CRYPTREC Report 2009

平成 22 年 3 月

独立行政法人情報通信研究機構
独立行政法人情報処理推進機構

「暗号方式委員会報告」

目次

はじめに

本報告書は、総務省及び経済産業省が主催している暗号技術検討会の下に設置されている暗号方式委員会の 2009 年度活動報告である。

電子政府(e-Government)での利用に資する暗号技術のリストアップを目的として、暗号技術監視委員会の前身とも言える暗号技術評価委員会では、2000 年度から 2002 年度の 3 年間をかけて、暗号技術評価活動(暗号アルゴリズムの安全性評価)を推進してきた。その結果、2003 年 2 月に、暗号技術検討会を主催する総務省、経済産業省が電子政府推奨暗号リストを公表する運びとなり、暗号技術評価活動も一区切りを迎えた。2003 年度からは、電子政府推奨暗号の安全性の監視等を行う「暗号技術監視委員会」と電子政府推奨暗号を実装する暗号モジュールの評価基準・試験基準の作成等を行う「暗号モジュール委員会」の 2 委員会の体制になった。

2009 年度からは、それぞれ「暗号方式委員会」及び「暗号実装委員会」に名称を変更した上で、新たに「暗号運用委員会」を設置して、電子政府推奨暗号の適切な運用についてシステム設計者・運用者の観点から調査・検討を行うための活動を開始した。

暗号方式委員会は、旧暗号技術監視委員会と同じく、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。

2009 年度は、2013 年以降に利用を推奨する新しいリスト作成に向けて、「電子政府推奨暗号リスト改訂のための暗号技術公募（2009 年度）」を行い、計 6 件の応募があった。2010 年 3 月には、「CRYPTREC シンポジウム 2010」応募暗号説明会を開催し、応募された暗号技術に関する質疑・応答やパネルディスカッションを行い、暗号技術に関する活発な議論が交わされた。2010 年度の暗号方式委員会では、公募された暗号技術の安全性評価をはじめとして、電子政府推奨暗号リストの改訂に関する事項を審議していく予定である。また、暗号技術調査ワーキンググループ(WG)では、昨年度に引き続き、リストガイド WG を開催し、ID ベース暗号、ペアリング利用技術や擬似乱数生成器に関する調査を行った。

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ねばならない活動である。また、この活動は、暗号実装委員会及び暗号運用委員会との連携を保ちつつ、暗号技術やその実装及び運用に係る研究者及び技術者等の多くの関係者の協力を得て成り立っているものであることを改めて強調しておきたい。

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

暗号方式委員会　委員長　今井 秀樹

本報告書の利用にあたって

本報告書の想定読者は、一般的な情報セキュリティの基礎知識を有している方である。たとえば、電子政府において電子署名や GPKI システム等暗号関連の電子政府関連システムに関係する業務についている方などを想定している。しかしながら、個別テーマの調査報告等については、ある程度の暗号技術の知識を備えていることが望まれる。

本報告書の第 1 章は暗号方式委員会及び監視活動等について、第 2 章は電子政府推奨暗号リストの改訂について説明してある。第 3 章は今年度の監視活動、調査等の活動概要の報告である。第 4 章は暗号方式委員会の下で活動している暗号技術調査ワーキンググループの活動報告である。

本報告書の内容は、我が国最高水準の暗号専門家で構成される「暗号方式委員会」及びそのもとに設置された「暗号技術調査ワーキンググループ」において審議された結果であるが、暗号技術の特性から、その内容とりわけ安全性に関する事項は将来にわたって保証されたものではなく、今後とも継続して評価・監視活動を実施していくことが必要なものである。

本報告書ならびにこれまでに発行された CRYPTREC 報告書、技術報告書、電子政府推奨暗号の仕様書は、CRYPTREC 事務局（総務省、経済産業省、独立行政法人情報通信研究機構、及び独立行政法人情報処理推進機構）が共同で運営する下記の Web サイトで参照することができる。

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

本報告書ならびに上記 Web サイトから入手した CRYPTREC 活動に関する情報の利用に起因して生じた不利益や問題について、本委員会及び事務局は一切責任をもっていない。

本報告書に対するご意見、お問い合わせは、CRYPTREC 事務局までご連絡いただけると幸いである。

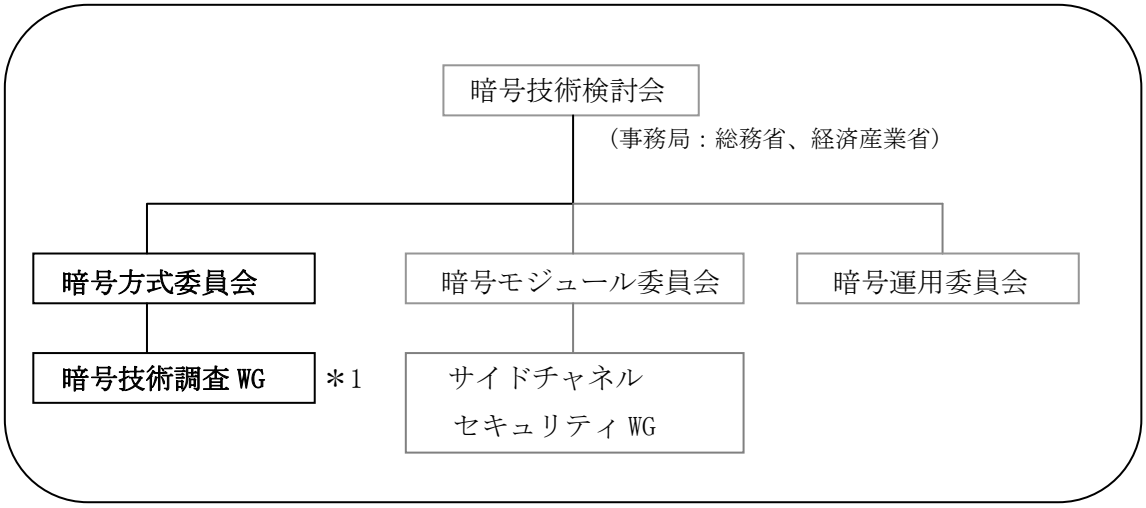
【問合せ先】　info@cryptrec.go.jp

委員会構成

暗号方式委員会(以下「方式委員会」)は、総務省と経済産業省が共同で主催する暗号技術検討会の下に設置され、独立行政法人情報通信研究機構(NICT)と独立行政法人情報処理推進機構(IPA)が共同で運営する。方式委員会は、暗号技術の安全性及び信頼性確保の観点から、電子政府推奨暗号の監視、電子政府推奨暗号に関する暗号アルゴリズムを主な対象とする調査・検討を適宜行う等、主として技術的活動を担い、暗号技術検討会に助言を行う。また、将来的には、電子政府推奨暗号リストの改訂に関する調査・検討を行う予定であり、暗号技術関連学会や国際会議等を通じての暗号技術に関する情報収集、関係団体の Web サイトの監視等を行う。

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

方式委員会と連携して活動する「暗号実装委員会」及び「暗号運用委員会」も、方式委員会と同様、暗号技術検討会の下に設置され、NICT と IPA が共同で運営している。



＊1 今年度実施されている調査項目：

・電子政府推奨暗号リストに関するガイドの作成

図 1　CRYPTREC 体制図

委員名簿

暗号方式委員会

委員長	今井 秀樹	中央大学 教授
顧問	辻井 重男	中央大学 教授
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	高木 剛	公立大学法人公立はこだて未来大学 教授
委員	田中 秀磨	独立行政法人情報通信研究機構 主任研究員
委員	松本 勉	国立大学法人横浜国立大学大学院 教授
委員	山村 明弘	国立大学法人秋田大学 教授
委員	渡辺 創	独立行政法人産業技術総合研究所 副研究センター長

暗号技術調査ワーキンググループ

委員	金岡 晃	国立大学法人筑波大学大学院 助教
委員	小林 鉄太郎	日本電信電話株式会社 研究主任
委員	白石 善明	国立大学法人名古屋工業大学大学院 准教授
委員	高島 克幸	三菱電機株式会社 主席研究員
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	花岡 悟一郎	独立行政法人産業技術総合研究所 研究員

オブザーバー

中嶋 良彰	内閣官房情報セキュリティセンター
山口 利恵	内閣官房情報セキュリティセンター
根本 農史	内閣官房情報セキュリティセンター
大橋 一夫	警察庁情報通信局[2009 年 7 月まで]
末澤 洋	警察庁情報通信局[2009 年 7 月より]
松本 和人	総務省行政管理局
藤井 信英	総務省地域力創造グループ[2009 年 8 月まで]
館　圭輔	総務省地域力創造グループ[2009 年 8 月より]
山﨑 敏明	総務省自治行政局
佐々木 信行	総務省情報流通行政局[2010 年 2 月より]
荻原 直彦	総務省情報通信国際戦略局[2009 年 7 月まで]
島田 淳一	総務省情報通信国際戦略局[2009 年 7 月より]
古賀 康之	総務省情報通信国際戦略局[2009 年 8 月より]
梶原 亮	総務省情報通信国際戦略局

齊藤 修啓	総務省情報通信国際戦略局
東山 誠	外務省大臣官房[2009 年 8 月まで]
荒木 美敬	外務省大臣官房[2009 年 8 月より]
山中 豊	経済産業省産業技術環境局
下里 圭司	経済産業省商務情報政策局
花田 高広	経済産業省商務情報政策局[2009 年 5 月まで]
池西 淳	経済産業省商務情報政策局[2009 年 5 月より]
坂下 圭一	防衛省運用企画局
千葉 修治	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
大塚 玲	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、田中秀磨、松尾真一郎、王立華、黒川貴司、金森祥子、赤井健一郎、持永大）

独立行政法人情報処理推進機構（矢島秀浩、山岸篤弘、大熊建司、神田雅透、小暮淳、近澤武、星野文学、鈴木幸子）

第 1 章　活動の目的

1.1 電子政府システムの安全性確保

電子政府、電子自治体における情報セキュリティ対策は根幹において暗号アルゴリズムの安全性に依存している。情報セキュリティ確保のためにはネットワークセキュリティ、通信プロトコルの安全性、機械装置の物理的な安全性、セキュリティポリシー構築、個人認証システムの脆弱性、運用管理方法の不備を利用するソーシャルエンジニアリングへの対応と幅広く対処する必要があるが、暗号技術は情報セキュリティシステムにおける基盤技術であり、暗号アルゴリズムの安全性を確立することなしに情報セキュリティ対策は成り立たない。

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

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

CRYPTREC では、2005 年度にハッシュ関数の安全性評価を実施し、2006 年 6 月に SHA-1 の安全性に関する見解を公表した。これに基づき、第 1 次基本計画の年度計画である「セキュア・ジャパン 2007」では、「電子政府推奨暗号について、その危殆化が発生した際の取扱い手順及び実施体制の検討を進める」こととされ、NISC をはじめとする政府機関において、暗号の危殆化に備えた対応体制等を整備することが喫緊の課題であることが認識された。そして、2006 年度には素因数分解問題の困難性に関する評価を実施し、RSA1024 の安全性の評価を公表した。これらの SHA-1 及び RSA1024 に関する安全性に関する CRYPTREC からの見解に基づき、NISC が事務局を務める情報セキュリティ政策会議において「政府機関の情報システムにおいて使用される暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針」が決定されるに至った。

第 1 次基本計画に引き続いて、中長期計画(2009～2011 年度の 3 ケ年計画)として「第 2 次情報セキュリティ基本計画」が NISC の情報セキュリティ政策会議において 2009 年 2 月に決定され、同計画において、「「政府機関の情報システムにおいて使用される暗号アルゴ

リズム SHA-1 及び RSA1024 に係る移行指針」の策定時の経験を適切に継承し、安全性が低下した暗号について速やかに安全な暗号への移行を進める」こととされた。

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

1.2 暗号方式委員会

電子政府システムにおいて利用可能な暗号アルゴリズムを評価・選択する活動が2000年度から2002年度まで暗号技術評価委員会（CRYPTREC: Cryptography Research and Evaluation Committees）において実施された。その結論を考慮して電子政府推奨暗号リスト（付録１参照）が総務省・経済産業省において決定された。

電子政府システムの安全性を確保するためには電子政府推奨暗号リストに掲載されている暗号の安全性を常に把握し、安全性を脅かす事態を予見することが重要課題となった。

そのため、2007年度に電子政府推奨暗号の安全性に関する継続的な評価、電子政府推奨暗号リストの改訂に関する調査・検討を行うことが重要であるとの認識の下に、暗号技術評価委員会が発展的に改組され、暗号技術検討会の下に暗号技術監視委員会が設置された。暗号技術監視委員会の責務は電子政府推奨暗号の安全性を把握し、もし電子政府推奨暗号の安全性に問題点を有する疑いが生じた場合には緊急性に応じて必要な対応を行うことである。さらに、暗号技術監視委員会は電子政府推奨暗号の監視活動のほかにも、暗号理論の最新の研究動向を把握し、電子政府推奨暗号リストの改訂に技術面から支援を行うことを委ねられている。

平成２０年度において、暗号技術監視委員会では、「電子政府推奨暗号リストの改訂に関する骨子（案）」及び「電子政府推奨暗号リスト改訂のための暗号技術公募要項（2009 年度）（案）」を策定したが、平成２１年度からは次期リスト策定のために新しい体制に移行し、名称を「暗号方式委員会」と変更した。また、平成２０年度に引き続き、暗号技術調査ワーキンググループ（リストガイド）において、電子政府推奨暗号リストの適切な利用のために、アウトリーチ活動として、暗号技術に詳しくない情報システム調達担当者及び運用担当者を対象とした、リストに係る技術的解説書として、電子政府推奨暗号リストガイドの作成を継続して行った。詳細については、第 4 章を参照こと。

1.3 電子政府推奨暗号リスト

平成１２年度から平成１４年度のCRYPTRECプロジェクトの集大成として、暗号技術評価委員会で作成された「電子政府推奨暗号リスト（案）」は、平成１４年に暗号技術検討会に提出され、同検討会での審議ならびに（総務省・経済産業省による）パブリックコメント募集を経て、「電子政府推奨暗号リスト」（付録１参照）として決定された。そして、「各府省の情報システム調達における暗号の利用方針（平成１５年２月２８日、行政情報システム関係課長連絡会議了承）」において、可能な限り、「電子政府推奨暗号リスト」に掲載された暗号の利用を推進するものとされた。

電子政府推奨暗号リストの技術的な裏付けについては、CRYPTREC Report 2002 暗号技術評価報告書（平成１４年度版）に詳しく記載されている。CRYPTREC Report 2002 暗号技術評価報告書（平成１４年度版）は、次のURLから入手できる。

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

なお、平成２１年度は、平成２０年度に検討した「電子政府推奨暗号リスト改訂のための暗号技術公募要項（2009 年度）」に基づき、電子政府推奨暗号リスト改訂のための暗号技術公募が行われた。

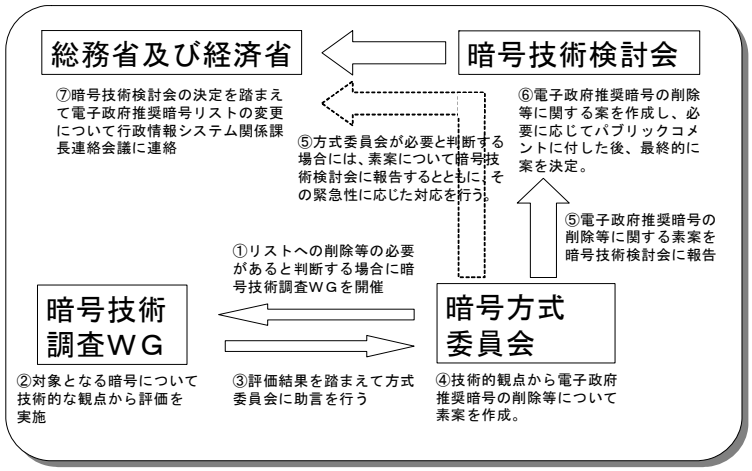
1.4 活動の方針

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

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

(1) 実運用環境において安全性に問題が認められた電子政府推奨暗号は原則としてリストから削除する。
(2) 電子政府推奨暗号の仕様変更は認めない。
(3) 電子政府推奨暗号の仕様変更に到らないパラメータの修正等の簡易な修正を行うことにより当該暗号の安全性が維持される場合には、修正情報を周知して当該暗号をリストに残す。

電子政府推奨暗号の削除等の手順



第２章 電子政府推奨暗号リストの改訂について

2.1. 改訂の背景

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

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

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

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

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

これらの状況を踏まえ、2012 年度、現リストを改訂することが必要である。

2.2. 改訂の目的

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

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

2.3. 電子政府推奨暗号リスト改訂のための暗号技術公募（2009 年度）

2.3.1. 公募の概要

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

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

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

暗号方式委員会、暗号実装委員会及び暗号運用委員会が、評価結果に基づき、「CRYPTREC 暗号リスト（仮称）」（以下、「次期リスト」という。）への暗号技術の記載について判定し、暗号技術検討会に答申する。答申された暗号技術の次期リストへの記載については、暗号技術検討会での検討を経た後、最終的に総務省及び経済産業省において決定される。決定については、2012 年度実施を予定している。

2.3.2. 2009 年度公募カテゴリ

2009 年度公募の対象となる暗号技術の種別は、以下の表 2.1 の通りである。ただし、主な留意事項としては、

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

等を挙げている。

表 2.1 2009 年度公募カテゴリの概要

2009 年度公募カテゴリ	仕様の概要
ブロック暗号	平文及び暗号文ブロックサイズが 128 ビットであり、鍵長が 128 ビット、192 ビット又は 256 ビットであるブロック暗号。
暗号利用モード	秘匿に関する 128 ビットブロック暗号及び 64 ビットブロック暗号を対象にした利用モード。
メッセージ認証コード	鍵長が 128 ビットである 128 ビットブロック暗号及び 64 ビットブロック暗号を利用したメッセージ認証コード。
ストリーム暗号	鍵長が 128 ビット以上であり、平文をビット単位もしくはバイト単位で暗号化するストリーム暗号。
エンティティ認証	共通鍵暗号技術、公開鍵暗号技術、MAC によるチャレンジ・レスポンスを用いたエンティティ認証。

2.3.3. 公募期間

2009 年 10 月 1 日～2010 年 2 月 4 日 17 時（必着）

2.3.4. 評価スケジュール

2012 年度の電子政府推奨暗号リストの改訂に向けた今後の応募暗号の評価スケジュールをまとめると以下の図 2.2 の通りである。

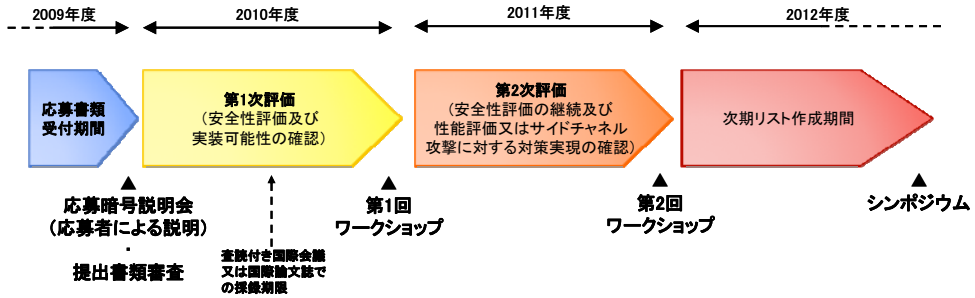


図 2.2. 評価スケジュール

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

2.3.5. 評価項目

安全性評価項目と実装性評価項目の２つに大別される。

（１）安全性評価項目

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

（２）実装性評価項目

提出資料に基づいて、実現可能性の確認を行います。性能の評価に関して、ソフトウェア実装では、標準的なプラットフォーム上での性能（処理速度、メモリ使用量等）を評価する。また、ハードウェア実装（エンティティ認証を除く）では、使用するプロセス（FPGA[1]、ASIC[2]等）別に性能（処理速度、使用セル数又はゲート数等）を評価する。また、一部の暗号技術に対しては、サイドチャネル攻撃に対する対策実現の確認も行う。

なお、今回公表した公募要項では、実装性評価の実施に際して、明確でない部分があるので、次年度以降に詳細を検討する必要がある。その結果は、CRYPTREC 統一 Web サイト（http://www.cryptrec.go.jp/）などを通じてアナウンスする予定である。詳細については、「電子政府推奨暗号リスト改訂のための暗号技術公募要項（2009 年度）」を参照のこと。

2.3.6. 応募暗号技術

下記のとおり 6 件の暗号技術について応募があった。

① 128bit ブロック暗号

・CLEFIA	ソニー株式会社
・HyRAL	株式会社ローレルインテリジェントシステムズ

② ストリーム暗号

・Enocoro	株式会社日立製作所
・KCipher－2	KDDI 株式会社

③ メッセージ認証コード

・PC-MAC-AES	日本電気株式会社

④ 暗号利用モード

なし

[1] FPGA：Field Programmable Gate Array

[2] ASIC：Application Specific Integrated Circuit

⑤ エンティティ認証

・無限ワンタイムパスワード認証方式（Infinite One-Time Password）

日本ユニシス株式会社

2.3.7. 事務局選出暗号技術

CRYPTREC におけるリストガイド策定時の検討結果などを参考に、国際標準化等の実績がある以下の暗号技術を暗号技術検討会の了承のもと選出した。

① 128bit ブロック暗号

なし

② ストリーム暗号

なし

③ メッセージ認証コード（リストガイド策定時の検討により選定）

・CBC-MAC

・CMAC

・HMAC

④ 暗号利用モード（リストガイド策定時の検討等により選定）

・CBC モード

・CTR モード

・CFB モード

・OFB モード

・CCM モード

・GCM モード

⑤ エンティティ認証（標準策定状況により選定）

・ISO/IEC 9798-2 共通鍵暗号利用による認証プロトコル

・ISO/IEC 9798-3 電子署名利用による認証プロトコル

・ISO/IEC 9798-4 検査関数（MAC）による認証プロトコル

2.3.8. CRYPTRECシンポジウムの開催

応募された暗号技術の評価を開始するにあたり、応募者自ら公の場で、応募暗号技術の技術仕様、安全性、実装性、公開状況、及びライセンス等について説明する機会を設けた。

また、CRYPTREC での最新の評価結果を公表し、それらを検討する場（ワークショップ）を設ける予定である。この機会を利用して、応募者が自らの意見を述べることもできる。

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

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

2.4. CRYPTRECシンポジウム 2010 ―応募暗号説明会―について

2.4.1. 開催目的

電子政府推奨暗号リストの改訂のための暗号技術公募（2009 年度）に応募された暗号技術についての現状の報告と、暗号研究の方向性や今後策定する CRYPTREC 暗号リスト（仮称）の在り方を議論するため、シンポジウムを開催することとした。

2.4.2. プログラムの概要

日時：3月2日（火）、3月3日（水）10：00～16：00
場所：コクヨホール
主催：独立行政法人情報通信研究機構(NICT)、独立行政法人情報処理推進機構(IPA)
共催：総務省・経済産業省
参加人数：約230名
プログラム： 下記の表2.3の通り

表 2.3　プログラム

3 月 2 日(火) (講演者敬称略)	
時間	内容(講演者)
10:00	開会挨拶(経済産業省)
10:10	講演 「2009 年度の CRYPTREC 活動の概要と今後について」 ・暗号技術検討会座長 今井秀樹(中央大学教授)
10:40	「応募状況について 1」 (CRYPTREC 事務局)
11:00	「応募暗号のプレゼンテーション 1」 ストリーム暗号 ・Enocoro　株式会社日立製作所 ・KCipher-2　KDDI 株式会社 メッセージ認証コード ・PC-MAC-AES　日本電気株式会社
12:30	昼休み
13:45	「公募カテゴリーの事務局選出暗号および評価についての事務局見解 1」 (CRYPTREC 事務局)
14:30	休　憩
14:45	パネル 1 「暗号技術の実装について」 モデレータ ・松本勉(横浜国立大学) パネリスト ・崎山一男(電気通信大学) ・佐藤証(産業技術総合研究所) ・中嶋純子(三菱電機株式会社)
16:00	挨拶(NICT)

3 月 3 日(水)(講演者敬称略)	
時間	内容(講演者)
10:00	挨拶(IPA)
10:10	講演 「暗号研究の普及と今後について」 ・暗号技術検討会顧問 辻井重男(中央大学教授)
10:40	「応募状況について 2」 (CRYPTREC 事務局)
11:00	「応募暗号のプレゼンテーション 2」 128bitブロック暗号 ・CLEFIA　ソニー株式会社 ・HyRAL　株式会社ローレルインテリジェントシステムズ エンティティ認証 ・無限ワンタイムパスワード認証方式　日本ユニシス株式会社
12:30	昼休み
13:45	「公募カテゴリーの事務局選出暗号および評価についての事務局見解 2」 (CRYPTREC 事務局)
14:30	休　憩
14:45	パネル 2 「公開鍵暗号技術の最新動向について」 モデレータ ・高木　剛(公立はこだて未来大学) パネリスト ・田中圭介(東京工業大学) ・宮地充子(北陸先端科学技術大学院大学) ・伊豆哲也(株式会社富士通研究所)
16:00	閉会挨拶(総務省)

2.4.3. 意見・コメントの概要

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

（1） 暗号技術の実装について

- 実装性評価の実施方針

(ア) 評価プラットフォーム

① ソフトウェア評価（PC環境／組み込み）について

- ソフトウェア実装評価の対象については、PCやサーバだけでなく、組み込み環境も重要である。
- ただし、同一環境での横並びの評価をするのが難しいため、評価環境に関する検討が必要である。

② ハードウェア評価（FGPA／ASIC）について

- ハードウェアの実装エリアの広さと処理速度のトレードオフを考慮すべきである、このトレードオフを定性的にグラフなどで表し、比較できることを評価基準に入れて欲しい。

(イ) 評価フローについて

① 使用言語（C言語／アセンブラ、Verilog／Custom Cell）の規定も検討すべきである。

② 多くのパラメータ(C言語のコンパイルオプション、実装条件等)も決める必要がある。

(ウ) 評価基準について

① 実装効率（例：スループット、レイテンシー、回路規模、消費電力）

- 実装効率のどの値を重視すれば良いのか選択が難しい。
- 実装効率毎の評価情報も必要である。

- サイドチャネル攻撃の実施方針

(ア) 安全性評価

- アルゴリズム評価と対物理攻撃耐性は分けて考えるべきである。

（2） 公開鍵暗号技術の最新動向について

- 共通鍵・RSA 暗号・楕円曲線暗号の間の等価安全性を評価し、暗号アルゴリズム・鍵長をいつまで安全に使用できるのかを評価して欲しい。
- 暗号アルゴリズム・暗号プロトコル・暗号実装の脆弱性情報をリアルタイムに提供して欲しい。

第３章 監視活動

3.1. 監視活動報告

電子政府推奨暗号の安全性評価について 2009 年度の報告時点では収集した全ての情報が「情報収集」、「情報分析」フェーズに留まり、「審議及び決定」には至らず、電子政府推奨暗号の安全性に懸念を持たせるような事態は生じていないと判断した。以降、収集、分析した主たる情報について報告する。

3.1.1. 共通鍵暗号に関する安全性評価について

Eurocrypt 2009 ランプセッションでフルラウンドの AES-256 に対する関連鍵攻撃が報告された。この報告を端緒とした一連の研究により、AES に対する暗号解析が大きく進展している。現時点における最良の攻撃は、いずれも関連鍵のシナリオで AES-256 に対して事前計算テーブルサイズ（データ計算量）$2^{99.5}$、実行時間（時間計算量）$2^{99.5}$、必要メモリーサイズ（領域計算量）2^{77}、AES-192 に対して事前計算テーブルサイズ 2^{123}、実行時間 2^{176}、必要メモリーサイズ 2^{152} と見積もられている。使用する鍵が独立な乱数とみなせる場合、これらの結果が現実的な脅威となることは無い。AES を理想暗号として使用するハッシュ関数、暗号利用モードあるいはメッセージ認証コードなどの理論的安全性については、これらの結果の影響を受ける可能性がある。また、ブロック長 64 ビット、鍵長 128 ビットの MISTY1 に対して積分攻撃を適用した結果、FL 関数を全部入れた 6 段(フルスペックは 8 段)が 2^{32} 個の選択暗号文と暗号化 $2^{126.1}$ 回分の計算量で攻撃可能との見積が示された。また、ブロック長・鍵長ともに 128 ビットの Camellia に対しては不能差分攻撃が有効で、FL 関数なしの 12 段を選択平文 $2^{116.3}$ 個、計算複雑度 $2^{116.6}$ で攻撃可能との見積が示された。

3.1.2. 公開鍵暗号に関する安全性評価について

素因数分解問題に関して、IACR[1] のCryptology ePrint ArchiveにThe RSA Factoring Challenge[2] のRSA-768（768 ビットRSA合成数）が一般数体篩法で素因数分解されたとの報告があった。数百台のPCを 2 年程度使用したとのこと。この結果はCRYPTRECで 2006 年度に実施した安全性評価の見解と良く一致している。

離散対数問題に関しては、SCIS 2010 にて GF($3^{6\cdot71}$)上の離散対数計算（676 ビット,位数の最大素因子 112 ビット）が関数体篩法で実現されたとの報告があった。100 コア弱の PC

