CRYPTREC Report 2006

平成 19 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

現在、CRYPTREC 活動は平成 15 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セキュリティ要件及び試験要件の策定等を行っている。本書は、**“暗号技術監視委員会の平成 18 年度の活動報告書”**である。

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平成 12 年度から平成 14 年度の 3 カ年をかけて我が国の電子政府で利用可能な暗号技術のリストアップを目的とした暗号技術評価活動(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、平成 14 年度末に、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。

平成 15 年度からは、暗号技術の安全性に係る研究開発動向の監視活動を担うため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。

“監視活動元年”の平成 15 年度は、暗号技術監視委員会、暗号技術調査ワーキンググループの設置等、監視体制の樹立に始まり、監視活動方針・手順の確立とそれに従った監視活動及び関連調査活動等を行った。平成 16 年度は、8 月にはハッシュ関数 SHA-0、SHA-1 に対する衝突（collision）発見方法について注目すべき学会発表があり、監視活動の一環として SHA-1 の危殆化に関する調査を強化した。平成 17 年度は、ハッシュ関数の危殆化が危惧されることからハッシュ関数の安全性について再検討するとともに、電子署名法の指針の改訂および電子政府推奨暗号リストの見直しに向けた活動を重点に実施した。平成 18 年度は、素因数分解問題や有限体及び楕円曲線上の離散対数問題の有する数論的困難性に関する安全性について調査を行い、主に公開鍵暗号の鍵生成における、より大きなサイズのセキュリティパラメータの選択について検討を行った。

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なけれ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、暗号技術の研究者、実装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.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。

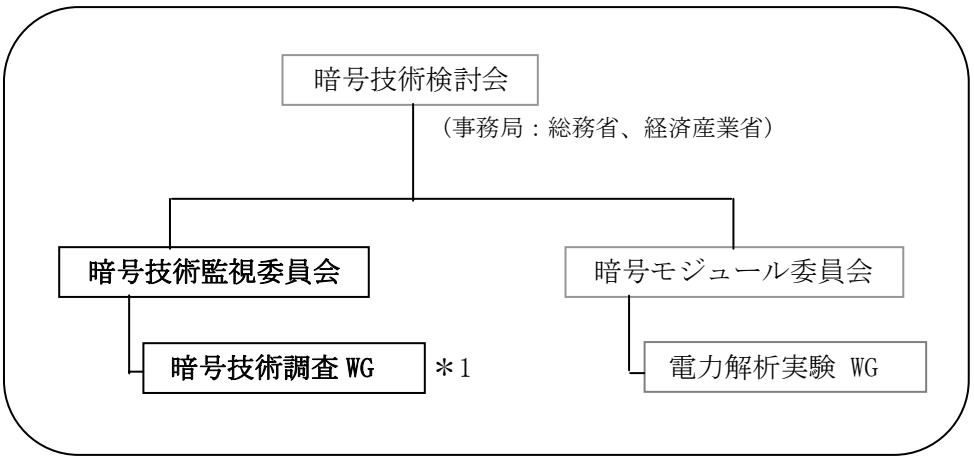
【問合せ先】　info@cryptrec.jp

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 18 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､「公開鍵暗号のセキュリティパラメータ」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) 公開鍵暗号の鍵生成におけるセキュリティパラメータの調査

図 1　CRYPTREC 体制図

委員名簿

暗号技術監視委員会

委員長	今井 秀樹	中央大学 教授
顧問	辻井 重男	情報セキュリティ大学院大学　学長
委員	太田 和夫	国立大学法人電気通信大学 教授
委員	金子 敏信	東京理科大学 教授
委員	佐々木 良一	東京電機大学 教授
委員	松本 勉	国立大学法人横浜国立大学 教授
委員	大塚 玲	独立行政法人情報処理推進機構 主任研究員
委員	田中 秀磨	独立行政法人情報通信研究機構 主任研究員
委員	山村 明弘	独立行政法人情報通信研究機構 グループリーダ
委員	渡辺 創	独立行政法人産業技術総合研究所 副研究センター長

暗号技術調査ワーキンググループ

委員	荒木 純道	国立大学法人東京工業大学 教授
委員	有田 正剛	情報セキュリティ大学院大学 教授
委員	小暮 淳	株式会社富士通研究所 主任研究員
委員	酒井 康行	三菱電機株式会社 チームリーダ
委員	四方 順司	国立大学法人横浜国立大学 助教授
委員	新保 淳	株式会社東芝 主任研究員
委員	洲崎 誠一	株式会社日立製作所 主任研究員
委員	藤岡 淳	日本電信電話株式会社 主幹研究員
委員	松崎 なつめ	松下電器産業株式会社 チームリーダ
委員	青木 和麻呂	日本電信電話株式会社 研究主任
委員	川村 信一	株式会社東芝 室長
委員	香田 徹	国立大学法人九州大学 教授
委員	古原 和邦	独立行政法人産業技術総合研究所　主幹研究員
委員	下山 武司	株式会社富士通研究所 研究員
委員	角尾 幸保	日本電気株式会社 主席研究員
委員	時田 俊雄	三菱電機株式会社　主席研究員
委員	古屋 聡一	株式会社日立製作所 研究員
委員	森井 昌克	国立大学法人神戸大学 教授
委員	廣瀬 勝一	国立大学法人福井大学 助教授
委員	盛合 志帆	ソニー株式会社　シニアリサーチャー
委員	内山 成憲	公立大学法人首都大学東京　准教授

オブザーバー

大貫 秀明	内閣官房 情報セキュリティセンター
掛川 昌子	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
山本 寛繁	総務省 行政管理局
田中 敦仁	総務省 自治行政局
澤田 邦彦	総務省 自治行政局
藤田 和重	総務省 情報通信政策局
川崎 光博	総務省 情報通信政策局
網野 尚子	総務省 情報通信政策局
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
臼井 伸幸	防衛省 運用企画局
神藤 守	防衛省 陸上幕僚監部
滝澤 修	独立行政法人 情報通信研究機構
大蒔 和仁	独立行政法人 産業技術総合研究所

事務局

独立行政法人 情報通信研究機構

篠田陽一、山村明弘、黒川貴司、松尾真一郎、松尾俊彦、金森祥子

独立行政法人 情報処理推進機構

三角育生、山岸篤弘、大熊建司、伊東徹、鈴木幸子、大久保美也子、杉田誠

第 1 章　活動の目的

1.1 電子政府システムの安全性確保

電子政府システムが平成 15 年度に本格的に始動した。電子政府システムの安全性の確保は緊急に対処しなければならない。内閣府高度情報通信ネットワーク社会推進戦略本部(IT 戦略本部)(http://www.kantei.go.jp/jp/singi/it2/index.html)は e-Japan 戦略 II(平成 15 年 7 月)を発行し、「新しい IT 社会基盤整備」において「安心・安全な利用環境の整備」を唱え、電子政府や電子自治体、重要インフラ等の公共的分野のサービスの情報セキュリティ対策の一層の充実が求めている。また、平成 15 年 8 月には、e-Japan 重点計画-2003、平成 16 年 6 月には、e-Japan 重点計画-2004 と計画の進展にともなってより具体的な施策が示されている。

これらの電子政府、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。

このため、平成 17 年までに世界最先端の IT 国家になるとの目標を達成するための e-Japan 戦略Ⅱ加速化パッケージ(平成 16 年 2 月)においてもセキュリティ(安全・安心)政策の強化が政府として取り組むべき重点施策とされていて、各府省庁の情報セキュリティ確保において「攻撃の予兆や被害に関する情報収集・分析」が重要案件としてあげられている。また、政府の IT 戦略本部が平成 17 年 5 月 30 日に設置した情報セキュリティ政策会議から出された「政府機関の情報セキュリティ対策のための統一基準（平成 17 年 12 月版（全体版初版))」（平成 17 年 12 月 13 日）においても、新規（更新を含む）に暗号化又は電子署名の付与のアルゴリズムを導入する場合には、電子政府推奨暗号リストの中から選択することが基本遵守事項として明記されている。

平成 18 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」が決定されている。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 2006」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とともに、電子政府推奨暗号のあり方の見直し等を含めた暗号利用に関する政府内の推進体制について、2006 年度に検討を開始する」こととされている。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・分析すること及び内閣官房情報セキュリティセンターをはじめとする各政府機関における暗号の危殆化への対応体制の整備が不可欠である。

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14年度版）は、次のURLから入手できる。
http://www.cryptrec.jp/report.html

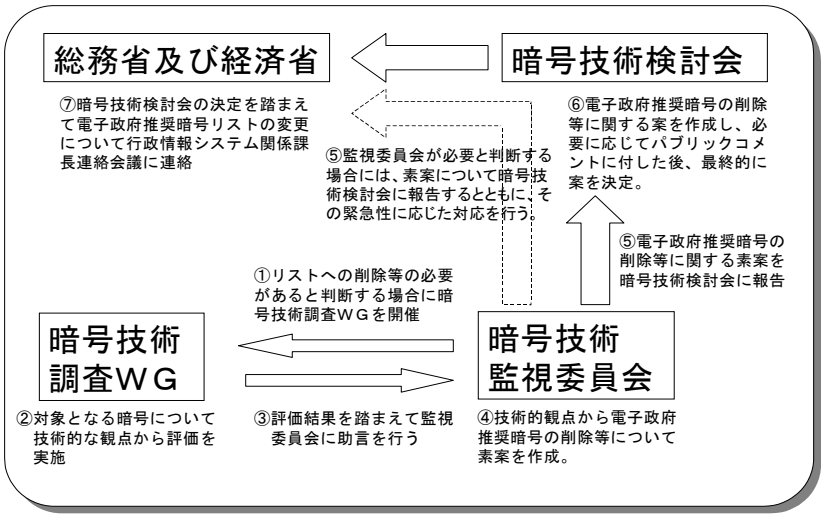
1.4 活動の方針

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18年度は、素因数分解問題や有限体及び楕円曲線上の離散対数問題の有する数論的困難性に関する安全性について調査を行い、主に公開鍵暗号の鍵生成における、より大きなサイズのセキュリティパラメータの選択について、検討する。

第 2 章 監視活動

2.1. 概要

電子政府推奨暗号リストに記載されている公開鍵暗号方式の安全性は、(a) n=pq 型素因数分解問題 (Integer Factoring Problem、以下 IFP と略する。)、(b) 有限体上の離散対数問題 (Discrete Logarithm Problem、以下 DLP と略する。)、(c) 楕円曲線上の離散対数問題 (Elliptic Curve Discrete Logarithm Problem、以下 ECDLP と略する。) のいずれかの困難性に依存している。「暗号技術検討会 2002 年度報告書」の 3.2.4.節 暗号技術評価結果の概要、(1) 公開鍵暗号方式の総評について(p.12) では、それぞれ以下のような判断をしてきた。

(a) n=pq 型 IFP　安全性の観点から法パラメータ n=pq のサイズは 1024 ビット以上のものを利用することを強く推奨する。
(b) DLP　安全性の観点からパラメータ p のサイズは 1024 ビット以上を選択することを強く推奨する。
(c) ECDLP　安全性の観点から群位数が 160 ビット以上の素因子をもつようなパラメータを選択することを強く推奨する。

一方、NIST (National Institute of Standards and Technology : (米国)国立標準技術研究所) は、Special Publication 800-57、Recommendation for Key Management - Part 1: General (Revised)[1] の 66 ページの Table 4 において、表 2.1 に示されるような推奨値を与えており、2010 年以降、上記のような数論的問題の困難性に関するパラメータ選択では強い安全性を求められる利用に関しては安全性が十分でないことを示唆している。

また、ECRYPT[2]では、年次報告書 (ECRYPT Yearly Report on Algorithms and Keysizes[3]) を公表しており、Chapter 7、Table 7.2において、表2.2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。

そこで、平成 18 年度は、数論的問題 (素因数分解問題や有限体及び楕円曲線上の離散対数問題) の困難性について調査を行い、主に公開鍵暗号方式のセキュリティパラメータサイズの選択について検討を行うため、新規に公開鍵暗号ワーキンググループを組織した。ワーキンググループ (WG) が活動した主要活動項目は、表 2.3 の通りである。

[1] http://csrc.nist.gov/publications/nistpubs/ から入手可能。
[2] http://www.ecrypt.eu.org/index.html
[3] http://www.ecrypt.eu.org/documents.html から入手可能。

表 2.1 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2.2 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

表 2.3　平成 18 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
公開鍵暗号 WG	太田和夫	①素因数分解問題の困難性の計算量についての調査・検討 ②有限体及び楕円曲線上の離散対数問題の計算量についての調査・検討 ③電子政府推奨暗号リストに記載されている公開鍵暗号技術に関する仕様書の改訂等(NIST や ANSI における見直しに伴うもの)について調査・検討

特に、①に関しては、理論的な考察だけではなく、ソフトウェア実装及びハードウェア実装を実施し[4]、実験を基にして攻撃に必要な計算量の見積もりを行った。2.2.1 節において、上記の数論的問題の困難性の安全性評価についての概要を示す。詳細は、第 3 章を参照のこと。また、③に関しては、今年度、NIST の FIPS186-3(ドラフト版)と FIPS186-2 との差異については調査を行ったが（2.2.2.2 節を参照)、詳細な調査・検討は、次年度に実施することとした。

2.2.　監視活動報告

2.2.1. 公開鍵暗号技術に係わる安全性評価について

2.2.1.1.　　n=pq 型 IFP の安全性評価

＜ソフトウェア評価＞

表 2.1 に示された NIST による「法サイズが 1024 ビットの n=pq 型 IFP が 2010 年まで有効(暗に、それ以降の有効性は保証していない)」との根拠を、ソフトウェア実装・実行して実績が上がっている技術を基にして、検証することを目的とした。現在のところ最も有望である一般数体ふるい法を用いて、n=pq 型 IFP の計算量を評価した。今回は時間的な制約から、1536 ビットと 2048 ビットの「ふるい処理」のみをソフトウェア実装することで、計算量を見積もることとした。また、ほぼ同様な手順で評価された 768 ビットと 1024 ビットの結果についても補足している。ここで、一般数体ふるい法における計算時間の主要項である「ふるい処理」と「線形代数処理」は、漸近的な実行時間の評価において同等であり、これまでのところ、一般数体ふるい法により分解された合成数の世界記録において、ふるい処理の方が線形代数処理より多くの時間を要していることが知られていることから、

[4] 実際には、それぞれ、暗号技術監視委員会から依頼された外部評価者、及び、情報通信研究機構（NICT）の委託研究による実装である。

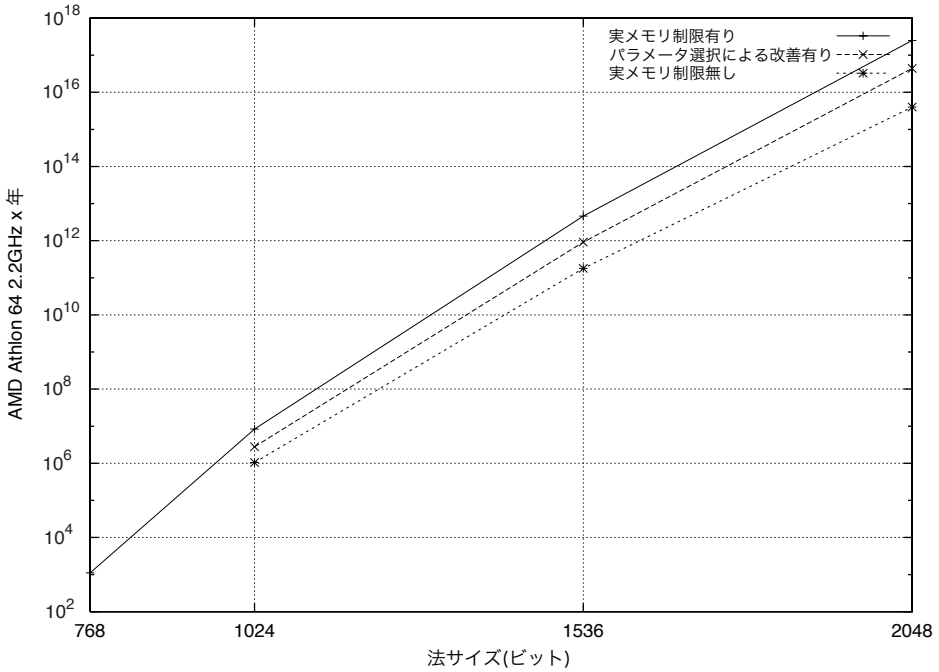
この計算量見積もりには妥当性がある。

表2.4にソフトウェア評価の結果を示す。表2.4をグラフにすると、図2.1のようになる。評価に利用したCPUはAMD Athlon 64 2.2GHz (2GB RAM)である。表2.4の各行において、下の行ほどふるい処理のパラメータ選択が最適化されているが、仮定の積み重ねであるため見積もりの精度が落ちてくることに注意する。詳細は、第3章を参照のこと。

表2.4　ふるい処理時間の推測（単位は、AMD Athlon 64 2.2GHz x 年[5]）

法パラメータのサイズ（ビット） ふるい処理の パラメータ選択の最適さ	768	1024	1536	2048
実メモリに制約（2GB RAM）がある場合の見積もり	1108	8.4×10^{6}	4.5×10^{12}	25×10^{16}
ふるい処理に関するパラメータ選択をより改善した場合の見積もり	-	2.8×10^{6}	0.92×10^{12}	4.4×10^{16}
実メモリにそれほど制約がない場合の見積もり	-	1.05×10^{6}	0.18×10^{12}	0.4×10^{16}

図2.1　ふるい処理時間の推測（単位は、Athlon 64 2.2GHz x 年）



＜ハードウェア評価＞

[5] AMD社製CPUであるAthlon 64 2.2GHz を1年間動作し続けたときに得られる計算量を意味する。

素因数分解専用ハードウェアの処理性能を、動作可能なハードウェアとして設計・製造されたシステムを基に、その処理性能を計測し、ソフトウェアの性能と比較することで推測した。ハードウェア装置としては、情報通信研究機構(NICT)による委託研究[6]によって開発された素因数分解ハードウェア装置(ふるい処理装置)を利用して、実験を行った。

ふるいの結果として抽出される要素の個数、並びに、ふるい処理が終了するまでに実施する log 加算の延べ回数は、ふるい処理を行なう際に入力するパラメータを固定すれば[7]、ふるい処理を実施する装置(専用ハードウェア、PC 上のソフトウェア)にかかわらず一定である。このことを利用して、ハードウェア(HW)とソフトウェア(SW)における処理時間の比較を行った。

表 2.5 にハードウェア評価の結果を示す。現在のところ、専用ハードウェア装置の実装に要するコストは不明であるが、仮に実装が可能となった場合には、攻撃可能となる時期が、ソフトウェア処理による場合よりもさらに早まる可能性がある[8]。詳細は、第 3 章を参照のこと。

表 2.5　ハードウェア（HW）とソフトウェア（SW）の処理性能の比率

法パラメータのサイズ（ビット）	1024	1536	2048
処理性能の比率（SW の処理時間／HW の処理時間）	5.73	8.83	10.41

＜計算量と計算能力についての考察＞

表 2.4 で示された計算量を換算して、素因数分解が所定の時間内に可能になるものと推測される時期について考察する。

第一に、n=pq 型 IFP の攻撃に必要な計算量に関しては、以下のような前提を設けた。

前提 1:　ふるい処理の計算量見積もりについては、表 2.4 の値を採用する。

前提 2:　素因数分解のアルゴリズムに関しては、これから 30 年間はブレークスルーがなく、一般数体ふるい法よりも効率の良いアルゴリズムが発見されないものとする。また、アルゴリズム等の大きな改良もないものとする。つまり、計算機性能の向上による計算能力の増大が、安全性を脅かす主な要因とみなす。

前提 3:　ふるい処理の計算が 1 年間で処理し終えることをもって、素因数分解が完了したものとみなす。漸近的な実行時間の評価において、ふるい処理

[6] 情報通信研究機構（NICT）の委託研究「素因数分解の困難性に基づく暗号の技術的評価に関する研究開発」、http://www2.nict.go.jp/q/q265/s802/s1_seika.htm

[7] 実際には、処理時間を最適化するために、法サイズに依存して変えるのが一般的である。

[8] 独立行政法人理化学研究所が構築したピーク性能 1 ペタフロップス(PFLOPS)を実現する分子動力学シミュレーション専用コンピュータ・システム MDGRAPE-3 のような可能性が考えられる。
http://www.riken.jp/r-world/info/release/press/2006/060619/index.html

と線形代数処理は同じオーダーであること、一般数体ふるい法により分解された合成数の世界記録において、これまでのところふるい処理の方が線形代数処理より多くの時間を要していることから[9]、このように仮定した。

第二に、計算機性能の将来予測に関しては、さまざまなモデルを設定可能であるが[10]、本ワーキンググループでは、以下のような前提を設けた。

前提 4: 計算機性能の将来予測に関しては、スーパーコンピュータのベンチマーク結果[11]の 1 位から 500 位を 1993 年から半年毎に集計している Web サイト TOP500.Org[12]に過去掲載された計算機における FLOPS(ピーク性能)の統計値を外挿することにより算出する。ここを取り上げたのは、このような情報を収集している場所が他にはなく、実際に構築されたスーパーコンピュータのうち、高性能なものの代表として相応しいと考えられるからである。

前提 5: 近年の汎用 CPU 及びスーパーコンピュータにおける整数演算性能と浮動小数点演算性能については、ほぼ同等（1 対 1）であるとした。

最後に、計算量の換算に関しては、以下のような前提を設けた。

前提 6: 一般数体ふるい法の処理はもっぱら CPU の整数演算を用いるものなので、計算能力の比較には、整数演算性能を用いるのが適当であるが、前提 5 により、CPU における浮動小数点演算性能への換算を行った。

前提 7: 基準点として用いる Athlon 64 2.2 GHz の FLOPS[13](ピーク性能)値は、(クロック周波数)x(浮動小数点演算ユニット数)によって見積もる。Athlon 64 2.2 GHz の場合は、4.4 GFLOPS である。

以上の前提の基、将来獲得するものと予測される計算処理能力の推移と n=pq 型 IFP の攻撃に必要な計算量の関係をグラフにすると、図 2.2 のようになる。

---

[9] DLP の場合には、線形代数処理の方がふるい処理よりも時間がかかることがある。

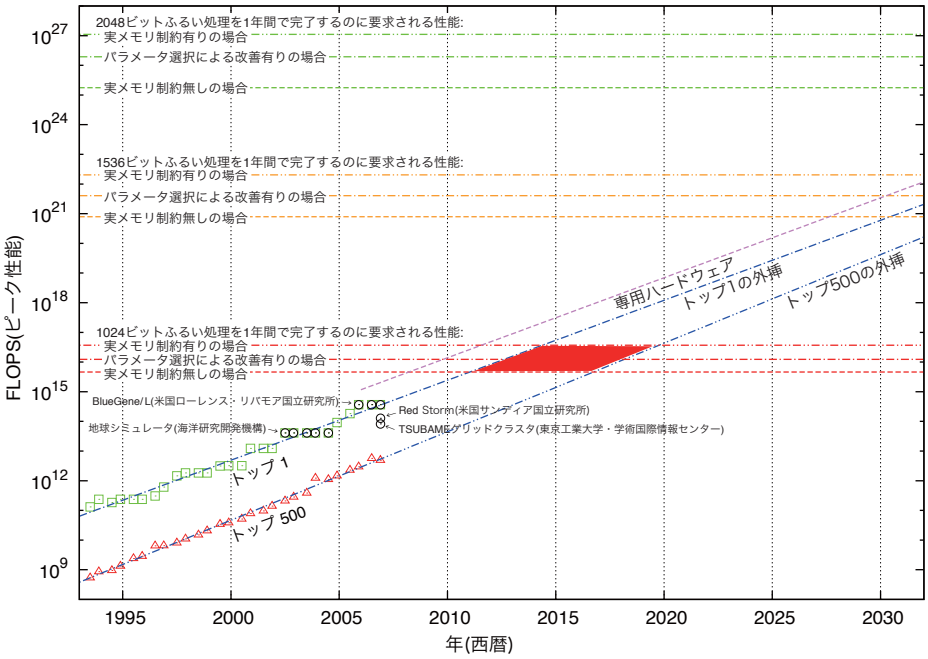
[10] 独立行政法人 情報処理推進機構、電子政府行政情報化事業「将来の暗号技術に関する安全性要件調査」調査報告書、2004 年 2 月、第 4 章
http://www.ipa.go.jp/security/fy15/reports/crypt_requirement/documents/crypt_requirement.pdf

[11] 実際の順位付けには、浮動小数点演算性能を測るために、一般的な線形方程式系を解く速さを測定する LINPACK というベンチマークプログラムの結果が利用されている。LINPACK 性能はピーク性能とは異なる。また、計算機のアーキテクチャによっては、ここには載らないようなスーパーコンピュータもある。

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

[13] フロップス（FLOPS）= 1 秒間に何回浮動小数点演算ができるかを表す単位。

図 2.2　1 年間でふるい処理を完了するのに要求される処理性能の予測[14]



【n=pq 型 IFP の安全性評価のまとめ】

新たな攻撃法によって、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。次に、表 2.4 で示された計算量を利用して、サイズが 1024、1536、2048 ビットの法パラメータの素因数分解を 1 年間で完了するには、その計算機の CPU がどの程度の処理性能を持つ必要があるかを見積もり、それをもって高性能なスーパーコンピュータがその処理能力を獲得する時期について予測した。一般数体ふるい法の処理はもっぱら CPU の整数演算を用いるものであるが、スーパーコンピュータの計算能力はその CPU の浮動小数点演算によって規定されることが多いため、CPU の浮動小数点演算性能は整数演算処理性能と同等とみなし評価を行った。なお、表 2.4 において言及されている Athlon 64 2.2GHz は、4.4 GFLOPS（ピーク性能）である。ここでは素因数分解はふるい処理の計算を終えることをもって完了したものとみなす。また、今後の研究の進展によって一般数体ふるい法等のアルゴリズムの計算量が低減することもあり得るが、今回の評価では、計算機性能の向上による計算能力の増大が主な危殆化の要因と考えた。

以上の仮定のもと、法パラメータのサイズが 1024 ビットの IFP （n=pq 型素因数分解問題）を 1 年間の計算によって完了させるためには、10^{15}FLOPS から 10^{17}FLOPS の処理能力を持

[14] 参考（コスト）：地球シミュレータ（海洋研究開発機構）約 400 億円、TSUBAME（東京工業大学）約 20 億円、BlueGene/L（米国ローレンス・リバモア国立研究所）約 1 億ドル、Red Storm（米国サンディア国立研究所）約 9000 万ドル

つ計算機が要求され、高性能なスーパーコンピュータが過去の成長率を続けて成長した場合に、そのレベルに到達する時期は、図 2.2 に示すように 2010 年～2020 年の間と推定することができた。

従って、法パラメータ n=pq のサイズが 1024 ビットである n=pq 型 IFP は強い安全性を求められる利用には有効とは言えない。仮に専用ハードウェア装置の実装が可能となった場合には、攻撃可能となる時期がソフトウェア処理による場合よりもさらに早まる可能性があるが、NIST が示す推奨アルゴリズムと最小鍵長（表 2.1）における、法パラメータ n=pq のサイズが 1024 ビットの n=pq 型 IFP の利用期限の根拠に関しては、不明な部分も残るため、引き続き注意していくことが必要と考える。

2.2.1.2. DLP の安全性評価

新たな攻撃法によって、安全性に懸念を持たせるような事態は生じていないことを確認した。

DLP と n=pq 型 IFP の漸近的な計算量のオーダーは同じである。現状では DLP の解かれた記録は、n=pq 型 IFP での解かれた記録に比べ、10 進 50 桁程度ビットのサイズが小さい。これは DLP に関する評価研究が素因数分解問題の研究ほど活発に行われていないためであると考えられる。

従って、DLP ベースの安全な鍵サイズは、n=pq 型 IFP ベースの安全な鍵サイズと同等である。詳細は、第 3 章を参照のこと。

2.2.1.3. ECDLP の安全性評価

新たな攻撃法や既存の攻撃法の改良によって、安全性に懸念を持たせるような事態は生じていないことを確認した。

楕円加算・倍算1回の処理速度と、共通鍵暗号の暗号化1回分の処理速度を比較すると、概算で同程度であることが経験的に知られている。一般的なECDLP に対する解法としては、Rho 法が最も有効であり、ECDLP の入力サイズを k とすると、その計算量は$O(2^{k/2})$ となる[15]。このことから、ECDLP に基づく公開鍵暗号の安全な鍵サイズの評価には、共通鍵暗号の安全な鍵サイズの評価を用いた。

従って、ECDLP に基づく公開鍵暗号の安全な鍵サイズは、160ビット以上であれば、少なくとも2010年までは安全であると評価できる。詳細は、第3章を参照のこと。

[15] $f(n)=O(g(n))$ とは、n に依存しない正の定数 c と整数 m が存在して、$n \geqq m$ である任意の n について $f(n) \leqq cg(n)$ が成立することを意味し、このとき、$f(n)$ は オーダー $g(n)$ であるという。

2.2.2. 実装の不備がもたらす脆弱性

RSA 署名（電子政府推奨暗号リストに記載されている RSASSA-PKCS1-v1_5 を含む）について、公開指数（public exponent） e が小さく、署名検証時のパディング長のチェックを無視した不適切な実装に対する攻撃方法が CRYPTO 2006（2006 年 8 月）のランプセッションにて発表されている。署名検証時において、ハッシュ値のデータの後に無意味なデータがないことのチェックを実行することや、RSA 署名の公開指数 e に、e=3 等の小さな値を利用しない等の偽造防止策が必要である。

2.2.3. NIST の暗号技術標準化動向

2.2.3.1. ハッシュ関数関連

本節では、2006 年 8 月に行われた NIST 2nd Hash Workshop の動向についてまとめる。2nd Hash Workshop では、主に次世代ハッシュ関数（Advanced Hash Standard、略して AHS）の仕様、および公募プロセスに関連する議論が行われた。以下に概要を記載し、詳細は付録 4 に記載する。

(1) NIST Hash Workshop における議論

下記において、会議トピックごとに概要を記載する。

(a) ハッシュ関数の構成法と安全性に関する研究について

本 WS ではハッシュ関数の構成法と安全性に関する研究成果がいくつか発表された。主な研究テーマは主に以下のように分かれている。

- Merkle-Damgaard の構成法を用いないハッシュ関数の構成法
- その安全性を証明が可能であるようなハッシュ関数の構成法
- 既存のハッシュ関数を用いて必要とされる安全性を担保するための手法

(b) 実システムにおけるハッシュ関数の利用形態について

実システムにおけるハッシュ関数利用用途を分類し、それに基づいて標準のハッシュ関数を構成すべきであるとの提案が行われた。

(c) SHA-256 と今後数年間の動向に関するパネルディスカッション

(i) 現在、SHA-1 と SHA-256 が抱えている問題について

- SHA-1 の利用については当面問題ないのではないか、ハッシュ関数の設計に際してはセキュリティパラメータを導入するべきではないか、といった議論があった。

(ii)　長期的な観点からハッシュ関数に求められる性質について

- ハッシュ関数の安全性については従来どおり collision-resistance を求めるべきである、実際の利用形態に即した性質を持たせるべきである、といった議論がなされた。

(iii)　AHS のデザインについて

- AHS としては単一のハッシュ関数を選定することとし、利用用途に応じて柔軟に対応できるように variant を用意しておく必要があるとの意見が大勢であった。
- AHS は十分な計算機環境で実装できるものを目指し、その他の環境への実装は、各実装側のリスクで行うべきとの見解が出された.
- AHS の設計においては、既存ハッシュ関数に修正を施したものと、全くの新しい設計思想に基づいたものが有り得るとの見解が出された。
- AHS の設計は、AES プロジェクトと同様に行われるとの見解が出された。

