フルラウンド SHA-1 にかかるコストの見積もりを示した。質疑では、ランプセッションで 70 段 SHA-1 の衝突発見を報告したレッシュベルガー氏から質問があり、フルラウンドの場合での解読に要するコンピュータを用いた実測値について質問があったが、現状多大な計算量が必要であるとの見積もりであるが、差分パスの改良により 2^{63} 回の SHA-1 にまで計算量削減が可能であるという回答であった。

Producing Collisions for PANAMA, Instantaneously [FSE 2007]

Joan Daemen and Gilles Van Assche

PANAMA はストリーム暗号として用いられる場合とハッシュ関数として用いられる場合とがあるが、ここではハッシュ関数として用いられた場合の衝突探索に関する解析。従来法よりも効率的な手法を提案。M1 はある任意の値で、M, M*はある一定の差分を持つような値に

ついて、(M1|M) , (M1|M*) のペアを見つけることが出来る。但し、本提案方式はストリーム暗号としての PANAMA の安全性を下げるものではない。

Grindahl - a family of hash functions [FSE 2007]

Lars R. Knudsen, Christian Rechberger and Soren S.T homsen

Grindahl と呼ばれるハッシュアルゴリズムの提案。具体的にここでは Grindahl-256 と Grindahl-512 を公開。他ハッシュ関数に比べ、必要となるメモリ量が小さいくとのこと。Rijndael(AES の元となっている共通鍵暗号アルゴリズム)の構成を基本としており、collision-attack・second-pre-image attack pre-image attack いずれに対しても探索にかかる計算量は、2^{256} 及び 2^{512} であるとしている。処理速度は AES と同程度。

The collision intractability of MDC-2 in the ideal-cipher model [Eurocrypt 2007]

John P. Steinberger

並列な２個のブロック暗号を利用したハッシュ関数用の圧縮関数の一種である MDC-2 の安全性を証明した。証明には、9 種類の図に対する 40 通りの場合分けについて解析した。定数はスペックに応じて最適化した。今回の評価は最適に近くないので、改良すればより良いバウンドが得られることを示唆した。

Chosen-prefix Collisions for MD5 and Colliding X.509 Certificates for Different Identities [Eurocrypt 2007]

Marc Stevens, Arjen Lenstra and Benne de Weger

MD5 の衝突耐性の不備を利用して、署名が同じで文面が異なる X.509 に従った一対の署名が作れることを、実例によって示した。この署名対を作るのに要する計算量は MD5 の圧縮関数 2^{52} 回分であり、Eindhoven 技術大学のクラスター計算機と分散 PC(ボランティア 1200 名)を利用した HashClash プロジェクト(ピーク性能 400 GFlops)で合計６カ月掛かった。同じ研究グループによる ACISP 2005 の発表では、意味のある部分を持つ X.509 の証明書を一対を作ることに成功していたが、意味のある部分が共通であるという制限が付き、現実的な脅威にはならないものだった。今回の研究では、意味のある部分を任意の異なるものにできるように改良しており、より脅威が現実的なものになっている。今回の方法が X.509 証明書に限定した理由は、この形式だと衝突用のランダムブロック列が RSA モジュールに埋め込むことにより隠せるからである。さらに、複数の異なる予言で同じ署名値を持つ証明書を作るノストラダムス攻撃にも今回の方法が適用できることを紹介した。これらの結果を踏まえ、今後 MD5 は使ってはならないことを強調した。

Automatic search of differential path in MD4 [ECRYPT Hash Workshop 2007]

Pierre-Alain Fouque, Gaetan Leurent and Phong Nguyen

MD4 に対する差分経路探索を自動化し、さらに NMAC に対する偽造が可能であることを示した。この自動化された経路探索法の SHA-1 や MD5 に対して適用できていない。

Hash functions and the (amplified) boomerang attack [ECRYPT Hash Workshop 2007]

Antoine Joux and Thomas Peyrin

ブロック暗号に対する差分解読法の一種として開発されたブーメラン攻撃を、SHA-1 に適用することにより、有効な一部の段における差分経路の発見に成功した。この結果を Wang らによる SHA-1 の衝突探索に適用すると計算量が 1/32 に削減できると主張している。これが正しいとすると、Wang による評価が 2^{63} なので、SHA-1 の解読に必要な計算量は 2^{58} となる。計算量が削減できるのは、メッセージ変形探索の必要がないためである。

On the full cost of collision search for SHA-1 [ECRYPT Hash Workshop 2007]

Christophe De Canniere and Florian Mendel and Christian Rechberger

70 段に縮小した SHA-1 に対する衝突を、圧縮関数 2^{44} 回の計算量で発見した。フルラウンドが 80 段であり、衝突が発見できた最高段数が同じ研究グループによる 64 段(Asiacrypt 2006 で発表)なので、SHA-1 の衝突発見がますます現実味を帯びてきた。攻撃の特徴は、経路の探索に Greedy アルゴリズムの改良版を利用したことで、通常の Greedy アルゴリズムでは注目するビットが 1 ビットであるところを 7 ビットに拡大することで探索効率を高めた。また、A. Joux らによるブーメラン攻撃も検討したが、それほど経路の探索効率は改善しなかったことを指摘した。

How to Evaluate a Hash Proposal [ECRYPT Hash Workshop 2007]

John Kelsey

NIST によるハッシュ関数の公募(AHS)の概要と検討すべき課題について述べた後、参加者の意見を聞いた。公募の締め切りは 2008 年 8 月頃で、公募要領の発表から約 1 年後。ハッシュ関数は HMAC や DSA、ECDSA など様々な他の規格で利用されているので、既存の SHA-1、SHA-2 の置き換えができることが最も基本的な要件となる。そこから入出力のサイズや安全性や実装性能に関する要件の一部が導かれる。

安全性に関しては、衝突発見困難性、原像計算困難性、第 2 原像計算困難性が基本的であるが、どの程度の安全性を要求し、どのように解析するかは決まっていない。また、電子署名方式などの設計の多くで、ハッシュ関数をランダム・オラクルとして利用しており、ランダム性をどの程度重視し、評価するかも問題である。また、形式にも、同じ(圧縮)関数の繰り返し型かブロック暗号の動作モードかの 2 種類があり、NIST のリソースから両方は出来ない。また、投稿件数も現実の問題となり、15-20 件程度だと特に問題ないが、50 件もあると何らかの対処が必要となる。参加者に投稿の意思を聞いたところ、10 名前後が手を上げた。

ハッシュ関数に対する要件についての質疑では10件前後の意見が出て、研究者の間でコンセンサスが取れていないことが明らかになり、今後のプロジェクト運営が容易でないことが感じられた。

A critical look at cryptographic hash function literature [ECRYPT Hash Workshop 2007]

Scott Contini, Ron Steinfeld, Josef Pieprzyk and Krystian Matusiewicz

collision resistant hash function が次の３条件を満たすべしとする見解が広く受け入れられているが、文献を調べると必ずしも全部を要求していない。セキュリティの証明の多くで、ハッシュ関数を Random Oracle(RO)とするモデルが利用されているが、実際に RO を作ることは不可能である。このような状況を踏まえ、ハッシュ関数が満たすべき要件についての研究者間のコンセンサスの形成を早急に進めるべきである。

MAME：A compression function with reduced hardware requirements [ECRYPT Hash Workshop 2007]

Hirotaka Yoshida, Dai Watanabe, Katsuyuki Okeya, Jun Kitahara, Hongjun Wu, Ozgul Kucuk and Bart Preneel

日立とカトリック・ルーベン大学が共同で設計したMerkle-Dangard型ハッシュ関数の提案。圧縮関数の設計では PGV*構成の理論を適用して MMO 構造とし、メッセージ撹拌部は非等分Feistel 構造、実装性能を高めるため 4-bit S-box と XOR のみで構成した。ハッシュ関数としては安全性のマージンを考慮して 96 段とした。hash 関数としての衝突発見困難性とHMAC のサイドチャネル攻撃耐性が保証できると主張。衝突耐性の評価では、差分攻撃、線形攻撃、高階差分攻撃、補間攻撃、スクェア攻撃といった攻撃を考慮している。実装性能はSHA-256 と比較している。ハードウェアについては、MAME がスループット 440 ms, Gate数 8.2 KGates に対し、SHA-256 が 2600 ms, 18.0 KGates。ソフトウェアについては IC カード用マイコンへの実装で、MAME が処理時間 49.4 ms, RAM 96 Bytes に対し、SHA-256 が31.4 ms, 128 Bytes となっいる。MAME のソフトウェアではビットスライス実装で高速化している点について、Kelsey から通常の実装での性能を聞かれ、チェックしておくとの回答だった。

*PGV: Preneel-Govaerts-Vandewalle

Improved fast syndrome based cryptographic hash function [ECRYPT Hash Workshop 2007]

Matthieu Finiasz, Philippe Gaborit and Nicolas Sendrier

衝突発見困難性が証明可能な Augot-Finiasz-Sendrier によって提案された hash 関数を次の２点について改良した。

・セキュリティレベルが出力値長の半分になるように、最終圧縮変換を追加
・ハッシュ関数が短く記述できるように本質的にランダムな行列からランダムな準循環行

列に置き換えた
Augot-Finiasz-Sendrier の方式は、Fast Syndrome の原理を利用しており、その安全性は符号理論における問題に帰着する。

この結果、安全性を SHA-1 に対する誕生日攻撃耐性と同等(2^{80})に設定したとき、前回の方式で掛かった処理量が 517(cycle/byte)だったのが、281(cycle/byte)と削減され、1.8 倍強高速化した。SHA-256 では、20.6(cycle/byte)と約 13.6 倍処理時間が掛かるので、実用的になるためには、なお一層の高速化が必要である。

Building application-agile hash functions: the MCM construction [ECRYPT Hash Workshop 2007]

Thomas Ristenpart and Thomas Shrimpton

MCM 構成法は、衝突耐性が標準モデルで証明でき、かつ、理想的な暗号モデルを仮定するとランダムオラクルと区別できないハッシュ関数を設計するための構成法である。具体的には、衝突耐性のあるハッシュ関数を H、擬似ランダムな２個の単射写像 ε1、ε2 をとし、入力メッセージを M としたとき、ε2(H(ε1(M)))と表せる。

Collisions for 70-step SHA-1: On the Full Cost of Collision Search [SAC 2007]

Christophe De Canniere, Florian Mendel, and Christian Rechberger

70 段に縮小した SHA-1 に対する 2 ラウンドの衝突を発見した。ハッシュ関数に対する衝突発見攻撃における小さな改良について暗号研究者の関心が集まっている。例えば、Eurocrypt 2005 での X.Wang らの発表した 58 段縮小 SHA-1 に対し、杉田らによるグレブナー基底を使った方法は 8 倍の高速化を達成している。しかし、個々の改良法の性能を比較するのは、各々の計算量の見積もりが曖昧なため困難である。そこで、精度良く計算量を比較する方法が必要である。本論文では、探索のノードを適切に計算する方法を開発し、中立ビットを利用する方法やブーメラン攻撃などの計算量を比較したところ、差分経路による情報利得が最大化になるように状態変数をしらみつぶしに探索する方法が最も効率的だと判断した。この方法を利用して、70 段に縮小した SHA-1 の 2 ブロック・メッセージでの衝突を発見した。

Attacks on the ESA-PSS-04-151 MAC Scheme [SAC 2007]

Georg Illies and Marian Margraf

鍵長 2940 ビットのうちある 60 ビット分の情報と 80-100 程度のメッセージ・平文のペアの情報があった場合、その情報を用いて、勝率 5%以上でどの様なメッセージに対しても MAC を偽造でき、また残りの鍵の殆どをも推定することが出来るとしている。手段として、LLL アルゴリズムを用いて解くべきマトリックスを小さなマトリックスに reduction させ、探索に必要となる計算量を削減している。

Second Preimage Attack on 3-Pass HAVAL and Partial Key-Recovery Attacks on Security-Amplifying Combiners for Collision-Resistant Hash Functions [Crypto 2007]

Marc Fischlin and Anja Lehmann

衝突発見耐性がある２種類のハッシュ関数を利用して、より耐性の高いハッシュ関数を構成する従来と比べ性能の良い方法を開発した。衝突発見耐性がある２種類のハッシュ関数を利用して、より耐性の高いハッシュ関数を構成する方法にとして、単純に２種類のハッシュ関数出力の連結を取る方法がある。出力値が n ビットのハッシュ関数 $H_0(M)$, $H_1(M)$の衝突発見に要する時間を各々T_0, T_1 としたとき、両者の連結 $H_0(M)||H_1(M)$の衝突を発見するのに要する時間は、$(n/2)T_0+T_1$ であることが、A.Joux によって示されている。本発表では、ブロック長を b ビットに対し、メッセージサイズを tb ビット(t は $t<n/4$ を満たす正整数)に限定した。その結果、衝突発見に要する時間の下限として、$\alpha(T_0+T_1)$が保証されることが分かった。ただし、αは 1 より大きい数。さらに、発展した形 $H_0(M)||H_1(H_0(M)(+)M)$でも同様の結果が成立することも分かった。

Amplifying Collision Resistance: A Complexity-Theoretic Treatment [Crypto 2007]

Ran Canetti, Ron Rivest, Madhu Sudan, Luca Trevisan, Salil Vadhan and Hoeteck Wee

スタンダードモデルにおいて、弱い衝突耐性しか持たないハッシュ関数を使って、より強い衝突耐性を持つハッシュ関数を作る構成法を開発した。簡単な構成の MD4, MD5, SHA-1 などのハッシュ関数の安全性低下が問題となり、弱い衝突耐性しか持たないハッシュ関数を使って、より強い衝突耐性を持つハッシュ関数を作ることの意義が高まっている。本発表では、弱いハッシュ関数が公開情報である鍵に依存するモデルを導入し、衝突耐性のレベルとして、衝突が起こる確率の鍵選択における最大値と定義した。その結果、短い鍵、短いハッシュ値、高い衝突耐性の３つに対して良いトレードオフを実現する構成法を示した。具体的には、ハッシュ値の連結を利用する構成法と誤り訂正符合を利用する構成法の２種類の例を示した。

Hash Functions and the (Amplified) Boomerang Attack [Crypto 2007]

Antoine Joux and Thomas Peyrin

ブロック暗号に対する差分解読法の一種であるブーメラン攻撃をハッシュ関数に対する衝突探索に適用することにより、必要な計算量が下がることを実証した。ブーメラン攻撃は平文から暗号化して得られた暗号文に固定値を足し、それを復号して戻す計算を行うことからブーメランの名が付いた攻撃法である。ハッシュ関数に対する差分解読法は、大きな確率を持つ差分経路の探索と、発見された差分経路を満たすメッセージ対の探索の 2 段階

で構成される。ブーメラン攻撃は、既存の探索法と比較して、後者のメッセージ探索において優位性がある。Eurocrypt 2007 で、De Canniere らは 2 ブロック・メッセージに対する 70 段の衝突を発見しており、発見に必要な圧縮関数の呼び出し関数は第１ブロックと第２ブロックに対し、各々、2^{41}回、2^{44}回だった。同じ差分経路に対してブーメラン攻撃を適用したところ、呼び出し回数は各々、$2^{36.5}$回、2^{39}回と約 1/30 に削減することが出来た。計算時間は、openSSL の効率的な SHA-1 実装を利用し、PC8 台のクラスタを使って 10 時間以内だった。

Efficient Hash Collision Search Strategies on Special-Purpose Hardware [SHARCS 2007]

Tim Gu"neysu, Christof Paar, and Sven Scha"ge

Merkle-Damgard 構成のハッシュ関数として代表的な MD4 型のハッシュ関数の衝突探索に適したハードウェア構成を検討した結果、専用 ASIC が汎用 CPU や低価格の FPGA より高い費用性能比を示すことが明らかになった。最近、SHA-1 を始めとする MD4 型ハッシュ関数の衝突探索の研究が進んでいる。最も有効な攻撃法は差分解読法に基づく方法で、大きな確率を持つ差分経路の探索とその探索で求めた差分経路を持ったメッセージ対の探索という２段階で構成される。実際により大きな計算量を要するのは後者のメッセージ対探索である。この発表では、汎用 CPU によるソフトウェア実装、専用 ASIC 及び低価格 FPGA によるハードウェア実装の 3 種類で最適化を行い、費用性能比を比較した。ASIC 版では、32 ビットで最小のマイクロプロセッサ構造を採用し、基本プロセッサをμMD、メモリを合わせた全体をμCS と名づけた。ASIC 実装μMD の費用性能比が最も高く、Pentium 4 の 2.9 倍だった。μMD で MD5 の衝突探索を行なった結果、4.8×10^{11} cycles で発見でき、動作周波数は 228.8MHz で計算時間は約 2100 秒だった。面積はμCS が 0.960mm^2。μMD の面積は 0.0266mm^2 でμCS の 2.8%で面積のほとんどはメモリに占められた。FPGA 実装との費用性能比の比較は書いてなかった。

MAME: A compression function with reduced hardware requirements [CHES 2007]

Hirotaka Yoshida, Dai Watanabe, Katsuyuki Okeya, Jun Kitahara, Hongjun Wu, Ozgul Kucuk, Bart Preneel

軽量･高速で既存の攻撃に対する安全性が高いハッシュ関数用の圧縮関数 MAME を開発した。安全なハッシュ関数は、原像計算困難性、第２原像計算困難性、衝突発見困難性を満たすことが要求されるが、近年の研究の発展により、MD5 と SHA-1 の安全性が揺らいでいる。より安全性の高いハッシュ関数に SHA-256 があるが、32-ビット・プロセッサには向いているが、低リソース環境では計算コストが高い。また、SHA-256 や SHA-1 の基本構成となっている Merkle-Damgard 構造自体の安全性も疑問が持たれている。このような状況から、高い安全性と実装性能を持つハッシュ関数が求められている。そこで、差分解読法などの攻撃法に対する安全性解析がしやすいように、MMO (Matyas-Meyer-Oseas)構造を採用し、メッセ

ージブロックと連鎖データのサイズを 256 ビットとした。その結果、差分解読法を始めとする各種の攻撃に対する安全性が保証でき、SHA-256 と同等の速度で実装サイズが小さいハッシュ関数の設計に成功した。保守的な構成であるが、既存の攻撃法に対する安全性はしっかり評価されている。

Cryptanalysis of the Tiger Hash Function [Asiacrypt 2007]

Florian Mendel and Vincent Rijmen

Tiger は Anderson と Biham が FSE 1996 で発表したハッシュ関数であり、フルラウンドは 24 段で 192 ビットのハッシュ値を出力する。最近、Kelsey らは FSE 2006 で、16〜17 段の縮小版に対する衝突を発見したが、24 段に対する衝突発見には誰も成功していない。この発表ではフルラウンドの Tiger に対し、2^{47}回分の計算量で pseudo-near 衝突が発見できることを導いた。この pseudo-near 衝突は、最終段における値が一致するものの、出力する際には初期値が足されるため、完全な衝突にならないというものである。

Cryptanalysis of Grindahl [Asiacrypt 2007]

Thomas Peyrin

Grindahl はデファクトの共通鍵暗号 AES の要素と構造を利用して設計したハッシュ関数のファミリーであり、ハッシュ値が 256 ビットの Grindahl-256 と 512 ビットの Grindahl-512 がある。発表では Grindahl-256 を対象に、衝突探索を切詰め差分法を利用した衝突対策の研究成果が発表された。この研究の特徴は、通常とは異なり、最初に全てのバイトが異なる状態から始まる差分経路を探索対象としたところである。これに加え、探索における早期での枝狩りを組合わせることで、効率を高め、ハッシュ関数 2^{112}回の計算量で衝突を発見できることを理論的に導いた。これは、ハッシュ値サイズから要求される 2^{128}回を下回る。

A Simple Variant of the Merkle-Damga*rd Scheme with a Permutation [Asiacrypt 2007]

Shoichi Hirose, Je Hong Park, and Aaram Yun

ハッシュ関数の SHA-1 や MD5 は Merkle-Damgard(DM)型という構造を持つ。この構造を持つハッシュ関数を使ってメッセージ認証子を作る方法である HMAC が広く使われているが、構造に起因する脆弱性のため偽造の可能性が指摘されている。この発表では、MD 型の繰り返し段構造における最終段の直前に置換を挿入するだけで、ほとんどオーバーヘッドなしに、安全性の改善が可能であることを示した。

Seven-Property-Preserving Iterated Hashing: ROX [Asiacrypt 2007]

Elena Andreeva, Gregory Neven, Thomas Shrimpton, and Bart Preneel

FSE 2004 で Rogaway と Shrimpton はハッシュ関数が満たすべき性質として、衝突発見耐性、３種ずつの原像計算困難性と第２原像計算困難性の計７個を提案した。この発表では、７

つの性質を満たす初めての繰り返し型ハッシュ関数の構成 ROX を提案した。ROX は、Random-Oracle-XOR の略で、設計要素として理想化されたランダム・オラクルを使っている点を発表者自身、不満だとしていた。

How to Build a Hash Function from Any Collision-resistant Function [Asiacrypt 2007]

Thomas Ristenpart and Thomas Shrimpton

MD5 や縮小型 SHA-1 の衝突発見によって、衝突発見耐性(CR)が理論的に証明できるハッシュ関数への要求が生じる。この発表では、Mix-Compress-Mix(MCM)型の構造が CR を実現でき、出力がランダム・オラクルと識別できないことを示した。

Boosting Merkle-Damga*rd Hashing for Message Authentication [Asiacrypt 2007]

Kan Yasuda

ハッシュ関数を利用したメッセージ認証子の構成法として HMAC と NMAC が広く使われている。この発表では、HMAC/NMAC より計算効率が良く、かつ、認証子が擬似ランダム関数であるためのハッシュ関数が満たすべき条件が緩くて済む方式を提案した。

On Efficient Message Authentication via Block Cipher Design Techniques [Asiacrypt 2007]

G. Jakimoski and K. P. Subbalakshmi

ブロック暗号の設計技術を応用して計算効率の良いメッセージ認証子を生成する方法を提案した。提案された方法は MACH と名づけられ、Wegman-Carter 二分木構造を利用している。MACH は利用するブロック暗号の段関数に AES、Feistel 型、SPN 型の各々を利用した３種類を用意し、各々、MAC-AES、MAC-FES、MAC-F64 と名づけている。MAC-AES は他の２つと比べ、安全性は指数尺度で２倍弱高いものの速度は半分強と劣っており、トレードオフが成り立っている。

Collisions for Step-Reduced SHA-256 [FSE 2008]

Ivica Nikolic and Alex Biryukov

SHA-1の後継ハッシュ関数であり推奨暗号でもあるSHA-256に対する衝突発見の攻撃を行い、フルスペックが64ステップのところ、21ステップに縮小したものに対する衝突を発見した。技術的なポイントは、確率1/3で成立する9ステップの差分パスを発見したことであり、さらにステップ数を伸ばすには、より長い差分パスの発見が必要となる。なお、条件を緩め、本来固定の初期ベクタを一部自由にし、ハッシュ値の少数ビットの違いを許容すると25ステップまで伸ばせ、ハッシュ値が256ビット中15ビットしか違わないメッセージペアが求められる。

Collisions on SHA-0 in One Hour [FSE 2008]

Ste'phane Manuel and Thomas Peyrin

ハッシュ関数SHA-1の改良前のバージョンであるSHA-0のフルスペックに対し衝突は発見されていたが、今回の発表では、ブーメラン攻撃の利用などの改良を行い、衝突発見に必要な計算量をハッシュ関数$2^{33.6}$回分にまで削減した。これを通常のPC上で実装たところ、１時間程度で衝突が発見できた。

MD4 is Not One-Way [FSE 2008]

Gae"tan Leurent

ハッシュ関数に要求される性質として、衝突発見困難性、第二原像計算困難性、原像計算困難性の三種類がある。MD4 では、最初の２つが破れているものの、原像計算困難性までは破れていないと考えられてきた。この発表では、2^{102} 回の計算量で破れることを理論的に示した。これは、MD4 は暗号用のハッシュ関数としては一切利用すべきでないことを意味する。この結果は理論評価に留まり、実際に原像を計算して見せたわけではないが、同じ設計原理に基づく SHA-1 や SHA-2 ファミリの原像計算困難性を揺るがす、重要な結果である。

Cryptanalysis of LASH [FSE 2008]

Scott Contini, Krystian Matusiewicz, Josef Pieprzyk, Ron Steinfeld, Guo Jian, Ling San, and Huaxiong Wang

ハッシュ関数LASHは、安全性が証明できるハッシュ関数の構造GGHを元にしつつ、実装性能を高めるために安全性を犠牲にして作られた。その後の解析で、LASHに対して衝突発見攻撃と原像計算攻撃が可能であることが分かったが、その理由の一つは初期ベクトルのビットが全部0という特異な選択にあった。そこで、これを変更することでLASHの安全性が向上するか解析したが、否定的な解析結果が得られた。

New Techniques for Cryptanalysis of Hash Functions and Improved Attacks on Snefru [FSE 2008]

Eli Biham

SnefruはMD4と同時期に発表されたハッシュ関数であるが、発表後数年で差分解読法によって破れたため、MD4とその後継が広く利用されるようになった。しかし、最近、MD4は差分解読法によってSnefruより安全性が低いことが明らかになった。この発表ではSnefruに対する従来の攻撃法を改良し、従来の攻撃手法に対して殆どメモリを必要とせずにSnefruが攻撃可能な手法を提示した。また、paddingの方法によってその安全性が大きく異なり安易なpadding の方法は原像計算攻撃のリスクを高めることになることが主張されていた。

NMAC/HMAC-3-Pass HAVAL［FSE 2008］

Eunjin Lee, Jongsung Kim, Donghoon Chang, Jaechul Sung, and Seokhie Hong

HAVALは1992年にY.Zheng氏が提案したハッシュ関数であり、衝突を発見するのに非常に有効な差分経路が知られている。この発表では、今まで提案されていなかった第２原像計算発見の方法を提案し、この方法を利用して効率的にHAVALを利用したメッセージ認証子生成方式HMACとNMACに対する鍵探索攻撃を提案した。

A (Second) Preimage Attack on the GOST Hash Function［FSE 2008］

Florian Mendel, Norbert Pramstaller, and Christian Rechberger

GOST Hash Functionはロシア政府によって利用されているハッシュ関数である。通常の圧縮関数に加え、入力メッセージブロックに対するチェックサムを計算し、ハッシュ値の一部とすることで安全性を高める工夫がされている。この発表では全数探索より少ない計算量で、原像及び第２原像が発見できることを示した。

The Hash Function Family LAKE［FSE 2008］

Jean-Philippe Aumasson, Willi Meier, and Raphael C.-W. Phan

BihamとDunkelmanによるHAIFAフレームワークに基づいた、ハッシュ値のサイズが256ビットと512ビットのハッシュ関数の属LAKEを提案した。設計上の新しいアイデアとして、入れ子型フィードフォワード構造と内部処理におけるワイド・パイプ構成を導入している。サイドチャネル攻撃などにも配慮して構成されている。SHA-256に比べ、小メモリで高パフォーマンスな構成となる。NISTの公募への応募も視野に入れているとのこと。

SWIFFT: A Modest Proposal for FFT Hashing［FSE 2008］

Vadim Lyubashevsky, Daniele Micciancio, Chris Peikert, and Alon Rosen

高速フーリエ変換を利用して拡散効果の高いハッシュ関数SWIFFTを設計した。また並列処理に適した構造が意識して構成されている。安全性に関しては、このハッシュ関数は漸近的な安全性が証明されているということだったが、これは入力やハッシュ値のサイズが大きくなる極限での話であり、実際の有限サイズでの安全性の保証にはなっていない。処理速度はSHA-256に勝っている。

(Short talk) Accelerating the Whirlpool Hash Function Using Parallel Table Lookup and Fast Cyclical Permutation［FSE 2008］

Yedidya Hilewitz, Yiqun Lisa Yin, and Ruby B. Lee

欧州の暗号評価プロジェクトNESSIEで選ばれたハッシュ関数Whirlpoolに対する高速なソフトウェア実装を行った。基本的アイデアはRISCアーキテクチャのモジュールにおいて、

テーブル参照を並列化することである。これはWhirlpoolがベースとしているAESやDES等の高速化にも用いられる手法である。本手法の適用により、7.2 cycles/bytes とSHA-2が 12 cycle/byte に比べ高速化を実現している。

A One-Pass Mode of Operation for Deterministic Message Authentication: Security beyond the Birthday Barrier [FSE 2008]

Kan Yasuda

圧縮関数を使った決定論的なメッセージ認証方式であり、実装効率が良く、安全性がバースデー・バリアを超える動作モードを提案した。この動作モードは固定入出力長の擬似ランダム関数に対する領域拡張と見なせ、入力に対するチェックサムとtweakを利用したブロック暗号の構成法を利用している。この方式はstatelessかつsinge-keyで構成可能であり、擬似ランダム関数などへの適用に有効である。

Improved Indifferentiability Security Analysis of chopMD Hash Function [FSE 2008]

Donghoon Chang and Mridul Nandi

SHA-1やMD5などで利用されているハッシュ関数の基本構造Merkle-Damgard(MD)型は、最近の研究で安全性の弱点が指摘されており、解決策としてハッシュ関数の出力(ハッシュ値)の一部を捨てて短くすることにより安全性の改善を目指したchopMDが提案されている。この発表では、chopMDに対する最新の安全性評価結果が報告された。indifferentiabilityに着目した安全性評価を行っており、またその観点から新しいハッシュ関数の構成についても提言している。提案構成は、クエリの回数が 2^n / 3n +1 より少なければ、第2原像攻撃に対して安全であり、$2^{n(r-1)/r}$ より少なければ、r-multi-collision 攻撃に対して安全である。(ここで、nは出力ビット長)

2. ストリーム暗号

Analysis of QUAD [FSE 2007]

Bo-Yin Yang, Owen Chia-Hsin Chen, Daniel J. Bernstein and Jiun-Ming Chen

QUAD はフランステレコム等が最近提案したストリーム暗号である。状態数のビット数 n に対して指数関数的に安全性が増し、n を十分に大きく取れば安全であることが証明可能であるという画期的な特長を持つ。この発表では、安全性に関する主張は正しいものの、掛かっている係数が驚くほど小さく、n をかなり大きく取らなければならないということを明らかにした。

Differential Cryptanalysis of the Stream Ciphers Py, Py6 and Pypy [Eurocrypt 2007]

Hongjun Wu and Bart Preneel

eSTREAM は、欧州の暗号評価活動 ECRYPT の一環としてストリーム暗号の公募・評価を行なうプロジェクトであり、2008 年 5 月に最終選考結果・報告書が発表される予定である。

Py と Pypy は Biham と Seberry が設計した RC4 に類似の構造のストリーム暗号で、ソフトウェア向け暗号として eSTREAM に応募された。Py は 2.85 cycles/byte、Pypy は 4.88 cycles/byte と動作が高速である。Py6 は Py の内部状態を縮小した小型版である初期鍵設定の時間が Py の約 1/3 と高速である。Pypy は安全性を高めるため、Py の出力の半分を削除した。これら 3 個の暗号に対する攻撃は、内部状態と出力される鍵ストリームが満たす方程式を解くことが出来る。この発表では、利用する初期ベクタの数を増やすことによって解読効率を改善した。Py と Pypy に対する攻撃では鍵、初期ベクタのサイズが 16 bytes のとき、13 bytes の鍵が $2^{-23.2}$ の確率で導出できた。また、鍵、初期ベクタのサイズが 32 bytes のとき、29 bytes の鍵が $2^{-11.45}$ の確率で導出できた。これらの攻撃の結果、Py と Pypy は eSTREAM の Phase 3 には進めなかった。

Differential Cryptanalysis of the Stream Ciphers Py, Py6 and Pypy [Eurocrypt 2007]

Hongjun Wu and Bart Preneel

eSTREAM は、欧州の暗号評価活動 ECRYPT の一環としてストリーム暗号の公募・評価を行なうプロジェクトであり、2008 年 5 月に最終選考結果・報告書が発表される予定である。

Py と Pypy は Biham と Seberry が設計した RC4 に類似の構造のストリーム暗号で、ソフトウェア向け暗号として eSTREAM に応募された。Py は 2.85 cycles/byte、Pypy は 4.88 cycles/byte と動作が高速である。Py6 は Py の内部状態を縮小した小型版である初期鍵設定の時間が Py の約 1/3 と高速である。Pypy は安全性を高めるため、Py の出力の半分を削除した。これら 3 個の暗号に対する攻撃は、内部状態と出力される鍵ストリームが満たす方程式を解くことが出来る。この発表では、利用する初期ベクタの数を増やすことによって解読効率を改善した。Py と Pypy に対する攻撃では鍵、初期ベクタのサイズが 16 bytes のとき、13 bytes の鍵が $2^{-23.2}$ の確率で導出できた。また、鍵、初期ベクタのサイズが 32 bytes のとき、29 bytes の鍵が $2^{-11.45}$ の確率で導出できた。これらの攻撃の結果、Py と Pypy は eSTREAM の Phase 3 には進めなかった。

Passive-only Key Recovery Attacks on RC4 [SAC 2007]

Serge Vaudenay and Martin Vuagnoux

概要: RC4 の受動的鍵回復攻撃の解読性能を従来法より改善した。RC4 は無線通信の国際規格 IEEE 802.11b で規定された WEP と WPA を守るために利用されるストリーム暗号である。WEP に対しては、攻撃者が攻撃用に不正なパケットを流す能動攻撃が可能であったため、能動攻撃を不可能にした改良版が WPA である。しかし、WPA に対しても受動攻撃が有効であることが分かり、2004 年に暗号方式に RC4 の代わりに AES も選べる WPA2 が IEEE 802.11i と

して規格化された。本発表では、自己相関を利用して、状態変数に関する特定の部分の情報を他の部分とは切り離して推定した。その結果、2^{15} 個のパケットを盗聴すれば解読できた。また、探索に必要な計算は従来法より 2^{15}～2^{20} 倍高速化した。

Permutation After RC4 Key Scheduling Reveals the Secret Key [SAC 2007]

Goutam Paul and Subhamoy Maitra

RC4 において状態変数のバイト置換に関する公式を見つけ、それを利用して鍵を求める方法を開発した。RC4 は 8 ビット要素の配列を内部状態変数と持ち、生成した擬似乱数を利用するストリーム暗号である。配列の初期化を行う鍵スケジュール処理(KSA)とそれに続く擬似乱数生成処理(PRGA)で構成される。これらの処理で特徴的なのは、配列要素を配列要素の値に依存して入れ替える shuffle-exchange 機構が中心的役割を果たしていることである。従来の RC4 に対する攻撃は PRGA の弱さを利用するものが多かった。1995 年に A.Roos は、KSA 直後の置換の初期バイトが秘密鍵のある結合と強い相関を持つことを観測したが、そのことを数学的に証明するのは困難だとコメントしていた。本発表では、KSA における交換(swapping)の効果を展開して解析する。その結果、KSA 直後の初期バイトに鍵に依存した強い相関があり、鍵の総数の平方根回程度の計算量で鍵を特定できることを理論的に示した。さらに、ここで示した KSA の弱点は、shuffle-exchange 機構を利用する擬似乱数生成法に特有なものであることを示した。

Two Trivial Attacks on Trivium [SAC 2007]

Alexander Maximov and Alex Biryukov

欧州のストリーム暗号公募選考プロジェクト eStream に提案された TRIVIUM に対し、状態復元や線形判別攻撃を含む暗号解析を行い、有効性を確認するとともに、これらの攻撃が有効でない改良暗号 TRIVIUM/128 を提案した。欧州の暗号評価プロジェクト NESSIE では暗号プリミティブの評価をし、推奨暗号のリストを発表したが、ストリーム暗号に関しては全提案アルゴリズムに安全性の欠陥があり、１つも選べなかった。後継の ECRYPT において、ストリーム暗号の公募評価プロジェクト eStream を実施した。ここで、ハードウェア向きストリーム暗号では、TRIVIUM を含む４方式が選考に残っている。本発表では、内部状態を復元する手法と、線形の識別子(distinguisher)を用いた手法を組み合せて適用した。その結果、状態の復元に $c*2^{83.5}$ 回の計算しかかからない攻撃法を実現した。これは従来より、2^{30} 倍高速である。