[1] International Association for Cryptologic Research
[2] RSA 社(米国)の素因数分解問題に関するコンテスト。既に終了している。

を 1 月程度使用したとのこと。離散対数問題に関しても、素因数分解問題と同様に解析技術が向上していると考えられる。

楕円曲線上の離散対数問題に関しては、SHARCS 2009 にて 112-bit の素体楕円曲線離散対数計算が Pollard の ρ 法で実現されたとの報告があった。200 台の PlayStation 3 を半年程度使用したとのこと。

3.1.3. ハッシュ関数に関する安全性評価について

Crypto 2009 では段数縮小版 SHA-1 の原像攻撃可能段数が 48 段まで向上した事が報告された。また、Asiacrypt 2009 では、段数縮小版 SHA-256 と段数縮小版 SHA-512 に関して原像攻撃可能段数がそれぞれ 64 段中 43 段および 80 段中 46 段まで向上した事が報告された。これらおよび後述の完全版 MD5 の攻撃など、近年の原像攻撃の発展は概ね中間一致攻撃の高度化による成果である。

3.1.4. その他の暗号技術に関する安全性評価について

計算機の能力と解析アルゴリズムの向上に伴い、現実的な暗号応用システムの攻撃リスクが顕在化しており懸念が広がっている。

The 26th Chaos Communication Congress (26C3)にて、GSM 標準採用の A5/1 ストリーム暗号をリアルタイムに攻撃する為の公開事前計算テーブル作成プロジェクトに関する発表が行われた。この発表を契機として、携帯電話の通話秘匿に対する懸念が数多く報道されている。A5/1 および、その鍵長を制限した A5/2 は 20 年以上前に設計され世界中で使用されており、10 年以上前から沢山の攻撃が発表されている。GSM で使用する A5/1 の鍵長は実質的に 54 ビットであり、現在では汎用的攻撃が十分可能であると考えられている。A5/1 は国内の携帯電話網には採用されていない。

Eurocrypt 2009 では、一般のアプリケーションに多用されている MD5 ハッシュ関数に関して、理論的な原像困難性が否定された。衝突に関しては、既に数多くの現実的攻撃が知られており、X.509 公開鍵証明書の偽造（chosen-prefix collision attack）など現実的脅威も多数報告されている。

Eurocrypt 2009 ランプセッションにて、国際民間航空機関（ICAO）の次世代IC旅券などに採用されているISO/IEC9796-2:2002（RSA文書回復型署名）のScheme 1 に関して、パディング[3]の問題により現実的計算量で存在的偽造が可能な事が報告された。必要な署名の数などから、この攻撃が直ちに現実的脅威となる訳ではないが、今後新たな規格を考える場合は証明可能安全な方法を採用すべきとしている。

Asiacrypt 2009 ランプセッションにて、第三世代移動通信で採用されている A5/3

[3] 署名を生成する為のデータフォーマット

(KASUMI) ブロック暗号に対する実時間関連鍵攻撃が報告された。この攻撃は選択平文と関連鍵の両方の設定を必要としており、通話秘匿の攻撃などに直ちに適用できる訳ではない。

3.2. 暗号技術標準化動向

3.2.1. 米国NISTによる次世代ハッシュ関数SHA-3

米国NISTは、2009年7月24日に第2ラウンドに進むことができるSHA-3候補のハッシュ関数アルゴリズムを14個選出した。それらは以下の通りである。

表 3.1 第2ラウンドに進んだSHA-3候補一覧

BLAKE	Grøstl	Shabal
BLUE MIDNIGHT WISH	Hamsi	SHAvite-3
CubeHash	JH	SIMD
ECHO	Keccak	Skein
Fugue	Luffa	

選出したハッシュ関数に関する概要については、NISTが「Status Report on the First Round of the SHA-3 Cryptographic Hash Algorithm Competition」[4]として公表されている。また、次回の第 2 ラウンド SHA-3 候補会議は、2010 年 8 月 23・24 日に開催される予定である。

なお、NIST による SHA-3 評価・選定の結果を参考にして、国内における電子政府推奨暗号におけるハッシュ関数の推奨を行うことが考えられるため、CRYPTREC では NIST の評価プロセスに対して評価基準に関する提案を行うべく、電気通信大学、産業技術総合研究所、及び、NICT を主なメンバーとして、「ハードウエア評価に関する評価基準」及び「プロトコルの安全性を考慮した方式の安全性評価基準」について検討中であり、その結果を第 2 ラウンド SHA-3 候補会議にて発表する予定である。

3.3. 学会等参加記録

国内外の学術会議に参加し、暗号解読技術に関する情報収集を実施した。監視要員等を派遣した国際会議は、表3.2に示す通りである。

[4] http://csrc.nist.gov/groups/ST/hash/sha-3/Round1/documents/sha3_NISTIR7620.pdf

表 3.2 国際会議への参加状況

学会名・会議名		開催国・都市	期間
TCC 2009	Theory of Cryptography Conference	サンフランシスコ (米国)	2009 年 3 月 15 日～3 月 17 日
PKC 2009	International Conference on Practice and Theory in Public Key Cryptography	アーバイン (米国)	2009 年 3 月 18 日～3 月 20 日
Eurocrypt 2009	International Conference on the Theory and Applications of Cryptographic Techniques	ケルン (ドイツ)	2009 年 4 月 26 日～4 月 30 日
Pairing 2009	International Conference on Pairing-based Cryptography	パロアルト (米国)	2009 年 8 月 12 日～8 月 14 日
SAC 2009	Workshop on Selected Areas in Cryptography	カルガリー (カナダ)	2009 年 8 月 13 日～8 月 14 日
Crypto 2009	International Cryptology Conference	サンタバーバラ (米国)	2009 年 8 月 17 日～8 月 20 日
ECC 2009	Workshop on Elliptic Curve Cryptography	カルガリー (カナダ)	2009 年 8 月 24 日～8 月 26 日
FDTC 2009	Workshop on Fault Diagnosis and Tolerance In Cryptography	ローザンヌ (スイス)	2009 年 9 月 6 日
CHES 2009	Workshop on Cryptographic Hardware and Embedded Systems	ローザンヌ (スイス)	2009 年 9 月 6 日～9 月 9 日
SHARCS 2009	Special-purpose Hardware for Attacking Cryptographic Systems	ローザンヌ (スイス)	2009 年 9 月 9 日～9 月 10 日
Asiacrypt 2009	International Conference on the Theory and Application of Cryptology and Information Security	東京 (日本)	2009 年 12 月 6 日～12 月 10 日
FSE 2010	Fast Software Encryption workshop	ソウル (韓国)	2010 年 2 月 7 日～2 月 10 日

以下に、国際学会等に発表された論文を中心に、暗号解読技術の最新動向について述べる。

3.3.1. ブロック暗号の解読技術

・Distinguisher and Related-Key Attack on the Full AES-256 [Crypto 2009]
・Related-key Cryptanalysis of the Full AES-192 and AES-256 [Asiacrypt 2009]
Crypto 2009 において、ルクセンブルグ大の Dmitry Khovratovich らが、フルラウンドの AES-256 に対する関連鍵攻撃の発表を行い、データおよび時間の複雑度 2^{131}、メモリ量 2^{65} で 2^{35} 個の関連鍵のうちの 1 つを鍵回復できるとの見積もりを示した。この結果は Eurocrypt 2009 のランプセッションで紹介されたものと同じである。また、同研究グループは Crypto 2009 のランプセッションで、選択鍵のシナリオではなく全ての鍵に適用できる、4 個の関連鍵に対するブーメラン攻撃を使った関連鍵攻撃を発表し、フルラウンドの AES-256 に対してデータおよび時間複雑度 $2^{99.5}$、メモリ量 2^{77} で攻撃可能、フルラウンドの AES-192 に対してデータ複雑度 2^{123}、時間複雑度 2^{176}、メモリ量 2^{152} で攻撃可能と見積もった。これらの結果が AES を直接使う現実的なアプリケーションに対して今すぐ脅威となることは無いが、AES を使用したハッシュ関数の理論的安全性に関しては何らかの影響を与える可能性はある。また、今回の結果は、関連鍵攻撃に関する AES-256 の理論的安全性が AES-128 より低いという逆転現象が起こっていることを意味し、長期的な安全性を目標とした暗号システムの要素としてブロック暗号を使用する場合、関連鍵攻撃のシナリオが有効であるなら、AES 以外の暗号を使う必要が生じる可能性も考えられる（使用方法により安全性レベルが逆転する事は、使用者の立場からは好ましい状況ではない)。今後も攻撃技術の進展を継続的に監視し続ける必要がある。

・Key Recovery Attacks of Practical Complexity on AES variants with up to 10…[Crypto 2009 rump]
・Key Recovery Attacks of Practical Complexity on AES ... [ePrint 2009/374]
10 段の step-reduced AES-192 の実時間関連鍵攻撃.Crypto 2009 においてフルスペックの AES-192/-256 に対する関連鍵攻撃が発表されたが、計算量は現実的でない。そこで、現実的な計算量だと AES-256 が 14 段中何段まで攻撃可能か解析した結果、10 段まで攻撃可能という評価を得た。より具体的には、9 段縮小モデルでは、復号 2^{39} 回の計算量、関連鍵 2 個、選択暗号文 237 個(平文総数 2^{38} 個)、メモリ 2^{32} バイトで鍵の全 256 ビットが攻撃可能。10 段縮小モデルでは、復号 245 回の計算量、関連鍵 2 個、選択暗号文 2^{43} 個(平文総数 244 個)、メモリ 2^{33} バイトで鍵の全 256 ビットが攻撃可能だった。また、現実的に準じる(quasi-practical)ものとして、復号 2^{70} 回の計算量で 11 段まで攻撃可能という結果も示した。これらの関連鍵攻撃は、AES-CTR の利用において特に有効であるとしている。

・A Practical-Time Attack on the Encryption Algorithm Used in Third Gener… [Asiacrypt 2009 Rump]
・A Practical-Time Attack on the A5/3 cryptosystem used in third generation GSM [ePrint 2010/013]
携帯電話の規格 GSM では、第１及び第２世代において、通信の秘匿にストリーム暗号 A5/1 と A5/2 が使用されてきた。現在、これが第３世代に置き換わりつつあり、MISTY1 をベースとする KASUMI が A5/3 ブロック暗号として秘匿に利用されている。この論文では、フルラウンドの KASUMI が関連鍵とブーメラン攻撃の改良版であるサンドイッチ攻撃を使って、現実的な計算量で攻撃可能であることを示した。具体的には、KASUMI(フルスペックが 8 段)の 7 段が 2^{-14} という高い確率の識別子(distinguisher)を持つことを利用し、4 個の関連鍵、2^{26} 個のデータ(暗号文 2^{25} 個と対応する平文 2^{25} 個)、2^{30} バイトのメモリ、復号 2^{32} 回分の計算量で攻撃可能と評価した。なお、携帯電話電話の通常の利用においては、この攻撃が現実的な脅威となる可能性は低い。

・Improved integral attacks on Misty1 … [SAC 2009]
ブロック長 64 ビット、鍵長 128 ビットの MISTY1 に対して積分攻撃を適用した結果、FL

関数を全部入れた6段(フルスペックは8段)が2^{32}個の選択暗号文と暗号化$2^{126.1}$回分の計算量で攻撃できることを示した。

・New results on impossible differential cryptanalysis of reduced-round Camellia-128 … [SAC 2009]
ブロック長・鍵長ともに128ビットのCamelliaに対しては不能差分攻撃が有効で、今まで最も成功した攻撃は、SAC 2008でWuらが発表したFL関数なしの18段中12段で、選択平文2^{65}個、計算複雑度$2^{111.5}$だった。この発表では、Wuらの解析に誤りがありFL関数なしの12段は今まで攻撃できていなかったことを指摘し、今回、FL関数なしの12段を選択平文$2^{116.3}$個、計算複雑度$2^{116.6}$で攻撃できるという結果を示した。

3.3.2. ストリーム暗号の解読技術

・New Cryptanalysis of Irregularly Decimated Stream Ciphers [SAC 2009]
欧州のストリーム暗号研究プロジェクトeSTREAMにおいて、ハードウェア向け方式として最終候補(Phase 3)に残ったDECIMv2とDECIM-128は、Krawczykのパラメータを使った収縮生成器(shrinking generator)が使用されており、不規則に破棄する(irregularly decimated)ストリーム暗号と呼ばれる。この論文では、相関攻撃を改良することにより、この収縮生成器を使った機構に対する従来よりもずっと良い相関を発見し、それを使って、初期状態を復元する攻撃法に対する安全性を評価した。その結果、DECIMv2(192ビットLFSR使用)は160ビット縮小版が、DECIM-128(288ビットのLFSRを使用)は256ビット縮小版が、初期状態についての総当たり攻撃より効率であると評価した。具体的には、160ビット縮小DECIMv2では、計算量が操作$2^{76.3}$回分、メモリが$2^{71.3}$ビット、データが$2^{35.1}$ビット必要。また、256ビット縮小DECIM-128では、計算量が操作2^{124}回分、メモリが2^{117}ビット、データが$2^{36.1}$ビット必要だった。同じ手法はストリーム暗号LILI-IIのフルスペックに対しても適用可能であり、計算量が操作$2^{72.5}$回分、メモリが$2^{24.1}$ビット、データが$2^{74.1}$ビットを必要とする。これらの結果は、DECIM族に対するtime/memory/dataトレードオフ以外の最初の自明でない解析結果である。DECIMv2は2009年にストリーム暗号の国際規格ISO/IEC 18033-4:2005に追加されている(ISO/IEC 18033-4:2005/Amd1:2009)。

・GSM-SRSLY? [26C3]
A5/1ストリーム暗号のリアルタイム攻撃を目的とする、公開事前計算テーブル（レインボーテーブル）作成プロジェクトに関する解説および計算資源募集の発表。この講演が契機となり、携帯電話の通話秘匿用暗号に対する懸念が数多く報道された。A5/1および、その鍵長を制限したA5/2は20年以上前に設計され世界中で使用されているが、国内の携帯電話網では基本的に採用していない。GSMで使用するA5/1の鍵長は実質的に54 bitであり、現在では汎用的攻撃が十分現実的であると考えられている。

3.3.3. ハッシュ関数の解読技術

・Preimages for Step-Reduced SHA-2 [Asiacrypt 2009]
SHA-2ファミリーはNISTがSHA-1の後継としたハッシュ関数であり、今まで衝突探索の研究は比較的進んでおり、SHA-256に対しては、Nicolic,I.とBiryukov,A.によるFSE 2008の論文、および、Indesteege,S.らによるSAC 2008の論文で、64段中24段まで衝突攻撃が提案されている。一方、原像攻撃の論文は少なく、筆者らの知る限り、Isobe.TとShibutani,T.がFSE 2009で示した24段という結果だけだった。Asiacrypt 2009では、中間一致を利用した原像攻撃をSHA-2族に適用した結果が報告された。
SHA-224は擬似衝突探索が43段まで可能で計算量$2^{219.9}$。
SHA-256は衝突及び擬似衝突の探索が43段まで可能で、計算量は各々$2^{254.9}$と$2^{251.9}$。
SHA-384は擬似衝突探索が43段まで可能で、計算量は2^{366}。

SHA-512 は衝突及び擬似衝突の探索が 46 段まで可能で、計算量は各々2^{509}と$2^{511.5}$。

・Short Chosen-Prefix Collisions for MD5 and the Creation of a Rogue CA Cert… [Crypto 2009]

MD5 に対し、冒頭のビットを特定の値に固定した(chosen-prefix)ときの衝突の探索法を提案するとともに、この衝突探索法を利用して、X.509 証明書の偽造に成功した。正当なシリアル番号や有効期限を要求したとき、X.509 証明書の偽造用の衝突を作るのに要する計算量は MD5 圧縮関数実行2^{49}回分だった。さらに探索法を改良することにより、単一ブロック衝突探索を MD5 圧縮関数実行2^{16}回分という現実的な計算量にまで削減した。

・Finding Preimages in Full MD5 Faster than Exhaustive Search [Eurocrypt 2009]

MD5 ハッシュ関数に対する原像攻撃を示した。本攻撃により、$2^{116.9}$の計算量により MD5 の準原像を求め、$2^{123.4}$の計算量により MD5 の原像を求めることができる。領域計算量は$2^{45}\times 11$ワードである。従来の最良の原像攻撃は2^{127}の計算量が必要であり、研究者によってはこれを MD5 の原像攻撃とは見なしていなかったが、今回は明確な（但し理論的な）原像攻撃となった。

・Could The 1-MSB Input Difference Be The Fastest Collision Attack … [Eurocrypt 2009 poster]

2004 年に Wang らは、どのブロックにも 3-bit の入力差分がある MD5 の 2 ブロック衝突差分を発見した。2007 年に Xie らも、同じ性質をもつ別の 2 ブロック衝突差分を発見している。これらの差分は後にそれぞれ 1 分および 30 分以内にデスクトップ PC 上で衝突が発見出来るよう改良されたが、他の衝突差分、あるいは、より効率の良い衝突アルゴリズムが課題として残されていた。本研究では、1MSB 入力差分（ワード境界の MSB に差分があること）しか持たない新しい衝突差分を提案し、詳細に解析し、完全衝突差分特性を示した。この方法で衝突を生成するのには、まだ 2 ブロックメッセージが必要ではあるが、第一ブロックは 1MSB 差分しか持たず、第二ブロックは全く同じである（疑衝突）。新しい差分特性は明らかに計算困難であるが、衝突探索効率を劇的に改善する分割統治戦略を提案している。結果として、平均計算量が 2^{20.96}（単位 MD5 圧縮計算）の衝突攻撃アルゴリズムが得られた。これは、現在最速の攻撃であり、任意のランダムな初期値に対して一般的な PC 上で 1 秒以内に衝突を発見でき、妥当な確率で 1/1000 秒以内に衝突が見つかるとのこと。現実的なプロトコルの実行中の攻撃に使用することが出来る。

・MD5 is Weaker than Weak: Attacks on Concatenated Combiners [Asiacrypt 2009]

異なるハッシュ関数の入力を共通とし、各々の出力の連接を出力とするハッシュ関数結合(hash function combiner)は、個々のハッシュ関数の安全性低下に対する対策として利用され、実際に MD5||SHA-1 の形の結合が SSL 3.0/TLS 1.0 と TLS 1.1 に採用されている。Joux,A.は Crypto 2004 においてハッシュ関数結合に対する攻撃法を示し、計算量が birthday-bound を下回る攻撃法は可能かという問いを発し、それが今まで未解決の問題となっていた。この論文はこの問題に対する肯定的な回答を与えるもので、論文中で Type 3 と呼ばれる差分経路パターンに着目した衝突探索法を提案した。

・Meet-in-the-Middle Preimage Attacks Against Reduced SHA-0 and SHA-1 … [Crypto 2009]

これまで、中間一致攻撃をハッシュ関数の原像攻撃に利用する方法は、メッセージ・スケジュールがビット置換であるハッシュ関数にしか適用されていなかったが、この論分ではメッセージ･スケジュールが線形変換の場合にも使えるように拡張し､SHA-0 と SHA-1 に適用した。その結果、SHA-0 では圧縮関数計算$2^{156.6}$回で 52 ステップまで、SHA-1 では圧縮関数計算$2^{159.3}$回で 48 ステップまで、原像攻撃可能であると評価した。これまでの最良の結果は、Crypto 2008 で De Canniere らが示した、SHA-0 が 49 ステップ、SHA-1 が 44 ステップであった。この論文では最近開発された補助的な手法である､slice-and-cut、partial-fixing、initial structure が利用されている。

・SHA-1 Differentials for Boomerang Attack … [Crypto 2009 rump]

SHA-1 に対するブーメラン攻撃に必要な計算量を考慮し、25 ステップの差分パターンを導いた。計算量の評価には、高い差分確率とメッセージ生成の高速性が必要であるとし、１段の非線形確率とブーメラン攻撃の組み合わせに注目し、この差分を導いたとしている。導出の詳細は不明。

・Constructing New Differential Paths and Implementing Algebraic … for Full-SHA-1 [SCIS 2010]

SHA-1 の衝突探索の計算量評価としては、McDonald,C.らが Eurocrypt 2009 のランプセッションで示した 2^{52}(回分の圧縮関数計算)が最小であるが、本論文は発表されていない。この発表では、McDonald らの方法をグレブナー基底に基づいて定式化し直し、disturbance ベクトルから差分経路と十分条件を自動的に導く方法や新しい手法（段ごとの準中立ビット、広域ブーメラン、適応的増幅ブーメラン）を適用した。その結果、McDonald らによる新しい disturbance ベクトルに基づくフルスペックの SHA-1 に対する十分条件を導くことに成功した。この結果に基づいて評価した、衝突探索に必要な計算量は 2^{60} 程度ということである。

・Improved generic algorithms for 3-collisions [Asiacrypt 2009]

関数の r-衝突とは出力が等しい r 個の異なる入力の組のことである．要素数 N の有限集合上のランダム写像の r-衝突発見には、逐次機械上で少なくともおよそ N^{(r-1)/r} の時間計算量を要する．r = 2 は良く研究されており，無視しうるサイズの領域計算量で効率よく並列化出来るアルゴリズムが知られている．本論文では r >= 3 の時，領域効率が良く並列化可能なアルゴリズムを研究している．こうした多衝突発見アルゴリズムは、ハッシュ関数の攻撃ツールとしての応用が知られており，本結果を利用して AURORA-512 の攻撃に必要な記憶領域の削減が可能とのこと．この論文は Asiacrypt 2009 の最優秀論文賞に選ばれた．

・Cryptanalysis of MDC-2 [Eurocrypt 2009]

本論文では MDC-2 に対する衝突攻撃および原像攻撃を示した。MDC-2 は、1988 年に IBM の研究者 Meyer と Schilling らにより提案された、n ビットブロック暗号から 2n ビットハッシュ関数を構成する方法であり、１９９０ 年 3 月に US 特許が発行され、1994 年に ISO/IEC 10118-2 で標準化された。衝突攻撃では、ベースとなるブロック暗号には非標準的なことは仮定せずに、バースデイ境界を下回る攻撃を示す。例えば 128 ビットブロック暗号で MDC-2 によりハッシュ関数を構成した場合、本衝突攻撃の計算量は約 $2^{124.5}$ となる。また、原像攻撃では、タイムメモリトレードオフとなる方法であり、時間計算量と空間計算量との積は約 2^{2n} となり、空間計算量は $1 \sim 2^n$ の間の値を取る。これまでの最良の攻撃は 1992 年に Eurocrypt で発表された Lai/Massey らによる、時間計算量約 $2^{3n/2}$、空間計算量約 $2^{n/2}$ となる攻撃である。本論文の攻撃では、時間計算量は約(n+1) 2^n、空間間計算量は約 2^{n+1} となる。

・How Risky is the Random-Oracle Model [Crypto 2009]

本論文では RSA-PSS、PKCS #1 v2.1、IEEE P1363 他、非常にたくさんの規格で採用されている任意出力長ハッシュ関数（ハッシュ関数を複数回呼んで大きい値域のハッシュ関数を構成するモードの一種）をランダムオラクルと仮定する事は非常に危険であると主張している。1024 bit メッセージ要約に関して、Bellare-Rogaway’93 に対する計算量 2^{67}の原像攻撃、Bellare-Rogaway’96 に対する 2^{106}の衝突攻撃が示された。また、PKCS や IEEE 標準で暗に提示されている任意出力長ハッシュ関数の具体例について、出力サイズによらず SHA-1 の衝突から直接的に衝突が構成できるとの注意が与えられている。さらに Coron らによる理論的な構成に関しても、利用する暗号プリミティブが MD5 や SHA-1 である場合にはその暗号プリミティブ自身より衝突に対して強くなる事はない事を示している。この結果がすぐ現実的脅威となることは無いであろうが、MD5 や SHA-1 の脆弱性については既報の通りであり、今後の進展について継続的に監視する必要がある。

・On Randomizing Hash Functions to Strengthen the Security of Digital … [Eurocrypt 2009]

メッセージランダム化アルゴリズム RMX を使用した hash-then-sign 電子署名スキームに対する存在的偽造攻撃を示した。Crypto 2006 で Halevi と Krawczyk は、hash-then-sign 署名スキームが、ハッシュ関数の耐衝突性に安全性を依存しないよう、ハッシュの前にメッセージをランダム化する手法(RMX)を示した。2008 年の NIST Special Publication(SP) 800-106(2nd ドラフト)には、RMX の variant が記載されている。本論文では、Ｍｅｒｋｌｅ－Ｄａｍｇａｒｄハッシュ関数の第二原像を求める Dean のテクニック(固定点拡張可能メッセージ)を使用し、Davies-Meyer 圧縮関数を使う t ビットの RMX ハッシュ関数をベースとした署名スキームに対し、$2^{t/2}$ の選択メッセージ、$2^{t/2+1}$ の(オフライン)圧縮関数計算、$2^{t/2}$ のメモリにより、存在的偽造を行う方法を示す。

3.3.4. 公開鍵暗号の解読技術

・Factorization of a 768-bit RSA modulus [ePrint 2010/006]
RSA factoring challenge の 768 ビット(10 進 232 桁)合成数 RSA-768 の素因数分解に成功した(これまでの世界記録は、663 ビット、10 進 200 桁)という報告が IACR ePrint Archive(2010/006)に掲載された。スイス連邦工科大学ローザンヌ校、日本電信電話株式会社、ドイツ・ボン大学、フランス・国立情報学自動制御研究所、アメリカ・マイクロソフト研究所、オランダ・国立情報工学・数学研究所らの共同研究により、一般数体篩法を用いて約 2 年間で達成された。計算量の支配的なステップは以下の処理である。

篩処理：Opteron 2.2GHz 換算で 1500 年
線型代数処理：Opteron 2.2GHz 換算で 155 年

CRYPTREC Report 2006 における評価では、768 ビット篩処理の計算量を Athlon 64 2.2GHz 換算で 1108 年と見積もっており、評価の妥当性を示す実験結果と言える。

・Practical Cryptanalysis of ISO 9796-2 and Europay-Mastercard-Visa Signatures [Crypto 2009]
1999 年 Coron, Naccache, Stern は 2 つの普及していた RSA 署名標準 ISO/IEC9796-1,2 に対して存在的偽造を発見した。この攻撃を受けて、ISO/IEC 9796-1 は取り下げられ、ISO/IEC9796-2 はメッセージ要約の長さが最低 160bit となるよう修正された。この修正版への攻撃は少なくとも 2^{61}の演算が必要であるとされた。本研究では、アルゴリズムの改良により、修正版の ISO/IEC9796-2 のどのサイズの法に対しても攻撃が可能となることを示した。素因子が知られていない RSA-2048 challenge modulus に対し、e=2 の場合に、Amazon EC2 grid 上の 19 個のサーバを用いて、たった 2 日で現実的な偽造を構成出来たと報告されている。指数が奇数の場合でもそれほど時間が延びるわけではないとのこと。この結果は “Practical Cryptanalysis of ISO/IEC 9796-2 and EMV Signatures” のタイトルで CRYPTO 2009 に受理された。

・GF(3^(6・71))上の離散対数計算実験（676 ビットの解読） [SCIS 2010]
関数体篩法により、GF(3)の 6×71 次拡大体(676 ビット)における離散対数計算に成功し、世界記録を更新した(これまでの記録は GF(2)の 613 次拡大)。関係探索ステップでは 96 コアの計算機で約 18 日、線型代数ステップでは 80 コアで約 0.5 日、特定の元の離散対数計算ステップでは 48 コアで約 14 日を費やした。

・Pollard Rho on the PlayStation 3 [SHARCS 2009]
SHARCS2009 において、スイス連邦工科大学ローザンヌ校およびアメリカ・マイクロソフト研究所により、112 ビット素体上楕円曲線離散対数問題の解読に成功した(これまでの世界記録は Certicom Challenge の 109 ビット)と報告された。攻撃対象の楕円曲線は、SEC2 では secp112r1、Wireless Transport Layer Security Specification では curve number 6 として標準化されているもの。標準では生成元の点しか与えられていないが、ターゲットの点として、x 座標が(π-3)×10^{34}(整数部)となるものを取ることによりランダム性を保証している。解読は、Pollard の ρ 法を 200 台の PlayStation3 で実行することにより約半年(連続使用であれば 3.5 ヶ月と見積もられる)で行われた。

・The Certicom Challenges ECC2-X [SHARCS 2009]
・Breaking ECC2K-130 [ePrint 2009/541]
SHARCS2009 において、18 名の著者により、Certicom ECC challengeのうち、ECC2K-130、ECC2-131、ECC2K-163、ECC2-163 関して、様々なプラットフォーム(FPGA/ハードウェア/ソフトウェア)上でのパラレルρ法による解読計算量に関する評価が発表された。それによると、ECC2K-130(130 ビットKoblitz曲線)の解読には、$2^{60.8}$ のρ法iteration関数呼び出しが必要であるが、実現可能であるとのこと。同著者らを含む 23 名の著者による ECC2K-130 解読実験の途中経過報告が、IACR ePrint Archive(2000/541)に掲載されており、それによると複数プラットフォームによる解読実験を 2009 年 10 月から開始しており、2010 年前半には解読に成功する見込みとのこと。その後の経過は、ウェブサイト(http://ecc-challenge.info/)に逐次報告されている。

・楕円曲線暗号とＲＳＡ暗号の安全性比較 [SCIS 2010]
素因数分解問題や楕円離散対数問題の実用的パラメタにおける困難さの理解が進んだ. 従来 1024 bit の RSA は 160 bit の楕円曲線暗号と同等の強度と認識されていたが、この評価によると 136 ～ 142 bit の楕円曲線暗号と同等の強度しか持たない. 他のパラメタの評価については以下の通り.