(d)　ハッシュ関数の攻撃方法と攻撃ツールについて

MD5 や SHA-1 の安全性に関する解析や、攻撃ツールに関する発表が行われた。

(e)　今後の公募スケジュールについて

AHS 標準化のスケジュールについて､FIPS180-2 は 2007 年と 2012 年に見直される予定で、2012 年が AHS を標準化されるタイミングであることが示された。AHS もこれに合わせる形で考えられ、NIST は将来、最低限の要求条件と評価基準、そして応募のための基準を示すと述べた。その後パブリックコメントを募集するが、2012 年を期限とすることが述べられた。プロセスにおいては、フィードバックをもとにアルゴリズムを修正できることが提案され、その他知的財産権の観点などで公平性を保つことが確認された。最後に、ハッシュ関数が幅広いアプリケーションに適用されるものであることが求められており、ラウンド数や出力長が可変であることが良いと述べた。また、AES と同様のプロセスを取り、性能よりも安全性を強調し、選ばれるハッシュ関数は 1 つで、mode は許すことが示された。

(2)　次世代ハッシュ関数公募の仕様

2007 年 1 月に、NIST は AHS アルゴリズムの公募について、Federal Register Vol.72 に掲載しており、現在パブリックコメントを募集している。パブリックコメントの締め切り

は 2007 年 4 月 27 日である。Federal Register に掲載された公募の要項のポイントは以下の通りである。

(a)　候補のアルゴリズムのドラフトにおいて最低限必要な事項

- アルゴリズムは公開され、非独占使用が可能で、特許使用料を放棄すること
- アルゴリズムは広範囲なハードウェアとソフトウェアに実装できること
- アルゴリズムは 224,256,384,512 ビットの出力を持ち、少なくとも 2^{64} ビットの入力に対応すること

(b)　応募に関する要件

- アルゴリズムについて、実装に必要な全ての数式、テーブル、パラメータを含む完全な仕様が記述されていること。
- ドキュメントは設計の根拠やセキュリティの根拠を含むこと。
- ドキュメントは、セキュリティを向上させるための、ラウンド数などの修正可能な 1 つ以上のパラメータや、その他の修正可能な部分についての記述を行うこと。
- ANSI C によるリファレンス実装と、最適な実装を記述すること。
- 8bit, 32bit, 64bit プラットフォームにおける計算量と必要なメモリ量の見積もりを示すこと。
- メッセージとハッシュ値の例を示すこと。
- 特許の情報を記述すること。
- アルゴリズムの利点と制限を記述すること。

(c)　評価基準

- 一方向性、2^{nd} pre-image resistance, collision resistance を含む安全性
- ランダムオラクルとの識別不可能性
- アルゴリズムの安全性に対する数学的な健全性
- 評価過程で出てきた他のセキュリティ要素における安全性
- 計算量的性能
- 必要なメモリ量
- ラウンド数などのパラメータ、実装における柔軟性
- 実装のシンプルさ

(3)　次世代ハッシュ関数選定仮スケジュール

AHS アルゴリズムの公募については、NIST より仮のタイムスケジュールが以下のように示されている。

表 2.6　次期ハッシュ関数選定の仮スケジュール[16]

Year 1(2007)	
1Q	・ 最小限の要求仕様、公募における要件、評価基準の案の公開とパブリックコメントの募集
2Q	・ コメントに対する対応の実施
3Q	・ 最小限の要求仕様、公募における要件、評価基準の最終版の公開 ・ 新ハッシュ関数の募集開始
Year 2(2008)	
3Q	・ 新ハッシュ関数の公募締め切り
4Q	・ 応募アルゴリズムのレビューと、基本的な公募要件に沿った候補のアルゴリズムの選定 ・ 第 1 ラウンドの候補をアナウンスする 1st Hash Function Candidate Conference の開催し、応募者によるプレゼンテーションの実施 ・ 第 1 ラウンドの候補アルゴリズムに対するパブリックコメントの募集
Year 3(2009)	
4Q	・ パブリックコメントの締め切り ・ 2nd Hash Function Candidate Conference を開催し、応募アルゴリズムの評価結果についての議論、応募者によるアルゴリズムの修正の提示を行う
Year 4(2010)	
1Q	・ 応募アルゴリズムに対するパブリックコメントの結果を参考に、最終候補アルゴリズムの選定作業を実施し、選定のためのレポートを作成する
2Q	・ 最終候補アルゴリズムのアナウンスと選定レポートの公開 ・ 最終候補アルゴリズムの応募者よる修正の実施 ・ 最終ラウンドの開始
Year 5(2011)	
2Q	・ 最終ラウンドのパブリックコメント終了
3Q	・ Final Hash Function Candidate Conference の開催し、最終候補アルゴリズムの応募者によるコメントについてのディスカッションの実施
4Q	・ パブリックコメントの結果を参考に、次期ハッシュ関数を決定 ・ 最終選定結果のレポートを作成 ・ 次期ハッシュ関数のアナウンス
Year 6(2012)	
1Q	・ 次期ハッシュ関数の仕様のドラフトを作成 ・ ドラフトの公開とパブリックコメントの募集

[16] 1Q（1 月-3 月）、2Q（4 月-6 月）、3Q（7 月-9 月）、4Q（10 月-12 月）

2Q	・ パブリックコメントの締め切りと、コメントに対する対応の実施
3Q	・ 次期ハッシュ関数に対する商務長官の承認の実施

2.2.3.2. 公開鍵暗号技術関連

NISTは、2006年3月にデジタル署名に利用される暗号アルゴリズムの改訂に向けてドラフト版仕様を公表した。この公表された規格案 FIPS186-3(Draft): Digital Signature Standard (DSS) は、2000年1月に発行されたFIPS186-2に代わるものであり、2006年6月12日にパブリックコメントを終了している。FIPS186-2とFIPS186-3(Draft)との主な相違点を以下にまとめる。詳細な比較に関しては付録5に掲載する。

(1) DSAの仕様について

FIPS186-2ではセキュリティパラメータpの値として64の倍数であるような512から1024ビットの間の値を指定していたが[17]、FIPS186-3では1024、2048、3072ビットから選択をするように規定している。

(2) RSAの仕様について

FIPS186-2ではセキュリティパラメータの値を指定していなかったが、FIPS186-3では1024、2048、3072ビットから選択をするように規定している。

(3) ECDSAの仕様について

FIPS186-2 では ANSI X9.62 (1998 年版) に準拠するように指定しているが、FIPS186-3ではANSI X9.62 (2005年版) に準拠するよう規定されている。

2.2.3.3. CMVP関連

NISTはFIPS規格やSP文書で規定された暗号アルゴリズムやプロトコルが正しくソフトウェアやハードウェアに実装されているか認定するプログラムとして、暗号モジュール認証プログラム(CMVP)を運用している。暗号モジュールの評価はFIPS140-2(2001年発効、2002年に change notice 2,3,4 が発効)に基づいて行われる。当該規格では、Cryptographic Module Testing laboratoriesとして登録されている第三者検査機関が、ターゲットとなる暗号モジュールが必要なセキュリティレベルを満足しているかを検証し、基準を満たすモジュールに関してはNIST及びCSE (カナダ政府通信安全保障局) からFIPS140-2認証を与える。現在NISTはFIPS140-2の改訂版であるFIPS140-3のドラフト版を作成中である。以下にFIPS140-3の作成状況を記載する。

[17] Change Notice 1 (2001年10月) の発行後には、1024ビットの値のみを指定している。

- 2005/01/12　NIST が FIPS140-2 の改訂版である FIPS140-3 の作成をアナウンス
- 2005/02/28　FIPS140-3 で規定するセキュリティ要件に関するコメント受付を終了
- 2005/09/26　Physical Security Testing Workshop を開催
- 2007 年 3 月現在　FIPS140-3 ドラフト第 1 版を NIST が作成中。ドラフトのパブリックレヴューを 2007 年第一四半期から 90 日間程度の期間で実施予定

表 2.7 において、FIPS140-2 認証を受けたハッシュ関数実装 IC カードのリストを記載する。

表 2.7　FIPS140-2 認証を受けたハッシュ関数実装 IC カードのリスト

製品名	ベンダ	発効日	SHA	詳細
PIV EP v. 108 Java Card Applet on Oberthur ID-One Cosmo 64 v5 Smart Card	Oberthur Card Systems	4/11/2006	SHA-1 (#209)	**Optional PIV Data Object Implemented: *** **1) Card Holder Facial Image** **2) Card Holder Printed Information** **3) X.509 Certificate for Digital Signature** **4) X.509 Certificate for PIV Key Management** **5) X.509 Certificate for Card Authentication**
SafesITe FIPS 201 applet, Version 1.20 on Gemalto GemCombi'Xpresso R4 E72 PK Card	Gemalto Corp.	4/20/2006	SHA-1 (#427)	**Optional PIV Data Object Implemented:*** **1) Card Holder Facial Image** **2) Card Holder Printed Information** **3) X.509 Certificate for Digital Signature** **4) X.509 Certificate for PIV Key Management** **5) X.509 Certificate for Card Authentication**
SETECS Inc.'s OneCARD™ PIV-II Java Card Applet (Version 1.2) on Gemalto GemCombi Xpresso R4 E72 PK card	SETECS Inc.	6/6/2006	SHA-1 (#427)	**Optional PIV Data Object Implemented: *** **1) Card Holder Facial Image** **2) Card Holder Printed Information** **3) X.509 Certificate for Digital Signature** **4) X.509 Certificate for PIV Key Management** **5) X.509 Certificate for Card Authentication**

2.2.4. ISO/IEC JCT 1 /SC 27 の暗号技術標準化動向

ISO において、ハッシュ関数は 10118 で規格化されている。2006 年 5 月に行われたマドリッド会議では、10118-1（General Part)、10118-2（ブロック暗号利用）について、見直しの議論が行われた。10118-3（専用ハッシュ関数）については、すでに SC27 の Web サイトで NIST の見解に追従するコメントが掲載されているが、引き続き状況を監視することが確認された。10118-4（算術演算利用）については、廃止に関する投票が行われたが、廃止は否決され、規格が継続することとなった。2006 年 11 月に行われた南アフリカ会議では、10118-2 について、訂正文書について議論が行われたほか、各国から見直しの寄書があり、見直しについての議論が行われた。その中で既存の技術への攻撃 の指摘、修正案、新たな

ハッシュ関数の提案がなされた。今後、再度改訂の議論を行うこととなった。

2.2.5. IETF の暗号技術標準化動向

IETF（Internet Engineering Task Force）は、インターネットに関する技術の標準を定める団体であり、インターネットで用いられるプロトコルの標準化を行っている。IETF 標準は、RFC という形で広く周知され、インターネットに接続する、あるいはインターネットを利用する製品の仕様、設計に反映されている。IETF では、年に 3 度行われる国際会議と、Mailing List による議論を経て標準化作業が進められる。IETF のセキュリティエリアでは、セキュリティ関連技術や、その基礎となる暗号技術を用いたセキュリティ技術について標準化を行う WG が活動している。当該エリアでは、暗号通信や電子署名機能などをサポートしている電子メール技術 PGP や S/MIME、サーバ-クライアント認証技術 Kerberos、トランスポート層で暗号化通信を実現するプロトコル TLS など、世の中で広く用いられているセキュリティ技術の規格化も行っており、今後は MD5 や SHA-1 に代わる新たなハッシュ関数の利用が可能となるように規格が改訂されていくものと予想される。表 2.8 では 2007 年 3 月時点において、セキュリティエリアで規格化を行っているセキュリティ技術の中でハッシュ関数を用いている技術を記載する。

表 2.8　IETF 標準規格におけるハッシュ関数の利用状況[18]

WG名	対象技術	関連RFC	利用ハッシュ関数	ハッシュ関数の用途
kerberos	サーバ-クライアント認証技術 (Kerberos)	RFC4556 RFC4120 RFC3962 RFC3961 など	SHA-1	• MACの生成 • 完全性の確保
openpgp	メール技術 (PGP)	RFC2440 など	MD2,MD5, RIPEMD160, SHA-1	• 電子署名における メッセージダイジェスト の生成
smime	メール技術 (S/MIME)	RFC2634 RFC2630 RFC2311 など	MD5,SHA-1	• MACの生成 • 完全性の確保
msec	グループ間秘匿通信プロトコル (MSEC)	RFC4650 RFC4359 RFC4534 RFC3830 RFC4442 RFC3547 RFC4383 など	MD5,SHA-1	• MACの生成 • PRF • 電子署名におけるメッセージダイジェストの生成
tls	サーバ-クライアント認証プロトコル (TLS)	RFC2246 など	MD5,SHA-1	• MACの生成 • PRF • 電子署名におけるメッセージダイジェストの生成

[18] 表中の PRF は擬似ランダム関数、MAC はメッセージ認証コードを表す。記載 WG の他に pkix、pki4ipsec で規格化している公開鍵証明書においても利用可能なハッシュ関数が規定されている。

以下では、第66回、第67回IETF meetingにおいて行われた議論をWG毎に記載し、それ以前の議論については付録6に記載する。

(1) 66th IETF Meeting

[開催日]：2006年7月9日-14日

本ミーティングでは、NISTのFIPS改定との整合性や、プロトコル仕様が議論された。

(a) Public Key Infrastructure (X.509) WG (pkix)

(i) DSA,ECDSAおよびSHA-2のアルゴリズム識別子について

- 新しいドラフトは、他のPKIX I-Dsと同様に、FIPS186-3の仕様に準拠する。ここで注目すべき変更は、CAsはECDSA署名の場合に使われるハッシュ関数アルゴリズムを常に明確に指定するという要件である。しかし、RPsにはハッシュ関数アルゴリズムを指定しない証明書の受理を許している。

(ii) PKIXの楕円曲線暗号用ID用アルゴリズムについて

- 提案文書は、ECC アルゴリズムのためにアルゴリズム IDs を指定する。Subject public･key infoのパラメータフィールドを通して表現することにより、その鍵が使われるアルゴリズムの記述法の慣例を採用する。これはANSI標準の表記法に準拠している。ただし、それはPKIXがこれまでにこの種の情報の表現方法とは一致していない。

(b) Transport Layer Security WG (tls)

(i) SHA-384について

NSA "Suite B" はSHA-384を利用しているので、SHA-384を含むべきであるとの提案がなされ、反対意見は出なかった。

(2) 67th IETF Meeting

[開催日]：2006年11月05日-10日

セキュリティエリアのWGにおいて、ハッシュ関数の取り扱いについて明に議論を行ったのはtls-WGのみであった。

(a) TLS (tls-WG)

- TLS1.2で用いられるPRFのデフォルトPRFについて議論がなされた。新たなcipher

suite では SHA-1、SHA-256 に対応した PRF を定義することができるものとし、デフォルト PRF は各 suite の設定に従うこととした。各 suite で完全性を保証するために用いられるハッシュ関数は最低でも SHA-1、あるいはそれ以上の安全性をもつハッシュ関数であること、デフォルトのハッシュ関数は SHA-256 とすることが合意された。

- TLS1.2 については、すでに十分な検討を終えており、今後は仕様に関するコメントは求めないこととした。ハッシュ関数の agility 確保への要求は新たな拡張を要し、仕様の改訂を迫ることになるため、現時点の仕様で固定するべきだとの意見が出た。

2.2.6. ECRYPT の動向

ECRYPT [19]は、科学・技術の研究・開発を支援するための、欧州連合（European Union）が策定する、研究と技術開発のための第6次(2002-2006)枠組み計画（Sixth Framework Programme）[20]において、情報社会技術プログラム（Information Societies Technology Programme）の一環として実施されている、主としてEUの情報セキュリティ研究者のための支援活動であり、2004年2月から続けられているものである。ECRYPTは、

(1) Symmetric techniques virtual lab (STVL)、
(2) Asymmetric techniques virtual lab (AZTEC)、
(3) Protocols virtual lab (PROVILAB)、
(4) Secure and efficient implementations virtual lab (VAMPIRE)、
(5) Watermarking and perceptual hashing virtual lab (WAVILA)

の5つの活動に分かれている。Webサイト[21]には各活動の報告書が公表されている。

STVLでは、eSTREAMという名称で、各国の研究者から提案されたストリーム暗号の評価プロジェクトが継続中である。今年度は、フェーズ3 候補の選定のため、SASC 2007 ワークショップ（2007年1月31日-2月1日）が行われ、Fast Software Encryption 2007（2007年3月26日-28日、ルクセンブルク)のランプセッション[22]において、表2.9の通り、フェーズ3 候補のリストが公表されている。2008年にはeSTREAMの最終的な評価が報告される予定となっている。ハッシュ関数に関しては、来年度、2007年5月にワークショップを開催する予定になっている[23]。また、VAMPIREでは、暗号解読に係わるハードウェア等の研究を目的とした、SHARCS(Special-purpose Hardware for Attacking Cryptographic Systems) 2006 ワーク

[19] http://www.ecrypt.eu.org/index.html
[20] http://www.cordis.lu/fp6/
[21] http://www.ecrypt.eu.org/documents.html
[22] http://fse2007.uni.lu/rump.html
[23] http://events.iaik.tugraz.at/HashWorkshop07/

ショップ（2006年4月3日-4日）を2005年に引き続き、今年度も開催している。来年度も開催予定である[24]。その他の今年度の主な動向としては、AZTECでは、量子コンピュータが実現されたとしても安全であるような公開鍵暗号系を研究することを目的とした、PQCrypto 2006 ワークショップ（2006年5月24日-26日）を開催している。

表2.9　eSTREAM フェーズ 3 候補のリスト

Profile 1 (SW)	Profile 2 (HW)
CryptMT (CryptMT Version 3)	DECIM (DECIM v2 and DECIM-128)
Dragon	Edon80
HC (HC-128 and HC-256)	F-FCSR (F-FCSR-H v2 and F-FCSR-16)
LEX (LEX-128, LEX-192 and LEX-256)	Grain (Grain v1 and Grain-128)
NLS (NLSv2, encryption-only)	MICKEY (MICKEY 2.0 and MICKEY-128 2.0)
Rabbit	Moustique
Salsa20	Pomaranch (Pomaranch Version 3)
SOSEMANUK	Trivium

2.2.7. IC カードへのハッシュ関数 SHA-256 実装状況

IC カードとは、カード内に半導体メモリ（RAM、ROM、EEPROM）を組み込む事により、従来の磁気ストライプカードに較べ数十倍から数千倍の情報量の取り扱いを可能にしたカードである。CPU やコプロセッサを組み込むことで、情報処理を可能とした IC カードも各カードベンダーから提供されている。

IC カードは IC チップでアクセス制御を行う事ができるため、IC チップを分解し、専用装置を用いて内部を解析しない限りは偽造が不可能であり、一般に磁気カードに較べ安全であると考えられている。 しかし、1990 年代中頃から、Kocher や Anderson らの研究により、実装上の脆弱性を利用したサイドチャネル攻撃などの攻撃方法が開発され、秘密鍵の読み出しが容易な IC カードの存在が判明している。このため多くの IC カードベンダーは、自社の IC カードが正しく暗号アルゴリズムを実装し、安全に利用できることを示すため、Common Criteria（CC）による評価・認証を獲得するケースが多くなってきている。

Common Criteria はセキュリティ製品の国際的統一評価基準として、1996 年に CC 第 1 版、1997 年に CC 第 2 版として CC 評価基準が策定、発行された。その後 CC 第 2 版に若干の修正を加えた CC 第 2.1 版が ISO/IEC15408 として国際標準規格となっている。現在の評価基準は、2006 年 9 月に策定された CC 第 3.1 版が使用されている。日本では情報処理推進機構（IPA）が 2004 年より ISO/IEC15408 の認証業務を開始している。Common Criteria では、評価対象となる製品（あるいは機能）がどのようなセキュリティ機能を備えているかというセキュリティ技術要件と、それらのセキュリティ機能が正確かつ

[24] http://www.ruhr-uni-bochum.de/itsc/tanja/SHARCS/

適正に実装されているかというセキュリティ保証要件を明らかにする必要があり、後者がどの程度の信頼性をもって実装されているかを 7 段階の評価保証レベル（EAL）によってレベル分けを行っている。

表 2.10 では、暗号技術を用いたサービスで多く利用されているハッシュ関数を実装したカードのうち、SHA-256 に対応した製品と EAL について記載する。

IC カードを利用したサービスは、実装されている暗号アルゴリズムの危殆化の影響が最も大きいサービスの一つであると考えられる。カードを不特定多数のユーザに配布するサービスが多く、実装アルゴリズム更新のためにカードを回収するコストが莫大になる。現在、CC 認証を受けている IC カードにおいて実装されているハッシュ関数のほとんどは危殆化が懸念されている SHA-1 であり、SHA-256 に対応しているカードは少数である。

表 2.10　SHA-256 対応 IC カード製品

製品名	TEMD version 1.0 (2004-3)
製造元	Microelectronica Espanola S.A.
保証レベル	EAL4+
認定日	2006/01/23
製品名	Java Card Open Platform
製造元	Axalto
保証レベル	EAL4+
認定日	2006/05/10
製品名	Renesas AE55C1 (HD65255C1) smartcard integrated circuit version 02 with ACL version 1.43 and additional SHA-256 function
製造元	Renesas Technology Corporation
保証レベル	EAL4+
認定日	2006/05/15

2.3. 学会等参加記録

平成 18 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。参加した国際会議・国内会議は、表 2.11 に示す通りである。今回調査した研究発表の中で、

ハッシュ関数 SHA-1 に対する解析の進展が、電子政府推奨暗号の安全性に大きく関わるものとして挙げられる。SHA-1 は近年、安全性への懸念が高まり、昨年度は衝突の発見が 58 段までだったのが 64 段まで伸びており[25]、今後の研究に注目する必要がある。また、米国 NIST がこれを受け、新規のハッシュ関数を公募するというアナウンスをしている。

表 2.11　国際会議・国内会議への参加状況

学会名・会議名		開催国・都市	期間
FC	Financial Cryptography and Data Security '06	Anguilla, British West Indies	2006/2/27 ～ 2006/3/2
TCC	Theory of Cryptography Conference 2006	New York, USA	2006/3/4 ～ 2006/3/7
FSE	Fast Software Encryption 2006	Graz, Austria	2006/3/15 ～ 2006/3/17
PKC	9th International Conference on Theory and Practice of Public Key Cryptography	New York, USA	2006/4/24 ～ 2006/4/26
EUROCRYPT	EUROCRYPT 2006	St. Petersburg, Russia	2006/5/28 ～ 2006/6/1
ACNS	4th International Conference on Applied Cryptography and Network Security	Singapore, Singapore	2006/6/6 ～ 2006/6/9
ACISP	11th Australasian Conference on Information Security and Privacy	Melbourne, Australia	2006/7/3 ～ 2006/7/5
SAC	13th Annual Workshop on Selected Areas in Cryptography	Montreal, Canada	2006/8/17 ～ 2006/8/18
CRYPTO	CRYPTO 2006	Santa Barbara, USA	2006/8/20 ～ 2006/8/24
NIST HW	NIST Second Hash Workshop	Santa Barbara, USA	2006/8/24 ～ 2006/8/25
VietCrypt	International Conference on Cryptology in Vietnam 2006	Hanoi, Vietnam	2006/9/25 ～ 2006/9/28
Asiacrypt	Asiacrypt 2006	Shanghai, China	2006/12/4 ～ 2006/12/7

[25] Fast Software Encryption 2007 (2007 年 3 月 26 日-28 日、ルクセンブルク)のランプセッションにおいて、70 段の衝突結果が報告されている (http://fse2007.uni.lu/slides/rump/sha.pdf)。なお、実際に使われる SHA-1 は 80 段であり、衝突が発見されたのはその短縮版である。

SCIS(国内)	Symposium on Cryptography and Information Security 2007	長崎, 日本	2007/1/23 ～ 2007/1/26
CT-RSA	RSA Conference Cryptographers Track	San Francisco, USA	2007/2/5 ～ 2007/2/9
TCC	The fourth Theory of Cryptography Conference	Amsterdam, Netherlands	2007/2/22 ～ 2007/2/24

また、情報収集を行なった学会等で発表された主要論文を付録 3 に示す。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 については従来の衝突発見段数の記録が 58 段から 64 段に更新（フルラウンドは 80 段）されたことが注目される。従来の衝突発見の記録が 1 ブロックのテキストに対し 80 段中 58 段の短縮版までだったのに対し、この結果では 2 ブロックのテキストで 64 段短縮版まで伸ばすのに成功している。この研究は、非線形キャラクタリスティックという新概念の導入により衝突発見効率を向上させた点に特徴がある。[Finding SHA-1 Characteristics, Christophe De Cannière and Christian Rechberger , Asiacrypt 2006]

現在 MAC (Message Authentication Code)として HMACS-SHA-1 が SHA-1 と組み合わされて標準的に用いられているが、近年の SHA-1 に対するアタックを利用した HMACS-SHA-1 などに対するアタックについて新しい報告があった。HMAC と NMAC は 1996 年にカリフォルニア大学サンディエゴ校の Bellare 氏により提案されていたメッセージ認証コードの方式で、特に HMAC は標準化され広く用いられている。今回の報告で、HMAC-MD4 や HMAC-MD5、HMAC-SHA-0 については現実的なアタックが可能であり、HMAC-SHA-1 については 34 段短縮版 SHA-1 を用いた HMAC についてはアタック可能であるというものであったが、フルラウンド SHA-1 を用いた HMAC-SHA-1 については現段階でアタック不能である。[Forgery and Partial Key Recovery Attacks on HMAC and NMAC Using Hash Collisions, Scott Contini and Yiqun Lisa Yin, Asiacrypt 2006]

SHA-224, 256 についてもアタックの試みがあった。しかしこの結果は SHA-224 の場合で 19 段短縮版、SHA-256 の場合で 18 段短縮版の衝突発見が可能（フルラウンドは 64 段）というもので、現段階でフルラウンドの安全性は脅かされていない。[Analysis of Step-Reduced SHA-256, F.Mendel, N.Pramstaller, C.Rechberger and V.Rijmen, FSE 2006]

2.3.2. ストリーム暗号の解読技術

ストリーム暗号については、ストリーム暗号の国際規格 ISO/IEC 18033-4 に採用されている SNOW 2.0 に対するアタックが発表されたことが注目される。このアタックは 2^{179} の長さの出力系列を得ることにより統計的な偏りが検出できるというものである。まだ必要とされる系列長が長く、現実的な脅威にはなっていない。[Improved Linear Distinguishers for SNOW 2.0, K.Nyberg, J.Wallén C.Rechberger and V.Rijmen, FSE 2006]

2.3.3. ブロック暗号の解読技術

ブロック暗号については、中国科学院の研究者による 7 段または 8 段簡略版 192 ビット鍵 AES に対する関連鍵不能差分攻撃による解析が注目される。従来の解読記録は更新してはいないため電子政府推奨暗号の安全性には影響は無いものの、近年中国が急速に暗号解析の研究レベルを向上させてきており、今後の動向に注目する必要がある。[Improved Related-Key Impossible Differential Attacks on Reduced-Round AES-192, Wentao Zhang, Wenling Wu, Lei Zhang and Dengguo Feng, SAC06]

2.3.4. 公開鍵暗号の解読技術

RSA署名について、正しくない実装に対する効果的な攻撃方法が発表された。具体的には、PKCS #1 (RSA Cryptography Standard) 等に基づくRSA署名について公開鍵の指数 e が小さく、署名検証時のパディング長のチェックを省略した実装に対し、不正につける string を調節することにより、検証で受理されてしまう署名の偽造が比較的容易に実現できる可能性を指摘した。CRYPTRECとしては、既に2002年にその危険性を指摘していた。(CRYPTREC Report 2002 P112 参照) 本発表をトリガに各種関係機関はレポート・対応策などを提示した。[Forging some RSA signatures with pencil and paper, Daniel Bleichenbacher, CRYPTO 2006, Rump session]

RSA 暗号に関して、秘密鍵 d が小さい場合の効率的な解析手法の研究結果がいくつか従来結果として示されている。CRT(Chinese Remainder Theorem) 等を用いる方法や Lattice を利用した方法、従来方法の効率的な部分を併用した方法など結果が示されている。また、d が小さい場合の攻撃手法に対する一般化への試みなども行なわれている。[New Attacks on RSA with Small Secret CRT-Exponents, Daniel Bleichenbacher and Alex May, PKC 2006], [A Strategy for Finding Roots of Multivariate Polynomial with New Applications in Attacking RSA Variants, Ellen Jochemsz and Alexander May, Asiacrypt 2006]

また、離散対数問題の解法に関しても研究が活発化してきている。実質的な脅威をもたらすにはいたっていないが、その効率的な解析方法に関する研究は進んでおり、以後の動向に注意が必要である。[An Algorithm to Solve the Discrete Logarithm Problem with the Number Field Sieve, An Commeine and Igor Semaev, PKC 2006], [Cryptanalysis of an Efficient Proof of Knowledge of Discrete Logarithm, Sébastien Kunz-Jacques, Gwenaëlle Martinet, Guillaume Poupard and Jacques Stern, PKC 2006]

その他、近年活発化している動きとしては、ID ベースを利用した各種効率のよいアルゴリズム・プロトコルや Lattice を用いた解析などが挙げられる。欧米では、電子投票に関する研究なども注目されているようであり、 CRYPTO 2006 の Invited Talk の一つにもなっていた。[Receipt-Free Universally-Verifiable Voting With Everlasting Privacy, Tal Moran and Moni Naor, CRYPTO 2006], [Defeating Malicious Servers in a Blind Signatures Based Voting System, Sebastien Canard, Matthieu Gaud and Jacques Traore, FC06], [Cryptographic Protocols for Electronic Voting, David Wagner, CRYPTO 2006 Invited talk]

安全性証明のモデルに関しては、従来よく用いられていたランダムオラクルモデルを離れる動きがあり、より現実に即したモデルの模索が活発化している。一例では、フォーマルメソッドの概念とを融合したモデルの検討[Automated Security Proofs with Sequences of Games, Bruno Blanchet and David Pointcheval, CRYPTO 2006]や複数のアルゴリズムが混在するようなプロトコルの安全性証明等に有効と考えられる ユニバーサルコンポーザブルモデル(Universal Composable Model)に関して、従来提案されているモデルからより使いやすいモデルや現実に即したモデルへのアプローチに関する研究も進んできている。また、近年取上げられ始めている危殆化等の概念等を加味したモデルの検討なども発表された。

[Generalized Environmental Security from Number Theoretic Assumptions, Tal Malkin, Ryan Moriart and Nikolai Yakovenko, TCC 2006], [Universally Composable Security with Global Setup, Ran Canetti, Yevgeniy Dodis, Rafael Pass and Shabsi Walfish, TCC 2007], [Long-term Security and Universal Composability, Jörn Müller-Quade and Dominique Unruh, TCC 2007]

2.4. 委員会開催記録

平成 18 年度、暗号技術監視委員会は、表 2.12 の通り 2 回開催された。暗号技術調査ワーキンググループは、表 2.13 の通り計 6 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 18 年 7 月 24 日	活動方針確認、監視状況報告
第 2 回	平成 19 年 3 月 9 日	監視状況報告、CRYPTRYC report 2006 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の開催

回	年月日	議題
第 1 回	平成 18 年 8 月 4 日	第 1 回公開鍵暗号 WG（活動方針の審議）
第 2 回	平成 18 年 9 月 7 日	第 2 回公開鍵暗号 WG（活動内容の審議）
第 3 回	平成 18 年 12 月 27 日	第 3 回公開鍵暗号 WG（中間報告の審議）
第 4 回	平成 19 年 2 月 5 日	第 4 回公開鍵暗号 WG（最終報告の審議）
第 5 回	平成 19 年 2 月 5 日	第 5 回公開鍵暗号 WG（同上）
第 6 回	平成 19 年 3 月 7 日	第 6 回公開鍵暗号 WG（CRYPTREC report 2006 審議）

第3章　暗号技術調査ワーキンググループ

3.1　公開鍵暗号ワーキンググループ

3.1.1　調査背景とその意義

数論的問題の困難性に関する評価については、電子政府推奨暗号リストの作成 (付録 5) に向けて、数論的問題の困難性に依存して暗号プリミティブの安全性を主張する暗号スキームを横断的に評価した際、2002 年度までに CRYPTREC Report 2002[C02] にまとめられた。その他に、電子政府推奨暗号リストの作成と並行して CRYPTREC が実施した素因数分解実験プロジェクトによって 2003 年度までに調査・研究された内容については、CRYPTREC Report 2003[C03, 3.3 節] にまとめられ、実験データから合成数のサイズが 1024 ビットの一般数体ふるい法に必要な計算量見積もりについて予測がなされている。また、同年度には、一般数体ふるい法を効率的に行うための計算機のアーキテクチャである TWIRL の実現可能性についても調査を行ってきている [C03, 3.1 節]。

以上の調査・研究を踏まえ、CRYPTREC では、当面の間、1024 ビット以上の IFP（n=pq 型素因数分解問題）の安全性には問題がないものと判断してきた。しかしながら、電子政府推奨暗号リストの作成から既に約 4 年経ち、当時の評価が現在も有効かどうかを含めて再評価を行う必要性が高まってきている。

EU においては、ECRYPT が年次報告書（ECRYPT Yearly Report on Algorithms and Keysizes）[E05, E06, E07] の中で、表 3.1 を提供し、各暗号技術におけるパラメータの比較を示している。特に、米国においては、NIST が SP 800-57, Recommendation on Key Management, Part 1[BBB+06] の中で、表 3.2 を提供しており、2010 年までは IFP（n=pq 型素因数分解問題）において 1024 ビット以上の法サイズの使用を推奨しているが、それ以降は 2048 ビットを推奨している。

本ワーキンググループでは、電子政府関連システムに限らず、暗号技術を利用したシステムに関する業務に就いている方々に、安全なパラメータサイズを含めて公開鍵暗号技術の安全な利用方法について情報を提供する必要があると考えている。なお、調査結果の概要は、第 2 章を参照のこと。

3.1.2　活動目的

本ワーキンググループでは、数論的問題（素因数分解問題や有限体及び楕円曲線上の離散対数問題）の困難性について調査・検討を行い、公開鍵暗号の鍵生成に関するセキュリ

表 3.1: [E06, E07, p.26,Table 7.2: Key-size Equivalence.]