Distinguishing Attack against TPypy [SAC 2007]

Yukiyasu Tsunoo, Teruo Saito, Takeshi Kawabata, and Hiroki Nakashima

TPypy が生成する 2^{199} バイトの擬似乱数と真性乱数を区別できることを示した。ストリーム暗号 TPypy(ティールピー)は、欧州のストリーム暗号評価プロジェクト eSTREAM で安全性に関する問題点が指摘された Py(ルー)の改良版であり、E.Biham と J.Seberry によって 2007 年に提案された。擬似乱数生成には"rolling away"というプロセスが使われている。このプロセスは２種類の配列と 1 つの変数を内部変数として状態更新を行い、擬似乱数を生成するものである。本発表では、基本的には Py に対する攻撃法を適用した。そして、真性乱数とは異なる分布を持つ関係式とそれが満たされる内部状態に関する条件式、及び、関係式が出現する確率を示した。その結果、鍵ストリームが 2^{205} ビットあれば真正乱数と識別できることが分かった。

A fast stream cipher with huge state space and quasigroup filter for software [SAC 2007]

Makoto Matsumoto, Mutsuo Saito, Takuji Nishimura, and Mariko Hagita

ソフトウェアに適した高速のストリーム暗号を提案した。最近の PC では、高速の CPU と豊富なメモリが利用できるので、それを活かした高速のストリーム暗号を設計を目指した。発表者らは、欧州のストリーム暗号評価プロジェクト eStream に今回と同様のストリーム暗号を提案しているが、初期設定に時間が掛かるなど性能の低さが響いてスクリーニングで落とされたという経緯があり、残った暗号と比べて遜色のない新アルゴリズムの開発を目指していた。本発表では、線形フィードバック・シフトレジスタ(LFSR)の出力をメモリ付の一様化準群フィルタを通して鍵ストリームを生成した。その結果、周期が $2^{19937}-1$ 以上で、1248 次元空間で均等に分布する性質を持つ鍵ストリームの生成に成功した。本方式は eStream の最終選考候補となっている。

Full Key-Recovery Attacks on HMAC/NMAC-MD4 and NMAC-MD5 [Crypto 2007]

Pierre-Alain Fouque, Gae"tan Leurent and Phong Nguyen

ハッシュ関数に MD4 を使用した場合、HMAC と NMAC はともに、鍵を回復する攻撃が可能であることが示された。HMAC と NMAC は、ハッシュ関数を利用したメッセージ認証子生成法であり、ハッシュ関数が擬似乱数ファミリであるとき安全であることが CRYPTO 2006 に Bellare によって証明されている。しかし、近年の Wang らによる MD4 及び同系の RIPE-MD, MD5, SHA-0, SHA-1 などのハッシュ関数に対する衝突発見攻撃により、ハッシュ関数が擬似乱数ファミリとする仮定が成立しなくなっている。本発表では、初期ベクタ IV を復元し、IV に依存した望ましい条件を満たす差分経路を探索し、その結果を使って鍵を特定した。その結果、2^{88} 回の選択 MAC 出力で NMAC-MD4 の鍵が回復できた。同じ条件で HMAC-MD4 の鍵回復はできないものの MAC の偽造に必要な情報は入手できた。理論的に立派な結果だが、攻撃に必要な計算量が鍵の全数探索を超えているので、現実的な意味は低い。

Hardware-Assisted Realtime Attack on A5/2 without Precomputations [CHES 2007]

Andrey Bogdanov, Thomas Eisenbarth, Andy Rupp

GSM で使用されているストリーム暗号 A5/2 に対する攻撃が最近提案されているが、攻撃中に行う連立線形方程式の効率解法である Gauss-Jordan 法の専用 ASIC チップを設計し、性能を評価した。欧州で広く使われている携帯電話の規格 GSM では元々ストリーム暗号 A5/1 が使われていたが、欧州外に GSM 携帯を輸出する際、輸出管理対策として意図的に安全性を低くした A5/2 が開発・実装された。A5/2 の仕様はリバースエンジニアにより 1999 年に公開された。A5/2 に対する最初の攻撃は 1999 年の Goldberg らによるもので、1326 フレーム離れた 2 個の平文フレームを利用するものだった。Crypto 2003 で Barkan と Biham らは、guess-and-determine 法による A5/2 に対する暗号文単独攻撃を発表した。この攻撃では、全ての guess に対する事前計算が必要だった。そこで、A5/2 の攻撃に必要な線形方程式系を求めて解く専用ハードウェアを開発した。LSE Solver 要素を実現するため、Gauss-Jordan アルゴリズムの並列ハードウェアの ASIC チップを設計する。ソースは VHDL で書き、VST 標準ライブラリを使って、UMC L180 0.18μ 1P6M ロジックプロセスで合成した。合成には Synopsis Design Compiler version-2006.06 を使用した。LSE Solver の動作周波数は 256MHz とした。事前計算無しで、約 1 秒で秘密の初期状態を復元した。

A Key Recovery Attack on Edon80 [Asiacrypt 2007]

Martin Hell and Thomas Johansson

Edon80 は欧州のストリーム暗号評価プロジェクトである eSTREAM に提案され、設計を変更することなく、現在、最終選考に残っているハードウェア向けストリーム暗号である。鍵長 80 ビット、初期ベクトル長 64 ビットであり、80 個の構成要素を結合した新しい構造を採用している。この発表では、内部状態である要素が高い確率で繰返し現れることを利用することによって、2^{69} 回の状態更新の計算量で鍵を復元できることを示した。

(Short talk) Differential Fault Analysis of Trivium [FSE 2008]

Michal Hojsik and Bohuslav Rudolf

欧州のストリーム暗号評価プロジェクトeSTREAMに提案され、評価されているハードウェア向きストリーム暗号Triviumに対し、差分故障攻撃を適用した。実験の結果、ランダムな位置で起きる43回の誤動作(故障)で内部状態と秘密鍵を特定できた。攻撃は選択暗号文攻撃が可能な場合に有効である。攻撃に必要となる演算コストは小さくまた容易に実装可能な攻撃手法である。

Guess-and-Determine Algebraic Attack on the Self-Shrinking Generator [FSE 2008]

Blandine Debraize and Louis Goubin

Self-Shrinking Generator(SSG)はEurocrypt 1994で提案されたストリーム暗号で、線形フィードバック・シフトレジスタ(LFSR)が利用されている。SSGに対して、推測・決定攻撃が可能であることが示されているが、この発表では、LFSRのハミング重みが5以下という制限の元で攻撃効率を高める方法を提案した。この攻撃法では、連立方程式を代数的に解くためのフリーソフトであるSAT solverが利用される。

New Form of Permutation Bias and Secret Key Leakage in Keystream Bytes of RC4 [FSE 2008]

Subhamoy Maitra and Goutam Paul

RC4は広く利用されているストリーム暗号の一つで、鍵セットアップ(KSA)の後、擬似乱数生成(PRGA)を行うという２段階の動作を行う。従来から、KSA後の状態S[y]に偏りがあることが知られ、それを利用した攻撃法が提案されてきたが、致命的ではないと考えられてきた。この発表では、鍵に関する情報に関わりなく、S[S[y]]に偏りが生じ、1番目、256番目及び257番目の出力バイトで、状態の偏りが最も大きくなることを明らかにした。

Efficient Reconstruction of RC4 Keys from Internal States [FSE 2008]

Eli Biham and Yaniv Carmeli

ストリーム暗号RC4に対し、仮定と推測を利用することで効率を従来より改善した攻撃法を提案した。計算機実験の結果、40ビット鍵では0.02秒で成功確率86.4%で解読でき、解読に失敗した場合でも、鍵に関する情報が得られることを示した。

(Short talk) Some Remarks on the Salsa20 Core Function [FSE 2008]

Julio Cesar Hernandez-Castro, Juan M. E.Tapiador,
and Jean-Jacques Quisquater

Salsa20 は欧州のストリーム暗号評価プロジェクトeSTREAMに投稿され、大きな攻撃も発表されずに最終選考フェーズに残っている。この発表では、Salsa20 のコア関数が2^{32}個の入力に対して剰余2倍算として振舞う性質を発見し、第２原像計算困難性を満たさないことを指摘した。

New Features of Latin Dances: Analysis of Salsa, ChaCha, and Rumba [FSE 2008]

Jean-Philippe Aumasson, Simon Fischer, Shahram Khazaei, Willi Meier,
and Christian Rechberger

eSTREAMに投稿されたストリーム暗号Salsa20には、フルスペックの20段を8段に縮小したSalsa20/8も含まれている。また、eSTREAMには投稿されていないがSalsa20を改良したChaChaとSalsa20の構成要素を利用したハッシュ関数Rumbaも発表されている。この発表では中立ビットを利用した差分解読法を適用することによって、Salsa20/8とChaChaの7段縮

小版を破り、Rumbaの3段縮小版に対する衝突が発見できる可能性を理論的に示した。

Correlated Keystreams in MOSTIQUE [SASC 2008]

Emilia Kasper, Vincent Rijmen, Tor E. Bjorstad, Christian Rechverger, Matt Robshaw, and Gautham Sekar

MOSTIQUE は、eSTREAM に応募されたストリーム暗号の一つである。本発表では、related-key attack で 2^{38} の操作で鍵ストリームが復元可能となってしまうことを示した。本攻撃で、攻撃者は秘密鍵を用いて生成された暗号文とその秘密鍵の related-key で生成された暗号文の 2 つの出力を観測することが出来るという仮定の下では、2^{69} の操作を行って、96 ビットの鍵ストリームの復元が可能である。また、上記に加え攻撃者は更にもう一つの related-key で生成された暗号文の観測が可能であるという仮定の下では、探索コストを 2^{38} 軽減することが出来る。また、この方式の中で使われている related key は、non-related key の設定下であっても鍵の全数探索のコストをやや軽減することが出来る。

An Improved Estimate of the Correlation of Distinguisher for Dragon [SASC 2008]

Joo Yeon Cho

Dragon は eSTREAM の最終フェーズに残ったストリーム暗号の一つである。方式の中で用いられている F 関数は、鍵生成および内部状態の更新における安全性を左右する中心的な関数である。本発表では、この F 関数に線形解読法を適用した結果、従来結果に比べ、2^9 倍ほど高い相関関係があることが示された。本発表で示した攻撃手法は線形関数による相関関係を持つような非線形関数の解析に適用できる。

On the Security of Optimal Decimation Components [SASC 2008]

Blandine Debraize

ストリーム暗号に用いられる擬似乱数生成の強度を上げるために用いられる圧縮方式では、一般的にその出力レートと安全性の間にはトレードオフの関係がある。ここでは eSTREAM の最終フェーズに残ったストリーム暗号の一つである DECIM の中で用いられる圧縮方式 ABSG をターゲットとし、equations retrieval attack により解析を行い従来結果に比べ、メモリコストを $O(2^{n/2})$ に比べ、$O(2^{n/4})$ に削減できることを示し、ABSG 圧縮方式は、SSG ほど安全で無いことを示した。

Chosen IV Statistical Analysis for Key Recovery Attacks on Stream Ciphers [SASC 2008]

Simon Fischer, Shahram Khazaei, and Willi Meier

eSTREAM の最終フェーズに残ったストリーム暗号 Grain-128 および Trivium に対し、選択初期ベクタ(IV)を用いた統計学的解析による攻撃結果が発表された。IV 設定の繰り返し部分

を 256 から 180 以下にしたもの、また 1152 から 672 に削減したものについて解析し、数ビットの鍵ストリームの推定では、全数探索よりも解読効率が良いという評価を得た。IV の繰り返し部分がフルビットの場合は本手法では、計算コストの削減は出来ない。

Analysis of Grain's Initialization Algorithm [SASC 2008]

Christophe De Canniere, Ozgul Kucuk, and Bart Preneel

sSTREAM の最終フェーズに残ったストリーム暗号 Grain に対する 2 種類の解析結果を示した。1 つは初期化の部分のスライド特性を指摘し、これを利用し鍵ストリームの回復に全数探索の約半分の探索コストで回復可能であることを示した。2 つ目は、初期化部分の差分特性を指摘し、差分攻撃を用いて 2 つの related key と 2^{55} の選択 IV ペアを用いると 2^{9} 個の鍵ストリームの回復が可能であることを示した。

Comparing and Optomising Two Generic Attacks on Bivium [SASC 2008]

Tobias Eibach, Enrico Pilz, and Sebastian Steck

ストリーム暗号 Bivium に対して２種類の汎用攻撃法攻撃法を適用し、有効性を検証した。Bivium は eSTREAM の最終フェーズに進んだ Trivium の縮小版であり、内部状態が 177 ビット、鍵長が 80 ビットである。初期ベクトルに対して 4*177 回の操作を行って、状態の初期化を行う。２種類の攻撃法とは、Bivium の動作を記述する代数方程式を SAT Solver で解く方法と、状態更新と出力が満たすべき条件を BDD(Binary Decision Diagrams)を利用して解く方法である。計算機実験で両攻撃法による内部状態の推定に掛かる時間を比較したところ、SAT Solver を用いた方法がずっと速く、200 ビットのキーストリームから変数 50 個の方程式を解く時間は SatElite preprocessor を使うと、0.26 秒である。

RC4 Keystream Always Leaks Information about the Hidden Index j [SASC 2008]

Riddhipratim Basu, Shirshendu Ganguly, Subhamoy Maitra, and Goutam Paul

SSL や TLS を初め、広く利用されているストリーム暗号 RC4 の脆弱性については多くの報告があり、鍵セットアップや初期の鍵ストリームにおける分布の偏りが指摘されている。この発表では、初期に限らず、常に鍵ストリームから秘密の内部変数 j に関する情報が漏れていることが示された。これらの情報は、他の内部変数 i や j との関係式の形で表される。

Treatment of the Initial Value in Time-Memory-Data Tradeoff Attacks on Stream Ciphers [SASC 2008]

Orr Dunkelman and Nathan Keller

Time-Memory Tradeoff 攻撃は、共通鍵暗号系に対する鍵の全数探索を事前に計算した表を用いることで効率化する方法である。この発表では、複数の初期ベクタ(IV)を公開情報として扱うことで、鍵長と IV が n ビットのとき、時間、メモリ、データの複雑度を $2^{4n/5}$ に抑

えることに成功した。これは従来の 2^n という下限を更新したものである。

Algebraic Description and Simultaneous Linear Approximation of Addition Modulo 2^n [SASC 2008]

Nicolas T. Courtois and Blandine Debraize

共通鍵暗号の基本演算には、非線形 S-box やブール演算に加え、剰余加算が多用される。暗号強度の解析において、線形近似がしばしば利用されるが、剰余加算が使われている場合、それをどのように線形化するのが最適かは分かっていない。著者らは、多重・同時線形近似の概念を導入して、出力または入力の一方がある制約を満たすときに、剰余加算をブール演算上で部分的または完全に線形化できることを示した。この線形化を SNOW 2.0 の鍵ストリームに適用し、2^{294} 回の動作の計算量で鍵ストリームが復元できるという評価を得た。これは鍵の全数探索の計算量 2^{256} より大きいものの、同程度の大きさであり、現在の鍵長を短縮すべきでないことを意味する。

Equivalent Representations of the F-FCSR Keystream Generator [SASC 2008]

Simon Fischer, Willi Meier, and Dirk Stegemann

F-FCSR は eSTREAM の最終フェーズに残ったハードウェア向き暗号で、線形フィードバック・シフトレジスタにキャリーを加えた FCSR を利用している。最近、F-FCSR に Fibonacci 型または Galois 型の等価表現が見つかっており、それらの表現を利用することで解読効率が従来より改善するか否かが問題となっていた。この論文では、新たな等価表現に対して線形化を利用した攻撃を適用した結果、解読効率の改善には直接寄与しないという評価になった。ただし、新しい表現は今後のさらなる解析には有益であるとしている。

Construction of FCSR algebraic equations and empirical analysis [SASC 2008]

Benjamin Pousse and Marine Minier

F-FCSR は eSTREAM の最終フェーズに残ったハードウェア向き暗号で、キャリー付きのフィードバック・シフトレジスタ(FCSR)を利用している。F-FCSR に対しては、IV モードに対する代数攻撃が２種類提案されていて、攻撃には成功していないが、パラメータの選び方が悪いと安全性が損なわれる可能性が指摘されている。この発表では、FCSR を記述する代数方程式を立て、いくつかの長さに対して計算機実験で安全性を確かめてみた。その結果、eSTREAM に投稿された F-FCSR のパラメータが注意深く選ばれたものであることが確認できた。

Cache Timing Analysis of HC-256 [SASC 2008]

Erik Zenner

キャッシュ・タイミング攻撃はキャッシュに掛かる時間の測定を利用する攻撃法であり、

AES のような S-box 処理を利用する暗号に有効であることが知られている。この攻撃に対する対策として、実装の仕方を工夫することが提案されている。この発表ではアプローチを変え、特別な実装上の対策をしないとして、どのように暗号を設計すればキャッシュ・タイミング攻撃に対して強くなるか、eSTREAM の最終フェーズに残った HC-128 を対象に検討した。その結果、次のような設計を推奨した。(1)S-box やテーブル参照は避ける。(2)テーブル参照をするときは、１回の機能呼び出しで出来るだけ多くのテーブルを参照するようにする。(3)キャッシュ参照で得られる情報量より内部状態サイズが大きくなるようにする。(4)キャッシュ参照で LSB が不確定である事実を利用する。

Susceptibility of eSTREAM Candidates towards Side Channel Analysis [SASC 2008]

Benediky Gierlichs, Lejla Batina, Christophe Clavier, Thomas Eisenbarth, Aline Gouget, Helena Handschuh, Timo Kasper, Kerstin Lemke-Rust, Stefan Mangard, Amir Moradi, and Elisabeth Oswald

eSTREAM に投稿されたソフトウェア向け及びハードウェア向け、各 8 個、計 16 個のストリーム暗号に対してサイドチャネル攻撃に対する安全性を同じ基準で評価した。評価の枠組みは次の通り。

・攻撃者は次の３要件を満たす。

(1)IV と鍵ストリームが観測できる。IV を選択する権利はオプションとする。

(2)動作のリセットが可能。

(3)目的は鍵の復元。

・攻撃法

(1)タイミング攻撃

(2)電力解析 – 漏洩モデル、SPA、DPA について規定。

・ 対策のコスト

結果を総合的に見て評価が高いのは、ソフトウェア向けでは CryptMT と Rabbit、ハードウェア向けでは F-FCSR、Grain、Moustique、Trivium だった。

Comparison of FPGA-Targeted Hardware Implementations of eSTREAM Stream Cipher Candidates [SASC 2008]

David Hwang, Mark Chaney, Shashi Karanam, Nick Ton, and Kris Gaj

Xilinx Spartan 3 FPGA ボードを用いて最終選考に残っている全てのストリーム暗号を対象として、ハードウェアの効率比較を行った。最小エリア/最大エリアでの処理速度は Grain および Trivium が高速性に関して優れていた。低いエリアのバランスに関しては Mickey も優れていた。

Hardware performance of eStream phase-III stream cipher candidates [SASC 2008]

Tim Good and Mohammed Benaissa

最終フェーズに残ったストリーム暗号のハードウエア評価結果。0.13μm Standard CMOS 上に設計し、処理速度、ゲート数、消費電力、最大スループット、など様々な比較評価を行っている。無線 LAN の利用環境下を想定した場合の性能比較や low-end な RFID/WSN などアプリケーションでの利用環境下を想定した場合の性能比較などを示している。結果、最高クロック数は Trivium, WLAN を想定した場合のパフォーマンスおよび RFID を想定した場合のパフォーマンスは Grain 80、Flexibility は Trivium、Simplicity は Mickey128 という結果。

On the Parallelization of the MICKEY-128 2.0 Stream Cipher [SASC 2008]

Deian Stefan and Christopher Mitchell

eSTREAM の最終フェーズに残っているストリーム暗号 MICKEY の高速化の実装結果。Xilinx Virtex-II Pro FPGA ボートを利用し、2 並列処理を施すことにより、スループットが 560 Mbps, erea-efficient が 392slices という結果を得た。

Lightweight Implementation of the S-Box in Pomaranch Stream Cipher [SASC 2008]

Cees J.A. Jansen, Tor Helleseth, and Alexander Kholosha

Pomaranch は鍵ストリーム生成部分に複雑な回路計算を含まずハードウェア実装に適したストリーム暗号である。通常の構成ではトータルで約 6300 ゲート必要とする。本発表ではアルゴリズムの中で用いている S-box のゲート削減を施すことにより、全体として約 200 ゲート(2 入力 Boolean ゲート数)程度に収めることが出来る。S-box は $GF(2^9)$ 上の乗算群の逆元を利用して構成される。これを $GF(2^9)$ 上での表現を利用することにより必要となるゲート数を削減することが出来た。

A low-cost implementation of Trivium [SASC 2008]

Nele Mentens, Jan Genoe, Bart Preneel, and Ingrid Verbauwhede

レイアウトの違いによるチップサイズの違いを検証し、効率的なレイアウトを施すことにより、チップサイズを小さく抑えることが出来ることを示した。比較対象として用いたのは、Standard Cell Core および C2 MOS フリップフロップを用いた Dynamic Core. 1 枚のチップの上に両デザインの core を搭載した結果、C2 MOS フリップフロップを用いた Dynamic Core の方がそのサイズを小さく抑えられることが分かった。

A New Approach to Keystream Based Cryptosystems [SASC 2008]

Orhun Kara and Imran Erguler

ノイズと誤り訂正符合を利用したストリーム暗号の新しい構成を提案した。この暗号系では、有限状態モデルで作った鍵ストリームにランダムノイズを加えて雑音入り鍵ストリー

ムを作り、誤り訂正符合で符号化された平文にこれを加算して暗号文とする。ここで、送信者と受信者はランダムノイズがどのようなパターンに限定されるかの情報を共有しておく。この構成を実現する方法として、Accumulation Model、Confusion Model、Feedback Model の３種類を示し、安全性を検討した。

Stretching the Speed Asymmetry of Edon80 [SASC 2008]

Danilo Gligoroski

eSTREAM の最終フェーズに残った８個のハードウェア向け暗号について、Xilinx tool ISE WebPACK ver.9.2.04i 上での実装で実行速度の非対称性を調べたところ Edon80 が 725 で最大だった。この非対称性とは、ソフトウェア実装で 1 バイト暗号化するのに必要な cycle 数をハードウェア実装での cycle 数で割ったもので、Edon80 では、各 cycle 数は 5,800 と 8 だった。Edon80 のパイプライン処理数 80 をふやすことで、非対称性がどこまで上がるか試してみた、その結果、パイプライン処理 8000 で 72587 となり、それを超えると合成ツールがまともに動かなくなることが分かった。

EnRUPT First all-in-one symmetric cryptographic primitive [SASC 2008]

Sean O'Neil

EnRUPT はバイト単位の演算しか使わない、単純でスケーラビリティのある暗号プリミティブであり、ブロック暗号、ストリーム暗号、ハッシュ関数などに利用できる。時刻 r における状態を x_r、鍵を k_r とすると、状態更新は次の式で表せる。$x\_r{+}{=}rotr(2*x_{r-1}+x_{r+1}+k_r+r,8)*9+k_r$ 。8 ビット･プロセッサでの実装性能を比較したところ、より少ない RAM で、AES の 4 倍以上、SHA-1 の 30 倍の処理速度を実現した。さらに、発表者はこの方式は、特許化できる要素は含んでいないと主張している。

ChaCha, a variant of Salsa20 [SASC 2008]

Daniel J. Bernstein

Salsa20 は eSTREAM の最終フェーズに残ったソフトウェア向け暗号であり、フルスペックで 20 段であるが､段数を減らしたセキュリティを低める代わりに実装性能を高めた Salsa20/8 や Salsa20/12 も提案している。この発表では、Salsa20 の安全性向上のため拡散効果を高めた ChaCha20 を提案した。両暗号方式を実装した結果、実装速度は同等であった。

3. ブロック暗号

Related-Key Rectangle Attacks on Reduced AES-192 and AES-256 [FSE 2007]

Jongsung Kim, Seokhie Hong and Bart Preneel

Related-Key Rectangle Attack と呼ばれる秘密鍵同士にある関係があることを仮定した場

合の攻撃手法に対する解析結果。2 related-key を想定した場合の AES-192 について 8 段、64 若しくは 256 related-key を想定した場合の AES-192 について 10 段、4 related-key を想定した場合の AES-256 について 9 段の解析が行えることを示した。AES-192 に関しては 4 related-key を想定した場合での 8 段の解析が示されていたが、本発表では必要となる related-key を 4 から 2 に削減することが出来ている。また、AES-192 について 10 段までの解析結果については初めての結果である。AES-256 の解析結果については従来結果に比べ、data complexity・time complexity 共にコンパクトに抑えることが出来る方式となっている。

A New Attack on 6-Round IDEA [FSE 2007]

Eli Biham, Orr Funkelman and Nathan Keller

6 段に短縮した IDEA に対して、従来よりも高い効率で鍵推定が可能であることを示した。5.5 段に対しては、2^{34} 個の選択平文と暗号化約 2^{127} 回分の計算で鍵が推定可能で、全数探索に比べ解読効率は 2 倍になる。また、5 段に対しては、既知平文 $2^{18.5}$ 個と暗号化約 2^{103} 回分の計算、または、既知平文 16 個と暗号化約 2^{114} 回分の計算で鍵が推定できる。

128 bit Blockcipher CLEFIA [FSE 2007]

Taizo Shirai, Kyoji Shibutani, Toru Akishita, Shiho Moriai and Tetsu Iwata

CLEFIA はソニーと名古屋大学が共同開発した 128 ビットブロック暗号であり、鍵長は 128 ビット・192 ビット・256 ビットの 3 種類で、それぞれ対応する段数は 18 段・22 段・26 段となっている。Feistel 構造が利用されているが、従来よく用いられていた 2 分岐ではなく 4 分岐する構造を採用し、F 関数の中で用いる s-box を 2 種類にするなどの点で独自性がある。安全性に関する自己評価では、従来提案されている攻撃手法が単純には適用できないとしている。実装効率は、AES など従来提案方式と比較して、ソフトウェアに関しては同程度かやや劣るものの、ハードウェアに関しては有利としている。

New Light-Weight DES Variations Suited for RFID Applications [FSE 2007]

Axel Poschmann, Gregor Leander, Kai Schramm and Christof Paar

DES をベースに組込みに適したアルゴリズムを提案。HW の縮小化の為に 8 種類あった s-box を一種類の S-box で代替する。Kim らによって示されている要件を満たす S-box を提案。実際、この S-box で代替した場合、HW の領域を 20%抑えることが出来る。

Feistel Networks made Public, and Applications [Eurocrypt 2007]

Yevgeniy Dodis and Prashant Puniya

Feistel 型ブロック暗号の安全性に関しては、ラウンド関数を擬似ランダム関数とすると 4 段で擬似ランダム置換となることを示した Luby-Rackoff の研究がある。しかし、実際のラ

ウンド関数は擬似ランダム関数ではないので、この条件を緩和して、ラウンド関数を予測不能(unpredictable)関数にするという An-Bellare のアイデアが出されていたが、結論は出ていなかった。本発表では、ラウンド関数が予測不能関数であるとき、ブロック幅を 2n ビットとすると、Feistel 構造は ω(log n)段で擬似ランダム関数になることを示した。

Linear Cryptanalysis of Non Binary Ciphers with an Application to SAFER [SAC 2007]

Thomas Baigneres, Jacques Stern, and Serge Vaudenay

非バイナリ・ブロック暗号に適した線形解読法を開発した。バイナリであるブロック暗号とはビット単位の排他的論理和と S-box だけで構成されるものであり、剰余演算やデータ依存のビット回転などを含むものは非バイナリ・ブロック暗号と呼ぶ。非バイナリ暗号の扱い方を示した論文は今まで、Granboulan らによる FSE 2006 の論文しかなく、差分解読法に関するもので、線形解読法に関する論文は無かった。本発表では、線形解読法を任意の集合に適応させた。その結果、SAFER に対する最も良い攻撃法が実現できた。

MRHS Equation Systems [SAC 2007]

Havard Raddum

非線形要素が S-box だけのブロック暗号を記述する MRHS 方程式を提案する。近年の暗号解読分野では非線形方程式解法による攻撃の研究が盛んである。GF(2)上の多変数多項式(MP)を代数的標準形(ANF)で記述するのが主流だが、実際に非線形方程式をどのように解くのが最適かは不明で、しばしば計算規模が大きくなり実用的でなかった。本発表では、GF(2)上の変数を選択して複数の線形結合で作った配列は複数の値を取る。このように線形方程式で書いたときの右辺が複数の値を取りうる形式である Multiple Right Hand Sides(MRHS)を利用した。この結果、従来の N.Courtois の方法やグレブナー基底を利用した場合より、解読方程式の記述が単純化される。DES について具体的に記述を示した。

Cryptanalysis of White-Box DES Implementations with Arbitrary External Encodings [SAC 2007]

Brecht Wyseur, Wil Michiels, Paul Gorissen, and Bart Preneel

DES の White-Box 実装から暗号化鍵を復元する方法を開発した。White-box 実装とは、暗号化鍵を守るため、鍵を設定した暗号アルゴリズムを等価な参照テーブルのネットワークに変換することで難読化する実装法である。本発表で、差分解読法を難読化したラウンドに適用した。その結果、2^{14} の計算量で解読することができた。

Improved Side-Channel Collision Attacks on AES [SAC 2007]

Andrey Bogdanov

AES に対する内部状態で起こる衝突を利用した電力解析を提案した。K.Schramm らはブロック暗号の S-box 入力における衝突を利用した攻撃を提案し、FSE 2003 で DES、CHES 2004 で AES に対する電力解析結果を示した。AES の解析では、第 2 段目の各 S-box に対する 1 バイト入力を電力波形から識別し、比較することで衝突の有無を推定した。本発表では、入力が同じかどうか(衝突の有無)を電力波形から推定する対象を異なる S-box に拡張した。また、鍵推定には無向グラフを利用した探索を行なった。この結果、6 回の測定と $2^{37.15}$ ステップのオフライン計算により、確率 0.85 で解読に成功した。測定を 7 回に増やすと必要なオフライン計算は $2^{34.74}$ ステップで確率 0.99 での解読に成功した。この攻撃でメモリは無視できるほどしか必要としない。

The Security of the Extended Codebook (XCB) Mode of Operation [SAC 2007]

David A. McGrew and Scott R. Fluhrer

2004年に提案されていたXCB mode of Operationの安全性評価を行った。具体的には、IEEE SISWGに提案(2006年9月)・Key storageの効率化・安全性証明の簡素化・nonce modeの提示とその中でのXCB mode の安全証明などを行なった。nonce mode では平文の長さがブロック暗号の長さの2倍よりも小さな場合であっても安全に利用することが出来る。XBC mode は内部関数として、Galois Counter Mode(GCM) of operation を利用しており、ハードウェア・ソフトウェア両面での効率性の高いモードであるとしている。

A Generic Method to Design Modes of Operation Beyond the Birthday Bound [SAC 2007]

David Lefranc, Philippe Painchault, Valérie Rouat, and Emmanuel Mayer

新しい mode operation の提案。任意の generator の minimal distance d が 1 以上の linear code のマトリックスから PRF (Pseudo Random Function)を構成することが出来、この PRF を利用して新しい mode of operation である MEMO を構成することが出来る。MEMO のセキュリティレベルは、構成部品となっている PRF のセキュリティレベルと同等である。PRP(Pseudo Random Permutation)から PRF を構成する汎用的な手法が提案されており、既存方式として PRP から PRF を構成するモードとして知られる CENC も彼らの手法の特別なケースとして捉えることも出来るとしている。

How to Steal Cars – A Practical Attack on KeeLoq [Crypto 2007](Rump session)

Eli Biham, Orr Dunkelman, Sebastiaan Indesteege, Nathan Keller, *and Bart Preneel*

KeeLoq という高級車などの電子鍵に近年導入されている軽量のブロック暗号に対する攻撃。KeeLoq はブロックサイズ 32 ビット、64 ビット鍵で GM・ホンダ・トヨタなど大手会社の車の鍵に導入されている。発表されたのは、Key Recovery Attack で スライド攻撃と meet-in-the-middle 攻撃とを組み合わせ、2^{16} の既知平文(もしくは暗号文)を用いて、$2^{44.5}$ 暗号化程度の演算量と 3MB 以下のメモリを用いて解くことが出来るとしている。

1 万€と 50 個の dual core machines があれば、約 2 日程度で攻撃が可能であるとのこと。本結果は、従来示されていた結果に比べ 500 倍程度速く解くことが出来る。

Invertible Universal Hashing and the TET Encryption Mode [Crypto 2007]

Shai Halevi

TET(for linear-Transformation; ECB; linear-Transformation) と呼ばれる mode of operation の提案。構成は、hash-ECB-hash 系の形をしており、効率と言う点では hash-CTR-hash に近い。hash-ECB-hash を構成するために、新たにブロック単位での universal hash の構成を提案、TET の中に組込んでいる。また、OMAC の若干の改良版も考案し TET の中に利用している。

A First-Order DPA Attack Against AES in Counter Mode with Unknown Initial Counter [CHES 2007]

Josh Jaffe

AES のカウンタモードに対して、カウンタの初期値とブロック暗号の出力値を知ることなく、鍵を復元する電力差分解析を開発した。従来の 1 次 DPA では、平文または暗号文のどちらかが必要だった。カウンタモードを攻撃対象とし、平文の下位 16 ビットに相当する 2 個の第 1 段 S-box 入力の規則性に着目する。連続する 216 個の入力に対する消費電力波形を使った DPA で、暗号化鍵 128 ビットを特定できた。実際に使うデータは、216 個から選らんだ連続する 213 個である。DPA でありながら平文・暗号文の両方を不要とする点に新規性がある。

Differential Behavioral Analysis [CHES 2007]

Pascal Manet, Bruno Robisson

行動差分解析(DBA)とは、電力差分解析(DPA)に故障利用攻撃の一種である safer-error 攻撃を組合わせた、サイドチャネル攻撃の一種である。DBA は AES の実装に対するシミュレーションの結果、非常に有効であることを確認した。スマートカードなどに対する実装攻撃には、DPA のような受動的攻撃、回路の誤動作を利用する故障攻撃、チップ・デザインを直接観測する破壊攻撃などがある。故障攻撃の中でも計算を正常に実行したか否かをチェックするのは safe-error 攻撃(SEA)だけである。そこで、故障攻撃の一種である SEA と DPA

を組合わせた攻撃法を Differential Behavioral Analysis
(DBA)を開発し、AES を実装した回路に適用した結果、現実的な環境で DBA が成功することが分かった。例えば、8 ヶ所より少ない誤動作を繰返し引き起こすことで全鍵ビットが復元できた。また、1 ビットだけの誤動作が引き起こせるとき、最低 16 回の測定で拡大鍵の 8 ビットが復元できた。

Collision Attacks on AES-based MAC: Alpha-MAC [CHES 2007]

Alex Biryukov, Andrey Bogdanov, Dmitry Khovratovich, Timo Kasper

ブロック暗号を利用した認証子生成方式の Alpha-MAC に対し、内部衝突に着目した電力攻撃を行い、署名の偽造に成功した。Alpha-MAC は AES のラウンド関数を利用した MAC(メッセージ認証子)であり、既に AES の実装があれば容易に MAC の機能が追加できる。さらに、安全性に関しても同じ MAC 値を持つ同じサイズのメッセージは 5 ブロック以上(1 ブロックは 128 ビット)であることが保証されている。DPA を適用したところ、Alpha-MAC の鍵付き演算部以外の内部状態を DPA で推定する方法を開発でき、29 回の既知メッセージに対する測定だけで、各々、4 ブロックと 1 ブロックで同じ MAC 値を持つメッセージを発見した。衝突発見に内部状態を利用するアイデアが面白い。