表 4.4.4.1 現実的計算量の等価なパラメタサイズの見積もり (単位 bit)

共通鍵暗号(全数探索)	素因数分解(RSA)	楕円離散対数(素体)	楕円離散対数(２の拡大体)	楕円離散対数(Koblitz 曲線)
56	696	105	104	110
60	768	113	111	117
64	850	121	119	125
72	1024	137	136	142
80	1219	151	150	156
92	1536	176	174	181
108	2048	205	203	210
112	2206	213	212	219
128	2832	244	243	250
192	6281	370	369	376
256	11393	596	495	503

・Factoring pq^2 with Quadratic Forms: Nice Cryptanalyses [Asiacrypt 2009]
本論文では N=pq^2 型の整数を素因数分解する二元二次形式に基づく新しいアルゴリズムを提案している. 一般に, その実行時間は指数時間となるが, 特殊な(算術的)ヒントが利用出来るときは多項式となる. 90 年代末期に提案された二次体に基づく公開鍵暗号, いわゆる NICE ファミリーに対する攻撃がまさにこの場合に相当する. この暗号系には二次体の虚実に従って二種類の版が存在する. 本論文のアルゴリズムは NICE のどちらの版に対しても機能し, 多項式時間一般鍵回復攻撃を実現する. Castagnos と Laguillaumie は最近 虚-NICE の完全解読を与えたが, この攻撃は 実-NICE には適用できなかった. 本論文のアルゴリズムは CL 攻撃と同様に 虚-NICE の公開鍵をヒントとして効率の良い素因数分解を与えるが, 実-NICE の場合でも, 二次体 Q(√p)の単数規準が著しく小さいという知識を使って効率の良い素因数分解を与える事が出来る. 一般的な N=pq^2 型の素因数分解ではこのアルゴリズムは指数時間で, 一般化(ESIGN の場合など)については未解決とのこと.

・Reconstructing RSA Private Keys from Random Key Bits … [Crypto 2009]
RSA 公開鍵の指数が小さく、かつ秘密ビットのうち 27%以上が漏洩した場合に、秘密鍵が解読可能となることを示した。例えば Cold Boot 攻撃が可能な状況において、本攻撃を適用することができる。本攻撃では、秘密情報 p、q、d、d mod p、d mod q のうちランダムな 27%のビット情報から秘密鍵を回復することができる。PKCS#11 に含まれる情報は

冗長と言える。

3.3.5. その他の解読技術

・Conditional Multiple Differential Attack on MiFare Classic Smart Cards [Eurocrypt 2009 rump]

MiFare は FeliCa（フェリカ）と同じ 13.56MHz の近距離無線通信技術を搭載した非接触 IC カードのシリーズで、12 億個の IC カード用チップと、500 万台のリーダが出荷されたと言われており、世界で最も普及した非接触型 RFID カードのシリーズである。1994 年 MIFARE Standard（MiFare Classic）が発表されると 1996 年には韓国ソウルの交通機関で採用され、以降、ロンドン、北京、台北、釜山、香港、ドイツ、オランダ、等の公共交通機関でも採用された。この MiFare Classic は ID カードや社員証、入館証、会員証等にも幅広く利用され、少なくとも 2 億枚以上の使用実績があると推計されている。2007 年 12 月にリバースエンジニアリングにより、MiFare Classic のアルゴリズムの解析や幾つかの脆弱性が報告されると、2008 年 3 月には、認証/暗号化アルゴリズムが特定され、効率的な鍵回復及びクローンカードの作成といった現実的な脆弱性が指摘されている。これらの指摘を受けて 2008 年 3 月に MiFare Classic の代替として 128 ビット鍵の AES を使った MiFare Plus いう拡張規格が発表され、成人識別 IC カード taspo 等に使用されている。従来、MiFare Classic のクローンカードを作成するには、使用されているカードリーダーを入手するか、通信傍受などの手段で通信履歴を入手する必要があった。本発表ではそうした手段を用いずに、カードに数百回の照会を行うだけでクローンカードが作成出来るとの報告が行われた。“THE DARK SIDE OF SECURITY BY OBSCURITY - and Cloning MiFare Classic Rail and Building Passes, Anywhere, Anytime”のタイトルで SECRYPT 2009 にて発表されたとのこと。

3.4. 暗号調査ワーキンググループ開催状況

2009 年度は、各ワーキンググループ（WG）が活動した主要活動項目は、表 3.3 の通りである。

表 3.3　2009 年度の主要活動項目

ワーキンググループ名	主査	主要活動項目
リストガイド WG	高木　剛	・ ID ベース暗号技術の電子政府への適用に応じた推奨される利用方法の調査 ・ ペアリングに依存しない ID ベース暗号の研究動向の調査 ・ 「擬似乱数生成系」の推奨仕様の調査

3.5. 委員会開催記録

2009 年度、暗号方式委員会は、表 3.4 の通り 2 回開催された。暗号技術調査ワーキンググループは、表 3.5 の通り計 3 回開催された。各会合の開催日及び主な議題は以下の通りである。

(1) 暗号方式委員会

表 3.4　暗号方式委員会の開催

回	年月日	議題
第 1 回	2009 年 8 月 5 日	活動方針の検討、監視状況報告
第 2 回	2010 年 2 月 18 日	WG 活動報告、監視情報報告、報告書の検討

(2) 暗号技術調査ワーキンググループ

表 3.5　暗号技術調査ワーキンググループ(リストガイド)の開催

回	年月日	議題
第 1 回	2009 年 9 月 1 日	WG 活動方針の検討、作業の割り振り
第 2 回	2009 年 10 月 22 日	調査内容の中間報告とその検討
第 3 回	2010 年 2 月 4 日	報告書案の検討

第４章 暗号技術調査ワーキンググループ

4.1. リストガイドワーキンググループ

4.1.1. 活動目的

2013 年から開始される、新たな電子政府推奨暗号リストの体系において、リストガイドは NIST における SP (Special Publication) 文書に相当する文書として定める予定であり、2008 年度には電子署名、メッセージ認証子、暗号利用モードのリストガイドを作成するとともに、近年技術的な成熟度が高まっている ID ベース暗号についての調査を行った。

本年度は、昨年度からの継続として、新たな技術のリストガイドの作成を行うとともに、昨年度の ID ベース暗号に関する調査において、調査が不足している点の追加調査を実施する。

4.1.2. 委員構成（敬称略、五十音順）

主査： 高木 剛（公立はこだて未来大学）
委員： 金岡 晃 （国立大学法人筑波技術大学）
委員： 小林 鉄太郎（日本電信電話株式会社）
委員： 白石 善明 （名古屋工業大学大学院）
委員： 高島 克幸 （三菱電機株式会社）
委員： 田中 秀磨 （独立行政法人情報通信研究機構）
委員： 花岡 悟一郎（独立行政法人産業技術総合研究所）

4.1.3. 活動方針

本年度の活動項目としては、ID ベース暗号に関する追加調査とリストガイドの拡充の、2 つの大きな項目を実施する。

IDベース暗号の追加調査

2008年度にIDベースワーキンググループにおいて、将来のCRYPTRECにおける評価を見据える形で、IDベース暗号に関する全般的な調査を行った。その結果、基本的な技術についての知見を得ることができた。一方で、現実のシステムに適用したときの適切な利用方法については、より多くの検討が必要であるとの結論に至った。

そのため、本年度の活動として、電子政府システムにおけるIDベース暗号利用のモデルケースを設定し、このモデルケースに対応して安全性および実装性の観点から利用方法に

ついての検討を行う。検討の手順としては、以下の進め方を想定している。
(1) 電子政府での利用が想定されるアプリケーション、および実装することが想定されるプラットフォームを設定する。
(2) (1)で設定した利用方法に対して、2008年度の調査結果を参考にしながら、安全性を考慮した技術（ペアリング、安全性仮定）の選択方法、実装性を考慮した技術の選択方法の比較検討を行い、推奨を示す。

リストガイドの拡充

本年度のリストガイド拡充の活動として、擬似乱数生成技術に関するリストガイドの作成を行う。擬似乱数生成については、ISO および、NIST において標準化が行われている。

一方で、CRYPTREC では、擬似乱数生成に関しては、電子政府推奨暗号リストにおける例示として取り扱われているのみとなっている。擬似乱数生成に関しては、一般的に互換性の必要性が低いため、暗号モジュール評価においても役立てるよう、一意に特定できる仕様をリストガイドとして記載することとする。

4.1.4 活動概要

ID ベース暗号については、(1)ID ベース暗号を現実のシステムに適用する場合の課題、(2)電子政府で想定されるアプリケーションでの推奨技術の検討、(3)ペアリングに依存しない ID ベース暗号の調査、の 3 点を検討することが決められた。

なお、(1)の内容については、PKIなどの既存のセキュリティ機構が保証するトラストの仕組みとIDベース暗号が保証するトラストを比較し、IDベース暗号に求められる課題についての議論を行った。(2)の内容については、NISCが提示している電子政府システムのモデル[1]について、どのモデルを検討対象とするかが議論され、Webサービスシステムと電子メールシステムが対象として選ばれた。

擬似乱数生成については、安全性、および著作権などの面での検討の結果、JCMVP での認証対象の技術について執筆することとなった。

上記の内容について、調査報告書としてとりまとめ、暗号方式委員会に報告した。

4.1.5 成果概要

2009 年度版のリストガイドは、ID ベース暗号のパートと擬似乱数生成のパートに分かれる。以下、2009 年度版のリストガイドの目次と記述内容を示す。

[1] 「情報システムの構築等におけるセキュリティ要件及びセキュリティ機能の検討に関する解説書」 2007 年 11 月 内閣官房情報セキュリティセンター

1 ID ベース暗号

1.1 ID ベース暗号の実システムへの適用

- ID ベース暗号を実社会に適用する際の課題、PKI における信頼との対比
- ID ベース暗号の利用が適する領域に関する提言

1.2 アプリケーションモデルとアプリケーションへの適用の際の実装

- 電子メールに応用した場合の実装と推奨(メールの暗号化)
- Web を利用した情報提供と管理に利用した場合の課題(認証)

1.3 ペアリングを用いない ID ベース暗号

- 格子理論を用いた ID ベース暗号(Gentry-Peikert-Vaikuntanathan、Agrawal-Boyen、Cash-Hofheinz-Kiltz、Peikert)の方式の概要、メリット・デメリット
- 格子理論に基づく暗号の特徴
- 平方剰余判定問題に基づく ID ベース暗号(Cocks、Boneh-Gentry-Hamburg)の方式の概要、メリット・デメリット

2 擬似乱数生成

- 擬似乱数生成の概要とセキュリティ要件
- 実装仕様
  - 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
  - ANSI X9.31 Appendix A.2.4 Using 3-Key Triple DES
  - ANSI X9.31 Appendix A.2.4 Using AES
  - Hash_DRBG
  - HMAC_DRBG
  - CTR_DRBG
- 方式間の比較

4.1.6 まとめ

本年度の活動では、ID ベース暗号の実システムへの適用事例、及び、擬似乱数生成系の推奨技術について検討した。活動結果をまとめた報告書を、「2009 年度版リストガイド」として公表しているので、詳細についてはそちらを参照して欲しい。

付録 1

電子政府推奨暗号リスト

平 成 15年 2月 20日
総　　務　　省
経　済　産　業　省

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

注釈：

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

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

(注 3)　新たな電子政府用システムを構築する場合、より長いブロック長の暗号が使用できるのであれば、128 ビットブロック暗号を選択することが望ましい。

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

1) FIPS46-3 として規定されていること

2) デファクトスタンダードとしての位置を保っていること

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

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

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

別添

電子政府推奨暗号リストに関する修正情報

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

付録 2

電子政府推奨暗号リスト掲載暗号の問い合わせ先一覧

1. 公開鍵暗号技術

暗号名	DSA
関連情報	仕様 ・NIST Federal Information Processing Standards Publication 186-2 (+ Change Notice) (January 2000, Change Notice 1 は October 2001), Digital Signature Standard (DSS) で規定されたもの。 ・ 参照URL <http://csrc.nist.gov/publications/PubsFIPS.html>

暗号名	ECDSA (Elliptic Curve Digital Signature Algorithm)
関連情報 1	公開ホームページ 和文：http://jp.fujitsu.com/group/labs/techinfo/technote/crypto/ecc.html 英文：http://jp.fujitsu.com/group/labs/en/techinfo/technote/crypto/ecc.html
問い合わせ先 1	富士通株式会社 電子政府推奨暗号 問い合わせ窓口 E-MAIL：soft-crypto-ml@ml.css.fujitsu.com
関連情報 2	仕様 ・ANS X9.62-2005, Public Key Cryptography for The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA) で規定されたもの。 ・参照URL <http://www.x9.org/> なお、同規格書は日本規格協会(http://www.jsa.or.jp/)から入手可能である。

暗号名	RSA Public-Key Cryptosystem with Probabilistic Signature Scheme (RSA-PSS)
関連情報	仕様 公開ホームページ ・PKCS#1 RSA Cryptography Standard (Ver.2.1) ・参照URL <http://www.rsa.com/rsalabs/node.asp?id=2124> 和文： なし 英文： http://www.rsa.com/rsalabs/node.asp?id=2005
問い合わせ先	〒100-0005 東京都千代田区丸の内 1-3-1 東京銀行協会ビルヂング 13F RSA セキュリティ株式会社 ソリューション営業本部 副本部長 齊藤賢一 TEL：03-5222-5210, FAX：03-5222-5270, E-MAIL：ksaito@rsasecurity.com

暗号名	RSASSA-PKCS1-v1_5
関連情報	仕様　公開ホームページ ・PKCS#1 RSA Cryptography Standard (Ver.2.1) ・参照URL <http://www.rsa.com/rsalabs/node.asp?id=2124> 和文：　なし 英文：　http://www.rsa.com/rsalabs/node.asp?id=2125
問い合わせ先	〒100-0005 東京都千代田区丸の内 1-3-1 東京銀行協会ビルヂング 13F RSA セキュリティ株式会社 ソリューション営業本部 副本部長　齊藤賢一 TEL：03-5222-5210, FAX：03-5222-5270, E-MAIL：ksaito@rsasecurity.com

暗号名	RSA Public-Key Cryptosystem with Optimal Asymmetric Encryption Padding (RSA-OAEP)
関連情報	仕様　公開ホームページ ・PKCS#1 RSA Cryptography Standard (Ver.2.1) ・参照URL <http://www.rsa.com/rsalabs/node.asp?id=2124> 和文：　なし 英文：　http://www.rsa.com/rsalabs/node.asp?id=2146
問い合わせ先	〒100-0005 東京都千代田区丸の内 1-3-1 東京銀行協会ビルヂング 13F RSA セキュリティ株式会社 ソリューション営業本部 副本部長　齊藤賢一 TEL：03-5222-5210, FAX：03-5222-5270, E-MAIL：ksaito@rsasecurity.com

暗号名	RSAES-PKCS1-v1_5
関連情報	仕様 ・PKCS#1 RSA Cryptography Standard (Ver.2.1) ・参照URL < http://www.rsa.com/rsalabs/node.asp?id=2125>
問い合わせ先	〒100-0005 東京都千代田区丸の内 1-3-1 東京銀行協会ビルヂング 13F RSA セキュリティ株式会社 ソリューション営業本部 副本部長　齊藤賢一 TEL：03-5222-5210, FAX：03-5222-5270, E-MAIL：ksaito@rsasecurity.com

暗号名	DH
関連情報 1	仕様 ・ANSI X9.42-2003, Public Key Cryptography for The Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography で規定されたもの。 ・参照URL <http://www.x9.org/>　なお、同規格書は日本規格協会(http://www.jsa.or.jp/)から入手可能である。
関連情報 2	仕様 ・NIST Special Publication 800-56A (March 2007), Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revides) において、FCC DH プリミティブとして規定されたもの。 ・参照URL <http://csrc.nist.gov/publications/PubsSPs.html>

暗号名	ECDH (Elliptic Curve Diffie-Hellman Scheme)
関連情報 1	公開ホームページ 和文:http://jp.fujitsu.com/group/labs/techinfo/technote/crypto/ecc.html 英文:http://jp.fujitsu.com/group/labs/en/techinfo/technote/crypto/ecc.html
問い合わせ先 1	富士通株式会社 電子政府推奨暗号 問い合わせ窓口 E-MAIL：soft-crypto-ml@ml.css.fujitsu.com
関連情報 2	仕様 ・NIST Special Publication SP 800-56A (March 2007), Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revides) において、C(2,0,ECC CDH)として規定されたもの。 ・参照URL <http://csrc.nist.gov/publications/PubsSPs.html>

暗号名	PSEC-KEM Key agreement
関連情報	公開ホームページ 和文　http://info.isl.ntt.co.jp/crypt/psec/index.html 英文　http://info.isl.ntt.co.jp/crypt/eng/psec/index.html
問い合わせ先	〒180-8585 東京都武蔵野市緑町 3-9-11 日本電信電話株式会社　NTT情報流通プラットフォーム研究所 PSEC-KEM 問い合わせ窓口　担当 TEL. 0422-59-3462　　FAX. 0422-59-4015 E-MAIL: publickey@lab.ntt.co.jp

2. 共通鍵暗号技術

暗号名	CIPHERUNICORN-E
関連情報	公開ホームページ 和文：http://www.sw.nec.co.jp/middle/SecureWare/advancedpack/ http://www.nec.co.jp/access/prod/cipherunicorn.html
問い合わせ先	〒108-8558 東京都港区芝浦 4-14-22 日本電気株式会社　第一システムソフトウェア事業部 TEL：03-3456-3248, FAX：03-3456-7689 E-MAIL：info@mid.jp.nec.com

暗号名	Hierocrypt-L1
関連情報	公開ホームページ 和文：http://www.toshiba.co.jp/rdc/security/hierocrypt/ 英文：http://www.toshiba.co.jp/rdc/security/hierocrypt/
問い合わせ先	〒212-8582 神奈川県川崎市幸区小向東芝町 1 (株) 東芝 研究開発センターコンピュータ・ネットワークラボラトリー 主任研究員 秋山浩一郎 TEL：044-549-2156, FAX：044-520-1841 E-MAIL:crypt-info@isl.rdc.toshiba.co.jp

暗号名	MISTY1
関連情報	公開ホームページ http://www.mitsubishielectric.co.jp/corporate/randd/information_technology/security/code/misty01_b.html
問い合わせ先	〒100-8310　東京都千代田区丸の内 2-7-3（東京ビル） 三菱電機株式会社　インフォメーションシステム事業推進本部 情報セキュリティ推進センター　担当課長　畠山有子 TEL:03-3218-3406　FAX:03-3218-3638 E-MAIL:Hatakeyama.Yuko@aj.MitsubishiElectric.co.jp

暗号名	Triple DES
関連情報	仕様 ・NIST SP 800-67 (Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, May 2004) ・参照URL〈http://csrc.nist.gov/publications/nistpubs/800-67/SP800-67.pdf〉

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

暗号名	Camellia
関連情報	公開ホームページ 和文： http://info.isl.ntt.co.jp/crypt/camellia/index.html 英文： http://info.isl.ntt.co.jp/crypt/eng/camellia/index.html
問い合わせ先	〒180-8585 東京都武蔵野市緑町 3-9-11 日本電信電話株式会社　NTT情報流通プラットフォーム研究所 Camellia 問い合わせ窓口　担当 TEL. 0422-59-3456　　FAX. 0422-59-4015 E-MAIL: camellia@lab.ntt.co.jp

暗号名	CIPHERUNICORN-A
関連情報	公開ホームページ 和文：http://www.sw.nec.co.jp/middle/SecureWare/advancedpack/ http://www.nec.co.jp/access/prod/cipherunicorn.html
問い合わせ先	〒108-8558 東京都港区芝浦 4-14-22 日本電気株式会社　第一システムソフトウェア事業部 TEL：03-3456-3248, FAX：03-3456-7689 E-MAIL：info@mid.jp.nec.com

暗号名	Hierocrypt-3
関連情報	公開ホームページ 和文： http://www.toshiba.co.jp/rdc/security/hierocrypt/ 英文： http://www.toshiba.co.jp/rdc/security/hierocrypt/
問い合わせ先	〒212-8582 神奈川県川崎市幸区小向東芝町 1 (株) 東芝 研究開発センターコンピュータ・ネットワークラボラトリー 主任研究員 秋山浩一郎 TEL：044-549-2156, FAX：044-520-1841 E-MAIL：crypt-info@isl.rdc.toshiba.co.jp

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

暗号名	MUGI
関連情報	公開ホームページ 和文： http://www.sdl.hitachi.co.jp/crypto/mugi/ 英文： http://www.sdl.hitachi.co.jp/crypto/mugi/index-e.html
問い合わせ先	〒244-8555 神奈川県横浜市戸塚区戸塚町 5030 番地 (株) 日立製作所 ソフトウェア事業部 システム管理ソフトウェア本部　担当本部長　松永和男 TEL： 045-862-8498,　FAX： 045-865-9055 E-MAIL： kazuo_matsun.bz@hitachi.com

暗号名	MULTI-S01
関連情報	公開ホームページ 和文： http://www.sdl.hitachi.co.jp/crypto/s01/index-j.html 英文： http://www.sdl.hitachi.co.jp/crypto/s01/index.html
問い合わせ先	〒244-8555 神奈川県横浜市戸塚区戸塚町 5030 番地 (株) 日立製作所 ソフトウェア事業部 システム管理ソフトウェア本部　担当本部長　松永和男 TEL： 045-862-8498,　FAX： 045-865-9055 E-MAIL： kazuo_matsun.bz@hitachi.com

暗号名	RC4
関連情報	仕様 ・問い合わせ先RSA セキュリティ社(http://www.rsasecurity.co.jp/) ・仕様 RC4 のアルゴリズムについては、RSA Laboratories が発行した CryptoBytes 誌(Volume5, No.2, Summer/Fall 2002) に掲載された次の論文に記載されているもの。Fluhrer, Scott, Itsik Mantin, and Adi Shamir, "Attacks On RC4 and WEP", CryptoBytes, Volume 5, No.2, Summer/Fall 2002 ・参照URL <http://www.rsasecurity.com/rsalabs/cryptobytes/index.html>

3. ハッシュ関数

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

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

4. 擬似乱数生成系

暗号名	PRNG in ANSI
関連情報	仕様

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

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

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

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

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

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

付録 3　　学会等での主要論文発表等一覧

目次

1.1. 具体的な暗号の攻撃に関する発表

表 1 に具体的な暗号の攻撃に関する発表のリストをカテゴリー別に示す。★は電子政府推奨暗号の安全性に直接関わる技術動向、☆はその他の注視すべき技術動向である。

表 1 具体的な暗号の攻撃に関する発表

	ハッシュ関数	**頁**
☆	On Randomizing Hash Functions to Strengthen the Security of Digital Signatures [Eurocrypt 2009]	76
☆	Cryptanalysis of MDC-2 [Eurocrypt 2009]	76
・	Cryptanalysis on HMAC/NMAC-MD5 and MD5-MAC [Eurocrypt 2009]	76
☆	Finding Preimages in Full MD5 Faster than Exhaustive Search [Eurocrypt 2009]	76
★	Automatic Differential Path Searching for SHA-1 [Eurocrypt 2009 rump]	86
・	More Differential Paths for TIB3 [Eurocrypt 2009 rump]	86
☆	Could The 1-MSB Input Difference Be The Fastest Collision Attack For MD5? [Eurocrypt 2009 poster]	92
・	Practical collisions for SHAMATA-256 [SAC 2009]	100
・	Improved cryptanalysis of the reduced Groestl compression function, ECHO permutation and AES block cipher [SAC 2009]	100
・	Cryptanalyses of Narrow-Pipe mode of operation in AURORA-512 hash function [SAC 2009]	100
・	Cryptanalysis of the LANE hash function [SAC 2009]	101
・	Practical pseudo-collisions for hash functions ARIRANG-224/384 [SAC 2009]	101
・	Cryptanalysis of Dynamic SHA(2) [SAC 2009]	105
☆	Meet-in-the-Middle Preimage Attacks Against Reduced SHA-0 and SHA-1 [Crypto 2009]	107
☆	Short Chosen-Prefix Collisions for MD5 and the Creation of a Rogue CA Certificate [Crypto 2009]	107
・	MD5 Collisions Live [Crypto 2009 rump]	
・	A Live Trojan Message for MD5 [Crypto 2009 rump]	
・	SHA-1 Differentials for Boomerang Attack [Crypto 2009 rump]	
・	Near Collisions for the Compression Function of Hamsi-256 [Crypto 2009 rump]	
・	What happened to LANE? [Crypto 2009 rump]	
・	Finding Preimages of Tiger Up to 23 Steps [FSE 2010]	150
・	Cryptanalysis of ESSENCE [FSE 2010]	150
・	Security Analysis of the Mode of JH Hash Function [FSE 2010]	151
・	Higher Order Differential Attack on Step-Reduced Variants of Luffa v1 [FSE 2010]	152
・	Rebound Attack on Reduced-Round Versions of the JH [FSE 2010]	152
・	Pseudo-cryptanalysis of the Original Blue Midnight Wish [FSE 2010]	152
・	Differential and Invertibility Properties of BLAKE [FSE 2010]	153
・	Rotational Cryptanalysis of ARX [FSE 2010]	154
・	Super-Sbox Cryptanalysis: Improved Attacks for AES-like Permutations [FSE 2010]	154
	ストリーム暗号	
・	Cube Attacks on Tweakable Black Box Polynomials [Eurocrypt 2009]	79
・	Solving Low-Complexity Ciphers with Optimized SAT Solvers [Eurocrypt 2009 poster]	91
・	Cryptanalysis of the DECT Standard Cipher [FSE 2010]	149
	ブロック暗号	
★	AES-256 is Not Ideal [Eurocrypt 2009 rump]	85
・	Attacks on MRG ciphers [Eurocrypt 2009 rump]	85
・	Finding Good Linear Approximations of Block Ciphers and its Application to Cryptanalysis of Reduced Round DES [Eurocrypt 2009 poster]	90

	rump]	
•	New Birthday Attacks on Some MACs Based on Block Ciphers [Crypto 2009]	109
☆	How Risky is the Random-Oracle Model [Crypto 2009]	113
•	Solving Hidden Number Problem with One Bit Oracle and Advice[Crypto 2009]	
•	Hacking Helios and Its Impact [Crypto 2009 rump]	
•	Cross-VM Vulnerabilities in Cloud Computing [Crypto 2009 rump]	
•	Computing Scalar Multiplication with Many Cores [ECC 2009]	120
•	Security of compositions with implicit certificate schemes [ECC 2009]	119
•	A Practical Message Falsification Attack on WAP [JWIS 2009]	
•	Breaking the Myths of Extended Validation SSL Certificates [BlackHat 2009]	
•	MD5 Chosen-Prefix Collisions on GPU [BlackHat 2009]	

1.2. TCC 2009 の発表

1.2.1. TCC 2009 の発表(1 日目)

An Optimally Fair Coin Toss [TCC 2009]
Tal Moran; Moni Naor; Gil Segev

本論文ではコイン投げプロトコルのバイアス(出力分布の偏り) を研究している。Cleve の古典的な結果[STOC'86] によれば、如何なる 2-者 (two-party) r ラウンドコイン投げプロトコルに対しても、正直な参加者 (honest party) の出力に Ω(1/r) のバイアスを作る効率的な攻撃者が必ず存在する。一方で従来の r ラウンドプロトコルは、高々 O(1/√r) のバイアスしか保証しておらず Cleve の限界が最適(tight) なのか否かは 20 年以上もの間未解決問題であった。本研究では、紛失通信を仮定して、この問題に対して肯定的な結果を与えている。即ち、紛失通信が存在するならば正直な参加者の出力が高々 O(1/r) ほどのバイアスしか持たない r ラウンドプロトコルが存在する事を構成的に証明した。

Complete Fairness in Multi-Party Computation Without an Honest Majority [TCC 2009]
S. Dov Gordon; Jonathan Katz

プロトコルが公平性 (fairness) を持つとは、プロトコルが実行され正常または異常終了した時に、参加者全員が同時にプロトコルの出力結果を得るか何も学習出来ないかのどちらかの状態しか無い事を意味している。Cleve は大多数正直 (honest majority) でない時、プロトコルが完全公平性 (complete fairness) を持つ事は“一般には”不可能である事を証明した[STOC '86]。この結果を受け、完全公平に計算可能な非自明関数は存在しないとの誤解が長い間広がっていたが、Gordon らはある特定の非自明な関数が 2-者 (two-party) セッティングで完全公平に計算可能であることを示した[STOC '08]。本論文では Gordon らの結果の多者 (multi-party) セッティングへの拡張を研究している。k をセキュリティパラメタとし、n をプロトコル参加者数とする。また、プロトコル参加者を 2 つのグループに分割し、多者関数を無理やり 2-者関数と解釈する分析法を“分割 (partition) ”と呼ぶとする。本論文では適当な暗号学的仮定の下で次の結果を得た。