Security(bits)	RSA	DLOG		ECC
		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

表 3.2: [BBB+06, p.66,Table 4: Recommended algorithms and minimum key sizes]

Algorithm security lifetime	Symmetric key algothrims (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

ティパラメータ選択及び鍵長に関する利用期限に関するガイドラインを作成することを目的としている。また、電子政府推奨暗号リストに記載されている公開鍵暗号技術に関する仕様書の改訂等について調査・検討を行い、各仕様書の変更点の洗い出しをすることを目的としている。なお、NIST の FIPS186-3(ドラフト版) と FIPS186-2 との差異については、今年度調査を行ったが（付録 2)、数論的問題の困難性についての調査・検討に注力したため、電子政府推奨暗号リストに記載されている公開鍵暗号技術に関する仕様書の改訂等 (NIST や ANSI における見直しに伴うもの) の詳細な調査・検討は、次年度に実施することとした。

3.1.3 委員構成

主　査：太田　和夫　　国立大学法人電気通信大学

委　員：青木　和麻呂　日本電信電話株式会社

委　員：内山　成憲　　公立大学法人首都大学東京

委　員：下山　武司　　株式会社富士通研究所

委　員：洲崎　誠一　　株式会社日立製作所

委　員：松本　勉　　国立大学法人横浜国立大学

委　員：渡辺　創　　独立行政法人産業技術総合研究所

3.1.4 素因数分解問題の計算量の見積 (ソフトウェアの場合)

3.1.4.1 目的

素因数分解問題の解法についてはおよそ 400 ビット程度以上について現在のところ一般数体ふるい法の利用が最も効率的である[1] 。合成数 N の分解計算量は

$$L_N[1/3, (\frac{64}{9})^{1/3} + o(1)] \tag{3.1}$$

と評価されている[2] 。ここで $o(1)$ は $N \to \infty$ のとき 0 に近付く関数である。具体的に $\log_2 N = 1024$ の時にどの程度の値になるのかは有効な見積りが出来ておらず、また、そもそもの式 (3.1) の見積りは平均計算量の上限であり、現実の計算量はさらに低い可能性もある。このようなことから具体的な N に対し一般数体ふるい法の計算量を見積もることは困難で、これまでに様々な仮定により見積りが行なわれてきた。

一般数体ふるい法の困難さを見積もるには

1. PC 上のソフトウエアを利用する方法

[1] [C93] により $L_N[1/3, \left(\frac{1}{3}(92 + 26\sqrt{13})\right)^{1/3} + o(1)]$ となる改良法も知られているが、数千ビット以上にならないと通常の方式より高速にならないと信じられているので本稿では考察対象外とする。

[2] $L_N[s, c] = \exp(c(\log N)^s(\log\log N)^{1-s})$

2. 専用ハードウェアを利用する方法

3. (現時点では実現可能かどうか不明な) 数百 qubit 以上の量子計算機を利用する方法

があり得るが、本節では 1 のみを対象とする。

3.1.4.2 評価手順

先に述べたように、一般数体ふるい法の計算量の評価は非常に困難である。暗号技術の安全利用のためには、計算量の下限、つまり下からの評価が重要である。しかし、これは非常に困難を伴うので、今回は実際にどれくらいの計算量を要するかを実際にソフトウェア実装・実行した結果から推測し、上からの評価を行なった。また、一般数体ふるい法においては主要な計算として

- ふるい
- 線形代数

があるが、今回は評価の時間的制約、また線形代数の実行時間の見積りの困難性を考えてふるいのみの評価とした。一般数体ふるい法により分解された合成数の世界記録の更新において、これまでのところふるいの方が線形代数より多くの時間を要していること、漸近的な実行時間の評価でもふるいと線形代数は同じオーダーであることからそれほど乱暴な見積りではないと考えられる。

実際のソフトウェアの実装実験による評価においてはふるい領域の一部をサンプルで選び、その範囲のふるい処理を実際に行なうことにより全体のふるい処理時間の推測を行なった。このような見積り計算量の削減を行なったとしても、1024 ビット以上の合成数に対し有意な結果を得るためには非常に大量の計算コストを要することから今回は評価対象を 1536 ビットと 2048 ビットのみに絞った。具体的な 1536 ビットと 2048 ビットの数は RSA factoring challenge numbers[3] から選んだ。

3.1.4.3 評価結果

今回の評価の基準となる PC は Athlon 64 2.2GHz とした。現状の素因数分解の世界記録を目指すにはコストパフォーマンスが非常によい PC である。

実際の 1536 ビットおよび 2048 ビットの結果については現在の素因数分解世界記録の保持者の一人である Kleinjung 博士に評価依頼した [K07a, K07b]。本稿では、ほぼ同様の手順で評価された 1024 ビットの結果 [K06] も合わせて利用した。

図 3.1 及び表 3.3 に今回の評価結果を示す。「[K07] (upper bound)」は実際にふるい処理を行なった結果からの推測である。なお、推測に当たってはふるいの部分的適用だけでも

[3] http://www.rsasecurity.com/rsalabs/node.asp?id=2093

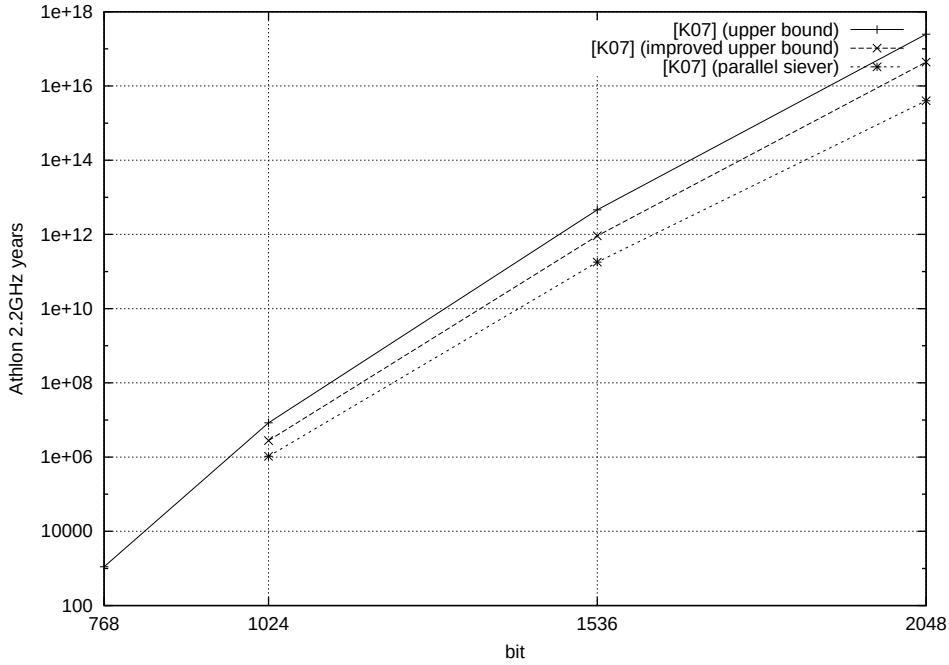


図 3.1: 評価結果

表 3.3: 評価結果

# of bits	768	1024	1536	2048
[K07] (upper bound)	1108	$8.4 \cdot 10^6$	$4.6 \cdot 10^{12}$	$25 \cdot 10^{16}$
[K07] (improved upper bound)	—	$2.8 \cdot 10^6$	$0.92 \cdot 10^{12}$	$4.4 \cdot 10^{16}$
[K07] (parallel siever)	—	$1.05 \cdot 10^6$	$0.18 \cdot 10^{12}$	$0.4 \cdot 10^{16}$

相当の時間がかかることから、いわゆる cofactoring 対象の合成数の分布に対し Dickman ρ を用いた smooth となる確率から求めた。さらに実際の実装プログラムの制約上、必ずしも optimal と思われないパラメータを選んでいる。また、部分結果からふるい処理全体への推測の導出に当たっては非常に保守的なパラメータ設定を行なっている。特に利用メモリ量については 1536 ビットについては 60TB、2048 ビットでは 6PB の実メモリ利用が期待されるが、推測に用いた計算機の制約から 2GB での推測となっている。「[K07] (improved upper bound)」は、「[K07] (upper bound)」を元にしたふるいプログラムや実装実験時間の制約がそれほどなかったとした場合の見積りである。但し、仮定の積み重ねであるので読み取りには注意が必要である。「[K07] (parallel siever)」は「[K07] (improved upper bound)」からさらにメモリ量の制限を取り除くため並列ふるいが理想的に実装されたと仮定された場合の見積りである。詳細については [K07a] を参照のこと。

3.1.4.4 これまでの評価

[LV01] は下からの評価である。一方 [Br00] ではこれまでの世界記録の更新が桁数の三乗根に比例するという仮説であり、ある意味、上からの評価と考えられる。但し、「年」を計算量に換算するのは困難なので、そのまま図 3.2 に引用する。

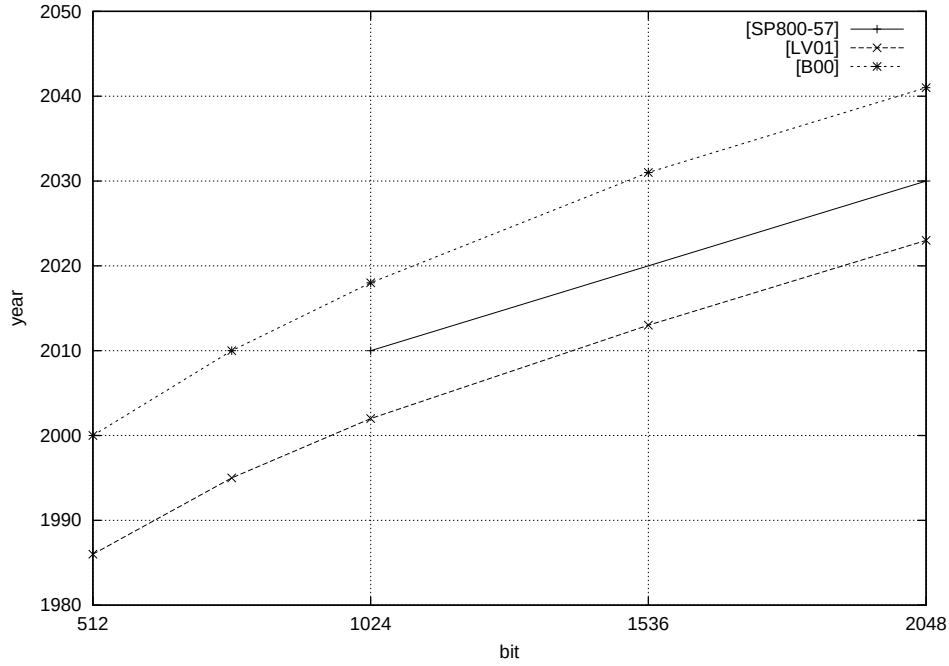


図 3.2: これまでの評価

3.1.4.5 コメント、注意点

先に述べたように一般数体ふるい法の正確な計算量評価は非常に難しい。以下に注意点及び関連情報を述べる。

1. 今回の評価はふるいのみである。これまでに行なわれた一般数体ふるい法による素因数分解ではふるい処理が支配的であったが、ビット数が増えるに従って線形代数処理の方が支配的になるとの意見もある [S00]。実際、線形代数処理は並列処理が自明ではなく、通信コストが膨大になる可能性もある。

2. 今回の評価では 2GB 程度の RAM 利用しか考えていない。単純に理論評価式から得られる最適と考えられる量の RAM は 1536 ビット分解の場合に 60TB、また 2048 ビット分解の場合に 6PB と先に述べたが、そのように巨大な RAM を準備することが未来においても費用対効果にあっているかどうかは不明である。また、そのように巨大な RAM が 2GB RAM と同じ性能で利用可能かどうかも重要な考慮点である。

3. 参考までに共通鍵暗号の全数探索性能について distributed.net が行なっている Project RC5(-72) を利用した結果を報告する。この Project RC5 は RSA 社が主催する secret-key challenge の一つである RC5-72 の鍵の全数探索プロジェクトである。この全数探索を行なうソフトウェアはその目的のため高度に最適化されており、PC の共通鍵暗号の全数探索性能を評価する上で相応しいと考えられる。実際に `dnetc v2.9011-496-CPR-05060815 for FreeBSD (FreeBSD 5.4-RELEASE)`」というバージョンでいくつかのパラメータを試したところ `dnetc -bench rc5 1` が最も速く、8,803,527 keys/sec という性能が観測された。

4. 今回、ソフトウェアでの計算量評価を主眼に置いて評価した。共通鍵暗号の全数探索の費用対効果については、FPGA 実装ではソフトウェア実装に比べて 8〜9 ビットも違うとの報告がある [KPP+06]。一般数体ふるい法においてもこのような差が出るのかどうかは明らかではない。

3.1.4.6 まとめ (ソフトウェアの場合)

今回、Athlon 2.2GHz (2GB RAM)・年という限られた評価ではあるが、従来よりも精密な評価が出来た。暗号安全性の評価に当たっては最終的には結局コスト (費用) で計るべきであるが、非常に困難である。そもそもの数体ふるい法の計算量評価が難しい上に、将来にどのような計算資源がどれくらいのコストで利用可能かが不明であることから非常に困難である。本稿のデータは様々な仮定の元で導出されたものであるので仮定が省かれて使われることのないよう十分な注意を持って使って欲しい。

A ふるい実行時間内訳

[K07b] によるとふるい実行時間の内訳は次の通りである。

# of bits	sc	sieve	td	cof
768	16%	47%	14%	21%
1024	16%	43%	12%	28%
1536	10%	31%	10%	47%
2048	9%	23%	4%	63%

sc coordinate transformation to special-q lattice and computation of the two auxiliary vectors

sieve addition of log p to memory

td evaluation of polynomial values, trial division and pseudoprime tests

cof cofactorization

B 多項式とパラメータ

[K07b] によると 768 ビット及び 1024 ビット分解のふるい時間の推測に用いたパラメータは次の通りである。

B.1 RSA-768

$$
\begin{aligned}
&265482057982680 && x^6\\
&+ 1276509360768321888 && x^5\\
&- 5006815697800138351796828 && x^4\\
&- 464778544717278542717726774 50 && x^3\\
&+ 652543726193598939710966737189 4785 && x^2\\
&- 181857793520885943567260188624348 03054 && x\\
&- 277565266791543881995216199713801103343120
\end{aligned}
$$

$$
\begin{aligned}
&34661003550492501851445829 && y\\
&- 129118745658002122316354779157481 0881
\end{aligned}
$$

side	factor base bound	large prime bound
algebraic	1100000000	2^{37}
rational	200000000	2^{37}

B.2 RSA-1024

$$
\begin{aligned}
&1000000001002023904806000 && x^6\\
&+ 269697895236768163056606416340 && x^5\\
&- 621283881860852419610022789684474 7498 && x^4\\
&- 847105251394275537650757048185246 2668136 && x^3\\
&+ 738608916851310255504408252889378679701231117 95 && x^2\\
&+ 103239504258459269088961583772414261637624065053206 && x\\
&- 113943198561639198776937620503643872967091171901277555912
\end{aligned}
$$

$$
\begin{aligned}
&5146620559617247177525524125973348 61 && y\\
&- 226511983014638262784476372319943180970205534545
\end{aligned}
$$

side	factor base bound	large prime bound
algebraic	1150000000	2^{42}
rational	250000000	2^{42}

3.1.5 素因数分解問題の計算量の見積 (ハードウェアの場合)

3.1.5.1 まえがき

巨大な合成数に対する素因数分解問題は、RSA 暗号・RSA 署名等公開鍵の安全性の根拠となっており、近年の情報セキュリティにおける大きなトピックの一つになっている。数

体ふるい法 (Number Field Sieve、NFS) は、RSA 暗号・署名の鍵として用いられる一般的な形の合成数を分解する方法として、現在知られている最も効率的な方法であり、2007 年 3 月現在の一般数体ふるい法に基づく素因数分解最高記録は 200 桁 である。

これらの従来結果は、数多くの PC 上でソフトウェアプログラムを数ヵ月間駆動することにより得られたものである。現在の記録、ならびにこれまでの記録の伸びから考えて、公開鍵暗号として一般にもちいられる 1024 ビット (308 桁) の RSA 暗号・RSA 署名は、当分の間安全と信じられてはいるものの、このような予想も、上記 PC 上のソフトウェア環境を仮定したものである。

その一方で、最近になって、素因数分解を専用ハードウェアを用いて実現しようとする提案が、アルゴリズムレベルであるが、いくつか見られるようになっており、専用ハードウェアを用いた場合の素因数分解能力について議論されるようになりつつある。

数体ふるい法は、以下の 4 種類の処理、

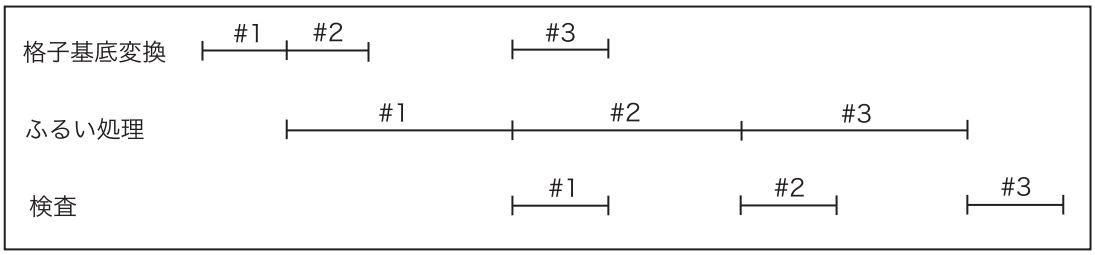
1. 多項式探索ステップ、
2. 関係式抽出ステップ、
3. 線形代数ステップ、
4. 平方根ステップ

で構成されている。これらの処理のうち、線形代数ステップならびに、関係式抽出ステップ、更にその中でもふるい処理と呼ばれる部分が、数体ふるい法の処理全体において、多くの時間を占めることが、理論的にも経験的にも分かっている。よって、数体ふるい法を効率化しようとした場合、これらのステップを効率化すべきであり、ハードウェアアルゴリズムを構築する最にも、これらから考察するのは、自然な考え方である。

2001 年 Bernstein らは、データソーティングアルゴリズムをベースとして線形代数を解く ASIC による専用ハードウェアを提案している。Lenstra らは、このアルゴリズムを改良し、ASIC 上のデータルーティングアルゴリズムをベースとした線形代数解法アルゴリズムを提案している。2003 年、2004 年には、Geiselmann 及び Steinwandt らにより、これらのアルゴリズムをふるい装置に当てはめた方式が提案されている。その一方で、時間は遡るが、1999 年には、Shamir と Tromer らにより、光子送信受信装置を用いてふるい処理を行なうハードウェア装置 TWINKLE を提案し、さらに Shamir らは光子送受信装置から ASIC によるデザインに置き換えたふるい処理専用ハードウェア装置 TWIRL を提案している。また、2005 年には Franke らは、同じく ASIC 実装ではあるが、より実現性を高める為に Butterfly ソートを利用した関係式抽出装置 SHARK を提案している。なお本装置の特徴としては、関係式検査部、特にミニ素因数分解 (楕円曲線法) もデバイス内のコプロセッサで行なうことを想定している点にある。

ただし、これら素因数分解専用ハードウェア装置の提案はあくまで理論的なものであり、現時点ではこれらの装置が実現されたという報告は聞かれない。その理由の一つとして挙

図 3.3: 全体処理



げられるのが、ハードウェアの設計ならびに開発にかかる費用の問題である。従来提案されている素因数分解ハードウェアの論文の多くは、専用ハードウェアのコスト算出方法として、ウェハ一枚の価格 (数千円〜数万円) を回路規模から予想される実装面積 (ウェハの 1/3 等) で割った値×必要チップ数 (数千個) という、単純な算出方法に基づいており、必然的に実現するためのコストを過小評価する文献が多い。また装置の動作周波数は、提案者の言い値であり、例えば TWIRL の場合には 1GHz と記載されてはいるものの、その数値に理論的根拠や証拠に基づく保証があるわけではない。

それでは一体、現実的には、どのようなシステムが動作可能であり、その処理能力はどれぐらいなのか、さらに将来的には素因数分解問題を根拠とした暗号に対してどれぐらい脅威になり得るのか、という点について回答となるべき指針が、現時点で我々が知る限りにおいては存在しない。このようにハードウェアによる安全性に対する脅威が未知のままであるという状態が続くのは好ましくなく、ハードウェアによる素因数分解装置の将来性を計ることが必須であると考えられる。これらに対し正しい評価を与えるためには、「動作可能」な素因数分解ハードウェア装置を実際に設計、製作し、動作させた上で、その処理能力を評価すべきであると結論づけた。

本文書の目的は、素因数分解の処理性能に関し、動作可能なハードウェアとして設計、製造されたシステムを元に、その処理性能を計測し、ソフトウェアの性能と比較することで、その将来性について議論することを目標とする。ハードウェア装置としては、NICT による委託研究に基づき富士通株式会社によって開発された素因数分解ハードウェア装置 (ふるい処理装置) を利用して評価することとする。

なお、本来であれば、処理性能をコストで評価するべきかもしれないが、ハードウェアについては、量産効果やまた将来的な評価を行なうことが非常に困難であることから、今回の報告ではコストに関する評価は行なわないこととした。

3.1.5.2　開発された専用ハードウェア装置の概略

以下に本装置の概略を表 3.4 に示す。

本装置は机上アルゴリズムやシミュレーションではなく、FPGA 上に実装され現実に動

図 3.4: ふるい処理内訳

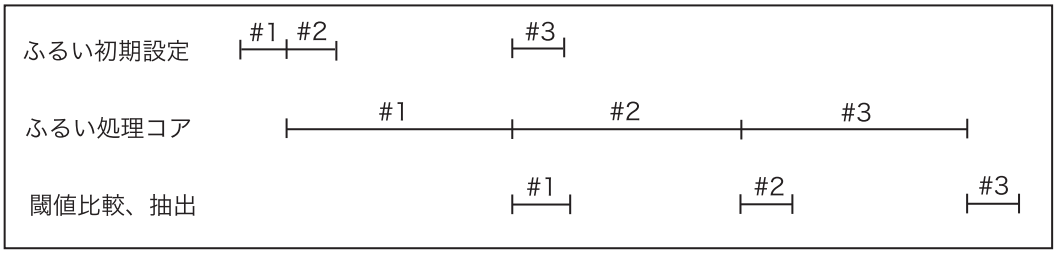
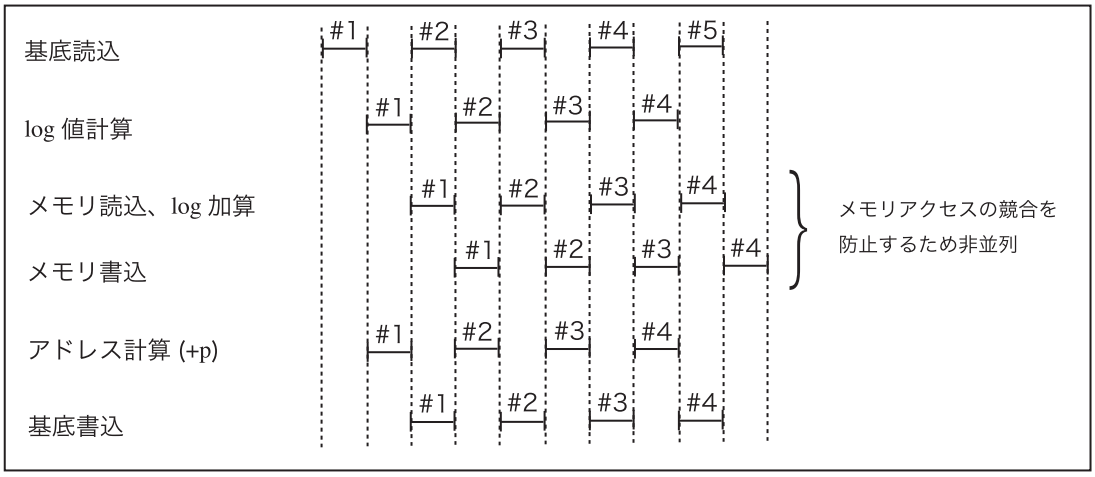


図 3.5: ふるい処理コア内訳



作することを最優先として実装されている。ハードウェア開発プロジェクトは、ハードウェア要件抽出目的で実施された 2 年間の間に実装された 2 種類の実装実験を経ており、今回の装置は、それを踏まえた上で今回の装置については、アルゴリズム設計から実装までに要した期間は 10ヵ月である。

今回開発した装置の動作周波数は、論理合成ツール上でタイミングエラーが発生しないという条件の元でマッピングされた値であり、限られた開発期間において導かれた中では最良 (最大) の値である。ただし、本値は、論理回路だけでなく FPGA の型番にも依存して容易に変わり得る値であり、実装次第では事実、2005 年度に開発した装置では、ふるい装

表 3.4: 開発された装置の概略

アルゴリズム	Lattice Sieve
最大 factor base	algebraic 2^{30}, rational 2^{28}
FPGA	Xilinx Virtex 4 (XC4VLX200-10FF1513C) × 3 個
動作周波数	91 MHz
ふるい処理並列数	8

置 (line sieve) の処理動作周波数として 133 MHz を実現している。また用いた数々の実装パラメータ、数体ふるいパラメータは、出来る限りの性能向上を目指し最適化を図ってはいるものの、本ハードウェア装置にとって、理論的な最適値を用いているわけではない。

全体処理の流れとしては以下のとおりである。

1. 格子基底計算
2. ふるい処理
3. 関係式検査

本装置ではハードウェア化の特徴であるパイプライン処理による並列化を多段に実装することで、本質的に必要な演算時間がふるい処理のみとなるように設計されている（図 3.3 参照）。このふるい処理は次の機能の組み合わせで実現されている。

1. ふるい初期設定
2. ふるい処理コア
3. 閾値比較・抽出

同様にふるい処理内部に於いても、多くの機能はパイプライン化することが可能であり、ふるい処理コア部が本質的な時間を占めることとなる（図 3.4）。ふるい処理コア部は、以下の 6 種類の操作の繰り返しとして表される。

1. 格子基底の読込み
2. log 値計算
3. メモリ読出・log 加算
4. メモリ書込み
5. アドレス加算 (address + p)
6. 格子基底書込み

ほとんどの処理はパイプライン化することで、実質的に 1clock で処理できるが、メモリ読出 (3) から書込 (4) までの一連の作業についてはメモリへの競合を防ぐ観点からパイプライン化が容易ではないと判断された。このことから今回開発された装置では、(3) と (4) の処理は並列化せず逐次処理として実現し、これら二つの処理時間の合計である 2clock を処理全体の 1 単位として費すこととされている。

ふるい処理	ふるい初期設定	全体	メモリ容量× 1clock
	ふるい処理コア	メモリクリア	1clock
		パラメータ設定	1clock
		全体	メモリアクセス回数× 2clock
	閾値比較・抽出	格子基底の読込	1clock
		log 値計算	1clock
		メモリ読出・log 加算	1clock
		メモリへの書込	1clock
		アドレス加算 (+p)	1clock
		格子基底書込	1clock
		全体	メモリ容量× 1clock
		閾値比較	1clock
		関係式候補抽出	1clock

以上の実装により、本システムによる演算処理時間は、本質的にメモリアクセス回数 (log 加算回数) のみに依存して決まり、その他の処理時間は、並列処理により隠れて見えなくなる。

3.1.5.3 ソフトウェアとの比較評価

本章では、前章に記載した専用ハードウェアとソフトウェアによる実装との処理性能を比較について述べる。ふるい処理を行なう最に入力するパラメータ、factor base bound B_r, B_a、ならびに threshold 値を固定して考える。このパラメータによって実施されるふるい結果の共通項として抽出される要素の個数、ならびにふるい処理が終了するまでに実施する log 加算の延べ回数はふるい処理を実施する装置 (専用ハードウェア、PC 上のソフトウェア) にかかわらず一定である。このことを利用して、ハードウェアおよびソフトウェアの処理能力の比較を行なう。

ソフトウェアの処理能力について　ソフトウェアによる処理時間を掲載する。根拠とするデータとしては、節 3.1.4 のものを利用する。評価対象となる計算機の CPU は AMD Athlon 64, 2.2 GHz であると記載されている。また、ふるい領域は $(2^{16}, 2^{15})$ であるとされている。

# of bits	1024	1536	2048
rational FB	$2.5 \cdot 10^8$	$2.5 \cdot 10^8$	$2.5 \cdot 10^8$
algebraic FB	$1.15 \cdot 10^9$	$1.15 \cdot 10^9$	$1.15 \cdot 10^9$
#sp-Q	$1.95 \cdot 10^{12}$	$69.4 \cdot 10^{16}$	$315 \cdot 10^{20}$
sieve ratio	43%	31%	23%
sec per sp-Q	135	207.8	245
Athlon 2.2GHz years	$8.4 \cdot 10^6$	$4.6 \cdot 10^{12}$	$25 \cdot 10^{16}$

専用ハードウェアの処理能力について　ふるい処理以外の処理はふるい処理を行なっている最中に並行して実施されるので、処理時間は全てふるい処理を実施する時間と考えてよ

い。1024、1536、2048 の各々について、用いている factor base のサイズは共通である。ふるい処理は各々 2 cycle で実施され、またふるい処理全体が 8 並列組み込まれていることから、1 個の sp-Q の処理にかかる時間は以下の通りに計算される。

$$(2^{16} \cdot 2^{15} \cdot (M(1.15 \cdot 10^9) + M(2.5 \cdot 10^8)) \cdot 2)/(8 \cdot 91 \cdot 10^6) = 23.532 \text{ sec}$$

ただし $M(x) = \sum_{7<p\leq x} 1/p \approx loglog(x) - 0.9146932$ である。なお今回のハードウェアでは 7 以下の素数に対するふるいは行なっていない。上記値からふるい処理 (log 加算) のみで比較した場合は以下の通り。

	1024	1536	2048
times	2.46	2.73	2.39

さらに、処理全体の性能差を求めると以下の通りである。

	1024	1536	2048
times	5.73	8.83	10.41

3.1.5.4　コメント、注意点

専用ハードウェアの設計時点においては装置への 768 ビット を越える合成数に対するパラメータの入力は設定されておらず、実際 1024 ビット 以上の合成数に対する処理が可能かどうかは本稿執筆時点では分かっていない。特に、今回専用ハードでは、試し割算部やミニ素因数分解部の処理時間がふるい処理 (log 加算) に隠れることを期待しているが、試し割りやミニ素因数分解部の処理時間は、対象となる多倍長整数の大きさに強く依存していることから、実際にふるい処理に隠れるような実装が可能かどうかは現時点では未確認である。また、PC と 専用ハードでは、装置に内蔵されている RAM 容量等が全く異なっており、用いたパラメータ一つ取っても、両システムにとって公平なものであるとは限らない。

3.1.5.5　まとめ (ハードウェアの場合)

今回、素因数分解専用ハードウェアによる評価をソフトウェアとの比較という観点で実施し、ふるい処理単独の比較で約 2 倍、さらに全体処理では差がより拡大することが示された。今回の評価では、実際に動作可能なハードウェアの処理性能が元になっておりその意味で言えば、専用ハードウエアの処理能力の下限が示されたことを意味する。

今回の評価に用いた素因数分解専用ハードウェア装置は、短期間で設計、開発を完了させ、動作させることを最優先して設計実装されることが目標とされた為、多くの箇所で未だ改良の余地が残っている。性能に直接結び付く主な改良点としては次の 2 点。

(1) 動作周波数の向上

(2) 並列回路数の向上

(1)、(2) それぞれについて、2005 年度において線形ふるいアルゴリズムを実装した際に、133MHz、32 並列を実現させた実績があり、格子ふるいでも今後の改良次第では達成可能である可能性がある。

今後においても、ハードウェアの処理性能はより向上することが見込まれると、ソフトウェアとの処理性能の比はより広がることが予想される。ただし、ハードウェアがソフトウェアに比べて、対費用効果が、共通鍵暗号の全数探索について [KPP+06] で指摘されている 8〜9 ビットほど違うということが、素因数分解に関してもいえるかどうかについては, 現時点では明らかではない.