Secret external encoding do not prevent transient fault analysis [CHES 2007]

Christophe Clavier

通常のブロック暗号の前後を秘密の符号化で挟むとブロック暗号の入出力を隠すことで安全性が高まると考えられていたが、故障攻撃によって攻撃できることを DES と Triple DES の例で示した。Boneh らは、Eurocrypt 1997 で内部での計算誤りを利用して中国人剰余定理を使った RSA 暗号の実装が攻撃できることを示し、Biham らは DES に対しても同様に攻撃できることを示した。このような故障利用攻撃に対するブロック暗号の防御法として、ブロック暗号の前後を秘密の 1 対 1 写像で挟む方法が考案され、実際に GSM や pay-TV で実際に使われている。特定の操作において計算誤りを起こせると仮定し、その誤りの伝達を利用して内部状態を推定する方法を開発し、DES と Triple DES の例で有効性を検証した。未知の変換を含む暗号化に対する故障攻撃は新しい。

Two New Techniques of Side-Channel Cryptanalysis [CHES 2007]

Alex Biryukov, Dmitry Khovratovich

2 つの新しいサイドチャネル解読法である、不可能衝突攻撃と多重衝突攻撃を開発し、AES は各段の 128 ビット拡大鍵全部を守る必要性を指摘した。ブロック暗号に対する通常の電力解析では、最初と最後の数段が攻撃対象になるので、経済的に防御するには、最初と最後の数段だけマスクする方法が考えられる。このように防御対策を施した実装は、既知の暗号を未知の 1 対 1 変換で挟んで安全性を高めるのと同等の効果がある。これらに対し、

ブロック暗号の攻撃法である不能差分攻撃と部分関数衝突攻撃を電力解析に応用した攻撃法を適用した。その結果、最初の2段を完全にマスクしたAESに対する不可能衝突攻撃で、75回の測定と2^{32}回の計算で拡大鍵の32ビットが推定できた。最初の4段を完全にマスクしたAESに対する多重衝突攻撃で、2^{32}回の測定と$2^{44.5}$回の計算で拡大鍵96ビットが推定できた。

PRESENT: An Ultra-Lightweight Block Cipher [CHES 2007]

A. Bogdanov, L.R. Knudsen, G. Leander, C. Paar, A. Poschmann, M.J.B. Robshaw, Y. Seurin, C. Vikkelsoe

十分安全性で、非常に計算コストが低い、64ビットブロックのブロック暗号PRESENTを設計した。暗号化速度は eStream で選考中のトップレベルのストリーム暗号と同等である。NISTによるAESの標準化以降、新たなブロック暗号の必要性は低下した。しかし、制約が非常に大きいRFIDやセンサ・ネットワークのような環境ではAESも十分とは言えず、より軽量なブロック暗号の必要性は存在する。この要求に応え、安全性に関する要求を適度に抑えた、ブロック長64ビット、鍵長80ビットのブロック暗号PRESENTを開発した。全体は31段SPN構造で、32並列の4ビットS-boxと64ビット幅の置換を繰り返す。鍵スケジュールもon-the-flyで計算出来るようにした。VHDLのソースにVST標準ライブラリを使い、UMC L180 0.18μ 1P6M ロジック・プロセスで実装した。シミュレーションには Mentor raphics Modlsim SE PLUS 5.8c、合成には Synopsys Design Compiler version Y-2006.06 を使用した。既存の攻撃法である差分解読／線形解読、代数攻撃、関連鍵攻撃に対する安全性を確認した。スループットはチップサイズ1570GE、電力消費5μWで200Kbpsを達成した。128ビット鍵AESの小型実装では、0.35μm、3400GE で 12.4Kbps なのではるかに軽量である。軽量性では AES に勝っているが、それだけに安全性評価が定まるには最低でも 2 年程度の時間が必要である。

On the Power of Bitslice Implementation on Intel Core2 Processor [CHES 2007]

Mitsuru Matsui, Junko Nakajima

インテルの Core2 プロセッサの特性を活かしたビットスライス実装によって、3GPP や GPS などの携帯電話で使われるKASUMIや国際標準暗号AESの小型高速実装を実現した。ビットスライス実装は、BihamがRISCチップ上でDESの暗号化を並列にして高速にするために提案された。ビットスライス実装は S-box のテーブル参照を必要としないから、タイミング攻撃に耐性があることや、ブロック暗号のカウンタモードに適していることから、近年注目されている。しかし、実際にはビットスライスは実用的にはほとんど使われていない。その理由は、ビットスライスに必要なデータ形式の変換処理のコストが大きいからであった。そこで、Intel Core2 プロセッサの SIMD 構造を利用して、データ形式の変換を効率化することを試みた。KASUMI の実装で 4 倍の高速化、AES では 9.2 cycles/byte という世界

記録を達成した。

AES Encryption Implementation and Analysis on Commodity Graphics Processing Units [CHES 2007]

Owen Harrison, John Waldron

GPU へブロック暗号 AES を高速実装する新しいアプローチを示した。GPU の処理性能の伸びは CPU を上回るものの、今までプログラムの自由度が低かったため、画像処理以外にはあまり利用されなかった。最近は一般用途向けの傾向を強めつつあるが、浮動小数点演算があるだけで、暗号処理を意図した設計にはなっていない。GPU が暗号処理用に向いていると考えられる理由に、並列処理を高速化に活かせることと、CPU に暗号化・復号処理の情報を提示することを避けるという特徴がある。並列処理を活かせる暗号方式として AES を選び GeForce 7900GT 上でラスタ処理ユニットに基づくアプローチで 870.8Mbps を達成した。これは既存の CPU による最良の結果には及ばないが、GPU が広く一般的に利用されていれば、CPU の負荷を軽減するのに活用できる。GPU に暗号処理向けの命令セットが用意されれば、暗号処理性能も向上すると期待できる。

Multi-Gigabit GCM-AES Architecture Optimized for FPGAs [CHES 2007]

Stefan Lemsitzer, Johannes Wolkerstorfer, Norbert Felber, Matthias Braendli

暗号化とメッセージ認証を同時に行う GCM モードで、ブロック暗号に AES を使った場合について、FPGA 上で速度、使用面積、IO 動作のトレードオフを最適化した実装方法を開発した。AES は 2001 年に NIST により FIPS 197 として標準化され、AES の GCM モードは同年、NIST SP 800-38A に記載された。AES の GCM モードの高速実装では、ISCAS 2006 で佐藤が発表した 0.13μm CMOS ASIC 実装による 42.67Mbps という結果がある。速度、使用面積、IO 動作の間のトレードオフを実現すべく、VHDL でコード化、Synplify Pro で合成し、Xilinx ISE に実装した。Xilinx Virtex4-FX100 に 3 種類の鍵サイズをサポートした AES の GCM モードを実装し、スループット 14.1Gbps、実装領域 13.2k-slices(31%)、110MHz 動作の 114-block RAMs を達成した。

An Overview of the ECRYPT AES Security [TFC 2007]

Henri Gilbert

AES の安全性について ECRYPT がまとめた報告書の概要紹介。NIST による AES の決定から 5 年が経ったのを期して、ECRYPT では最新の研究成果を反映した AES に対する安全性評価の現状報告がまとめられ、2006 年 1 月付けで“AES Security Report”として公開された。この発表は報告書の概要を紹介したもので、結論は、サイドチャネル攻撃を別にすると、今まで提案された攻撃法で AES の安全性を脅かすものはないというものだった。技術的に細かく説明したのは、AES の構造、統計的攻撃法である差分解読法／線形解読法／ブーメラン

攻撃、多セット攻撃(Square 攻撃など)、代数攻撃、キャッシュタイミング攻撃など。128ビット鍵 AES に対しては、実質的には 6 段まで攻撃可能で、最も効率的なのは部分和攻撃(Partial Sum)で、2^{35} 個の選択平文と暗号化 2^{44} 回分の計算で攻撃可能と評価されている。この他に 6 段 AES に適用可能な攻撃法は、Square 攻撃(2^{32} 個、2^{72} 回)とブーメラン攻撃(2^{71} 個、2^{71} 回)である。7 段 AES に対しても Gilbert-Minier 攻撃は 2^{32} 個の選択平文で解けるとしているが、計算量が鍵の全数探索の 2^{128} 回とほぼ同じなので現実的な意義はない。ただし、Gilbert-Minier 攻撃は 192 ビット鍵と 256 ビット鍵の 7 段には有効で、ともに 2^{32} 個の選択平文と 2^{144} 回分の計算で攻撃可能である。

Algebraic Cryptanalysis of the DES [TFC 2007]

Nicolas Courtois and Gregory Bard

ブロック暗号 DES に対する代数攻撃の発表。DES に対して鍵に関する連立方程式を解く方法として、ガウス消去法を用いる方法と SAT-Solvers を用いる方法を試したところ、前者は既知平文 3 個で 5 段まで、後者は既知平文 1 個で 6 段まで解けた。フルスペックが 16 段なのでまだ現実的ではないが、興味深い結果ではある。

On Tweaking Luby-Rackoff Ciphers [Asiacrypt 2007]

David Goldenberg, Susan Hohenberger, Moses Liskov, Elizabeth Crump Schwartz, and Hakan Seyalioglu

tweaking とは、オリジナルの暗号化計算の途中に加算などの処理を追加することによって安全性を高める方法で、R.Schroeppel が NIST による AES 公募の際に導入した。ブロック暗号に tweaking を適用する場合、既存の暗号に後から適用するより、最初から tweaking を入れることを想定して設計するのが効率的かどうかは不明だった。この発表では、Luby-Rackoff 構造を利用することで、tweaking が今まで最も効率良く安全性を改善できる場合があることが示された。

Symmetric Key Cryptography on Modern Graphics Hardware [Asiacrypt 2007]

James Goodman and Jason Yang (Advanced Micro Devices, Inc.)

画像処理用のプロセッサである GPU は、CPU より実行速度の伸びが急速であるものの、整数演算機能や利用しやすいプログラム API が無かったため、暗号用には利用されなかった。しかし、最新の GPU では整数／２進演算機能が搭載されたため共通鍵ブロック暗号である AES と DES を実装してみた。AMD 社の HD 2900XT グラフィックカード１枚を使い、通常実装及びビットスライス実装を行ったところ、3～30Gps で計算できた。これは、通常の高速 CPU に対して同じ内容の実装を行ったのより 6～60 倍高速である。

Known-Key Distinguishers for Some Block Ciphers [Asiacrypt 2007]

Lars R. Knudsen, and Vincent Rijmen

distinguisher とは、段数を減らしたブロック暗号が満たす入出力関係のことで、暗号化鍵を推定する攻撃に利用される。通常、distinguisher は鍵によらず成立するものを利用するが、この発表では既知の鍵に対するものを利用し、特定の関係を満たす平文・暗号文のペアを見つけるという問題を設定した。具体例として、積分攻撃を利用した 7 段に縮小した AES に対するものと、7 段に縮小した Feistel 型暗号に対するものを構成した。

Generic Attacks on Unbalanced Feistel Schemes with Expanding Functions [Asiacrypt 2007]

Jacques Patarin, Valerie Nachef, and Come Berbain

Unbalanced Feistel はブロック暗号の構造の一つで、複数のサブブロックの状態を残りの 1 ブロックからの非線形出力値を加算する処理を 1 段として、これを繰り返すことで暗号化を行なう。この構造の暗号としては、AES の最終候補となった IBM の MARS や米国標準にもなった Skipjack が有名である。この発表では、２点攻撃、長方形攻撃、複数長方形攻撃の 3 種類を適用した。ブロックが k 個の n ビットのサブブロックで構成されるとき、長方形攻撃によって、暗号化 2^{kn} 回分の計算量で、3k-1 段まで既知平文攻撃が理論的に示され、6～8 段に対しては計算機実験で有効性が確認された。従来の記録は、Crypto 1998 で C.S.Jutla が発表した選択平文攻撃による 3k-3 段なので、攻撃の効率は高まっている。

Bit-Pattern Based Integral Attack [FSE 2008]

Muhammad Reza Z'aba, Haavard Raddum, Matt Henricksen, and Ed Dawson

AESに対する最も効率的な攻撃法として認められている積分攻撃法を拡張し、ブロック暗号のNoekeonとPRESENTに適用して攻撃の有効性を確認した。従来の積分攻撃法では、S-boxの出力が全パターン現れるか固定かのどちらかになるような入力しか考えていなかった。今回の発表では、ビット・パターンまで区別するという拡張を行った。

Experiments on the Multiple Linear Cryptanalysis of Reduced Round Serpent [FSE 2008]

Baudoin Collard, Franc,ois-Xavier Standaert, and Jean-Jacques Quisquater

線形解読はDESに対する最も効率の良い解読法として知られているが、通常は線形確率が大きな１つの線形経路を利用して暗号化鍵を推定する。この発表では、複数の線形経路の利用による解読効率の改善する方式を検討し、AES選考時の最終５候補に残ったブロック暗号Serpentに適用して有効性を確認した。

Impossible Differential Cryptanalysis of CLEFIA [FSE 2008]

Yukiyasu Tsunoo, Etsuko Tsujihara, Maki Shigeri, Teruo Saito, *Tomoyasu Suzaki, and Hiroyasu Kubo*

ソニーと名古屋大学が共同開発したブロック暗号CLEFIAに対する不能差分攻撃を試み、128ビット鍵の場合、フルスペックの18段に対し、12段まで鍵総当り攻撃より少ない計算量で攻撃できることを示した。開発者も不能差分攻撃に対する検討は行っており、攻撃効率の良い不能差分経路は見つけていたが、発表したグループはさらに効率の良い経路の発見に成功した。ただし、安全性を脅かす現実的な脅威にはなっていない。

A Unified Approach to Related-Key Attacks [FSE 2008]

Eli Biham, Orr Dunkelman, and Nathan Keller

ブロック暗号に対する有効な攻撃法の一つである関連鍵攻撃の改良に関する発表。本来の関連鍵攻撃は効率が良いものの適用範囲が限られていたので、適用範囲を広げるため差分型関連鍵攻撃が開発された。今回の発表では、両者の長所を活かして融合する方法を提案し、ブロック暗号IDEAの8段縮小版(フルスペックは8.5段)の解読に成功した。

Algebraic and Slide Attacks on KeeLoq [FSE 2008]

Nicolas T. Courtois, Gregory V. Bard, and David Wagner

KeeLoqは、メカニカルな鍵の代わりに携帯機による遠隔操作で自動車のドアの鍵などを開けるシステムで利用されているブロック暗号である。非線形フィードバック・シフトレジスタを利用した設計で、既に攻撃法がいくつか発表されていたが、既知平文が2^{32}個も必要である点で現実的でなかった。今回の発表ではスライド攻撃と代数攻撃を組み合わせることで、既知平文2^{16}個で解読できる方法を示した。

A Meet-in-the-Middle Attack on 8-Round AES [FSE 2008]

Huseyin Demirci and Ali Aydin Selc,uk (presented by Orhun Kara)

distinguisherとは暗号の構成要素がランダムでないことを判別するための関係式であるが、AESの段関数5段に対する新規のdistinguisherを構成し、それを利用して256ビット鍵のAESに対して8段まで(フルラウンドは14段)、192ビット鍵では7段まで(フルラウンドは12段)攻撃できた。

Block Ciphers Implementations Provably Secure Against Second Order Side Channel Analysis [FSE 2008]

Matthieu Rivain, Emmanuelle Dottax, and Emmanuel Prouff

強力なサイドチャネル攻撃の一つである２次の(差分)攻撃に対して安全なブロック暗号の２種類の実装法を提案した。ブロック暗号の主要な要素の一つである非線形関数S-boxの実装を工夫することにより、強い安全性モデルの下で安全性が証明できるようにしている。

An Improved Security Bound for HCTR [FSE 2008]

Debrup Chakraborty and Mridul Nandi

HCTRは値が公開の可変パラメータtweakを利用したランダム置換として見なせるブロック暗号の一つである。HCTRの実装性能は非常に高いものの、提案者の解析による安全性の下限は攻撃者による質問回数の３乗に比例するというもので、安全性は十分でなかった。この発表では、安全性の下限が、$4.5\sigma^2/2^n$（ここでn はブロック暗号の長さ、σは質問回数）で押さえられることを示し、提案者の見積もりよりも、より高い安全性が保証できることを示した。

How to Encrypt with a Malicious Random Number Generator [FSE 2008]

Seny Kamara and Jonathan Katz

共通鍵暗号に対する選択平文攻撃はランダムなコインを振るオラクルに対して質問する攻撃者としてモデル化される。この発表では、このコインがランダムに振られない場合について取り扱い、モデル化を行い選択乱数攻撃(CRA)を定義し、CRAに対する安全性概念を構成した。また、CRA-secureとなる具体的な方式を2つ提案した。一つは、固定長の構成で、CPA-secureな暗号アルゴリズムから構成する。もう一つは、可変長のメッセージに対応できるようにCTR-modeを前者の方式に適用した構成となっている。

4. 公開鍵アルゴリズム

Towards a Separation of Semantic and CCA Security for Public Key Encryption [TCC 2007]

Yael Gertner, Tal Malkin and Steven Myers

Non-Black Box の環境では、Semantic Secure public-key primitive であったとしてもそれはダイレクトには、Chosen Ciphertext attack に対して安全であることを示していることにはならない、ということを示した。Semantic Secure な encryption primitive からは CCA1 secure (すなわち CCA2 も)な方式を構成するような black-box reduction は存在しないことを示した。Semantic secure な encryption primitive を基に CCA を構成する方法としては、non-black-box とするか、特殊な条件を満たす encryption algorithm を、証明を行なう対象となるアルゴリズムの中の decryption algorithm の中で利用するしかない、としている。

Deterministic Polynomial Time Equivalence between Factoring and Key-Recovery Attack on Takagi's RSA [PKC 2007]

Noboru Kunihiro and Kaoru Kurosawa

RSA に類する方式として、RSA よりも復号演算が高速となる方式が高木氏により提案されて

いる。その提案方式では、$N=p^r q$, $ed=1 \bmod (p-1)(q-1)$ が用いられている。

本発表では、$ed=N^{4/r+1}$, $|p|=|q|$, $r=O(\log \log N)$ であるような場合に、N, e,d（但し、$ed=1 \bmod (p-1)(q-1)$）から N（$=p^r q$）の素因数分解を多項式時間で求めることが可能であることを示した。この結果は高木氏の提案する RSA に適用可能であり、上記の条件を満たす場合にその秘密鍵を求めることが出来ることを示した。

既存の May らの結果は、本発表の結果において r= 1 とした場合に相当しており、本発表で示した結果は May らの結果の自然な形での一般化となっていると考えられる。解析の具体的手法としては、Coron と May らが RSA の解析の際に用いた LLL を用いた手法を利用している。

Toward a rigorous variation of Coppersmith's algorithm on three variables [Eurocrypt 2007]

Aurelie Bauer and Antoine Joux

Coppersmith によって示されている lattice ベースの多項式の small root を見つける手法は様々な応用を持つがそれらの多くは heuristic な手法にとどまっている。この論文では、新たな応用方法を考え、それを用いての short RSA exponent attacks を実際試みた。技術的なアイディアとしては、lattice reduction technique でグレブナー基底を利用して構成している。

An L(1/3 + epsilon) algorithm for the discrete logarithm problem in low degree curves [Eurocrypt 2007]

Andreas Enge and Pierrick Gaudry

一般的な楕円曲線上のもので X や Y の次数がその genus(曲面の種数)に対して小さく、(解析に合うような)アンバランスなものに対して適用可能な離散対数問題の効率的な解法を示した。体は任意のものに対して適用できるがそのサイズは genus に比べてそれほど早く増加しないものに対して適用できる方式となっており、この場合、離散対数問題を、準指数的計算量で解法可能であるとしている。この論文は、優秀論文賞に選ばれた。

Non-Wafer-Scale Sieving Hardware for the NFS: Another Attempt to Cope with 1024-bit [Eurocrypt 2007]

Willi Geiselmann and Rainer Steinwandt

数体ふるい法専用ハードウェアを作成。これを用いて実際にふるい部分の高速化を図っている。同じようなハードウェアを利用したものとしては TWIRL (a wafer-scale design) が既に提示されているが、TWIRL に比べ本方式は 2～3.5 倍程度遅いが、メモリ量を削減している。DRAM を搭載し、memory 上で再利用可能な部分を効率的に利用していくことで全体で必要となるメモリ量を減らしている。チップの大きさは、172 cm^2 とのこと。コストはど

のくらいかかるかとの質問に、デバイスの作成に 10 百万ドル、トータルで 20 百万ドルかかるとのことであった。

Edwards Coordinates for Elliptic Curves [SAC 2007]

Dan Bernstein

Edwards 座標を使うことにより、サイドチャネル攻撃に強い楕円曲線暗号の実装が実現できる。楕円曲線暗号で通常使われる Jacobi 座標では、2 倍算と加算が異なる形の計算になるため計算時間に違いが生じ、これを利用したタイミング攻撃が可能になるという問題があった。Edwards 座標では、2 倍算と加算が同じ形なので計算時間に差が生じず、タイミング攻撃に対して安全な実装が実現できる。また、個々の演算に対する高速実装も可能である。参加者のほとんどが初めて耳にする話のようで、今後第 3 者による検証が待たれる。

Another Look at Square Roots (and Other Less Common Operations) in Fields of Even Characteristic [SAC 2007]

Roberto M. Avanzi

平方根の計算が高速に実行できる既約多項式の作り方を検討した。2004 年に A.Menezes らは適切な既約 3 項式を選ぶことで平方根の計算が高速化てぎることを示した。本発表では、奇数次数の既約多項式に対し、平方根の計算が軽くなるための十分条件を求めた。その結果、平方根の計算が高速に実行できる既約多項式の導出に成功するとともに、トレース計算や 2 次多項式の高速化も達成した。

Cryptography with Constant Input Locality [Crypto 2007]

Benny Applebaum, Yuval Ishai and Eyal Kushilevitz

FOCS 2004 において、出力の各々のビットは(暗号学的仮定に基づく場合)入力の定数程度のビット数からしか影響を受けていない、という結果が示されている。本発表では、入力側に着目する。否定的な結果としては、non-malleability の性質は入力の各々のビットが定数程度の出力ビット数にしかその影響が波及しない場合、構成することが不可能であることを示した。また、肯定的な結果としては、error correcting codes での相互作用性を仮定した場合、(すなわち、random linear code の decode の困難性や McElice 暗号の安全性など) 入力の各々のビットが、定数程度の出力にしか影響が波及しないような場合であっても、一方向性関数、擬似乱数生成器、コミットメント、semantically-secure な公開鍵暗号などが構成可能であることを示した。これらは、各々のアウトプットのビットが入力のコンスタント程度のビット数の影響しか受けてない場合にも構成可能であることを示した。これらの結果は HW での効率的な構成を実現可能とするものである。この論文は、今年

の最優秀論文に選ばれた。

A Hybrid Lattice-Reduction and Meet-in-the-Middle Attack Against NTRU
[Crypto 2007]

Nick Howgrave-Graham

公開鍵暗号 NTRU の秘密鍵を公開鍵から求める攻撃において、中間一致攻撃と格子還元を組合せることで攻撃に必要な計算量を削減した。NTRU は格子上の最短ベクトル問題を安全性の根拠とする公開鍵暗号である。公開鍵から秘密鍵を求める方法としては、中間一致攻撃と格子還元を利用した攻撃の 2 種類が知られていた。本発表では、中間一致攻撃と格子還元を組合せる。その結果、攻撃に必要な計算量を $2^{84.2}$ から $2^{60.3}$ に削減した。

Finding Small Roots of Bivariate Integer Polynomial Equations: A Direct Approach
[Crypto 2007]

Jean-Se'bastien Coron

2 変数連立整数係数多項式の小さな解を見つける効率の良い方法を開発した。2 変数連立整数多項式の小さな解を求めることは RSA 暗号とその変形を攻撃するのに利用できる。例えば、秘密鍵指数を d、法を N としたとき、$d<N^{0.29}$ を満たす RSA 暗号が攻撃できることが、Eurocrypt 1996 において D.Coppersmith によって示されている。そこでは格子還元の手法が使われている。Coopersmith の論文は分かりにくく複雑だったので、Coron はより単純な求解法を Eurocrypt 2004 で発表したが、漸近的な効率は Coppersmith の方法より劣った。本発表では、整数係数の 2 変数既約多項式を満たす整数のペアを利用した。その結果、Coopersmith の方法と効率が漸近的に同等でかつ単純な求解法が構成できた。

A Polynomial Time Attack on RSA with Private CRT-Exponents Smaller Than $N^{0.073}$
[Crypto 2007]

Ellen Jochemsz and Alexander May

RSA 暗号において、private CRT 指数がともに $d<N^{0.073}$ を満たすとき、公開鍵から秘密鍵を多項式時間で解けることを示した。RSA 暗号は、秘密鍵指数 d が $d<N^{0.25}$ と小さいとき、公開鍵から多項式時間で求められることが 1990 年 M.Wiener によって示され、2000 年に D.Boneh と G.Durfee が $d<N^{0.292}$ に拡張した。一方、RSA の実装には、中華人剰余定理(CRT)を利用して計算を効率化する方法があり、法 N の素因数 p,q(N=pq)に対して、private CRT 指数 d_p, d_q が中間計算でべき指数として利用される。d_p, d_q がともに小さいとき、RSA 暗号を破ることが可能かどうかは未解決問題だった。本発表では、D.Bleichen と A.May が PKC 2006 で示した方法をベースにして、より次元の高い格子を利用した。その結果、private CRT 指数がともに $d<N^{0.073}$ を満たすとき、公開鍵から秘密鍵を多項式時間で解けることが示せた。指数の 0.073 という指数は小さいが最初の結果として意味がある。

Deterministic and Efficiently Searchable Encryption [Crypto 2007]

Mihir Bellare, Alexandra Boldyreva and Adam O'Neill

決定論的な暗号アルゴリズムでのプライバシを定義し、これを実現する方式を提案。1番目は、"Encrypt-with-Hash" とよばれ、決定論的に平文を暗号化するが、暗号化アルゴリズムはハッシュ関数を使ったコイン投げによって選定する。ランダムオラクルと用いるアルゴリズムが IND-CPA であることを仮定している。2 番目は、RSA-OAEP をベースにし、パディングする部分は決定論的に処理されるが、2 段ではなく 3 段の Feistel 型の構成にしている。ランダムオラクルと RSA が一方向性であることを仮定している。３番目は、さらに効率的であり、searchable encryption scheme と呼ばれる。

FPGA Implementation of High Throughput Circuit for Trial Division by Small Primes [SHARCS 2007]

Gabriel Southern, Chris Mason, Lalitha Chikkam, Patrick Baier, and Kris Gaj

数体篩法による素因数分解を高速化するため、篩のステップにおける小さな素数で試行除算を行う処理を FPGA 実装で高速化した。数体篩法は、多項式選択、関係収集、線形代数計算、平方根計算の４ステップで構成され、計算量の大半は関係収集と線形代数計算に費やされる。関係収集(relation collection)は、篩処理と余因子分解(cofactoring)に分かれる。cofactoring は、B 未満の素数(本発表では B=100,000)によるブルートフォース型の試行除算とそれ以上の素数に対する複雑な方法(ρ法、p-1 法、楕円曲線法)から成る。複雑な方法を高速化するための専用ハードウェア実装の研究は広く行なわれているが、試行除算用ハードウェア実装の研究はあまり行なわれてこなかった。そこで、100,000 未満の素数 9592 個による除算を並列化することで、ハードウェア実装の優位性を活かすことにした。実装は Xilinx FPGA ファミリで行い、ブロック RAM と高速リップル・キャリ・ロジックを活用する。FPGA には安価な Spartan 3 XCS1500/2000 と高価な Virtex 4 XC4VLX25/40 の 4 種類で実装し、費用性能比を比較した。Spartan 3 XCS2000 が最も高い費用性能比を示し、1 ドル当たりのスループットが 512 ビット整数の試行除算を実測値で 178 回/秒となった。同じ処理を Intel Xeon XP 2.8Hz を使ったソフトウェア実装で 1.09 回/秒なので、費用性能比で約 170 倍優れている。

Elliptic Curve Factorization Method: Towards Better Exploitation of Reconfigurable Hardware [SHARCS 2007]

Giacomo de Meulenaer, Francois Gosset, Guerric Meurice de Dormale, and Jean-Jacques Quisquater

数体篩法に楕円曲線法(ECM)を組み合わせ、FPGA で並列実装することにより剰余乗算を高速化することに成功した。数体篩法は大きな合成数の素因数分解の最も効率の良い方法であ

ることが知られている。数体篩法の重要な段階の一つである関係収集(relation collection)は、篩処理技法と中サイズ数の素因数分解で構成される。中サイズ数の素因数分解を実行する方法としては、楕円曲線法(ECM)が複数多項式 2 次篩法と並んで最も効率の良いものとして知られている。楕円曲線法は規則性と並列性が高く、ハードウェア実装ではソフトウェア実装より費用性能比が高いことが示されている。しかし、ECM の数少ない FPGA 実装の論文では、低価格の FPGA によるビット連続アーキテクチャが最も費用性能比を持つとされていた。この発表では、最近の高性能 FPGA とその組込み乗算回路を活用することで、従来の FPGA 実装と比べ 15 倍の費用性能比を達成した。

CAIRN 3: An FPGA Implementation of the Sieving Step with the Lattice Sieving [SHARCS 2007]

Tetsuya Izu, Jun Kogure, and Takeshi Shimoyama

素因数分解の専用ハードウェアとして最も高い性能を持つ FPGA 実装の CAIRN 2 を富士通が開発していたが、格子篩法の適用によって線形篩法の実装効率を高めた CAIRN 3 を開発した。素因数分解の現在知られている最も効率の良い方法は数体篩法であり、４つのステップ：多項式選択、篩処理、線形代数計算、平方根計算で構成されている。計算コストのほとんどは、篩処理と線形代数計算に掛る。篩処理用のハードウェア設計は Bernstein や Lenstra らが提案し、線形代数計算用ハードウェア提案には、Geiselmann らによる DSH と YASD、Shamir と Tremer の TWIRL、Franke らの SHARK などがある。しかし、実際に ASIC や FPGA による専用ハードウェア実装はなかった。そこで、素因数分解の対象は 768 ビットまでの整数とし、新規の実装技術としてパイプライン篩(the pipelined sieving)を開発し、FPGA(Xilinx Virtex-4 XC4VLX200)で実装した CAIRN 2 を開発した。しかし、開発期間の制約から、CAIRN 2 では篩処理に線形篩法をしたものの、格子篩法を利用することによって、より高速化できることが分かっていた。そこで、CAIRN 2 の線形篩法処理を格子篩法に置換えた CAIRN 3 を開発した。篩処理において CAIRN 3 は CAIRN 2 の 38 倍高速になった。1 台の CAIRN 3 では、1 個の関係式を平均 3.92 秒に 1 回見つけるので、768 ビット RSA の法の素因数分解に必要な 2.17×10^9 個の関係式を求めるのに約 270 年掛るという見積もりになった。

CAIRN2: An FPGA Implementation of the Sieving Step in the Number Field Sieve Method [CHES 2007]

Tetsuya Izu, Jun Kogure, Takeshi Shimoyama

素因数分解に用いる篩処理専用の FGPA 実装 CAIRN2 を開発し、現実に動くハードウェア実装として世界最高を達成した。素因数分解の現在知られている最も効率の良い方法は数体篩法であり、４つのステップ：多項式選択、篩処理、線形代数計算、平方根計算で構成されている。計算コストのほとんどは、篩処理と線形代数計算に掛る。篩処理用のハードウ

ェア設計は Bernstein や Lenstra らが提案し、線形代数計算用ハードウェア提案には、Geiselmann らによる DSH と YASD、Shamir と Tremer の TWIRL、Franke らの SHARK などがある。しかし、実際に ASIC や FPGA による専用ハードウェア実装はなかった。そこで、素因数分解の対象は 768 ビットまでの整数とし、新規の実装技術として開発したパイプライン篩(the pipelined sieving)を利用し、FPGA(Xilinx Virtex-4 XC4VLX200)で実装した CAIRN 2 を開発した。423 ビットの整数の素因数分解に成功した。開発期間が制約されていたため、663 ビットや 768 ビットといったサイズの整数の素因数分解はできなかった。これらの素因数分解には、線篩処理をより効率の高い格子篩処理に置換えることが有効であり、既にそれを実現した CAIRN 3 が開発済みであり、その結果は直前に開催された SHARCS 2007 で発表している。

Collision Search for Elliptic Curve Discrete Logarithm over GF(2^m) with FPGA [CHES 2007]

Guerric Meurice de Dormale, Philippe Bulens, Jean-Jacques Quisquater

GF(2^m)上の楕円曲線における離散対数問題を解くために、現在ソフトウェアで最も対コスト性能比の良い、並列化された Pallard のアルゴリズムを実装した。楕円曲線暗号において実装性能と安全性に関する適切なトレードオフを実現する法のサイズを決定するには、楕円曲線上の離散対数問題(ECDLP)を解くための計算コストを知る必要がある。2006 年までに発表された ECDLP の攻撃は汎用ハードウェアを利用したものだけであり、専用ハードウェアを利用したときの計算コストは評価されていなかった。そこで、曲線は素体で無くハードウェア実装が有効な 2 の拡大体に限定した専用ハードウェアを設計した。攻撃の方法としては、Pollard の ρ 法と Shanks の Baby-step Giant-step 法に注目し、実装には、van Oorschot と Wiener による並列化された ρ 法を利用する。低コストの Spartan3E FPGA での実装とソフトウェア実装を GF(2^{109})で比較すると、購入コストで 35 倍、電力消費で 500 倍の差が有った。SECG 規格の GF(2^{113})は容易に解けたが、GF(2^{163})での計算時間は $4.7*10^{15}$ 秒と見積られた。163 ビットの ECDLP を解くのは現在の技術レベルでは困難である。

Highly Regular Right-to-Left Algorithms for Scalar Multiplication [CHES 2007]

Marc Joye

楕円曲線暗号で使われるスカラー倍演算を電力解析に対して安全になるように Right-to-Left アルゴリズムを開発した。アーベル群上のべき乗演算は通常スカラー積と呼ばれ、リソースが限られたデバイス上で計算する際は、通常、double-and-add アルゴリズムが利用される。このアルゴリズムは 2 倍算と加算で処理が異なるため、単純電力解析(SPA)や safe-error 攻撃で秘密の値が推定できるという欠点があった。そこで、モンゴメリ・ラダー法を利用して、規則性が高い右から左へ計算するアルゴリズム構成したところ、単純電力解析(SPA)や safe-error 攻撃に対する耐性があり、非常に簡潔で必要とするメモリも

少なくて済む実装が可能になった。

Arithmetic Operators for Pairing-Based Cryptography［CHES 2007］

Jean-Luc Beuchat, Nicolas Brisebarre, Je're'mie Detrey, Eiji Okamoto

楕円曲線上のペアリング暗号の FPGA 実装として、加算、乗算、３乗算を $F_{3^{97}}$ 上で統一的に表すことで高速化した。楕円曲線上のペアリング暗号が近年盛んになっており、より効率的な方式の研究が進められている。最初に提案された Weil ペアリングより、Tate ペアリングは効率が良く、それを拡張／改良した η_T ペアリングを Barreto らが提案した。Beuchat らは、$F_{3^{97}}$ 上の算術演算において Barreto らの計算法を改良した。ペアリングの計算は、ソフトウェアでは遅く、ハードウェア実装の研究が盛んである。$F_3[x]/(x^{97}+x^{12}+2)$ 上の η_T ペアリングの計算を Xilinx Virtex-II Pro 4 FPGA で実装した。言語には VHDL、合成は Xilinx ISE WebPACK 8.2.03i を利用した。1888slices と 6 メモリブロック、クロック周波数 147MHz で $\eta_T(P,Q)^W$ の計算を 222μs で実行した。従来より、構造が簡単で領域が少なくて済む実装になっている。