(1) あらゆる分割が 2-者関数として O(1) ラウンドで完全公平に計算できるが、多者関数としては O(log k) ラウンドでは完全公平に計算出来ない 3-者関数が存在する。(分割ベースアプローチに対する否定的な結果。多者の公平性は 2-者より本質的に難しい事の証左と主張している。)
(2) 3-者多数決関数 (3-party majority function) を完全公平に計算するω(log k) ラウンドプロトコルが存在する。(多者セッティングで完全公平性の実現可能性を示した最初の結果)
(3) n-者論理和関数 (n-party boolean OR function) を完全公平に計算するΘ(n)ラウンドプロトコルが存在する。

Fairness with an Honest Minority and a Rational Majority [TCC 2009]
Shien Jin Ong; David Parkes; Alon Rosen; Salil Vadhan

本論文では、閾値秘密分散系における単純で汎用的な秘密復元プロトコルを与え、それが少数の正直な参加者 (honest party) と多数の合理的参加者 (rational party) の下で実行されるとき、公平 (fair) であることを証明している。このプロトコルに従えば、少数の正直な参加者が正直にプロトコルに従い、多数の合理的参加者が己の利益に従って (摂動完全均衡の集合-Nash 均衡に相当する概念(set-Nash analogue of trembling hand perfect equilibrium) で捉えられるよう) 行動すれば、すべての参加者が高い確率で秘密を学習できる。このプロトコルは標準的な (同期的) 同報通信路しか必要とせず、早期停止 (early stopping) と不正文書 (incorrectly computed messages) の両方に耐性を持ち、たった 2 ラウンドのラウンド計算量しか必要としない。暗号学的あるいは経済学的モデルにおけるこの問題に対する従来のプロトコルは大多数正直 (honest majority) が必要であったか、同時交換可能な強い通信路を用いるか、安全性/均衡の近似概念に甘んじていたかのいずれかであった。それらは全て非定数ラウンドのラウンド計算量を必要としていた。

Purely Rational Secret Sharing [TCC 2009]

Silvio Micali; abhi shelat

合理的秘密分散（rational secret sharing）とは暗号とゲーム理論の学際領域の問題であり、各参加者が合理的（rational）に行動しさえすれば、主催者（dealer）の秘密を各々が必ず学習できる事を目的としている。従来の方法は単に合理性に依存するだけではなく、参加者の信念（belief）にも依存しており、しかも極めて非効率的であったので、本論文では、この問題のより完全な定義を与え、検証可能高信頼通信路（verifiable trusted channel）を用い、効率的で純粋に合理性のみに基づく解を示したとのこと。

Non-Malleable Obfuscation [TCC 2009]

Ran Canetti; Mayank Varia

どのようなプログラムの族（program family）に対しても適用可能な、汎用プログラム難読化（program obfuscation）が実現不可能である事は良く知られている。しかし、例えばパスワードチェックや対称鍵暗号化のような幾つかの有用なプログラム族に対する難読化は実現可能である。これらのプログラム族に対する従来の難読化の定義では、難読化プログラムの変造攻撃（malleability attacks）は排除されていない。本論文ではプログラム難読化に関する 2 通りの頑強性概念（functional non-malleability と verifiable non-malleability）を定式化し、それらは一般に異なる概念であることを示している。そして、有用なプログラム族に対する両方の型の頑強難読化法（non-malleable obfuscator）をランダムオラクルモデルまたは CRS モデル（common reference string model）で構築している。

Simulation-Based Concurrent Non-Malleable Commitments and Decommitments [TCC 2009]

Rafail Ostrovsky; Giuseppe Persiano; Ivan Visconti

本論文では非同期並列中間者攻撃（concurrent man-in-the-middle (cMiM) attack）に対して安全なコミットメント（commitment scheme）の研究を行っている。通常コミットメントの安全性は秘匿性(hiding)と束縛性(binding)によって定義される。競争入札のような応用を考えると、競合相手の入札(コミットメント)を、中間者攻撃により攻撃者が変造して 1 円高い入札が作成できてしまうような性質は望ましくない。従って hiding の定義として 1 ビットの情報も漏れない性質(強秘匿)では不十分であり、より強い性質である頑強性（non-malleability）が必要とされ、そうした性質を持つコミットメントは頑強コミットメント(non-malleable commitment)と呼ばれる。コミットメントには委託段階（commitment phase）と公開段階(opening phase)の2つの段階が存在するので、そのどちらの段階に対してもそれぞれ中間者攻撃を考えることができる。また、コミットメントの頑強性は元々コミットされた文書の独立性に基づき定義されていたが、より強力なシミュレーションに基づく定義が提案されている。本論文では、どちらの段階に対してもシミュレーションに基づいて非同期並列頑強性を持つコミットメントを提案している。本方式はプレインモデルで定数ラウンドの対話しか必要とせず、シミュレーションに基づく定義の下これらの性質をすべて満足する初めての方式であるとのこと。

Proofs of Retrievability via Hardness Amplification [TCC 2009]

Yevgeniy Dodis; Salil Vadhan; Daniel Wichs

Juels, Kaliski [JK07] により導入された、復元可能性証明（proof of retrievability, PoR）を用いると、何らかの(比較的大きい)データを信頼性の低い(遠隔)サーバ上に格納した後で、サーバがそのデータを保持していることを証明する監査プロトコルを効率的に実行できる。クライアントとサーバの記憶容量、監査の通信量、サーバが監査中にアクセスするファイルのブロック数を最小化すること等がこの分野の中心的課題となる。本論文では、幾つかの状況設定(使用回数限定-無制限など)においてこの問題を考え、それぞれに近最適な復元可能性証明系を与え、以下の結果を得た。

- Juels と Kaliski [JK07]の使用回数限定(bounded-use)PoR の変種に対する形式的安全性証明
- 通信量がセキュリティパラメタに対し線形で、ランダムオラクルに依存しない使用回数無制限(unbounded-use)の PoR。(Shacham-Waters[SW08]の未解決問題(Random Oracle 除去)解決)
- 初めての情報理論的安全な使用回数限定 PoR

本研究では、PoR と計算量分野で広く研究されている困難性増幅(hardness amplification)の概念の関連を研究し、PoR 符号(PoR codes)なる純粋に情報理論的な概念の抽象を行い、符号理論および計算量理論の既知の結果を用いて近最適な PoR 符号を構築することにより、この結果を得たとのこと。

Security amplification for interactive cryptographic primitives [TCC 2009]

Yevgeniy Dodis; Russell Impagliazzo; Ragesh Jaiswal; Valentine Kabanets

“弱安全 (weakly secure)” な暗号用基本関数 (cryptographic primitive) から ″強安全 (strongly secure)″ な同じ基本関数を構成する事は安全性増幅 (security amplification) と呼ばれ、暗号学の中心的な課題の一つである。従来、この問題は一方向関数、衝突困難ハッシュ関数、暗号系、および弱検証可能問題 (weakly verifiable puzzle) などの、多種多様な基本関数に対して継続的に研究されてきた。本論文では MAC、署名、擬似ランダム関数などの基本関数に対して安全性増幅を研究し、以下の結果を得た。

(1) 弱検証可能問題をより対話的な動的弱検証可能問題 (dynamic weakly verifiable puzzles) に一般化し、動的弱検証可能問題に対して新たにチェルノフ型の直積定理 (direct product theorem) を示した。
(2) 系として MAC/署名に対しては自然な直積定理が成立する事を示した。
    - チェルノフ型の直積定理は imperfectly completeness の時でも成立
(3) 系として疑似ランダム関数に対して自然な XOR 補題が成立する事を示した。
    - [May03] の反例(δ =1/2)は最悪ケース

Composability and On-Line Deniability of Authentication [TCC 2009]

Yevgeniy Dodis; Jonathan Katz; Adam Smith; Shabsi Walfish

否認可能認証(deniable authentication)は、メッセージ認証プロトコルの一種で、プロトコル完了時点で受信者は送信者がメッセージを認証したと確信できるが、どちらの参加者も相手がプロトコルに参加した事を他の誰かに確信させることは出来ないような2-者プロトコルの事である。一般的な電子署名はメッセージに一度署名を付けてしまうと否認出来ないため、署名者に不利な目的で署名が再利用されてしまう危険性がある。否認可能認証は、このような署名(あるいはプロトコルの履歴)の再利用を避けるために考案された。本論文では参加者の一方がプロトコル実行中に第三者と共謀したとしても否認可能性(deniability)が維持される実行時否認可能性(on-line deniability)の概念を導入し、従来モデルで無視されてきた攻撃を定式化し、実行時否認可能な否認可能認証と GUC メッセージ認証が等価である事を示した(Proposition 1)。そして、もし適応的買収(addaptive corruption)が可能なら、PKI モデルで GUC メッセージ認証は(従って否認可能認証も)実現不可能であることを示した(Theorem 1)。さらに、静的買収(static corruption)に対しては実現可能なこと(Theorem 3)や、上記の否定的な結果を回避するための条件緩和(deniability with incriminating abort)について論じている。

Authenticated Adversarial Routing [TCC 2009]

Yair Amir; Paul Bunn; Rafail Ostrovsky

この論文は、低信頼の同期的動的アドホックネットワーク上で送信者が指定した受信者にメッセージを送る際、大多数のネットワークノードが敵性(mallicious)で、どのノードが正直であるか不明な時、効率的な通信(ルーティング)が可能か否かを研究している。そして、

- 攻撃者は任意のノードを適応的敵性買収し、一旦買収されたノードは戻らない。
- 攻撃者は任意のエッジを操作して通信を停止あるいは開始することが出来る。
- 通信のどのステップでも送信者と受信者の間に必ず動作中のエッジで繋がった正直なノードの列が存在する。

なるセッティングの下で、一方向関数が存在するなら、あらゆる上記条件の多項式時間攻撃者に耐える線形スループットのルーティングが存在する事を構成的に証明した。但しノード当たり必要なメモリはノード数 n に対して $O(n^4 \log n)$で、多項式個ではあるが実用性に関して改善の余地があるとのこと。

1.2.2. TCC 2009 の発表(2 日目)

Adaptive Zero-Knowledge Proofs and Adaptively Secure Oblivious Transfer [TCC 2009]
Yehuda Lindell; Hila Zarosim

実例依存コミットメント(instance-dependent commitment schemes)とは、言語 L に関する命題(実例)x をパラメタに持つコミットメントであり、その安全性が L の判定問題の実例 x に依存して変化するコミットメントの事である。例えば、もし x ∈ L なら、計算量的秘匿(computationaly hiding)、x ¥not ∈ L なら完全束縛(perfect binding)を満たすようなコミットメントの事である。このようなコミットメントは場合によって零知識性と健全性を使い分ける用途に非常に向いている。本論文では適応的実例依存コミットメントを x ∈ L のとき多義(equivocal, コミットメントをどちらにもオープン出来ること)となるよう拡張し、その構成を示した。従って、一方向関数の存在を仮定すると NP に属するあらゆる言語が適応的零知識証明を持つ。また、適応的安全な紛失通信と拡張落とし戸置換(enhanced trapdoor permutation)のブラックボックス分離(適応的安全な紛失通信は拡張落とし戸置換からブラックボックス的に構成出来ないこと)を示し、適応的安全性が静的安全性より真に困難な場合がある事も示したとのこと。

On the (Im)Possibility of Key Dependent Encryption [TCC 2009]
Iftach Haitner; Thomas Holenstein

秘密鍵に依存した文書の暗号文が攻撃者に与えられると仮定しても、暗号の安全性が保たれる時、その暗号を鍵依存入力安全 (key-dependent input secure) であると言う。鍵管理系や匿名信用証明系においては、誰かの秘密鍵に何らかの暗号化を施して送受信する事がある。この時、システムの設計によっては、秘密鍵の暗号化が循環してしまう場合があり、そのような鍵の使用状況を鍵循環(key cycle)と呼ぶ。最も単純な鍵循環は秘密鍵がその鍵自信(あるいは対応する公開鍵)で暗号化されるような状況で、例えば暗号化ディスクの使用者がそのディスク上に秘密鍵(あるいはそのハッシュ値)のバックアップを作成してしまうような事象を、うまく抽象している。一般に鍵依存入力安全性を論じる場合、秘密鍵を攻撃者が指定した(ハッシュ)関数で評価した値の暗号文が攻撃者に与えられるとする。この論文は、鍵依存入力安全な共通鍵暗号系の実現に関して、以下の2つの否定的な結果(ブラックボックスセパレーション)を示した。

- 一方向置換からブラックボックス的に構成された暗号の鍵依存入力安全性の攻撃を一方向置換の原像に帰着するブラックボックス帰着が存在しないような、poly (n) 対の独立したハッシュ関数の族 H が存在する。
- 暗号の鍵依存入力安全性から任意の暗号学的仮定への強ブラックボックス証明を持つ帰着は存在しない。

On the (Im)Possibility of Arthur-Merlin Witness Hiding Protocols [TCC 2009]
Iftach Haitner; Alon Rosen; Ronen Shaltiel

3-彩色問題(3-colorability)[GMW] やハミルトン閉路問題(Hamiltonicity)[Blum] のような、健全性の誤り確率が定数の定数ラウンド零知識プロトコルは、その逐次繰り返し実行により健全性誤り確率を無視しうるほど小さく出来る。しかしこの方法ではプロトコルに必要なラウンド数がセキュリティパラメタに比例して増大してしまう。定数ラウンドプロトコルを得るため、これらのプロトコルの同期並列実行(parallel repetition)を考えると、以下の事実が知られている。

- 健全性誤り確率は無視しうるほど小さく出来る
- 証拠識別不能(witness-indistinguishable, WI)になる
- ブラックボックスシミュレーターを使って零知識(ZK)になる事は無い [Goldreich-Krawczyk]

では、これらのプロトコルは零知識と証拠識別不能の中間的な概念である証拠秘匿(witness-hiding, WH)となるであろうか?このような疑問を動機として、本論文では、どのような言語あるいは分布であれば、これらのプロトコルが WH となるのか(あるいは、ならないのか)を研究し、証拠(witness)が一つしかないような言語に対してはブラックボックス定数ラウンド公開硬貨 WH プロトコルが存在しない事を示した

とのこと。

Secure Computability of Functions in the IT setting with Dishonest Majority and Applications to Long-Term Security [TCC 2009]

Robin Kunzler; Jorn Muller-Quade; Dominik Raub

スタンダードモデルにおける一般の情報理論的な秘匿関数計算（secure function evaluation）は参加者の大多数を買収（corrupt）されると実行不可能となるが、(公平性(fairness)無しの）計算量的秘匿関数計算なら大多数が動的に買収されても実行可能である（Goldreich ら [STOC'87])。しかし、プロトコルの実行時点では計算量的仮定が受け入れられたとしても、それが未来永劫正しいとは限らない。むしろ、時々刻々解析能力が増大する攻撃者によって、重要なデータの秘匿がある日突然破られる可能性の方が問題となる。それゆえ本論文では、如何なる関数であれば、(大多数敵性の時）長期間安全性(long-term security)（計算実行時は計算量的仮定を認めるが、一旦結果が得られたら情報理論的安全性を求める事）が可能かについて研究している。また、この関数クラスを特徴付ける為、認証通信路モデルの下、受動的、準正直（semi-honest)、能動的、あるいは量子的な攻撃者が存在する場合の情報理論的安全に計算可能な関数クラスについても研究している。

Complexity of Multi-party Computation Problems: The Case of 2-Party Symmetric Secure Function Evaluation [TCC 2009]

Hemanta Maji; Manoj Prabhakaran; Mike Rosulek

本論文では 2-者対称秘匿関数計算（symmetric secure function evaluation ,SSFE)（symmetric とは，どちらの参加者も同じ出力を得るという意味）で計算できる関数の計算量クラスについて研究し、以下の結果を与えた。

- 受動的攻撃者に対し無条件安全に実現可能な SSFE 関数と、受動的攻撃者に対し統計的安全に実現可能な SSFE 関数と、理想コミットメントハイブリッドモデルで能動的攻撃者に対し汎用結合可能安全に実現可能な SSFE 関数は厳密に等しい（Theorem 3,4)。
- 孤立実現可能（standalone-realizable，hybrid でなく実現可能？）な SSFE 関数の新しい特徴づけ（saturation，飽和）を与えた（Theorem 5)。また、孤立実現可能であるが汎用結合可能安全に実現可能ではない SSFE 関数は、非同期並列自己結合（concurrent self-composition）の下で安全なプロトコルを持たない事を示した（Theorem 6)。
- F を受動的攻撃者に対し安全な m ラウンドプロトコルの汎用結合可能安全な理想関数（functionality）とし、f を深さ n>m+1 の一意分解（unique decomposition）を持つ SSFE 関数とする。f を F-ハイブリッドモデルで実現する如何なる汎用結合可能安全なプロトコルも存在しない（Theorem 7)。これを用いて様々な結果を得た（Corollary 8-10)。

Realistic Failures in Secure Multi-Party Computation [TCC 2009]

Vassilis Zikas; Sarah Hauser; Ueli Maurer

安全なマルチパーティ計算においては、いろいろな（暗号学的）買収（corruption）の方法が提案されている。3 つの最も典型的な方法は、動的買収（active-corruption，被買収者を完全に制御できること)、受動的買収(passive-corruption，被買収者から秘密を貰うこと)、故障的買収(fail-corruption，被買収者を機能停止させること)である。しかし故障的買収では回復可能な故障を正しくモデル化出来ないので、省略的買収（omission-corruption）が提案され、主にビザンチン合意（Byzantine Agreement）の状況で研究された。省略的買収とは、攻撃者が買収した参加者の通信を選択的に妨害可能だが、その中身を見ることは出来ないような買収の事である。本論文では、送信省略（send-ommition）および 受信省略（receive-ommition）の概念を導入し、動的買収、受信省略、送信省略が混在するモデルでの安全性の定義を行い、それぞれ t_a, t_ρ, t_σ 人まで買収可能な攻撃者に対して $3t_a + t_\rho + t_\sigma < n$ の時およびその時に限り無条件安全なマルチパーティ計算が可能であることを示し、この限界（bound）でビザンチン合意（プロトコル）を構成した。動的買収および省略的買収に関して、それぞれ t_{-a}，$t_{-\omega}$ 人まで買収可能とした時、従来の限界は $3t_a + 4t_\omega < n$ であったが（Koo, [TCC'06])、本結果に $t_\rho = t_\sigma = t_\omega$ を適用すれば、新しい限界 $3t_a + 2t_\omega < n$ が得られる。

Secure Arithmetic Computation with No Honest Majority [TCC 2009]
Yuval Ishai; Manoj Prabhakaran; Amit Sahai

本論文では有限環上算術回路秘匿計算 (securely evaluationg arithmetic circuits over finite rings) の計算量を研究している。敵性参加者(malicious party)に対し安全な 2 者プロトコルの場合に注目し、環演算のブラックボックス呼び出しと標準的暗号プリミティブしか使わないこと、および通信オーバーヘッドと環演算の数を最小化することを目標として、効率、一般性、仮定の異なる幾つかの解を示した。

- 任意の環 R をブラックボックス的に使用できるが、環演算の数が log |R|(上のある上界)に対して線形で増大する紛失通信ハイブリッドモデルで無条件安全なプロトコル。
- プロトコルで使う特定の環しか使用できないが、環演算の数は環のサイズに依存しない紛失通信ハイブリッドモデルで計算量的安全なプロトコル。このプロトコルは線形符号に関する既知の計算量仮定に依存し、適当なクラスの環を使った最も効率的な実例では、乗算ゲート当たりの通信量は定数個の環要素のみで、計算量は k をセキュリティパラメタとしてゲート当たり O(log k) の体演算で抑えられる。この結果は Naor-Pinkas の秘匿多項式計算(secure polynomial evaluation) [SIAM J. Comput., 2006] の拡張である。
- 準同系暗号をブラックボックス的にしか使わない, 環 Z_m = Z/mZ に対するプロトコル。m が素数の時, 回路の各ゲート当たり必要な暗号系の呼び出し回数は定数。

本論文の全てのプロトコルは紛失通信ハイブリッドモデルで汎用結合可能安全であり、任意の数の敵性参加者が存在する多者(multiparty)計算に一般化可能である。

Universally Composable Multiparty Computation with Partially Isolated Parties [TCC 2009]
Ivan Damgard; Jesper Buus Nielsen; Daniel Wichs

攻撃者が任意の数の参加者を買収できる時、セットアップの仮定無しではスタンダードモデルで汎用結合可能多者計算(UC multiparty computation)が一般には達成不可能である事はよく知られている。この問題を回避する一つの方法は、TTP(trusted third party)を使って CRS(common reference string)や PKI(public key infrastructure)のような何らかの大域的セットアップを利用することである。最近 Katz は TTP を利用する代わりに、物理的仮定、特に耐タンパーハードウェアトークン(tamper-proof hardware token)が利用可能であることを示した。本論文は Katz の仮定よりも弱い物理的仮定である"隔離(isolation)"の利用を研究している。隔離はオフィスなどの限定された安全なエリアで何らかの鍵のやり取り等を行ってから、外に出て計算を実行するようなプロトコルを抽象化した概念で、参加者(Alice)が計算のある一部分に対しては、他の参加者(Bob)を部分隔離(partially isolate)し、その間は Bob がある有限のビット数以上を環境と通信することを制限できるとする。(1ビットも通信できないなら完全隔離(full isolation)。) そして、F_{isolate} を部分隔離の理想関数(ideal functionality)とすると、標準的な暗号学的仮定の下、任意の数の参加者を動的および適応的に買収できる攻撃者が存在する場合に、あらゆる多者計算が $F_{isolate}$ ハイブリッドモデルで汎用結合可能安全に実現できる事を証明した。

Oblivious Transfer from Weak Noisy Channels [TCC 2009]
Jurg Wullschleger

雑音通信路 (noisy channel) の仮定を使って紛失通信(oblivious transfer)が実現可能である事を示すいろいろな結果が知られている。しかし暗号学的な設定においては雑音通信路には強い安全性要件が必要なため、この仮定の条件緩和が研究されている。例えば不公平雑音通信路 (unfair noisy channels) は Damgard, Kilian, Salvail [Eurocrypt'99] によって導入された概念で、攻撃者は通信路のエラー率を幾らか変更出来る(がゼロにはできない)ようなモデルであり、単純な雑音通信路よりも安全性要件は弱い。しかし、このモデルにも欠点がある。例えば、通信エラーが起こらなかった事実を攻撃者がある確率で検出できるような通信路はこのモデルで捉えることができない。本研究では不公平雑音通信路の概念の一般化を行い、弱消失通信路(weak erasure channel)および弱二元対称通信路(weak binary symmetric channel)と呼ぶ 2 つの暗号学的雑音通信路の新しい現実的なモデルを導入し、これらを使った紛失通信の構成法を示した。

Composing Quantum Protocols in a Classical Environment [TCC 2009]
Serge Fehr; Christian Schaffner

本論文では、古典的(非量子的)な 2 者ハイブリッドプロトコルで、ベースとなる理想関数(functionarity)を量子プロトコルに置き換えた場合の(逐次)合成可能安全性(composability)について研究している。まず、古典的ハイブリッドプロトコルを、正常系では古典的入出力を持つ 2 者量子プロトコル(量子演算子)の列と考え、この 2 者量子プロトコルの汎用的な安全性の定義を提案している。そして、この量子プロトコルを逐次的に呼び出す古典的ハイブリッドプロトコルの安全性、即ち(逐次)合成定理(composition theorem)を示している。最後に、最近提案された限定量子メモリモデル(bounded-quantum-strage model)におけるパスワードベースの個人識別(secure identification)が本論文の安全性定義を満たし、上記の意味で合成可能である事を示している。

LEGO for Two Party Secure Computation [TCC 2009]
Jesper Buus Nielsen; Claudio Orlandi

本論文は 2 者計算(two-party computation)に対する Yao の garbled circuit(判読不能回路)を能動的攻撃者(active adversary)に対しても安全となるよう拡張する方法を研究し、LEGO (Large Efficient Garbled-circuit Optimization) と呼ばれる新しい分割選択(cut-and-choose)に基づく方法を提案している。LEGO は特に大きい回路向けに設計されており、計算する回路 C のサイズを|C|と記述すると、従来の分割選択ベースの方法と比べて、計算量および通信量で漸近的に log|C| 倍の改善が得られる。提案法は静的および動的攻撃者に対して紛失通信ハイブリッドモデルで汎用結合可能である。紙面の都合により、定数分の効率改善は full version を参照せよとのこと。

http://eprint.iacr.org/2008/427/

Simple, Black-Box Constructions of Adaptively Secure Protocols [TCC 2009]
Seung Geol Choi; Dana Dachman-Soled; Tal Malkin; Hoeteck Wee

本論文は、適応的準正直攻撃者(adaptive semi-honest adversary)に対して安全な紛失通信(oblivious transfer, OT)を、適応的敵性攻撃者(adaptive malicious adversary)に対して安全な紛失通信に変換する翻訳系(compiler)を提案している。この翻訳系は、理想コミットメント(ideal commitment functionality)ハイブリッドモデルで汎用結合可能(universal composability, UC)安全であり、基礎プロトコルへのブラックボックスアクセスを用いている点、およびラウンド通信量が定数倍のオーバーヘッドで済んでいる点で同じ安全性の従来法より優れている。この紛失通信路と [IPS08, Theorem2] を組み合わせると、(落とし戸)シミュレーション可能暗号系((trapdoor) simulatable cryptosystem)へのブラックボックスアクセスを用いて、任意の数の参加者を買収できる適応的敵性攻撃者に対して、理想コミットメントハイブリッドモデルであらゆる秘匿多者計算(secure multi-party computation)を汎用結合可能安全に実現するプロトコルを得ることが出来る。この結果と [IPS08, Theorem3] を組み合わせると、攻撃者が m 者関数(m-party functionarity)に対して m-1 者まで買収可能として、同様の安全性の定数ラウンド秘匿 m 者計算プロトコルが得られる。系として、普通の適応的買収に対する汎用結合可能安全性より弱い、適応的実行後買収(addaptive post-execution corruption)[C00] を使い、(落とし戸)シミュレーション可能暗号系へのブラックボックスアクセスを用いて、スタンドアローンモデル(stand-alone model、ハイブリッドでない事)で、適応的敵性攻撃者に対して安全な定数ラウンド強紛失通信(string OT)プロトコル、適応的任意数敵性買収可能秘匿多者計算プロトコル、適応的 m-1 者敵性買収可能定数ラウンド秘匿 m 者計算プロトコルを初めて構築した。

Black-Box Constructions of Two-Party Protocols from One-Way Functions [TCC 2009]
Rafael Pass; Hoeteck Wee

本論文では、一方向関数へのブラックボックスアクセスのみを仮定した、以下の 2-者暗号プロトコルの構成法を示している。

- 定数ラウンドゼロ知識論証(zero-knowledge argument)

- 定数ラウンド落し戸付きコミットメント
- 定数ラウンド並列コイン投げ（parallel coin-tossing）

従来の構成法は、強い計算量的仮定（例えば衝突困難性）、非ブラックボックスアクセス、定数超ラウンド数、のいずれかが必要であった。系として、準正直紛失通信（semi-honest oblivious transfer）のみを仮定した、秘匿 2 者計算プロトコル（secure two-party computation protocols）の定数ラウンドブラックボックス構成法が得られた。さらに、既知の結果と組み合わせて、以下の構成法を示した。

- 非同期並列ゼロ知識論証（concurrent zero-knowledge argument）
- O(log n)ラウンド頑強コミットメント（non-malleable commitments）
- O(n)ラウンド非同期並列頑強コミットメント

1.2.3. TCC 2009 の発表(3 日目)

Chosen-Ciphertext Security via Correlated Products [TCC 2009]
Alon Rosen; Gil Segev

任意の一方向関数の集合(collection)から複数の一方向関数を選択し、その直積結合(product)を関数と見なすと、適当な条件の下でこの直積も一方向となる事が良く知られている。しかし一般に入力の組が相関を持つ場合はこの一方向性は保証されない。本論文では、入力に相関がある場合にも一方向性が保証できる入力の組の分布と一方向関数の集合に対する必要十分条件を研究し、単純で CCA 安全な公開鍵暗号系の構成に応用した。本論文の成果は以下の通りである。

1. ある大変自然な相関結合(correlated product)の下で安全な落し戸付き単射関数 (injective trapdoor function) のあらゆる集合を使用して、CCA 安全な公開鍵暗号系を構成できる事を示した。構成法は単純でブラックボックス的で直接の安全性証明が可能である。
2. (パラメタが適切に選ばれた)損失落とし戸関数(lossy trapdoor function)のどんな集合からも上記の暗号系に必要な関数を得ることが出来る事を示した。従って、既知の損失落とし戸関数の構成法に習い、Diffie-Hellman 判定問題、および Paillier の合成数剰余判定問題に基づき、この暗号系を構成出来る。
3. 相関結合の下での安全性は、計算量的仮定として損失落とし戸関数より潜在的に弱い事を示した。特に相関積の下で安全な落とし戸関数 (および拡張落とし戸置換) から損失落とし戸関数を構成する完全ブラックボックス構成(fully-black-box construction)は存在しない事を証明した。