3.1.6 有限体及び楕円曲線上の離散対数問題の計算量の見積もり

本節では、暗号技術の基礎となる数学的なアルゴリズムが持つ困難性、特に有限体上の離散対数問題及び有限体上の楕円曲線上の離散対数問題の困難性について、最近の研究について調査した結果について報告する。

3.1.6.1 有限体上の離散対数問題

有限体上の離散対数問題（DLP）に対する、現在までのところ漸近的に最高速なアルゴリズムは、数体ふるい法（NFS）であり、これは素因数分解問題（IFP）に対するアルゴリズムとしても漸近的に最高速である。本節では、素体 $\mathbb{F}_p$ 上の DLP のみについて考える。$\mathbb{F}_p$ 上の DLP に対する数体ふるい法の計算量は準指数時間と呼ばれ

$$L_p[1/3, (64/9)^{1/3}]$$

で表される。サイズが同じ合成数に対する IFP の計算量も同じである。p が特殊な形の場合に適用できる NFS を SNFS、一般の場合を GNFS と呼ぶ。

3.1.6.2 有限素体上の離散対数問題の数値実験

ここでは、有限素体上の DLP の数値実験について述べる. 有限素体上の DLP の数値実験は、IFP の数値実験ほど注目されておらず、数も多くはないがいくつか報告されている [JL99, LC]. 特殊な形ではない素数を標数とする有限素体上の DLP の年代ごとの桁数の記録を、以下の表 3.1.6.2 に IFP と並べてまとめる. 但し、DLP には、GNFS ではなく Gaussian Integer Method と呼ばれる手法を使ったものも含まれており（以下の表 3.1.6.2 では、* を記している）、IFP には MPQS（複数多項式 2 次ふるい）と呼ばれるものの記録も含まれる（以下の表では、 + を記している）.

年	DLP	IFP
1990		116+
1991	58*	
1992		
1993		120+
1994		129+
1995	65	
1996	85*	130
1997		
1998	90	
1999	100	155
2000		
2001	120	
2002		158
2003		174
2004		
2005	130	200
2006		
2007	160	

3.1.6.3　公開鍵暗号への安全な鍵サイズ

NFS を用いた攻撃に対する安全性についてのみ考えることにする．上記の表 3.1.6.2 のデータに基づき、[Br00] で与えられている IFP に対する予測と同様の式を求めると

$$Y = 9.89D^{1/3} + 1953.5$$

となる。ここで、D は p の桁数、Y はその桁数の DLP が解かれる西暦を表す。この結果から判ることは、同じ西暦年数での IFP との差が、現状では 50 桁程度となるが、DLP の数値実験例が IFP のそれと比べて少ないため単純な比較は難しい。実際、[Br00] の予測式は 1960 年代以降のデータに基づいているが、ここでの DLP に対する予測式は 1990 年代以降のみのものに基づいていることに注意しておく。漸近的な計算量評価に関しては、上述のように、IFP も DLP もオーダは同じであり、さらなる数値実験と実用的な改良 [**?**] などを考慮して、安全な鍵サイズについては、DLP に対するものも IFP に基づくものと同じ鍵サイズにしておく必要があると考えられる。公開鍵暗号に関する安全な鍵サイズの予測に関しては、[Br00] の他には [LV01] が代表的である．

3.1.6.4　有限体上の楕円曲線上の離散対数問題

有限体上の楕円曲線の有理点のなす有限アーベル群上の DLP（ECDLP）への解法アルゴリズム研究は 1990 年代に入って盛んになり、特殊な曲線に対しては準指数時間となるものや（確率的）多項式時間で動くアルゴリズムも提案されているが、一般的な曲線を選んだ場合は、Rho 法と呼ばれるものが最も有効である。ECDLP の入力サイズを k とすると、その計算量は $O(2^{k/2})$ となる。

3.1.6.5 楕円曲線上の離散対数問題の数値実験

ECDLP の数値実験については、カナダの Certicom 社による 1997 年に始まった ECC challenge が有名である。問題は大きく 2 つに分類され（Koblitz 曲線と呼ばれるものも含まれているので、それも含めると 3 つ、 定義体の標数が 2 の場合と奇素数の場合である. それぞれの問題（曲線と言っても良いが）は、ECC2-**、 ECC2K-** や ECCp-** などと記される. 但し、 ** にはビットサイズが入る.

以下の表 3.1.6.5 に、 現在までの ECC challenge の結果を抜き出しておく. 詳しくは Certicom の web ページを参照 [CT]。

年	ECC2	ECC2K	ECCp
1997	79		79
1998	97	95	97
1999			
2000		108	
2001			
2002			109
2003			
2004	109		

3.1.6.6 公開鍵暗号への安全な鍵サイズ

上述のように、一般的な楕円曲線を用いる限りは ECDLP に対する解法としては、Rho 法が最も有効である。現在のところ、高速実装による 256 ビット有限素体上の楕円加算 1 回の速度 [Be06] と、128 ビット AES の暗号化 1 回分の処理速度 [MF06] を比較すると、概算で、楕円加算の方が 6.5 倍程度遅くなると見積もられる（実際、楕円スカラー倍の速度が 832457 cycles（Pentium III）で、楕円の加算と倍算が同じ速度として、256 ビットの楕円加算 1 回は、$832457/(256 * 2) \approx 1626$ cycles。AES の暗号化 1 回は 251 cycles（Pentium 4）であり、その差は約 6.5 倍である。）ソフトウエア実装による攻撃と言う観点からは、共通鍵暗号の安全な鍵サイズの評価が ECDLP に基づく公開鍵暗号の安全な鍵サイズの評価には有効と考えられる。従って、現時点では 160 ビット程度であれば、十分安全であると考えられる. また、ハードウエア実装という観点からは、FPGA を用いた並列計算に基づく攻撃の研究も進められているが、160 ビットの鍵長を持てば今後 20 年間は十分安全であろうという報告がされている [KPP+06]。ECDLP に基づく公開鍵暗号の安全な鍵サイズの予測に関しても、上述の [LV01] が代表的である.

参考文献

[Br00] R. P. Brent, “Recent Progress and Prospects for Integer Factorisation Algorithms,” In D.-Z. Du, P. Eades, V. Estivill-Castro, X. Lin, and A. Sharma, editors, Computing and Combinatorics: 6th Annual International Conference, COCOON 2000, Volume 1858 of Lecture Notes in Computer Science, pp.3–22, Springer-Verlag, 2000.

[BBB+06] E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid, “Recommendation for Key Management – Part1: General (Revised),” U.S. Department of Commerce, National Institute of Standards and Technology, NIST Special Publication 800-57, March, 2007. Available at http://csrc.nist.gov/publications/nistpubs/index.html.

[Be06] D. Bernstein, “Curve25519: New Diffie-Hellman Speed Records,” Proc. of PKC 2006, Volume 3958 of Lecture Notes in Computer Science, pp.207–228, Springer-Verlag, 2006.

[CT] Web page for the Certicom ECC Challenge, http://www.certicom.com/index.php?action=ecc,ecc_challenge.

[C93] D. Coppersmith, “Modifications to the Number Field Sieve,” Journal of Cryptology, Vol. 6, No. 3, pp.169–180, Springer-Verlag, 1993.

[C02] Information-technology Promotion Agency, Japan and Telecommunications Advancement Organization of Japan, “CRYPTREC Report 2002,” Japanese version is available at http://www.cryptrec.jp/report.html.

[C03] Information-technology Promotion Agency, Japan and Telecommunications Advancement Organization of Japan, “CRYPTREC Report 2003,” Japanese version is available at http://www.cryptrec.jp/report.html.

[E05] IST-2002-507932, ECRYPT - European Network of Excellence in Cryptology, D.SPA.10, “ECRYPT Yearly Report on Algorithms and Keysizes (2004),” available at http://www.ecrypt.eu.org/documents.html.

[E06] IST-2002-507932, ECRYPT - European Network of Excellence in Cryptology, D.SPA.16, “ECRYPT Yearly Report on Algorithms and Keysizes (2005),” available at http://www.ecrypt.eu.org/documents.html.

[E07] IST-2002-507932, ECRYPT - European Network of Excellence in Cryptology, D.SPA.21, “ECRYPT Yearly Report on Algorithms and Keysizes (2006),” available at http://www.ecrypt.eu.org/documents.html.

[I04] 独立行政法人 情報処理推進機構, “将来の暗号技術に関する安全性要件調査”, 電子政府行政情報化事業 調査報告書, 2004 年 2 月, available at http://www.ipa.go.jp/security/fy15/reports/crypt_requirement/index.html.

[JL99] A. Joux and R. Lercier, “State-of-the-art in implementing algorithms for the (ordinary) discrete logarithms problem,” Talk at ECC 99 (Elliptic Curve Cryptography), November 1999, slides are available at http://www.cacr.math.uwaterloo.ca/conferences/1999/ecc99/slides.html.

[JL03] A. Joux and R. Lercier, “Improvement to the general number field sieve for the discrete logarithms in prime finite fields,” Math. Comp. 72, 242, pp.953–967, 2003.

[K06] T. Kleinjung, “Estimates for factoring 1024-bit integers,” Securing Cyberspace: Applications and Foundations of Cryptography and Computer Security, Workshop IV: Special purpose hardware for cryptography: Attacks and Applications, 2006, slides are available at http://www.ipam.ucla.edu/schedule.aspx?pc=scws4.

[K07a] T. Kleinjung, “Evaluation of Complexity of Mathematical Algorithms,” CRYPTREC technical report No.0601 in FY2006, 2007, available at http://www.cryptrec.jp/estimation.html.

[K07b] T. Kleinjung, “Questions and answers regarding [K07a],” 2007.

[KPP+06] S. Kumar, C. Paar, J. Pelzl, G. Pfeiffer, and M. Schimmler, “Breaking Ciphers with COPACOBANA - A Cost-Optimized Parallel Code Breaker,” In E. F. Brickell, editor, Cryptographic Hardware and Embedded Systems – CHES 2006, Volume 4249 of Lecture Notes in Computer Science, pp.101–118, Springer-Verlag, 2006, slides are available at http://www-mlab.jks.ynu.ac.jp/ches/Sandeep%20Kumar.pdf.

[LC] Web page for R. Lercier, http://medicis.polytechnique.fr/~lercier/.

[LV01] A. K. Lenstra and E. R. Verheul, “Selecting Cryptographic Key Sizes,” Journal of Cryptology, Vol.14, No.4, pp.255–293, Springer-Verlag, 2001, available at http://www.springerlink.com/content/6d8hb94aenemfm5g/fulltext.pdf. (The extended abstract was presented at PKC 2000, Volume 1751 of Lecture Notes in Computer Science, pp.446-465, Springer-Verlag, 2000).

[MF06] M. Matsui and S. Fukuda, “How to Maximize Software Performance of Symmetric Primitives on Pentium III and 4,” IEICE Trans. Fundamentals, Vol.E89-A, No.1, pp.2–10, IEICE, 2006.

[S00] R. D. Silverman, “A Cost-Based Security Analysis of Symmetric and Asymmetric Key Lengths (Revised November 2001),” RSA Laboratories Bulletin No.13, RSA Security Inc., April, 2000, available at http://www.rsasecurity.com/rsalabs/node.asp?id=2088.

[SIK07] 下山 武司, 伊豆 哲也, 小暮 淳, “数体篩法による素因数分解専用ハードウェア装置の開発および実験,” 2007 年 暗号と情報セキュリティシンポジウム (SCIS2007), 3A2-3, 2007.

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

1.1　公開鍵暗号技術

暗号名	DSA
関連情報	仕様 ・ANSI X9.30:1-1997, Public Key Cryptography for The Financial Services Industry: Part 1: The Digital Signature Algorithm (DSA) で規程されたもの。 ・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	ECDSA (Elliptic Curve Digital Signature Algorithm)
関連情報	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	富士通株式会社 電子政府推奨暗号 問合わせ窓口 E-MAIL：crypto-ml@ml.soft.fujitsu.com

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	仕様 ・ANSI X9.42-2001, 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。

暗号名	ECDH (Elliptic Curve Diffie-Hellman Scheme)
関連情報	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	富士通株式会社 電子政府推奨暗号 問合わせ窓口 E-MAIL：crypto-ml@ml.soft.fujitsu.com

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	〒239-0847 神奈川県横須賀市光の丘 1-1-609A 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 セキュリティプラットフォームグループ　主任研究員　神田雅透 TEL：046-859-2437, FAX：046-855-1533, E-MAIL：kanda@isl.ntt.co.jp

1.2　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/camellia/ 英文： http://info.isl.ntt.co.jp/camellia/
問い合わせ先	・〒239-0847 神奈川県横須賀市光の丘 1-1-609A 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 セキュリティプラットフォームグループ 主任研究員 神田雅透 TEL： 046-859-2437, FAX：046-855-1533, E-MAIL：kanda@isl.ntt.co.jp ・〒104-6212 東京都中央区晴海 1-8-12 ﾄﾘﾄﾝｽｸｴｱｵﾌｨｽﾀﾜｰ Z13 階 三菱電機株式会社 通信システム事業本部 NTT 事業部 NTT 第一部第一課 課長 富田文隆 TEL:03-6221-2634, FAX:03-6221-2771 E-MAIL: fumitaka.tomita@hq.melco.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>

1.3 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>

1.4 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

Finding SHA-1 Characteristics [Asiacrypt06]

Christophe De Cannière and Christian Rechberger

ベルギーカトリック大学ルーベン校の若手研究者 *Cannière* 氏らによる SHA-1 衝突発見段数の新記録達成の報告で、従来 1 ブロックの場合 80 段中 58 段短縮版で発見されていたのに対し、2 ブロック 64 段短縮版で発見に成功したというもの。今回の講演では非線形キャラクタリスティックという新概念の導入により衝突発見効率を向上させることで発見に成功したと報告している。この講演に対して、今回の最高論文賞が与えられた。この講演では Shamir 教授よりフルラウンドの場合の今後の展望について質問がなされたが、現在チャレンジ中でありまだ見通しが立っていない様子であった。

Forgery and Partial Key Recovery Attacks on HMAC and NMAC Using Hash Collisions [Asiacrypt06]

Scott Contini and Yiqun Lisa Yin

HMAC と NMAC は 1996 年にカリフォルニア大学サンディエゴ校の Bellare 氏により提案されていたメッセージ認証コードの方式で、特に HMAC は標準化され広く用いられている。この HMAC は MD4, MD5, SHA-1 などのハッシュ関数を内部関数として用いているが、近年王氏らによって発見された衝突発見法を利用することで HMAC の安全性も損なわれてしまうことが報告された。具体的な例として MD4 を用いた HMAC に対する攻撃が報告された。

Finding SHA-1 Characteristics [2nd NIST HW]

Christophe De Cannière and Christian Rechberger

SHA-1 の衝突発見段数を従来の 58 段から 64 段まで更新したもので、Non-Linear Characteristic なる概念を新規に使っている

Cryptanalysis of the Full HAVAL with 4 and 5 Passes [FSE06]

H.Yu, X.Wang, A.Yun and S.Park

Searching for Differential Paths in MD4 [FSE06]

M.Schläffer and E.Oswal

A Study of the MD5 Attacks [FSE06]

J.Black, M.Cochran and T.Highland

The Impact of Carries on the Complexity of Collision Attacks [FSE06]

F.Mendel and N.Pramstaller

Wang 氏らが提案した、ハッシュ関数 MD4, MD5, HAVAL に対する攻撃法の非公開の部分を解明し、実際に衝突の発見に成功したという発表が相次いた。ただし、現在までに発表されているのはMD5までである。なお今回発表された結果は従来の手法を単純に応用したものであり、従来よりも容易に衝突を発見する手法を提案したものではない。

Analysis of Step-Reduced SHA-256 [FSE06]

F.Mendel, N.Pramstaller, C.Rechberger and V.Rijmen

電子政府推奨暗号リストに掲載されているハッシュ関数 SHA-256 に対して Wang 氏らによるアタックを適用した最初の結果が報告された。現状まだ SHA-256 の安全性は脅かされていないものの、今後新しいテクニックを開発することにより急速に進展する可能性も否定できないとの見解を述べた。

Herding Hash Functions and the Nostradamus Attack [Eurocrypt06]

John Kelsey and Tadayoshi Kohno

NIST で暗号安全評価、標準化関連を担当している Kelsey 氏から、ハッシュ関数を用いて改竄検出をしている文書について、ノストラダムスアタックと呼ばれる改竄手法により改竄可能であるという講演がなされた。この改竄手法では、元の文書は隠しておき、出力ハッシュ値だけ公開しておくことを前提としており、後で文書を公開したときに同じ出力ハッシュ値を持つように文書を自由に改竄する手法である。この手法により 128 ビットハッシュ関数の場合で 2^{87} 回の演算で改竄が可能であるとしている。

VSH, an Efficient and Provable Collision-Resistant Hash Function [Eurocrypt06]

Scott Contini, Arjen K. Lenstra and Ron Steinfeld

Lenstra 氏らによる新しいハッシュ関数 VSH (Very Smooth Hash) の提案。VSH は従来までの経験則に基づく安全性しか持たないハッシュ関数と異なり、RSA 暗号と同様に数学的に解くことが難しいことが証明可能である。安全性が証明可能でありかつ実際的であるという特徴は従来に無い画期的なものであるが、SHA-1 の代替としては処理速度が 1GHz ペンティアム III で 1 Mbyte/s と遅く、現状理論的なものに留まっている。

Collision-resistant no more: Hash-and-sign paradigm revisited [PKC06]

Ilya Mironov

通常のハッシュ関数を用いたメッセージのハッシュ値を利用して署名を生成する方法は、ハッシュ関数の collision によって、安全性が損なわれる。この問題を解決方法として、最近 target-collision resistant hash function (従来から UOWHF : Universal One-way Hash Function として知られている) を用いた構成が注目されている。ところが UOWHF を用いる場合ビット長が長くなってしまうという問題点があった。本発表ではビット長を短く抑えつつ UOWHF を構成可能とする方法を提案した。

Higher Order Universal One-Way Hash Functions from the Subset Sum Assumption [PKC06]

Ron Steinfeld, Josef Pieprzyk and Huaxiong Wang

2004 年に Hong、Preneel、Lee 氏らにより、MD の構成を利用してセキュアに UOWHF を構成する為の security notion が提唱されている。本発表では Subset Sum Assumption に基づき構成した Subset Sum ハッシュ関数を提案し、本提案方式により、上記で示された安全性要件を満たす UOWHF が構成可能であることを示した。また、提案方式を用いての long-input を必要とする UOWHF のビット長の短縮化などへの適用例なども示した。

Constructing Secure Hash Functions by Enhancing Merkle- Damgard Construction [ACISP06]

Praveen Gauravarum, William Millan, Ed Dawson and Kapali Viswanathan

MD5 や SHA1 などもベースとしている MD(Merkle-Dangard)-structure を基本とした、新しいハッシュ関数の構成方法を提案。提案方式に対して、従来知られている攻撃手法を適用しその安全性評価を行った。提案方式は、3C と呼ばれるもので、MD5 や SHA-1 の構成に類似した構成で、付加的に各段の f 関数の出力を排他的論理和で足し合わせ、結果を最終出力の直前の G 関数の入力の一つとする方式となっている。また、改良版として 3C+も合わせて提案されている。3C との構成の違いは、f 関数の出力値をはじめの 2 段の出力を含むものと含まないものとの 2 種類セットし、両者共に最終出力の直前の G 関数の入力とするものである。3C の構成のメリットとしては従来よく用いられている MD5 や SHA-1 な

どからの構造的な変更点が少ない移行しやすい点を挙げている。

Forgery and Key Recovery Attacks on PMAC and Mitchell's TMAC Variant [ACISP06]

Changhoon Lee, Jongsung Kim, Jaechul Sung, Seokhie Hong and Sangjin Lee

MAC(メッセージダイジェスト；Message Authentication Code, 送信されたメッセージが改竄されていなことや本人が送信したものであることを確認するために使う。）に類するいくつかのバリエーションのうち、PMAC と TMAC に関する安全性解析を行なった結果を発表。PMA 及び TMAC についてその偽造可能性を指摘した。また、両方式に対して、Key Recovery 攻撃の適用可能性も指摘し、これら PMAC や TMAC は、他の MAC に類するバリエーションの方式に比べた優位性は見出せないと結論付けている。

Side Channel Attacks against HMACs based on Block-Cipher based Hash Functions [ACISP06]

Katsuyuki Okeya

ハッシュ関数を構成する圧縮関数にはいくつかの構成方法が提案されている。中でもブロック暗号をベースとして圧縮関数を構成する PGV 法と呼ばれる方式がある。本発表では、その PGV 法により構成できる圧縮関数に対するサイドチャネル攻撃への耐性についての解析結果を示した。具体的には中で使われるブロック暗号が理想的な場合には 12 種類の圧縮関数が衝突攻撃に対する耐性を有するとの従来の発表がある。ここではサイドチャネル攻撃の 1 種である DPA(差分電力解析；Differential Power anaysis)を用いてその 12 種類の圧縮関数の解析を行なった。結果、12 種類中 8 種類は攻撃が適用でき、中で用いられる秘密鍵を特定し、選択的偽造を行なうことができてしまう。また残り 4 種類のうち 3 種類についても DPA もしくはそれに類する攻撃が適用できてしまう場合があり、その場合は鍵の一部を特定することが出来てしまう。

Strengthening Digital Signatures via Randomized Hashing [CRYPTO06]

Shai Halevi and Hugo Krawczyk

SHA-1 などの脆弱性の解析が進む中、実際に SHA-1 が使われているシステムなどの中で、出来る限り小規模な変更で安全性を保ちたい、という要求に対する研究結果。Randomized hash と呼ばれる方式を提案。署名などの中で用いているハッシュ関数の部分を、SIGN(HASH(m))という構成から、SIGN(r| HASH(r|m))という構成に変えることにより、中で使われているハッシュ関数が、Collision-Resistance の性質を有さずとも署名の安全性は保てる、という結果を示した。提案方式は、ハッシュ関数部分はブラックボックスのまま、システムへの改変を施すことが可能な構成となっており、ハッシュ関数そのものを入れ替えるのに比べて比較的小さな負担の改善で済ませることが出来るとのこと。Target collision resistance 等の概念を提案し、提案方式の安全性証明も行なっている。

On the Impossibility of Efficiently Combining Collision Resistant Hash Functions [CRYPTO06]

Dan Boneh and Xavier Boyen

新たなハッシュ関数 H を、2 種類のハッシュ関数 H_a, H_b を用いて構成することを試みる場合に、いずれか一方が Collision-Resistance の性質を有すれば、全体の出力値も Collision-Resistance の性質を有するような構成方法に関する解析結果。最もシンプルな方式としては 2 種類のハッシュ関数 H_a, H_b の出力値をそのまま新たなハッシュ関数 H の出力値とする方法があるが、この場合出力値のサイズは、ハッシュ関数 H_a の出力値のサイズ + H_b の出力値のサイズ となってしまう。本発表では、より短い出力値でありながら、Collision-Resistance の性質を有するような新たなハッシュ関数 H を 2 種類のハッシュ関数 H_a と H_b から構成することは不可能であることを示した。

New Proofs for NMAC and HMAC: Security without Collision-Resistance [CRYPTO06]

Mihir Bellare

HMAC や NMAC が PRF(Pseudo Random Function ; 擬似乱数関数)としてみなせることを示す(証明する)為には、圧縮関数が PRF であることと、中で使われているハッシュ関数が Collision-Resisance であることが必要であるとされていた。本発表では、一つ目の条件 ; 圧縮関数が PRF である、のみが満たされていれば、HMAC や NMAC は PRF とみなすことが出来る、ということを示した。また、さらに条件を緩め、PRF でなくても計算量的に大よそ散らばっていれば、MAC としての機能は果たすことが出来る、事も示した。

Keynote Speech: "Message Modification, Neutral Bits and Boomerangs: From Which Round Should we Start Counting in SHA?" [2nd NIST HW]

Antoine Joux

従来 MD4, MD5, SHA-0, SHA-1 等の解析で中心的役割を果たしてきたフランス国防省兼ベルサイユ大学助教授の Joux 氏による SHA の安全性に関する講演で、ニュートラルビット、メッセージ修正技法と呼ばれる衝突発見技法について解説し、ブーメランアタックと呼ばれる新しい技法について解説し、SHA-1 の衝突が近い将来発見されるであろうという見解を述べた。

Gröbner Basis Based Cryptanalysis of SHA-1 [2nd NIST HW]

Makoto Sugita, Mitsuru Kawazoe and Hideki Imai

SHA-1 に関する最新結果について講演し、パネリストとしても発言した。NIST の Kelsey 氏から様々な SHA-1 の評価手法を SHA-256 の安全性評価に適用した場合のついての見解についての質問があり、現状 SHA-256 への適用を試みて困難にぶつかり停滞しているもの

の、近い将来それが克服され、新しい解析法が提案される可能性が高いという見解を述べられた。

Precise Probabilities for Hash Collision Paths [2nd NIST HW]

Werner Schindler, Max Gebhardt and Georg Illies

ドイツ BSI の Schindler 氏による講演で、確率的モデルを用いたハッシュ関数の差分解読法に対する安全性評価法の提案。講演者自身も認めている通り、この方法はおおまかな評価である。

Automated Search for Round 1 Differentials for SHA-1:Work in Progress [2nd NIST HW]

Philip Hawkes, Michael Paddon and Gregory Rose

Wang 教授による衝突発見法で最後に残された謎であった差分パスの発見法についての講演で、探索木のアルゴリズムを用いているものの、まだ完全な解明はなされていない。

NIST HW でのその他新アルゴリズムの提案 [2nd NIST HW]

Eli Biham 教授によるハッシュアルゴリズム HAIFA の提案、福井大学の廣瀬助教授による 2 ブロック長ハッシュ関数の提案。

Classification of Hash Functions Suitable for Real-life Systems [2nd NIST HW]

Yasumasa Hirai, Takashi Kurokawa, Shin'ichiro Matsuo, Hidema Tanaka, and Akihiro Yamamura

現実世界におけるハッシュアルゴリズムについての産業側からの見解と提言について。ハッシュ関数の分類・取扱の方針等に関する考察。利用シーン・利用用途などを分類の軸とし、分類した各々のハッシュ関数に求められる要求事項などに対する考察を行った。

Formalizing Human Ignorance: Collision-Resistant Hashing without the Keys [VietCrypt06]

Phillip Rogaway

ハッシュ関数を内部で用いる署名などのアルゴリズムの安全性証明について、定義では用いるハッシュ関数は鍵付きハッシュ関数で表現されるにも関わらず、実際には鍵無しのハッシュ関数が用いられることがある。本発表ではこのギャップに注目し、鍵無しのハッシュ関数を用いた場合に対する安全性証明について言及し、digital signature, pseudorandom function, Merkle-Damgard construction について具体的にその手法・捉え方を示した。具体的手法は Black-box reduction に類似した概念に基づいている。

Discrete Logarithm Variants of VSH [VietCrypt06]

Arjen K. Lenstra, Dan Page and Martijn Stam

著者らの以前の提案方式で、RSA などと同様の問題を仮定とした安全性証明可能なハッシュ関数 VSH が提案されていた。本発表では、同様の構成方針に基づき、仮定とする問題を離散対数問題とした VSH-DL を提案。更にそのバリエーションの一つとして、楕円を用いた方法も提示している。それらバリエーション及びオリジナルな VSH について効率などの比較も提示している。楕円などを用いる場合は効率性が劣化するが、安全性が向上するなどのトレードオフがある。

How to Construct Sufficient Conditions for Hash Functions [VietCrypt06]

Yu Sasaki, Yusuke Naito, Jun Yajima, Takeshi Shimoyama, Noboru Kunihiro, and Kazuo Ohta

Wang らによって提案されているハッシュ関数の解析手法の要となる手順の一つに探索を可能とする sufficient condition を決定する過程がある。本発表では、この sufficient condition を自動的に抽出するアルゴリズムを提案している。この SC アルゴリズムの入力から出力までにかかる時間は、わずか数秒である。また、MD-family ハッシュ関数及び SHA-family ハッシュ関数に適用可能なアルゴリズムである。この SC アルゴリズムを実際に Wang らの攻撃手法に適用し、MD4・MD5・SHA-0・SHA-1 等についての解析結果を得ている。特に、MD5 については、Wang 氏らからは提示されていなかった condition を見つけるのにも成功している。