On the Implementation of a Fast Prime Generation Algorithm［CHES 2007］

Christophe Clavier and Jean-Se'bastien Coron

高速の素数生成アルゴリズムにおいて実装が適切でないと、サイドチャネル攻撃が可能であることが分かっている。この発表で、パリティ・ビットが単純電力解析で特定できるとき、1024 ビット RSA に対し 1/1000 の鍵が復元できることを示した。電力解析の攻撃対象は主として暗号化か復号が対象であり、鍵生成にはほとんど適用されていない。RSA 暗号の鍵生成では、ランダムに生成された整数から素数判定に通って得られた素数を利用するが、その過程がサイドチャネル攻撃の対象となり得る。本発表では、CHES 2006 で Joye と Pailler が提案した高速素数生成アルゴリズムを攻撃対象とした。SPA によって推定した素数判定で使われるパリティ・ビットを利用して、生成される素数を推定した。パリティ・ビットが正しく推定できると、1024 ビット鍵の RSA 暗号の場合、$8.4*10^{-4}$ の確率でモジュラスを正しく推定できた。成功確率は 1/1000 と低いが、現実的な脅威ではある。

Space-efficient identity based encryption without pairings［IEEE / FOCS 2007］

Dan Boneh, Craig Gentry and Mike Hamburg

ペアリングを用いない IBE としては、Cocks が IMA-ICCC01 で提案したものが知られている。本発表では、ペアリングを用いない新しいトラップドアを構成し、それを用いて Cocks の方法より暗号文のサイズが小さくて済む IBE 方式の設計に成功した。L ビットの平文に対して、暗号文のサイズを L+1+ a single element 程度に抑えることが出来る。ただし、計算効率は劣る。安全性に関しては、両方式とも Quadratic residuosity 問題(平方剰余問題)に基づいており、新しいトラップドアが提案されたことにより、今後これを応用した様々

な研究結果が出てくると予想される。また、本論文はFOCS07のbest paperに選ばれた。

Construction of a Hybrid HIBE Protocol Secure Against Adaptive Attacks (without Random Oracle) [ProvSec 2007]

Palash Sarkar and Sanjit Catterjee

DBDH(Decisional Bilinear Diffie-Hellman)仮定の下で、Boneh-Franklin(2001)が示したのと同レベルの安全性を持ち、adaptive ID and CCA secure の安全性証明がランダムオラクルなしで証明でき、公開パラメータのサイズがより小さくできる方式を提案した。(H)IBE を基にして、黒澤-Desmedt(2004)で用いられた構成法を適用した初めての方式だと主張している。

A Kilobit Special Number Field Sieve Factorization [Asiacrypt 2007]

Kazumaro Aoki, Jens Franke, Thorsten Kleinjung, Arjen K. Lenstra, and Dag Arne Osvik

1039 ビットの合成数 $2^{1039}-1$ の素因数分解を特殊数体篩法(SNFS)を利用して実現した。既にこの合成数が 5080711 という素因数を持つことは分かっていたので、今回の発表では、これで割った 1017 ビット数の素因数分解ができることを示した。5080711 という素因数で割っても、$2^{1039}-1$ の SNFS を容易にはしないので、1039 ビットの素因数分解を実行したのと問題の困難さは同じだと著者らは主張している。なお、特殊数体篩法は大部分の合成数に対して適用できないので、1024 ビット鍵の RSA 暗号の安全性が決定的に低下したというわけではない。

When e-th Roots Become Easier Than Factoring [Asiacrypt 2007]

Antoine Joux, David Naccache, and Emmanuel Thome'

条件付きながら、剰余系で素因数分解より e 乗根の計算が簡単であることが示された。その条件とは、c を定数、x_i を小さな数としたとき、x_{i+c} の e 乗根を準指数時間で返すオラクルが存在することである。この結果は、RSA 暗号の頑健性などに影響を与える。

Miniature CCA2 PK Encryption : Tight Security Without Redundancy [Asiacrypt 2007]

Xavier Boyen

GDH(Gap Diffie-Hellman)仮定に基づき、ランダムオラクルモデルで CCA2-secure な方式を提案。提案方式は、暗号文サイズのコンパクト化に注力し、冗長性をなくす試みをしている。アイディアとしては、Hybrid タイプの構成は用いずに、El Gamal 暗号の構成をベース年、2 つのハッシュ関数を利用して、2 重に暗号化処理を行うような構成をとることで、El Gamal 暗号タイプの構成の持つ malleability の性質を消し、redandancy-free の性質を持

ちえる方式を構成している。

Bounded CCA2-Secure Encryption [Asiacrypt 2007]

Ronald Cramer, Goichiro Hanaoka, Dennis Hofheinz, Hideki Imai, Eike Kiltz, Rafael Pass, abhi shelat, and Vinod Vaikuntanathan

公開鍵暗号の安全性として、能動的な攻撃者に対する安全性として CCA2 があるが、ここではやや CCA2 のモデルを緩くし、攻撃者が問い合わせることの出来るクエリの回数を q に制限した bounded CCA2 を定義した。この bounded CCA2 に対して、black-box モデルで任意の IND-CPA-secure な暗号方式から q-bounded IND-CCA2-secure な方式が構成可能なことと、non-black-box モデルで任意の IND-CPA-secure な暗号方式から q-bounded NM-CCA2-secure な方式が構成可能なことを示した。さらに、この bounded CCA2 に関しては、non-malleability と indistinguishability が等価でないことも示した。

Relations Among Notions of Non-Malleability for Encryption [Asiacrypt 2007]

Rafael Pass, abhi shelat, and Vinod Vaikuntanathan

Non-malleability に関しては、実用的な indistinguishabile-base の定義の仕方と、理論的な simulation-base の定義の仕方とがある。本稿では、その両者で示された定義間の関係を考察し、帰着関係などを示している。本稿では、上記 2 種類の定義に対して、各々の定義に対しやや緩めた弱い定義を示し、その弱めた定義と本来の強い定義との関係性なども併せて考察を行い、その帰着関係を示している。

Faster Addition and Doubling on Elliptic Curves [Asiacrypt 2007]

Daniel J. Bernstein and Tanja Lange

楕円曲線暗号の新しい標準形である Edwards 座標を使うと、各種演算が従来の Weierstrass 座標や Jacobi 座標より高速で実行でき、特に加算と 2 倍算が同じ形で計算できることからサイドチャネル攻撃に強いという長所を持っていることを最近、著者らが紹介してきた。今回、計算量の比較を広範囲の演算に対して行った。全ての演算で Edwards 座標が高速であることを示そうとしたが、論文投稿後に反例が見つかったため、変型判の Inverted Edwards 座標を新たに開発し、優位性を確保した。

5. 暗号プロトコル

Tackling Adaptive Corruptions in Multicast Encryption Protocols [TCC 2007]

Saurabh Panjwani

Non-adaptive で安全な Broadcast Encryption プロトコルについて、その adaptive corruption に対しての安全性を評価する一般的手法を提案した。ある鍵で別の鍵を暗号

化して配送する BE (Broadcast Encryption) プロトコルにおいて、ユーザ数を n とし、鍵配送 chain が深さ L の無サイクル有向グラフになるとき、そのグラフの sink に相当する部分の鍵（corrupt して得られた鍵から順次復号しても辿れない鍵）に関する安全性を評価した。Adaptive から Non-adaptive への帰着効率が $(2n)^L$ となる。結果は passive adversary の場合についてのみ成り立つ。BE 以外のプロトコルに応用できるかどうかは未解決の問題である。

Long-term Security and Universal Composability [TCC 2007]

Jörn Müller-Quade and Dominique Unruh

Long-term セキュリティ（プロトコルの transcript についての危殆化. プロトコル実行中の攻撃者は計算力に制限を持つが, プロトコル終了後は攻撃者が無制限の計算力をもてるとする）を UC (Universal Composable) Framework で扱うために、UC Framework の安全性定義で, Real-life と Ideal において Environment が得る view の差を statistically close に強化した。このモデルでは、CRS(Common Reference String) モデルでの Bit Commitment や ZK(Zero-Knowledge) は実現不可能であり、さらに Setup Assumption として Coin-toss・ PKI・ZK を仮定する場合も不可能であることを述べている。

Long-term UC が可能になるセットアップの例としては、Signature Card Assumption（各ユーザが自分のディジタル署名を生成できるカードを持つが、カード内にある自分の秘密鍵は知り得ない）をあげ、このモデルでの ZKP （"I know Sig(w) or I know SK" を実行する）が可能であることを示した。ZK と BC 以外のプロトコルが Long-Term UC できるかどうかは Open Problem。

Secure Linear Algebra Using Linearly Recurrent Sequences [TCC 2007]

Eike Kiltz, Payman Mohassel, Enav Weinreb and Matthew Franklin

Matrix の singularity を相手に他に何も情報を漏らすことなく判別することのできる interactive プロトコルの提案。O(log n)の communication round と total での communication complexity が O(n^2)程度の複雑さで実現できる(input は n^2 である)。準同型公開鍵暗号と Yao の garbed circuit protocol を利用している。Yao のプロトコルは approximate symmetric key encryption と semi-honest な攻撃者に対して安全な OT (Oblivious Transfer；紛失通信路) とを用いて構成することが出来る。提案プロトコルを利用して Kaltofen らによって提案されたアルゴリズムを解くプロトコルを構成することが可能である。技術的にはこのアルゴリズムはマトリクスのランクに依存しており、このマトリックスのランクの計算はプロトコルのプライバシを害する。そこで暗号化されたマトリックスのランクの暗号化を行うプロトコルを構成することにより、上記の問題点であるプライバシを保ちつつアルゴリズムの解法を実現するプロトコルを構成可能とした。

Towards Optimal and Efficient Perfectly Secure Message Transmission [TCC 2007]

Matthias Fitzi, Matthew Franklin, Juan Garay and S. Harsha Vardhan

チャネル数 n, そのうち corrupt されているチャネル数 t で、n>2 の場合、従来知られている結果としては、2 ラウンドプロトコルの場合、その communication complexity は $O(n^3 L)$ があった。(ここで L はメッセージの長さ。) 本発表では、チャネルが n ≧(2+ε)t (ここで ε は任意の小さな定数)な場合について、communication complexity が optimal になるプロトコルを提案。提案方式の場合、従来結果と同等のチャネルの条件の下で communication complexty が O(L)とすることが出来る。

Designated Confirmer Signatures Revisited [TCC 2007]

Douglas Wikström

Designated Confirmer Signature の新しい定義を提示し、その定義に基づく安全性証明可能な方式を提案した。従来の定義では confirmer が不正を行なうことを想定したような定義としては十分でなかったり、正しい鍵が用いられない場合の情報の流出がケアされていなかった。本発表では特に署名が正しく変換されている証明・鍵が正しく規定に沿った鍵であることの証明に関する定義を提唱し、それらの定義を満たす安全性証明可能な方式をも提案した。提案方式は strong-RSA Assumption と DH(Diffie Hellman) Assumption に基づく方式となっている。

Unifying Classical and Quantum Key Distillation [TCC 2007]

Matthias Christandl, Artur Ekert, Michal Horodecki, Pawel Horodecki, Jonathan Oppenheim and Renato Renner

事前共有していたディジタルデータと quantum データを基にして鍵共有を行なうプロトコルを提案。通信者 A と B 及び攻撃者 E の state のコピーから特定される鍵のビット数の upper bound をも見積もった。さらに事前共有を必要としない方式への改良をも示した。また、その安全性解析を行ない、攻撃者のメモリに対する assumption の設定が QKD の閾値を正確に見積もる為に重要であることを示した。

Message Freedom in MD4 and MD5 Collisions: Application to APOP [FSE 2007]

Gaetan Leurent

メールなどの受信時の認証などとして用いられている、チャレンジレスポンス型で MD5 を利用したプロトコル APOP に関しての解析結果。プロトコルの中で用いているパスワードについて 3 文字まで現実的な時間内で推定可能であることを示した。実装も行い、プログラムも公開された。

Full-Domain Subgroup Hiding and Constant-Size Group Signatures [PKC 2007]

Xavier Boyen and Brent Waters

グループ署名で利用している群の要素がコンスタント程度の場合について、署名サイズが大変小さく抑えられ、standard モデルで安全性証明可能な方式を提案した。従来の Boneh-Water らの提案方式では、用いていた bit ごとの NIZK(Non-Interactive Zero Knowledge)を示さねばならなかったが、本提案方式では 1 つの NIZK で取扱うことが可能となっている。bilinear group について Hiding Strong Diffie-Hellman Assumption という Strong Diffie-Hellman assumption よりもやや強い仮定を定義し、それを用いて NIZK の証明を行なっている。署名は 2 階層の IBS の構成を利用しており、1 階層目でユーザの ID を規定し(この部分で上記の新たな NIZK を利用している)、2 階層目でメッセージに対する署名を生成できる仕組みとなっている。
本発表は、今回の会議の最優秀論文賞に選ばれた。

A Direct Anonymous Attestation Scheme for Embedded Devices [PKC 2007]

He Ge and Stephen R. Tate

Direct Anonymous Attestation (DAA) とは、Trusted Computing Group で採択されている匿名性を持つ認証方式を指す。本発表では、組込みデバイスを意識した軽量の演算で処理可能な DAA 方式を提案。Camenish と Michel が提案したグループ署名の構成を利用した方式となっている。CM98 の方式で、署名生成を行なう際にユーザ側の匿名性を保つ為に ElGamal 暗号化などの処理を施していた部分を改造し、ユーザ側に割り当てられている鍵にランダムに選んだ blinding integer を乗じる処理で代替している。結果として、処理すべき計算量を軽減することが出来るとしている。

Anonymous Signatures Made Easy [PKC 2007]

Marc Fischlin

署名者の匿名性を保持できる署名方式の構成手法についての一般化を行なった。提案方式にのっとれば、ランダムオラクルモデルで効率的な署名方式を構成することが可能であり、またスタンダードモデルでも効率性は落ちるものの安全な署名方式の構成が可能であるとしている(スタンダードモデルの場合はハッシュ関数に対して衝突困難性の仮定を必要とする)。但し、設定の条件として攻撃者が認識していないメッセージ m が配布されていると仮定した場合に限られる。署名者の ID 情報を漏らしてしまうが偽造不可能な署名方式による署名 Sig(sk,H(m))があった場合、これを署名者の匿名性を保持できる署名への変換は次のように考えることが出来る。Sig’(sk,m) = Sig(sk,H(m)) xor Ext(m)。この際に条件としては Ext()は randomness extractor であり、Ext(m)は m を知らない限りはランダムな値と区別が出来ないものでなくてはならない。また、H(m)の値が知られた状態であっても Ext(m) の分散はランダムな値と区別が出来ないものでなくてはならない。本発表では、

上記の条件を満たす構成方法の一般化を示した。

On the Generic and Efficient Constructions of Secure Designated Confirmer Signatures [PKC 2007]

Guilin Wang, Joonsang Baek, Duncan S. Wong, and Feng Bao

2005 年に Gentry, Molnar, Ramzan は一般的な署名方式を DCS (Designated Confirmer Signature)に変換する方法を提案している。本発表では、彼らの方法によって構成されたDCSの安全性を解析し、公開鍵暗号を用いた暗号化などを必要としない安全なDCSの構成方法を新たに提案した。GMR では、署名対象となるメッセージをコミットする際に用いたランダム値及びそのランダム値のみを暗号化した値を再利用して別の署名を生成することが可能となる。この署名を利用してConfirmerとの交信を行なうと、DCSが何れのメッセージに対する署名なのかを識別することが出来てしまう。新たに提案する方式は、上記のような再利用が行なえないようにランダム値のコミットメントなどは用いずに、Confirmer の公開鍵と OR 証明を用いて DCS を構成している。

Cryptanalysis of Non-Standard Key Agreement Protocols [PKC 2007]

Adi Shamir

招待講演。subgroup distance function を利用した鍵共有プロトコルに対する解析。これに対し、まず distance-based attack の理論的なフレームワークを構成し、具体的な攻撃のサンプルとして、Thompson’s group を利用した Shpilrain-Ushakov プロトコルの解析を行なった。結果、一台のマシンを使って数秒で鍵の半分を特定することができた。過去示されている length-based attack をはるかに上回る解析結果となっている。この結果に関連する話としては、Asiacrypt 2006 のランプセッションで Shamir 教授の共同研究者である Jacques Stern により紹介され、また 2007 年 4 月には IPA のフォーラムで Shamir 教授により紹介された。また、この講演後の下記の発表も関連論文である。この後開催される Eurocrypt 2007 には本研究に類する結果が Jacques Stern 教授の学生らの論文に採録されている。なお、最新結果は現在、Shamir 教授と Jacques Stern 教授の共著論文として Crypto に投稿中とのことである。また、このタイプの攻撃は本会議で発表があった J. Ding, C. Wolf, and B. Y. Yang による“l-Invertible Cycles for Multivariate Quadratic Public Key Cryptography” にも適用可能と考えられており、本発表の著者らも回避方法が見つからないようであった。

Length Based Attack and Braid Groups: Cryptanalysis of Anshel-Anshel-Goldfeld Key Exchange Protocol [PKC 2007]

Alex D. Myasnikov and Alexander Ushakov

Shamir 教授の学生による発表。Anshel-Anshel-Goldfeld による鍵共有プロトコルに対す

る解析手法、Length-based attack についてこれまでに知られていた方式に対する考察を行った上で、新たに 2 種類の解析アルゴリズム (Generalized LBA with conjugation, LBA with dynamic set)を提案。実装も行なわれており、成功確率が評価されていた。実験結果としては LBA with dynamic set の手法が高い成功確率を示していた。

Efficient Ring Signatures Without Random Oracles [PKC 2007]

Hovav Shacham and Brent Waters

ランダムオラクルを用いずに安全性証明可能な Bilinear Group を利用したリング署名(署名者の匿名性を保持できる署名)の構成方法を提案。メンバ数 L で構成するリング署名を 2L+2 の群の要素で構成でき、署名検証の際に必要となる paring の演算量は 2L+3 である。基本構成は、Eurocrypt 2006 で Boneh と Water により提案されたグループ署名の構成に類似している。但し、彼らの構成では、署名対象のメッセージは暗号化されて公開されるのに対し、本提案方式のリング署名ではメッセージは公開されている。一方で、署名の検証鍵は署名者によって構成され、暗号化された状態で公開となる。それぞれのメンバの鍵は、setup-free ではなく Trusted Third Party により生成され配布される必要がある。また、署名の長さはリング署名を構成するメンバの数に依存する。

Traceable Ring Signature [PKC 2007]

Eiichiro Fujisaki and Koutarou Suzuki

tag を利用してリング署名を構成した。署名者は tag ごとに一度だけリング署名を生成することが出来る。署名者が同じ tag を用いて別のメッセージの署名生成を試みた場合、その署名者を特定することが出来る。また、リング署名の構成メンバである署名者以外の者がそのリング署名の生成に用いた tag やメッセージに対して真の署名者に成りすまして署名を生成しようとしても作成することが出来ない方式となっている。このような方式は、例えば電子投票等に利用した場合、投票者の匿名性を保持した上で、2 重投票などを追跡できる・偽造投票を阻止できるなどの利点がある。技術的構成としては、通常のリング署名で署名者が署名を生成する際に選ぶ乱数を tag とリンクさせたある条件下で選択した値で代替し、不正が生じた場合のトレースを可能にしている。

Chosen-Ciphertext Secure Key-Encapsulation Based on Gap Hashed Diffie-Hellman [PKC 2007]

Eike Kiltz

PKI を前提とせずにメッセージを暗号化・復号する仕組みとして KEM/DEM の構成が知られている。本発表ではスタンダードモデルで安全性証明可能な KEM(Key Encapsulation mechanism)を提案している。方式の構成に、GHDH(Gap Hashed Diffie-Hellman)仮定を利用している。この KEM を用いた Hybrid encryption は誰もが検証可能な public verifiability

の性質を有することが出来る。また、従来方式との比較として Kurosawa-Desmedt により Crypto 2004 で発表された方式に比べやや効率の改善が図られている。

A Closer Look at PKI: Security and Efficiency [PKC 2007]

A. Boldyreva, M. Fischlin, A. Palacio, and B. Warinschi

現在の PKI のシステムよりも効率の良い構成方法に対する試み。従来の CA の certificate に相当する部分を Schnorr signature で構成し、その署名を各ユーザの秘密鍵の一部として構成し、ElGamal 暗号タイプの暗号アルゴリズムの構成や Schnorr signature タイプの署名アルゴリズムの構成を示した。提案の構成を用いると、従来 PKI で行なわれる暗号化・署名の演算処理に比べ、その演算量を軽減できるとしている。安全性についても上記のコンセプトに沿ったモデルの提案をしており、そのモデルの中で、PKI ベースで用いられる本来のアルゴリズムがそれぞれ IND-CCA-secure・EUF-CMA の性質を満たせば、上記で提案したアルゴリズムについてもその安全性を保つことが出来るとしている。

Mesh Signatures [Eurocrypt 2007]

Xavier Boyen

リング署名のように、匿名性を壊せるような特定の権限者が存在しないような署名方式の提案。提案方式では、ペアリングを利用して構成するもので、各署名に相当する部分を certificate chain に置き換えることが出来る点などはリング署名の構成に類似した特長となっている。署名サイズは、メンバの数に liner に増加する。また、SDH 仮定を元にもう少し relax した仮定を提示し、それ基づきランダムオラクルを用いずに安全性証明が行える方式となっている。

Cryptanalysis of SFLASH with Slightly Modified Parameters [Eurocrypt 2007]

Vivien Dubois, Pierre-Alain Fouque and Jacques Stern

SFLASH は、2003 年に NESSIE で選ばれたディジタル署名方式で、スマートカードのような低リソースの環境での利用に向いている。SFLASH は有限体上の多変数連立二次方程式の解法の困難性に基づく C^{*-}スキームの一種である。今回の発表では、多くのパラメータ選択に対し C^{*-}スキームが安全でなく攻撃可能であることと、SFLASH のパラメータは攻撃には至らないことが示された。なお、この研究後、A.Shamir との最近の共同研究により、SFLASH 自体も攻撃可能であることが明らかになっており、8 月に開催される Crypto 2007 で発表されることが紹介された。

Divisible e-cash systems can be truly anonymous [Eurocrypt 2007]

Sebastien Canard and Aline Gouget

bank, marchant に対しても匿名性を保てるような、strong unlinkable anonymous divisible off-line e-cach system の提案。提案方式では従来方法の多くが仮定していたTTP（Trusted Third Party）を必要としない。具体的にはuserの秘密鍵とリンクするようなtagを想定し、2重使用の摘出やwithdrawなどをuserの秘密鍵に基づいて行うのではなく、その秘密鍵にリンクしている tag を利用して実現することができる方式となっている。また本提案手法を Nakanishi らの提案した diviable e-cash 方式（bankやmerchant に対しては unlinkable ではない）に適用し、bank や merchant に対しても unlinkable anonymousを確保でき、またTTPを必要としない方式を構成できるとしている。

Indigestion: Assessing the impact of known and future hash function attacks [ECRYPT Hash Workshop 2007]

Eric Rescorla

ハッシュ関数は電子署名などで広く利用されており、近年の MD5 や SHA-1 に対する衝突発見が困難でなくなりつつあることは無視できない問題である。しかし、現在運用されているシステムでは、電子署名の入った証明書の発行以外の手順があるため、最近のハッシュ関数に対する攻撃はそれほど脅威になっていない。もちろん、安全性に問題のあるハッシュ関数の置き換えは進める必要があり、IETF でもプロトコルの更新作業を行っている。

Revisiting security relations between signature schemes and their inner hash functions [ECRYPT Hash Workshop 2007]

The French Saphir Project

フランスでは国家予算を付けて、最近のハッシュ関数に対する攻撃が電子署名の安全性にどのように影響するかを明らかにする French Saphir プロジェクトを推進している。今回はその予備的結果の発表であり、ハッシュ関数がMerkle-Dangard型の場合の解析結果を発表した。非決定論的署名が決定論署名と同じ安全性にしかならないことも示された。

Practical Cryptanalysis of SFLASH [Crypto 2007]

Vivien Dubois, Pierre-Alain Fouque, Adi Shamir and Jacques Stern

SFLASH v2、SFLASH v3 ともに破れることが示された。SFLASHは多変数２次連立方程式に基づく署名方式で、提案者はPatarin, Goubin, Courtoisの３名。求解がNP完全であることが分かっている多変数２次連立方程式がベースとなっており、多変数２次連立方程式の一部を公開鍵とする。全ての連立方程式を公開した C*スキームによる方式が破られたので、方程式の一部を公開しないC*-スキームを採用している。元の方式を守るために、McEliece型の落し戸が利用されている。SFLASH は計算が非常に軽く、ローエンドのスマートカードに適している。SFLASH v2は2003年からNESSIE推奨暗号で、さらに安全性の高いSFLASH v3がある。Eurocrypt 2007 で、SFLASH v2 のパラメータを変更すると攻撃できることが発表されていたが、SFLASH v2 そのものは破られていなかった。本発表では、Eurocrypt 2007

で公開鍵の差分を利用した攻撃法が提案されたが、今回はそれに極座標形式(polar form)を利用することで連立方程式の線形化を行なった。結果: SFLASH v2、SFLASH v3 ともに破れることが示された。ここでの攻撃とは署名を偽造することであり、公開鍵に対する数分間の計算をしておくことで、任意のメッセージに対し 1 秒で偽造署名を生成できることを示した。

Universally-Composable Two-Party Computation in Two Rounds [Crypto 2007]

Omer Horvitz and Jonathan Katz

CRS(Common Reference String)を仮定して、UC(Universally Composable) model で static adversary に対して安全性証明可能な、single-output を出力する 2 party プロトコルを 2 ラウンドで構成する方式を提案。構成ツールとして、Yao の garbled circuit と Tauman の the two-round oblivious transfer protocol と De Santis らの the non-interactive zero-knowledge proofs を利用している。この方式をベースにし、Goldreich のテクニックを用いると two-output を出力するプロトコルを 3 ラウンドで構成できる。2 ラウンドでの構成を実現可能にした技術の効用により、このプロトコルの応用として、UC-secure なブラインド署名を構成することが出来る。

Indistinguishability Amplification [Crypto 2007]

Ueli Maurer, Krzysztof Pietrzak and Renato Renner

複数のシステムの組合せによる複合システムに対する information theoretic な upper bound についての解析結果。複合システム全体の distinguisher の advantage は受動的な攻撃者を想定したとしても、個々のシステムの各々の distinguishability の advantage の積の 2 倍程度に抑えられる。また、能動的な攻撃者を想定した場合、個々のシステムの弱いタイプの攻撃者に対する各々の disinguishability の advantage の和程度に抑えることができることを示した。技術的な注目点としては、distinguishing advantage と証明問題の game-winning probability の reduction の関係を tight に示すことができた点にある

How Many Oblivious Transfers are Needed for Secure Multiparty Computation? [Crypto 2007]

Danny Harnik, Yuval Ishai and Eyal Kushilevitz

Honest なメンバが多数を占めないような party で、セキュアな演算を行うために必要となる OT (Oblivious Transfer)をできる限り少なくする試み。計算量的安全性に基づく場合は、t = (1-ε)n, (n は party の数、ε は 0 より大きな小さな任意の値)の party での演算では O(n)の OT channel で実現可能であることを示した。Beaver(2005,2006) の結果と組み合わせると、任意の関数を計算するのに必要となる time-complexity は O(nk) であることを示した。また、information theoretic な場合もしくは、party の数が小さい場合、それぞれ

のメンバ間で１つのOTを用いて構成するプロトコルで任意の関数がセキュアに計算できることを示している。これらの結果は、information theoreticにセキュアな演算を行うために必要となるOTの数のnecessary conditionは、各々のpartyのメンバ間同士で少なくとも１つのOTを用いることであることを意味していることに近い。構成した関数のデメリットとしてはtime-complexityが partyの数 n に対して指数関数的に増加することである。更に、このtime-complexityの増加を抑えることのできる関数のクラスをも示している。

Secure Identification and QKD in the Bounded-Quantum-Storage Model
[Crypto 2007]

Ivan Damgård, Serge Fehr, Louis Salvail and Christian Schaffner

bounded storage model を前提として、ユーザが量子メモリを全く必要としないidentification schemeを提案。更に、互いに高いエントロピーを持つ共通の秘密鍵kを共有することにより、man-in-the-middle 攻撃に強い方式を提案。いずれの方式もsequential な対話を仮定している。対話に用いる小さなデータ(パスワードなど)や共有する秘密情報 k は再利用可能である。これらの構成を利用し、QKD (Quantum-key-distribution) を構成することができる。従来の方式に比べ、authentication channelを必要とせず、秘密鍵を再利用できるなどの利点を持つ。

A Tight High-Order Entropic Quantum Uncertainty Relation With Applications
[Crypto 2007]

Ivan Damgård, Serge Fehr, Renato Renner, Louis Salvail and Christian Schaffner

bounded-quantum-storage モデルでのセキュアな量子1-out-of-2 OT(Oblivious Transfer)と量子Bit Commitment を提案。また、bounded-quantum-storage モデルでの盗見をする攻撃者に対する現実的な量子鍵配送を提示。standard modelの場合に比べて高いerror rateでも構成可能である。また、min-entropyに基づく uncertain-key の lower boundを求めている。

Reducing Trust in the PKG in Identity Based Cryptosystems [Crypto 2007]

Vipul Goyal

IBE(ID-Based Encryption)での PKG(Private Key Generator)の権限を弱められる方式に対する試み。新たな試みとして accountable authority IBE を考案。ツールとして使う IBEとしては、T-IBE(traceable identity based encryption)を用いた。１つめのアプローチはGentry (2006)が示した方式を利用し、これをT-IBEに変換して利用している。この場合は効率的だが強い仮定を必要とする。2 つ目のアプローチは BDH(Bilinear Diffie-Hellman)仮定に基づき、Waters (2005)が提案したIBEと Sahai-Waters (2005)が提案したFuzzy IBE

を利用して構成するのもである。この場合、一般的な仮定に基づき構成できるが効率はあまりよくなく、復号の度に複数回のペアリング演算の処理が必要となる。実現方式では、ひとつの ID に関連する復号鍵は指数個存在し、ユーザは key generation protocol を通して PKG にどの鍵を実際の private key としたかを知られることなく、自分の decryption key を得ることができる。PKG が不正にあるユーザの復号鍵を生成しようとしても、その行為を追跡することができる、などの利点を持つ。

Scalable and Unconditionally Secure Multiparty Computation [Crypto 2007]

Ivan Damgård and Jesper Buus Nielsen

効率的な multiparty computation プロトコルの提案。C をサーキットのゲート数とし、n を party のメンバ数とし、k を要素のビット長とし、D を演算を行うサーキットの深さとし、κをセキュリティパラメータとする。adaptive で active な攻撃者に対して、攻撃者の数 t が　t< n/3 の場合、通信コスト(communication complexity)は $O(Cn)k + O(Dn^2)k + poly(n\kappa)$に抑えられる。passive な攻撃者の場合、攻撃者の数が t < n/2 に対して通信コストを O(nC)k に抑えることができる。更に adaptive で active な攻撃者に対して、攻撃者の数が t< n/2 の場合、everlasting security と呼ばれるある仮定に基づき、その通信コストを $O(Cn)k + poly(n\kappa)$に抑えるプロトコルも提案。

FPGA Design of Self-Certified Signature Verification on Koblitz Curves [CHES 2007]

Kimmo Ja"rvinen, Juha Forsten, Jorma Skytta"

楕円署名方式で署名検証の高速化に特化した FPGA 実装を設計した。楕円曲線暗号の計算は、NIST が K-163 として規格化した Koblitz 曲線上で高速に実行できる。署名検証は公開鍵暗号系の基本的な操作の一つである。近年、暗号アルゴリズムのハードウェア実装の研究が盛んになっており、特に FPGA 実装において顕著である。事前計算の高速化に効果的な統一的加減算の公式を導き、3 項のスパースな形式の事前計算の新しいアルゴリズムを開発し、楕円曲線上での並列計算における計算時間と単位時間内の処理回数のトレードオフを明らかにした。Altera Stratix II FPGA 向け並列計算用の高効率実装法を開発し、1 秒間に 166,000 回の署名検証を達成した。

Power and EM Attacks on Passive 13.56 MHz RFID Devices [CHES 2007]

Michael Hutter, Stefan Mangard, Martin Feldhofer

AES をソフトウェアとハードウェアで実装した受動的 RFID のプロトタイプに対する電磁波解析攻撃を行ったところ、700 回程度の電磁波観測で鍵が復元できた。RFID の応用は近年急速に広がりつつあり、顕著な例は国際規格 ISO/IEC 14443 に規定された受動的 RFID を利用した非接触スマートカードである。RFID の利用は広まってきた割には、発表されたサイドチャネル攻撃の研究結果は少ない。タイミング攻撃、電力解析、電磁波解析が有効だと

考えられるが、RFIDを対象としたものは今までに3編しか発表されていない。RFIDSec 2005でのCarluccioらによるRFIDに対する電磁波解析、Handshuhがweb上で公開したRSA署名生成の非接触機器に対するラジオ周波数攻撃(Radio Frequency Analysis)、OrenとShamirらがweb上で公開した、電力解析の手法でRFIDタグのパスワードを明らかにした研究。しかし、これらは900MHz前後のUHF領域の周波数帯を使用したものであり、実際に広く使われているのは、HF帯を利用したRFIDである。UHF体での結果はそのままHF帯に適用できない。そこで、13.56MHzのRFIDタグのプロトタイプに対し、電力解析と電磁波解析を適用した。電力解析はRFIDのプロトタイプにおけるディジタル回路とアナログ回路の繋ぎ目に抵抗を入れて観測する。現実のRFIDには適用できないが、電磁波解析による結果との参照用に利用する。電磁波解析のプローブには、ループ型の近接磁場プローブとISO/IEC 10373-6に規定されたHelmholtzアセンブリを利用した。AESをソフトウェア実装したRFIDに対して何種類かの攻撃を試したところ、いずれも成功した。RFIDリーダの領域に置かれた受動型のRFIDでは、700回の波形観測で鍵が復元できた。これは、13.56MHzのRFIDに対するサイドチャネル攻撃の公開された初の成功結果である。

RFID Noisy Reader How to Prevent from Eavesdropping on the Communication? [CHES 2007]

O. Savry, F. Pebay-Peroula, F. Dehmas, G. Robert, J. Reverdy

受動的なPFIDの通信を安全に保つ方法として、送信の際にリーダがノイズを加える方法を提案した。RFIDは物理的な接触が不要で、場所が容易に特定できるといった特長がある。しかし、逆に常に盗聴とプライバシ侵害の危険性が伴う。盗聴対策としては通信データの暗号化やユーザ認証が自然な対策法であるが、状況によってはコストを掛けられない場合がある。受動的な盗聴者に対して防御する場合、物理層の対策で安全性が確保することが可能である。そこで、RFIDに対してリーダが送る電力供給用の信号にノイズを重ねることにより、盗聴者が意味のある情報を入手することを防ぐ方法を開発した。リーダはノイズを除去してRFIDからの応答を受ける。盗聴者のプローブがカードに接触し、カードとリーダの距離が3cmのとき、リーダによる読み取りのビット・エラー率(BER)が10^{-3}で盗聴のBERが0.3を達成した。安全性のレベルは暗号化と比べると低い。また、発表者達がこの方式の特許を所有している。

Round complexity of authenticated broadcast with a dishonest majority [IEEE / FOCS 2007]

Juan Garay, Jonathan Katz, Chiu-Yuen Koo and Rafail Ostrovsky

不正者 t がメンバ全体 n の 1/3 以上である状況で安全なbroadcastを行なうには、何らかのセットアップの条件が必要となる。一般に用いられるものとしては、PKI とディジタル署名であり、authenticated broadcast と呼ばれる。deterministic（決定論的）プロト