Hierarchical Identity Based Encryption with Polynomially Many Levels [TCC 2009]
Craig Gentry; Shai Halevi

この論文は、定数階層以上の階層に対して安全な階層型 ID ベース暗号(HIBE)を提案している。従来の HIBE は安全性の帰着が階層の深さに関して指数関数的に低下するので、安全性は定数の ID 階層に対してしか証明できず、深い階層に関しては選択-ID 安全性(selective-ID security)しか証明出来なかった。本論文の提案法は、階層数に依存しないタイトな安全性証明を与えるので、多項式個の階層に対して安全である。この結果は、指数-逆数型 ID ベース暗号 (exponent-inversion IBE) から HIBE を構成する Boyen のフレームワークを、タイトな帰着を持つ Gentry の IBE に適用できるよう、修正したものと見なすことができる。まず始めに、鍵乱数化 ID ベース放送用暗号(KR-IBBE)から HIBE への汎用変換を記述し、その後、Gentry の IBE の拡張である Gentry-Waters の IBBE を修正することによって KR-IBBE を構成している。必要な困難性の仮定は Gentry の IBE と概ね同じである。

Predicate Privacy in Encryption Systems [TCC 2009]
Emily Shen; Elaine Shi; Brent Waters

述語暗号 (predicate encryption) とは、暗号化された平文に関する特定の述語評価能力を、秘密鍵所有者が第三者に提供できる暗号のことである。秘密鍵所有者は、何らかの述語集合の任意の述語 f に対して秘密鍵トークン (secret key token) と呼ばれる情報を生成でき、これを第三者に提供する。トークン所有者はトークンと暗号文のみから、述語 f に平文 x を代入した値 f(x) を評価できるが、平文 x の内容について非自明な情報を得ることは出来ないとする。暗号としての要件の他に、トークンが秘密を漏洩しない事が必要となる。従来の公開鍵述語暗号は、平文秘匿(plaintext privacy)、即ち暗号化されたデータに関する一切の情報を暗号文が漏洩しない性質、には注意を払って来たが、述語秘匿(predicate privacy)、即ち符号化された述語に関する情報をトークンが漏洩しない性質、については頓着して来なかった。公開鍵の設定では、トークンを持つ攻撃者は自分で暗号文を生成し述語を評価出来るので、一般の述語に関しては本質的に述語秘匿を達成できない。本論文では、対称鍵の設定で述語暗号を考え、内積照会 (inner product query) に対応した対称鍵述語暗号系を提案し、この暗号系が平文秘匿と述語秘匿の両方を達成することを証明している。

Simultaneous Hardcore Bits and Cryptography Against Memory Attacks [TCC 2009]
Adi Akavia; Shafi Goldwasser; Vinod Vaikuntanathan

本論文では、同じような証明手法を用いて、以下の2つの結果を得ている。

- メモリー攻撃と呼ばれる非常に強力なサイドチャネル攻撃の攻撃クラスを与え、Regev[STOC 2005]の公開鍵暗号および、Gentry, Peikert, Vaikuntanathan [STOC 2008] の ID ベース暗号が、この攻撃に対して特に頑健(robust)であることを示している。メモリー攻撃は Halderman らが最近発表した ”冷却起動攻撃(cold-boot attack)” を抽象化した概念で、秘密鍵の有意な量の情報が攻撃者に漏洩するセッティングの下での攻撃である。攻撃者に課せられた制約は観測可能な情報量の上限のみで、例えば、RSA では 24%、AES では 85%、の鍵の漏洩があれば、暗号の安全性は完全に毀損することが知られている。
- 上記 [STOC 2008] で提案された落とし戸一方向関数(の変種)に対して、N − o(N) 個の入力ビットが同時ハードコアであることを示した。一方向関数 f(x) が与えられた時、x のあるビットブロックが同じ長さの乱数列と区別が付かないとき、そのブロックを f(x)に対する同時ハードコア(simultaneous hard-core) であるという。 あらゆる一方向関数候補は入力長に対して対数の同時ハードコアを持つことが示せるが、線形の同時ハードコアを持つ一方向または落し戸関数の例は素因数分解系のもの以外はあまり知られていなかった。

How Efficient can Memory Checking be? [TCC 2009]

Cynthia Dwork; Moni Naor; Guy N. Rothblum ; Vinod Vaikuntanathan

この論文は、遠隔サーバ上の大容量データベースを、端末上の小さいメモリー(storage)を使用して保守運用するときの、記憶検査 (memory checking) の問題を研究している。遠隔データベースは大容量で広く公開されており信頼性が低いとする。容量は小さいが信頼性が高く非公開の端末を使って、このデータベースの故障を検出したい。記憶検査器 (memory checker) はユーザーから大容量データベースへの格納および取り出し操作を受理する。そして、遠隔ストレージへ問い合わせを行い回答を受理する。それから、これらの回答と端末ストレージを使って、全ての問い合わせが正しく回答された事を確かめる。(あるいは遠隔ストレージに故障があることを報告する。) この分野の一連の研究によって、記憶検査の計算量が、照会計算量(query complexity, 記憶検査器によりユーザー要求当たり発行される照会数)および領域計算量(space complexity, 必要な高信頼端末ストレージのサイズ)の意味で、調査された。この問題を最初に定式化した Blum らは (故障が発生するとすぐ報告される) オンライン検査機と(故障が長い操作列の終了時のみ報告される) オフライン検査機の違いを明らかにした。本研究では記憶検査の問題を再訪し、「記憶検査はどこまで効率化できるか？」を問うた。オンライン検査機に関しては Blum らがデータベースサイズ n に対して対数オーダーの照会計算量を持つ検査機(の上界)を与えた。本論文では、決定的で非適応的に遠隔記憶装置にアクセスする検査機に対して、照会計算量の下界 Ω(log n/log log n)を与えている。また、この否定的な結果に対処するため、本論文ではオンライン記憶検査機の読み出し計算量と書き込み計算量のトレードオフの方法を示している。即ち、任意の対数基底 d に対して、読み出しあるいは書き込みのどちらか一方が照会計算量 O(log_d n)を持つオンライン記憶検査機を構成している。その対価として、この検査機は、もう一方の操作(書き込みあるいは読み出し)が照会計算量 O(d log_d n) を持つ。この対価が受け入れ難い場合には、オフライン記憶検査が利用できる。本論文では、1 操作あたりの見做し照会計算量を O(1) とする為には、最低 n 操作列が必要であった Blum らの構成を改良して、短い操作列に対しても O(1)を実現するオフライン記憶検査系を提案している。

Goldreich's One-Way Function Candidate and Myopic Backtracking Algorithms [TCC 2009]

James Cook; Omid Etesami; Rachel Miller; Luca Trevisan

Goldreich は d 変数の小さな述語 P とエキスパンダグラフ G によって記述される一方向関数候補の構成法を提案した。G は n 頂点の頂点集合を左右にそれぞれ持ち、全ての枝が左右両方の頂点集合に端点を持つ二部グラフで、左側の頂点をそれぞれ入力ビット、右側の頂点をそれぞれ出力ビットと見なす。右側の各頂点の枝数は d で、d 個の左側隣接頂点を入力変数と見なした d 変数述語 P の値をその右側頂点の値とする。Goldreich 関数の逆像は、ある制約充足問題の求解問題に等しく、従って SAT solver を使った攻撃を考えることができる。本研究では先ず、最も入手が容易な SATsolver である MiniSat を使って、Goldreich 関数の逆像を求める解析実験を行った。この実験によれば、逆像に必要な実行時間は入力長に対して指数関数的に増大し、この攻撃が短い入力長 (数百ビット) で既に手にお

えないことが実験的に示された。この結果を受けて、バックトラッキングに基づく SAT solver の限界の厳密な研究を行った。Alekhnovich, Hirsch, Itsykson の結果は、もし 3 項パリティ述語 (3-ary parity predicate) $P(x_1,x_2,x_3) = x_1 \oplus x_2 \oplus x_3$ が使われるなら Goldreich 関数は“近視眼的 (myopic)”バックトラッキングアルゴリズムに対して安全であることを意味している。しかしながら、線形述語を用いた場合は Gauss の消去法による自明な攻撃が存在するので、非線形述語を使用した場合の結果を与える方が現実的であろう。本論文では Alekhnovich らの研究を、より一般の述語のクラスを扱えるよう拡張して、述語 $P_d(x_1,\ldots,x_d) := x_1 \oplus x_2 \oplus \ \ldots \ \oplus x_{d-2} \oplus (x_{d-1} \wedge x_d)$ およびランダムグラフを用いた構成について、この攻撃の計算量の下界を提案している。

Secret Sharing and Non-Shannon Information Inequalities [TCC 2009]

Amos Beimel; Ilan Orlov

既知の秘密分散法は大抵のアクセス構造に対して効率的でない。n をアクセス構造への参加者の数とすると、1 ビットの秘密に対してさえ、分散情報 (share) の長さは 2^{O(n)} となる。こうした秘密分散法の改善、あるいは改善不可能性の証明は長い間の未解決問題となっている。Csirmaz (J. Cryptology 97) は，最低一人の参加者の分散情報のサイズは $n / \log n \times$(秘密サイズ)であるようなアクセス構造が存在することを証明した。これが既知の最良の下界である。Csirmaz の証明には当時知られていた唯一の情報不等式である Shannon 型情報不等式を使用する。即ち Csirmaz は Shannon 型情報不等式しか使えないなら分散情報のサイズに関して $\omega(n)$ の下界は証明できないことを証明した。ところで、この 10 年ほどの間に一連の非 Shannon 型情報不等式が発見された。新しい不等式を使えば n を超える下界の改善が可能かもしれないが、本論文では今日までに知られているどの情報不等式も、分散情報のサイズに関して $\omega(n)$ の下界を証明できないことを示した。

Weak Verifiable Random Functions [TCC 2009]

Zvika Brakerski; Shafi Goldwasser; Guy N. Rothblum; Vinod Vaikuntanathan

Micali, Rabin, Vadhan が提唱した検証可能ランダム関数 (verifiable random function,VRF) とは疑似ランダム関数の一種で、秘密鍵の所有者が、対応する公開鍵を生成して、あらゆる正しい入出力値に対し、関数を正しく計算したことの証明が可能な関数の事である。生成された証明は VRF の疑似乱数性を壊すことがなく、また如何なる公開鍵を用いても一つの入力につき一つの出力のみ証明可能であることが要求される。VRF は自然で使い勝手の良い基本関数 (primitive) であるので、いろいろな構成法や応用が提唱されてきたが、VRF の研究には沢山の未解決問題が残っており、とりわけ他の暗号用基本関数との関係、および、様々な暗号学的仮定からの構成が重要な未解決問題となっている。本論文では VRF の条件を緩和して、擬似乱数性がランダムに選択された入力についてのみ満たされる、弱検証可能ランダム関数 (weak verifiable random function, WVRF) を定義し、その応用、構成、および他の暗号用基本関数との関係について研究を行い、以下の結果を得た。

- WVRF とあらゆる NP 言語に対する common random string モデルにおける非対話ゼロ知識論証(argument)は等価である(一方があれば他方が作れる)事を証明した。
- WVRF の落し戸置換 (trapdoor permutation) からの構成法、および、Gap-DDH 群における CDH 仮定からの構成法を示した。
- WVRF と一方向置換のブラックボックス分離(black-box separation)を示した。(一方向置換から WVRF(従って VRF)をブラックボックス的に構成することは出来ない。)

Efficient Oblivious Pseudorandom Function with Applications to Adaptive OT and Secure Computation of Set Intersection [TCC 2009]

Stanislaw Jarecki; Xiaomin Liu

紛失擬似ランダム関数(oblivious pseudorandom function,OPRF)とは、送信者 S と受信者 R との間の 2-者プロトコルで、S が持つ鍵 k と R が持つ入力 x に対し R は擬似ランダム関数 f_k(x)の値のみ学習し S は何も学習しない安全な f_k(・)の対話計算のことである。本論文では O(1)個の剰余べき乗しか必要とせず、定数ラウンド(ランダムオラクルモデル(ROM)では 2 ラウンド)のコミットされた入力に対する紛失擬似ランダム関数プロトコルを提案する。q を疑似ランダム関数の定義域のサイズとし、あらゆる k に対して f_k

が単射であるとする。この時このプロトコルは合成数剰余判定（composit decisional residuosity, CDR）仮定のもと CRS モデル（common reference string model）で安全であるが、一方で疑似ランダム関数自体は多項式サイズの定義域に関して合成数位数の群上の q-Diffie-Hellman 逆算判定仮定のもとで安全である。単射疑似ランダム関数に対する実用的な OPRF は、多項式サイズ定義域に限定されるが、安全なプロトコル設計で多くの用途をもつ道具だ。本論文ではこの OPRF が ROM なしで安全な新しい実用的な完全シミュレーション可能適応的（コミット付き）紛失通信プロトコルを含意することを示す。また、N をある2つのデータ集合の最大サイズとして、コミットされたデータの積集合を O(N)個のべき乗で安全に計算する初めてのプロトコルを、この OPRF の構成は含意している。

Towards a Theory of Extractable Functions [TCC 2009]
Ran Canetti; Ronny Ramzi Dakdouk

抽出可能関数（extractable function）とは値域上の値を出力できる攻撃者は必ず対応する原像を"知っている"ような関数のことである。ここで、知識とは "攻撃者の内部状態" から原像を回復できる効率的な抽出機（extractor）の存在によって捉えることができる。関数の抽出可能性は完全一方向関数の文脈にて著者ら（ICALP'08）によって定義された。それは KEA 仮定（Hada, Tanaka, Crypto 1998）のような知識仮定の抽象化とみなす事が出来る。本論文では次の2つを研究している。一つ目は抽出可能性の概念そのものの研究で、特に、弱い抽出可能性が強い抽出可能性を含意することを示し、抽出（extraction）と難読化（obfuscation）が相補的概念であるという直感を厳密化した。二つ目は抽出可能性を保持したまま単純なあるいは弱い暗号の基本関数から、いろいろな基本関数を構築できる可能性についての研究である。結果は一般に肯定的で、特に幾つかの暗号学的帰着は "知識保存(knowledge-preserving)" であるか、そうなるよう改造可能である。例えば、抽出可能弱一方向関数から抽出可能強一方向関数への帰着、抽出可能擬似乱数生成から抽出可能擬似ランダム関数への帰着、抽出可能一方向関数から抽出可能コミットメントへの帰着などは知識保存である。抽出可能一方向関数から抽出可能擬似乱数生成を構成するなどの問題は未解決である。

1.2.4. TCC 2009 rumpの発表

Public-Key Cryptosystems Resilient to Key Leakage [TCC 2009 rump]
Moni Naor, Gil Segev

広い範囲のサイドチャネル攻撃をモデル化する、鍵漏洩(key leakage)に対する安全性の研究が流行の話題となっている。本研究では、任意の汎用ハッシュ証明系(universal hash proof system)[CS'02]から、鍵漏洩に対して安全な公開鍵暗号の汎用的構成法を示した。この構成法は追加の計算量的仮定は必要とせず、既存の様々な数論的仮定(DDH, d-Linear, QR, Pailier)に基づく汎用ハッシュ証明系を使用することが出来る。また、DDH あるいは d-Linear に基づく新しいハッシュ証明系も提案する。さらに鍵循環安全な暗号系(circular-secure encryption scheme)[BHHO'08] もこの構成に利用可能であることを示す。これらの構成は L-o(L) bit の鍵漏洩に対して安全である。この結果は同じタイトルで Crypto 2009 にて発表が予定されており、以下の preprint が公開されている。

http://eprint.iacr.org/2009/105.pdf

Efficient, differentially, private statistical estimators [TCC 2009 rump]
Adam Smith

差分プライバシー(differential privacy)とは、統計データベースのプライバシー保護に関する厳密な安全性概念で、最近注目されている。大きい範囲のパラメトリック確率モデルに対して、分布が最尤推定量(maximum likelihood estimator)の分布に収束する差分プライバシー推定量(differentially private estimator)が存在する事が示されている。今回の発表では、統計学の用途に使える、非常に効率的な、差分プライバシー統計推定量が出来たと報告された。以下に関連すると思しき論文が公開されている。

http://arxiv.org/abs/0809.4794v1

Hash and Sign Signatures from the RSA Assumption (in the standard model) [TCC 2009 rump]
Susan Hohenberger, Brent Waters

標準モデルで安全な "hash-and-sign"型の(tree 型でない)署名が幾つか存在するが、大抵 Strong RSA や q-Strong DH のような、都合の良い強い仮定に依存している。本研究グループは、標準モデルで安全な hash-and-sign 型の署名を Eurocrypt 2009 に発表する予定であるが、この方式では署名者は状態(署名発行数カウンター)を管理する必要がある(stateful な署名)。本発表では、RSA 仮定に基づく stateless の署名について報告された。この結果は"Short and Stateless Signatures from the RSA Assumption"なるタイトルで Crypto 2009 にて発表が予定されており、以下の preprint が公開されている。

http://eprint.iacr.org/2009/283.pdf

Efficient Robust Private Set Intersection [TCC 2009 rump]
Dana Dachman-Soled, Tal Malkin, Mariana Raykova, Moti Yung

互いに他を信用できない2者間で、それぞれが持つ秘密の集合の積を、安全に計算する効率的な2者プロトコルは未解決である。Yao の garbled circuit を robust にすれば実現出来るが、出力を受け取る方の入力サイズを n、もう一方の入力サイズを m とすると、その通信量は robustness を抜きにしても $\Omega(n\,m)$ となり効率が悪い。本発表では k をセキュリティパラメタとして $O(m\,k^2\,\log^2(n) + n\,k)$ のプロトコルが構成出来たとの報告が行われた。この結果は同じタイトルで ACNS 2009 にて発表された。

Fully Homomorphic Encryption Using Ideal Lattices [TCC 2009 rump]
Craig Gentry

暗号化されたままで自身の復号回路(および NAND 復号回路)を評価可能な暗号系 E があれば、それ

を用いて proxy re-encryption(暗号が KDM 安全性を持つなら、只の re-encryption)を構成し、NAND を使って回路を構成する事により、あらゆる回路を評価可能な暗号系が作れる。イデアル格子を使った暗号系は、元々環準同型性を持っているが、一般に演算の度に暗号文が大きくなってしまうので非自明な環準同型暗号は実現出来ない。しかし、上記の復号回路の構成が十分に小さければ E が構成可能となり得るので、工夫して復号回路の演算量を小さくし、イデアル格子を使って実現したとのこと。セキュリティパラメタを k とすると、ゲート当たりの準同型回路評価に $\tilde{O}(k^6)$ のビット計算量が必要とのこと。この結果は同じタイトルで STOC 2009 にて発表された。

Swifftx [TCC 2009 rump]

Alon Rosen

SHA-3 の公募に提案された SWIFFTX ハッシュ関数の提案者による紹介。名前に含まれる通り FFT に基づく設計であるとのこと。

Somewhat Non-Committing Encryption and Efficient Adaptively Secure Oblivious Transfer [TCC 2009 rump]

Juan Garay, Daniel Wichs, Hong-Sheng Zhou

本研究では、準適応的安全性(semi-adaptive security)なる適応的安全性(adaptive security)と静的安全性(static security)の中間概念を導入し、準適応的安全なプロトコルを適応的安全なプロトコルに変換するコンパイラを構成し、この結果を Peikert らの紛失通信プロトコル[Crypt 2008]に適用して、定数ラウンド、定数回公開鍵演算の適応的安全な紛失通信プロトコルを非消失モデル(non-erasure model)で構成したとのこと。この結果は同じタイトルで Crypto 2009 にて発表が予定されており、以下の preprint が公開されている。

http://eprint.iacr.org/2008/534.pdf

Conditional Oblivious Transfer and Private Authentication [TCC 2009 rump]

Stanislaw Jarecki, Xiaomin Liu

言語 L に対する条件付き紛失通信(conditional oblivious transfer, COT)とは、送信者が文書 m を命題 x のもと暗号化して送信し、受信者は命題 x と証拠 w が L に関する関係 R を満たすときのみ文書 m が得られるような紛失通信のことである。秘匿条件付き紛失通信(private COT)とは証拠を持たない受信者に対して文書 m の内容だけでなく、命題 x も秘匿されるような条件付き紛失通信路のことである。本発表では、命題 x に含まれる群要素の離散対数表現の等価性、非等価性、総和、積などの法算術制約条件により定義される言語に対して DDH 仮定の下安全な秘匿条件付き紛失通信を構成し、それを用いて効率的な完全秘匿認証(fully private authentication)を構成したとの報告がなされた。この結果は“Private Mutual Authentication and Conditional Oblivious Transfer”なるタイトルで Crypto 2009 にて発表が予定されている。

Almost-Asynchronous MPC with Faulty Minority [TCC 2009 rump]

Zuzana Beerliova-Trubiniova, Martin Hirt, Jesper Buus Nielsen

同期ネットワーク上では、秘匿多者計算(secure multiparty computation)は、買収された参加者数 t が全参加者数 n に対して $t < n/2$ であるなら実現可能である。一方、非同期ネットワーク上では $t < n/3$ が必要である。では、その中間的なネットワーク構成の場合の条件はどうだろうか？本発表では、1 ラウンドだけ同期的(同報)通信を利用可能な時 $t < n/2$ である事が報告された。以下の preprint が公開されている。

http://eprint.iacr.org/2008/416.pdf

Resolving the Simultaneous Resettability Conjecture [TCC 2009 rump]

Vipul Goyal, Amit Sahai

Canetti, Goldreich, Goldwasser, Micali (STOC 2000) は悪意ある検証者が証明者をリセットする事により、証明者に同じランダムテープを何度も使わせることが可能な、リセット可能零知識性の概念を提案した。またそのすぐ後で Barak, Goldreich, Goldwasser, Lindell (FOCS 2001) は悪意ある証明者が検証者をリセットする事により、検証者に同じランダムテープを何度も使わせることが可能な、リセット可能健全性の概念を提案した。しかし、リセット可能零知識性とリセット可能健全性を同時に満たすプロトコルについては未解決であった。本発表では、その両方を満たすプロトコルを与え、この問題を解決したとのこと。以下の preprint が公開されている。

http://eprint.iacr.org/2008/545.pdf

On the Composition of Public-coin Zero-knowledge [TCC 2009 rump]

Rafael Pass, Dustion Tseng, Douglas Wikstrom

元々の零知識プロトコルは公開硬貨で実現可能な事がよく知られている。一方、非同期並列零知識プロトコルは秘密硬貨の下でしか実現されていない。今まで公開硬貨の非同期並列零知識が実現可能かどうか良く分かっておらず、零知識プロトコルの合成に対して秘密硬貨である事が本質的に重要であるか否かは未解決であった。本発表では、同期並列の場合ですら BPP に含まれない言語は公開硬貨ブラックボックス零知識論証(argument)を持たない事が報告された。この結果は、"On the Composition of Public-Coin Zero-Knowledge Protocols"なるタイトルで Crypto 2009 にて発表が予定されている。

Non-malleability Amplification [TCC 2009 rump]

Huijia Lin, Rafael Pass

本発表では一方向関数とブラックボックス技法を使って、定数ラウンドで頑強コミットメント(non-malleable commitment)を構成する方法が報告された。長さ t の k ラウンド stand-alone 頑強コミットメントから O(k) ラウンドの Concurrent 頑強コミットメントを構成し、それを用いて長さ $\Omega(2^t)$の stand-alone 頑強コミットメントを構成するとのこと。この結果は、同じタイトルで STOC 2009 にて発表された。

A Unified Framework for Concurrent Security: UC from Stand-alone Non-malleability [TCC 2009 rump]

Huijia Lin, Rafael Pass, Muthu Venkitasubramaniam

本発表では、UC プロトコルによる安全な非同期並列計算に関して、準多項式時間シミュレーションのような条件緩和モデルで得られる結果と、CRS モデルなどのセットアップ仮定により得られる結果を統合するような安全性証明の統合的なフレームワークについての報告が行われた。この結果は"A Unified Framework for Concurrent Security: Universal Composability from Stand-alone Non-malleability"のタイトルで STOC 2009 にて発表された。

A Zero-One Law for Composable Security [TCC 2009 rump]

Hemanta Maji, Manoj Prabhakaran, Mike Rosulek

この研究グループは TCC 2009 にて計算量無制限の攻撃者に対して UC 安全な 2-者対称秘匿関数評価(symmetric secure function evaluation)で計算できる関数の計算量クラスに関する研究を行い、その中に無限階層がある事を示したが、本発表では計算量が確率的多項式時間に制限された攻撃者に対する同様の研究結果が報告された。この場合は計算量クラスが2つの階層のみから構成されるとのこと。以下の preprint が公開されている。

http://www.cs.uiuc.edu/homes/rosulek/pubs/zero-one/

On Public v.s. Private Coins in Zero-knowledge Proofs [TCC 2009 rump]

Rafael Pass, Muthu Venkitasubramaniam

秘密硬貨対話証明系で認識可能な言語が公開硬貨プロトコルでも認識可能である事を示した Goldwasser らの結果は有名である。本発表では定数ラウンド零知識、非同期並列零知識、並列繰り返しなどに関する結果について報告された。

Bounded-Retrieval Model and Huge Secret against Side Channel Attacks / MAC from block ciphers [TCC 2009 rump]

Yevgeniy Dodis

次の 2 つの研究の紹介

- Leakage Attacks に対して、従来の relative leakage モデルでは、漏洩限界(leakage bound,実際に漏洩が許される情報量)はセキュリティパラメタに依存している。コンピューターウイルスが計算機から情報を盗み出すような状況を想定した時、RSA の 1024 bit の鍵の内の何パーセントが漏洩しているかを問うのは実効的な安全性の議論とはならないであろう。本研究では、Bounded Retrieval Model を用い、予め決められた漏洩限界によって秘密鍵の長さを決定する事によってこの問題を解決しようとしている。秘密鍵の長さが公開鍵等のパラメタに影響が出ないようにする必要がある。この結果は“Leakage-Resilient Public-Key Cryptography in the Bounded-Retrieval Model”なるタイトルで Crypto 2009 にて発表が予定されている。
- unpredictable なブロック暗号から birthday security の任意入力長 keyd MAC を構成するモードを提案した。使用するブロック暗号が PRF なら MAC も PRF である。また、CBC などと違い“leaky block-cipher” model で PRF である事が証明出来、サイドチャネル攻撃に耐性を持つ。Rate は 3 で CBC などより 3 倍遅い。安全性は概ね birthday barrier 程度。この結果は“Message Authentication Codes from Unpredictable Block Ciphers”なるタイトルで Crypto 2009 にて発表が予定されている。

1.3. PKC 2009 の発表

1.3.1. PKC 2009 の発表(1 日目)

Implicit Factoring: On Polynomial Time Factoring Given Only an Implicit Hint [PKC 2009]
Alexander May and Maike Ritzenhofen, HGI, Ruhr-University of Bochum (ドイツ)

PKC2009 の Best Paper Award を受賞した論文。RSA モジュラスの素因数に関する implicit な情報を与えるオラクルを仮定した場合に、多項式時間で RSA モジュラスを素因数分解することができることを示した。即ち、$N_1=p_1\times q_1$ に対し、p_1と下位 t ビットを共有する p_2を素因子として持つ別の RSA モジュラス $N_2=p_2\times q_2$を返すオラクルを用いると、t が十分に大きい場合に、N_1 および N_2をビット長の 2 次オーダーの時間で素因数分解するアルゴリズム(2 次元格子の最小ベクトルを求める)を示した。更に、オラクルを k 個用いた場合への拡張および、p、q のビット長が同じ場合の結果も示した。

The Security of All Bits Using List Decoding [PKC 2009]
Carla Rafols and Paz Morillo, Universitat Politecnica de Catalunya (スペイン)

リスト復号とハードコア述語との関係は、ある種の述語の困難性を証明するための、きれいで容易な方法論を与えてきた。これまでのところこの方法論は、(最もよく知られた数論的トラップドア置換を含む)乗法的アクセスを持つ任意の関数の O(loglog N)最下位および最上位ビットの安全性を証明することのみに使われてきた。我々は、N が素数または RSA モジュラスの場合、乗法的アクセスを持つ位数 N の巡回群上定義された任意の関数のすべてのビットに対して、この方法が適用できることを示す。結果として、RSA、素数位数の群の離散対数、Paillier 暗号スキームのすべてのビットの安全性を再度証明する。

A New Lattice Construction For Partial Key Exposure Attack For RSA [PKC 2009]
Yoshinori Aono, Tokyo Institute of Technology(日本)

RSA 暗号の秘密鍵 d が小さく、かつ、d の一部が知られている場合に、RSA 暗号に対する格子攻撃を適用できる条件を拡げることに成功した。(e,N)を公開鍵、l_N を N のビット長、l_d を d のビット長、l_0 を d の知られている下位ビット長、$\beta = l_d / l_N$ 、$\delta =(l_d- l_0)/ l_N$ とする。格子攻撃における新しい格子構成法を導入し、攻撃が有効となる β および δ の範囲を示した。これまでに知られていた Ernst らの攻撃が有効となる範囲を拡張し、実行性能も改善するものである。

Subset-Restricted Random Walks for Pollard rho Method on GF(pm) [PKC 2009]
Minkyu Kim, Jung Hee Cheon, and Jin Hong, Seoul National University(韓国)