On the Internal Structure of ALPHA-MAC [VietCrypt06]

Jianyong Huang, Jennifer Seberry and Willy Susilo

MAC には、ハッシュ関数を用いたメッセージ認証であるが、その構成に共通鍵暗号の AES の構成の一部を利用したものに、ALPHA-MAC がある。本発表では、まず ALPHA-MAC に対する第 2 原像探索攻撃(Second Pre-image Attack) について代数的攻撃方法を用いた解析を行ない、更に内部衝突探索に関する解析を行なった。それらから AES の一部を用いて MAC を構成するような場合に関する内部構成方法の知見を得ている。

Improved Collision Search for SHA-0 [Asiacrypt06]

Yusuke Naito, Yu Sasaki, Takeshi Shimoyama, Jun Yajima, Noboru Kunihiro and Kazuo Ohta

電気通信大学の内藤氏らによる SHA-1 の旧バージョンである SHA-0 の衝突発見に関する講演で、従来 Wang 氏により与えられていた 2^{39} という衝突発見効率を 2^{36} に削減したとい

うもの。

Indifferentiable Security Analysis of Popular Hash Function with prefix-free padding [Asiacrypt]

Donghoon Chang, Sangjin Lee, Mridul Nandi and Moti Yung

インドの若手研究者ナンディ氏による理想的に安全なブロック暗号をベースにハッシュ関数を構成する方法についての講演。SHA-1 等でも用いられている Markle-Damgaard と呼ばれる古典的な構成法をベースにした 16 PGV と double block length 関数と呼ばれる Nandi 氏提案の 2 種の構造の安全性についての証明を与えている。

Multi-Property-Preserving Hash Domain Extension and the EMD Transform [Asiacrypt06]

Mihir Bellare and Thomas Ristenpart

Multi-party Preserving 変換と呼ばれるハッシュ関数の新しい構成法を提案したもので、安全性が証明可能かつ効率的なハッシュ関数の構成が可能であるとしている。

Combining Compression Functions and Block Cipher-Based Hash [Asiacrypt06]

Thomas Peyrin, Henri Gilbert, Frédéric Muller and Matt Robshaw

フランステレコムの Peyrin 氏らによる double block length 呼ばれるブロック暗号ベースのハッシュ関数の構成法に関する講演で、多重ブロック長ハッシュ関数という新しいフレームワークを提案し、攻撃法を DF（Degree of Freedom）攻撃と MUL（Multicollisions or Multipreimages）攻撃という２つに分類している。この分類を踏まえて、安全なハッシュ関数の構成法について提案している。

Cryptanalysis of Reduced Variants of the FORK-256 Hash Function [CT-RSA07]

Florian Mendel, Joseph Lano and Bart Preneel

FOLK256 について非線形部分で構成される部分が、仮に線形であると仮定した場合の L-FOLK256 に対する truncated differential attack による解析結果の発表。解析の中では Coding Theorem で用いるテクニックを利用。Low Hamming Weight となった場合に解析がしやすいケースが存在する。これらの解析テクニックはオリジナルの FOLK への解析に展開することが可能であるとのこと。本発表を更に進展させた結果を e-Print に掲載との事。更に FSE 2007 での発表が予定されている。

Second Preimages for SMASH [CT-RSA07]

Christian Rechberger and Vincent Rijmen

Pattern construction property (PCP) と Forward prediction property (FPP) を解析する

ことにより output の差分をコントロールし、Second Pre-image attack の解析を行なった。中で用いる行列 （nxn） とメッセージの長さとの関係が t≦n+1 の場合は確率 1 で成功し、t > n+1 の場合は 1/ poly 程度の確率で成功することを示した。

A Bit-Slice Implementation of the Whirlpool Hash Function [CT-RSA07]

Karl Scheibelhofer

AES をベースに構成されているハッシュ関数 Whirlpool の高速実装手法の発表。Bit-slice のテクニックを用いて Whirlpool の効率的な実装を行なった。その効率について Table ベースの実装と比較した結果を示した。本提案実装では、table look up を必要とせず、Timing attack が適用困難な構成となっており、table ベースの実装に比べ 95%のデータ量を削減でき、37% interaction が増加し、63%メモリ量(code + data)を削減できる、としている。

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 [SCIS07(国内)]

内藤 祐介、太田 和夫、國廣 昇

Differential Path Search Algorithm for First Round of MD4 [SCIS07(国内)]

王 磊、佐々木 悠、太田 和夫、國廣 昇

Strategy for Selecting Disturbance Vector of SHA-1 [SCIS07(国内)]

岩崎 輝星、内藤 祐介、矢嶋 純、佐々木 悠、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 [SCIS07(国内)]

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

SHA1 差分パス自動生成ツール [SCIS07(国内)]

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

電子通信大学太田研、富士通研究所、中央大学によるチームによるハッシュ関数の解析に関する講演である。SHA-1 の Disturbance Vector の探索、差分パスの自動生成、Message Modification の新たなる改良についての最新成果であり、現在近い将来の SHA-1 の衝突発見を目標に改良が進めているが、衝突発見にはまだ解決しなければならない課題が残されているということであった。

Groebner basis based cryptanalysis of SHA-1 [SCIS07(国内)]

杉田 誠、川添 充、松浦 幹太、今井 秀樹

杉田らによるグレブナー基底を用いた SHA-1 の解析に関する講演で、グレブナー基底の理論をベースに誤り訂正符号アルゴリズムを組み合わせて Wang らによる解析法を改良している。この方法を用いて 58 段で衝突発見に成功し、また従来詳細が明かされていなかったフルラウンドの場合の計算量評価を行なっている。

(2) ストリーム暗号

New Guess-and-Determine Attack on the Self-Shrinking Generator [Asiacrypt06]

Bin Zhang and Dengguo Feng

Self shrinking generator と呼ばれる 1994 年にドイツの Meyer 氏らによって提案されたストリーム暗号方式の解析で、Time-Memory Trade-off という 2000 年に Shamir 教授らにより提案された解析法よりも高速な、guess-and-determine という解析法を提案した。この方式により解析に必要なメモリ量を大幅に削減しており、暗号学的に興味深い結果ではあるが、パラメータを大きく取ることでこの攻撃を回避することは容易であるためこのストリーム暗号を用いることの実用上の問題は無いと考えられる。

On the (In)security of Stream Ciphers Based on Arrays and Modular Addition [Asiacrypt06]

Souradyuti Paul and Bart Preneel

SSL などで使われている RC4 などが属する array-and-addition というタイプのストリーム暗号に対する解析で、各段の状態のアップデートがわずかであることを利用することで解析が可能であることを指摘した。この方法により、従来不用意に設計されたものに対しては解析可能であるとしているが、慎重に設計することにより解読不可能にすることは困難ではないとしている。

Efficient Computation of Algebraic Immunity for Algebraic and Fast Algebraic Attacks [Eurocrypt06]

F. Armknecht C. Carlet, P. Gaborit, S. Ku"nzli, W. Meier and O. Ruatta

ストリーム暗号に対する代数攻撃及び高速代数攻撃に対する安全性評価計算を効率を改善したという発表。従来の安全性評価法は実際の攻撃と同等の計算量が必要で、あまり実用的ではなかった。この発表では、グレブナー基底の最高次数を順次上げていくなどの方法で、安全性評価の計算効率を高めている。

Construction and Analysis of Boolean Functions of $2t+1$ Variables with Maximum Algebraic Immunity [Asiacrypt06]

Na Li and Wen-Feng Qi

代数的攻撃に対する安全性の尺度として Algebraic Immunity という尺度がドイツの Meyer 教授らにより提案されていたが、この尺度に対して最大の安全性を持つような(2t+1)変数（t は整数）のブール関数の構成法を提案し、この関数を用いることで安全なストリーム暗号の構成が可能であるとしている。ただし Algebraic Immunity という尺度は理論的に

は興味深い対象であり安全性の大体の目安にはなるものの、100%安全性を保障するものではない。

Improved Linear Distinguishers for SNOW 2.0 [FSE06]

K.Nyberg, J.Wallén C.Rechberger and V.Rijmen

ストリーム暗号の国際規格 ISO/IEC 18033-4 で標準化されている SNOW 2.0 に対するアタックが発表された。このアタックは 2^{179} の長さの出力系列を得ることにより統計的な偏りが検出できるというものである。まだ必要とされる系列長が長く、このアタックはまだ現実的な脅威ではないと考えられる。

Cryptanalysis of Achterbahn [FSE06]

T.Johansson, W.Meier and F.Muller

Cryptanalysis of Grain [FSE06]

C.Berbain, H.Gilbert and A.Maximov

Cryptanalysis of Stream Cipher DECIM [FSE06]

H.Wu and B.Preneel

Chosen Ciphertext Attacks Against MOSQUITO [FSE06]

A.Joux and F.Muller

Distinguishing Attack on the Stream Cipher Py [FSE06]

G.Sekar, S.Paul and B.Preneel

Resynchronization Attack on WG and LEX [FSE06]

H.Wu and B.Preneel

e-STREAM に提案された Achterbahn、Grain、DECIM、MOSQUITO、Py、WG、LEX に対する攻撃法が発表された。攻撃が発表されたからといって自動的にその暗号が落選となるわけでなく、アルゴリズムの改良の機会は与えられている。e-STREAM は 2006 年 2 月で第 1 次評価フェーズを終え、2006 年 7 月から第 2 次評価フェーズを開始し、2008 年 1 月に最終レポートを出す予定である。

The Design of a Stream Cipher [SAC06]

Lex, Alex Biryukov

Dial C for Cipher [SAC06]

Thomas Baignères and Matthieu Finiasz

On the Problem of Finding Linear Approximations and Cryptanalysis of Pomaranch Version 2 [SAC06]

Martin Hell and Thomas Johansson

Multi-Pass Fast Correlation Attack on Stream Ciphers [SAC06]

Bin Zhang and Dengguo Feng

Crossword Puzzle Attack on NLS [SAC06]

Joo Yeon Cho and Josef Pieprzyk

ECRYPT で提案された様々なストリーム暗号についての解析結果が発表された。CRYPTREC 推奨暗号とは関連は無いが、ストリーム暗号の解析法が着実に進歩していることを感じさせる。

QUAD: a Practical Stream Cipher with Provable Security [Eurocrypt06]

C. Berbain, H. Gilbert and J. Patarin

多変数連立２次方程式を解くこと（MQ 問題）の数学的困難性を利用して、安全性が証明できるストリーム暗号 QUAD を設計した。安全性の証明だけなら、これ以前にいくつか提案されているが、それらは計算量が大きく実用的でなかった。QUAD は通常の PC で 4.6Mbps であり AES よりかなり遅いが、発表者は既存提案よりずっと効率が良いと主張している。 安全性の根拠とする多変数連立 2 次方程式の解法は、グレブナー基底を利用した方法の研究が進んでおり、証明に欠陥がないか慎重な検討が必要だろう。また、共通鍵の研究者から、評価が粗く、具体的攻撃法に対する安全性は保証できていないという感想も聞かれた。

Ensuring Fast Implementations of Symmetric Ciphers on the Intel Pentium 4 and Beyond [ACISP06]

Matt Henricksen and Ed Dawson

eSTREAM に応募されたストリーム暗号(Py, Phelix, Mir-1, MAG, HC-256, Dragon など) の Intel Pentium 4 上で implement した際の効率についての考察結果を発表。多くの algorithm は eSTREAM の公募の際のガイドラインに則ったつくりになっているが、完全に満たせているものが全てではないとしている。ここでの考察結果は、アルゴリズムを差別化する意図ではなく、将来の知見のひとつとして位置づけている。

MV3 --- A New Stream Cipher Based on Random Walks [CT-RSA07]

Stephen Miller, Ramarathnam Venkatesan, Ilya Mironov and Nathan Keller

ストリーム暗号を provable secure に構成する為に、self masking を施せる構成を提案。アイディアとしては graph の random walk の概念を利用する。また、[LPS86]のテクニックを用いて効率的に random walk の expander を構成し、効率的な構成方法を提案。

A Simple Related-Key Attack on the Full SHACAL-1 [CT-RSA07]

Eli Biham, Orr Dunkelman and Nathan Keller

ハッシュ関数 SHA-1 に似た構造を持つストリーム暗号 SHACAL について、Related-Key attack による解析結果の発表。直接適用する場合、time complexity や data complexity が大きくなってしまいがちである。本発表では、Slide attack が適用しやすいような関係を入力データ間に仮定し他場合の Related-Key Slide attack による解析を行ない、time complexity が constant 程度に削減できることを示した。

Differential Power Analysis of Stream Ciphers [CT-RSA07]

W. Fischer, B. M. Gammel, O. Kniffler and J. Velten

サイドチャネル攻撃の対象としてストリーム暗号が取上げられている研究は、共通鍵暗号や公開鍵暗号に比べると数少ない。あったとしても弱いタイプのアルゴリズムや理論的な解析結果に留まっていた。本発表では、eSTREAM にもエントリされている 2 つのストリーム暗号(Grain, Trivium)をターゲットとした解析結果を発表。IV をうまく操作することでデバイスのノイズを取り除き純粋にサイドチャネル攻撃を実現可能とした。また、本解析は、サイドチャネル攻撃に得てして用いられる Template をサンプルデータを用いずに秘密鍵を推定することが出来る、としている。

ストリーム暗号に対する代数攻撃の実行可能性の検証[SCIS07(国内)]

穴田 啓晃、岡村 利彦

ストリーム暗号に対する代数攻撃について、F4 アルゴリズムと鍵ビット全数探索を効率的に組み合わせることにより解読に要する時間の短縮に成功したという講演。組み合わせる際に全数探索するビット数の最適化を行なっている。

(3) ブロック暗号

The Security of Triple Encryption and a Framework for Code-Based Game-Playing Proofs [Eurocrypt06]

M. Bellare and P. Rogaway

Triple DES のように、同じ暗号化処理を異なる鍵で 3 回繰り返す安全性強化法は、鍵の全数探索攻撃に対しては確実に安全性は向上するが、それ以外の攻撃法に対して安全性が向上するか否かは未解決の問題だった。今回の発表では、符号理論に基づくゲーム・プレイ証明法によって、Triple DES が DES より安全であることを示した。ただし、今回の結果は一つの評価尺度に基づく評価に過ぎず、内部構造を一切考慮していない点に注意する必要がある。

A Zero-Dimensional Groebner Basis for AES-128 [FSE06]

J.Buchmann, A.Pychkine and R.Weinmann

2002年ごろブロック暗号AESが代数的攻撃によって解読できる可能性があるという報告がなされ、世間に注目を集めたが、その後代数的攻撃がグレブナー基底アルゴリズムに帰着することが示され、現在学会では代数的攻撃ではAESは解くことは困難であるという見解が支配的である。今回の発表ではAESの拡大鍵に関するグレブナー基底を計算することに初めて成功したというものであるが、この結果は解読には直接結びつかず、今後の課題であるとしている。

Improved Related-Key Impossible Differential Attacks on Reduced-Round AES-192 [SAC06]

Wentao Zhang, Wenling Wu, Lei Zhang and Dengguo Feng

簡略版 AES に対する各種アタック。中国科学院の研究者による 7 段または 8 段簡略版 192 ビット鍵 AES に対する関連鍵不能差分攻撃による解析である。従来の解読記録は更新してはいないため電子政府推奨暗号の安全性には影響は無いものの、今後の発展の可能性は感じさせる講演であった。

Advances on Access-driven Cache Attacks on AES [SAC06]

Michael Neve and Jean-Pierre Seifert

以前シャミア教授の講演と同種の cache attack と呼ばれる解析法による AES の解析で、128 ビットの AES の鍵が 20 個の暗号化しただけで推定できるというものである。一般的に cache attack を含むサイドチャネル攻撃と呼ばれる解析法は実装に依存するため、AES が直ちに危殆化したことを意味しないが、世界標準暗号である AES についての結果だけに注目される。

An AES Smart Card Implementation Resistant to Power Analysis Attacks [ACNS06]

Christoph Herbst, Elisabeth Oswald and Stefan Mangard

近年その手法が様々有るサイドチャネル攻撃への耐性を持たせる手法の提案。通常行なわれるマスキングだけでは、いくつかの攻撃手法に対しては完全に防ぐことができない。そこで、ランダム化の処理を中に加えることにより、更に強固な耐性を導くことが可能となる。マスキングは演算量的には比較的負担が小さく、ランダム化は比較的負担が大きい。そこで、両者の技術の組み合わせを実装し、効率面・得られる強度とを評価し、適した方式を提案した。

Cache Based Power Analysis Attacks on AES [ACISP06]

Jacques Fournier and Michael Tunstall

AES に対して、cache を用いた解析についての結果を示した。基本的には、2004 年に D.J.Bernstein によって発表された cache timing attack や 2006 年に Shamir らにより発

表された同じく cache による timing の解析を攻撃に類した手法であるが、特に cache にヒットした際のパターンの解析を重視し、それをうまく解析に展開して全体の解析効率を上げている。解析対象として 2 種類の方法が提示されており、一つには ByteSub function を target としもので、2 つめの方法として、MixColumn operation の xtimes を target とした解析を行った。これらの手法の適用により、AES の平文の探索 space を 2^{128} から 2^{68} に削減することが出来る。また本手法はサイドチャネル攻撃の対策として施される masking があったとしても有効な攻撃である、との主張。

KFC - the Krazy Feistel Cipher [Asiacrypt06]

Thomas Baignères and Matthieu Finiasz

KFC(Krazy Feistel cipher)と呼ばれるブロック暗号の新提案。スイス連邦工科大ローザンヌ校の Serge Vaudenay 教授による decorrelation 理論に基づく安全性評価手法により安全性が初めて証明された実際的な暗号であると主張している。ただし安全性証明もある種の仮定があって初めて成り立つものであり、この暗号が電子政府推奨暗号よりも安全性が高いとは必ずしも言えない。

Generic Attacks on Unbalanced Feistel Schemes with Contracting Functions [Asiacrypt06]

J.Patarin, V.Nachef and C.Berbain

電子政府推奨暗号のブロック暗号でも多数用いられているフェステル構造と呼ばれる構造で、三菱電機の MISTY などで用いられている不均等分割タイプの場合の安全性を精密に評価したもの。ある種の仮定の元で大変精密な評価であり暗号学的に大変興味深い結果であるが、具体的な暗号の安全性に直接繋がる結果ではなく、電子政府推奨暗号への直接的な影響は無い。

New Cryptanalytic Results on IDEA [Asiacrypt06]

Eli Biham and Orr Dunkelman and Nathan Keller

OpenSSL などに用いられているブロック暗号 IDEA に対するイスラエルの Biham 教授、Dunkelman 氏らのチームによる安全性評価結果で、従来の解読がフルスペック 8.5 段を 5 段に縮小したモデルでの解読であったのに対し、関連鍵線形攻撃と呼ばれる攻撃法で 7.5 段縮小版に対して鍵の全数探索よりも高速な解読が可能であるというもの。ただしこの解析法は従来の解読法に比べて特殊な場合に適用可能な解読法であり、単純に解読が進んだとは言えないものの、ブロック暗号解析手法が着実に進歩して続けていることは示している。

Cache Based Remote Timing Attack on the AES [CT-RSA07]

Onur Aciçmez, Werner Schindler and Çetin Kaya Koç

一般に cache attack と呼ばれる攻撃手法には Trace-driven attack, Access-driven attack, Timing-driven attack などがある。remote からの操作に適している攻撃は中でも Timing-driven attack である。従来知られている remote attack として発表されているものの多くは、リアルな remote ではなく、若干の仮定を含んでいた。本発表の攻撃手法はそれらの仮定を取り除いたリアルな remote attack となっている。解析の方針は 2002 年に DES に対して解析を行なった Tunoo らのテクニックに類似した解析手法であるが、本提案方式は Tunoo らの手法の中で必要とされていた cache cleaning の動作を必要としない。

(4) 公開鍵アルゴリズム

Forging some RSA signatures with pencil and paper [CRYPTO06, Rump]

Daniel Bleichenbacher

RSA署名では、公開鍵指数 e が小さく、署名検証時のパディング長のチェックを省略した実装の場合、比較的簡単に署名が偽造される危険性がある。通常、PKCS #1 (RSA Cryptography Standard) の RSA 署名では、文書にメッセージのハッシュ値をパディングして得られたビット列を d 乗することにより(d は秘密鍵指数)、署名を生成する。正しい実装では、検証の際にパディングに用いたハッシュ値の長さをチェックし、パディングに余計なstringが付いていないか確かめることになっている。しかし、ハッシュ値の長さのチェックを省略した実装では、不正な string を付け加えても検知できない。発表者は、公開鍵指数 e が 3 などの小さな値の場合には、不正につける string を調節することにより、検証で受理されてしまう署名の偽造が比較的容易に実現できる可能性を指摘した。

上記の発表に対して、CRYPTRECとしては、既に2002年のCRYPTREC Report 2002にてその危険性を指摘していた。(CRYPTREC Report 2002 P112 参照)

※上記発表をトリガに各種関係機関はレポート・対応策などを提示している。

【NIST】

Web上でその事実を公開し、CMVPの一環として実施するCAVPのテストで、上記の不適切な実装がされてないかチェックするように修正した。上記攻撃による署名の偽造防止の具体策として、

* RSA署名の公開鍵指数には e=3 を利用しないこと
* ハッシュ値の長さのチェックを確実に行なうこと

などを挙げている。

RSA-statement_10-17-06

http://csrc.nist.gov/news-highlights/RSA-statement_10-17-06_.pdf

【JPCERT】

JPCERT/CC REPORT 2006-09-21 等で下記内容を掲載。

(抜粋)

【6】複数の RSA 実装において署名が正しく検証されない脆弱性情報源

US-CERT Vulnerability Note VU#845620

Multiple RSA implementations fail to properly handle signatures

http://www.kb.cert.org/vuls/id/845620

関連文書（日本語）

JP Vendor Status Notes JVNVU#845620

複数の RSA 実装において署名が正しく検証されない脆弱性

http://jvn.jp/cert/JVNVU%23845620/

JPCERT/CC REPORT 2006-09-13 号

【2】OpenSSL に証明書が正しく検証されない脆弱性

http://www.jpcert.or.jp/wr/2006/wr063501.html#2

【CERT】

下記レポートを掲載。

http://www.openssl.org/news/secadv_20060905.txt

OpenSSLに関するパッチを公開。

http://www.openssl.org/news/patch-CVE-2006-4339.txt

An Algorithm to Solve the Discrete Logarithm Problem with the Number Field Sieve [PKC06]

An Commeine and Igor Semaev

素因数分解問題の高速解法手法として近年注目されている数体ふるい法の概念を用いて、離散対数問題に対する高速解法手法を構成する試みについての考察。素因数分解に対する解法手法として知られている Matyukhin の方法をベースとし、解法の過程で独立に事前計算等が可能となる部分の演算処理の高速化について考察したところ、性能向上が可能であるとの評価結果を得た。実際の実装をやった結果ではなくあくまでも机上の見積もりにとどまっている。

New Attacks on RSA with Small Secret CRT-Exponents [PKC06]

Daniel Bleichenbacher and Alex May

CRT (Chinese Remainder Theorem) を利用した RSA 暗号の実装で、秘密鍵 d が小さい場合について、従来到達していた解析の bound を上回る結果を導くことに成功した。具体的には 2002 年に May が提案した 2 種類の攻撃手法 (Coppersmith's method をベースとした手法)の良い部分同士を組み合わせる手法や lattice を利用した手法等を用いて解析効率を改善した。本論文で提案した解析手法は、RSA を改良した様々な方法（Galbraith, Heneghan, McKee らにより提案されている方法や Sun, Wu らにより提案されている方法等)に対しても適用することが出来る。

Cryptanalysis of an Efficient Proof of Knowledge of Discrete Logarithm [PKC06]

Sébastien Kunz-Jacques, Gwenaëlle Martinet, Guillaume Poupard and Jacques Stern

公開鍵暗号アルゴリズムの仮定とする問題として素因数分解と並んでよく用いられる離散対数問題について、用いる group の order がきちんと指定されていないような場合について witness を求める事が出来てしまう可能性があることを示した。これらはパラメータの設定が不適切であったりする限定的なケースに起こる為、適切に電子政府推奨暗号を用いている場合への影響はあまり無いと考えられる。

On the security of OAEP [Asiacrypt06]

Alexandra Boldyrava and Marc Fischlin

OAEP は様々な世界標準として認められている(PKCS の#1 v2.1, ANSI X9.44, IEEE 1363, ISO/IEC 18033-2, SET)RSA を基本として安全性を向上させた暗号方式である。 構成の中には、一般に 3 種類の一方向性関数が用いられ、その安全性についてはランダムオラクルモデルなどを用いて証明されている。一方、ランダムオラクルを用いないモデルでは、場合によってはその安全性が証明できないケースが過去に報告されている。本発表では、これら中に用いられている関数がどのような条件下であれば、その出力にはどのような安全性までは保障できるか、を示した。OAEP として、一般化した結果が得られたわけではないが、中で使われている関数に対する条件が、ある一定条件を満たす場合はどのようになるかについて明確に出来た、という点で今後のより安全な構成に対する知見が深められた結果であると考えられる。

Chosen-Ciphertext Security from Tag-Based Encryption [TCC06]

Eike Kiltz

(elective-tag secure)Tab Based Encryption scheme の安全性について考察し、CCA-secure TBE(選択暗号文攻撃に対してセキュアな Tag-Based Encryption) ・weakly CCA-secure TBE ・stag- weakly CCA-secure TBE の関係と CCA-secure PKE (選択暗号文攻撃に対してセキュアな Public Key Encryption) ・ CPA-secure PKE (選択平文攻撃に対してセキュアな Public key Encryption)、及びに CCA-secure IBE (選択暗号文攻撃に対してセキュアな ID Based Encryption) ・CPA-secure IBE・sID CPA-secure IBE (selective ID に対して選択平文攻撃に対してセキュアな ID Based Encryption) の関係性を解析し、reduction の関係を示した。それぞれの優位性をきっちり示せている点に新たな知見を得られている。また、ペアリングをダイレクトには用いずにランダムオラクルモデルを用いずに安全性証明可能な TBE 方式を提案した。さらに、より効率化した方式を rump session で公開した。

Simplified Threshold RSA with Adaptive and Proactive Security [Eurocrypt06]

Jesús F. Almansa, Ivan Damgård and Jesper Buus Nielsen

適応的攻撃および積極的な攻撃を行なう攻撃者に対して安全な閾値付き RSA の従来の構成方式効率が低く、実用的でなかった。本発表では上記の安全性を満たすより効率的な方式を提案。特に分散された鍵の一部が漏えいした場合の対応策として、従来方式で非効率の原因となっていた refresh を行なわずに効率的に再構成することが可能な方式となっている。更に提案方式は近年安全性の証明モデルとして注目されている UC モデル(Universal Composable Model)でもその安全性が証明可能である。

A Strategy for Finding Roots of Multivariate Polynomial with New Applications in Attacking RSA Variants [Asiacrypt06]

Ellen Jochemsz and Alexander May

RSA に関して、ed = 1 mod N なる d が小さい場合に対する攻撃は従来いくつか知られた結果がある。本発表では、d が小さい場合の攻撃手法に対しての手法の一般化を試み、従来知られている結果より進歩した結果を示した。基本的には、Coppersmith が提案した手法に則り、LLL algorithm などを用いて具体的な結果として、Qiao-Lam 方式(復号プロセスの中で中国人剰余定理を利用した方式)や Common Prime RSA(p-1=2ga, q-1=2gb for a large primeg, Φ(N) = (p-1)(q-1) の構成を持つ RSA)などに対する解析結果を示した。手法(解いていく手順)に関する一般化はされたとしても、中の過程の多くは heuristic な部分が多いようである。

Towards a Separation of Semantic and CCA Security for Public Key Encryption [TCC07]

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、選択暗号文攻撃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。

Analysis on Bleichenbacher's Forgery Attack [SCIS07(国内)]

伊豆 哲也、下山 武司、武仲 正彦

CRYPTOのランプセッションでBleichenbacher 氏が提案した実装のバグを利用した RSASSA-PKCS1-v1 5 等に対する攻撃法の発展版の考察結果を発表。具体的にRFC 3161

で提案されているタイムスタンプの偽造が現実に可能であることを示した。また世の中で使われているRSA署名の中で、e=3が利用されているケースが案外あることを指摘、これらについては特にCAなどの役割を担っている機関は早急に変更を行なうことを推奨した。

Generic Transforms to Acquire CCA-Security for Identity Based Encryption: the Case of FOpkc and REACT [ACISP06]

Takashi Kitagawa, Peng Yang, Goichiro Hanaoka, Rui Zhang, Hajime Watanabe, Kanta Matsuura and Hideki Imai

一般の公開鍵暗号アルゴリズムに対してよりセキュアなアルゴリズムに変換することの出来る手法として、FO(藤崎-岡本)変換や REACT などが知られている。本発表では、それらが IDB 暗号にも適用することがあることを示し、適用した際のセキュリティの帰着効率などを考察した。また、FO 変換方式を改良し IDB 暗号に適用した際に、セキュリティの帰着効率をよりタイトにすることが出来る変換方式も提案し合わせて評価を行った結果を示した。

Tag-KEM from Set Partial Domain One-Way Permutations [ACISP06]

Masayuki Abe, Yang Cui, Hideki Imai and Kaoru Kurosawa

長いメッセージなどを効率的に暗号化・復号することのできるハイブリッド暗号の構成について、従来 Tag-KEM/DEM が提言されている。本発表では、RSA や Rabin 暗号など部分一方向性関数と組み合わせたときに、従来方法と同様のセキュリティ要件を満たすより効率的な Tag-KEM を作ることの出来るエンコードの方法を提示した。また、従来よりもより一般的な素因数分解問題に基づき、従来方法と同様のセキュリティ要件を満たせるより効率的な tag-KEM の構成方法も示し、その考察を行った結果を示した。

An Ideal and Robust Threshold RSA [VietCrypt06]

Hossein Ghodosi and Josef Pieprzyk

署名生成などに関し、署名側を頑健に保とうとする場合閾値付きアルゴリズムを用いる場合が多い。従来からいくつかその具体的手法は提示されている。特に RSA を用いる手法に関する従来方法の問題点としては、シェアするメンバが増えるほど、各メンバが所有しなければならない鍵サイズが大きくなってしまうという点がある。本発表では、閾値付き RSA 署名を生成する場合に、各メンバが所有する鍵のサイズは、シェアするメンバの数に依存しない方法を提案。提案方式に関する、安全性・効率性についての解析を行なっている。

The 2-adic CM method for genus 2 curves with application to cryptography [Asiacrypt06]

Pierrick Gaudry, Thomas Houtmann, David Kohel, Christophe Ritzenthaler

and Annegret Weng

超楕円型の公開鍵暗号において安全な曲線を構成するために必要な位相クラス多項式を計算する手法で、この方式は毎回必ずしも成功するとは限らないものの、多くの場合従来よりも高速に計算できると主張している。これにより超楕円曲線暗号の構成が従来よりも容易になったと主張している。

Relationship between standard model plaintext awareness and message hiding [Asiacrypt06]

Isamu Teranishi and Wakaha Ogata

PA(Plaintext Awareness) は[BR94,BDPR98]らにより提唱された公開鍵暗号アルゴリズムに対する概念で、スタンダードモデルでの PA は[BP04]で示されている概念である。本発表では、『公開鍵暗号アルゴリズムが PA の条件を満たし、更に OW(One-way)であることが示せる場合は、そのアルゴリズムは、CPA-secure である』ことを示した。従来結果として、『公開鍵暗号アルゴリズムが PA の条件を満たし、更に CPA(Chosen Message Attack)に対して安全であれば、それは CCA2(Chosen Ciphertext Attack)に対して安全である』ことが示されている。本発表の結果と従来結果から、結果として、『公開鍵暗号アルゴリズムが PA の条件を満たし、更に One-Way であることが示される場合、そのアルゴリズムは CCA2-secure である』ということが示された。