コルを用いる場合、少なくとも t +1 ラウンド以上の通信を必要とすることが知られている。ここにランダム化の要素が加わることによる効用の大きさについて考察を行った。結果、不正者の数が n/2+ k の場合、$O(k^2)$程度のラウンド数が必要であり、t が大よそ n/2 + O(1) の場合、ある程度の定数ラウンドで済むこと示された。また、不正者が半数以上の場合は最低限 Ω(2n /n-t)程度のラウンド数は必要であることが示された。

Stronger Security of Authenticated Key Exchange [ProvSec 2007]

Brian LaMacchia, Kristin Lauter and Anton Mityagin

鍵交換プロトコルについて、従来提示されていた安全性証明モデルとしては、カネッティ氏らにより Eurocrypt 2001 提案されている。また、クラウチェック氏により更に考えられうる攻撃が Crypto 2005 で示されている。本発表では、これら従来の安全性モデルで想定されている攻撃を考慮した安全性証明モデルを提案。従来のモデルに比べ、コンパクトで包括的な実システムを反映したモデルとなっており、更に、その安全性モデルの下で安全性証明可能な方式 NAXOS を提案。GDH(Gap Diffie-Hellman 問題)を仮定した方式、および Paring Diffie-Hellman 問題を仮定した方式、を提案した。

An Hybrid Approach for Efficient Multicast Stream Authentication over Unsecured Channels [ProvSec 2007]

Christophe Tartary, Huaxiong Wang and Josef Pieprzyk

Merkle hash tree と TWMDS coding 技術(Tartary-Wang が提案した Maximum Distance Separable(TWMDS) coding) の技術を組み合わせて効率的な認証方式を提案。オリジナルの TWMDS に比べてわずかに通信コストのオーバーヘッドがあるものの、認証に必要となる計算コストを軽減でき、高速な認証方式を実現可能とする。データ全体の確からしさを示すのにディジタル署名のような方法をとるのではなく hash tree の構成を利用して検証に必要となる計算量を軽減することができる。本方式の効果的な適用先としては、ブロードキャスト配信などが挙げられる。

A CDH-based Strongly Unforgeable Signature without Collision Resistant Hash Function [ProvSec 2007]

Takahiro Matsuda, Nuttapong Attrapadung, Goichiro Hanaoka,
Kanta Matsuura and Hideki Imai

(Bilinear) CDH 仮定に基づく ID ベース署名で EUF-CMA 安全が証明されている効率的な署名方式としては、Boneh-Shen-Waters(2005)があり、中で用いるハッシュ関数が CR(衝突発見困難性)を持つことを仮定していた。本提案方式では、ハッシュ関数に対する要求を弱めて、TCR(Target Collision-Resistance)を仮定し、EUF-CMA 安全が証明可能な署名方式を提案した。アイディアとしては、署名の一部分のランダム値が、中で用いられる keyed hash の鍵になるような構成をとり、また、DL ベースのカメレオンハッシュも用いて構成されている。

Does Secure Time-Stamping Imply Collision-Free Hash Functions? [ProvSec 2007]

Ahto Buldas and Aivo Jurgenson

本論文では、Simon(1998)が Black-box モデルで one-way permutation に対して行なったのと同様の手法を用いて、collision-free なハッシュ関数が存在しない中でセキュアなタイムスタンプが存在することが示せるようなオラクルを示し、実際にハッシュ tree による構成方法により、collision-free なハッシュ関数が存在しない状況下でも安全性を保つことの出来るタイムスタンプの構成を示した。このことは、collision-finding attack が存在するようなハッシュ関数を用いて構成されているタイムスタンプであったとしても、そのハッシュ関数の脆弱性がタイムスタンプの安全性に与える影響は極めて小さい、ということである、と主張している。

A Non-Interactive Shuffle with Pairing Based Verifiability [Asiacrypt 2007]

Jens Groth and Steve Lu

近年、効率的として提案されているシャッフル(一般に言う Mix-net を指す)の多くは、完全性を保証するため対話的ゼロ知識証明を用いている。本稿では、シャッフルの完全性証明に用いるゼロ知識証明について、非対話で効率的なものを提案。また、提案手法は Groth, Ostrovsky らにより提案されている bilinear group での 非対話 witness-indistinguishability の証明手法(GS proof と呼ぶ)を利用している。提案する非対話証明に必要となる要素は、入力数 n について、15n 要素必要である。これは、ステートメントのサイズが 6n であることを考えると現実的な大きさであると主張している。

On Privacy Models for RFID [Asiacrypt 2007]

Serge Vaudenay

RFID のタグの認証に注目し、満たされるべき安全性の要求条件により 8 つ安全性レベルを定義し、それらの定義間の帰着関係を示した。ここ 2〜3 年の間、RFID の認証関係の論文は数多く出ているが安全性に関してきちんと議論されているものはあまり多くない。本結果は、今後の RFID の認証方式を提案していく上でも一つの指標になると考えられる。参考までに定義されている安全性レベルは、”strong”, “destructive”, “forward”, “weak”, ”narrow-strong”, “narrow-destructive”, “narrow-forward”, “narrow-weak” である。また、2008 年 3 月に開催される AsiaCCS では本結果を基盤とし、更にリーダの認証を考慮したうえでの安全性レベルについて同様の考察結果が示される予定。

Obtaining Universally Composable Security: Towards the Bare Bones of Trust [Asiacrypt 2007]

Ran Canetti

安全な暗号要素を利用して、安全な暗号プロトコルを設計する方法論として Universally Composable という方法論があるが、実際のシステムに適用しようとすると、信頼できる設定(set-up)を仮定する必要があった。この講演では、いくつかの設定法について調べた結果が報告された。

Group Encryption [Asiacrypt 2007]

Aggelos Kiayias, Yiannis Tsiounis, and Moti Yung

グループ署名と対称的なコンセプトの暗号方式の提案。受取り手の匿名性を確保する暗号方式について、定式化、満たすべき性質として Soundness と Anonymity を提示し、具体的な構成方法を提案。具体的な構成には Paillier encryption をベースに、Decisional Composite Residuosity(DCR) 仮定および、UOWF(Universal One Way Function)の target collision resistance の性質を仮定して構成されている。以前、anonymous encryption として、Moti 氏らが e-print に掲載していた論文の更新版と思われる。

Identity-Based Broadcast Encryption with Constant Size Ciphertexts and Private Keys [Asiacrypt 2007]

Cécile Delerablée

ID ベースブロードキャスト暗号について、コンスタントサイズの暗号文、及び秘密鍵で実現可能な方式を示した。従来法では、暗号文のサイズと秘密鍵のサイズとはトレードオフの関係にあり、暗号文をコンスタントにすると秘密鍵のサイズはコンスタントにすることが困難であった。本稿では、その両方をコンスタントサイズで実現可能な方式を提案している。具体的には KEM-DEM のコンセプトを持ち込み IBE と共通鍵暗号とで構成されている。安全性に関しては、やや一般的でない仮定(General Diffie-Hellman Exponent Assumption)が用いられている。また、安全性レベルは、IND-sID-CCA までが示されている。

Blind Identity-Based Encryption and Simulatable Oblivious Transfer [Asiacrypt 2007]

Matthew Green and Susan Hohenberger

本稿では、DBDH (Decisional Bilinear Diffie-Hellman) 仮定に基づき、Boneh-Boyen (2004) や Waters (2005)のスキームをベースとしたブラインド IBE を提案。さらに、そのブラインド IBE 方式を利用して、送信者および受信者の両者をシミュレート可能な OT(Oblivious Transfer)を示している。ブラインド IBE に関しては、IND-sID-CPA を満たす方式と IND-ID-CPA を満たす方式とがある。提案方式であるブラインド IBE の応用として Privacy-preserving delegated keyword search、ブラインド署名、partially-ブラインド

署名、Temporary anonymous identitiesなどが考えられるとのこと。Open problemとして、DBDH仮定に基づきスタンダードモデルでadaptive な攻撃者に対して安全なブラインドIBEの構成が示された。

Information-theoretic Security without an Honest Majority [Asiacrypt 2007]

Anne Broadbent and Alain Tapp

任意の攻撃者に対して(攻撃者が大多数の場合であっても) information-theoretic に安全なプロトコルを提案。veto, vote, anonymous bit transmission, collision detection, notification, anonymous message transmission 等が具体的に示されている。通信コスト・計算コストはいずれも多項式程度に抑えられる効率的な方式となっていると主張。partyのそれぞれのペアに対して、2種類の秘密鍵と、2種類のauthentic channel を持っていること、およびbroadcast channelが存在することを仮定している。

Anonymous Quantum Communication [Asiacrypt 2007]

Gilles Brassard, Anne Broadbent, Joseph Fitzsimons, Sébastien Gambs, and Alain Tapp

active な攻撃者の数が任意の場合に information-theoretically secure に (匿名の送信者と匿名の受信者との) 量子通信可能なプロトコルの提案。また、提案方式は quantum message のプライバシを守ることが出来る方式となっている。モデルを定義し、提案プロトコルの匿名性について証明を示している。課題の点としては、参加者の誰もが通信を妨害することが出来、またプロトコルを停止させることが出来てしまう点である。

Authenticated Key Exchange and Key Encapsulation in the Standard Model [Asiacrypt 2007]

Tatsuaki Okamoto

DDH(dicisional Diffie-Hellman)仮定・TCR(target collision resistant)なハッシュ関数の仮定・PRFs(pseud-random functions)仮定に基づき、スタンダードモデルで安全性証明可能な Key exchange および Key encapsulation の新しい構成方法を提案。構成方法はredundancy-free(もしくは validity-check free)に構成することが出来る。また、DEM 部分として redundancy-free な共通鍵暗号と組合せることにより、CCA-secure で redundancy-free なハイブリッド暗号を構成することが出来る。

SQUASH – a New MAC With Provable Security Properties for Highly Constrained Devices Such As RFID Tags [FSE 2008]

Adi Shamir

RFIDなどローエンドの環境でも快適に動作するメッセージ認証子方式SQUASHの提案。暗号

名は自乗算(SQUARE)とハッシュ(HASH)を合成したもの。RFID等で用いるメッセージ認証目的に特化して構成してあるハッシュ関数である為、ハッシュのcollision-resigtance などを満たすようには構成されていない。方式に用いるモジュラス n には、Mersenne 数の合成数もしくは、Cunningham prohject number を利用することが提唱されている。この方式は実装性能が具体的に評価されており、またその安全性は、Rabin公開鍵暗号と同等の安全性を持つことが証明できる。

6. その他

Does Privacy Require True Randomness? [TCC 2007]

Carl Bosley and Yevgeniy Dodis

暗号プロトコルにおいて、ランダムソースが利用できない場合 Extractable source（短い乱数から PRNG で長い pseudorandom string を出す）で代替できる。Soundness や Authentication については別に使える source があることが知られているが、Privacy/ Indistinguishability については知られていなかった。本発表では Info-theoretic Private Key Encryption にはほぼ完全な randomness が必須であること、また、seed のビット長を n として (log n - log log n)程度の十分短い平文の暗号化には Extractable-Source は必ずしも必要ないことを示した。

Universally Composable Security with Global Setup [TCC 2007]

Ran Canetti, Yevgeniy Dodis, Rafael Pass and Shabsi Walfish

従来の UC Framework では、セットアップで生成した CRS(Common Reference String) を利用できることを前提としてプロトコルを構成することがほとんどであったが、異なるプロトコル実行の間で CRS を共有することは許されていなかった。よって、一つのセッションが生成されるたびに一つの CRS が必要となっていた。さらに、CRS を作る Functionality は Real-life にのみ存在し、Ideal-model ではシミュレータが CRS を生成するため Real-life と Ideal-model での CRS が（計算量的に識別できないが）同一ではなかった。（別の表現をすれば，攻撃者とシミュレータの間に非対称性が存在していた。）これは効率上問題となるだけでなく、非対話ゼロ知識証明が不可能になるなど、構成上の問題も引き起こしていた。この論文では Real-life と Ideal-model でセットアップ用の functionality を共有する GUC と呼ばれるモデルを提唱した。さらに、すべてのユーザが公開鍵を登録し不正を働いたユーザの秘密鍵が晒されるという 強化 PKI モデルを提案し、そのモデルで任意のプロトコルが GUC(Global Universal Composable) 構成可能であることを示した。（[CLOS02]の構成が GUC でも成り立つことを示した。）

Perfect NIZK with Adaptive Soundness [TCC 2007]

Masayuki Abe and Serge Fehr

NP 完全言語に対する非対話統計的ゼロ知識 argument の構成方法を示した。NI(Non-Interactive)完全言語に対する SNIZK(Statistical Non-Interactive Zero-Knowledge) を構成することは長年の未解決問題の一つであった。Groth らは 2006 年に Subgroup 判定問題に基づいて SNIZK を構成したが、その健全性には CRS(Common Reference String)と証明の statement が独立である、もしくは、証明の statementCRS に比べて十分に小さくなければならないという制限があった。本発表の提案方式では、健全性に制限が無く、従来方式と異なり大きな p に対しても Z_p 上の演算関係を効率的に証明できる、CRS の生成が容易かつ re-use できる、CRS を検証者が提供する場合、ZAP として利用できる、などの特徴を持つ。

Universally Composable Secure Computation Using Tamper-Proof Hardware [Eurocrypt 2007]

Jonathan Katz

UC(Universal Composable) モデルで、プロトコル等の安全性証明をなしえる為には何らかの setup assumption を必要とする。従来結果の多くは、CRS(Common Reference String) 等を仮定している場合が多いが、これは現実の世界では、何らかの信頼できる第 3 者による初期化を仮定するもので、信頼できる第 3 者への依存が大きいとの主張から、他に現実的な setup assumption として物理的な耐タンパデバイスを仮定し、それに基づいた UC モデルでの安全性証明などを示している。

Generic and Practical Resettable Zero-Knowledge in the Bare Public-key Model [Eurocrypt 2007]

Moti Yung and Yunlei Zhao

(sub-exponentially strong な)任意の一方向性関数を仮定した bara public-key モデルで、NP 問題に対する constant -round concurrently sound resettable zero-knowledge (rZK-CS) argument の構成方法を示した。提案方式は、weak (black-box) な意味では、concurrent knowledge-extractability property も満たす方式となっている。構成の中では preimage-verifiable OWF などを用いている。

Zero Knowledge and Soundness are Symmetric [Eurocrypt 2007]

Shien Jin Ong and Salil Vadhan

zero-knowledge argument を持つ NP 問題のクラスの解析を行った。その特徴として、zero-knowledgeness と soundness との間に対称性があることを証明している。すなわち、zero-knowledge argument を持つ $NP \cap coNP$ の問題のクラスはその補集合のクラスに閉じていることを示し、更に、computational zero-knowledge proof があるときのみ

statistical zero-knowledge argument を持つような NP 問題が存在することを示した。この論文は、本会議の最優秀論文賞に選ばれ、他選ばれた2件の優秀論文とともに Journal Cryptology の特別枠に掲載される。

Non-Interactive Proofs for Integer Multiplication [Eurocrypt 2007]

Ivan Damgard and Rune Thorbek

Universal composable な verifiable な非対話証明可能な secret sharing の方法を 2 種類提案。1 つの方式には[ACF]で示されている pederson VSS を利用した方式を導入し、Shamir secret sharing が使われていた部分を Integer Secret Sharing に置き換え、効率化を図っている。Pederson VSS でも Integer Secret Sharing に置き換えることが出来るとしている。2つめは、攻撃者の数が 1/3 より小さい場合に適用可能な方式となっており、pseudorandom secret sharing technique を Integer Secrete Sharing のケースに展開した手法を利用している。これらの方式は、MPC(Multiparty Computation) に有効であり、set-up assumption を前提とし、ランダムオラクルモデルは用いずに安全性証明可能であるとしている。

A Fast and Key-Efficient Reduction of Chosen-Ciphertext to Known-Plaintext Security [Eurocrypt 2007]

Ueli Maurer and Johan Sjodin

弱い擬似ランダム関数*(WPRF: weak pseudorandom function)とは、擬似ランダム関数の条件を弱めた概念である。この論文では、次の３点を実現した。

1. WPRF の出力範囲を広げる最も効率の良い構成法を与える(Range Extension)。
2. WPRF を利用して通常の PRF を構成する方法を提案する。
3. 前２項により、Damgard-Nielsen が提案したものより効率の良い、選択暗号文攻撃に対して安全な暗号スキームが導かれる。

* 定性的な説明では、ランダムな入力列に対する出力列の観測結果から、一様ランダム関数との区別が効率的に出来ない関数。

Improved Analysis of Kannan's Shortest Lattice Vector Algorithm [Crypto 2007]

Guillaume Hanrot and Damien Stehle'

Kannan による最小格子ベクトル探索アルゴリズムの複雑度の上限を改善した。背景: 格子上の最短ベクトル探索問題(SVP)は、NTRU, GGH, Ajtai-Dwork などの公開鍵暗号の安全性の根拠となっている。SVP を解く方法として、小さな凸面体内の格子点を全数探索する検定論的方法があり、暗号研究者には Kannan のアルゴリズムとして知られている。本発表では、格子の探索範囲として、平行多面体の代わりに楕円体を利用した。その結果、探索範囲の変更によって高次元空間内での点生成が高速化され、Helfrich による Kannan アルゴリズム

の計算複雑度の上限が約 $d^{0.5}$*d+o(d)から $d^{0.184}$*d+o(d)に改善した。ここで、d は格子の生成ベクトルの個数。

A Security Analysis of the NIST SP 800-90 Elliptic Curve Random Number Generator [Crypto 2007]

Daniel R.L. Brown and Kristian Gjøsteen

NIST の提唱している NIST SP 800-90 の楕円曲線を利用した random number generator に関する解析結果。次の 3 つの仮定を満たすとき、 ECRNG(Elliptic curve random number generator)は安全であるといえる。すなわち、楕円曲線上での DH 問題の困難性、2 つの新たな問題に対する困難性(x-アルゴリズム問題、truncated point problem) 。truncated problem に関して、NIST が規定している範囲内でごく小さなビット数が truncate されている場合であっても、解けてしまうことがあることを示した。すなわち、ストリーム暗号に用いられているような場合はその安全性を保障できないことを意味している。これらの結果はあったとしても、nonce としての使用や鍵生成などの場合には無害である。

A Generalization of DDH with Applications to Protocol Analysis and Computational Soundness [Crypto 2007]

Emmanuel Bresson, Yassine Lakhnech, Laurent Mazaré and Bogdan Warinschi

一般化した DDH 問題の利用法についての提案。一般化した DDH 問題から従来の DDH 問題へ帰着できることを示した。この一般化した DDH 問題を取扱うことにより、例えば DH ベースの鍵交換プロトコルの安全性証明や computational soundness の証明の簡素化を行なうことができる。但し、これらの結果は、受動的な(Passive)攻撃者についてのみ言及しており、能動的(Active)な攻撃者については今後の Open Problem となっている。

On Secure Multi-Party Computation in Black-Box Groups [Crypto 2007]

Yvo Desmedt, Josef Pieprzyk, Ron Steinfeld and Huaxiong Wang

従来、black-box groups については、アーベル群に限ったものについては結果が示されている。本発表では、アーベル群ではない群における black-box groups の取扱い方についての一般化を行い、セキュアな演算を実現する為には honest なメンバーが半分以上は必要であることを示した。また、k-of-k の秘密分散方式に基づく black-box プロトコルの構成方法示した。これらの結果を planar graph の色の塗り分け問題などに適用すると事が出来る。ここでは 2 種類の構成を提案。1 つ目は、通信コスト(communication complexity)が指数オーダーになってしまうが collision resistance は optimal($t< n/2$, t は不正数、n は全体数)になる構成。2 つ目は、collision resistance はやや劣る($t < n/\mu$, μ は 2.948 以下)が、通信コスト(communication complexity)を $O(nt^2)$程度に抑えることが出来る。

Crypto 2007 BoF [Crypto 2007]

NISTによる"Standardizing New Public Key Crypto Algorithms"とRSA社による"THE RSA CRYPTO CHALLENGE"が企画された。NIST の企画では、参加者の割合は大学・企業半々であった。議論は様々にとび、今後新たに行なうべきか、行なうとしたらその評価手法のスタンスをどの様にするべきか、どの程度先までを見通した方針とするか、新しく出てきている IBE なども検討に入れていくべきか、etc,,,このミーティング内で一致した同意事項などは無く、スタンスとしてNISTが多くの関係者のスタンスや意見を求めた場、となった。

Better price-performance ratios for generalized birthday attacks [SHARCS 2007]

Daniel J. Bernstein

Wagner が提案した誕生日攻撃は効率が高いことが知られているが、それを並列化することで費用性能比を高めた実装の設計を行った。一般化誕生日問題とは、k個($k \geqq 2$)の計算が簡単な出力がBビットの関数$f_1, f_2, \cdots, f_k$に対し、$f_1(x_1)+f_2(x_2)+\cdots+f_k(x_k) \bmod 2^B = 0$ を満たす$m_1, m_2, \cdots, m_k$を求める問題である。なお、B=1 のとき、mod 2^Bを省略し、加算を排他的論理和に置き換えたものになる。この発表では、計算効率向上のため、Wagner の方法と比べ一度に試す(m_1, m_2)や(m_3, m_4)の個数（ベクトルのサイズ）を計算機の容量に合わせて増やした。その結果、Wagner の方法で要求された計算時間と計算機サイズが各々$2^{B/2}$, $2^{B/i}$であったのを、今回の提案手法で各々$2^{B/(2i+1)}$, $2^{2B/(2i+1)}$に削減した。計算機サイズの削減はわずかだが、計算時間は大幅に下がった。

Side Channel Cryptanalysis of a Higher Order Masking Scheme [CHES 2007]

Jean-Se'bastien Coron, Emmanuel Prouff, Matthieu Rivain

SchrammとPaarによるマスクを用いた高次の防御法が、3次の電力差分解析で破れることを示した。DPA対策として守るべき変数を変数d個の和にランダムに分割する高次(d次)マスキング法がある。CT-RSAでSchrammとPaarは、d次マスキングでd次DPAが無効になる防御法を提案した。SchrammとPaarによるd次マスキングに3次の欠陥が存在することを利用し、combining 3次DPAとprofiling 3次DPAという2種類の3次DPA攻撃を利用した。2種類の3次DPAはいずれもd次マスキングを施した回路に対して有効である。

同じ実験でcombining型では正しい鍵推定に必要なサンプルが$4*10^6$個以上であったのに対し、profile 型では 2800 個以上で済み、profile 型がより効率が良い。マスキングの次数が高くても必ず安全性が向上するわけでないことを実証した。profile型は鍵推定の効率が良いが、攻撃者が実装に伴う漏洩パターンを観測できることを仮定しているので、combining型しか使えない状況も少なくない。

High-Speed True Random Number Generation with Logic Gates Only [CHES 2007]

Markus Dichtl, Jovan Golic

ロジックゲートだけを用いて、エントロピーが高く生成速度が速い乱数生成器を設計した。論理ゲートだけで構成された従来の擬似乱数生成器は、回路規模が大き過ぎるか、安定的に製造することが困難なプロセスを利用したものだった。そこで、2 種類のリング振動子、Fibonacci 型と Gauss 型を利用し、FPGA で実装したところ、デジタル論理回路だけを使った擬似乱数生成器で、従来よりもずっと高いエントロピーを実現した。類似のより効率の良い擬似乱数生成器が提案される可能性もあり、これが決定版かどうかは時間を置いて判断する必要がある。

FPGA intrinsic PUFs and their use for IP protection [CHES 2007]

Jorge Guajardo, Sandeep Kumar, Geert-Jan Schrijen, Pim Tuyls

FPGA の IP(Intelectual Property)を守るために、物理的に複製不可能な関数を用いた FPGA に特化した保護方式を開発した。FPGA 上の IP(Intelectual Property)をネットワークで書換える場合、cloning 攻撃に対する防御として暗号化は必須であるが、FPGA が鍵をどのように保管するかが問題となる。解決策として、FLASH のような不揮発メモリを FPGA に着けるか、外付けバッテリーを用意して FPGA 内の RAM を利用するなどの方法があるが、コストが掛り現実的でなかった。そこで、SRAM を利用して物理的クローン不可関数(PUF)を作り、ファジィ関数と誤り訂正などを利用して鍵を作り、IP 保護用のプロトコルを新たに設計し、実験により動作を確認した。SRAM の 1023 ビットから、278 ビットの鍵が作れた。ファジィ関数や誤り訂正を利用しており、安定動作は疑問であり、経年変化も気になるが、オリジナリティは高い。

Evaluation of the Masked Logic Style MDPL on a Prototype Chip [CHES 2007]

Thomas Popp, Mario Kirschbaum, Thomas Zefferer, Stefan Mangard

電力解析攻撃に対する防御法であるマスクロジック・スタイルである MDPL を実装したプロトタイプに対する評価を行った。DPA に対する防御法としてマスクロジックの一種である MDPL(Masked Dual-rail Pre-charge Logic)が提案されている。8051 互換マイクロコントローラを含む 0.13μm のプロトタイプに MDPL を実装し、DPA 攻撃を行なった。その結果、内部メモリ上の 1 バイトに対する MOV 操作に対する DPA で大きな情報漏洩が見られた。シミュレーションで検討したところ、その原因は初期伝播効果(early propagation effect)が原因であることが明らかになった。また、DPA 耐性を改善する MDPL の改良も提案した。

Masking and Dual-rail Logic Don't Add Up [CHES 2007]

Patrick Schaumont, Kris Tiri

DPA に対する防御法であるマスキングと二重レールロジックや事前チャージの組合わせである MDPL を無効にする電力差分解析に成功した。DPA 対策としてマスクロジックが提案さ

れているが、電力消費波形からマスクビット値が推定できるので、簡単なフィルタ処理によって DPA が可能になる。単純なマスクの改良として、マスク二重レールロジックやマスク・プリチャージロジックが提案されている。ルーティングのアンバランスに注目してマスクビットを推定したところ、AES を実装したサンプルに対し、マスクと二重レールロジックを無力化できることがシミュレーションで示しせた。回路の特性に基づいた攻撃法であり説得力がある。

DPA-Resistance Without Routing Constraints? A cautionary note about MDPL security [CHES 2007]

Benedikt Gierlichs

ルーティングに注目した MDPL ゲートに対する攻撃法を示し、DPA に対する防御にはルーティングに対する制限を課す必要があることを指摘した。DPA 対策として MDPL(Masked Dual-rail Pre-charge Logic)が提案され、それを無効にする方法として、グリッチや早期伝播効果(early propagation effect)を利用するものであった。本発表では、MDPL 回路のアンバランスなルーティングと擬似乱数生成器(PRNG)の偏りに注目し、MDPL で防御された AES-128 を実装した VLSI チップに対する実験により、有効性を確認した。前の発表と似た内容であるが、擬似乱数生成系の偏りを仮定している点が異なる。

Information Theoretic Evaluation of Side-Channel Resistant Logic Styles [CHES 2007]

F. Mace, F.-X. Standaert, J.-J. Quisquater

サイドチャネル攻撃に対する防御を施した実装ロジックの攻撃耐性を情報理論的に評価する方法を定式化した。処理時間、消費電力波形、電磁波放射などを利用して暗号系の秘密情報を得るサイドチャネル攻撃とそれに対する防御法は近年盛んに研究されている。ソフトウェアによる対策では、時間やデータのランダム化により物理的漏洩情報と標的となるデータの相関を弱めようとしており、完全な防御にはなっているものはないものの、攻撃を困難にするものと受け入れられている。ハードウェアによる防御法は実装の物理的構造を変更することで実現されている。2006 年に Standaert らは情報理論的尺度とセキュリティの尺度を組合わせてサイドチャネル攻撃を分析する理論的枠組みを発表した。

この論文では次の 3 つの目標を設定した。

(1)情報理論的尺度を利用した各種ハードウェア的対策の分析

(2)シミュレーションに基づくセキュリティ評価の改良

(3)対策のセキュリティ評価に対するボトムアップ的アプローチの開発

相互情報量を評価尺度として次の 6 種類の対策を評価した。

・Sense Amplifier Based Logic (SABL)

・Wave Dynamic Differential Logic (WDDL)

・Dynamic Current Mode Logic (DyCML)

・Low-Swing Current Mode Logic (LSCML)

・Masked Dual-Rail Pre-Charge Logic (MDPL)

・Gammel-Fischer Logic (GF)

3 つ目標の各々について次の結果を得た。

(1)相互情報量を用いて種種の対策による相互情報量の評価式を導出した。

(2)各種対策を施した単一ゲートにおける情報漏出をシミュレーションで評価した。

(3)シミュレーション結果を利用したボトムアップ的アプローチの原型を開発した。

サイドチャネル攻撃を可能とする情報漏出の基礎的物理過程を対象とする本格的な研究である。

Lower bounds on signatures from symmetric primitives [IEEE / FOCS 2007]

Boaz Barak and Mohammad Mahmoody-Ghidary

one-time signature を black-box 形式を持ちいてランダムオラクルから構成する場合いかなるケースも upper bound は、poly (q) 2^q となることを示した。ここで、q は署名オラクル・検証オラクル・鍵生成オラクルなどあらゆるクエリの総数である。この結果は、random permutation や ideal cipher oracle 等にも拡張でき、また、これはディジタル署名と symmetric algorithm(ハッシュ関数、ブロック暗号、mac など)との根本的なギャップを意味する結果となっている。

Post-Processing Functions for a Biased Physical Random Number Generator [FSE 2008]

Patrick Lacharme

物理乱数では0と1の出方に偏りがあるため、後処理が必要となる。この発表では、可変入力長と可変rate に対して、システマティックに偏りの尺度として利用する最小エントロピーによる評価が良くなるような後処理法を設計した。本提案構成は、ハードウェアの構成がコンパクトに出来、ICカード等への搭載に適している。

(Short talk) Entropy of the Internal State of an FCSR in Galois Representation [FSE 2008]

Andrea Ro"ck

キャリー・シフト・レジスタを持ったフィードバック回路(FCSR)は、暗号や擬似乱数生成における基本的構成要素としてしばしば現れる。安全性上、FCSRの内部状態の特定が困難なことが望ましいが、それには内部状態のエントロピーが高いことが要求される。この発表では、内部状態のエントロピーの変化について解析し、1回の状態更新で大きなエントロピー(L/2 bit, ここで L はハミング重み-1 のcarry bit 長) を失い、最終的には周期状態に陥ること、エントロピーはメイン・レジスタのサイズ以下には小さくならないことを導いた。

付録４

公開鍵暗号技術に関する調査報告

平成２０年３月

暗号技術調査ワーキンググループ（公開鍵暗号）

暗号技術調査ワーキンググループ（公開鍵暗号）委員構成

主査：	太田　和夫	電気通信大学
委員：	内山　成憲	首都大学東京
委員：	駒野　雄一	株式会社東芝
委員：	小暮　淳	富士通研究所
委員：	洲崎　誠一	日立製作所
委員：	藤岡　淳	日本電信電話株式会社
委員：	松本　勉	横浜国立大学
委員：	渡辺　創	産業技術総合研究所

委員交代（10 月）

青木和麻呂（日本電信電話株式会社）　→　藤岡淳（日本電信電話株式会社）

下山武司（富士通研究所）　→　小暮淳（富士通研究所）

目次

1. DHについて

1.1. 対象技術

- DH in ANS X9.42
  ANS X9.42, Agreement of Symmetric Keys Using Discrete Logarithm Cryptgraphy, American National Standard for Financial Services, November, 2007.
- DH in NIST SP 800-56A
  NIST Special Publication 800-56A, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised), National Institute of Standards and Technology, March, 2007.

1.2. 技術概要

ANS X9.42は現在の電子政府推奨暗号リストにおけるDHの仕様参照先として指定されている、DH の仕様である。一方、NIST SP 800-56A (以下、SP 800-56A と記す)の方は、DH と ECDH(楕円曲線上の離散対数暗号に基づく DH)を共に含む仕様であり、近年ではDHの仕様として参照されることが多くなっている。ここでは、ANS X9.42と、SP 800-56AのDHに関する部分の間に存在する、技術仕様上および安全性評価上の差異について述べる。下の図 1はDHの簡単なブロック図である。

1.3. 技術仕様

NIST SP 800-56A Appendix A: Summary of Differences between this Recommendation and ANS X9 Standardsには、SP 800-56Aと他の仕様との差異が纏められている。ANS X9.42と SP 800-56A の間に存在する、DH の仕様に関する差異を、この Appendix から抽出すると以下のようになる。

1.3.1. ドメインパラメータ

- FCC ドメインパラメータ生成の際に使用する Hash アルゴリズムについて、SP 800-56A ではHashアルゴリズムを特定しているが、ANS X9.42では明確な規定が無い。
- FCC メインパラメータの生成において、SP 800-56A では素数生成・判定のための Shawe-Taylorアルゴリズムの選択的使用をサポートしているが、ANS X9.42ではサポートしていない。

- FCC ドメインパラメータ生成法の一つとして verifiably random generation を SP 800-56A はサポートしているが、ANS X9.42 ではサポートしていない。
- FFC ドメインパラメータのうち、有限体のオーダーp のサイズについて、SP 800-56A では 1024bit 又は 2048 bit に限定しているが、ANS X9.42 では 1024bit 以上 256bit 刻みである。FFC ドメインパラメータのうち、p-1 の素因数 q について、SP 800-56A では 160bit か 224bit か 256bit に限定しているが、ANS X9.42 では最小サイズを 160bit と限定するのみである。
- FFC ドメインパラメータの識別子について、SP 800-56A では ANS X9.63 と一貫しているが、ANS X9.42 では Annex A で SEED,pgenCounter しか識別されていない。
- static key 生成に使用するドメインパラメータの組 A と ephemeral key 生成に使用するドメインパラメータの組 B について、SP 800-56A ではどのスキームでも同じ組(A=B)を使用しなければならないが、ANS X9.42 では別の組(A≠B)も認める。

1.3.2. スキーム

- DH のスキームの種類について、SP 800-56A では dhHybrid2 を認めていないが、ANS X9.42 では認めている

1.3.3. KDF 関数

- KDF 関数について、SP 800-56A と ANS X9.42 で構造は同一であるが、KDF 関数内部の Hash 関数への入力の構成方法が異なる。
- KDF 関数の OtherInfo について、SP 800-56A では通信する者(party)の識別情報を含むことを要求するが、ANS X9.42 では要求しない。
- KDF を呼んだ後であり、かつ、DerivedKeyingMaterial を発行する前での Shard Secret ゼロ化について、SP 800-56A では要求するが、ANS X9.42 では要求しない。

1.3.4. その他

- 公開鍵の検証について、SP 800-56A では必須であるが、ANS X9.42 では任意である。
- 鍵配送手法について、SP 800-56A では AES key-wrapping のような Approved key-wrapping アルゴリズムの使用を規定しているが、ANS X9.42 では規定がない。
- 鍵確立プロセスにおける Key Confirmation(KC)について、SP 800-56A では KC を行うための包括的な仕様が書かれているが、ANS X9.42 では KC の議論が無い。
- ephemeral key の特殊な場合における例外的な使い回しについて、SP 800-56A では認め

ているが、ANS X9.42 では認めていない。

1.4. 安全性評価

以上の結果を纏めると安全性上の差異に主に次のことが言える。

- DH の FCC ドメインパラメータについては、ANS X9.42 の FCC ドメインパラメータは、SP 800-56A に適合しない場合があるが、SP 800-56A の FFC ドメインパラメータは ANS X9.42 に適合する。
- KDF 関数について差異が存在する。詳しくは本報告書の KDF 関数の項を参照すること。
- その他、DH のスキームの種類、公開鍵の検証、鍵配送手法、鍵確立プロセスについて、SP 800-56A の方がより強い制限を課している。

1.5. まとめ

現在の電子政府推奨暗号リストにおける DH の仕様参照先は ANS X9.42 であり、その安全性は CRYPTREC Report 2002 において検証されている。ANS X9.42 と SP 800-56A の間に存在する技術仕様上の差異について安全性評価だが、KDF 関数以外においては SP 800-56A の方がより厳しい規定を課していると言え、また、KDF 関数についても安全性上の差は無い(あるいは SP 800-56A の方が厳しく規定している面(Shard Secret ゼロ化)がある)。その他については SP 800-56A の方がより厳しい規定を課しているので、SP800-56A について安全性上の問題は無い。

参考文献

[1] ANS X9.42-2001, Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptgraphy, American National Standard for Financial Services, March, 2001.
[2] ANS X9.42-2003, Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptgraphy, American National Standard for Financial Services, November, 2003.
[2] NIST Special Publication 800-56A, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised), National Institute of Standards and Technology, March, 2007.