Pollard の ρ 法を高速化する手法(subset-restrict 法)を提案する。ρ 法の iteration 関数として、値域のサイズが定義域のサイズよりもはるかに小さくなるような関数を使うことにより、衝突が早期に起きるようにする。特に大きな拡大次数を持つ有限体の乗法群の離散対数問題に適用した場合には、有限体を $GF(p^m)$と書いたときに、オリジナルの ρ 法と比較して、$(3p-3)\sqrt{m}/(4p-3)$倍の高速化が図れることを示した。ペアリングベース暗号の安全性は MOV 変換により標数 2 または 3 の有限体上の離散対数問題に帰着され、我々の方式を適用することができるため、部分群位数を m 倍程度増やす必要がある。今後の課題としては、subset-restrict 法を素体に適用すること、tag-tracing 法(著者らによる ASIACRYPT2008 発表の手法)と組み合わせることが挙げられる。

From Signatures to Anonymous Credentials and Anonymous Delegation[PKC 2009、招待講演]
Anna Lysyanskaya, Brown University

例えば新聞を購読する際に、身分を明かしたくないが、正規の購読手続きを行ったことは証明したいという例を取り、匿名の信用証明を実現する際の課題や解決に関する近年の結果が紹介された。認証技術を用いてできることは、匿名認証技術を用いても実現することができ、その理論的裏づけの際に知識の署名(Signature of Knowledge)のテクニックが非常に強力なツールとなることが主張された。

Signing a Linear Subspace: Signature Schemes for Network Coding [PKC 2009]
Dan Boneh, Stanford; David Freeman, CWI and Universiteit Leiden; Jonathan Katz, University of Maryland; Brent Waters, University of Texas at Austin(オランダ、米国)

ネットワーク符号化は、完全に中央制御されていないネットワークにおいて、スループットを向上させ、ランダムな故障に対して堅牢性を持たせる。しかしながら従来のルーティングと異なり、ネットワーク符号化は途中でデータパケットを変更する中間ノードを必要とするため、標準的な署名スキームを適用することはできず、悪意のあるノードの改竄に対し回復性を持たせることは、挑戦的な研究テーマである。我々は、悪意のあるデータ改竄を防ぐため、ネットワーク符号化と組み合わせて使うことのできる 2 つの署名スキームを提案する。我々のスキームは、線型部分空間Ｖ上の署名 σ はＶのベクトルを認証するという意味において、線型部分空間に署名していると見ることができる。1 つめのスキームは準同型性を持ち、公開鍵サイズとパケット毎のオーバーヘッドが一定となるため効率的である。2 つめのスキームはランダムオラクルに依存せず、より弱い仮定に基づいている。更に、線型部分空間への署名長の下界を証明し、我々のスキームはこの観点から最適であることを示す。

Improving the Boneh-Franklin Traitor Tracing Scheme [PKC 2009]
Pascal Junod, University of Applied Sciences - Western Switzerland; Alexandre Karlov and Arjen K. Lenstra, EPFL, Switzerland

不正者追跡スキームは、共謀者の特定を可能とする暗号学的に安全な放送型手法である。l 人の正規ユーザーの静的な集合の内 k 人の不正者により海賊鍵が生成された場合、海賊鍵が与えられればすべての不正者を特定することができる。本論文では、Boneh-Franklin の不正者追跡スキームにおける 3 つの実用性および安全性の問題を検討する。はじめに、元のスキームを変更することなく、元の追跡計算量が O~(l)であったものを O~(k^2)になるよう、非ブラックボックスモデルにおける追跡プロセスを修正した。新しい追跡プロセスは、秘密鍵に透かしをつけることに使われたリードソロモン符号の性質とは独立に機能する。これにより何十億のユーザーを持つアプリケーションにおいても、大規模な共謀を特定するのに、通常のデスクトップコンピューターで数分しかかからない。次に、k 人以上の不正者を特定するのにリスト復号アルゴリズムの実用的価値が欠けていることを示す。最後に、2k 人の不正者は、すべての正規ユーザーの鍵を引き出すことができることを示し、この安全性の問題に対する修正を提案する。

Modeling Key Compromise Impersonation Attacks on Group Key Exchange Protocols [PKC 2009]
M. Choudary Gorantla, Colin Boyd, and Juan Manuel Gonzalez Nieto, Queensland University of Technology

鍵交換プロトコルは、複数のパーティが、公のネットワーク上で秘密のセッション鍵を共有することを可能とする。2 パーティ間の鍵交換(Two-Party Key Exchange, 2PKE)プロトコルは、様々なモデルの下、異なる攻撃行動を考慮して、厳密に分析されてきた。しかしながら、グループ鍵交換(Group Key Exchange, GKE)プロトコルの分析は、2PKE のそれほど広範囲には行われていなかった。なりすましによる鍵漏洩(Key Compromise Impersonation, KCP)に対する耐性の安全性属性は、これまでのところ GKE プロトコルの場合は無視されてきた。我々はまず、内部および外部の敵による KCI 攻撃を取り上げ、GKE プロトコルのセキュリティをモデル化する。次に、既存のいくつかのプロトコルは外部の KCI 攻撃に対しても安全でないことを示す。これらのプロトコルに対する攻撃は、KCI への対策を考慮することの必要性を示している。最後に、ランダムオラクルを仮定した修正モデルのもとで、ある GKE プロトコルの安全性に新しい証明を与える。

Zero-Knowledge Proofs with Witness Elimination [PKC 2009]
Aggelos Kiayias and Hong-Sheng Zhou, University of Connecticut

証拠消去(Witness Elimination, WE)を持つゼロ知識証明は、証拠が与えられたあるステートメントに有

効であり、更に証拠が消去された証拠に属していなければ、対話を受け入れる検証者に対して、証明者が証拠の知識を示すことができるプロトコルである。消去された証拠の集合は、公開の関係 Q と検証者の秘密の入力により決められる。このように、証拠消去を持つゼロ知識証明は、ゼロ知識の性質を緩和を必要とし、ステートメントがその有効性を立証するかもしれない多数の証拠を持つような設定にに関連する。このようなプロトコルの設計において、様々な問題が表れる。プロトコルの転写により、検証者は終わった後に証拠をテストできるのかどうか、証明者は証拠が消去されたかどうかを知ることができるべきかなどの問題である。このプリミティブは、ユーザーがあるアクセスポイントに対して匿名性を保ったまま自身を認証したく、アクセスポイントは、ユーザーが正規でありかつオーソリティに追跡されている容疑者の ID ではないことを認証したいような ID スキームの設定が動機となっている。
我々は UC(Universal Composability)の設定の下で、証拠消去を持つゼロ知識証明を定式化し、効率的なスキームの設計に適したスムース射影ハッシュに基づいた一般的な構成を与え、例として証拠消去を持つ、Boneh-Boyen 署名の知識を証明する効率的なスキームを示す。我々のスキームは、線型 ElGamal 暗号文の言語に対するスムース射影ハッシュの設計を必要とする。証拠消去を持つゼロ知識証明はパスワードベース鍵交換やプライベート等価テストなどのプリミティブとも自然に関係を持つ。

Distributed Public-Key Cryptography from Weak Secrets [PKC 2009]

Michel Abdalla, ENS; Xavier Boyen, Stanford; Celine Chevalier, ENS; David Pointcheval, ENS

分離された場所に保管されたエントロピーの低いパスワードの結合としてエントロピーの高い仮想的なパスワードが暗に定義される、分散パスワードベース公開鍵暗号の概念を導入する。ユーザーは、パスワードの共有や再構成をすることなく、個々のパスワードに基づいた、任意の通信路上におけるメッセージの交換により、協力して秘密鍵を操作することができる。例として ElGamal 暗号の場合に焦点を当て、UC モデルにおいて、分散公開鍵生成と仮想秘密鍵計算のための理想機能の定義を定式化する。更に、RO モデル(効率のため)の下でも、CRS モデル(優雅さのため)の下でも安全に実現できる、効率的なプロトコルを構成する。我々の分散プロトコルは、ID ベース暗号を含む、より広いクラスの離散対数ベース公開鍵暗号への一般化である。これは、各々がマスター鍵の小さな部分を記憶している人々により作られる仮想 PKG を持つ IBE への強力な拡張への扉を開く。

Asynchronous Multiparty Computation: Theory and Implementation [PKC 2009]

Ivan Damgard, Martin Geisler, Mikkel Kroigaard, and Jesper Buus Nielsen, Aarhus University

一般のマルチパーティ計算のための、非同期プロトコルを提案する。プロトコルは完全な安全性を持ち、通信計算量は、n をパーティの数、|C|を計算回路のサイズ、k を基礎体の要素のサイズとすると、O(n^2|C|k)となる。攻撃者が事前プロセスフェーズを終わらせたいときは、プロトコルは終了を保証するが、何の情報も公開されない。プロトコルの通信計算量は、受動的に安全な解決方式と高々定数項しか違わない。プロトコルは、n/3 以下のプレイヤーが不正をするような適応的かつ能動的な攻撃者に対して安全である。我々はまた、VIFF(Virtual Ideal Functionality Framework)と呼ばれる、非同期プロトコルを実装するためのソフトウェアフレームワークを紹介する。これにより、複雑なマルチスレッドに頼る必要なく、安全な乗算などのプリミティブな演算を自動的に並列化することができる。我々のプロトコルの VIFF 実装のベンチマークは、実際の簡単でない安全な計算に適用可能であることを裏付ける。

Multi-Party Computation with Omnipresent Adversary [PKC 2009]

Hossein Ghodosi, James Cook University; Josef Pieprzyk, Macquarie University

本論文ではマルチパーティ計算プロトコルのプライバシーを調べ、プロトコルから消し去ることのできない、偏在する攻撃者(Omnipresent Adversary)の概念を導入する。偏在する攻撃者は、受動的でも能動的でもそれらの混合でも良い。不正をする参加者の数がいかなる時にも事前に決められた閾値を超えないという制限の下で、能動的な攻撃者により買収されない少数の参加者まで受動的に不正者となり得ることを仮定する。我々はまた、n 人の参加者グループの t-resilient(t 人までが不正者であってもプロトコルは正しい)なプロトコルの存在は、n'(>= n-t) 人の参加者グループの t'(t/2 <= t' <= t)-private(t' 人までが不正者であってもプライバシーは保たれる)なプロトコルの存在を意味する。即ち、t-resilient なプロトコルから不正な参加者を消去することは、プロトコルの分解を導く。我々の攻撃モデルは、マルチ

パーティ計算プロトコルは、真に正直な参加者の集合で機能することはないことを要求する。これはより現実的なシナリオと言える。それゆえ、プロトコルに適切に従ったすべての参加者のプライバシーは保たれる。我々は、プロトコルに適切に従った参加者のプライバシーが失われることを避けるための、新しい失格(disqualification)プロトコルを示す。

1.3.2. PKC 2009 の発表（2 日目）

Blind and Anonymous Identity-Based Encryption and Authorized Private Searches on Public-key Encrypted Data [PKC 2009]
Jan Camenisch, IBM Zurich; Markulf Kohlweiss and Alfredo Rial, Katholieke Universitit Leuven; Caroline Sheedy, Dublin City University

検索可能暗号(Searchable Encryption)スキームはデータを暗号で保護しつつ、検索やアクセスを可能とする重要なメカニズムを提供する。その構成における通常のアプローチでは、暗号化するエンティティは、データの暗号化記録の内容を記述するキーワードを選択する。検索を行うときは、ユーザーは、興味のあるキーワードの落とし戸を得て、このキーワードにより記述されるすべてのデータを見つけるのに、落とし戸を使う。
我々は公開鍵設定において暗号化されたデータをキーワードで秘密に検索し、検索結果を復号することができる検索可能暗号スキームを示す。このために、2 つのプリミティブを定義し実装する。一つは PEOKS(Public key Encryption with Oblivious Keyword Search, キーワードを記憶しないキーワード検索を持つ公開鍵暗号)であり、もう一つは CBAIBE(Committed Blind Anonymous Identity-Based Encryption)である。PEOKS では、ユーザーはキーワードを漏らすことなく、秘密鍵保持者から落とし戸を得ることができる。我々は初めてのブラインドかつ匿名の IBE スキームを構成する。ブラインドとは、鍵生成エンティティが ID を知ることなしに、ユーザーが ID の復号鍵を要求することができることであり、匿名は、暗号文はそれが暗号化された鍵(ID)を漏らさないということである。これによりキーワードも検索結果も秘密にすることができる。

Anonymous Hierarchical Identity-Based Encryption with Constant Size Ciphertexts [PKC 2009]
Jae Hong Seo, Seoul National University; Tetsutaro Kobayashi, Miyako Ohkubo, and Koutarou Suzuki, NTT Labs, Tokyo

一定サイズの暗号文を持つ匿名 HIBE(Hiearchical Identity-Based Encryption, 階層型 ID ベース暗号)スキームを提案する。これは、暗号文のサイズが階層の深さに拠らないことを意味する。更に、復号フェーズにおける復号計算コストが一定であるため、我々のスキームは最小計算コストを達成する。安全性は、合成数位数の双線型群に基づいており、ランダムオラクルを用いずに、合理的な仮定の下で証明される。スキームは選択的-ID CPA 安全性を達成する。

Towards Black-Box Accountable Authority IBE with Short Ciphertexts and Private Keys [PKC 2009]
Benoit Libert and Damien Vergnaud, UCL Crypto Group and Ecole Normale Superieure

CRYPT2007 において、Goyal は ID ベース暗号における、オーソリティへの信頼依存を減らす便利なツールとして AAIBE(Accountable Authority Identit-Based Encryption)の概念を導入した。このモデルでは PKG がユーザーの復号鍵を再配布すると、捕まり訴えられる危険を冒すことになる。Goyal は 2 つのスキームを与えたが、一つは効率的ではあるが良い形の復号鍵しか追跡することができず、もう一つは、弱ブラックボックス追跡性(weak black-box traceability)を与えるよう拡張できるが、効率は悪いものであった。本論文では、効率性と非常に単純な弱ブラックボックス追跡メカニズムを持った、新しい構成を提案する。我々のスキームは選択的 ID モデルにおいて記述されるが、適応的 ID モデルにおけるすべての安全性の性質を満たすように容易に拡張できる。

Removing Escrow from Identity-Based Encryption - New Security Notions and Key Management Techniques [PKC 2009]
Sherman S.M. Chow, New York University

ID ベース暗号において、キーエスクローは生得の性質であるが、鍵生成センター(KGC)は、暗号文が誰宛のものかを知らなかったとしても、復号できるのであろうか？我々は、KGC の匿名暗号文識別不可性(Anonymous Ciphertext Indistinguishability, ACI-KGC)を定式化することにより、この問題に答える。

ランダムオラクルを用いない既存のすべてのペアリングベースの IBE スキームは、受信者が匿名か否かにかかわらず、ACI-KGC よりも弱い概念である KGC 一方向性を満たさない。この観点から、我々は Gentry の IBE スキームにいかにして ACI-KGC を持たせるかを示す。次に我々は、KGC がユーザーID のリストを知ることなく、認証されたユーザーに秘密鍵を発行することができるような匿名秘密鍵生成プロトコルを持つ新しいシステムアーキテクチャーを提案する。我々の提案は、キーエスクロー問題を、分散 KGC アプローチとは別の次元において和らげる。

A New Paradigm for Secure Protocols [PKC 2009、招待講演]

Amit Sahai, UCLA

広い意味での暗号学の基本的な目標の一つとして、いかなる悪意を持つ参加者がいても安全なプロトコルを設計することがあげられるが、1986 年に Goldreich-Micali-Wigderson により示された、正直ではあるが好奇心のある参加者に対してセキュリティを保証するプロトコルが、ここ 20 年ほど 1 つのパラダイムとして存在してきた。

本講演では、ゼロ知識証明を用いずに、参加者の多数が正直であるというより単純な設定による新しいパラダイムとなるプロトコルが示された。ゼロ知識証明を用いないことにより、プロトコルの構成要素をブラックボックスとして扱うことが可能となり、より一般的かつ効率的なプロトコルの設計が可能となった。

On the Theory and Practice of Personal Digital Signatures [PKC 2009]

Ivan Damgard and Gert Lassoe Mikkelsen, Aarhus University

より現実的な個人電子署名のモデルを考える。人間のユーザー、モバイル機器、PC、サーバーは、それぞれ独立なプレイヤーと見なし、人間のユーザーのみが不正をしないと仮定して、ユーザーの代わりに署名を発行するプロトコルを提案する。各操作フェーズにおいて高々1 つのプレイヤーしか不正をしないと仮定すれば、このプロトコルは proactive に UC 安全となる。即ち、モバイル機器と PC との両方が同時に不正をしない限りは、必ずしも信頼できるとは限らない PC を用いて安全に署名することができる。例えばフィッシングや PC のキーロギングでは、我々のプロトコルは破ることはできない。本プロトコルにより、計算能力が非常に小さいモバイル機器でも、計算を PC に安全に任せることができ、また、適切な通信を行うのであればいかなる PC でも使用することができる。本プロトコルのプロトタイプ実装についても報告する。

Security of Blind Signatures Under Aborts [PKC 2009]

Marc Fischlin and Dominique Schroder, Darmstadt University of Technology

ブラインド署名の安全性に関して、ユーザーまたは署名者が対話型署名発行プロトコルを早めに中止する場合を検討する。ブラインド署名の安全性は、プロトコルが完了することを前提とすることが多く、中断する場合に、強い安全性を要求することは、あまりない。Eurocrypt 2007 において、Camenisch-Neven-Shelat は、選択的失敗ブラインド性の概念を導入した。大雑把に言うと、選択的失敗ブラインド性とは、署名者がある実行が中断したことを知ることができる場合でもブラインド性が成り立たなければならないということである。我々は、安全なブラインド署名スキームを選択的失敗ブラインド署名スキームに変換する方法を示す。我々の変換は、コミットメントの計算を付加することのみが必要であり、オーバーヘッドは無視できる。更に、Camenisch らの唯一選択的失敗ブラインド署名から適応的紛失送信プロトコルを構成する手法を再検討する。

Security of Sanitizable Signatures Revisited [PKC 2009]

Christina Brzuska, Marc Fischlin, Tobias Freudenreich, Anja Lehmann, Marcus Page, Jakob Schelbert, Dominique Schroder, and Florian Volk, Darmstadt University of Technology

ESORICS 2005 において Atenieseらが定義したように、墨塗り署名スキームにおいては、署名者が、部分的に署名する権利を墨塗り者と呼ばれる他者に委任することができる。即ち、墨塗り者は、元のメッセージの予め決められた部分を、残りの部分の真正性および認証性が検証可能なまま、修正することができる。Atenieseらは、このようなスキームに対して求められる5つの安全性を特定し、それらを満たす例を与えたが、それらの安全性の定義を定式化していなかった。我々は墨塗り署名スキームの安全性を再検討し、初めての総合的な定式化を与え、これらの性質の関係を調べ、元のスキームを我々のモデルに沿うよう修正したスキームの安全性証明を与える。

Identification of Multiple Invalid Signatures in Pairing-based Batched Signatures [PKC 2009]

Brian J. Matt, John Hopkins University

ペアリングベース署名スキームにおいて、署名の一括検証に失敗した後、その中の無効な署名を特定する新しい方法を示す。本方式は、多数の署名の中から、無効な署名を効率的に特定する。バッチの中の無効な署名を特定するため、分割攻略による検索を行うが、ペアリング計算を大幅に削減するよう検索木を削減する。サイズ N のバッチにおける w (< N/2)個の無効な署名を特定するのに、従来の分割攻略による検索では、O(w(log_2{N/w}+1))回のペアリング積計算が必要だったが、我々の方法では、平均で O(w)回である。

CCA-Secure Proxy Re-Encryption without Pairings [PKC 2009]

Jun Shao and Zhenfu Cao, Shanghai Jiao Tong University (中国)

代理再暗号化スキームにおいて、代理人は、アリスの公開鍵による暗号文を、ボブが復号できる暗号文へ変換することができるが、平文にアクセスすることはできない。例えば暗号化電子メールの転送などに用いることができる。本論文では、知識の署名と藤崎-岡本変換を用いて、ペアリングを用いない一方向代理再暗号化スキームを提案する。提案スキームは、ランダムオラクルモデルにおいて、選択暗号文攻撃および結託攻撃に対し、$(Z/N^2Z)^*$ における Diffie-Hellman 決定問題および素因数分解問題の困難性をそれぞれ仮定すれば安全となり、両安全性を持つ一方向代理再暗号化スキームは初めてのものである。

Compact CCA-Secure Encryption for Messages of Arbitrary Length [PKC 2009]

Masayuki Abe, NTT; Eike Kiltz, CWI; Tatsuaki Okamoto, NTT (日本、オランダ)

本論文では、任意長メッセージに対し暗号文オーバーヘッドが小さい、エルガマル暗号変形タイプの選択暗号文攻撃に対して安全な公開鍵暗号スキームを提案する。暗号文のオーバーヘッドは、群要素一つ分のみである。このような性質は、バンド幅に制約のある環境において、暗証番号やクレジットカード番号などの短いメッセージを暗号化する場合に特に有効である。更に、暗号化および復号のコストは、エルガマル暗号とほとんど同じであり、安全性はランダムオラクルモデルにおいて強 Diffie-Hellman 仮定のもと証明される。

Verifiable Rotation of Homomorphic Encryptions [PKC 2009]

Sebastiaan de Hoogh, Berry Schoenmakers, Boris Skoric, and Jose Villegas, Technical University of Eindhoven (オランダ)

準同型暗号のリストが与えられたときに、検証可能な巡回プロトコルの問題を考える。すなわち、準同型暗号のリストX_0、X_1、…、X_{n-1}が与えられたとき、ある巡回オフセットrをランダムに選び、Y_kがX_{k-r}のランダムな再暗号化となるような暗号リストY_0、Y_1、…、Y_{n-1}を生成するが、オフセットは秘密にしなければならない。基本的には巡回オフセットと再暗号化の指数の知識のゼロ知識証明を用いる。我々の提案する 2 つのプロトコルのうち 1 つは、離散フーリエ変換を用いたものであり、これらの知識の効率的なゼロ知識証明の構成に初めてフーリエ変換を用いたものであるが、用いるパラメーターにある制限を加えている。もう 1 つのプロトコルはより一般的なものであり、これらの制限はないが、離散フーリエ変換ベースのプロトコルに比較するとやや効率的でない。Reiter-Wangらのプロトコルは検証可能シャフリングをサブプロトコルとして用い、4 回呼び出しているが、我々の構成は直接的であり、検証可能シャフリング 1 回相当の性能である。

1.3.3. PKC 2009 の発表(3 日目)

A practical key recovery attack on basic TCHo [PKC 2009]
Gregor Leander, Technical University of Denmark; Mathias Herrmann, HGI, Ruhr-University of Bochum (デンマーク、ドイツ)

TCHo はストリーム暗号風に設計された公開鍵暗号スキームであり、RFID などの低コストデバイスに適しているとして提案された。TCHo の基本版は IND-CCA2 セキュリティを有していないため、発明者らは Fujisaki-Okamoto 変換などを使用することを勧めているが、この場合ハードウェア規模が増大するため、低コストデバイスに適しているというメリットが失われてしまう。本論文では、d を秘密多項式の次数としたときに、およそ $d^{3/2}$ 回の復号により秘密鍵を暴く選択暗号文攻撃を示す。特に、ACISP2007 において提示されたすべてのパラメーターは、通常の PC により数時間～数十時間で解読することができる。このため、TCHo は FO 変換なしに用いることはできないが、FO 変換を用いると、低コストデバイス向きという利点が失われてしまう。

An algebraic surface cryptosystem [PKC 2009]
Koichiro Akiyama, Toshiba; Yasuhiro Goto, Hokkaido University of Education; Hideyuki Miyake, Toshiba (日本)

代数曲面のセクション求解問題(高次元多変数方程式系の求解(NP 完全問題)以外の解法は知られていない)をベースとする公開鍵暗号(代数曲面暗号と呼ぶ)を提案する。PQCrypto 2006 において発表した版の暗号アルゴリズムを改良したものであり、既知の攻撃に対して対策を施している。セキュリティパラメータを n と置いたとき、必要となる鍵サイズは、公開鍵も秘密鍵も O(n)となり、他の耐量子計算機公開鍵暗号(格子ベース暗号、多変数方程式ベース暗号、ナップサック暗号)と比較して、最小にすることができる。ただし、実現の際の適切なパラメーターはまだ与えられていない。
質疑応答
Q:復号の際の素因数分解の処理がボトルネックになるのではないか？
A:1 変数多項式の因数分解なので整数の素因数分解より簡単である。ただし、何次の多項式にすればよいかについては、具体的な値を持っていない。
Q:80 ビットセキュリティを主張できる根拠は？
A:小さいパラメータで解読実験を行い、点のプロットを延長して予測した。
Q:解読実験における解読アルゴリズムは何を使ったか？
A:一般的なセクション求解アルゴリズムを使用した。

Fast Multibase Methods and Other Optimizations for Elliptic Curve Scalar Multiplication [PKC 2009]
Patrick Longa and Catherine Gebotys, University of Waterloo (カナダ)

楕円曲線スカラー倍算において、非常に効率的なマルチベース鎖を見つける新しいアルゴリズム(Refined mbNAF 法)を提案する。Fractional ウィンドウのマルチベースへの適用、点演算公式の改良などにより、事前計算を用いない方法の中で、曲線の選択によらず、最も低コストの演算を実現した。スカラー倍算のコストはヤコビアン座標では 1459M(体の積演算)であり、inverted エドワーズ座標では 1350M であり、ヤコビ 4 次座標では 1267M となる。

Revocable Group Signature Schemes with Constant Costs for Signing and Verifying [PKC 2009]
Toru Nakanishi, Hiroki Fujii, Yuta Hira, and Nobuo Funabiki, Okayama University

あるタイプの取り消し可能グループ署名においては、署名／検証アルゴリズムの計算量は、N をグループのサイズ、R を取り消されたメンバーの数とすると、O(N)または O(R)となる。一方、Camenisch-Lysyanskaya らによるスキームは、署名／検証アルゴリズムの計算量は O(1)となるが、署名の前に秘密鍵の更新が必要となり、最悪の場合、O(R)の計算量となる。本論文では、署名／検証アルゴリズムの計算量が O(1)であり、秘密鍵の更新を必要としないスキームを提案する。その代わり、公開鍵は O(N)と長くなる。更に我々は、公開鍵の長さが O(√N)、署名／検証は一定数の余分なコストしか必

要としないスキームへと拡張した。

An Accumulator Based on Bilinear Maps and Efficient Revocation for Anonymous Credentials [PKC 2009]

Jan Camenisch, IBM Zurich; Markulf Kohlweiss, Katholieke Universiteit Leuven; Claudio Soriente, University of California at Irvine

本論文では、証明書ベースのプライバシー保護認証システムにおける取り消しの問題を考察する。現在有効な証明書の蓄積は定期的に出版され、各ユーザーは、匿名性を保ったまま信用証明の有効性を証明することのできる証拠を持つが、ユーザーの証拠は、少なくとも信用証明が取り消されるたびに更新しなくてはならず、ユーザーと証明書発行者双方の計算コストが問題となっている。
本論文では、双線型写像に基づいた、新しい動的蓄積スキームを提案し、匿名信用証明の取り消しの問題にどのように適用するかを示す。本スキームにおいては、信用証明の有効性を証明することと証拠の更新は、信用証明の保持者にも検証者にも、(仮想的に)コストをかけずに行うことができる。これにより、eID カードのような電子トークンや運転免許証などの実装に適した、プライバシーの保護を持つ初めての認証システムを提供する。

Controlling Access to an Oblivious Database using Stateful Anonymous Credentials [PKC 2009]

Scott Coull, Matthew Green, and Susan Hohenberger, Johns Hopkins University

本論文では、コンテンツ提供者が、匿名のユーザーにより実行される、記憶されないプロトコル(Oblivious Protocol)において複雑なアクセス管理ポリシーを強制することを可能にすることを考える。我々の主要な応用として、紛失送信(Oblivious Transfer)と増強された匿名信用証明システムを組み合わせることにより、プライバシーの保護されたデータベースの構築法を示す。これにより、データベースのオペレーターは、ユーザーの ID や項目の選択を知ることなしに、各ユーザーがどの項目にアクセスしてよいかを制限することができる。我々の構成は広範囲のアクセス管理ポリシーをサポートし、金融や防衛のアプリケーションに使用される Brewer-Nash や Bell-Lapadula などのポリシーを効率的かつプライベートに実現する。更に我々のシステムは、標準モデルにおける標準的な仮定に基づいており、初めの設定フェーズにおいては、各トランザクションは一定時間しか必要としない。

1.4. Eurocrypt 2009 の発表

1.4.1. Eurocrypt 2009 の発表(1 日目)

Possibility and Impossibility Results for Encryption and Commitment Secure under Selective Opening. [Eurocrypt 2009]
Mihir Bellare, Dennis Hofheinz, Scott Yilek

SOA(Selective Opening Attack)のもとで安全な暗号およびコミットメントスキームの存在は未解決であったが、この設定における送信者の不正に対して安全な初めての公開鍵暗号を、Lossy Encryption のテクニックを用いて示す。更に、非対話型もしくは完全に binding なコミットメントスキームは、標準的な計算量仮定へのブラックボックス帰着により安全と証明されないが、静的に hiding な任意のコミットメントスキームは安全となることを示す。