On the Equivalence of RSA and Factoring w.r.t. Generic Ring Algorithms [Asiacrypt06]

Gregor Leander and Andy Rupp

Factoring 問題と RSA 問題の等価性はいまだ示されていない問題であるが、本発表では、flexible LE(Low exponent)-RSA 問題を取扱い、LE-RSA を効率的に解ける環境上で構成した generic algorithm が存在するならば、それは Factoring 解法アルゴリズムに変換することが出来ることを示した。すなわち、この構成の場合に関しては、LE-RSA 問題と Factoring 問題が等価になるということを示した。但し、本発表の結果はあくまで generic algorithm に限る結果であり、non-generic algorithm に対して何かを示せた結果ではない。full paper 版がそのうち e-print に掲載されるとのこと。

Trading One-Wayness against Chosen-Ciphertext Security in Factoring-Based Encryption [Asiacrypt06]

Pascal Paillier and Jorge L. Villar

KPBB(Key-Preserving Black-Box Reduction)という reduction 方法を用いて Factoring 問題に基づく暗号の安全性と一般に確率的公開鍵暗号に対して提示される IND-CCA、IND-PCA などのスタンダードモデルでの関係性について考察結果を示した。FACT (全ての素数要素のリストを計算する問題) という問題を取扱い、更に UBK

(Unbreakabiloty)という概念を持ちだし、UBC-CPA が FACT と等価であることを示した。更に、FACT は OW-CPA とは等価になれないこと、IND-CCA とは等価にはなれないという結果を KPBB reduction を用いて示している。従来の結果としてランダムオラクルモデルで IND-CCA と FACT が等価であることを意味する結果も示されているが、本発表の結果を加味するとランダムオラクルモデルでの安全性証明にはギャップがあることが分かる。factoring ベースの暗号アルゴリズムが IND-CCA-secure になれるのは、encryption twinning technique が用いられている場合に限られる。

Impossibility Proofs for RSA Signatures in the Standard Model [CT-RSA07]

Pascal Paillier

RSA 署名についてスタンダードモデルではその安全性を証明できないことを証明した。証明手法としては、攻撃者の環境として、CMA・KMA・KOA を想定し、安全性のレベルを EF・UF・RE・BK を想定し、EFA が Inversion of RSA と同等であるとすると、その事実を用いて REA を構成することが出来てしまうことを示し、結果として仮定していた instance-non-malleable RSA の仮定に矛盾が生じることを示した。本結果はランダムオラクルモデルの持つ仮定の強さと現実モデルとの間にギャップがあることを明示している。この結果は、RSA-PSS などに対しても同様に示すことが可能との事。

A Practical Optimal Padding for Signature Schemes [CT-RSA07]

Haifeng Qian, Zhibin Li, Zhijie Chen and Siman Yang

RSA タイプのメッセージ回復署名で、通常 Optimal というと|メッセージ|+|乱数成分|=|modulus| となっていることをさす。従来の optimal なメッセージ回復署名の構成には ideal cipher モデルが用いられていたが、ブロックサイズが大きいため実在の cipher で効率的に構成することが困難であった。本発表では小さいブロックサイズの ideal cipher で optimal なメッセージ回復署名を構成した。

Timing Attacks on NTRUEncrypt Based on Variation in Number of Hash Calls [CT-RSA07]

Joseph H. Silverman and William Whyte

NTRU はその構成の特徴から、復号処理を行ない際に、G で表される関数の演算がその input の長さに依存して処理時間に変化が生じる。このデータの違いによる関数 G の処理時間の違いはその後の演算としてあるハッシュ関数の処理開始時間にも影響する。そこで本発表ではこのハッシュ関数の処理開始時間に注目し解析が行なえることを示した。具体的に 80bit parameters に対しては、47.2bit の pre-compute で解析可能であり、128bit parameters では 70.0bit pre-computation で解析可能であるとしている。本攻撃の緩和策としては、上記ハッシュ関数を施す処理を 2 重にするなどの案が挙げられていた。

A Practical and Tightly Secure Signature Scheme Without Hash Function [CT-RSA07]

Benoit Chevallier-Mames and Marc Joye

Gennaro-Halevi-Rabin らにより提案された署名方式をベースに[GHR]で必要となる division-intractability の性質を必要としない tight reduction で安全性証明可能な方式を提案する。tool として chameleon hash function を用い、いわゆる challenge に相当する部分を random ではなく random prime を用い、ハッシュ関数を用いずに上記の性質を満たす方式を実現している。提案方式は strong RSA assumption に基づく方式で、スタンダードモデルで安全性証明可能。

How to Strengthen any Weakly Unforgeable Signature into a Strongly Unforgeable Signature [CT-RSA07]

Ron Steinfeld, Josef Pieprzyk and Huaxiong Wang

従来結果として、Boneh-Shen-Water らが PKC 2006 で partitionated signature として示せる署名方式であれば、strong unforgeable signature に変換可能な変換方式を提案している。本発表では、上記のような性質が無い場合でも任意の構成の署名を strong unforgeable signature に変換可能な変換方式を提案している。[BSW07]で partitionability が必要であったのは証明の際にうまくシミュレートできるようなコントロール可能な部分を確保する為であった。提案方式ではこの部分を 2 重の trapdoor 付ハッシュ関数を用いて、上記の性質が無い構成であっても simulatable となる仕組みを構成することにより、任意の署名方式への適用を可能としている。

Token-Controlled Public-Key Encryption in the Multi-User Setting [SCIS07(国内)]

林 良太郎、田中 圭介

公開鍵暗号アルゴリズムで暗号化などが行なわれる際にランダム値が利用され、暗号化の処理に用いられるが、本発表ではその暗号化に用いられたランダム値が漏洩した場合の暗号文の秘匿性に対する安全性の解析を行なった。上記を想定した場合、その秘匿性を確保できない公開鍵暗号アルゴリズムと上記を想定しても尚且つその暗号文の秘匿性を守れる暗号アルゴリズムとがあることを示した。

代数曲面を用いた公開鍵暗号の安全性について [SCIS07(国内)]

内山 成憲、徳永 浩雄

2005 年から 2006 年前半にかけて東芝の秋山らにより提案された代数曲面上のセクションを求める問題(求セクション問題)に基づく公開鍵暗号の安全性についての解析結果を発表。公開鍵として利用する代数曲面の定義方程式が Weierstrass 標準形の楕円曲面等、一定の条件を満たす形状をしている場合、グレブナ基底に関する基本的な性質を用いて、求セク

ション問題を解くことなく暗号文に対応する平文を効率よく求めることが可能であることを示した。

Some aspects of CVP oracle attack on knapsack cryptosystems [SCIS07(国内)]

小暮 淳、篠原 直行

2005年ごろからNguyenとSternらによって提案されているCVPオラクルを想定したナップザック暗号に対する攻撃法に対して、実際にどの程度の実行能力があるのかを実装実験を行なうことでの検証を試みた。攻撃手法の効率性の考察として、Lagarias-Pdlyzko によって提案されている攻撃手法との比較を行なった。

(5) 暗号プロトコル

Receipt-Free Universally-Verifiable Voting With Everlasting Privacy [CRYPTO06]

Tal Moran and Moni Naor

従来から電子投票によく用いられている手法を用いているが、ネットワークを介しての方式ではなく投票所を利用し、物理的に印刷されたデータを用いる行為をプロトコルの中に取り込んでいる。方式に対して、定式化を行い、UC(Universal Composable) モデルでの安全性証明を行った。提案方式の大きな特徴の一つとしては、Receipt-free の性質を有する従来方式はいずれも効率がさほどよくないものが多かったのに対して、本方式は、その性質を物理的に紙に印刷したデータを利用して実現する事により、方式全体として効率的な方式になっているとの主張。

Defeating Malicious Servers in a Blind Signatures Based Voting System [FC06]

Sebastien Canard, Matthieu Gaud and Jacques Traore

FOO[Auscrypt92]により提案された電子投票方式(Votpia として 2002 年の FIFA world cup(日・韓で共催) の the most valuable players を選出する際に利用された方式)に対して traceability に特に注目。OA[Asiacrypt00]による Hybrid Mix-net と AO[Asiacryot01] による revocable fair blind signature を組み合わせ、不正追跡が効率的に追跡可能な電子投票方式を提案。実装レベルまでは行っているよう。本研究は、ヨーロッパで設置されている e - poll という電子投票プロジェクトの活動の一環として行われているもので、2003 年から 3 年計画のプロジェクトとして進められている。現在実証実験レベルで大学内での投票等に実際に導入している。OA[Asiacrypt00] の (匿名通信路を実現するための) Hybrid Mix-net と同じく AO[Asiacryot01] の (不正者を追跡するための) revocable blind signature の方式に辿り着いた後は直ぐに実装に取り掛かった。構成法については既に別の研究者が発表しており、本発表では具体的に方式を実装し、実証実験を行った結果が報告された。 *[E-poll Web サイト] http://www.e-poll-project.net/index.htm*

Key Exchange Using Passwords and Long Keys [TCC06]

Vladimir Kolesnikov and Charles Rackoff

従来提案されている方式 (Halevi-Krawczyk らによる Hybrid 型鍵交換方式) の一般化を行なった。また、新たに効率的な鍵交換プロトコルを提案した。提案方式も Long key と short key の 2 種類の鍵を用いる Hybrid model となっている。short key の update をチャレンジレスポンス型としカウンタを用いて更新を行なう。安全性証明は、ゲームスタイル(攻撃者とシステムの間の行動をゲームとしてモデル化した上で攻撃の成功確率を求める手法)を導入している。プロトコルよりもっと低い(深い)レイヤー部分での攻撃として位置づけられる(防ぎ難い)攻撃である DoS 攻撃や counter を利用した攻撃の存在について言及した。

Efficient Blind and Partially Blind Signatures Without Random Oracles [TCC06]

Tatsuaki Okamoto

NTT の岡本氏の発表。ペアリングを用いた効率的なブラインド署名・部分ブラインド署名の提案。Boneh-Boneh らの提案する方式よりも効率的な方式となっているが、彼らの方式が仮定している SDH (Strong Diffie-Hellman assumption) よりも若干強めの 2SDH に基づいている。ブラインドを可能としている構成は、他の機能をも可能とする性質を持っており、今後様々な応用の展開が期待できる方式である。

Ring Signatures: Stronger Definitions, and Constructions without Random Oracles [TCC06]

Adam Bende, Jonathan Katz and Ruggero Morselli

署名者の匿名機能を持つ署名法としてリング署名が近年注目を集めている。従来、いくつかの方式が提案されているが新たに出てきた署名法であるためか安全性の定義がまちまちであった。そこで本論文では、リング署名に対する偽造不可能性・匿名性などについて定義化を行い、これまで提案されている論文で示されている定義に対する考察を行った。偽造不可能性についてはほぼどの論文も取り扱いは同等と考えることができる。匿名性については、 AOS[Asiacrypt02] により提案されている論文についても言及され、従来の提案方式の中では参照されうる定義として示されていた。その上で、不足している概念を補い新たな定義化を行なった。また後半部分では自分たちの提案するリング署名の構成を利用した応用例を 2 つほど示した。

On the Definition of Anonymity for Ring Signatures [VietCrypt06]

Miyako Ohkubo and Masayuki Abe

署名者の匿名性を保持できる署名方式として、リング署名がある。その安全面に関しては、

署名の偽造不可能性に関する定義については、ある程度定着した概念が存在する一方、匿名性の定義に関しては、論文によりその定義がまちまちである。本発表では、匿名性の定義として定義し得る 3 種類の定義を提示し、それらの関係性についての結果を示した。また、署名者が複数人であるような閾値付きリング署名についても匿名性の定義を展開し、それらの関係を示し適切な定義を提示している。

Parallel and Concurrent Security of the HB and HB+ Protocols [Eurocrypt06]

Jonathan Katz and Ji Sun Shin

モバイル機器など演算処理能力が豊富でないデバイスを想定した認証プロトコルに関する発表。近年、このような使用環境を意識した上でのプロトコル設計が注目されており、CRYPTO や Asiacrypt 等にもこの部類の発表が出てきている。本発表は、前年の CRYPTO 2005 で A.Juel らにより提案された認証プロトコルの安全性に関わる不備を指摘している。A.Juel らの発表でもその安全性について議論されていたが、sequential なケースのみを取扱っていた。本発表では、parallel attack をも想定した上での安全性に関する考察がなされている。結果として、HB+が安全に用いられる（transaction に関する）条件は Ari らが示した条件よりもより限定された条件となることを示した。

On the Generic Construction of Identity-Based Signature with Additional Properties [Asiacrypt06]

David Galindo, Javier Herranz and Eike Kiltz

ID ベース署名という個別の ID を利用した署名方式(受信者が送信者の公開鍵を知らなくても ID 情報から送信者の公開鍵を計算し、その公開鍵を用いて署名の検証を行うことが出来る)と、従来提案されている PKI を前提とした様々な機能付き署名(ブランド署名、否認不可署名、など)を組み合わせて、PKI のインフラを用いずに実現する方法を提案。概要としては、従来 PKI のインフラを仮定していた部分を ID ベース署名で構成する、という内容。PKI ベースのプロトコルで authority の署名をベースにその後のプロトコルを走らせるのに対して、ID ベース署名を利用した厚生では、authority が ID の持ち主に渡す ID に対応する密鍵を用いてその後のプロトコルを走らせるとう構成。様々な機能付き署名などと組み合わせることが出来る、としている。

Identity-Based Multi-Signatures from RSA [CT-RSA07]

Mihir Bellare and Gregory Neven

RSA ベースの構成で interactive ID ベース multisignature を構成。ID ベースにすることにより、Certificate を必要とせずコンパクトな構成を実現している。[GQ88]の方式を基とし,それを multi/aggregation 署名に改造した。non-interactive のものはまだ実現できていない。メリットとしては、検証演算量が exponentiation 1 回で済み、検証者の負担を軽減

できる。安全性に関しては、[BN06]のテクニックを利用しランダムオラクルモデルで concurrent な環境での安全性が証明可能であることのこと。以後の課題としては、non-interactive aggregation 署名の構成やランダムオラクルモデルを用いない安全性証明などが挙げられていた。

Public Key Cryptography and RFID Tags [CT-RSA07]

Maire McLoone and Matt Robshaw

真がん性検査(製品の偽造防止)などを目的としてRFIDが用いられる場合の偽造防止用に用いる署名方式の提案。Server 側が公開鍵/秘密鍵のペアを生成し、各 tag には ID ごとに unique な coupon が割り当てられる。認証方式は interaction のあるチャレンジ-レスポンス型を用いている。アルゴリズムには楕円を用いた方式が用いられている為、Tag 側で行なわなければならない演算処理量を小さく抑えることが可能とのこと。tag ごとに割り当てられている coupon を更新したい場合は、新たに server から unique な値を発行し、外部からの書き込みが必要となる。(この点は本発表の主眼ではない)

Pairing Based Threshold Cryptography Improving on Libert-Quisquater and Baek-Zheng [FC06]

Yvo Desmedt and Tanja Lange

近年実用化が試み始められている IBE の技術に対して、本来の仕組みでは trusted authority を必要とするところを、trusted authority にかかる権限の強さを緩和する試み。secret sharing と threshold decryption の技術を応用。 trusted authority を複数分散させる代わりに user に secret の一部を配信してしまい、それらの配信された値を利用してユーザの秘密鍵・効果鍵のペアを生成する構成によりプロトコルを構成。

Efficient Provably Secure Restrictive Partially Blind Signatures from Bilinear Parings [FC06]

Xiaofeng Chen, Fangguo Zhang, Yi Mu and Willy Susilo

Restrictive signature の構成の中に、AO[Crypto01] により提案されている partially blind signature の構成を入れ込んだ。また、ペアリングを用いることにより暗号文長の短縮化・演算量の削減を行え、効率的な方式となっていると主張している。この方式の安全性は、ランダムオラクルモデルで証明可能としている。また trace が行われた際には、使用したユーザの ID にまでダイレクトにリンクする点も特長となっている。

Privacy-Protecting Coupon System Revisited [FC06]

Lan Nguyen

昨年度発表された CESSS05 の方式と同様のモデルを用い、Unlinkability, Unforgeability,

Unsplittability（利用回数の不正偽装防止）の性質を満たす。ペアリングを利用し全体の効率化が図られている。 q-SDH および DBDH をベースにランダムオラクルモデルで安全性証明できるとのこと。方式構成のツールとしては、Dodis 氏らにより提案されている verifiable random function を利用。また revocability の実現には Camenish・Lysyanskaya 氏による accumulating approach を導入している。複数人による複数人のクーポンは可能かとの質問に対して、可能であるが computationality と intractability の複雑さが増すと回答した。

Efficient　Broadcast Encryption Scheme with Log-Key Storage [FC06]

Yong Ho Hwang and Pil Joong LeeEfficien

Key storage の efficiency の改善を狙った新しい方式の提案。鍵の生成を行う際にハッシュ関数を用いた chain を構成するが、その構成を 2 つのハッシュ関数を用いて、縦の階層に用いる関数と横の階層に用いる関数の組み合わせにより暗号化して broadcast したデータの復号に用いる鍵の割り当てを行う。結果として、従来の方式に比べ、 computational complexity, transaction complexity が減少し、 効率化できた。

Cryptographic Protocols Realizing E-Markets with Price Discrimination [FC06]

Aggelos Kiayias and Moti Yung

オークション等では個人の提示額の秘匿性は保たれることが性質として求めらる。多くのオークション方式はこれを効率的に満たすことを目指して構成される。本方式では、更にフレキシブルな状況を想定し、売り手が最低限得たい金額と、買手の提示額とを見極め売り手にとっては自分の希望した金額が得られ、買手は売り手の希望金額に沿って、買手間の提示額の割合に沿ったディスカウントを買手同時の提示額は互いに秘匿したまま実行できる特徴を持つ。アプリケーションのひとつとしてオークションが挙げられていたが、問題解決に用いられている技術は秘匿性を保たせながら演算を行う様々なアプリケーションに適用できる可能性を持っているものであると考えられる。

Parallel Key-Insulated Public Key Encryption [PKC06]

Goichiro Hanoaka, Yumiko Hanaoka and Hideki Imai

今年の SCIS2006(日本国内の暗号関係の研究学会として最大の会議)で発表した内容をさらにブラッシュアップした結果を発表した。従来の Key Insulated scheme に対して、 key update が行える仕組みを従来 1 種類の鍵で行っていたところを 2 つの鍵を用意し update の度に交互に用いることにより、従来方法に比べて、鍵が expose した場合のダメージをより小さくとどめることが可能となる方式を提案。

Strongly Unforgeable Signatures Based on Computational Diffie-Hellman [PKC06]

Dan Boneh, Emily Shen and Brent Waters

ペアリングを用いた署名方式に対して、従来は weak unforgeability までは証明可能な安全性が示されていた。本発表では、より強い strong unforgeability までその安全性証明が可能な構成方法を示した。また、本提案方式の構成を用いることにより、 weak unforgeability を strong unforgeability の性質を持つ署名に改良可能であることを示した。これらの証明はスタンダードモデルでの安全性証明が可能となる。

On the Limitations of the Spread of a IBE-to-PKE Transformation [PKC06]

Eike Kiltz

Canetti, Halevi,Katz らにより 2004 年に提案された IBE(ID Based Encryption scheme)を PKE (Public-Key Encryption scheme) に変換する方法が提案されている。 IBE としては従来良く知られた 2 種類の方法があり、本発表ではそれら 2 種類の IBE 方式に関する PKE への変換を考察した。結果として 2 種類の IBE 方式から変換して得られる PKE はほぼ同一の PKE 方式の構成となることを示した。また、本発表による考察は、 TCC06 で発表された TBE (Tag based Encryption scheme) と IBE との関係に関する考察結果にも沿うものとなっている。

New Online/Offline Signature Schemes Without Random Oracles [PKC06]

Kaoru Kurosawa and Katja Schmidt-Samoa

茨城大学の黒澤教授が共著となっている発表。strong RSA assumption に基づき、スタンダードモデルで EF-CMA(Existentially unforgeable against chosen message attack)の安全性証明可能な方式を、従来 Shamir-Tauman により提案されていた方式をベースに新たに提案した。また、本発表では、Gennaro-Halevi-Rabin らにより、 on-line / off-line 署名が満たすべき条件として示されていた division intractability の性質について、より弱いタイプの division intractability で十分であることも示している。

Anonymous Signature Schemes [PKC06]

Guomin Yang, Duncan S. Wong, Xiaotie Deng and Huaxiong Wang

署名の検証者に対して、署名者の匿名性が保たれる署名方式の提案。署名者の匿名性を保つ為の requirement を定義し、その定義に基づき提案方式の安全性についても考察し adaptive secure となることを示している。ベースとしてはよく知られる Shnorr 署名アルゴリズムをはじめとし PSS アルゴリズムや RSA 署名アルゴリズム等にも適用可能である。本提案方式の適用先としては、匿名の鍵交換プロトコル等が考えられる。

Security Analysis of KEA Authenticated Key Exchange Protocol [PKC06]

Kristin Lauter and Anton Mityagin

従来提案されていた一般的な鍵交換プロトコルでは、攻撃者が自由に公開鍵と秘密鍵のペアを正規の鍵として登録することが出来る設定の場合、不正行為が可能となる(A と B との間で取り交わされるべき鍵を両者に対して平行に interaction を持ち、相手から受け取った情報から、本来 A と B の 2 者間で用いるべき鍵を推定することが出来てしまう：Unknown Key Share(UKS) attack)。そこで上記のような行為を攻撃者に許したとしても不正行為を防ぐことが出来る方式(KE+)を提案。また、複数の仲介者を通して end-to-end で最終的な鍵の共有が行える鍵交換プロトコル (KEA+C) を提案。具体的には、先提案の KEA+ に仲介者間の communication で検証可能な confirmation を付けた方式となっている。

SAS-Based Authenticated Key Agreement [PKC06]

Sylvain Pasini and Serge Vaudenay

SAS-based AKA protocol(Short Authenticated Sharing - based Authentication Key Agreement protocl ： 物理的に 2 者間の通信が閉じられている通信路（電話や FAX 等）を介して共有した Human-memorizable な秘密情報を用いて、インターネット等の公開のネットワーク上に秘密通信路を構成できるような鍵を共有可能とするプロトコル）の構成方法を提案。（SAS をベースとしたプロトコルの概念は、CRYPTO 2004 で本発表の著者の一人でもある Vaudenay 氏により提案されたものである。）更に、上記提案方式を元に SAS-based Message Mutual Authentication protocol や SAS-based Message Cross-Authentication Protocol の構成方法を提案した。

Conditional Oblivious Cast [PKC06]

Cheng-Kang Chu and Wen-Guey Tzeng

あらたなコミュニケーション上のツールとして、Conditional Oblivious Cast (COC) を提案。提案方式では、A と B とのやり取りに関して、仲介者 S が介在する形の秘密情報交換方法であり、interaction の後に A が得る情報が S や B に漏れることはなく、また、B が得る情報が A や S に漏れることがない、という性質を満たす方式となっている。

On Constructing Certificateless Cryptosystems from Identity Based Encryption [PKC06]

Benoit Libert and Jean-Jacques Quisquater

効率的な Certificateless encryption scheme (CLE) の提案。一般に PKC (Public key Cryptosystems)は、正規の Certification を通信に含む構成になっているが、モバイル機器など演算機能が乏しい通信媒体では、 Certification の検証が重い場合がある。そこで Certification を通信に含まないセキュアな communication を確立したいという動機によって、 Certificateless Cryptography の概念が提案されている。本発表では、従来の提案

方式に対する安全性解析を行った上で、ランダムオラクルモデルで CCA2 secure な CLE scheme を設計した。

Building Better Signcryption Schemes with Tag-KEMs [PKC06]

Tor E. Bjorstad and Alexander W. Dent

従来方式に比べ効率的で安全な署名付き暗号化方式の提案。ツールとして、 tag-KEMs を利用して、 Hybrid signencryption を構成した。この Signencryption Tag-KEMs を用いて Key Agreement なども構成することが出来る。新たに定義した攻撃者モデルに対し提案方式の安全性が証明可能であることを示した。効率性・安全性両面において従来方式を上回る性質を持つ方式となっているとの主張している。

Do Broken Hash Functions Affect the Security of Time-Stamping Schemes? [ACNS06]

Ahto Buldas and Sven Laur

タイムスタンプの中で用いるハッシュ関数に求められる性質についての考察を行った結果が示された。クライアント側がタイムスタンプの中で用いるハッシュ関数としては、衝突困難性や 2 次原像探索困難性等の性質は無くてもよい。また、サーバ側にいたっては一方向性の性質すら必要ないという主張である。ラフな理由としては、たとえハッシュ関数のそれらの脆弱性につけこんだとしても、それらの情報を利用してタイムスタンプ自体に対して意味の有る偽造を行なうことが困難である為としている。

Certificateless Public-Key Signature: Security Model and Efficient Construction [ACNS06]

Zhenfeng Zhang, Duncan S. Wong, Jing Xu and Dengguo Feng

通常の PKI の世界の構成(信用できる第 3 者により発行された証明書により信頼関係を築く)の構成から離れ、信頼できる第 3 者からの証明書なしにネットワーク上での信頼関係を築く(ここでは署名の正しさを提示された公開鍵を用いて検証する、に該当)構成を提案。基本的には最近の流れである ID-base の構成を拡張したものとなっている。署名を生成する公開鍵・秘密鍵のペアを master key・ユーザ自身の ID 情報・ユーザ自身の公開鍵から生成する為、生成された鍵ペアは、確かにその鍵の生成に用いられたユーザ ID のユーザのものである事を示すことになり、結果としてとして PKI の世界での電子証明書の役割を構成することが可能となる。

Public Key Cryptography sans Certificates in Ad Hoc Networks [ACNS06]

Nitesh Saxena

Ad Hoc Network 上で互いの信頼関係を得る為に、信頼する第 3 者により発行された電子証明書を用いる場合があるが、電子証明書の演算は Ad Hoc Network を利用して通信を行な

うような媒体にとっては演算量の負担が大きい場合が多い。そこで本発表では、そのような電子証明書を用いずに信頼関係を持つ為の方式が提案された。具体的には、検証可能な秘密分散方式としてよく知られる Feldman VSS と呼ばれるテクニックを鍵の分配に利用し、分配された部分秘密情報に基づいて通信を行なう事により、有る程度の信頼関係を導くことが出来る。本発表は本会議の優秀学生賞に選ばれた。(会議全体で 2 本の論文が選出された)

An Improved Poly1305 MAC [ACNS06]

Dayin Wang, Dongdai Lin and Wenling Wu

IPMAC と呼ばれる（Poly1305 Message Authentication Code）の安全で高速な MAC の構成を提案。提案方式に対して、安全性に対する考察を示し証明をつけている。2 種類の 16-byte の鍵と 16-byte の nonce との合計 48-byte のみで構成可能な方式となっている。

How To Shuffle in Public [TCC07]

Ben Adida and Douglas Wikström

Mix プログラムを code obfuscator を使って公開し、秘密の計算が一切無い Mix を構成した。一般化 Paillier 暗号を二重に利用して Permutation Matrix を計算する方法を考案した。効率は n^2 なので、従来（n）よりも悪い。

Adaptively Secure Traitor Tracing against Key Exposure and its Application to Anywhere TV Service [ACISP06]

Kazuto OGAWA, Goichiro HANAOKA and Hideki IMAI

ブロードキャストを利用したメディアなどのコンテンツ配信は徐々に広まりつつある。これらサービスでは、攻撃者が秘密鍵を不正に得てしまった場合等、コピーしたコンテンツの他用途への転用などの攻撃が考えられるため、それらを防止しまた不正者を追跡できる仕組みがあることが望ましい。本発表では、そのような攻撃者に対して追跡可能な方式となっており、また鍵が利用できるコンテンツ(期間)をある一定期間に制限し、鍵の更新を行なう事により、一旦不正者が秘密鍵を得てしまった場合についても、ある一定期間以上前後のコンテンツは保護することが出来る方式となっている。具体的な適用例として、例えば NHK の行なうブロードバンド配信などのサービスに適用できるとして紹介されていた。

Escrowed Linkability of Ring Signatures and its Applications [VietCrypt06]

Sherman S. M. Chow, Willy Susilo and Tsz Hon Yuen

リング署名は複数人から構成される署名グループのいずれかの者が署名者である事が検証できる一方で、真の署名者の匿名性を保持することが出来る署名方式である。この署名の場合、2 つの署名の署名者が同一であったとしても、一般にはそれを識別することは出来な

い。本発表では、特別の権限を持つ authority を存在させ、この authority だけが、2 つの署名が与えられた時にそれらが同一の署名者の作成したものであるか否かを識別できる機能を持つリング署名を提案している。また、このような特別の権限を持つ authority のみが不祥事が起きた場合に、署名者の情報からその署名者が生成した署名を追跡できる、また署名からその署名を生成した真の署名者を追跡できるような方式を提案している。具体的な構成として、ユーザの ID を利用した方式などが示された。

HIBE with Short Public Parameters without Random Oracle [Asiacrypt06]

Sanjit Chatterjee and Palash Sarkar

HIBE(Hieratical Id-based Encryption)と呼ばれる、階層 ID ベース暗号方式については、従来結果として、Water が 2005 年に提案した、スタンダードモデルで安全性証明可能・DBDHP(The Decisional Bilinear Diffie-Hellman Problem)を仮定とする・PP(Public Parameter)が O(nh)程度の長さを必要とする(ここで n は ID の長さ、h は階層の深さ) などの特徴を持つ方式がある。本発表では、従来方式に対し優れた特徴をもつ方式を提案。主な利点としては、階層の異なる段で同じ PP を利用することが出来、その PP の必要となるサイズを O(n+h)にまで削減でき、スタンダードモデルで安全性証明可能、などである。

Forward-Secure and Searchable Broadcast Encryption with Short Ciphertexts and Private Keys [Asiacrypt06]

Nuttapong Attrapadung, Jun Furukawa and Hideki Imai

BE(Broadcast Encryption)の方式について、フォワードセキュアな性質(秘密鍵が漏洩したとしても過去に暗号化した暗号文の安全性は保たれる)をもつ方式を提案。また、暗号文の分散管理データベースなどへ適用可能な暗号文のキーワード探索可能な BE 方式も提案している。HICB(Hieratical Identity-Coupling Broadcast encryption)と呼ぶ構成を提案し、その構成を用いて 2 つの提案方式を実現している。

A Scalable Password-based Group Key Exchange Protocol in the Standard Model [Asiacrypt06]

Michel Abdalla and David Pointcheval

GPAKE(Group Password-based Authentication Key Exchange)と呼ばれるパスワードを基にグループで共有できるセッション秘密鍵の生成方式についての新しい方式の提案。提案方式は、ランダムオラクルモデルを用いずにその安全性証明が行えている。Burmester-Desmedt 方式に前処理として、パスワードを基本とした実質的には認証を行うプロセスを加えて構成している。関連結果として、TCC 2007(翌 2 月)で、Abdalla, Bohli, Gpnzalez, Steinwandt らにより、一般的な PAKE(2 者間のパスワードを基にセッション秘密鍵の生成方式)から GPAKE を構成する方式を紹介。その提案方式では、認証プロセスと