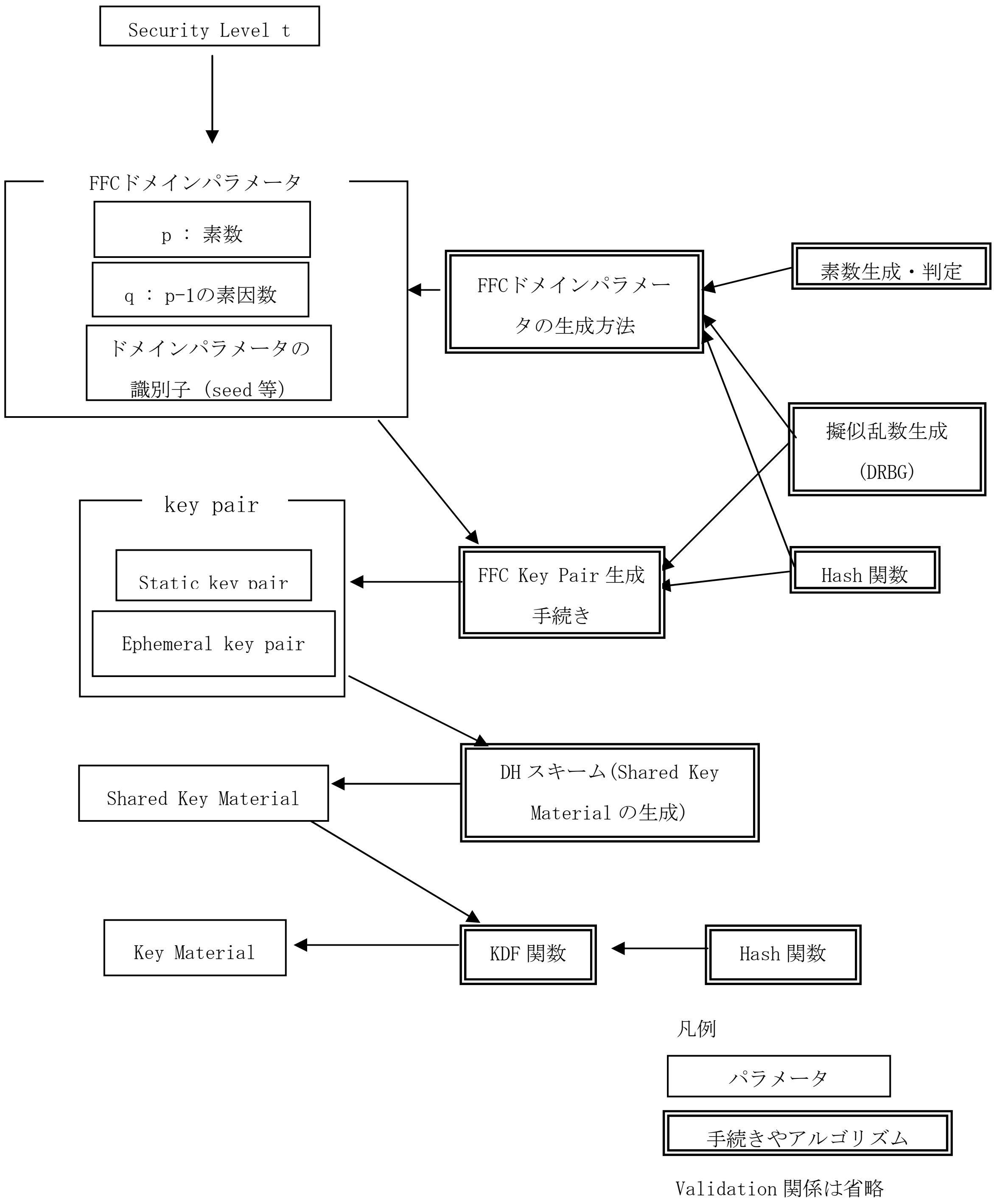


図１ DH における、パラメータや手続きの間の関係

2. ECDSA について

2.1. 対象技術

- ECDSA in SECG SEC 1 v1.0
  Standards for Efficient Cryptgraphy, SEC 1: Elliptic Curve Cryptgraphy, Certicom Research, Ver.1.0, September, 2000.
- ECDSA in SECG SEC 1 v1.7
  Standards for Efficient Cryptgraphy, SEC 1: Elliptic Curve Cryptgraphy, Certicom Research, Ver.1.7(draft), November, 2006.
- ECDSA in ANS X9.62-2005
  ANS X9.62, Public Key Cryptography for the Financial Services Industry The Elliptic Curve Digital Signature Algorithm (ECDSA), American National Standards Institute, November, 2005.

2.2. 技術概要

SECG SEC 1 v1.0 (以下、SEC 1 v1.0 と記す)は現在の電子政府推奨暗号リストにおける ECDSA の仕様参照先として指定されている、ECDSA の仕様である。一方、ANS X9.62 の方は、ECDSA の仕様であり、近年では ECDSA の仕様として参照されることが多くなっている。SEC 1 v1.0 の改訂版である Draft SEC 1 v1.7 (以下、SEC 1 v1.7 と記す)も ANS X9.62 に仕様を近づける方向で改訂されている。SEC 1 v1.0 の技術仕様および安全性評価については CRYPTREC Report 2002 に記述されている。ここでは、SEC 1 v1.0 と、ANS X9.62 の ECDSA に関する部分の間に存在する、技術仕様上および安全性評価上の差異について述べる。

2.3. 技術仕様

以下に、SEC 1 v1.0 の ECDSA に関する部分と、ANS X9.62 の ECDH の間の差異を列挙する。適宜、SEC 1 v1.7 との差異も述べる。尚、ANS X9.62 という場合は ANS X9.62-2005 を指すものとする。下の図 2 は ECDSA の簡単なブロック図である。

2.3.1. Security Level

- Security level t について、ANS X9.62 では 80 以上の 5 段階に限定(これは SEC 1 v1.7 と同じ)しているが、SEC 1 v1.0 では 56 以上 8 段階を指定している。

2.3.2. ドメインパラメータ

- 有限体 F_p 上に楕円曲線を取る場合の ECC ドメインパラメータの一つである p の bit 長と基点 G について。SEC 1 v1.7 では p の bit 長は Security level t に従って決められ、その値は SEC 1 v1.0 と同じかそれ以上である。一方、ANS X9.62 ではその制限に加え、基点 G の位数 n について Security level t による制限がある。
- ECC ドメインパラメータの一つである基点 G について、ANS X9.62 や SEC 1 v1.7 では SEC 1 v1.0 に比べ、MOV 条件等などを考慮したより厳しい条件が課されている。また、ANS X9.62 では、G の位数 n について Security level t による制限がある。
- 有限体 F_2m 上に楕円曲線を取る場合の ECC ドメインパラメータである m と、有限体を表現する多項式 f(x)と基点 G について、SEC 1 v1.0 と SEC 1 v1.7 では Security level t に従って決められている。一方、ANS X9.62 ではその制限に加え、基点 G の位数 n について Security level t による制限がある。
- ECC ドメインパラメータのランダムな生成方法について、ANS X9.62 では方法を規定しているが、SEC 1 v1.0 および SEC 1 v1.7 では「ランダムにドメインパラメータをする場合には」という形で ANS X9.62 に言及しているのみである。
- ECC ドメインパラメータの具体値について、ANS X9.62 では NIST FIPS 186-2 に記載されたものを強く推奨しているが、SEC 1 v1.0 では SECG SEC 2 に記載されたものを推奨している。FIPS 186-2 に記載されている ECC ドメインパラメータ具体値の集合は、SEC 2 に記載されている ECC ドメインパラメータ具体値の集合のサブセットである。

2.3.3. 擬似乱数

- 乱数である秘密鍵 d について、ANS X9.62 では、HMAC を使った DRBG を規定し、それを使って生成することと規定している(この HMAC を使った DRBG は ANS X9.82 として規定されている)。一方、SEC 1 v1.0 では擬似乱数生成器についての規定は無い。SEC 1 v1.7 では、ANS X9.82 や NIST SP 800-90 に準拠した DRBG を使って生成することと規定している。

2.3.4. その他

- 署名生成や署名検証において使う Hash 関数について、ANS X9.62 では X9 Registry Item 00003 SHS に準拠するとしているが、SEC 1 v1.0 では SHA-1 と規定している。SEC 1 v1.7 では SHA-224、SHA-256、SHA-384、SHA-512 が追加されている。
  なお、SEC 1 v1.7 では、SEC 1 v1.0 や ANS X9.62 には無い、Assisted Key Generation、self-signing、公開鍵の recovering などの手続きが規定されている。

2.4. 安全性評価

以上の結果を纏めると安全性上の差異について主に次のことが言える。

- ECC ドメインパラメータについて差異が存在する。その安全性評価については、本報告書の楕円曲線ドメインパラメータの項を参照すること。
- security level と擬似乱数生成器について、ANS X9.62 の方がより強い制限を課している。

2.5. まとめ

現在の電子政府推奨暗号リストにおける ECDSA の仕様参照先は SEC 1 v1.0 であり、その安全性は CRYPTREC Report 2002 において検証されている。SEC 1 v1.0 と ANS X9.62-2005 の間に存在する技術仕様上の差異についての安全性評価だが、ECC ドメインパラメータについては ANS X9.62-2005 が SEC 1 v1.0 に比べて安全性が低下している点はなかった。一般的には ANS X9.62-2005 の方がより厳しい規定を課している。よって、ANS X9.62 について安全性上の問題は無いと考えられる。

参考文献

[1] ANS X9.62-1998, Public Key Cryptography for the Financial Services Industry The Elliptic Curve Digital Signature Algorithm (ECDSA), American National Standards Institute, January, 1999.

[2] ANS X9.62-2005, Public Key Cryptography for the Financial Services Industry The Elliptic Curve Digital Signature Algorithm (ECDSA), American National Standards Institute, November, 2005.

[3] Standards for Efficient Cryptgraphy, SEC 1: Elliptic Curve Cryptgraphy, Certicom Research, Ver.1.0, September, 2000.

[4] Standards for Efficient Cryptgraphy, SEC 1: Elliptic Curve Cryptgraphy, Certicom Research, Ver.1.7(draft), November, 2006.

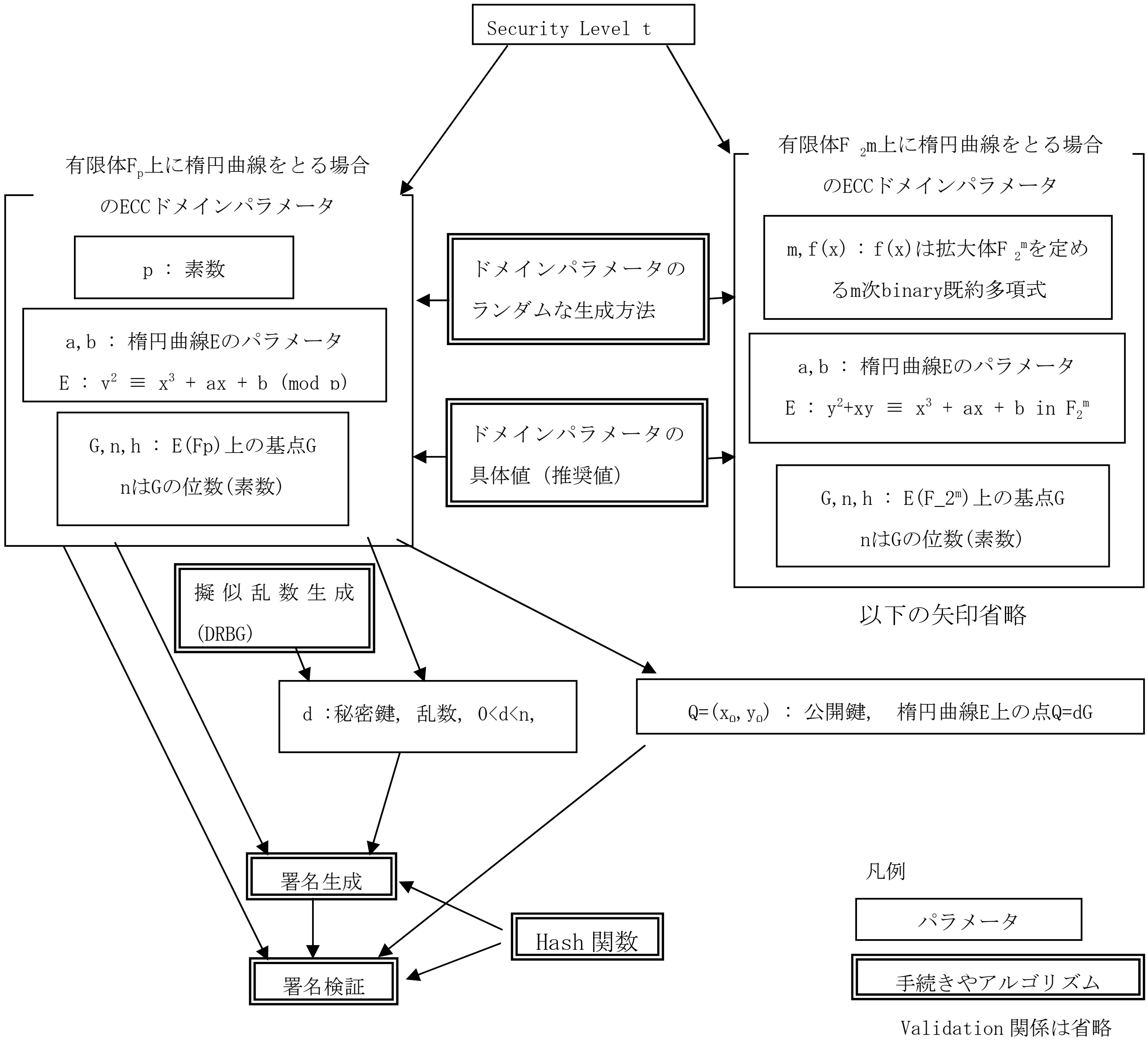


図２　ECDSA における、パラメータや手続きの間の関係

3.　ECDHについて

3.1. 対象技術

- ECDH in SECG SEC 1 v1.0
  Standards for Efficient Cryptgraphy, SEC 1:Elliptic Curve Cryptgraphy, Certicom Research, Ver.1.0, September, 2000.
- ECDH in NIST SP 800-56A,
  NIST Special Publication 800-56A, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised), National Institute of Standards and Technology, March, 2007.

3.2. 技術概要

SEC 1 v1.0は現在の電子政府推奨暗号リストにおけるECDHの仕様参照先として指定されている、ECDSAとECDHを共に含む仕様書である。一方、SP 800-56Aの方は、DHとECDHを共に含む仕様書であり、近年ではECDHの仕様として参照されることが多くなっている。ここでは、SEC 1 v1.0のECDHに関する部分と、SP 800-56AのECDHに関する部分の間に存在する、技術仕様上および安全性評価上の差異について述べる。下の図3はECDHの簡単なブロック図である。

3.3. 技術仕様

以下に、SEC1 v1.0のECDHに関する部分と、SP 800-56AのECDHに関する部分の間の差異を列挙する。なお、現在、SEC 1のVer.1.7がdraftとして発表されているが、このSEC 1 v1.7との差異や、ANS X9.62-2005との差異についても適宜述べる。

3.3.1. Security level

Security level(SP 800-56AではSecurity Strengthと呼ぶ) tについて、SP 800-56Aでは80以上の5段階に限定(これはSEC 1 v1.7と同じ)しているが、SEC 1 v1.0では56以上8段階を指定している。

3.3.2. ドメインパラメータ

ECCドメインパラメータについて、仕様内部で規定するのは条件のみであり、生成方法や

具体値については他の仕様を参照しているところは、SP 800-56A でも SEC 1 v1.0 でも同じである。

ECC ドメインパラメータのランダムな生成方法について、SP 800-56A では ANS X9.62-2005 Annex A.3 に示される方法であることを規定しているが、SEC 1 v1.0 では「ランダムにドメインパラメータをする場合には」という形で ANS X9.62 に言及しているのみである。

ECC ドメインパラメータの具体値について、SP 800-56A では FIPS 186-2 に記載されたものを強く推奨しているが、SEC1 v1.0 では SECG SEC 2 に記載されたものを推奨している。FIPS 186-2 に記載されている ECC ドメインパラメータ具体値の集合は、SECG SEC 2 に記載されている ECC ドメインパラメータ具体値の集合のサブセットである。

3.3.3. 擬似乱数

乱数である秘密鍵 d について、SP 800-56A では FIPS 186-3 Appendex B.4 に定める生成手続きに従うと規定し、FIPS 186-3 Appendex B.4 では擬似乱数生成器について NIST SP 800-90 に記載されたものと規定している一方、SEC 1 v1.0 では擬似乱数生成器についての規定は無い。

3.3.4. DH プリミティブ

DH プリミティブについては standard と cofactor の 2 種類があるが、SP 800-56A では cofanctor のみしか認めていないのに対して、SEC1 v1.0 では standard と cofactor の両方を認めている。

3.3.5. KDF 関数

KDF 関数について、SP 800-56A では concatenation-KDF と ASN1-KDF という 2 種類を規定し、さらに NIST FIPS 140-2 に準拠したものは使用可能としているが、SEC 1 v1.0 では ANS X9.63 に規定がある KDF 関数を使用するとしている。これらは、KDF 関数の構造は同一だが、KDF 関数内部の Hash 関数への入力の構成方法や、その入力の一部である OtherInfo のコードが異なる。

KDF 関数の内部で使用する Hash 関数について、SP 800-56A では FIPS 180-2 に準拠したものと規定しているが、SEC 1 v1.0 では SHA-1 と規定している。

3.3.6. 鍵とスキーム

static key と ephemeral key と ECDH のスキームの種類について。SP 800-56A では static key と ephemeral key について明確に区別している。その上でその区別によって生じる 5 種類の ECDH スキームを規定している。一方、SEC1 v1.0 では、static key と ephemeral key の明確な区別はなく、1 種類の ECDH スキームを規定している。この差異点については次に詳述する。

3.3.7. key の区別とスキームの種類について

SP 800-56A では key を、static key と ephemeral key とに区別している。

- ephemeral key：トランザクション毎に変えること(を通常とする)key
- static key：鍵交換のエンティティや秘密鍵のオーナーと結び付いた key であり、ephemeral key より長寿命な key

その上でその区別によって生じる 5 種類の ECDH スキームを規定している。例えば、鍵交換に参加するエンティティ 2 者について

- 両エンティティが ephemeral key のみを生成、交換するスキーム C(0,2)
- 両エンティティが static key のみを生成、交換するスキーム
- 両エンティティが static key と ephemeral key の両方を生成、交換するスキーム

という種類のスキームが 5 種類のスキーム中に含まれる。

一方、SEC1 v1.0 では、static key と ephemeral key の明確な区別はないが、以下の 2 点から、SEC1 v1.0 における key は SP 800-56A における ephemeral key に相当すると考えられる。

- SEC1 v1.0 では、key の development(Section6.1.2)と KDF 関数を使った key agreement (Section6.1.3)は単純に直列して行われる、つまり transaction 毎に key が生成されることになる
- 生成した public key の assurance of validity の取得手続きという観点から見ると、SP 800-56A の public key についての手続きは、SEC1 v1.0 の ephemeral public key についての手続きをやや厳しくしたものである

SEC1 v1.0 の ECDH スキームは、事実上、SP 800-56A の C(0,2)スキーム(ephemeral key のみを使う最も簡単な構造のスキーム)について制限をやや緩和したものと考えられる。

SEC1 v1.0 の key と、SP 800-56A の ephemeral key と、SP 800-56A の static key という、三者の間に存在する差異について、それらの生成や、assurance of validity を得る手続きという観点からまとめた表を以下に示す。

	SEC1 v1.0 key pair	SP 800-56A ephemeral key pair	SP 800-56A static key pair
公開鍵Qのvalidation手続き	Qとドメインパラメータの整合性をチェックする手続き (3.2.2.1)	Qとドメインパラメータの整合性をチェックする手続き (5.6.2.5)	Qとドメインパラメータの整合性をチェックする手続き (5.6.2.5)
鍵を生成する者	鍵交換に参加するエンティティ、あるいは trusted party	鍵交換に参加するエンティティ	鍵交換に参加するエンティティ、あるいは TTP
エンティティとIndentifierとの関係	特に規定せず	特に規定せず	関係すると規定
Ass. of Val.を得る公開鍵	交換相手エンティティから受け取った公開鍵	交換相手エンティティから受け取った公開鍵	交換相手エンティティから受け取った公開鍵 自分の公開鍵(Owner である公開鍵)
公開鍵のass. of val.を得る手続き・方法	次のいずれか (3.2.2) validation手続き(3.2.2.1)を使う trusted party(通常はCA)がvalidation 手続き(3.2.2.1)を使って得たものを得る。 trusted system を使って作ったkeyを使う trusted party(通常はCA)がtrusted system を使って作ったkeyを使う	次のいずれか(5.6.2.3) validation手続き(5.6.2.5)を使う TTPから得る	次のいずれか(5.6.2.1)(5.6.2.2) validation手続き(5.6.2.5)を使う TTPから得る TTP が(5.6.1)の鍵生成手続きに準拠して作ったkeyを使う 但し、相手のIdentifierと公開鍵をtrusted manner で受け取ること (Owner の公開鍵のass.of val.は、(5.6.1)の鍵生成手続きに準拠して鍵を生成したことで得られたとすることも可能)
部分val.を認めるか	認める(3.2.2)	認める(5.6.2.3)	認めない
秘密鍵に関して得るass.	規定無し	規定無し	正しい値の秘密鍵の所有に関するass.

ass.はassuranceの略。val.はvalidity の略。

部分val.とは、公開鍵をQとして、nQ=0のチェックを行わないvalidation。

(3.2.2.1)等は仕様における章節番号を示す。

3.4. 安全性評価

以上の結果を纏めると安全性上の差異について主に次のことが言える。

- ECC ドメインパラメータについて差異が存在する。その安全性評価については、本報告書のドメインパラメータの項を参照すること。
- KDF 関数について差異が存在する。詳しくは本報告書の KDF 関数の項を参照すること。
- security level、擬似乱数生成器、standard なプリミティブの使用、について、SP800-56A の方がより強い制限を課している。
- ECDH スキームについて、SP800-56A に規定されている 5 種類のスキームのうち、ephemeral key のみを使う最も構造の単純なスキームが、SEC1 v1.0 のスキーム(それにより強い制限を課したもの)に相当する。static key を使う、SP800-56A のその他 4 種類のスキームについては、static key の assurance 等に厳しい規約を課しているものの、その安全性は改めて検証されることが必要である。

3.5. まとめ

現在の電子政府推奨暗号リストにおける ECDH の仕様参照先は SEC 1 v1.0 であり、その安全性は CRYPTREC Report 2002 において検証されている。SEC 1 v1.0 と SP 800-56A の間に存在する技術仕様上の差異についての安全性評価だが、ECC ドメインパラメータについては SP 800-56A が SEC 1 v1.0 に比べて安全性が低下している点はなく、KDF 関数についても安全性上の差は無い。ECDH スキームについては、SP 800-56A の ephemeral key のみを使うスキームは SEC 1 v1.0 のスキームに相当し、安全性上の問題はない。これら以外の点については SP 800-56A の方がより厳しい規定を課している。よって、SP800-56A のうち ephemeral key のみを使うスキームについては、安全性上の問題は無いと考えられる。

参考文献

[1] Standards for Efficient Cryptgraphy, SEC 1:Elliptic Curve Cryptgraphy, Certicom Research, Ver.1.0, September, 2000.

[2] NIST Special Publication 800-56A, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised), National Institute of Standards and Technology, March, 2007.

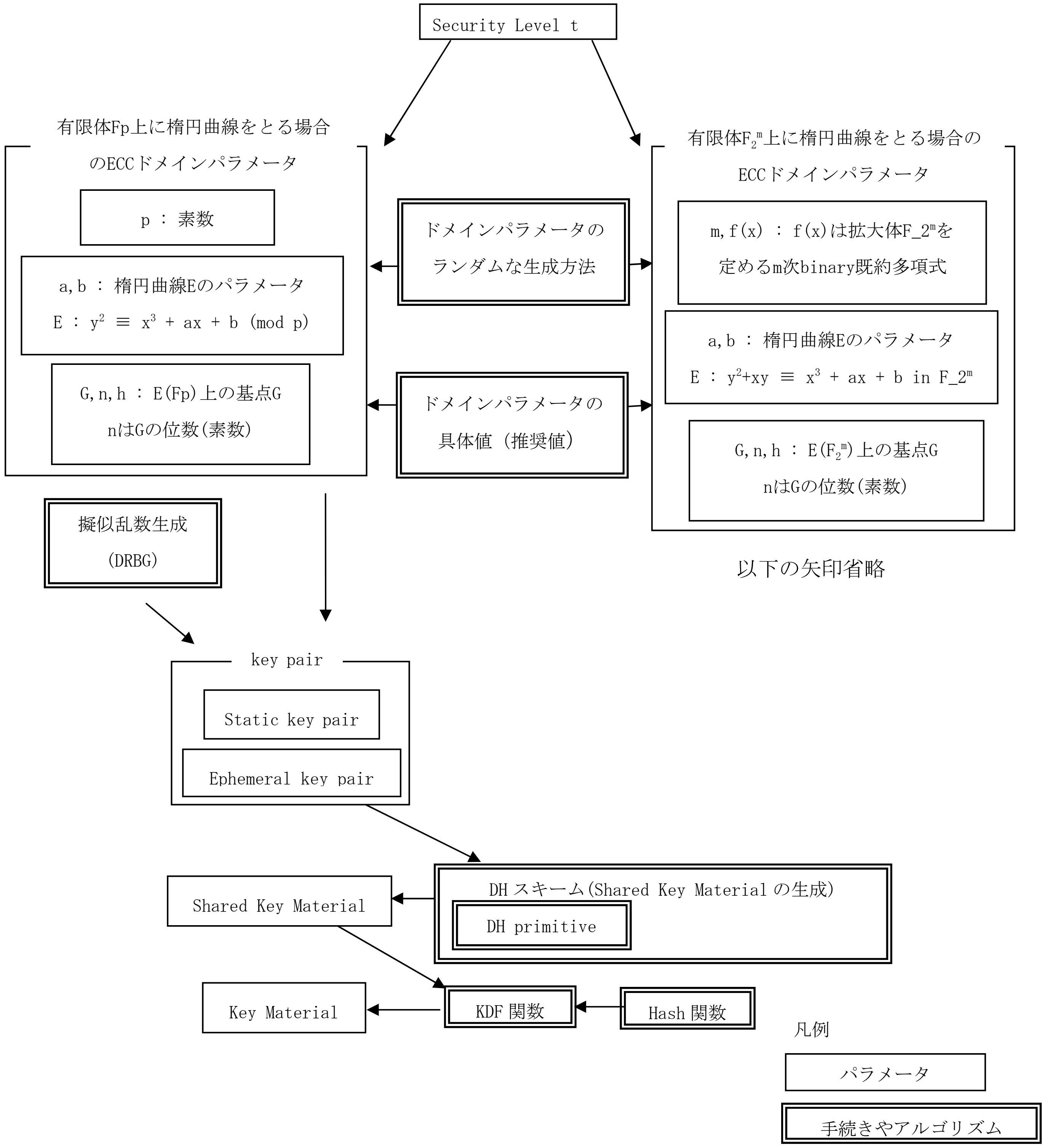


図 3　ECDH における、パラメータや手続きの間の関係

4.　PSEC-KEM について

4.1. 対象技術

ISO/IEC 18033-2 の審議過程において、エディタ並びに各国からのコメント等を吸収する形で提案された仕様に一部修正が加えられ、最終的に規格化されたものが電子政府推奨暗号リスト策定時のものと若干異なる仕様となった。そこで仕様書の変更の妥当性を判断できる資料を作成するために今年度安全性評価が行われた。評価に当たっては、提案者に新たに資料の提出を求めた。

- PSEC-KEM[1]
  PSEC-KEM Specification version 2.1, NTT Information Sharing Platform Laboratories, NTT Corporation, January 18, 2008 [注]

4.2. 技術概要

KEM は、別途定義される DEM と組み合わせることにより、IND-CCA2 の証明可能安全性を有する守秘目的のハイブリッド暗号を構成する(KEM-DEM 構成)。KEM-DEM 構成では、まず、KEM により、公開鍵暗号ベースでセッション鍵を送受信者双方で共有する。一方、DEM は共通鍵暗号部(SYM)と通信文の安全性を保障するための認証子生成部(MAC)からなる。送信側は、平文を SYM においてセッション鍵で暗号化し、また、平文に対して MAC で認証子を生成し、双方を結合して暗号文として伝送する。受信側は、暗号文を分割し、まず SYM においてセッション鍵で復号し復号文を求める。次に、復号文に対して MAC で認証子を生成して、送信側から送信されたものと比較して両者が一致していれば、復号文を出力する。

KEM-DEM 構成は、他の IND-CCA2 を満たす方法に比べ、長い平文を効率的に暗号化でき、

[1] http://www.cryptrec.go.jp/method.html から入手可能。

注： 第 3 回暗号技術検討会開催後、主に型変換関数に関する修正等が施された仕様書の再提出があった（2008 年 4 月 14 日)。それらの修正等は安全性には影響がないものと判断されたため、年度内での検討結果と併せ、最終的に 2008 年 4 月 14 日版である、
PSEC-KEM Specification version 2.2, NTT Information Sharing Platform Laboratories, NTT Corporation, April 14, 2008（及びその日本語版）
が仕様参照先として適当であると判断された。

また証明可能安全性を満たす KEM と DEM を独立に構成することにより、高いフレキシビリティを有する。KEM、および DEM を構成する SYM と MAC の証明可能安全性のインフォーマルな定義は次の通りである。

KEM : いかなる(多項式時間の) 攻撃者 A も、KEM の暗号文 C とビット列 K が与えられたとき、復号オラクルを用いて、ビット列 *K* が KEM により得られる正しい共有鍵 *Key* か、あるいはランダムなものかを有意な確率で判別できない

- SYM : 攻撃者Aが選んだ2つのメッセージのいずれかに対応した暗号文が得られたとき、その暗号文からもとのメッセージのいずれであるかを有意な確率で判別できない
- MAC : 使い捨ての鍵で生成されるOne-timeの認証子生成関数である

4.3. 技術仕様

PSEC-KEM の仕様(概要)は以下の通りである。詳細については、仕様書を参照されたい。PSEC-KEM は、以下に述べる鍵生成アルゴリズム KGP-PSEC, 暗号化アルゴリズム ES-PSEC-KEM-ENCRYPT 及び復号アルゴリズム ES-PSEC-KEM-DECRYPT からなる。

鍵生成アルゴリズム KGP-PSEC

PSEC-KEM では楕円曲線上の演算を行うため、まず、適切な楕円曲線 E 及びベースポイント P を決める。その後、以下の処理を行って公開鍵 PK 及び秘密鍵 SK を出力する。

1. 乱数 $s \in \{0,...,p-1\}$を生成
   ここで、p はベースポイント P の位数とする
2. W = sP を計算
3. 公開鍵 PK を PK = W として出力
4. 秘密鍵 SK を SK = s として出力

暗号化アルゴリズム ES-PSEC-KEM-ENCRYPT

暗号化アルゴリズム ES-PSEC-KEM-ENCRYPT は、PK を入力とし、暗号文 C 及び keyLen オクテットの共有鍵 K を出力する。

1. hLen オクテットの乱数 r を生成
2. (pLen + 16 + keyLen)オクテットの H = KDF(0x00000000||r)を生成
3. H を H = t || K として、H を(pLen + 16)オクテットの t と keyLen オクテットの K に分

割

4. α = t mod p を計算

5. Q = αW, C1 = αP を計算

6. hLen オクテットの H’ = KDF(0x00000001||C1||Q)を生成

7. hLen ビットの C2 = r $\oplus$ H’ を生成

8. 暗号文 C = C1||C2、及び共有鍵 K を出力

復号アルゴリズム ES-PSEC-KEM-DECRYPT

暗号アルゴリズム ES-PSEC-KEM-DECRYPT は、SK (=s)及び暗号文 C を入力とし、keyLen オクテットの共有鍵 K（もしくは“invalid”)を出力する。

1. 暗号文 C (= C1||C2)を C1 と C2 に分割　C2 は hLen オクテット

2. Q = sC1 を計算

3. hLen オクテットの H = KDF(0x00000001||C1||Q)を生成

4. hLen オクテットの r = C2 $\oplus$ H を生成

5. (pLen + 16 + keyLen)オクテットの G = KDF(0x00000000||r)を生成

6. G を G = t || K として、G を(pLen + 16)オクテットの t と keyLen オクテットの K に分割

7. α = t mod p を計算

8. C1 = αP が成立するかどうか検証

9. 成立すれば共有鍵 K を出力　(成立しなければ“invalid”を出力)

4.4. 安全性評価

●KEM の安全性

KEM (Key Encapsulation Mechanism)の IND-CCA2 (適応的選択暗号文攻撃に対して強秘匿)の定義は，公開鍵暗号方式の IND-CCA2 の定義と異なり，以下のように定義される.

「いかなる（多項式時間）攻撃者も，KEM の暗号文とビット列が与えられたとき，攻撃対象の暗号文を除いて自由に復号オラクルを用いても，ビット列が KEM で得られる正しい共有鍵かランダムなビット列かを有意な確率で識別することができない」

●安全性に影響を与える仕様変更部分

CRYPTREC 活動の成果として，総務省及び経済産業省から公表された「電子政府推奨暗号リスト」[2]に掲載された PSEC-KEM 仕様書 [2](以下,旧仕様)と,変更依頼のあった PSEC-KEM Specification version 2.1 [3] (以下，新仕様)との差異を表 1 にまとめる.

表 1. 2 つの仕様間の差分

番号	項目	旧仕様	新仕様
1	データ表現	ビット単位	オクテット単位
2	エンコード	ECP2OSP	ECP2OSP， PECP2OSP
3	公開鍵 システムパラメータ	*PK*=(E,W,*KDF*,*hLen*) なし	W E,*KDF*,*hLen*,*keyLen*
4	処理のサブルーチン化	あり	なし
5	ハッシュ関数	SHA-1	SHA-1,SHA-224,SHA-256 SHA-384， SHA-512
6	安全性のパラメータ	*pLen*≧160， *hLen*≧128	*pLen*≧20， *hLen*≧16
7	推奨値	*pLen*=160， *hLen*=160 *KDF*=MGF1(SHA-1, *hashLen*=160), R=Compressed *keyLen*=256	*pLen*=32， *hLen*=32 *KDF*=MGF1(SHA-256, *hashLen*=32), R=Compressed *keyLen*=32
8	付録(高速計算法)	記載あり	記載なし
9	付録(ASN.1)	記載なし	記載あり
10	復号時のエラー判定	等号あり	等号なし

●安全性への影響

表 1 の差分が安全性に与える影響についてまとめる.

1. データ表現 新仕様は，旧仕様を 8 ビット単位に限定した処理であり，この変更による安全性の低下は起こらない.