Breaking RSA Generically is Equivalent to Factoring [Eurocrypt 2009]
Divesh Aggarwal, Ueli Maurer

Z/NZ において RSA 暗号を解読する一般的な環アルゴリズムは、対応する RSA のモジュラス N を素因数分解するアルゴリズムに変換できることを示す。この結果は、N を素因数分解することなしに RSA 暗号を解読する試みは、一般的な環アルゴリズムではなく、従って Z/NZ における入力の特殊なビット表現を扱わなければいけない。RSA 暗号を解読することは、モジュラス N を素因数分解することに等価であろうことの新しい証拠と言える。

Resettably Secure Computation [Eurocrypt 2009]
Vipul Goyal, Amit Sahai

リセット可能なゼロ知識(Resettable Zero Knowledge, rZK)の概念は、FOCS01 において、Canetti、Goldreich、Goldwasser、Micali らにより、従来のゼロ知識の概念を強化するために導入された。rZK プロトコルは、検証者がプロトコル実行の任意の時点において、証明者を初期状態に戻し、同じランダムテープを何度も使用させることができたとしても、ゼロ知識のままとなる。我々はより一般的な機能に対するリセット可能性を研究する。はじめに 2 者間の計算におけるリセット可能性、即ち、一方(ユーザー)が他方(スマートカード)をリセットできるという設定を考える。この設定において、任意の PPT 計算可能機能を安全に実現するプロトコルを構成できることを示す。これにより、暗号プロトコルにおいて、ランダム性と状態を保持することへの依存を弱くすることができる。次に、多数のパーティが公正である、同時にリセット可能なマルチパーティ計算プロトコルを構成する。

On the Security Loss in Cryptographic Reductions [Eurocrypt 2009]
Chi-Jen Lu

ほとんどの重要な暗号プロトコルの安全性は、証明されていない仮定に基づいているが、それらは P≠NP を示唆するため、条件のない安全性証明は難しいように思われる。従って、研究の努力は、より基本的なプリミティブを定め、プロトコルの安全性をこれらのプリミティブに帰着させることになるが、しばしば、プロトコルの安全性は、より弱い(例えば実行時間がより少ない)攻撃者に対して測られることがある。我々は 2 つの最も基本的な暗号帰着、即ち、一方向性関数の困難増幅および一方向性関数からの乱数生成器構成を取り上げる。これらがある種のブラックボックス帰着によりなされる場合、このような安全性の低下は避けられないことを示す。

Practice-Oriented Provable-Security and the Social Construction of Cryptography [Eurocrypt 2009 招待講演]
Phillip Rogaway (米国、IBM)

証明可能安全性は、STOC1982 の Goldwasser-Micali による記念碑的論文に始まったが、MIT にいた 1980 年代半ばから後半にかけての時代は、証明可能安全性理論の鶏鳴期であり、Goldwasser/Micali らと非常に楽しい時を過ごした。1990 年代の初めに IBM へ移り、暗号の科学をコンピューターセキュリティへ実現することとなった。科学から技術そして社会への発展モデルで言えば、科学は発見し、産業は適用し、人間が社会に適合するというモデルがあてはまる。アプローチとしては、理論と実現という2つの帽子によるアプローチを取った。IBM でよく聞かれた質問の 1 つは、Kerberos をどう思うかというものであり、Kerberos は聞いたことがないとよく答えたが、Kerberos は何の問題を解決するものなのか明確にわからず、その後の 91 年の[BGHJKMY91]の仕事などに啓発され、93 年に Bellare と、エンティティ認証などの証明可能安全的に扱う論文を発表した。IBM でよく聞かれたもう 1 つの質問は、DEA 等の対称鍵暗号に関する質問であったが、古典的な証明可能安全性の理論は、漸近的な対象を扱っており、有限の対象に適用できないため、これらの対称鍵暗号の実際のセキュリティを扱えるよう、Practice-Oriented な証明可能安全性の理論を考え、新しい概念を導入し、1997 年に発表した[BDJR97]。2002 年に Shamir は、暗号研究は確かなものであるが、そのうち最も単純なアイディアのみが実際に役立つにすぎないであろうと言ったが、我々の理論は ANSI、CRYPTREC、IEEE、ISO/IEC、NESSIE、NIST、RFC、RSA/PKCS 等数多くの標準で採用され、成功していると言えるのではないか。

On Randomizing Hash Functions to Strengthen the Security of Digital Signatures [Eurocrypt 2009]

Praveen Gauravaram, Lars R. Knudsen (デンマーク)

メッセージランダム化アルゴリズム RMX を使用した hash-then-sign 電子署名スキームに対する存在的偽造攻撃を示した。Crypto 2006 で Halevi と Krawczyk は、hash-then-sign 署名スキームが、ハッシュ関数の耐衝突性に安全性を依存しないよう、ハッシュの前にメッセージをランダム化する手法(RMX)を示した。2008 年の NIST Special Publication(SP) 800-106(2nd ドラフト)には、RMX の variant が記載されている。本論文では、Merkle－Damgard ハッシュ関数の第二原像を求める Dean のテクニック(固定点拡張可能メッセージ)を使用し、Davies-Meyer 圧縮関数を使う t ビットの RMX ハッシュ関数をベースとした署名スキームに対し、$2^{t/2}$ の選択メッセージ、$2^{t/2+1}$ の(オフライン)圧縮関数計算、$2^{t/2}$ のメモリにより、存在的偽造を行う方法を示す。

Cryptanalysis of MDC-2 [Eurocrypt 2009]

Lars R. Knudsen, Florian Mendel, Christian Rechberger, Soeren S. Thomsen (デンマーク、オーストリア)

本論文では MDC-2 に対する衝突攻撃および原像攻撃を示した。MDC-2 は、1988 年に IBM の研究者 Meyer と Schilling らにより提案された、n ビットブロック暗号から 2n ビットハッシュ関数を構成する方法であり、1990 年 3 月に US 特許が発行され、1994 年に ISO/IEC 10118-2 で標準化された。衝突攻撃では、ベースとなるブロック暗号には非標準的なことは仮定せずに、バースデイ境界を下回る攻撃を示す。例えば 128 ビットブロック暗号で MDC-2 によりハッシュ関数を構成した場合、本衝突攻撃の計算量は約 $2^{124.5}$ となる。また、原像攻撃では、タイムメモリトレードオフとなる方法であり、時間計算量と空間計算量との積は約 2^{2n} となり、空間計算量は $1 \sim 2^n$ の間の値を取る。これまでの最良の攻撃は 1992 年に Eurocrypt で発表された Lai/Massey らによる、時間計算量約 $2^{3n/2}$、空間計算量約 $2^{n/2}$ となる攻撃である。本論文の攻撃では、時間計算量は約$(n+1)\ 2^n$、空間間計算量は約 2^{n+1} となる。

Cryptanalysis on HMAC/NMAC-MD5 and MD5-MAC [Eurocrypt 2009]

Xiaoyun Wang, Hongbo Yu, Wei Wang, Haina Zhang, Tao Zhan (中国)

HMAC/NMAC-MD5 への関連鍵を使わない識別攻撃を示した。dBB 衝突という新たな種類の衝突を探し、dBB 衝突が見つかったときには HMAC/NMAC-MD5 と判定することにより、2^{97} 回の問い合わせで、成功確率 87%で、ランダム関数の HMAC/NMAC と区別することができる。これまでの結果は、33 ラウンドに削減された MD5 を用いた HMAC に対して $2^{126.1}$ 回の問い合わせで、成功確率 92%であった。
更に、MD5-MAC に対しては、dBB 衝突は識別攻撃に使えるのみならず、2^{97} 回の問い合わせで、128 ビット部分鍵を回復する攻撃にも使用することができる。

Finding Preimages in Full MD5 Faster than Exhaustive Search [Eurocrypt 2009]

Yu Sasaki, Kazumaro Aoki (日本)

フル MD5 ハッシュ関数に対する原像攻撃を示した。本攻撃により、$2^{116.9}$ の計算量により MD5 の pseudo 原像を求め、$2^{123.4}$ の計算量により MD5 の原像を求めることができる。メモリ計算量は $2^{45}\times 11$ ワードである。これまでのフル MD5 に対する最良の攻撃は同著者らにより SAC2008 にて発表されたものであり、$2^{125.7}$ の計算量により MD5 の pseudo 原像を求め、2^{127}の計算量により MD5 の原像を求めるものであった。Local 衝突テクニックの一般化、absorption 性質の拡張、キャリーによらない部分固定テクニック、効率的な整合性チェックの改良など、ステップ削減した MD5 に用いられていたテクニックを一般化・改良することにより、より広い範囲のハッシュ関数に適用できるようにした。

Asymmetric Group Key Agreement [Eurocrypt 2009]

Qianhong Wu, Yi Mu, Willy Susilo, Bo Qin, Josep Domingo-Ferrer

グループ鍵共有(GKA、Group Key Agreement)プロトコルの定義を見直し、従来の(対称)グループ鍵共有と非対称グループ鍵共有(ASGKA、Asymmetric Group Key Agreement)プロトコルとを区別する。非対称グループ鍵共有においては、共通の秘密鍵の代わりに、暗号化鍵の共有を交渉する。この暗号化鍵は攻撃者がアクセスすることができ、各々が一人のグループメンバーのみにより計算可能な異なる復号鍵に対応する。ASBB(Aggregatable Signature Based Broadcast)という新しいプリミティブを使用した 1 ラウンドの非対称グループ鍵共有プロトコルを提案する。双線型ペアリングを用いることにより、効率的な ASBB スキームを実現する。一般的な構成に従い、1 ラウンドの非対称グループ鍵共有プロトコルが、標準モデルにおいて決定双線型 Diffie-Hellman 指数仮定にタイトに帰着されることを示す。

Adaptive Security in Broadcast Encryption Systems (with Short Ciphertexts) [Eurocrypt 2009]

Craig Gentry, Brent Waters

放送型暗号システムにおいて、適応的安全性を達成する新しいテクニックを示す。非常に短い暗号文を持ち、結託攻撃に完全に耐性のあるこれまでの放送型暗号システムは、静的な安全性しか考慮していなかった。はじめに、準静的安全性を新しく定義し、準静的安全システムから同程度のサイズの暗号文を持つ適応的安全システムへの変換を示す。次に双線型写像を用いることにより、標準モデルにおいて準静的安全で一定サイズの暗号文を持つ放送型暗号システムを構築する。システムにおけるインデックスもしくは ID の数が、セキュリティパラメーターに関して多項式であれば準静的安全な構成は成功する。ID ベース放送型暗号に関しては、潜在的なインデックスもしくは ID の数は指数的となるかもしれないが、暗号文サイズが sublinear となる初めての、標準モデルにおいて適応的安全なシステムを示す。

Traitors Collaborating in Public: Pirates 2.0 [Eurocrypt 2009]

Olivier Billet, Duong-Hieu Phan (フランス)

不正利用者追跡スキームに対する新たな攻撃の概念 Pirates 2.0 を導入した。名前の由来は、公な方法で不正者利用が結託することから来ている。結託の古典的モデルにおいては、不正利用者は海賊デコーダーのために各々の鍵全体を寄与し、お互い(もしくは第三者機関)を信頼しなければならない。Pirates 2.0 における結託では、不正利用者は互いを信頼する必要はなく、海賊デコーダーのために各々の鍵の一部を寄与すればよく、追跡不可能性を保証される。Pirates 2.0 攻撃のターゲットとして、符号ベーススキームと、NNL(Naor-Naor-Lotspiech)フレームワークを取り上げた。NNL フレームワークは、CRYPTO 2001 で発表され、HD-DVD やブルーレイディスクのコンテンツ保護技術 AACS のベースとなっている技術である。これらに対する Pirates 2.0 攻撃の可能性・必要な結託者数等を分析した。

1.4.2. Eurocrypt 2009 の発表(2 日目)

Key Agreement from Close Secrets over Unsecured Channels [Eurocrypt 2009]
Bhavana Kanukurthi, Leonid Reyzin

本論文では同一ではないが相関のある、同じ長さの秘密を持つ2者による、能動的攻撃に対し無条件安全な鍵共有の方法(安全でない通信路(unsecured channel)から安全な(認証暗号)通信路(secure channel)を作る方法)を研究している。この手の問題に関しては、情報一致(information reconciliation)あるいは秘匿性増幅(privacy amplification)あるいは曖昧抽出器(fuzzy extractors)などの名称で数多くの研究が行われてきた。Renner と Wolf は上記の2者が安全でない通信路から情報理論的安全な認証暗号通信路を構成できる事を示したが [RW04]、多項式時間プロトコルについて具体的記述を行わなかった。また Dodis らは、頑健曖昧抽出器(robust fuzzy extractor)なる多項式時間1ラウンドプロトコルを提案したが、非対話性(1ラウンド)のためにエントロピー損失が大きく、2つの秘密が半分以上一致する必要があった [DKR06]。本論文では、エントロピー損失が秘密の長さやエントロピーと事実上無関係で、セキュリティパラメタのみに依存する多項式時間プロトコルを提案し、PC上の実装結果について報告している。80 ビットセキュリティ(鍵)に対して 100,000 ビット程度の秘密を用い、2.4GHz Pentium 4 上で各参加者 1.5 秒程度の計算時間と 1 秒程度の通信時間で実装出来たとの事。

Order-Preserving Symmetric Encryption [Eurocrypt 2009]
Alexandra Boldyreva, Nathan Chenette, Younho Lee, Adam O'Neill

順序保存暗号(order-preserving encryption, OPE)とは、平文の順序と暗号文の順序が一致するような確定対称鍵暗号の事で、元々データベースの研究分野で暗号化されたデータの効率的な範囲照会(range query)を可能とするため Agrawal らにより提案された [SIGMOD 04]。その後、順序保存暗号はセンサーネットワークやマルチメディアコンテンツ保護の分野でも参照されるようになったが、暗号学的な安全性の研究は行われていなかった。このような暗号が標準的な意味の IND-CPA を達成出来ない事は明らかなので、本論文では順序保存暗号に適した安全性要件を研究し、平文空間に対して必要な暗号文空間のサイズなどに着目し、次の結果を得ている。

- 順序保存暗号の安全性として IND-CPA の自然な拡張である IND-OCPA(indistinguishability under ordered chosen-plaintext attack)を定義した。そして順序保存暗号が IND-OCPA を満たすには平文空間に対し暗号文空間を極端に(漸近的な意味では指数関数的に)大きくしなければならない事、即ち、(例えば平文空間が 128bit 等の)実用的な順序保存暗号は IND-OCPA を達成し得ない事を示した。
- 上記の結果により識別不可能性を諦め、順序保存暗号の安全性として、疑似ランダム置換の安全性要件 PRP-CCA の自然な拡張 POPF-CCA(pseudorandom order- preserving function under CCA)を提案した。また、順序保存関数と超幾何分布および負超幾何分布の関係を示し、超幾何分布のサンプリングアルゴリズム、または負超幾何分布の近似サンプリングアルゴリズムを利用して、ブロック暗号に基づく POPF-CCA 順序保存暗号を構成した。

A Double-Piped Mode of Operation for MACs, PRFs and PROs: Security beyond the Birthday Barrier [Eurocrypt 2009]
Kan Yasuda

任意長の入力を持つハッシュ関数や MAC のような暗号プリミティブは、圧縮関数あるいはブロック暗号の繰り返し構造によって構成される事が多い。このような、固定入力長の暗号プリミティブ(暗号学的基本関数)を任意入力長の同種の関数に変換する方法を定義域拡張(preserving domain extension, Pr)と呼ぶ。大抵の場合ベースとなる暗号プリミティブは出力長もまた固定である。その値を n bit とすると、例えば、Markle-Damgard 構成や CBC モードのような定義域拡張は、この出力長に合わせて n bit の中間状態を持つ。そして、このような n bit しか中間状態を持たない定義域拡張には、誕生日攻撃を使った中間状態の衝突に基づく汎用的攻撃戦略が存在しており、その攻撃計算量 O(2^{n/2}) (下位プリミティブ照会数)は誕生日"障壁"(birthday "barrier")と呼ばれている。Lucks はこの手の攻撃を排する為、出力長より大きな中間状態を持つ二列管路ハッシュ関数(double-pipe hash)を

考案した [17]。本論文では Lucks の二列管路構成を改造して、誕生日障壁を超える照会計算量 O(2^{5n/6})が証明出来る MAC-Pr を初めて構成した。その他、同様の技法を用いて照会計算量 O(2^n)の疑似ランダム関数定義域拡張(PRF-Pr)、疑似ランダムオラクル定義域拡張(PRO-Pr)を構成した。これらは同じ安全性の従来法より効率が良い。

On the Security of Cryptosystems with Quadratic Decryption: The Nicest Cryptanalysis [Eurocrypt 2009]

Guilhem Castagnos, Fabien Laguillaumie

NICE 暗号系は 1999 年に Hartmann らにより提案された虚二次体の整数環のイデアル類群の構造を使った公開鍵暗号である[HPT99]。暗号学的に注目すべき特徴は、この暗号が効率のよい(二次計算量の)復号アルゴリズムを持つ事である。NICE 暗号系に対する暗号解析は、Jaulmes と Joux の選択暗号文鍵回復攻撃[JJ00]以外は知られていなかった。本論文では NICE 暗号系の多項式時間選択平文鍵回復攻撃(即ち完全解読)を提示している。暗号設計者の主張によると、NICE 暗号系の完全解読に対する安全性は、使用する二次体の判別式の素因数分解の困難性にのみ依存するとされていた[HPT99]。しかしこの暗号の公開鍵には、高速復号に不可欠なイデアル類群の特殊な元が含まれており、この元が判別式の素因子に関する情報を持っている。本論文では、この元を用い三次計算量で判別式を素因数分解するアルゴリズムを提案している。標準的な PC による実験の結果、暗号学的な例に対しても一秒以下で暗号解析が完了する事が確かめられたとしている。

Cube Attacks on Tweakable Black Box Polynomials [Eurocrypt 2009]

Itai Dinur, Adi Shamir

大抵の暗号系は秘密変数(例:秘密鍵)と公開変数(例:平文/初期ベクトル)の両方を含む GF(2)上の“調整可能多項式系(tweakable polynomials)”で記述することができる。攻撃者は公開変数に好きな値を代入して多項式を調整し、それらの式に共通の秘密変数の多項式方程式の終結式系を解くことを目標とする。本論文ではそうした調整可能多項式系を解くための新しい技法、即ち cube 攻撃を提案し、従来の代数的攻撃手法の効率を大きく改善したとしている。調整可能多項式の適当な公開変数 k 個の組みについて、あらゆる可能な値($\in\{0,1\}^k$)を代入し得られる多項式系の和をとる事により、方程式を高い確率で線形化出来る事実に基づいた攻撃で、統計的な手法は使用せず純粋に代数的な攻撃であるが、GF(2)上では高階差分攻撃あるいは積分攻撃(SQUARE 攻撃)の概念と近い。n 個の変数を持つ次数 d のランダムな調整可能多項式に対して、変数のうちの d+log_d n 個以上が公開変数として使用できる時、その攻撃計算量は $2^{d-1}n+n^2$ であり、n に対して多項式である。従って d が小さい暗号系は cube 攻撃で容易に攻撃可能である。ストリーム暗号 Trivium の初期化ラウンド数 1152 を 672 に削減した修正-Trivium に関して、従来のベストアタックのビット演算量は 2^{55}(Fischer, Khazaei, Meier)であったが、cube 攻撃なら 2^{19} となる(PC1 台で 1 秒以下)。従来法では解読できなかった初期化ラウンド数 735 の場合でも、cube 攻撃ならビット演算量 2^{30} で解読できる。初期化ラウンド数 767 ならビット演算量 2^{45} で解読できるが、この計算量はおそらく 2^{36} 程度まで削減できるであろうとのこと。

Smashing SQUASH-0 [Eurocrypt 2009]

Khaled Ouafi, Serge Vaudenay

RFID Security Workshop 2007 にてAdi Shamir は RFID に適した Rabin 公開鍵暗号に基づく質疑応答プロトコル(challenge-response protocol)、SQUASH を提案した。このプロトコルには当初、線形混合関数(linear mixing function)が利用されていたが、すぐ後で非線形混合関数に変更された為、元のプロトコルを SQUASH-0 と呼んでいる。本論文では Rabin-SAEP に対する“既知ランダム硬貨攻撃(know random coin attack)”を完全窓(full window,ビット列の切り出しが無いこと)の SQUASH-0 に適用し、さらに任意窓の SQUASH-0 への攻撃に拡張した。この攻撃を使えば、推奨パラメタの法 $2^{1277}-1$ に関して 1024 個の選択質疑(chosen challenge)を使って鍵回復攻撃が可能と報告している。SQUASH の最終版に対しても、同様の安全性の議論が適用できるが、この攻撃は非線形混合関数を用いたときには非効率的であり、SQUASH の安全性の議論は未解決とのこと。

1.4.3. Eurocrypt 2009 の発表(3 日目)

Practical Chosen Ciphertext Secure Encryption from Factoring [Eurocrypt 2009]
Dennis Hofheinz, Eike Kiltz

Cramer-Shoup 暗号のような標準モデルで標準的な暗号学的仮定に帰着する CCA 安全で実用的な公開鍵暗号系が良く研究されている。これらの暗号系は基本的に判定問題の困難性に依存している。一般に判定問題の困難性は計算問題の困難性よりも強い仮定なので、Cash-Kiltz-Shoup 暗号や Hanaoka-Kurosawa 暗号のような計算問題の困難性に帰着する暗号系が研究されるようになった。しかし、これまで標準モデルで素因数分解問題(あるいは RSA 問題)の困難性に帰着する実用的な暗号は存在しなかった。本論文では標準モデルで素因数分解問題の困難性に帰着する CCA 安全な実用的公開鍵暗号系を提案している。必要な計算量は、冪乗剰余換算で、暗号化およそ2回、復号およそ1回であり、実用的である。この論文は Eurocrypt 2009 の最優秀論文賞を受賞した。

Realizing Hash-and-Sign Signatures under Standard Assumptions [Eurocrypt 2009]
Susan Hohenberger, Brent Waters

標準モデルで安全な“hash-and-sign”型の(tree 型でない)署名が幾つか存在するが、大抵 Strong RSA や q-Strong DH のような、都合の良い強い仮定に依存している。本論文では標準モデルで安全な hash-and-sign 型の署名を実現するための新しい方法を提案する。この方法では、署名者はその時点までに発行した署名の数を示す指数 i を各署名に割り当てる。この割り当てを利用して、2^{[lg(q)]} 以下の指数に関する署名の偽造に q 個の署名の照会が必要となるよう攻撃者を制限する技法を開発し、この制限された攻撃者を取り扱う方法を開発した。この方法に従ってRSA 仮定と双線形群上の CDH 仮定に基づく2つの署名を実現した。本論文の方式では署名者は状態(署名発行数カウンター)を管理する必要があるが、同じ著者らが RSA 仮定に基づく状態無しの署名を CRYPTO 2009 に投稿し受理されており、同内容と思しき論文が IACR の ePrint に投稿されている。

http://eprint.iacr.org/2009/283.pdf

A Public Key Encryption Scheme Secure against Key Dependent Chosen Plaintext and Adaptive Chosen Ciphertext Attacks [Eurocrypt 2009]
Jan Camenisch, Nishanth Chandran, Victor Shoup

鍵管理系や匿名信用証明系においては、誰かの秘密鍵に何らかの暗号化を施して送受信する事がある。この時、システムの設計によっては、秘密鍵の暗号化が循環してしまう場合があり、そのような鍵の使用状況を鍵循環(key cycle)と呼ぶ。最も単純な鍵循環は秘密鍵がその鍵自信(あるいは対応する公開鍵)で暗号化されるような状況で、例えば暗号化ディスクの使用者がそのディスク上に秘密鍵(あるいはそのハッシュ値)のバックアップを作成してしまうような事象を、うまく抽象している。このような秘密鍵に依存した文書の暗号化に関する安全性を鍵依存文書(key dependent message, KDM)安全性と呼ぶ。Boneh, Halevi, Hamburg, Ostrovsky(BHHO)は Crypto 2008 にて、標準モデルで DDH 仮定に基づき鍵依存選択平文攻撃に対し強秘匿(KDM-CPA 安全)な公開鍵暗号系を提案したが、KDM のもと CPA と CCA2 を同時に満たす(KDM-CCA2 安全な)暗号系に関しては未解決のままであった。本論文はこの問題を解決している。まず Naor-Yung の“二重暗号化(double-encryption)”の方法論を使って任意の KDM-CPA 安全な暗号系と任意の(普通の)CCA2 安全な暗号系を組み合わせ、適当な非対話ゼロ知識証明を加えることにより、KDM-CCA2 安全な暗号系が得られる事を示した。次に、上記の BHHO 暗号と CCA2 安全な(一般化)Cramer-Shoup 暗号を組み合わせ、最近開発されたペアリングに基づく非対話証明を加えて、KDM-CCA2 安全な暗号系の実例を構成した。この暗号の計算量は BHHO 暗号の計算量と(小さい)定数倍の違いしかない。

Salvaging Merkle-Damgård for Practical Applications [Eurocrypt 2009]
Yevgeniy Dodis, Thomas Ristenpart, Thomas Shrimpton

ハッシュ関数を用いた多くのアプリケーションが安全性の解析にランダムオラクルモデルを使用している。

しかし、SHA ファミリーのような具体的なハッシュ関数は、大抵何らかの圧縮関数に(強化)Markle-Damgård(MD)変換を反復適用して構成されており、仮に理想的な圧縮関数を利用したとしても、そうした"構造的"ハッシュ関数は、一般にランダムオラクルとして使用できない事が良く知られている。MD 構成を用いたハッシュ関数に至っては length extention 攻撃に対する脆弱性のような大きな欠点が知られており、とてもランダムオラクルと呼べるような代物ではない。それでも、多くのアプリケーションに対しては、こうした事実に基づく重大な攻撃が見つかっている訳ではない。単に安全性の保証が全くできていないだけである。本論文では、この状況を克服すべく以下の条件の下、衝突困難(CR)より強くランダムオラクル(RO)より弱いハッシュ関数の抽象概念を研究している。

(a) ランダムオラクルなら満たしているような自然で美しい性質であること
(b) アプリケーションの安全性を議論するのに十分強い(CR より強い)性質であること
(c) 何らかの強い性質の圧縮関数の(強化)MD 変換がその性質を持つ事が証明可能であること

そして、(a)-(c)を満たす二つの抽象概念、原像認知関数(preimage aware function)と公用ランダムオラクル(public-use random oracle)を提案し、以下の結果を得た。

- MD 変換は原像認知の性質保存変換(property-preserving transform)である
- h(x)を固定入力長ランダムオラクル(FIL-RO)、H(x)を可変入力長原像認知関数(VIL-PrA)とすると、関数 F(x) = h(H(x)) は可変入力長ランダムオラクル(VIL-RO)と強識別不能(indifferentiable)である
- 固定入力長衝突困難関数の様々な実例がまた原像認知を満たしている
- MD 変換は公用ランダムオラクル強識別不能性の性質保存変換である
- 固定長圧縮関数用の公用ランダムオラクルの変種を考えた

異なる研究グループから、関連する研究結果が発表されている。

http://eprint.iacr.org/2009/040.pdf
http://eprint.iacr.org/2009/075.pdf

On the Security of Padding-Based Encryption Schemes (Or: Why we cannot prove OAEP secure in the Standard Model) [Eurocrypt 2009]
Eike Kiltz, Krzysztof Pietrzak

padding ベースの暗号系とは、OAEP のように、暗号化アルゴリズムがまずメッセージに可逆な公知の変換、即ち padding を適用し、続いて落し戸置換を行うような公開鍵暗号の事である。本論文では、padding ベースの暗号系が標準モデルで CCA 安全である事を black-box 的に証明することは、たとえ理想落し戸置換の存在を仮定しても不可能である事(black-box separation)を示した。理想落し戸置換とは一様ランダム置換の安全性要件をすべて受け継いだ落し戸置換の事である。

Simulation without the Artifical Abort: Simplified Proof and Improved Concrete Security for Waters' IBE Scheme [Eurocrypt 2009]
Mihir Bellare, Thomas Ristenpart

Boneh-Boyen の IBE [6]はランダムオラクルモデルにも q-BDHI 仮定のような強い仮定にも依存せず、選択的 ID 攻撃に対する安全性が標準モデルで DBDH 仮定へ多項式帰着可能であるが、適応的 ID 攻撃に対する安全性は指数的帰着による証明しか与えられていなかった。Waters は幾分大きい公開パラメタを使って、Boneh-Boyen の IBE のこの欠点を克服し、適応的 ID 攻撃に対する安全性が標準モデルで DBDH 仮定へ多項式帰着可能な IBE を提案した [31]。この提案はペアリングを用いた暗号系やプロトコルの研究に大きい影響を与え、既に多種多様の用途に応用されているが、"人為的中止(artifical abort)"ステップを使った比較的複雑な安全性証明の為に、直観的で確実な安全性や暗号系の効率性が損なわれてしまっている。多くの研究者が Waters の IBE の安全性証明から人為的中止ステップを除去可能であるか否かを問い、このステップが除去不可能で安全性の本質であろうと予想していた。本論文では Waters の IBE に対して、人為的中止の無い比較的簡単な安全性証明を与え、このステップが安