して本発表で提案した認証プロセスと同様の方法を用いている、とのこと。

A Weakness in Some Oblivious Transfer and Zero-Knowledge Protocols [Asiacrypt06]

Ventzislav Nikov, Svetla Nikova and Bart Preneel

いくつかの Oblivious Transfer プロトコルに対する攻撃手法を提案。提案された攻撃手法は、準同系暗号を利用した NIZKA(Non-Interactive Zeroknoledge Argument)に対する攻撃にも適用することが出来る。攻撃では、いくつかの semantically secure な暗号アルゴリズムが用いられている場合で、それらのアルゴリズムは復号時に暗号化を行なう際に用いられたランダムコインの情報を漏らしていること・送信者/検証者の入力がある空間に偏っている(場合がある)こと・その空間が平文空間に比べて極めて小さいことなどを利用している。論文では、上記攻撃に対する方式の改善案も提案している。

Almost Optimum Secret Sharing Schemes Secure against Cheating for Arbitrary Secret Distribution [Asiacrypt06]

Satoshi Obana and Toshinori Araki

[OKS06]で提案された CDV モデルにおいて安全な 2 種類の秘密分散方式を提案。提案方式は分散する対象となる秘密情報がいかなる確率分布をもつものであったとしてもセキュアに分散可能な方式となっている。1 つめの方式は、分散秘密値のサイズの小さくすることを優先した方式となっており、その分散秘密値のサイズの lower bound +1 bit で構成することが可能な方式となっている。2 つ目の方式は、分散秘密値のサイズ及び不正者の成功確率を Flexible に設定可能な方式となっている。

Efficient Selectively Convertible Undeniable Signature Without Random Oracle [Asiacrypt06]

Kaoru Kurosawa and Tsuyoshi Takagi

否認不可署名(一般的に署名者が意図する受取人のみがその正しさを検証することが出来る署名方式)を誰もがその正しさを検証できる署名に変換可能な方式について、Cramer-Shoup 署名をベースに新しい方式を構成。提案方式は誰もが検証可能な署名への変換は、他の否認不可署名は維持したまま選択した署名のみに限定して変換可能な方式になっている。また、従来提案方法と異なり、ランダムオラクルを用いずに安全性証明可能な方式となっている。

Simulation-SOund Non-interactive Zero-Knowledge Proofs for a Practical Langage and Constant Size Group Signatures [Asiacrypt06]

Jens Groth

Eurocrypt06, CRYPTO06 に続く結果。pairing などの Non-Interactive Zero-Knowledge

proof に対する結果。simulation-sound extractable NIZK proof for satisfiability of paring product equations に対する。Common Reference String を利用する方法。ペアリングを用いたプロトコルの安全性をランダムオラクルを用いずに証明を行う有効なツールとなりえる。本 3 本の論文をまとめた本論文が既に書かれており web に公開中とのこと。

Human Identification through Image Evaluation using Secret Predicates [CT-RSA07]

Hassan Jameel, Riaz Ahmed Shaikh, Sungyoung Lee and Heejo Lee

Human Identification Protocol (HIP) を如何にセキュアに構成できるかに対する試み。意識できている者だけが識別できるような graphical な情報を用いるアプローチを検討。このようなアプローチによる従来結果としては、Completely Automatic Public Turing Test to Tell Computers and Humans Apart (CAPTCHA) が Eurocrypt2003 で Luis らにより提案されているが、彼らの方式では人間だと多くの人が識別できるが PC だとその識別が難しくなってしまうような Graph であった。本発表では PC でも人でも secret をシェアしている人間には識別可能であり、 secret をシェアしていない PC 及び人間にはその識別が困難であるような方法を提案している。現実的に取扱い可能である instance の数に限界がある・識別の困難さの図り方・よりアクティブな攻撃者への対処・一度 witness を知ってしまうとそれらに対する学習が行なえた事になってしまう等に対する検討は今後の課題となっている。

Directed Transitive Signature Scheme [CT-RSA07]

Xun Yi

Transitive 署名は 2002 年の CT-RSA で Bellare らにより提案された署名方式であるが、ベーシックな従来の方式では通っている path を順次検証していくような方式であった。ダイレクトに edge 部分の署名検証が行なえる方式として DL ベースの方式は既に提案されていたが、RSA ベースの方式については、提案されていなかった。本発表では、ダイレクトに edge に相当する部分の署名をダイレクトに検証できる RSA ベースの方式を提案。従来方式に比べて署名サイズが大幅に削減でき、path が長くなるほどにその効果は大きくなっている。

Improved Efficiency for Private Stable Matching [CT-RSA07]

Matthew Franklin, Mark Gondree and Payman Mohassel

個人の preference の匿名性を保ちつつ、マッチングを探索する方式として FC06 で Golli らが提案した方式がある。彼らの方式は communication complexity が大変大きくなってしまう特徴があった。本発表では Golli らの方式に比べ、communication complexity や round complexity が効率的な方式を提案。ツールとして modefy 1-out-of-n OT(Oblivious Transfer)と閾値付き準同型性暗号を用いている。更にマッチングを司る Matching

Authority(MA) が 2 人の場合も検討し、効率的な方式を提案。

Compact E-Cash from Bounded Accumulator [CT-RSA07]

Man Ho Au, QianHong Wu, Willy Susilo and Yi Mu

Nguyen らが提案している bounded accumulator を利用して、効率的な E-Cash の方式を提案。pairing を用いた revokable な signature を提案し、それを E-Cash system の中で利用している。2 重使用した場合にそのユーザの匿名性は破られる。revoke されたユーザは、不正を行なったトランザクションだけではなく、ID が認識され、そのユーザが行なった全てのトランザクションが revoke されてしまう方式となっている。

Authenticated Group Key Agreement Protocols with a Privacy Property of Afiliation-Hiding [CT-RSA07]

Stanislaw Jarecki, Jihye Kim and Gene Tsudik

本発表では、所属の匿名性(affiliation privacy)という概念を持ち出し、所属の匿名性を保持したままで Group Key Exchange を行なう方法を提案している。同著者により、ACNS06 で single use certificates を用いた方式を提案してるが、本発表では一般の PKI を前提として使うことの出来る方式を提案。基本は Burmster-Desmedt らにより提案されている Group Key Authentication の方式。これを Affiliation-Hiding な Authenticated Group Key Agreement に改造。もともとの方式と同等の効率を保てている。(2 communication round, 3-4 exponentiation per player)。RSA ベースでも DL ベースでも構成可能であり、ランダムオラクルモデルで安全性証明可能とのこと。

New Efficient Password-Authenticated Key Exchange Based on RSA [CT-RSA07]

Sangjoon Park, Junghyun Nam, Seungjoo Kim and Dongho Won

PAKE(Passward Authenticated Key Exchange)として効率的な方法としては離散対数問題に基づく方式などが提案されている。RSA タイプで構成しようとした場合、通常 DL タイプに比べ非効率になりがちである。本発表では、従来知られている DL タイプの PAKE よりも暗いアンド側の演算量が効率的な EPAKE を提案。安全性に関しては、ランダムオラクルモデルで安全性証明可能としている。

Non-Degrading Erasure-Tolerant Information Authentication with Application to Multicst Stream Authentication Over Lossy Channels [CT-RSA07]

Yvo Desmedt and Goce Jakimoski

再送信や erasure code などを多用できない環境でいかにしてその（ビデオや音声の配信）通信を実現するかを課題としている。従来方式としては TESLA があるが、この方式では packet ごとに MAC/tag をつけるような処理であった為、通信量・演算量ともに負担が大き

く、非効率であった。本発表では、これにかわる効率的な配信方法を提案。必要となる MAC/tag を出来る限り少なく押さえることにより全体の効率を上げた。必要となる最低限の MAC/tag 数を見極める為に、design theory, 特に cover-family(superimposed codes)に着目。また、TESLA 自身ももっと効率的な authentication code に入れ替え、更にそれを複数に分割して処理を行なう事により効率的な配信方法を構成できるとしている。(実際には鍵を使いまわせるという利点から authentication code の代わりにディジタル署名を利用)

Tackling Adaptive Corruptions in Multicast Encryption Protocols [TCC07]

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 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 (Broadcast Encryption)以外のプロトコルに応用できるかどうかは未解決問題。

Secure Linear Algebra Using Linearly Recurrent Sequences [TCC07]

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)。準同型性公開鍵暗号と 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 [TCC07]

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 $n \geqq (2+\varepsilon)t$ (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、従来結果と同胞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。

Concurrently-Secure Blind Signatures without Random Oracles or Setup Assumptions [TCC07]

Carmit Hazay, Jonathan Katz, Chiu-Yuen Koo and Yehuda Lindell

Fishlin が考案した CRS モデルで標準的仮定に基づく Concurrent-secure ブラインド署名を改良し、CRS を使わないで構成した。具体的には、暗号化と NIZK (Non-interactive Zero-Knowledge)をコミットメントと ZAP で代替することによって、CRS として参照していた暗号化鍵と NIZK 用の CRS を不要とした．なお，Simulation ベースの安全性定義を black-box 証明で満たすブラインド署名を構成することが不可能であることが Lindell によって証明されている．ここでの構成は，Game ベースの安全性定義になっている．

Designated Confirmer Signatures Revisited [TCC07]

Douglas Wikström

Designated Confirmet Signature について、新しい定義を提示。その定義に基づく安全性証明可能な方式を提案。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 仮定と DH(Diffie Hellman) 仮定に基づく方式となっている。

From Weak to Strong Watermarking [TCC07]

Nicholas Hopper, David Molnar and David Wagner

Watermark に対する新たな計算量的安全性定義を提示し、さらにそれよりはやや弱い実用上の利便性を加味した定義を提唱し、またそれらの弱い定義からここで提唱する強い定義への変換方法を提示した。最新版は、e-Print 2006/430 を参照するとのこと。

Private Approximation of Clustering and Vertex Cover [TCC07]

Amos Beimel, Renen Hallak and Kobbi Nissim

Private Approximation of search problems について、NP-complete search problem と一

般に呼ばれる - vertex-cover problem, k-center problem, k-median などの組み合わせにより成り立つ問題に対して、従来知られている結果より実現可能性が小さいことを証明した。vertex-cover problem に関しては、ρ(n)-approximates vertex-cover の場合は、少なくともΩ(n/ ρ(n)) bit の情報のリークが必要であること(ここで n はグラフの中の頂点の数)を示し、cluster problem に関しては、どんなに小さな近似率の approximation algorithm であってもΩ(n) bit のリークが必要(ここで n は instance の点の数)であることを示した。

Robuster Combiners for Oblivious Transfer [TCC07]

Remo Meier, Bartosz Przydatek and Jürg Wullschleger

A と B の間で OT(Oblivious Transfer)を構成する際に、従来に比べてより強力な定義を提唱。この定義のメリットは A と B とが異なる assumption を用いて構成されているような場合も取扱える点にある。また、この定義に沿う OT-combiner を提案。OT-combiner は両方向の通信での失敗数(不整数)のトータルの値が、通信全体の候補数の数よりも小さい場合に安全な OT を提供できることを示した。特徴的(典型的な)な例としては、両方向に共通の honest な候補が 1 つしかなく、一方のユーザ(例えば A にとって)は他全ての候補が不正であるような場合であっても安全な OT を構成することが出来る。また、候補者数の大半が不正であるような場合でも安全な OT-combiner の構成が physical swap を用いた場合は可能であることを示した。

Unifying Classical and Quantum Key Distillation [TCC07]

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仮定の設定が 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。

(Password) Authenticated Key Establishment: From 2-Party To Group [TCC07]

Michel Abdalla, Jens-Matthias Bohli, María Isabel González Vasco and Rainer Steinwandt

既存の 2-party AKE(Authenticated Key Exchange) から Group AKE への変換方法では、高エントロピーの鍵の使用とランダムオラクルや Ideal Cipher のような理想的仮定が必要だった。本発表では、そのどちらも必要としない変換方法を構成した。これによって標準モデルで安全な 2-party Forward Secure Password AKE から 標準モデルで安全な Group Forward Secure Password AKE を構成した。

Multi-Authority Attribute Based Encryption [TCC07]

Melissa Chase

Threshold ABE（複数の attribute のうち一定以上の attribute を持つ受信者のみが復号できる閾値暗号）での中心的課題は、ユーザの結託によって復号に必要な attribute を構成する攻撃への防御である。本発表では Multi-authority （attribute を発行する機関が複数ある）場合の Threshold ABE を構成した。構成には単一の Central authority が必要であり、この機関は絶対的に信頼でき、すべての authority に関する秘密を持つと仮定されている。

Conjunctive, Subset, and Range Queries on Encrypted Data [TCC07]

Dan Boneh and Brent Waters

さなざまな形式の記述を対象とした searchable public-key system の構成と解析のフレームワークを提示。さらに、比較問題及び部分問題を処理できる方式を提案。さらに任意の結合についても提案。提案方式について従来方式と比較。暗号文のサイズとトークンのサイズが改善されている。

LPN 問題を解決する新たなアルゴリズムと HB プロトコルの安全性評価への応用 [SCIS07(国内)]

Marc P. C. Fossorier、*Miodrag J. Mihaljevic*、*今井 秀樹*、*崔 洋*、*松浦 幹太*

近年、軽量のデバイスを想定した認証プロトコルの研究が活発化しており、CRYPTO 2005 や Eurocrypt 2006 などでも方式の提案などがされており注目を集めている。
Eurocrypt2006 では Katz らが CRYPT 2005 で Ari らが提案した方式に対する解析を行ない、プロトコルが安全に行われるためには制限される条件があることを示した。本発表では、Katz らの考察にも含まれていなかった解析手法による安全性解析を行ない、Ari らが示したプロトコルは、Katz らが示している安全性の範囲よりも更に狭まることを示した。この解析手法は Ari らの方式をベースに提案されている拡張的な方式にも適用可能であると考えられ、その技術的可能性は重要な意味を持つと考えられる。

ID ベース暗号からハイブリッド暗号への変換方法 [SCIS07(国内)]

阿部 正幸、*崔 洋*、*今井 秀樹*、*アイク キルツ*

ID ベース鍵暗号化方式(IDKEM) からハイブリッド暗号(PKE) への一般的な変換方法を提案。従来提案されている方式では変換のために必要となるオーバーヘッドがあったが、本提案方式は、IDベース鍵暗号化方式が partition と呼ばれる構造を持つ方式である場合、上記のようなオーバーヘッドを必要とせずに効率的な変換を可能とする変換方式の提案。IDベース暗号からハイブリッド暗号への変換は、活発に議論されている分野でもありその

社会的需要も大いにあると考えられ、今後注目すべきカテゴリであると考えられる。

効率の良い新しい放送用暗号 [SCIS07(国内)]

境 隆一、笠原 正雄

放送型暗号として適した性質を持つ新たな ID ベース暗号の提案。ヘッダの大きさは、得てして利用端末の数に依存して大きくなりがちであるが本提案方式によれば、端末の数に依存せずに一定のヘッダで方式が実現可能であるとの事。他いくつか放送暗号に適した性質を持つという。安全性の解析に関しては、まだ安全性証明等はつけられていない。

(6) その他

Rigorous Bounds on Cryptanalytic Time/Memory Tradeoffs [CRYPTO06]

Elad Barkan, Eli Biham, and Adi Shamir

解析や効率的な探索によく利用される最近注目を集めている Time-Memory Tradeoff と呼ばれるテクニックに関して、定式化を行なった。従来提案されているいくつかの効率的な手法等は全てこの定式化に基づく特殊なケースとして取扱うことが可能との事。statefull random graphs と言う概念を持ち出し、path の存在は内部情報である hidden state に依存しているとし、逆関数を持つような関数 f について y = f(x) の数の upper bound を示し、更にその結果から hidden states の数の lower bound を示した。また、近年効率的な手法として知られる rainbow-base の手法について新たな手法を提案し、提案方式は事前計算部分の解析の工夫によりオンラインで行なわなければならない Time complexity を軽減することが出来る方式となっている。

The Number Field Sieve in the Medium Prime Case [CRYPTO06]

Antoine Joux, Reynald Lercier, Nigel Smart and Frederik Vercauteren

数体ふるい法を用いた離散対数問題の高速解法手法を示した。本発表は、Eurocrypt06 で同発表者の Antoine Joux 氏らの結果に続く結果である。Eurocrypt06 では、素数 p が $L_p^n(1/3)$より小さい場合について、関数体篩法が有効的に働き、計算量を $L_p^n(1/3)$の計算量にまで削減することが可能であることを示していたが、本発表では、$L_p^n(1/3)$よりも大きな場合に対しても効率的にその計算量を減らすことの出来る数体ふるい法を提言し、それを用いることにより、素数 p が $L_p^n(1/3)$よりも大きな場合に関しても、その計算量を $L_p^n(1/3)$の計算量にまで削減することが可能であることを示した。具体的に実装も行なっており、具体例として、120bit の場合について実験を行なった結果を示した。解法の高速化には、メイン処理部分と後処理部分とを独立に処理できるような構造であることも貢献している。Eurocrypt06 での結果と本発表の結果から全ての離散対数問題の解法計算量は、$L_p^n(1/3)$に抑えることができる、という結論。

Automated Security Proofs with Sequences of Games [CRYPTO06]

Bruno Blanchet and David Pointcheval

近年盛り上がりつつある、安全性証明手法に関する研究結果。従来から安全性証明の手法として試みられているフォーマルメソッドに基づく手法とチューリングマシンを想定した計算量的な解析に基づく手法とを融合させて、計算量的仮定に基づくある程度自動的に安全性証明可能な手法の提案。具体例として、ある種の署名の安全性証明；unforgeability under chosen-message attacks of the Full-Domain Hash signature scheme under the (trapdoor)-one-wayness of some permutations を示した。

On the Relation Between the Ideal Cipher and the Random Oracle Models [TCC06]

Yevgeniy Dodis and Prashant Puniya

従来暗号アルゴリズムなどの安全性を議論するモデルとしてランダムオラクルモデルやイディアルサイファモデル（Ideal-Cipher Model）が起用されてきたが、果たしてどちらが実際の安全性を保障するモデルとなっているのか、という問いに対する考察を行った。発表内では、 Maurer 氏らにより提案されている Indifferentiability と言う概念に注目し、この観点から両モデルを考察した。 ICM で ROM を構成できることは既に示されている。本論文では、 ROM で ICM を構成する事を試みた。 ICM の Indifferentiability を保つ為には、より一般的な general model の場合も Honest-But-Curious model（general model より弱いモデル）の場合も、 Luby-Rackoff construction を少なくとも 6 ラウンドは必要とすることを示した。

Generalized Environmental Security from Number Theoretic Assumptions [TCC06]

Tal Malkin, Ryan Moriart and Nikolai Yakovenko

従来の UC モデルの概念に対する新たなコンセプトの提案。もともとの UC モデルでは CRS 等を前提としない限り provable secure な commitment 等の方式は構成しがたい。そこでもう少し求められるフレームワークを緩めたコンセプトとして、corrupt した participant に関してはその者の witness を用いた query and answer を構成可能とするものが［PS04］で提案されている。 Angel と呼ばれる新たなコンセプトを登場させることにより、従来必要とされていた setup assumption を必要とせずに provable secure であることが示せるというものである。しかしながら彼ら方式では、 collision-free なハッシュ関数を前提として構成されていた。 本発表では、同じく angel のコンセプトに基づくが angel の構成をより現実に近いものとし、更に［PS04］で仮定としていた collision-free のハッシュ関数は仮定とせず、代わりに relative discrete log assumption に基づくコンセプトを示し具体的にそのフレームワークで安全性証明可能なプロトコルを示した。

Universally Composable Security with Global Setup [TCC07]

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 モデル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。これは効率上問題となるだけでなく、NIZK(Non-Interacive Zero-Knowledge)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 モデル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。)

Does Privacy Require True Randomness? [TCC07]

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、シードのビット長を 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。

Private Circuits II: Keeping Secrets in Tamperable Circuits [Eurocrypt06]

Yuval Ishai, Manoj Prabhakaran, Amit Sahai and David Wagner

IC カード等、悪意の有る人間が簡単にタンパ出来るようなデバイスでは、タンパに対する対策技術は極めて重要である。本発表では、タンパに対しある程度自己防衛可能な演算器を提案している。技術的には秘密情報を分散して持つ分散演算技術・タンパされた事実を認識した場合に、自らデータを消去しデバイス内の秘密情報の reset を行なう技術等を組み合わせた構成になっている。但し、全体の構成には多くのゲート数を要する為、低コスト性を要求されるデバイス機器への即時導入には障壁があると考えられる。

Phoolproof phishing prevention [FC06]

Bryan Parno, Cynthia Kuo and Adrian Perrig

近年金融の分野では問題視されている phishing に対する技術的対策としての方式の提案。基本的にはチャレンジレスポンス型の相手認証の仕組みを取り込んだもの。考えうる脅威として、「setup account のハイジャック」「Theft of Trust device」「Malware on the trusted device」「Malware on the computer」「NW 上の attack」「local の NW 部分の Bluetooth への attack」等を想定しそれぞれについて言及した。

Threshold and Proactive Pseudo-Random Permutations [TCC06]

Yevgeniy Dodis, Aleksandr Yampolskiy and Moti Yung

効率的な proactive な攻撃者を想定した閾値付き擬似乱数置換方法を提案。[Dodis-Yovoin05]に提案された Pseudo random function の閾値化を行い、extractor を通して出力を構成する。ここで使われたテクニックは、他のアプリケーション(例えば、CBC block cipher mode のような mode of operation や authenticated encryption などへの適用が可能。

Adaptive Detection of Local Scanners [ACNS06]

Ahren Studer and Chenxi Wang

脆弱性の有るローカルホストを利用した攻撃をしようとする攻撃者によるローカルスキャニングの早期検知方法に関する試み。従来手法では、静的に検知する方法が提案されていた。本発表ではネットワークのトラフィックの状態により、動的に検出する方式を提案し、その効果を評価した。提案方式としては, 適応的に接続に成功する率を元に解析しながらそれを検知に反映させる Success based analysis とその反対の Failure based analysis の 2 種類を提案。両方式共に静的な検出方法に比べ、検出効率を挙げることができることを実験により示した。本発表は本会議の優秀学生賞に選ばれた。

Flexible Exponentiation with Resistance to Side-Channel Attacks [ACNS06]

Camille Vuillaume and Katsuyuki Okeya

サイドチャネル攻撃に対して耐性を持つ、べき乗剰余演算方法の提案。提案方式は、耐性を持たないべき乗剰余演算方法に比べてスピード・適応の柔軟性をそれほど損なうことなく構成することが可能であると主張した。対象とする攻撃手法は、Simple power analysis, Differential power analysis, Timing attacks, Cache attacks 等で、実際に実装を行い解析結果を評価した。演算スピードの低下は小さく、サイドチャネル攻撃に対する耐性を増すことが出来ることを実証した。

Template Attacks on Masking---Resistance is Futile [CT-RSA07]

Elisabeth Oswald and Stefan Mangard

Template-based DPA(Differenial Power analysis)による解析手法をもちいた、マスキングの効果に関する考察結果の発表。この解析手法は、デバイスに対する full control の権限を攻撃者与えるという強い仮定の下で行なわれる解析である。テンプレート(template)とは、消費電力の一通りのパターン情報を指し、一旦このテンプレートを作成し、更に解析フェーズで実際の消費電力の挙動と template を比較することにより鍵の推定を行なう。本発表では、サイドチャネル攻撃対策としてマスキングが施されているケースに注目し、マスキングはどの程度効果のある処理であるかを解析している。結果としてはとしては、もし上記のような強い仮定に基づく解析手法が許される場合、マスキングの効果は殆どない、と結論付けられている。

On the Power of the Randomized Iterate [CRYPTO06]

Iftach Haitner, Danny Harnik, and Omer Reingold

今年の Best award paper に選ばれた。擬似乱数生成器を構成する際に用いられることのある ”Randomized Iterate”と呼ばれる Goldreich らに提案された手法 [GKL93] の効果に関する解析を行ない、新たな擬似乱数生成器の構成を提案。提案方式では、擬似乱数生成器に用いる関数が一般的な一方向性関数であると想定した場合、シードの長さを O(n log n)bit にまで軽減することが出来、また、擬似乱数生成器に用いる関数を任意の一方向性関数であると想定した場合には、シードの長さは(O^7)bit に軽減することが出来ることを示した。

Factorization of Square-free Integers with High Bits Known [VietCrypt06]

Bagus Santoso, Noboru Kunihiro, Naoki Kanayama and Kazuo Ohta

素因数分解手法の提案。ビット長が等しい k 個の異なる素数からなる合成数 N に対する解法について、各素数の何ビットかの情報を与えられた状態で適用する手法であり、提案手法には Lattice ベースのアルゴリズムを取り入れている。実用的な脅威としては、例えば RSA が上記のような構成の N を用いて実装されているケースで、サイドチャネル攻撃などにより各素数の何ビットかの情報を攻撃者が得られてしまったような場合に、本手法は現実的な脅威を持つことになる。

Secure Sketch for Biometric Templates [Asiacrypt06]

Qiming Li and Yagiz Sutcu and Nasir Memon

安全なバイオメトリックを実現するための理論的な考察で、相対的エントロピーロスという新尺度を導入し、顔認証を例として論じていた。

Extending Scalar Multiplication using Double Bases [Asiacrypt06]

Roberto Avanzi, Vassil Dimitrov, Christophe Doche and Francesco Sica

ダブルベースを用いることで、Koblitz curve と呼ばれる楕円曲線におけるスカラー倍の高

速化に成功したという内容で、この手法を利用して楕円曲線暗号の高速化が可能であるとしている。

On the Provable Security of an Efficient RSA-Based Pseudorandom Generator [Asiacrypt06]

Ron Steinfeld, Josef Pieprzyk and Huaxiong Wang

Fischlin-Schnorr が提案した RSA ベースの擬似乱数生成器に改良を加え、同様の仮定(平文の一部が攻撃者に知られた状態であっても暗号文に対応する平文を推定することの困難性)の下で安全性証明の改良を行った。従来方法に比べて擬似乱数生成器から出力される出力値に対する証明可能な長さを伸ばすことが出来きるとしている。他アルゴリズムへの適用に関しては、今後の課題として挙げられている。

Selecting Secure Passwords [CT-RSA07]

Eric Verheul

パスワードの理想的なあり方について、数学的観点からの考察を行った。ここで取扱うパスワードとは近年注目されている人間が記憶可能な程度の短いパスワードを想定するものではない。考察の方針としてはエントロピーを考慮し従来配慮されていた Shannon entropy だけではなく、minimal entropy をケアし値を決定するのが望ましいとしている。実際実装を行いパスワードの個、optimal に解析したパスワードの長さ、それらの entropy などを実験値として示している。

Batch Processing of Interactive Proofs [CT-RSA07]

Koji Chida and Go Yamamoto

効率的な batch 処理手法の提案。本提案方式は、GQ identification, ID ベース identification, Multi-party secure Circuit Evaluation などに適用可能とのこと。p-additive な NP-Relation と言う概念を定義し、その定義を満たすものについてはバッチ処理を行なった結果が正しければその中の一つ一つの処理に対する soundness と zero-knowledgeness が成り立つことを示し、その性質を利用し、効率的なバッチ処理を可能とした。

Predicting Secret Keys via Branch Prediction [CT-RSA07]

Onur Aciçmez, Çetin Kaya Koç and Jean-Pierre Seifert

マイクロプロセッサ(MPU)の高速化処理手法として用いられている分岐予測(Branch Prediction)の挙動解析によるサイドチャネル攻撃。Branch Prediction が用いられていると先で命令が分岐するか否かでその挙動に変化が出てくる。この挙動の変化を解析し暗号化処理に施されている処理を解析する。解析の流れは同じくサイドチャネル攻撃の一種であるタイミングアタックの手法に沿う。この攻撃を緩和させるソフトを OpenSSL に展開した

との事。RSA conference 内でもデモも行なっていたもよう。

Long-term Security and Universal Composability [TCC07]

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) フレームワークで扱うために、UC フレームワークの安全性定義で，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 できるかどうかは未解決問題。

Parallel Repetition of Computationally Sound Protocols Revisited [TCC07]

Krzysztof Pietrzak and Douglas Wikström

k-fold parallel repetition で、error probability が k に依存せず、減少しない（及び communication complexity も k に依存しない) computational soundness を持つプロトコルを提案。プロトコルは 8 ラウンドで構成でき、[BG01]で示されている universal argument を利用している。その他いくつかの仮定に基づく複数の現実的な group を元に構成される generic group を利用した 4 ラウンドの方式をも提案。 Bellare らが提案しているプロトコルに比べてより現実的な group の組合せで実現できているとの主張。

Lower Bounds for Non-Interactive Zero-Knowledge [TCC07]

Hoeteck Wee

以下の 3 種類の NIZK(Non-Interactive Zero-Knowledge Proof) (証明者の計算能力が無限大）のセットアップを考えた。CRS モデル（一様乱数あるいは特定の分布からサンプリングした文字列を証明者と検証者が共有する）・Registered PKI モデル（秘密鍵の保持が確認された公開鍵だけを登録して共有する）・Bare PKI モデル（任意の文字列を公開鍵として正当性の確認なしで登録して共有する)。これら各モデルにおいて，共有する情報のサイズの上界と下界を求めた。

Perfect NIZK with Adaptive Soundness [TCC07]

Masayuki Abe and Serge Fehr

NP完全言語に対するNIZKA(Non-interactive Zero-knowledge 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 statement CRS 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 の生成が容易かつ再利用できる、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。

Security Against Covert Adversaries: Efficient Protocols for Realistic Adversaries [TCC07]

Yonatan Aumann and Yehuda Lindell

Covert Adversary とは、発見されないことが確実な場合にのみアクティブな攻撃を実行する攻撃者のモデルであり、Passive (semi-honest) Adversary と Active Adversary の中間的概念である。本発表では、Covert Adversary に対する MPC(Multi-Party Computing) の安全性定義を与え，Yao のプロトコルに基づいて Covert Adversary に対して安全な MPC を構成した。得られたプロトコルは semi-honest 安全なプロトコルの 8 倍遅い。

On the Necessity of Rewinding in Secure Multiparty Computation [TCC07]

Michael Backes, Jörn Müller-Quade and Dominique Unruh

STOC'06 で Rabin 等が主張した結果（Info-theoretic stand-alone secure protocol は info-theoretic UC secure である）に対する反例を示した。Simulation で Rewinding が必須になるような info-theoretic stand-alone プロトコルを構成した。UC(Universal Composable) の simulation は straight-line に限られるので、そのようなプロトコルは UC 安全にはなり得ない。

On Expected Probabilistic Polynomial-Time Adversaries: A Suggestion For Restricted Definitions And Their Benefits [TCC07]

Oded Goldreich

Simulation タイプの安全性証明の際に攻撃者及び Simulator いずれもを expected PPT (Probabilistic Poly-time Turing machine) として捉えようとする試みがいくつかなされている。この場合、expected PPT な攻撃者をどう定義するか、は重要な課題となる。従来結果として、expected PPT として捉えた攻撃者の定義は、Feig の定義と Goldreich の定義が知られているが [Katz-Lindell'05] はこれらがいずれも問題あることを示した。この論文

では,「攻撃者が無限の計算力を持つエンティティと対話する場合にも expected ppt である場合」にその攻撃者を expected ppt であると定義し、その有用性を検証している。

On Best-Possible Obfuscation [TCC07]

Shafi Goldwasser and Guy N. Rothblum

Hada に始まる Black-box タイプの安全性定義については様々な impossibility result が知られており、強すぎる定義と認識されている。この論文では「実現可能な最も難しく obfuscate されたコードと同程度に安全」という best-possible obfuscation の考えに基づく定義を提唱している。Black-box 安全ならば Best-possible 安全となる。

Obfuscation for Cryptographic Purposes [TCC07]

Dennis Hofheinz, John Malone-Lee and Martijn Stam

「オリジナルのコードにオラクルアクセスを許されるシミュレータがシミュレートできる Obfuscation」を安全な Obfuscation と定義する。この新しい定義は、Black-Box 定義に対する impossibility result を回避できるほどに弱くはないが、SKE --> PKE 変換を可能にする程度に弱い.