2. エンコード 安全性証明においてランダムオラクルであると仮定する *KDF* への入力が異なるため，証明の見直しが必要となる．実際，新仕様では異なる問題を経由して安全性を

[2] http://www.cryptrec.go.jp/list.html 及び本書の付録 1 を参照のこと。

証明する．安全性の根拠としては以下の計算困難とされる仮定を用いる．

・楕円曲線上の List DH 仮定：任意の多項式時間攻撃者 A で次がなりたつ：

$$\Pr[\mathrm{List} = \{Q_1, ..., Q_l\} \leftarrow A(P, aP, W) : aW \in \mathrm{List}] = \mathrm{negl}$$ [3]

・楕円曲線上の List xDH 仮定：任意の多項式時間攻撃者 A で次がなりたつ：

$$\Pr[\mathrm{xList} = \{x_1, \cdots, x_l\} \leftarrow A(P, aP, W) : x_{aW} \in \mathrm{xList}] = \mathrm{negl}$$

このとき，旧仕様と新仕様の安全性は以下のように証明される．

・旧仕様

- 楕円曲線上の List DH 仮定がなりたてば，旧仕様は IND-CCA2 をみたす

・新仕様

- 楕円曲線上の List DH 仮定がなりたてば，楕円曲線上の List xDH 仮定がなりたつ
- 楕円曲線上の List xDH 仮定がなりたてば，新仕様は IND-CCA2 をみたす
- 楕円曲線上の List DH 仮定がなりたてば，新仕様は IND-CCA2 をみたす

3. 公開鍵・システムパラメータ 現在の安全性モデルにおいては，公開鍵の利用者に依存しない変数を共有化しても安全性は低下しない．

4. 処理のサブルーチン化 処理手順の記述の差異のみで安全性には影響しない．

5. ハッシュ関数 SHA-224,SHA-256,SHA-384,SHA-512 を用いることで，現実的な安全性を向上させることができる．ハッシュ関数は安全性証明においてランダムオラクルと仮定する *KDF* の一部であり，証明可能安全性の観点からは安全性に影響しない．

6. 安全性のパラメータ データ表現による数値の差分のみで，現実的な観点でも，証明可能安全性の観点でも，安全性には影響しない．

7. 推奨値 推奨値を増大することで，現実的な安全性を向上させることができる．証明可能安全性の観点では，変数として議論が進められるため，安全性は影響しない．

8,9. 付録 付録記載の内容は実装に関する情報であり，安全性には影響しない．

10. 復号時のエラー判定 暗号文の長さが *hLen* と等しいとき，旧仕様では条件判定の等号

[3] 確率が指数関数的に小さくなることを意味する。

がなりたつことでエラー処理が実行される．新仕様では，条件判定ではエラー処理が実行されないが，OS2ECPP に不正な引数が渡されてエラー処理が実行されるため動作は本質的に同じになる．これらの処理は，安全性をモデル化する上でも同一視されるため，安全性には影響しない．

●安全性評価結果
新仕様の安全性は，ISO 規格になっている PSEC-KEM の安全性証明［1］と同様に示すことができる．ISO 規格は，PSEC-KEM を構成する群を楕円曲線上の加法群に限定せず，新仕様を包含する関係にある．すなわち，文献[1］の証明を楕円曲線上の群に限定して議論することで，新仕様の安全性を保証することができる．

新仕様は，以下の定理に示すように，ランダムオラクルモデルにおいて，楕円曲線上の List DH 仮定がなりたつならば，IND-CCA2 であることが確認できる．旧仕様と比べて，安全性評価結果の帰着効率が 2 倍程度低下するが，安全性への影響は小さいといえる．

定理１
新仕様に記載された PSEC-KEM の IND-CCA2 を実行時間 t，優位度 e で破る攻撃者が存在するならば，楕円曲線上の List DH 問題（リストの要素の個数は $O(q_1+q_D)$）を実行時間 t’，成功確率 e’で解くアルゴリズムが構成できる．すなわち，ランダムオラクルモデルにおいて，楕円曲線上の List DH 仮定がなりたつならば，新仕様に記載された PSEC-KEM は IND-CCA2 である．このとき，

$$e' \geqq 1/\{2(1+2^{-128}\})\}\{e-(q_0+2q_D)2^{-8pLen}(1+2^{-128})-(q_0+q_D)2^{-8hLen}\}$$

$$t' \leqq t + (q_1 + q_D)T$$

がなりたつ。ただし，q_0，q_1 は *KDF* をランダムオラクルとみなして I2OSP(0,4)，I2OSP(1,4) で始まる入力に関する質問の回数，q_D を復号オラクルへの質問回数とする．T は楕円曲線上のスカラー倍に要する計算時間をあらわす．

4.5. まとめ

一部仕様変更により、証明可能安全性において証明の見直しが必要となるものの、ISO/IEC 18033-2:2006 の規格そのままではなく、楕円曲線上の群に限定して議論することで、従来と同様の安全性を示すことができる。現仕様と比べて、安全性評価結果の帰着効率が 2 倍程度低下するが、安全性への影響は小さいといえる。

よって、ISO/IEC 18033-2:2006 における PSEC-KEM については楕円曲線上の群に限定することで安全性上の問題はないと考えられる。

参考文献

[1] V. Shoup, A proposal for an ISO standard for public key encryption (version 2.1), Cryptology ePrint Archive: Report 2001/112, Dec. 20, 2001, http://eprint.iacr.org/2001/112

[2] 日本電信電話株式会社 情報流通プラットフォーム研究所, PSEC-KEM 仕様書, 2001 年 9 月 26 日

[3] NTT Information Sharing Platform Laboratories, NTT Corporation, PSEC-KEM Specification version 2.1, Jan. 18, 2008

5. KDFの安全性について

5.1. はじめに

本報告書は、KDFの調査を行い安全性について検討した結果について述べる。KDFは学術的に様々なものが提案されている状況にあり、また、実システムでの構成法も多様である。そのため本報告では以下のように簡略化して分類した。
・入力を攻撃者にとって未知の情報(random)と既知の情報(OtherInfo)に分け、具体的な安全性に影響が無ければ入力フォーマットについては言及しない。
・KDFを構成する要素技術で分類し、分類単位で安全性の検討を行う。

以上のような簡略化の結果、SP 800-56A、ANS X9.42、SEC 1 v1.0のKDFについては同じ構造に分類されるので、第2節ではKDFの構造と安全性評価の概要を示し、第3節でこれらを対象とした検討結果を述べた。第4節には構成技術の安全性に関する2008年2月の状況をまとめ、第5節でまとめを示した。

5.2. 安全性評価概要

5.2.1. KDF概要

KDFはDH等で共有した値を元に、より安全性を強化した値を出力する関数である。図1に概略構造を示す。

$$\boxed{\text{DH等}}\rightarrow \text{SKM}\rightarrow \boxed{\text{KDF}}\rightarrow \text{KM}$$

図1　KDF概略構造

SKMはDH等からの出力(random)と公開された情報(OtherInfo)から成るKDFへの入力である。

SKM=(random‖OtherInfo)

OtherInfoの内容、またrandomとOtherInfoのSKM内での構造は仕様ごとに多様である。
KMはKDFからの出力である。

KM=(K1‖K2‖K3‖…‖Kn)

KMから必要なビット数を切り出し、秘密鍵として利用する。KDFの仕様によっては秘密鍵の大きさとKi(i=1,...,n)の大きさが異なる場合がある(Kiの大きさが160ビットであるの

に対し、秘密鍵の大きさが 128 ビットである場合など)。本報告書では、秘密鍵の大きさを Ki の整数倍の大きさと仮定する。この仮定の下では、秘密鍵の大きさと Ki の大きさの不整合を攻撃者が解決するために余計に必要となるデータ量や計算量を考慮しない。そのため攻撃者は有利な立場と言え、KDF にとっては安全性を重視した検討となっている。

5.2.2. 想定した攻撃シナリオと安全性要件

攻撃者が得た情報の種類によって以下の攻撃が考えられる。

1)SKM の部分情報を攻撃者が得た場合
プロトコルの脆弱性を利用して、SKM の一部の情報を攻撃者が得たと仮定する。攻撃者の目的は入手した SKM の部分情報から KM を推定することである。よって KDF に求められる安全性は SKM の部分的情報から KM を推定することを困難にすることである。もし攻撃者が random 全体を得たならば KDF はその機能を果たさないので、その場合については検討しない。

2)KM 全体を攻撃者が得た場合
攻撃者が共有された秘密鍵の全体(KM)を得たと仮定する。攻撃者の目的は KM から SKM の部分情報を取得し、SKM 生成に関わる情報を取得することである。よって KM から SKM を逆算できないことが KDF に求められる。

3)KM の一部を攻撃者が得た場合
攻撃者が共有された秘密鍵の一部(Ki)を得たと仮定する。攻撃者の目的は、Ki から別の秘密鍵 Kj(j≠i)を求めることである。KDF に求められる安全性は Kj が Ki を元に推定されることを困難にすることである。または、攻撃者の目的が Ki から SKM の部分情報を取得する場合も考えられる。

5.3. NIST SP 800-56A、ANS X9.42、SECG SEC 1 の安全性

SP 800-56A、ANS X9.42、SEC 1 v1.0 で利用されている KDF の構造を図 2 に示す。OtherInfo に記述される内容及び入力フォーマットは仕様で異なる。

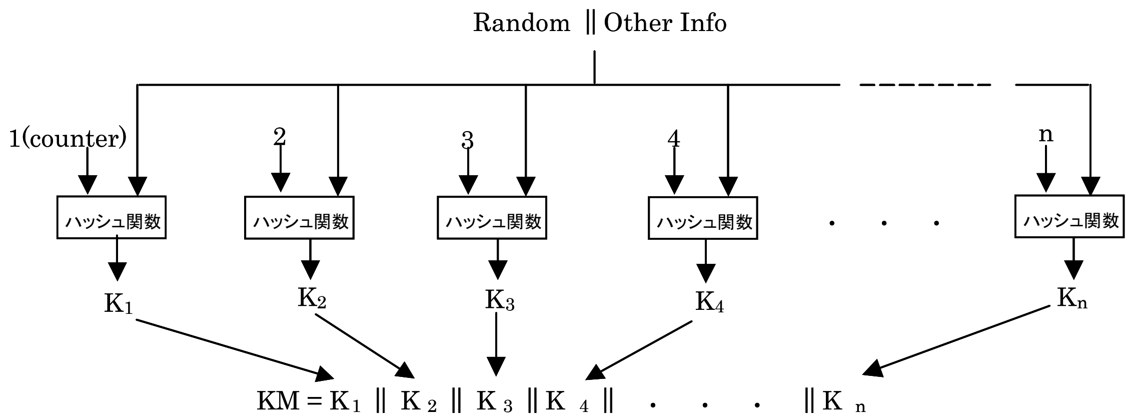


図 2 標準技術の KDF 構造

1)SKM の情報を攻撃者が得た場合の安全性

random 全体の大きさに対して攻撃者が得た random の部分情報の大きさで安全性が決定する。もし攻撃者が random 全体を得たならば KDF はその機能を果たさない。|random|=N、|Ki|=M、攻撃者が得た情報を n とすれば、未知の N-n ビットを推定しながら Ki を求める攻撃シナリオが考えられる。この場合は計算量が 2^{N-n} であり、計算機探索が実行可能である程度に小さいのであれば攻撃として成立する。ただし攻撃者が入手できると仮定するのに適当な n の大きさは random を共有するまでのプロトコルの安全性に依存し、KDF の安全性評価と異なるので割愛する。

2)KM 全体を攻撃者が得た場合の安全性

ここでの攻撃者の目的は SKM の部分情報を入手することである。SKM 生成に関する情報を入手することにより別の鍵交換における SKM を推定する、または既に行った鍵交換における SKM を推定するという攻撃シナリオが考えられる。

KM から random を逆算することはハッシュ関数の原像を求めることに等しい(図 2 参照)。random の大きさがハッシュ値よりも小さい場合は、全数探索によりその値を定めることができる。しかし、真の原像と第 2 原像を識別する必要が生じる。SP 800-56A、ANS X9.42、SEC 1 v1.0 ではハッシュ関数として SHA-1 もしくは SHA-1 を使った HMAC が採用されている。これらに対しては、

1. 全数探索より効果的な原像計算手法は発見されていない
2. 入力の一部が既知の場合でも効果的な原像計算に関する報告がない
3. 出力から入力の一部でも推定可能であるという解析手法が発見されていない
4. random の大きさは通常、DH の場合は 1024 ビット以上、ECDH の場合は 160 ビット以上が

選択されるため、全数探索による攻撃が実行不能である

という状況にある。一方で 1)の攻撃シナリオと組み合わせ、SKM の部分情報を攻撃者が得ていると仮定すれば、攻撃者既知の部分情報の大きさに応じて探索に必要な計算量を削減できる。

3)KM の一部を攻撃者が得た場合の安全性

複数の秘密鍵 Ki を攻撃者が入手し、これを利用して未知の秘密鍵 Kj を推定することが攻撃者の目的である。SP 800-56A、ANS X9.42、SEC 1 v1.0 は図 2 の構造を持つので、この場合は以下の攻撃手法が考えられる。

a.複数の Ki を用いて rondom を逆算し、それを用いて Kj を計算する

b.複数の Ki を用いて擬似衝突探索を利用して Kj を推定する

インデックス番号 i を攻撃者が未知の場合は、それを推定するための計算量が余計に必要になる。以下では既知であるという有利な条件を与えて検討する。また、a.の攻撃手法は前節の 2)の場合と同等であるので省略する。

b.の攻撃で用いる擬似衝突とはハッシュ関数の内部関数(途中段)における衝突である。このような途中段での衝突を利用して、NMAC や HMAC の秘密鍵を導出する攻撃手法がいくつか報告されている。これら攻撃手法を応用することにより、random を求めるのに必要な計算量を全数探索に比べて削減できる可能性がある。特に MD4 を使った HMAC 及び NMAC、または MD5 を使った NMAC については秘密鍵の導出結果が示されている。ただし擬似衝突を利用した攻撃は入力を自由に選べることが条件となっているため、入力フォーマットが決定されている KDF へ適用する場合は攻撃の必要条件を満たした入力が利用できない可能性もある。

SP 800-56A、ANS X9.42、SEC 1 v1.0 ではハッシュ関数として SHA-1 もしくは SHA-1 を使った HMAC が採用されている。SHA-1 については 80 段中 70 段での擬似衝突が発見されている。しかし擬似衝突を利用した SHA-1 を使った HMAC に対する効果的な攻撃手法はまだ報告されていない。

5.4. 構成技術の安全性

SP 800-56A、ANS X9.42、SEC 1 v1.0 ではハッシュ関数として SHA-1 もしくは SHA-1 を使った HMAC が採用されている。以下に SHA-1 及び SHA-1 を使った HMAC の安全性に関する現状をまとめた。

[SHA-1]

・2008 年 2 月現在では、衝突発見に必要な計算量は 2^{60} 程度と発表されている。グラーツ大

学ではグリッドコンピューティングによる SHA-1 の衝突発見プロジェクトが行われている。
・最長の擬似衝突は 80 段中 70 段である。
•原像計算または第 2 原像計算に関しては全数探索より効果的な手法が発見されていない。

[SHA-1 を使った HMAC(HMAC/SHA-1)]
・HMAC/SHA-1 に対するアルゴリズム攻撃の報告はない。
・34 段に減らした HMAC/SHA-1 について、HMAC の秘密鍵を復元する方法が報告されている。
・43 段に減らした HMAC/SHA-1 について、生成された値が HMAC/SHA-1 か乱数かを識別する識別攻撃が報告されている。ただし、識別攻撃による KDF の安全性への影響は無いと考えられる。

5.5. 安全性検討のまとめ

KDF への攻撃は、セッション鍵など秘密鍵を攻撃者が入手した後で行われる。SP 800-56A、ANS X9.42、SEC 1 v1.0 で使用される KDF の安全性は SHA-1 の原像計算困難性に帰着できる。2008 年現在では原像計算困難性については全数探索以外に有効な手段は発見されていない。また、SHA-1 を使った HMAC が利用されている場合は、SHA-1 の擬似衝突の発見が攻撃に繋がる可能性がある。80 段中 70 段の擬似衝突などが発見されているが、それらを利用した HMAC の攻撃への適用例は報告されておらず、SHA-1 を使った HMAC への攻撃も全数探索以外に有効な手段は発見されていない。

以上より、SP 800-56A、ANS X9.42、SEC 1 v1.0 については、使用している SHA-1 の危殆化及び移行計画などに注意が必要であるが、直ちに安全性が脅かされる状況ではないと考えられる。

参考文献

[1] X. Wang, Y. L. Yin, and H. Yu. Finding collisions in the full SHA-1. In CRYPTO2005, pages 17_36. International Association for Cryptologic Research (IACR), August 2005.
[2] X. Wang, A. C. Yao, and F. Yao. Cryptanalysis on SHA-1 hash function. In CRYPTOGRAPHIC HASH WORKSHOP. National Institute of Standards and Technology, November 2005.
[3] X. Wang. Cryptanalysis of hash functions and potential dangers. In Invited Talk at the Cryptographer's Track at RSA Conference 2006. RSA, February 2006.
[4] 内藤祐介, 太田和夫, 國廣昇. ハッシュ関数のコリジョン探索の改良 -新たな Advanced Message Modification の提案-. 暗号と情報セキュリティシンポジウム SCIS

2007, 1A1-1, 2007.
[5] Terutoshi Iwasak, Yusuke Naito, Jun Yajima, Yu Sasaki, Takeshi Shimoyama, Noboru Kunihiro, and Kazuo Ohta.Strategy for Selecting Disturbance Vector of SHA-1. 暗号と情報セキュリティシンポジウム SCIS 2007, 1A1-3, 2007.
[6] 佐々木悠, 内藤祐介, 矢嶋純, 岩崎輝星, 下山武司, 國廣昇, 太田和夫. SHA-1 差分パス構築アルゴリズム. 暗号と情報セキュリティシンポジウム SCIS 2007, 1A1-4, 2007.
[7] SHA-1 差分パス自動生成ツール. 矢嶋純, 佐々木悠, 岩崎輝星, 内藤祐介, 下山武司, 國廣昇, 太田和夫. 暗号と情報セキュリティシンポジウム SCIS 2007, 1A1-4, 2007.
[8] Sugita Makoto, Mitsuru Kawazoe, Kanta Matsuura and Hideki Imai. Grobner Based Cryptanalysis of SHA-1. 暗号と情報セキュリティシンポジウム SCIS 2007, 2A1-1, 2007.
[9] Sugita Makoto, Mitsuru Kawazoe and Hideki Imai. Grobner Based Boomerang Attack for SHA-1. 暗号と情報セキュリティシンポジウム SCIS 2008, 3A4-3, 2008.
[10] 矢嶋純 and 下山武司. SHA-1 のコリジョン探索におけるMessage Modification 適用可否判定法. 暗号と情報セキュリティシンポジウム SCIS 2008, 3A4-3, 2008.
[11] NIST. Secure hash standard. In Federal Information Processing Standard. National Institute of Standards and Technology, April 1995.
[12] M. Sugita, M. Kawazoe, and H. Imai. Gr ¨ obner basis based cryptanalysis of SHA-1. In Fast Software Encryption 2007. IACR, March 2007.
[13] F. Mendel, N. Pramstaller, C. Rechberger, and V. Rijmen. The impact of carries on the complexity of collision attacks on sha-1. In Fast Software Encryption 2006. International Association for Cryptologic Research (IACR), March 2006.
[14] E. Biham, R. Chen, A. Joux, P. Carribault, C. Lemuet, and W. Jalby. Collisions in SHA-0 and reduced SHA-1. In EUROCRYPT2005, pages 36_57. International Association for Cryptologic Research (IACR), May 2005.
[15] F. Chabaud and A. Joux. Di_erential collisions in SHA-0. In CRYPTO'98, pages 56_71. International Association for Cryptologic Research (IACR), August 1998.
[16] C. D. Cannière, F. Mendel, and C. Rechberger. On the full cost of collision search for SHA-1. In ECRYPT Hash Workshop. ECRYPT Network of Excellence in Cryptology, May 2007.
[17] C. D. Cannière and C. Rechberger. Finding SHA-1 characteristics: General results and applications. In ASIACRYPT2006. International Association for Cryptologic Research (IACR), December 2006.
[18] J. Yajima, Y. Sasaki, Y. Naito, T. Iwasaki, T. Shimoyama, N. Kunihiro, and K. Ohta. A new strategy for _nding a di_erential path of SHA-1. In ACISP2007, pages 45_58. International Association for Cryptologic Research (IACR), July 2007.
[19] Antoine Joux, Thomas Peyrin. Hash Functions and the (Amplified) Boomerang Attack.

In Alfred Menezes, editor, Advances in Cryptology - CRYPTO 2007, volume 4622 of Lecture Notes in Computer Science, pages 244-263. Springer-Verlag, 2007.
[20] SHA-1 Collision Search Graz. http://boinc.iaik.tugraz.at/sha1_coll_search/
[21] Scott Contini and Yiqun Lisa Yin. “Forgery and partial key-recovery attacks on HMAC and NMAC using hash collisions.” ASIACRYPT 2006, LNCS 4284, pp.37-53. Springer-Verlag, 2006.
[22] Pierre-Alain Fouque, Gaetan Leurent and Phong Nguyen, “Full Key-Recovery Attacks on HMAC/NMAC-MD4 and NMAC-MD5.” CRYPTO 2007, LNCS 4622, pp.15-30, Springer-Verlag, 2007.
[23] Christian Rechberger and Vincent Rijmen. “On Authentication with HMAC and Non-Random Properties.” Cryptology ePring Archive, Report 2006/290. http://eprint.iacr.org/2006/290.pdf.
[24] Katsuyuki Okeya. Side Channel Attacks Against HMACs Based on Block-Cipher Based Hash Functions. L. Batten and R. Safavi-Naini (Eds.): ACISP 2006, LNCS 4058, pp. 432-443, Springer-Verlag 2006.
[25] Donghoon Chang, Jaechul Sung, Seokhie Hong and Sangjin Lee, “Improved Cryptanalysis of APOP-MD4 and NMAC-MD4 using New Differential Paths.” Cryptology ePrint Archive, Report 2008/048, http://eprint.iacr.org/2008/048.pdf.
[26] Jongsung Kim, Alex Biryukov, Bart Preneel, and Seokhie Hong. On the Security of HMAC and NMAC Based on HAVAL, MD4, MD5, SHA-0 and SHA-1 (Extended Abstract). R. De Prisco and M. Yung (Eds.): SCN 2006, LNCS 4116, pp. 242-256, Springer-Verlag 2006.
[27] H. Krawczyk, M. Bellare, R. Canetti. “HMAC: Keyed-Hashing for Message Authentication.”
RFC 2104, Feburary 1997, http://www.ietf.org/rfc/rfc2104.txt.
[28] Mihir Bellare, Ran Canetti and Hugo Krawczyk, ″Keying Hash Functions for Message Authentication″, CRYPTO’96, pp1-15, 1996.
[29] Mihir Bellare, “New Proofs for NMAC and HMAC : Security Without Collision-Resistance.” C. Dwork (Ed.): CRYPTO 2006, LNCS 4117, pp. 602-619, 2006.

6. 楕円曲線ドメインパラメータの選択について

6.1. 概要

楕円曲線ドメインパラメータとは楕円曲線暗号システムを構成するのに必要なパラメータであり、

- 有限体F_qとその表現（基底の種類や既約な生成多項式）
- 楕円曲線E = (F_q, a, b)、
- E上の点のベースポイントG = (x_G, y_G)とその位数n = o(G)、
- その他、オプションとして、コファクターh = #E(F_q)/n や種 SEED等

からなる。これらは楕円曲線上の離散対数問題（ECDLP）に関する攻撃方法を適用できないように選択される必要がある。

現時点においてECDLPに対する既存の攻撃方法を適用できないようにするには、

(a)　位数#E(GF(q))が大きな素数n(> 2^{160})により割り切れること、

(b)　MOV条件を満たすこと、

(c)　アノマラス条件を満たすこと、

(d)　$q=2^m$の場合、mが素数であること。

の4つが成り立つことが必要である。選択方法は大別すると、

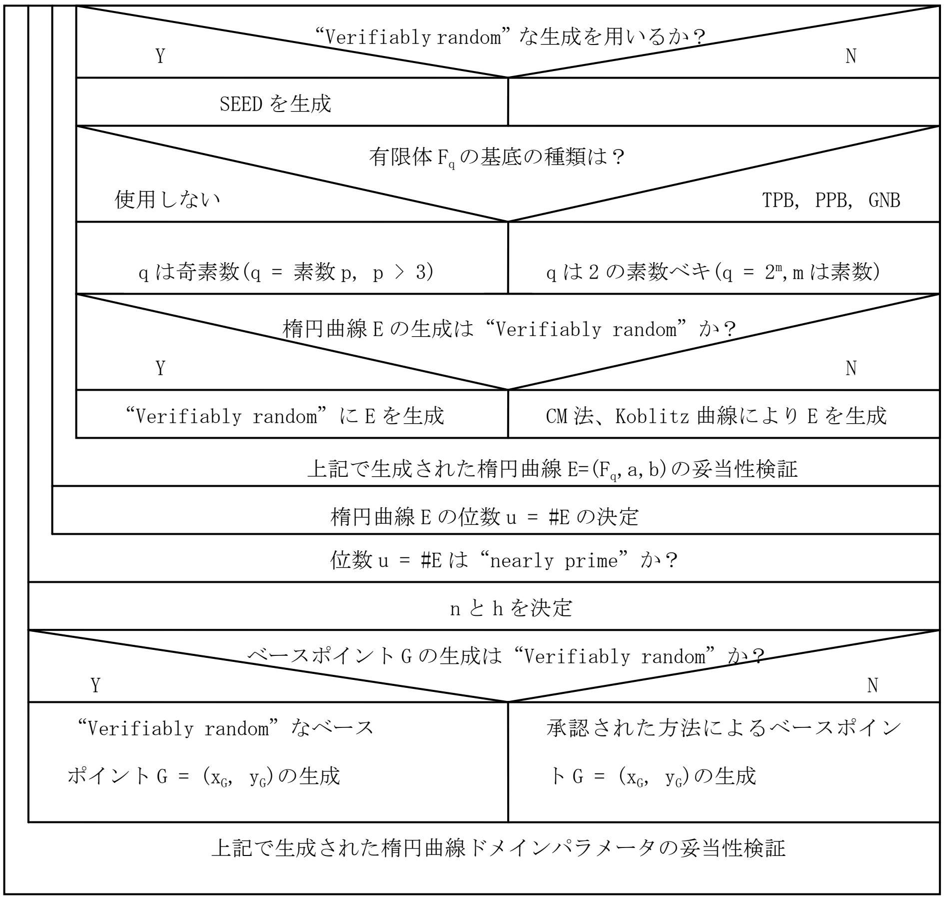
- ランダムに選択する方法、
- 特殊なクラスの楕円曲線を使用する方法（Complex Multiplication法やKoblitz曲線）

の2種類がある。ANS X9.62-2005における楕円曲線ドメインパラメータの生成のアルゴリズムを図で表すと以下の表1のようになる。

また、ANS X9.62-2005 における楕円曲線ドメインパラメータの妥当性検証の条件は以下のようになっている。

- n >= max (2^{2s-1}, 2^{160}) (s はセキュリティパラメータ)かつ、n は素数であること
- 付随した有限体表現を有する楕円曲線 E = (F_q, a, b)（及び、種 SEED が与えられている場合にはそれを含めて）が妥当性を有すること
- h’ = $\left\lfloor \left(\sqrt{q}+1\right)^2 / n \right\rfloor$ <= $2^{s/8}$ かつ、コファクターh が与えられている場合は、h = h’）
- MOV 条件を満たすこと
- Anomalous 条件を満たすこと
- ベースポイント G = (x_G, y_G)（種 SEED が与えられているときはそれを含めて）が妥当性を有すること

表１　ANS X9.62-2005における楕円曲線ドメインパラメータの生成の概要



6.2. MOV(Menezes-Okamoto-Vanstone)閾値B

MOV攻撃とは、GF(q)上の楕円曲線における離散対数問題を有限体GF(q^B)における離散対数問題へ帰着することに基づくものである。閾値Bは、有限体GF(q^B)における離散対数問題の困難さがGF(q)上の楕円曲線における離散対数問題の困難さに比べ、少なくとも同等であるように決められる。

ANS X9.62-1998[1]やSEC 1 v1.0[11]の策定時においては、B = 20と規定されていたが、ANS X9.62-2005やSEC 1 v1.7(Draft)[13]では、B = 100と変更されている。

6.3. 楕円曲線の選択

ANS X9.62-1998では、“verifiably random”な方法で曲線を生成する方法が規定されていたが、ハッシュ関数SHA-1のハッシュ値サイズ160（ビット）が（暗黙のうちに）固定的に使われている場合が見受けられた。ANS X9.62-2005では、使用が推奨されるハッシュ関

数が複数あるため、それに見合うように記述が若干変更されている。

6.4. G （Base point）の選択

ANS X9.62-2005 では“verifiably random”な方法で生成点（Base point）を生成（と検証）する方法が新たに規定され、追加された。G の選択において、G の位数 n(>160)が大きな素数である限りセキュリティ上問題になることは知られていない。しかしながら、将来起こりうるかも知れない攻撃や実装上のエラーから生じる脆弱性を避ける意味で、“verifiably random”な方法による G の選択方法を用いることが考慮されている。なお、SEC 1 v1.7(Draft)においても、この方法は ANS X9.62-2005 と整合性があると記載されている。

6.5. h （cofactor)に関する制限

コファクターh （=#E(GF(q))/n）については、ANS X9.62-1998 では大きさに関して特に制限はなく（楕円曲線ドメインパラメータ生成上における smooth さに関するガイドラインはあった)、SEC 1 v1.0 では 4 以下と規定されていた。ANS X9.62-2005 及び SEC 1 v1.7(Draft)ではどちらも、h はセキュリティレベルを s としたとき、$2^{s/8}$ 以下と規定されている。

6.6. $q=2^m$ の場合の次数 m に関する条件

ANS X9.62-1998では規格上は、$q=2^m$ のとき、mが合成数であることを排除していなかった。CRYPTREC Report 2002[3]においても記載があった通り、mが合成数の場合、Weil descent 攻撃が効率的に適用できる可能性があるため、この場合を排除してする必要がある。ANS X9.62-2005では、mを素数とすることになったので、この点は修正された。

6.7. 鍵長

ANS X9.62-2005 における変化としては、セキュリティレベルを定めるパラメータ s は、80,112,128,192,256 から選択して実装することになった([2]の補遺 A.3.1.4)。また、SEC 1 における変化としては、セキュリティレベルを定めるパラメータ s の集合が、SEC 1 v1.0 では、{56,64,80,96,112,128,192,256} であったのに対して、SEC 1 v1.7(Draft)では{80,112,128,192,256}になったことが挙げられる[4]。

CRYPTREC Report 2006 でも掲載したように、NIST は SP 800-57[9]の 66 ページの Table 4 において、表 2 に示されるような推奨値を与えている。また、ECRYPT では、年次報告書[4]

---

[4] SECG SEC 1 ではセキュリティパラメータは文字 t が使用されている。

を公表しており、Chapter 7、Table 7.2 において、表 3 に示されるような各種暗号技術におけるパラメータサイズの比較が示されている。

表 2　Table 4: Recommended algorithms and minimum key sizes

Algorithm security lifetimes	Symmetric key algorithms (Encryption & MAC)	FFC (e.g., DSA, D-H)	IFC (e.g., RSA)	ECC (e.g., ECDSA)
Through 2010 (min. of 80 bits strength)	2TDEA 3TDEA AES-128 AES-192 AES-256	Min.: L=1024; N=160	Min.: L=1024	Min.: f=160
Through 2030 (min. of 112 bits strength)	3TDEA AES-128 AES-192 AES-256	Min.: L=2048; N=224	Min.: L=2048	Min.: f=224
Beyond 2030 (min. of 128 bits strength)	AES-128 AES-192 AES-256	Min.: L=3072; N=256	Min.: L=3072	Min.: f=256

表3　Table 7.2: Key-size Equivalence

Security(bits)	RSA	DLOG		EC
		Field size	Subfield	
48	480	480	96	96
56	640	640	112	112
64	816	816	128	128
80	1248	1248	160	160
112	2432	2432	224	224
128	3248	3248	256	256
160	5312	5312	320	320
192	7936	7936	384	384
256	15424	15424	512	512

なお、ANS X9.62-2005 では[2]の補遺 K 2.4、SEC 1 v1.7(Draft)では[13]の補遺 B 2.1 に

において、NIST と同様な推奨値が与えられている。

ところで、NIST では、FIPS PUB 201[8]において米国の連邦政府施設へのアクセスを行う職員及び請負業者の向けの個人識別情報の検証（Personal Identity Verification）に関する標準を定めている。FIPS PUB 201 を実装するシステムの相互運用性を実現するためのガイドラインとして SP 800 シリーズの文書を多数発行しており、その中の一つ、SP 800-78[10]において PIV 用の暗号アルゴリズムと鍵長を規定している。SP 800-78 のその中において、以下の表 4 のように楕円曲線の推奨値を与えている例がある。

表 4　Table 3-6. ECC Parameter Object Identifiers for Approved Curves

Asymmetric Algorithm	Object Identifier
Curve P-256	antix9p256r1 ::= {iso(1) member-body(2) us(840) ansi-X9-62(10045) curves(3) prime(1) 7}
Curve P-384	antix9p384r1 ::= {iso(1) identified-organization(3) certicom(132) curves(0) prime(1) 34}

また、国際的なクレジットカード・ブランド企業が策定した、金融分野における IC カードと端末に関する仕様を定めた国際的なデファクト標準である EMV 仕様というものがある。現行の仕様 EMV 4.1 では RSA の鍵長に上限（1984 ビット）が設定されているため、RSA の鍵長が今後、より長くなることを想定して、上限を大きくしたケースや楕円曲線暗号を採用したケース等、いくつかの次期仕様を検討し始めている[5]。そこでは現在のところ、楕円曲線として NIST が推奨する楕円曲線 Curve P-256 と Curve P-521（ansix9p521r1）が挙げられている。

6.8. 保証(assurance)要件

楕円曲線暗号に限らず、公開鍵やドメインパラメータ等は必ずしも保護されていない環境下において保管されたり送受信されたりするので、それらを利用する暗号アルゴリズムの実行の前には、数学的に正当な情報であるかどうかの保証が得ることが必要である。

保証の考え方を政府レベルで正式に文書化している例は米国 NIST（以下、NIST）において見られる。鍵管理に関する推奨方法を定めた文書 NIST SP 800-57 の 5.4 節では、

（１）　完全性(Integrity)の保証
（２）　ドメインパラメータの妥当性の保証
（３）　公開鍵の妥当性の保証
（４）　（署名者による）秘密鍵の所有の保証

の 4 つが挙げられている。さらに、電子署名の仕様を定めた文書 NIST Draft FIPS 186-3[7]

では現行の NIST FIPS PUB 186-2[6]と比べて、署名検証及び署名の有効性を検証する方法として新規に保証の要件が加えられてきている。それらに関するガイドラインは NIST SP 800-89 において記述されている。

ANS X9.62-2005 には、上述の（２）～（４）の必要性が述べられているものの、詳細な手続きの規定は現時点ではまだない。なお、SECG の仕様書 SEC 1 には上述の（２）と（３）についての記述はある。

6.9. ハッシュ関数のオブジェクト ID

2000 年頃までの仕様と比べて、明示的に SHA-1 以外のハッシュ関数を利用した ASN.1 の Object Identifier（オブジェクト識別子）も正式に付与されてきている。

ANS X9.62-2005 及び SEC 1 v1.7(Draft)では、

```
===
ansi-X9-62 OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) 10045}
id-ecSigType OBJECT IDENTIFIER ::= {ansi-X9-62 signatures(4)}
ecdsa-with-Sha1 ::= {id-ecSigType sha1(1)}
ecdsa-with-Specified ::= {id-ecSigType specified(3)}
ecdsa-with-Sha224 ::= {ecdsa-with-Specified 1}
ecdsa-with-Sha256 ::= {ecdsa-with-Specified 2}
ecdsa-with-Sha384 ::= {ecdsa-with-Specified 3}
ecdsa-with-Sha224 ::= {ecdsa-with-Specified 4}
===
```

のように規定された。また、IETF でも、上述のアルゴリズムを指定可能なようにプロトコル等の規定が更新されてきている例がある。なお、IETF の PKIX においては現時点ではまだ RFC 化は未定のようである。

6.10.　擬似乱数生成器（DRBG）

ANS X9.62-2005では、鍵対を生成する際に、HMACを使った擬似乱数生成器（HMAC_DRBG）が推奨アルゴリズムの一つとして記載されている。

6.11.　まとめ

CRYPTREC Report 2002における内容と今回の報告をまとめたものが、表5である。SEC 1 のVer.1.0及びVer.1.7(Draft)においても、ANS X9.62-2005においても、1.の条件(a)～(d)を満たすように構成されている。

従って、どの仕様に基づいて楕円曲線ドメインパラメータを生成しても現時点では安全であると考えられる。なお、SEC 1とANS X9.62の仕様における楕円曲線ドメインパラメータの生成・検証のアルゴリズムについては異なる部分があるので、互換性に注意が必要である。

表5　仕様間の主な条件に関する比較

<table>
<tr><td>CRYPTREC Report 2002における項目</td><td>SECG SEC 1 Ver.1.0</td><td>SECG SEC 1 Ver.1.7(Draft)</td><td>ANS X9.62-2005</td></tr>
<tr><td>鍵長の確認</td><td>セキュリティパラメータtの範囲:
{56,64,80,96,112,128,192,256}.
・標数が素数：
奇素数pのサイズは、t<256ならば2t、t=256ならば521.
・標数が2：
t’は{64,80,96,112,128,192,256,512}の中でtより大きな最小の数. その時、mは2t<m<2t’を満たすような{113,131,163,193,233,239,283,409,571}の中の整数である.</td><td>セキュリティパラメータtの範囲: {80,112,128,192,256}.
・標数が素数：
奇素数pのサイズは、t=80ならば192、80<t<256ならば2t、t=256ならば521.
・標数が2：
t’は{112,128,192,256,512}の中でtより大きな最小の数. その時、mは2t<m<2t’を満たすような{163,233,239,283,409,571}の中の整数である.</td><td>セキュリティパラメータｓの範囲:
{80,112,128,192,256}

n >= $\max(2^{2s-1}, 2^{160})$.</td></tr>
<tr><td>位数nが素数であることの確認</td><td colspan="3">あり.</td></tr>
<tr><td>（標数が2の場合）既約多項式の確認</td><td colspan="2">f(x)が仕様書であらかじめ与えられているGF(2)[x]におけるm次の既約多項式であること.
(m=239の場合は、
$f(x)=x^{239}+x^{36}+1$ と $x^{239}+x^{158}+1$
の2通りある. それ以外は1通り.)</td><td>基底はTPB,PPB,GNBのいずれかとする.PBの場合、TPBを優先し、存在しない場合はPPBとする.PBの場合、最高次以外の単項式の次数をできるだけ小さく取る.[5]</td></tr>
<tr><td rowspan="2">係数の関係の確認</td><td colspan="2">・標数が素数：　$4a^3 + 27b^2 \neq 0 \pmod{p}$</td><td>・標数が素数：　$4a^3 + 27b^2 \neq 0 \pmod{q}$</td></tr>
<tr><td colspan="3">・標数が2：　$b\neq 0$ in $GF(2^m)$</td></tr>
<tr><td rowspan="2">曲線係数及びベースポイントGの座標の範囲確認</td><td colspan="2">・標数が素数：　$0 \le a, b, x_G, y_G \le p-1$</td><td rowspan="2">・標数が素数q:
$0 \le a, b, x_G, y_G \le q-1$
・標数が2:
a, b, x_G, y_G は長さmのビット列である（有限体をmビット表現している）.</td></tr>
<tr><td colspan="2">・標数が2：　a, b, x_G, y_G がGF(2)[x]におけるm-1次以下の多項式である（有限体を多項式表現している）.</td></tr>
<tr><td>ベースポイントGの座標の確認</td><td colspan="3">G≠OはE上の点である.</td></tr>
<tr><td>Gの位数の確認</td><td colspan="3">nG = O.</td></tr>
<tr><td>コファクターhの確認</td><td>$h \le 4$, $h = \left\lfloor \left(\sqrt{q}+1\right)^2 / n \right\rfloor$</td><td colspan="2">$h \le 2^{s/8}$, $h = \left\lfloor \left(\sqrt{q}+1\right)^2 / n \right\rfloor$</td></tr>
<tr><td>各種攻撃対策の確認</td><td>MOV条件(B >= 20) と Anomalous条件</td><td colspan="2">MOV条件(B >= 100) と Anomalous条件</td></tr>
<tr><td>その他</td><td>・推奨曲線として、SEC 2[12]がある.</td><td>・n-1は大きな素数を因数としてもつこと（生成の際）.
・擬似乱数生成器は、ANS X9.82またはNIST SP 800-90に従うこと.
・推奨曲線として、SEC 2[12]がある.</td><td>・HMACベースのDRBGが承認されたRBGとして規定された.
・推奨曲線として、セキュリティパラメータごとに3つずつ、合計15個挙げられている.</td></tr>
</table>

[5] ANS X9.62-1998及びANS X9.62-2005では、このような生成多項式を一意的に決定するルールがある。ANS X9.62-1998やSEC 1では、楕円曲線ドメインパラメータの検証の際、生成多項式の既約性を確認することが明示されているが、ANS X9.62-2005では同様の記述はない。

参考文献

[1] ANS X9.62-1998, Public Key Cryptography for the Financial Services Industry: the Elliptic Curve Digital Signature Algorithm(ECDSA), American Bankers Association, 1999.

[2] ANS X9.62-2005, Public Key Cryptography for the Financial Services Industry: the Elliptic Curve Digital Signature Algorithm(ECDSA), Accredited Standards Committee X9, Inc., 2005.

[3] CRYPTREC Report 2002, 暗号技術報告書(2002年度版), 情報処理振興事業協会, 通信・放送機構, 平成15年3月. Available at http://www2.nict.go.jp/y/y213/cryptrec_publicity/c02_report.pdf

[4] ECRYPT - European Network of Excellence for Cryptology, D.SPA.21, ECRYPT Yearly Report on Algorithms and Key Lengths (2006), Revision 1.1, January 2007. Available at http://www.ecrypt.eu.org/documents/D.SPA.21-1.1.pdf

[5] EMV Integrated Circuit Card Specifications for Payment Systems v4.1z ECC Book 2, Available at http://www.emvco.com/specifications.asp?show=94

[6] National Institute of Standards and Technology (NIST), Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-2(+ Change Notice 1), January 2000. Available at http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf

[7] National Institute of Standards and Technology (NIST), Draft Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-3, March 2006. Available at http://csrc.nist.gov/publications/drafts/fips_186-3/Draft-FIPS-186-3%20_March2006.pdf

[8] National Institute of Standards and Technology (NIST), Personal Identity Verification (PIV) of Federal Employees and Contractors, Federal Information Processing Standards Publication 201-1(+ Change Notice 1), March 2006. Available at http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf

[9] National Institute of Standards and Technology (NIST), Recommandation for Key Management - Part 1: General (Revised), Special Publication 800-57, March 2007. Available at http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf

[10] National Institute of Standards and Technology (NIST), Cryptographic Algorithms and Key Sizes for Personal Identity Verification, Special Publication 800-78-1, August 2007. Available at

http://csrc.nist.gov/publications/nistpubs/800-78-1/SP-800-78-1_final2.pdf
[11] Standards for Efficient Cryptography, SEC 1:Elliptic Curve Cryptography, Certicom Research, Ver.1.0, September 2000. Available at http://www.secg.org/download/aid-385/sec1_final.pdf
[12] Standards for Efficient Cryptography, SEC 2:Recommended Elliptic Curve Domain Parameters, Certicom Research, Ver.1.0, September 2000. Available at http://www.secg.org/download/aid-386/sec2_final.pdf
[13] Standards for Efficient Cryptography, SEC 1:Elliptic Curve Cryptography, Certicom Research, Working Draft Ver.1.7, November 2006. Available at http://www.secg.org/download/aid-631/sec1_1point7.pdf

以上

付録 5

要　　望　　書

2007 年 6 月 16 日

CRYPTREC
暗号技術検討会事務局
暗号技術監視委員会事務局　御中

暗号モジュール試験及び認証制度における
技術審議委員会　委員長　松本　勉

拝啓、時下益々ご清祥のこととお喜び申し上げます。
平素は、当制度の運営にご支援、ご協力を賜り厚く御礼申し上げます。

さて、CRYPTREC における安全性評価を経て電子政府推奨暗号リストに掲載されている暗号は、当制度(JCMVP)におきまして、セキュリティ機能として承認しております。ところが、制度運用に際し、幾つかの問題点が指摘されておりますので、以下にその背景、問題点、及び JCMVP 技術審議委員会として CRYPTREC へのお願い事項を示します。
ご多用中誠に恐縮ですが、2007 年 9 月 3 日(月)までにご回答を頂きたく存じます。
ご検討の程、宜しくお願いします。

敬具

記

１．暗号強度の経年劣化に伴う移行計画について

＜背景＞

米国 NIST が NIST Special Publication 800-57 Recommendation for Key Management を発表し、暗号強度の経年劣化に伴う移行計画を発表しています。これに伴い、2007 年 5 月 19 日をもって、80bit 未満のセキュリティ強度である DES のみを搭載した暗号モジュールに関する認証が取消されました。

また、2010 年 12 月 31 日をもって、80bit 以上 112bit 未満のセキュリティ強度の暗号アルゴリズムのみを搭載した暗号モジュールに関する認証が取消される予定です。

CRYPTREC REPORT 2006 において、RSA 1024bit についての危殆化の予測が詳細に求められていますが、その結果によって、上記の NIST の方針は誤っていないことが裏付けられたと考えらえます。

NIST が提示している移行計画の表を提示します。

Table 4: Recommended algorithms and minimum key sizes				
Algorithm security lifetimes	**Symmetric key Algorithms (Encryption & MAC)**	**FFC (e.g., DSA, D-H)**	**IFC (e.g., RSA)**	**ECC (e.g., ECDSA)**
Through 2010 (min. of 80 bits of strength)	2TDEA[21] 3TDEA AES-128 AES-192 AES-256	Min.: L = 1024; N =160	Min.: k=1024	Min.: f=160
Through 2030 (min. of 112 bits of strength)	3TDEA AES-128 AES-192 AES-256	Min.: L = 2048 N = 224	Min.: k=2048	Min.: f=224
Beyond 2030 (min. of 128 bits of strength)	AES-128 AES-192 AES-256	Min.: L = 3072 N = 256	Min.: k=3072	Min.: f=256

電子政府推奨暗号リストに記載されているもので、80bit 以上 112bit 未満のセキュリティ強度のものは、次の暗号アルゴリズムです。

- DSA (モジュラスとなる素数が 1024 ビット)
- Diffie-Hellman (DH) (モジュラスとなる素数が 1024 ビット以上 2048 ビット未満)
- RSA (モジュラスとなる合成数が 1024 ビット以上 2048 ビット未満)
  (RSASSA-PKCS1-v1_5、RSASSA-PSS、RSA-OAEP 及び RSAES-PKCS1-v1_5)
- ECDSA (楕円曲線の定義体及び位数が 160 ビット以上 224 ビット未満)
- ECDH (楕円曲線の定義体及び位数が 160 ビット以上 224 ビット未満)
- SHA-1

＜問題点＞

3 年後に 2010 年を迎えますが、現在、暗号アルゴリズムを実装している製品が、2010 年まで継続して使用される可能性は高く、ベンダに対して適切なアナウンスを緊急に行う必要があります。

＜お願い＞

当制度でも、北米の制度を倣い、2010 年の移行については実施するという方針で問題が無いか、ご検討いただきご回答下さい。

２．DSA の仕様の参照先の変更について

＜背景＞

電子政府推奨暗号リストが制定された時点では、DSA に関して、ANSI X9.30 と FIPS PUB 186-2 が全く同じでした。電子署名法の指針において、オブジェクト ID を指定することが求められ、当時 FIPS PUB 186-2 には、オブジェクト ID が掲載されていなかったことからオブジェクト ID がある ANSI X9.30 が採用されたため、ANSI X9.30 は電子政府推奨暗号リストにおける DSA の仕様の参照先にもなっています。

＜問題点＞

DSA を実装しようとして、ANSI X9.30 に従った場合、ANSI X9.30 Annex B(Normative)に記載されている擬似乱数生成器を使用しなければなりません。しかしながら、FIPS PUB 186-2 with Change Notice 1 に記載されている通り、この擬似乱数生成器に対して、攻撃方法が発見されています。

＜お願い＞

JCMVP が試験･認証の対象とする DSA の仕様の参照先として､ANSI X9.30 ではない、FIPS PUB 186-2 with Change Notice 1 として良いかご回答下さい。

併せて、電子政府推奨暗号リストの DSA の仕様の参照先の変更についてもご検討下さい。

３．DH 及び ECDH の仕様の参照先の変更について

＜背景＞

DH 及び ECDH に関して CRYPTREC で電子政府推奨暗号リスト案作成に向けて検討した当時は、Primitives と呼ばれるコアの部分の安全性評価が行われ、その際 DH に関しては ANSI X9.42、ECDH に関しては SEC 1 を仕様の参照先としていました。

＜問題点＞

CRYPTREC で検討した当時は、実際には鍵導出関数 KDF の詳細までを含めて技術的な検討をしておらず、仕様を指定した段階で自動的に KDF を含めた形になってしまっております。暗号アルゴリズム試験を行う場合は､KDF を含めて既知解テストを実施します。

このとき、SP800-56A を仕様の参照先とし北米 CMVP で認証された機器と、ANSI X9.42 及び SEC 1 を仕様の参照先とし日本 JCMVP で認証された機器との間で､鍵確立が出来ないという問題が発生します。

JCMVP 技術審議委員会の暗号アルゴリズム試験要件検討 WG からは、SP800-56A と ANSI X9.42 及び SEC1 の規格の違いが KDF だとすると、仕様を変更することに何ら問題は無いという答申を得ています。

＜お願い＞

JCMVP が試験･認証の対象とする DH 及び ECDH の仕様の参照先として､ANSI X9.42 及び SEC 1 を廃止し、SP800-56A として良いかご回答下さい。

併せて、電子政府推奨暗号リストの DH 及び ECDH の仕様の参照先の変更についてもご検討下さい。

以上

（案）

平成２０年×月×日

暗号モジュール試験及び認証制度における
技術審議委員会　委員長　松本　勉　殿

暗号技術検討会　　　座長　　今井　秀樹
暗号技術監視委員会　委員長　今井　秀樹

要望書に対する回答

拝復　時下ますますご繁栄のこととお慶び申し上げます。
日頃より格別のご支援を賜り心より御礼申し上げます。

さて、貴委員会から平成１９年６月１６日付けで、暗号技術検討会事務局及び暗号技術監視委員会事務局宛に頂戴いたしました「要望書」につきまして、暗号技術監視委員会として検討をしてまいりましたので、下記のとおりご回答申し上げます。

なお、「要望書」では、電子政府推奨暗号リストに記載されております暗号技術に関する、

１．暗号強度の経年劣化に伴う移行計画について
２．ＤＳＡの仕様の参照先の変更について
３．ＤＨ及びＥＣＤＨの仕様の参照先の変更について

の３点について問題点等のご指摘がありましたが、上記に関連する

１．ＥＣＤＳＡの仕様の参照先の変更について
２．ＰＳＥＣ－ＫＥＭの仕様の変更について

の２点についても、電子政府推奨暗号リストに記載されております暗号技術に関する仕様書の参照先の変更を伴いますので、併せてご報告申し上げます。

今後とも一層のご指導、ご支援を賜りますようお願い申しあげます。

敬具

記

１.暗号強度の経年劣化に伴う移行計画について

国内の政府機関の情報システムにおける暗号アルゴリズムの移行計画に関しては、平成１９年９月から内閣官房情報セキュリティセンター（ＮＩＳＣ）を中心に検討が開始され、先日の平成２０年×月×日[注]に、「政府機関の情報システムにおいて使用されてい

[注] 意見の募集については平成 20 年 2 月 4 日、結果の決定については平成 20 年 4 月 22 日。

る暗号アルゴリズムＳＨＡ－１及びＲＳＡ１０２４に係る移行指針」（案）に関する意見の募集[1]（の結果[2]）として、取りまとめられたところです。

この検討の中で、特に問題となるところは、公開鍵暗号基盤（ＰＫＩ）の移行計画であると考えております。公開鍵暗号基盤に関しては、商業登記、公的個人認証等で、多くの電子証明書が発行されていますが、この多くの有効期限が５～１０年と設定されています。そのため、認証書の更新が本格化する２０１５年を目途にアルゴリズムの移行を完了させる必要があると考えています。

しかし、ＰＫＩの移行に当たっては、単に暗号アルゴリズムの移行だけでなく、種々の課題が派生すると考えております。例えば、発行済みの認証書の有効期限が切れる前に電子証明書を発行する為のコスト負担などの運用上の問題や新旧両方の認証書の並行運用問題等の技術的課題など、ＰＫＩの移行に伴う未解決の問題が存在しています。

さらに、今後３年以内に、これら問題が解決できたとしても、現実に稼動しているシステムに対して、差分やパッチを適用する手順の確認、システム稼動上の影響の確認作業を実施する必要があります。つまり、十分な試験期間をおく必要があります。また、移行順序にも考慮する必要があります。

このため、暗号アルゴリズムの移行計画を明示することは重要なことと認識しており、そのためにも、今後とも、ＮＩＳＣ、総務省や経済産業省と連携をとって検討を進めていきますので、ＣＲＹＰＴＲＥＣ活動についてご理解とご協力のほど何卒宜しくお願いいたします。

２．ＤＳＡの仕様の参照先の変更について

ANS X9.30:1-1997 と NIST FIPS PUB 186-2 の仕様は基本的に同じでしたが、NIST FIPS PUB 186-2 の Change Notice 1 では、鍵サイズ（1024 ビット未満は仕様外）と擬似乱数生成器に対して仕様変更がありました。鍵サイズについては、従来から 1024 ビット以上を推奨していますし、擬似乱数生成系の問題点（DSA に関する Bleichenbacher の指摘[3]）については、電子政府推奨暗号リストにおける例示において、指摘されていた問題点を有する擬似乱数生成器は除外することで、既に対応済みです[4]。

このような理由から、NIST FIPS PUB 186-2 (+ Change Notice 1)の DSA については、安全性に問題はないと考えられます。また、擬似乱数生成系についても、既に例示から 5 年も経過しており、従来の参照先の削除についても問題がないと考えられます。

---

[1] http://www.nisc.go.jp/active/general/niscrypt.html

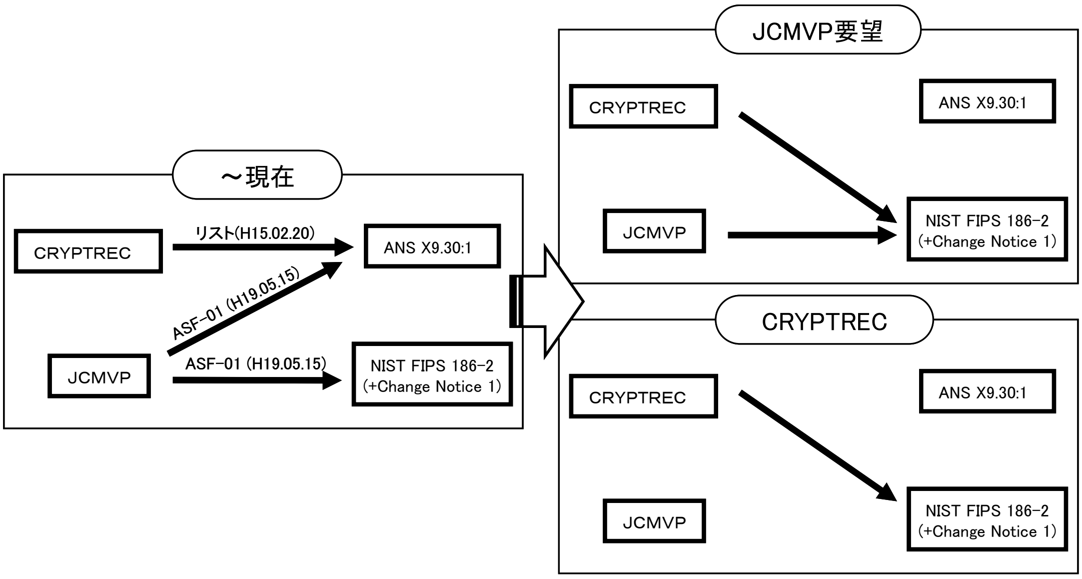
[2] http://www.nisc.go.jp/active/general/res_niscrypt.html

[3] r を160 ビットの乱数、q を160 ビットの素数としたときに, r mod q の分布が偏ることを利用したもの。

[4] CRYPTREC Report 2002 第５章 擬似乱数生成系の評価, http://www2.nict.go.jp/y/y213/cryptrec_publicity/c02_report.pdf

したがって、仕様書の参照先を変更する場合には、NIST FIPS PUB 186-2 (+ Change Notice 1)のみとするのが妥当であると判断いたしました（図１を参照のこと)。なお、この結果は、今後発表されます CRYPTREC Report 2007 や CRYPTREC の Web サイト上でも公表される予定です。

図１



３．ＤＨ及びＥＣＤＨの仕様の参照先の変更について

３．１．ＤＨの仕様の参照先の変更について

現在の電子政府推奨暗号リストにおける DH の仕様参照先は ANS X9.42-2001 です。ANS X9.42 と NIST SP800-56A の間に存在する技術仕様上の主な差異は、

（１） 有限体ドメインパラメータについては、ANS X9.42 のものは、SP800-56A に適合しない場合があるが、NIST SP800-56A のものは ANS X9.42 に適合する。

（２） KDF 関数について差異が存在する。どちらもハッシュ関数を使用する KDF 関数としては同じタイプに属するので、安全なハッシュ関数を使用すれば、安全性上問題はない。

（３） その他、DH のスキームの種類、公開鍵の検証、鍵配送手法、鍵確立プロセスについて、SP800-56A の方がより強い制限を課している。

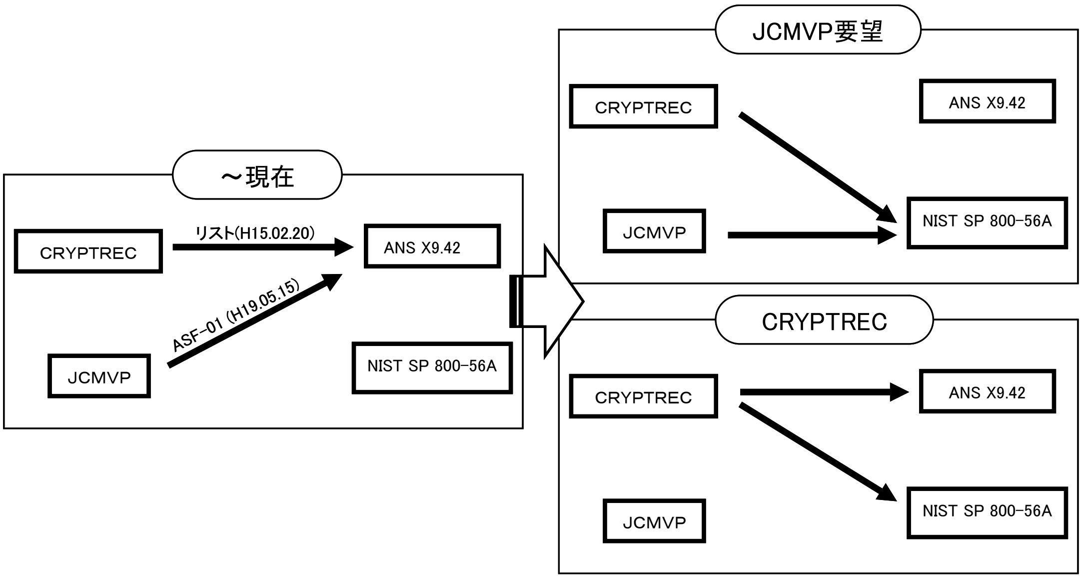
となっています。

このような理由から、NIST SP800-56A の DH については安全性に問題はないと考えられます。

したがって、仕様の参照先を変更する場合には、KDF 関数の仕様に関する差異による

相互接続性を考慮すれば、仕様の参照先としては、ANS X9.42[5]を残し、NIST SP 800-56Aを追加することが妥当であると判断いたしました（図２を参照のこと）。なお、この結果は、今後発表されますCRYPTREC Report 2007やCRYPTRECのWebサイト上でも公表される予定です。

図２



３．２．ＥＣＤＨの仕様の参照先の変更について

現在の電子政府推奨暗号リストにおけるECDHの仕様参照先はSECG SEC 1 Ver.1.0です。SECG SEC 1 Ver.1.0とNIST SP800-56Aの間に存在する技術仕様上の主な差異は、

（１） 楕円曲線ドメインパラメータについて差異が存在する[6]。安全性上の問題点はないものの、相互接続性に支障をきたす可能性がある。
（２） KDF関数について差異が存在する。どちらもハッシュ関数を使用するKDF関数としては同じタイプに属するので、安全なハッシュ関数を使用すれば、安全性上問題はない。
（３） security level、擬似乱数生成器、standardなプリミティブの使用、について、NIST SP800-56Aの方がより強い制限を課している。

また、NIST SP800-56Aではkeyを次のようにstatic keyとephemeral keyとに区別している：

[5] ANSI X9.42-2003という改訂版が発行されており、スキーム自体には変更はないものの、素数生成に関連する補助関数の記述に微修正があるため、参照先としては、ANSI X9.42-2003に変更すべきである。
[6] 第４節「ＥＣＤＳＡの仕様の参照先の変更について」も参照のこと。

(a)　ephemeral key：トランザクション毎に変えること(を通常とする)key
(b)　static key：鍵交換のエンティティや秘密鍵のオーナーの Identifier と結び付いた key であり、ephemeral key より長寿命な key。

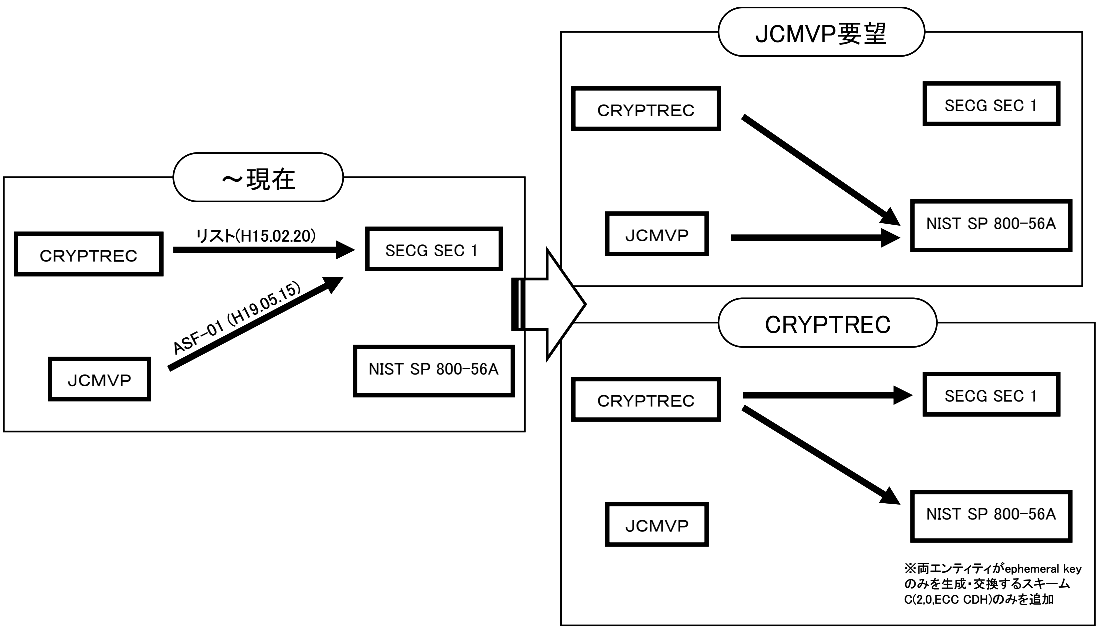
（４）NIST SP800-56A に規定されている 5 種類のスキームのうち、ephemeral key のみを使う最も構造の単純なスキームが、SECG SEC 1 v1.0 のスキーム(それにより強い制限を課したもの)に相当する。static key を使う、NIST SP800-56A のその他 4 種類のスキームについては、static key の assurance 等に厳しい規約を課している。

となっています。

このような理由により、NIST SP800-56A の ephemeral key のみを使うスキームについては、SECG SEC 1 v1.0 のスキームに相当し、安全性に問題はないものの、NIST SP800-56A の static key を用いる残りの 4 種類の ECDH スキームについては、SECG SEC 1 v1.0 で規定されているスキームの範囲を超えており、仕様書の参照先とするには年度内には結論が至りませんでした。

したがって、仕様の参照先を変更する場合には、KDF 関数の仕様に関する差異による相互接続性を考慮すれば、SECG SEC 1 を残し、NIST SP 800-56A の中の、両エンティティが ephemeral key のみを生成、交換するスキーム C(2,0,ECC CDH)[7]のみを追加することが妥当であると判断いたしました（図３を参照のこと)。なお、この結果は、今後発表されます CRYPTREC Report 2007 や CRYPTREC の Web サイト上でも公表される予定です。

図３



[7] 記号 C については、NIST SP 800-56A の 6 節、Table 4 及び Table 5 (p.51)を参照のこと。

４．ＥＣＤＳＡの仕様の参照先の変更について

現在の電子政府推奨暗号リストにおけるECDSAの仕様参照先はSECG SEC 1 v1.0です。SECG SEC 1 v1.0 と ANS X9.62-2005 の間に存在する技術仕様上の差異は、楕円曲線ドメインパラメータの選択方法にあり、以下が主なものである：

（１）　使用できる基礎体の範囲：
ANS X9.62-2005はセキュリティレベル[8]が80以上となっていて、SECG SEC 1 v1.0のようなセキュリティレベルが80未満のレベルは許容していない。

（２）　仕様できる基底の範囲：
SECG SEC 1 v1.0とANS X9.62-2005の間で、一方が許容するパラメータを他方が許容しない可能性があるため、相互接続できない場合があり得る。

（３）　コファクターの許容範囲：
ANS X9.62-2005はSECG SEC 1 v1.0よりも条件が緩和されているが、セキュリティレベルに依存して、ベースポイントの位数の下限が規定されているので、安全性が低下することはない。

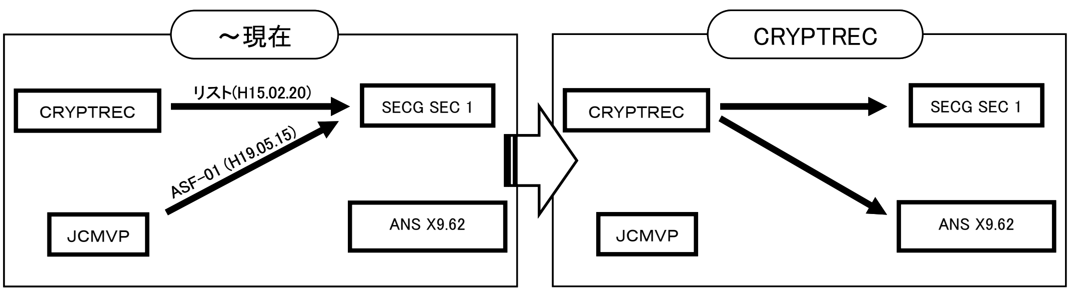
（４）　MOV条件：
ANS X9.62-2005はSECG SEC 1 v1.0よりも条件が厳しくなっているので、安全性に問題はない。

（５）　擬似乱数生成器：
HMAC_DRBGというHMACベースの擬似乱数生成器が承認されたものとして利用できる。これは、JCMVPにおいて評価されており、安全性に問題はない。

（１）～（５）の理由から、ANS X9.62-2005 の ECDSA については、安全性に問題はないものの、SECG SEC 1 Ver.1.0 と ANS X9.62-2005 のどちらを認証基準にするにしても、他方が認証されない場合があり得るものと考えられます。

したがって、仕様の参照先を変更する場合には、SECG SEC 1 を残し、ANS X9.62-2005 を追加することが妥当であると判断いたしました（図４を参照のこと）。なお、この結果は、今後発表されます CRYPTREC Report 2007 や CRYPTREC の Web サイト上でも公表される予定です。

図４



[8] セキュリティレベルについては、ANS X9.62-2005 の 6.1 節及び SECG SEC 1 v1.0 の 3.1 節を参照のこと。

５．ＰＳＥＣ－ＫＥＭの仕様の変更について

現在の電子政府推奨暗号リストにおける仕様参照先は、2002 年度までに提案者から応募された 2002 年 5 月 14 日付けの提出書類に基づくものです[9]。

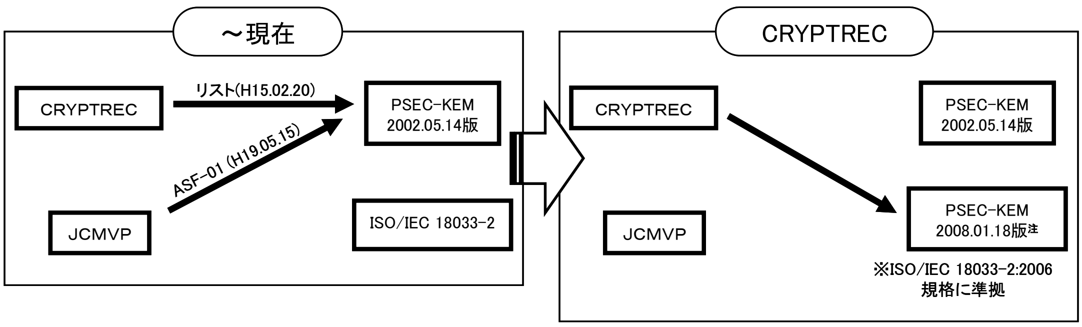
ISO/IEC 18033-2の審議過程において、エディタ並びに各国からのコメント等を吸収する形で提案された仕様に一部修正が加えられ、最終的に規格化されたものが電子政府推奨暗号リスト策定時のものと若干異なるものとなりました。そこで仕様書の変更の妥当性を判断できる資料を作成するために今年度評価を行いました。なお、評価に当たっては、提案者に新たに資料の提出を求めております。

一部仕様変更により、証明可能安全性において証明の見直しが必要となるものの、ISO/IEC 18033-2:2006 の仕様そのままではなく、楕円曲線上の点がなす群に限定して議論することで、現仕様と比べて、安全性評価結果の帰着効率が 2 倍程度低下しますが、従来と同様の安全性を示すことができることがわかりました。

このような理由により、ISO/IEC 18033-2:2006 における PSEC-KEM については、楕円曲線上の点がなす群に限定することで安全性に問題はないと考えられます。また、2002 年 5 月 14 日付けの仕様書に基づくものは普及しておらず、互換性維持の必要はありません。

したがって、仕様の参照先を変更する場合には、2008 年 1 月 18 日[注]付けの新しい提出書類に基づく仕様書のみにすることが妥当であると判断いたしました（図４を参照のこと）。なお、この結果は、今後発表されます CRYPTREC Report 2007 や CRYPTREC の Web サイト上でも公表される予定です。

図５



以上

[9] http://cryptrec.nict.go.jp/cryptrec_03_spec_cypherlist_files/PDF/02_02jspec.pdf

[注] 第 3 回暗号技術検討会開催後、主に型変換関数に関する修正等が施された仕様書の再提出があった（2008 年 4 月 14 日）。それらの修正等は安全性には影響がないものと判断されたため、2007 年度内での検討結果と併せ、最終的に 2008 年 4 月 14 日版である仕様書が参照先として適当であると判断された。

発行日　2008 年 5 月 30 日　第 1 版 第 1 刷
　　　　2008 年 7 月　7 日　第 2 版
発行者

・〒184-8795
東京都小金井市貫井北四丁目 2 番 1 号
独立行政法人 情報通信研究機構
（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