On Secret Sharing Schemes, Matroids and Polymatroids [TCC07]

Jaume Martí-Farré and Carles Padró

Secret sharing に関わる大きな Open Problem の一つとして、理想的な Secret Sharing 方式の中での access structure をどのように特徴付けるか、という課題がある。Brickell らの結果からある適切な特徴づけを行えば全ての access structure はそれぞれが unique な matroid を用いて表現できることを示している。本発表では、matroid を用いて表現した access structure についてその information rate が 2/3 以上であるときにそれが成り立つことを示した。

One-Way Permutations, Interactive Hashing and Statistically Hiding Commitments [TCC07]

Hoeteck Wee

一方向性置換から構成される統計的秘匿性を持つ（対話的）コミットメントのラウンド数について，Oblivious Construction と呼ばれる構成法では $\Omega(n / \log n)$ が下界であることを示した.

NIST 乱数検定における Maurer's "Universal Statistical" Test に関する考察 [SCIS07(国内)]

金田 学、奥富 秀俊、中村 勝洋

著者は NIST SP 800-22 の 2 つの検定に疑問を呈していた。 そこで、検定の PROPOTION（合格比率）の評価について疑問点を解決すべく検討を行った。本考察では検定を多数回繰り返した上で結果が二項分布に適しているか否かを判断するという評価法について述べた。更にユニバーサル統計検定について検討しモデルの修正を行い、シミュレーションにより確認を行った。重なりのあるテンプレート検定モデルについても、NIST 検定を修正した竹田の方法について同様の評価法に基づくシミュレーションにより正確な値に修正されていることを確認出来た。本評価法によって乱数検定の評価が明確に行えることを示した。

2n + α 個の量子ビットを用いた位数発見量子回路の厳密な評価 [SCIS07(国内)]

小関 恵梨、國廣 昇、高橋 康博、太田 和夫

Shor の素因数分解アルゴリズムは、量子計算機の有力な応用例である。このアルゴリズムで用いる位数発見量子回路は数多く提案されているが、Beauregard と高橋（著者）らは量子ビット数の少なさに注力した回路を提案した。理論的に評価した結果、両者の量子回路のサイズ，深さは漸近的に同じオーダになることがわかっている。そこで本発表では、それらの量子回路のサイズ、深さを厳密に評価し比較を行った．その結果、少しでも量子ビット数を小さくしたいときはは高橋らの回路を、それ以外の場合は Beauregarrd の回路を使用するのが良いという評価を得た。

単一光子源量子暗号について [SCIS07(国内)]

西岡 毅、Alexandre Soujaeff、長谷川俊夫、石塚 裕一、鶴丸 豊広、安部 淳一、竹内 繁樹

量子暗号(量子鍵配送)に利用される単一光子源の品質が悪いと、光子数分割攻撃が有効になる。符号理論によって、この攻撃による漏洩情報を減らすことは可能だが、伝送効率が悪くなるので、出来るだけ単一性の良い光源が求められる。この発表では、北海道大学で開発したパルスレーザによる単一光子源を利用することにより、厳密に安全性が保証できる条件下で通信距離 40km の量子鍵配布実験に成功した。

An Improved Security Evaluation of Y-00 under Heterodyne Measurement and Dedicated Fast Correlation Attacks [SCIS07(国内)]

Miodrag J. Mihaljevic、今福 健太郎、今井 秀樹

Y-00 プロトコルは、2000 年に H.P.Yuen が提案した光子を利用する量子鍵配送方式の一種で、データの秘匿性のために暗号的雑音と物理的雑音の両方を使うことを特徴とする。この方式が安全でないことは、三菱電機と東大・今井研(当時)のグループによって示され、具体的な攻撃法が提案されている。本発表では、Y-00 の攻撃専用に調整した高速相関法を適用することにより、従来より効率良く攻撃できることを示した。

Sequential Attack with Intensity Modulation on the Differential-Phase-Shift Quantum Key Distribution Protocol [SCIS07(国内)]

鶴丸 豊広

差分位相シフト量子鍵配送プロトコル(DPSQKD)は、光子数分割攻撃に対して安全であると期待されている。DPSQKD に対する攻撃法として、盗聴者が通信路上の光子パルスに位相変調を掛けることが出来るとするシーケンシャル攻撃が有効であることが分かっている。発表者は盗聴者が位相変調に加え振幅変調も掛けられるとし、離散ガウス強度分布に従うパルスを利用した DPSQKD の安全性を評価したところ、従来の結果を上回る攻撃性能を実現した。Diamanti らは最近、DPSQKD を用いて 100km の安全な通信実験に成功したと発表したが、改良した攻撃法を適用した結果、安全に送信できる距離は 95km 未満であることが示された。

Information-Disturbance Theorem for General Observables [SCIS07(国内)]

宮寺 隆之、今井 秀樹

情報擾乱定理は物理実験において、測定が実験系の量子状態に及ぼす影響の大きさを評価するものである。発表者らは前の論文で、この定理を利用して、ある強い仮定の下で、量子鍵配送における盗聴者の得る情報量と受信者が得る情報に含まれる雑音の関係を求めた。本発表では、情報擾乱定理を拡張することにより、前の論文で必要だった仮定を不要にした。

付録 4

NIST 2nd Hash Workshop での議論の詳細

Session 1: New Structure of Hash Functions

このセッションでは、ハッシュ関数の構成法に関する発表が行われた。

最初の発表では、現在広く使われている Markle-Damgaard 構成法には欠点があり、それまでのハッシュサイズと salt をパラメータとして加えた構成法を提案している。salt を加えたことが特に新しい点で、この修正により collision resistant と 2nd pre-image resistant を強化することができる。2 番目の発表では、Double Block Length Hash の手法が提案された。この手法はブロック暗号ベースのハッシュ関数に適用する方式であり、ハッシュ長がブロック暗号の出力の 2 倍になる方法ある。3 番目の発表では、Markle-Dangaard 構成法の代替として、multi-property-preserving domain extension transform を提案している。この方法には安全性の証明が付けられている。

Session 2: Hash Functions in Practices

このセッションでは、ハッシュ関数が現実にどのように用いられているかに関する発表が行われた。

最初の発表では、ハッシュ関数の現実の利用と、その利用方法に即した新しいハッシュ関数の分類が提案された。特に、Collision Resistant を量的な側面と質的な側面に分け、2 次元のマトリクスに分類した。そして、現実のハッシュ関数の利用方法がこれらのマトリックスに分類され、この分類をもとに標準のハッシュ関数を構成すべきであることが示された。2 番目の発表では、Randomized Hash に関して発表され、ランダムな salt を用いて、既存のハッシュ値をランダム化することで、ハッシュ関数のセキュリティを向上する方法が示された。

Session 3: Panel/Open Discussion -SHA 256 Today and Maybe Something Else in a Few Years: Effects on Research and Design

このセッションでは、以下の問題について議論された

(1)現在 SHA-1 と SHA-256 が直面している問題

Shamir は SHA-1 の問題は、受け取り方の問題で一部に認識されているほど問題は深刻でないと述べた。

Preneel は、MD5 はすでに安全ではないが未だに広く使われており、SHA-1 も似ている状況である。さらに SHA-256 の設計思想が明らかではなく、そのセキュリティ評価を下すのが

難しいと述べた。
Rivest は、将来のハッシュ関数は、現在の SHA-1 への攻撃を超えた攻撃にも対応できるようにすべき、とりわけセキュリティパラメータを導入すべきであると述べた。
Joux は、将来のハッシュ関数がどのように設計されるべきか、またどの性質を考慮すべきかについてまだ疑問点が残ると述べた。

(2)長期の観点では、ハッシュ関数に求められる性質

Ferguson は、システムでは脆弱性が見つかった後でもハッシュ関数は利用され続けるので、ハッシュ関数は resilient（回復力のある）であるべきだと述べた。また、ハッシュ関数はランダムマッピングとして利用されているので、これを必要な性質として加えるべきであると述べた。

Rivest は、将来のハッシュ関数に One-pass Stream mode と in-memory mode という 2 つの mode を入れるべきだと述べた。

Preneel は、ハッシュ関数に必要な性質は Collision Resistance であると強調した。

Joux は、あるハッシュ関数における Collision Resistance が形式的に定義できるかどうかについて疑問を投げかけた。また、Shamir は、Collision Resistance は、ハッシュ関数を Truncate しても保持されると述べた。

(3) 単一のハッシュ関数を作るべきか、目的毎に複数のハッシュ関数を作るべきか

多くのパネリストが議論を行い、各関数について実装、テスト、認証が必要であり、複数のハッシュ関数を用意するとコストが掛かるという指摘があった。そのため、単一ハッシュ関数が最適であるという意見が大勢であった。

Preneel は、単一ハッシュ関数に同意したが、mode やラウンド数を用いた variant を用意すべきだと述べた。

Shamir は、単一ハッシュ関数と複数 mode に同意したが、mode は圧縮関数の内部構造を置き換えるべきではないと述べた。

Joux は、ランダムオラクルをシミュレートできる単一関数が望ましいと述べた。しかし、ここで streaming mode だけでこの点で十分というわけではなく、in-memory mode も必要であると述べた。

Ferguson は、multiple pass やメッセージ全体に対する randomly accessing を用いた variant は実装が難しいと述べた

Rivest は、ラウンド数を変えていくつかの異なる強度にできるようにすべきであると述べた。また、アルゴリズム仕様にラウンド数を減らしたバージョンを含めるべきだと述べた。

また、計算環境において low-end 版と high-end 版についても議論された。NIST は High-end に注力すべきだというコンセンサスが得られた。low-end 環境への実装は、それぞれのリス

クの中で行われるべきだという意見となった。

(4) 次のアルゴリズムの設計方法

このトピックでは、1から新しいアルゴリズムを作るのか、既存のアルゴリズムを修正するのかという点で議論が行われた。

Shamir は現在のアルゴリズムには問題が多いが、既存のアルゴリズムより安全あアルゴリズムのセットの代替はないと信じていると述べた。既存のアルゴリズムの修正が良いと述べた。

Fergusonは、AESプロジェクトの経過が良い手本であり、AESによってブロック暗号の設計が進んだように、hashにおいても同様になるであろうと述べた。

Shamirは、ハッシュ関数の公募は2種類のProposalを伴うだろうと述べた。1つは既存の修正で、もう 1 つは全く新しい関数。新しい関数の評価方法と既存の修正の評価のどちらが可能かという疑問を投げかけた。

Rivest は、新しいアルゴリズムが選ばれるとは思わないが、このような提案はハッシュ関数の研究を進めさせると述べた。

ここで、異なる応募者のアイディアの混合は可能かという疑問がでた。理論的にはあり得るが、問題点もある。

Joux は、公募はSHA-256への攻撃の研究を促進させると述べた。

ここで、性能とセキュリティの問題が議論された。これはトレードオフであり、固定のラウンドの関数では、性能のために安全性のマージンを犠牲にしてでも必要最低限なラウンド数を選ぶだろう。ShamirとRivestは、ラウンド数のパラメータ化が問題を解決すると述べた。

ここで参加者から、セキュリティレベルの考察が必要であるという意見が出た。SHA256の代わりに SHA-512 が必要かどうかなど。Ferguson は、SHA-256 は、データ長の関連でAES-256 との相性がよいと述べた。Shamir は、AES-128 with SHA-256 で十分であると述べた。

ここでパネリストは、再び既存アルゴリズムと新規のアルゴリズムの問題に戻った。公募の期間から考えると、まったく新しいアルゴリズムを考えることには問題がある。Preneelは、Markle-Dangaardに代わる構成法を検討するリスクをとっても良いのではないかと述べた。

Keynote Speech: Message Modification, Neutral Bits and Boomerangs: From Which Round Should we Start Counting in SHA?

この基調講演では、1998 年の SHA-0 の解析から、差分攻撃における複雑度のカウントについての疑問を述べた。まず、SHA-0 に関する基本的な攻撃について述べ、差分攻撃への対

応として SHA-1 に変わった理由を述べた。さらにブーメラン攻撃と自動化ツールについて述べた。現在の成果として、SHA-1 は 1998 年現在の SHA-0 よりも弱いと指摘した。

Session 4: New Design of Hash Functions

このセッションでは、ハッシュ関数の新しい構成法について議論された。最初の発表では、PANAMA ハッシュ関数を用いたアプローチについて発表した。これは Markle-Dangaard の代替である。SHA-1 と同等の性能を持ち、SHA-1 より安全であると主張した。2 番目の発表では、ハッシュ関数 LASH について議論された。LASH は性能の面で SHA と同等であり、SHA のセキュリティの問題を修正していると述べた。

Session 5: Cryptanalysis and Attack Tools

このセッションでは、攻撃に関する論文発表とパネルディスカッションが行われた。最初の発表で、攻撃とツールの概要が述べられた。圧縮関数とハッシュ関数におけるコリジョンを見つける一般的なアプローチについて議論を行い、差分パスと single-block collision を見つける方法、message modification と multiple block の利用についても議論を行った。

2 番目の発表では、SHA における複雑さ￥について自動的に探索するツールについての発表が行われた。方法を示すために、64step の SHA-1 に対して 2-block collision を示した。また、SHA-2 などの他のハッシュ関数への適用についての議論を行った。

3 番目の発表では、MD-5 タイプのハッシュの Collision 攻撃について、differential collision-path の確率を見積もる手法について議論された。MD5 の 3 つの near-collision の確率により算出されることが示された。またこの手法の SHA-1 への適用が議論された。

4 番目の発表では、SHA-1 に対する 1 round differential の自動的な探索について議論された。ここでは、最初のラウンドに関する differential path の発見で、2 つの探査木を用いることで自動化している。

5 番目の発表では、Wang による SHA-1 の攻撃の解析を示しており、十分条件と message modification 技法について述べている。

Session 6: More New Design of Hash Functions

このセッションでは、ハッシュ関数の新たな設計について議論された。最初の発表では新しいハッシュ関数 Edon-R が提案された。これは可変長出力を持つハッシュ関数である。

2 番目の発表は、expander graph から証明可能な安全性を有する Collision Resistant ハッシュ関数を構成する方法について述べている。構成例として楕円曲線から構成する例が示されている。

3 番目の発表では、新しい証明可能な安全性を有する Collision Resistant ハッシュ関数について提案しており、FFT を用いている。安全性は、Lattice における shortest vector

を見積もるのと同等であることが示されている。

Session 7: The Way Forward

このセッションは、Workshop のまとめとして開かれ、新しい結果の報告、新しいハッシュ関数公募のスケジュール、そして公開議論が行われた。

Stuart Haber は、ハッシュ関数を用いた integrity の保証を延長する方法についてプレゼンを行った。また、Lisa は HAMC と NMAC に対するハッシュの Collision を用いた偽造と partial key recovery attack について述べた。また、MD5 とラウンド数を減少させた SHA-1 についての 2nd pre-image resistance についてのべ、最後に HMAC-MD4 は安全ではないが HMAC-MD5 と HMAC-SHA1 については実用的な攻撃はないことを述べた。(以下、本論に記載の通り)

付録 5

FIPS186-3(Draft)と FIPS186-2 との相違点

表　　FIPS186-2 と FIPS186-3(Draft)の差異

<table>
<tr><th></th><th></th><th>FIPS186-2</th><th>FIPS186-3(Draft)</th></tr>
<tr><td>DSA</td><td>パラメータ</td><td>Pair L and N
<table><tr><th>The bit length of a prime modulus</th><th>The bit length of a prime divisor</th></tr><tr><td>512≦L≦1024</td><td>160</td></tr></table>※ 4. DSA PARAMETERS 章の a prime modulus の説明中に記載あり
※ Change Notice 1 において、1024 ビットの値のみ指定することになっていることに注意</td><td>Pair L and N
<table><tr><th>The bit length of a prime modulus</th><th>The bit length of a prime divisor</th></tr><tr><td>1024</td><td>160</td></tr><tr><td>2048</td><td>224</td></tr><tr><td>2048</td><td>256</td></tr><tr><td>3072</td><td>256</td></tr></table>※4.2 Selection of Parameter Sizes and Hash Functions for DSA 節に記載あり</td></tr>
<tr><td></td><td>セキュリティの強さ</td><td>記載なし</td><td>セキュリティの強さについては SP800-57 を参照</td></tr>
<tr><td></td><td>秘密鍵の生成</td><td>記載なし</td><td>1 メッセージあたりの秘密鍵の生成については付録 B.2 を参照</td></tr>
<tr><td></td><td>署名生成</td><td>FIPS180-1 で示される SHA-1(M)の値を利用する。</td><td>付録 D.2 に記載</td></tr>
<tr><td></td><td>検証</td><td>FIPS180-1 で示される SHA-1(M)の値を利用する。</td><td>付録 D.2 に記載</td></tr>
<tr><td>RSA</td><td>典拠</td><td>ANSI X9.31 に準拠
（それ以外の記載なし）</td><td>ANSI X9.31 に準拠</td></tr>
<tr><td></td><td>典 拠 (PKCS #1)</td><td>記載なし</td><td>This Standard references only version 2.1.
※5. The RSA Digital Signature Algorithm節で、明確にANS X9.31とPKCS#1を分けているので、上記項目と別途記載しました。</td></tr>
</table>

<table>
<tr><td></td><td>The length of the modulus</td><td>記載なし</td><td>1024 , or 2048 , or 3072 (choose)</td></tr>
<tr><td>ECDSA</td><td>典拠</td><td>ANSI X9.62-1998 に準拠
（それ以外は、推奨楕円曲線を記載）</td><td>基本的に ANSI X9.62-2005 に準拠。ただし、ANSI X9.62 には”cofactor h in the set of domain parameters”に制限はないが、FIPS186-3 では範囲を明確に指定している</td></tr>
<tr><td></td><td>Per-message secret number の生成</td><td>記載なし</td><td>付録B.5に記載</td></tr>
<tr><td></td><td>推奨楕円曲線</td><td>推奨楕円曲線（例）
<table><tr><th>CV Length</th><th>Algorithm</th><th>Prime Field</th><th>Binary Field</th></tr><tr><td>80</td><td>SKIPJACK</td><td>‖p‖ =192</td><td>m=163</td></tr><tr><td>112</td><td>Triple-DES</td><td>‖p‖ =224</td><td>m=233</td></tr><tr><td>128</td><td>AES Small</td><td>‖p‖ =256</td><td>m=283</td></tr><tr><td>192</td><td>AES Medium</td><td>‖p‖ =384</td><td>m=409</td></tr><tr><td>256</td><td>AES Large</td><td>‖p‖ =521</td><td>m=571</td></tr></table></td><td>推奨楕円曲線（例）
<table><tr><th>CV Length</th><th>Algorithm</th><th>Prime Field</th><th>Binary Field</th></tr><tr><td>80</td><td>SKIPJACK</td><td>‖p‖ =192</td><td>m=163</td></tr><tr><td>112</td><td>Triple-DES</td><td>‖p‖ =224</td><td>m=233</td></tr><tr><td>128</td><td>AES Small</td><td>‖p‖ =256</td><td>m=283</td></tr><tr><td>192</td><td>AES Medium</td><td>‖p‖ =384</td><td>m=409</td></tr><tr><td>256</td><td>AES Large</td><td>‖p‖ =521</td><td>m=571</td></tr></table>
※FIPS186-2との差異は見られない</td></tr>
<tr><td colspan="2">Cross Index</td><td>a. FIPS PUB 46-3 ⟹
〈Data Encryption Standard〉
b. FIPS PUB 73 ⟹
〈Guidelines for Security of Computer Applications〉
c. FIPS PUB 140-1 ⟹
〈Security Requirements for Cryptographic Modules〉
d. FIPS PUB 171 ⟹</td><td>〈削除〉
〈削除〉
a. FIPS PUB 140-2
〈Security Requirements for Cryptographic Modules〉
〈削除〉</td></tr>
</table>

	〈Key Management Using ANSI X9.17〉 **e.** FIPS PUB 180-1 ⟹ 〈Secure Hash Standard〉 **f.** ANSI X9.31-1998 ⟹ 〈Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)〉 **g.** ANSI X9.62-1998 ⟹ 〈Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)〉 追加 追加 追加 追加	**b.** FIPS PUB 180-2 〈Secure Hash Standard〉 **c.** ANS X9.31-1998 〈Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)〉 **d.** ANS X9.62-2005, 〈Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)〉 **e.** ANS X9.80 〈Prime Number Generation, Primality Testing and Primality Certificates〉 f. Public Key Cryptography Standard (PKCS) #1 〈RSA Encryption Standard〉 **g.** Special Publication (SP) 800-57 〈Recommendation for Key Management〉 **h.** Special Publication (SP) 800-89 〈Recommendation for Obtaining Assurances for Digital Signature Applications 〉 **i.** Special Publication (SP) 800-90 〈Recommendation for Random Number Generation Using Deterministic Random Bit Generators〉
ハッシュ関数	FIPS180-1	FIPS180-2 に示されるハッシュ関数
乱数生成	SHA-1 を使用した PRNGs を付録 3 に記載 ※ Change Notice 1 において、改訂がなされていることに注意	SP800-90 を参照

付録 6

第 62 回から第 65 回 IETF Meeting での議論の詳細

ハッシュ関数に関する議論を中心に、第 62 回から第 65 回 IETF Meeting での議論の詳細を記載する。

62nd IETF Meeting

[開催日]：2005 年 3 月 6 日-11 日

62nd Meeting では、saag WG において、Eric Rescorla により“Current Status of MD5 and SHA-1”というタイトルでのプレゼンテーションが行われ、ハッシュの危殆化に関する議論が行われた。プレゼンテーションおよび meeting における論点を、以下にまとめる。

[プレゼンテーション]

- ✓ MD5 および SHA-1 の攻撃状況に関する説明
- ✓ 「影響の無いと考える技術」、「影響があると考える技術」の例（表 1 参照）
- ✓ 証明書に対する攻撃や HMAC の安全性について概要
- ✓ 新しいハッシュ関数に関する問題提起（例として SHA-224 が挙げられている）

表 1　技術と影響

技術	
影響の無いもの	Key derivation functions(PRFs)
	SSL, IPsec, SSH など
	HMAC
	Challenge and Response
影響のあるもの	Non-repudiation
	証明書
	タイムスタンプ

[論点]

- ➢ 新しいハッシュアルゴリズムや randomize SHA-1 への変更
- ➢ 証明書の偽造防止対策と、その問題点
  - ✧ シリアルナンバの長さの変更
  - ✧ subject name への GUID の追加

- NIST の 2010 年のアルゴリズム移行について

63rd IETF Meeting

[開催日]：2005 年 7 月 31 日-8 月 5 日

63rd Meeting では、一方向性ハッシュ関数について検討する hash WG において、ハッシュの危殆化に関するプレゼンテーションが行われ、それに対する議論が行われた。プレゼンテーションおよび meeting における論点ついて、以下にまとめる。

[プレゼンテーション]

- ✓ Hash BoF (Introduction)
  - Paul Hoffman (VPN consortium)
- ✓ Collision Resistant Usage of SHA-1 via Message Pre-processing
  - Michael Szydlo (RSA Security) and Yiqun Lisa Yin(Independent consultant)
  - IETF として対応すべき内容について
    - ◆ ハッシュアルゴリズムの更新
      - ✧ 新しいハッシュ関数の選定
      - ✧ SHA-256 への移行
      - ✧ SHA-256 を 160bit に Truncate したものの使用などの延命策
    - ◆ プロトコルへの影響（署名サイズ、PKCS#1）
  - Randomize Hashing for signatures
    - Shai Halevi and Hugo Krawczyk (IBM Research) -
  - ハッシュ関数の危殆化が Provable Secure な署名アルゴリズムに与える影響について
  - 署名で用いるハッシュのランダム化されたハッシュの必要性
- ✓ Deploying New Hash Functions
  - Steve Bellovin (Columbia univ) and Eric Rescorla (Network resonance)-
  - ハッシュ関数の攻撃に対する影響について分析の必要性について
- ✓ Hash Truncation - Tim Polk -
  - 現在あるアルゴリズムを利用する方式として提案されている、ハッシュ値の Truncate の方式について

［論点］

- ハッシュ対象メッセージに対する Pre-processing の技術の有効性について
- Randomized hashing における Initial Value(IV)について
- ランダム性の程度について
- ランダム化することによる攻撃に対する耐性
- IETF で標準化されているプロトコルにおけるハッシュの影響について
- ハッシュ関数の危殆化と、IETF が行うべき範囲について

また、今後、影響のあるプロトコルに対して WG にて検討を行っていく必要があるとの意見が述べられた。その他、ハードウェアの計算速度の問題など、ハッシュ関数の標準化を行う際の要件についてのコメントも述べられ、その後の議論は、メーリングリストを用いて行うこととなっている。

64th IETF Meeting

［開催日］: 2005 年 11 月 6 日-11 日

64th Meeting では、saag WG, pkix WG, smime WG, tls WG において、ハッシュの危殆化に関するプレゼンテーションが行われ、それに対する議論が行われた。プレゼンテーションおよび meeting における論点について、以下にまとめる。

- Open Security Area Drectorate (saag)

✓ IETF Security Area Response to the Hash Function “Breaks”- Russ Housley -

- NIST の Workshop を受けた、SHA-256 への対応の必要性について
- SHA-256 への対応について
- 各プロトコルの更新の優先度について
- SHA-256 以外への変更について
- WG 内での各プロトコルに対する分析は 65th の meeting までに各 WG で実施することとなった。

✓ SHA-1 Hash Function Replacement

-Uri Blumenthal (Intel Corporation) and Charanjit Jutla (IBM Corporation)-

- SHA-1 をマイナーチェンジした SHA1-IME の使用について

- Public-Key Infrastructure (X.509) (pkix)

✓ OCSP Hash Algorithm Independence - Russ Housley -

- Basic OCSP Response における SHA-1 危殆化の影響と対応方法について

✓ Additional Cryptographic Profiles with SHA-2 - Tim Polk -

- ECDSA や DSA といった、SHA-2 ファミリーへの対応が成されていないものへの対応について

- S/MIME Mail Security (smime)

✓ Hash Transition Updates - Jim Schaad (Soaring Hawk Consulting) -

- ESSCertID における、SHA-1 危殆化の問題と、その対策について

✓ SHA-256 as a alternative digest - Blake Ramsdell (Sendmail, Inc) -

- S/MIME におけるダイジェストアルゴリズムへの SHA-256 適用について

- Transport Layer Security (tls)

✓ Hash Functions, MACs, and PRFs, oh my! - Eric Rescorla -

- MD5、SHA-1、HMAC に対する攻撃の状況について
- TLS において handshake message などで用いられている MD5 および SHA-1 の扱いについて

65th IETF Meeting

[開催日]: 2006 年 3 月 19 日-24 日

65th Meeting では、krb-WG, smime WG, pkix WG, pki4ipsec WG, msec WG, tls WG において、ハッシュ関数の危殆化への対応に関するプレゼンテーションと、それに対する議論が行われた。

具体的に変更を検討している WG では、NIST のコメントを受け、現在使用されている MD5, SHA-1 から、SHA-256 への移行が検討されている。現段階で、対応が終了している WG は無く、今後もそれぞれの WG が、各 WG の責任として、ハッシュの危殆化への対応についての検討を行っていくこととなっている。特に議論が進んでいるのは、S/MIME だが、その他の標準については、議論は行われるが SHA-1 の移行方法まで議論が進んでいないか、移行そのものに積極的ではない状況であり、足並みが揃っていない状況である。

また、一部の暗号技術に精通している参加者は MD5 はもちろんのこと、SHA-1 についても変更すべきとの意見が述べられていたが、IETF の参加者の大部分を占めている開発者の間では、SHA-1 に関しては、現時点では MD5 のような攻撃は成功しないため、代替案が明確となっていない現在の段階での対応には積極的では無い状況である。

全体を通しては、Algorithm Agility (アルゴリズムの変更に対する柔軟性) を規格として加えるかがポイントとなっているが、キーワードとして出ているものの、具体的な方向性の決定はなされていない。

プレゼンテーション、および meeting における論点について、以下にまとめる。

- Kerberos （krb-WG）
  - PKINIT、RFC4120 における Hash Agility（ハッシュ関数のアルゴリズムの変更に対する柔軟性）の確保について議論された。
  - RFC4121 も対象になるとの意見が出された。
  - 対応の検討については、2006 年 9 月以降に実施する方向。

- S/MIME （smime-WG）
  - ハッシュアルゴリズムの取り替えが必要であることが述べられた。
  - 問題を複雑にする要因として、移行時期が不明確であることが挙げられた。
  - 移行計画として、alternative digest profile の作成、移行時期に関するガイダンスの作成、文書の改訂方法などが議論された。
  - ESSCertID におけるデフォルトのハッシュ関数を SHA-256 にする提案が行われた。
  - 全体として、デフォルトのハッシュ関数を何にするのか、SHA-1 からの移行時期、移行対象についてのテーマが示されたが、具体的議論は行われなかった。
  - また、S/MIME においてハッシュ関数が利用されている処理が示された。この上で、ハッシュ関数を固定で定義するか否かについては、固定されるべきであるという意見が述べられた。

- PKIX （PKIX-WG）
  - 現在証明書で利用されているアルゴリズムは固定ではないが、範囲は決められているため、規格にないアルゴリズムを使う場合には、規格の変更が必要である。
  - RFC3279、RFC4055 で利用されている MD5、SHA-1 の SHA-2 への変更の提案
  - CMP/CMC などの CA-RA 間における証明書管理プロトコルについては、RSA1024 のままでも良いのではないかという意見が述べられた。
  - OCSP については、OID でハッシュアルゴリズムを規定するため、新規のアルゴリズムの規定が必要である。

- PKI4ipsec (pki4ipsec-WG)
  - ハッシュ関数については、RFC3280 を参照しているため、RFC3280 の対応に従う。
  - PKI IPSec においては、MD5 を利用すべきでないという意見が述べられた。
  - SHA-256 に移行した場合、規格上は、MD5 は”should not”の扱いにするが、SHA-1 については、”should not”にしなくてもよいのではないかという意見が

述べられた。

- Multicast Security （msec-WG）
  - SHA-1 と MD5 の代わりとして、SHA-256 をサポートすることが提案された。
    - SHA-256 対応（GROUP-PULL）
    - HMAC-SHA2-256 を指定（IPSec ESP SAs）
    - HMAC-SHA2-256 を選択可能にする（IPSec AH SAs）

- TLS （tls-WG）
  - TLS の中でハッシュ関数が使われている部分が示された。
    - 電子署名
      - handshake message の結合された MD5/SHA-1 への署名
      - DSA/ECC の SHA-1 に対する署名
      - DSA/ECDSA への SHA-1
    - KDF

- H-MAC について
  - TLS には直接影響がないと考えており、現在、具体的な脅威がない等の理由から、本当に先行的に移行すべきなのかという疑問が投げかけられた。

発行日　2007 **年** 4 **月** 23 **日 第** 1 **版**
発行者

- **〒** 184-8795
  東京都小金井市貫井北町四丁目 2 **番** 1 **号**
  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**
  文京グリーンコートセンターオフィス 16 **階**
  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
  BUNKYO GREEN COURT CENTER OFFICE
  2-28-8 HONKOMAGOME, BUNKYO-KU
  TOKYO, 113-6591 JAPAN