全性の本質ではないことを示している。新しい安全性証明は、いくつかの実用的なパラメータ範囲において従来より良い帰着効率を与えており、結果としてこのパラメータ範囲では従来よりも小さいサイズの群が利用可能になっている。従来より帰着効率の悪い領域では従来の証明を使って群のサイズを選べば良い。小さい群を用いることにより、60～70 ビット安全性の範囲では最大 9 倍程度、80～100 ビット安全性の範囲では最大 5 倍程度の速度向上が見込めるとのこと。

On the Portability of Generalized Schnorr Proofs [Eurocrypt 2009]

Jan Camenisch, Aggelos Kiayias, Moti Yung

(知識の)ゼロ知識証明[ZKP]は暗号学において中心的な考え方であり、具体的なプロトコル設計に必要不可欠な一連の安全性概念を与えるのに使用される。これらの安全性概念は、あらゆる入力および検証者の内部状態に対して定義され、より大きいアプリケーションのサブルーチンとしての如何なる用途にも適用可能となるよう企図されている。しかし、ほんの少しのコスト増加も許されないような現実的なプロトコルの設計現場においては、僅かな効率改善の為に上記のような理論的な安全性概念を幾分逸脱した効率的なプロトコルが使用される事がある。こうしたプロトコルは“あらゆる”入力および検証者の内部状態に対して安全性を満たしている訳ではないので、いろいろな問題を抱えることになる。特に一般化 Schnorr 証明(GSP, 未知位数群上の Schnorr 証明)に関しては、何年もの間、沢山のアプリケーションで誤用が行われてきた。本論文では、あるプロトコルが大きいアプリケーションの逐次実行中にサブプロトコルとして呼ばれたとき、そのプロトコルがゼロ知識証明になるような入力と検証者の内部状態の分布を明らかにするプロトコル移植性(protocol portability)なる概念を導入し、非常に効率的で重用されている GSP に関して、そのプロトコル移植性を明らかにしている。また、プロトコル設計者に広く使用されている記法を改良した GSP プロトコルのためのコンパクトな仕様言語を与えている。それから GSP をどうしても使いたい設計者に対する代替案として無条件に移植性のある極めて効率の良い改良版 GSP プロトコルを示す。この構成は標準モデルで証明可能安全な最初の GSP プロトコルである。またこのフレームワークを既知のアプリケーションプロトコルに適用して、安全性に必要な仮定の抽出やプロトコルの効率化が見通し良く可能な事を(この論文の full version で)示した。

A Unified Framework for the Analysis of Side-Channel Key Recovery Attacks [Eurocrypt 2009]

Francoix-Xavier Standaert, Tal Malkin, Moti Yung

本論文では、サイドチャンネル攻撃に対して妥当な物理的仮定を研究し、サイドチャンネル攻撃の現実的なモデルを提案している。このモデルは計算によって漏洩が起こるというサイドチャンネルに関する広く受け入れられている仮定に基づいている。このモデルは、サイドチャンネルが本質的に漏らしている観測可能な情報に関する計量(情報理論的計量)と、サイドチャンネル解析アルゴリズムがノイズ込の信号から抽出できる情報に関する計量(実効的安全性計量)の2つの異なるタイプの計量を必要とする。そして、それらの計量の間の形式的関係を示し、それらの直感的意味を議論する。それから、このフレームワーク(定理)の現実的なシステムへの適用を議論し、統一的な評価の方法論を導く。

A Leakage-Resilient Mode of Operation [Eurocrypt 2009]

Krzysztof Pietrzak

弱擬似ランダム関数(wPRF)は擬似ランダム関数(PRF)によく似た暗号プリミティブであるが、疑似ランダム関数より弱い仮定しか持たない。wPRF の疑似ランダム性は、ランダムな入力に対してのみ成立すれば良い。本論文では wPRF は“普通の”PRF と違い、種圧縮不可能(seed-incompressible(秘密鍵の部分情報が漏えいしても(弱)疑似ランダム性が壊れないこと))であることを示した。そして、その応用として、どのような wPRF を使用しても“耐漏洩ストリーム暗号(leakage-resilient stream-cipher) ”を与える単純な暗号利用モードを構成した。このような暗号は、例え全体として任意長の秘密の漏洩の可能性があっても、ラウンド当たり漏洩する情報量が制限される限り“あらゆる”サイドチャネル攻撃に対して安全である。このような暗号系は既に存在しているが(Dziembowski-Pietrzak FOCS'08)、本論文の構成法はより単純である(その分証明は複雑とのこと)。

1.4.4. Eurocrypt 2009 の発表(4 日目)

ECM on Graphics Cards [Eurocrypt 2009]
Daniel Bernstein, Tien-Ren Chen, Chen-Mou Cheng, Tanja Lange, Bo-Yin Yang (米国、台湾、オランダ)

素因数分解の楕円曲線法(ECM)は、1987 年に H.W.Lenstra Jr.により導入され、現在では、10^{10}～10^{60}の範囲の一般の素因数分解に適していると考えられている。数体篩法(NFS)は、より大きな数の素因数分解を高速に行うが、その際、多くのより小さな補助的な整数の素因数分解を組み合わせる。補助的な整数の素因数分解を行う際に、ECM を用いることがあるが、どの程度の大きさの整数を ECM で素因数分解すべきかは ECM の実装速度に依存する。ECM の高速化は、NFS の高速化、ひいては NFS により素因数分解可能な整数を大きくするために非常に重要である。本論文では、ECM のプラットフォームとして GPU(Graphics Processing Unit)を使用することを提案し、そのための高速化テクニックおよび実験結果を述べる。ECM のバウンド制御パラメーターB1=8192 に取った場合、NVIDIA GTX295 は、1 秒あたり 41.88×10^6 回の280ビットモジュラ積演算が可能となり、Core 2 Quad Q6600 上の GMP-ECM では、1 秒あたり 13.03×10^6 回の 280 ビットモジュラ積演算が可能であった。Core 2 Quad Q6600 1 台とNVIDIA GTX295 2 台を組み合わせたシステムにおけるコストパフォーマンスは、Core 2 Quad Q6600 1 台のコストパフォーマンスと比較して、約 3 倍良い値となった。

Double-Base Number System for Multi-Scalar Multiplications [Eurocrypt 2009]
Christophe Doche, David Kohel, Francesco Sica

JSP(Joint Sparse Form)は、[n]P+[m]Q の形のマルチスカラー倍算を行うための標準的な表現システムである。n と m を同時に表現するために、DBNS(Double-Base Number System)の一般化として、JDBC(Joint Double-Base Chain)という概念を導入する。更に JDBC を与える単純で実装の容易な効率的なアルゴリズムを与える。展開における項の平均値は、0.3945log_2{n}となり、JSF に対して加算数を20%以上削減し、P+Q と P-Q の 2 つの事前計算を使う方法の中で、スカラー倍算に必要な乗算の数が最小となる。更に、基礎体 GF_{2^d}における高々2 回の乗算と 2 回の 2 乗算により、Frobenius 双対自己準同型を既存の最速手法より 50%高速化する。

Endomorphisms for Faster Elliptic Curve Cryptography on a Large Class of Curves [Eurocrypt 2009]
Steven Galbraith, Xibin Lin, Michael Scott

効率的に計算できる準同型が存在すれば、GLV(Gallant-Lambert-Vanstone)法により、楕円曲線の点の倍算を高速にすることができる。我々は、GF(p^2)で考えることにより楕円曲線の大きなクラスに対し、このような準同型を与える IMCT(飯島-松尾-趙-辻井)の結果を拡張し、GLV 法を適用できることを示す。Frobenius 展開が使える部分体曲線の場合を除いて、一般に楕円曲線の点倍算の実行時間は既存の最速法の 75%程度になることが期待され、実装では、70%から 84%程度になった。

Generating Genus Two Hyperelliptic Curves over Large Characteristic Finite Fields [Eurocrypt 2009]
Takakazu Satoh

超楕円曲線暗号に適した曲線の必要条件の一つは、ヤコビアンの位数が大きな素数と小さな数との積で書けることである。与えられた y^2=x^5+ux^3+vx の形の超楕円曲線のヤコビアンが、そのような性質を満たすか否かをテストし、もし満たすならば、その最大素因子を与える、確率的多項式時間アルゴリズムを示す。本アルゴリズムにより、ヤコビアンの位数が上記の意味でほぼ素数となるまで、上記の形の曲線をランダムに生成することができる。鍵となるアイディアは、ヤコビアンがスプリットする拡大体上のゼータ関数から基礎体のゼータ関数の候補を得ることである。

Optimal Randomness Extraction from a Diffie-Hellman Element [Eurocrypt 2009]
Pierre-Alain Fouque, Sebastien Zimmer, David Pointcheval, Celine Chevalier

有限体 Z/pZ の乗法群の素数位数部分群 G および楕円曲線の有理点群におけるランダムな Diffie-Hellman 要素からランダム性を引き出す決定的アルゴリズムを示す。大雑把に言うと、G のランダムな要素の最下位ビットもしくは E(F_p)のランダムな点の x 座標の最下位ビットはランダムなビット列と区別がつかないことを示す。このような操作は非常に効率的であり、LHL(Leftover Hash Lemma)とほぼ同程度のビット数を引き出すことができるため、良い乱数エクストラクターと言うことができる。べき和をバウンドするための新しいテクニックにより、Fouque らが ICALP06 で提案した方法よりも引き出すビット数を 2 倍にすることができ、また、Canetti らのバウンドも改良した。応用としては、CRYPTO07 で提案され、NIST による ECPRG(Elliptic Curve Pseudo Random Generator)の安全性証明に使われた仮定を数学的に証明することができ、また、与えられた Diffie-Hellman 要素から効率的に鍵を取り出すことができる。

Verifiable Random Functions from Identity-based Key Encapsulation [Eurocrypt 2009]

Michel Abdalla, Dario Catalano, Dario Fiore

検証可能ランダム関数(VRF, Verifiable Random Function)に適していると我々が呼ぶ ID ベース鍵カプセル化メカニズム(IB-KEM, Identity Based Key Encapsulation Mechanism)のクラスから VRF を構成する方法論を示す。大雑把に言うと、IB-KEM は、UD(Unique Decryption, ID に関して生成された暗号文が与えられたとき、別の ID'に対応するすべての秘密鍵による復号は同じ値となる)という性質を持ち、更に PRD(PseudoRandom Decapsulation, ID に関して生成された暗号文を、別の ID'に対応する秘密鍵で復号すると、能力を多項式に制限された観察者に対してはランダムに見える)という性質を満たすならば VRF に適している。既知の IB-KEM のほとんどは、PRD をすでに満たしていることを示す。我々の方法論は、ほとんどの既存の構成法と比較して、非効率的な Goldreich-Levin ハードコアビット変換を避けているという点において直接的な構成法であると言える。

A New Randomness Extraction Paradigm for Hybrid Encryption [Eurocrypt 2009]

Eike Kiltz, Krzysztof Pietrzak, Martijn Stam, Moti Yung

標準モデルにおいて IND-CCA2 安全なハイブリッド暗号スキームを設計する新たなアプローチを示す。我々のアプローチは、ハッシュ証明システム(Hash Proof System)において、1-ユニバーサルから 2-ユニバーサルへの効率的な一般的変換を与える。変換は、鍵導出関数として、4-点独立(4-wise independent)なハッシュ関数に基づいたランダム性エクストラクターを含む。我々の方式は、決定 Diffie-Hellman、平方剰余、Paillier の決定 CR(Composite Residue)などの標準的で困難な仮定に基づいた効率的なスキームにおいて具現化される。我々のフレームワークで、1991 年の Damgard による ElGamal 公開鍵暗号スキームのハイブリッド版の DDH 仮定の下での IND-CCA 安全性を証明することができる。

1.4.5. Eurocrypt 2009 rumpの発表

AES-256 is Not Ideal [Eurocrypt 2009 rump]
Alex Biryukov, Dmitry Khovratovich, Ivica Nikoli¥'{c} Dmitry Khovratovich

256bit 鍵AES(AES-256)のベストアタックは14ラウンド中の10ラウンドの攻撃に対して、2^6個の関連鍵、2^{114} のデータ、2^{173} の時間計算量を必要とするものであった。本研究では、フルラウンドの AES-256 に対する選択鍵識別攻撃および関連鍵攻撃を構成した。まず、差分 q-多衝突(differential q-multicollision)の概念を定義した。そして n をブロックサイズとすると、理想暗号(ideal cipher)の q-多衝突の構成には、およそ ～ q 2^n 程度の計算量(少なくとも O(q $2^{n\ (q-1)/(q+1)}$))が必要なのに対して、AES-256 の q-多衝突が q 2^{67} の時間計算量と無視しうる領域計算量で構成可能な事を示し、実際にPC 上の数時間の計算で部分 5-衝突の現実的識別攻撃を行った。また、理想暗号では証明可能安全なDavies-Meyer モードの AES-256 に対して、同様の手法と計算量で q-擬衝突を構成出来る事を示した。その他、2^{131} の時間計算量と鍵当たり 2^{96} のデータを用いて 2^{35} 個の関連鍵のうちの 1 つを鍵回復できる(関連鍵攻撃が可能)としている。この結果は“Distinguisher and Related-Key Attack on the Full AES-256”のタイトルでCrypto 2009にて発表予定である。また、同じ研究グループから、選択鍵のシナリオではなく全ての鍵に適用できる、ブーメラン攻撃を使ったこの攻撃の改良が報告されている。フルラウンドの AES-256 に対してデータおよび時間計算量 2^{119} 領域計算量 2^{77} で攻撃可能とのこと。注意深く解析すれば、計算量を $2^{110.5}$ まで削減できるかもしれないとの情報もある。さらにフルラウンドの AES-192 に対しても、増幅ブーメラン攻撃を使ってデータ計算量 2^{123} 時間計算量 2^{176} 領域計算量 2^{152} で攻撃可能とのこと。これらの結果がAESを直接使う現実的なアプリケーションに対して今すぐ脅威となることは無いが、AES を使用したハッシュ関数の理論的安全性に関しては何らかの影響を与えるかもしれない。

http://eprint.iacr.org/2009/317.pdf

Attacks on MRG ciphers [Eurocrypt 2009 rump]
Lu Xiao, Greg Rose

MRG 暗号(Multiple Recursive Generator)は、センサーノードやRFIDタグのような計算資源限定環境での暗号用途のため、IEEE GLOBECOM 2008 国際会議にて A. Olteanu らによって提案された軽量ブロック暗号である。本研究では、次の2つの効率的な攻撃を提案している。

(1) 218 個の暗号文と対応する平文の最上位ビットを使った、提案者が示したパラメタの MRG に対する識別攻撃
(2) 暗号の内部状態と続いて使用される副鍵を生成する既知平文攻撃。k を MRG の次数とすると、最適化されたMRG暗号に対して2k個の既知平文と僅かな計算量しか必要としない。また最適化されていなくとも、例えば次数 47 の MRG 暗号に対して 2^{12} ほどの既知平文と 2^{24} 回の以下の MRG 演算で攻撃可能である。

以上の事実により MRG 暗号には重大な欠陥があると断じている。詳細は以下を参照せよとの事。

http://eprint.iacr.org/2009/128

Computational Indistinguishability Amplification: Provable Security Amplification by Cascade Encryption [Eurocrypt 2009 rump]
Ueli Maurer, Stefano Tessaro

計算量的識別不能性の増幅(computational indistinguishability amplification)に関する汎用的なフレームワークを構築した。このフレームワークによると、ε<1/2 のとき、任意の数の異なる ε-PRP をカスケードすると安全性が向上する事の他に、ε>=1/2 でも Randomized Cascade なら任意の数の異なる strong ε-PRP をカスケードすると安全性が向上する事が示されたとの事。この結果は“Computational Indistinguishability Amplification: Tight Product Theorems for System Composition”のタイトルでCRYPTO 2009 に受理された。

Distinguishing Attacks on Highly-Iterated Ciphers [Eurocrypt 2009 rump]
Gregory Bard, Nicolas Courtois, Shaun Ault

ランダム置換πに対して、π^kの不動点の数の期待値を$\tau(k)$とする。kが素因子を沢山持つと$\tau(k)$が大きくなるのでπ^kとランダム置換との識別が容易になる。即ち同じ PRP をカスケードするとkを素数にしない限り一般には安全性が落ちる。

Message Authentication Codes from Unpredictable Block Ciphers [Eurocrypt 2009 rump]
Yevgeniy Dodis, John Steinberger

unpredictable なブロック暗号から birthday security の任意入力長 keyd MAC を構成するモードを提案した。使用するブロック暗号が PRF なら MAC も PRF である。また、CBC などと違い“leaky block-cipher” model で PRF である事が証明出来、サイドチャネル攻撃に耐性を持つ。Rate は 3 で CBC などより 3 倍遅い。安全性は概ね birthday barrier 程度。この結果は “Message Authentication Codes from Unpredictable Block Ciphers” のタイトルで CRYPTO 2009 に受理された。

Automatic Differential Path Searching for SHA-1 [Eurocrypt 2009 rump]
Cameron McDonald, Josef Pieprzyk, Phil Hawkes

既知の SHA-1 の最良の完全な差分経路は計算量2^{63}のものであった。2008 年 11 月に Stéphane Manuel が2^{57}の計算量の新しい擾乱ベクトル(disturbance vector)を公表したが、最初の 20 ステップの差分経路は示されなかった。Joux と Payrin のハッシュに関する増幅ブーメラン攻撃(amplified boomerang attack)を用いると、この最初の 20 ステップに対して独立な n 個の補助差分経路を持つ非線形差分経路を見つければ、攻撃の計算量を2^{57-n}に削減することが出来る。本報告によると、この 20 ステップに対してなるべく多くの補助経路を持つ非線形差分経路を探索したところ、5 つの補助経路を持つ差分経路が見つかったので、計算量2^{52}の完全な差分経路が見つかったとのこと。この報告が事実であれば、現実的な衝突の発見が、比較的大きな計算資源を持つ団体(大企業など)の手の届く範囲に到達したと解釈できる。詳細は以下を参照のこと。(ベースとなる論文に誤りが見つかったため、この論文は 2009 年 8 月 10 日に取り下げられた。)

http://eprint.iacr.org/2009/259

Beer-recovery analysis [Eurocrypt 2009 rump]
Jean-Philippe Aumasson and Dmitry Khovratovich Dmitry Khovratovich

SHA-3 候補の KECCAK に対して解析を行った結果、設計者の主張と矛盾するところは無かった。

More Differential Paths for TIB3 [Eurocrypt 2009 rump]
Harry Wiggins, Cameron McDonald, Phil Hawkes, Greg Rose Greg Rose

SHA-3 候補の TIB3 に対して解析を行った結果、使用されている鍵スケジュールと PHTX 関数に対して新しい性質を発見した。既知の擬衝突差分経路に関してはメッセージに差分が無かったが、この性質によってメッセージに差分のある新しい差分経路が見つかった。

The Biometric Passport: the Swiss Case [Eurocrypt 2009 rump]
Serge Vaudenay

1997 年に ICAO(International Civil Aviation Organization)が設立され、バイオメトリクスに基づく機械読み取り可能旅行文書(MRTD,machine-readable trabel documents)の制定作業が開始された。2004 年には ICAO MRTD 標準が公開され現在 50 ヵ国で採用されている。2006 年には拡張仕様(EAC, extended access control)が制定された。米国のビザ免除は ICAO 準拠のパスポートを必要としている。また、欧州のシェンゲン協定はあらゆるパスポートがバイオメトリックであることが必要としている。2008 年

6 月 13 日、スイス政府がこのパスポートおよびバイオメトリックサーバを導入する法案を提出した。スイスでは新しい法律に対して、ある一定期間内に 5 万人の反対者が集まると、法案が国民投票にかけられる。この法案は 2009 年 5 月 17 日に国民投票にかけられることに決まっている。この問題に対する一般の投票というのは初めての事で、結果が注目される。現在の情勢では賛成と反対が拮抗している。(その後、5 月 17 日に実際に国民投票が行われ、辛くも 50.14% の賛成によって可決されたとのこと。)

Conditional Multiple Differential Attack on MiFare Classic Smart Cards [Eurocrypt 2009 rump]
Nicolas T. Courtois, University College London

MiFare は FeliCa(フェリカ)と同じ 13.56MHz の近距離無線通信技術を搭載した非接触 IC カードのシリーズで、12 億個の IC カード用チップと、500 万台のリーダが出荷されたと言われており、世界で最も普及した非接触型 RFID カードのシリーズである。1994 年 MIFARE Standard(MiFare Classic)が発表されると 1996 年には韓国ソウルの交通機関で採用され、以降、ロンドン、北京、台北、釜山、香港、ドイツ、オランダ、等の公共交通機関でも採用された。この MiFare Classic は ID カードや社員証、入館証、会員証等にも幅広く利用され、少なくとも 2 億枚以上の使用実績があると推計されている。2007 年 12 月にリバースエンジニアリングにより、MiFare Classic のアルゴリズムの解析や幾つかの脆弱性が報告されると、2008 年 3 月には、認証/暗号化アルゴリズムが特定され、効率的な鍵回復及びクローンカードの作成といった現実的な脆弱性が指摘され、普通のノートパソコンを使ってロンドン地下鉄の乗車用スマートカードが現実に偽造できる事が示されるに至っている。これらの指摘を受けて 2008 年 3 月に MiFare Classic の代替として 128 ビット鍵の AES を使った MiFare Plus いう拡張規格が発表され、成人識別 IC カード taspo 等に使用されている。従来、MiFare Classic のクローンカードを作成するには、使用されているカードリーダーを入手するか、通信傍受などの手段で通信履歴を入手する必要があった。本発表ではそうした手段を用いずに、カードに数百回の照会を行うだけでクローンカードが作成出来るとの報告が行われた。内容は以下の論文の改良で、"THE DARK SIDE OF SECURITY BY OBSCURITY - and Cloning MiFare Classic Rail and Building Passes, Anywhere, Anytime"のタイトルで SECRYPT 2009 にて発表予定とのこと。

http://eprint.iacr.org/2009/137

Efficient Leakage-Resilient Public-Key Cryptograhpy [Eurocrypt 2009 rump]
Krzysztof Pietrzak and Eike Kiltz

標準モデルで安全で Leakage-resilient なストリーム暗号および tree-based 署名は存在するが、tree-based 署名は実用的でないし公開鍵暗号については未解決である。本発表では良くつかわれる系に対して Leakage-resilient な実例を研究し、Bilinear ElGamal 暗号および Waters 署名に対して汎用群モデル(generic group model)で証明を付け。幾分疑わしい仮定の下で ElGamal 暗号にも証明を付けたとの事。異なる研究グループから、以下の関連する研究結果が発表されており、"Public-Key Cryptosystems Resilient to Key Leakage" なるタイトルで Crypto 2009 に受理されている。

http://eprint.iacr.org/2009/105.pdf

Public Key Cryptography in the Bounded Retrieval Model [Eurocrypt 2009 rump]
Joel Alwen, Yevgeniy Dodis and Daniel Wichs

Leakage Attacks に対して、従来の relative leakage モデルでは、漏洩限界(leakage bound,実際に漏洩が許される情報量)はセキュリティパラメタに依存している。コンピューターウイルスが計算機から情報を盗み出すような状況を想定した時、RSA の 1024 bit の鍵の内の何パーセントが漏洩しているかを問うのは実効的な安全性の議論とはならないであろう。本研究では、Bounded Retrieval Model を用い、予め決められた漏洩限界によって秘密鍵の長さを決定する事によってこの問題を解決しようとしている。秘密鍵の長さが公開鍵等のパラメタに影響が出ないようにする必要がある。この結果は"Leakage-Resilient Public-Key Cryptography in the Bounded-Retrieval Model"のタイトルで Crypto 2009 に受理された。

A Billion-mulmods-per-second PC [Eurocrypt 2009 rump]

Daniel J. Bernstein, Hsueh-Chung Chen, Ming-Shing Chen, Chen-Mou Cheng, Chun-Hung Hsiao, Tanja Lange, Zong-Cing Lin, and Bo-Yin Yang

ECM 用の PC で、パーツを厳選すれば1台につき 13 億回/秒の 192 bit 一般法剰余乗算を実現でき、そのハードウェアコストは 1 台当たり 1997 米ドル(およそ 20 万円)と見積もられたとの報告。GeForce GTX 295 2 枚刺し構成と AMD K10 上の技巧的なプログラムを使用した場合の見積もりとのこと。

Securrity Proofs for OAEP in the Standard Model [Eurocrypt 2009 rump]

Eike Kiltz and Adam O'Neill

OAEP の安全性に関する話題。もし F が一方向なら F-OAEP は IND-CPA かつ plaintext-aware であることがランダムオラクルモデルでは証明されていたが、スタンダードモデルでは様々な否定的な結果が得られていた。本発表では、OAEP で使用されるハッシュの一つが 2-wise independent なる性質を持つなら、F が lossy trapdoor permutation のとき F-OAEP が IND-CPA であることが証明されたと報告された。RSA は Φ-Hiding 仮定のもと lossy である事と組み合わせて RSA-OAEP が Φ-Hiding 仮定のもと IND-CPA であるという系が得られる。

Practical Forgery of ISO 9796-2:2002 RSA Signatures [Eurocrypt 2009 rump]

Jean-Sebastien Coron, David Naccache, Mehdi Tibouchi, Ralf-Philipp Weinmann

1999 年 Coron, Naccache, Stern は 2 つの普及していた RSA 署名標準 ISO/IEC 9796-1,2 に対して存在的偽造を発見した。この攻撃を受けて、ISO/IEC 9796-1 は取り下げられ、ISO/IEC 9796-2 はメッセージダイジェストの長さが最低 160bit となるよう修正された。この修正版への攻撃は少なくとも 2^{61}の演算が必要であるとされた。本研究では、アルゴリズムの改良により、修正版の ISO/IEC 9796-2 のどのサイズの法に対しても攻撃が可能となることを示した。素因子が知られていない RSA-2048 challenge modulus に対し、e=2 の場合に、Amazon EC2 grid 上の 19 個のサーバを用いて、たった 2 日で現実的な偽造を構成出来たと報告されている。指数が奇数の場合でもそれほど時間が延びるわけではないとのこと。この結果は“Practical Cryptanalysis of ISO/IEC 9796-2 and EMV Signatures”のタイトルで CRYPTO 2009 に受理された。

http://eprint.iacr.org/2009/203.pdf

Fully Homomorphic Encryption Using Ideal Lattices [Eurocrypt 2009 rump]

Craig Gentry

自身の復号回路(および NAND 復号回路)を評価可能な暗号系 E があれば、それを用いて proxy re-encryption(暗号が KDM 安全性を持つなら、只の re-encryption)を構成し、NAND を使って回路を構成する事により、あらゆる回路を評価可能な暗号系が作れる。イデアル格子を使った暗号系は、元々環準同型性を持っているが、一般に演算の度に暗号文が大きくなってしまうので非自明な環準同型暗号は実現出来ない。しかし、上記の復号回路の構成が十分に小さければ E が構成可能となり得るので、工夫して復号回路の演算量を小さくし、実現したとのこと。STOC 2009 にて発表された“Fully Homomorphic Encryption Using Ideal Lattices”の内容。

Factoring Integers in Polynomial Time [Eurocrypt 2009 rump]

Claus P. Schnorr

Schnorr は 1993 年に適当な数論的仮定の下、素因数分解問題が同時ディオファントス近似問題に帰着できる事を示した。この同時ディオファントス近似問題は Schnorr-Adleman 素数格子なる格子の近似最近ベクトル問題(CVP)に容易に帰着できる。従って、もし非常に効率的な格子基底縮小アルゴリズムがあれば、効率的に素因数分解が可能となる。この発表では、幾つかの仮定(GSA(Geometric Series Assumption)等)の下で平均実行時間が高速な新しい CVP/SVP アルゴリズム“NEW ENUM”に関する報告が行われた。仮定が成立する条件等詳細については未確認。

1.4.6. Eurocrypt 2009 posterの発表

Physically Unclonable Pseudorandom Functions [Eurocrypt 2009 poster]
Frederik Armknecht, Ahmad-Reza Sadeghi, Pim Tuyls, Roel Maes, Berk Sunar

物理的複製不能関数(Physically Unclonable Function, PUF)は IC 内に秘密鍵の耐タンパー記憶を実現するための低コストな技術である。しかし PUF の応答には雑音が含まれ、外部環境の影響を受け結果が変化しやすいため、それ以外の暗号技術に応用される事が無かった。本研究ではPUFを使って耐タンパー性を持つ疑似ランダム関数(PRF)の実現を検討する。まず、PUF の理論的なモデルを与え、現実的な PUF の実装により正当化する。そのモデルを使って耐タンパー性を持つ疑似ランダム関数(PUF-PRF)の構成法を示す。但し、幾つかの理由により PRF を PUF-PRF で直接置き換えられる訳ではないとのこと。

Automatic Generation of sound Zero-Knowledge Protocols [Eurocrypt 2009 poster]
Endre Bangerter, Jan Camenisch, Stephan Krenn, Ahmad-Reza Sadeghi, Thomas Schneider

効率的な知識の零知識証明(ZK-PoK)は認証、グループ署名、秘匿多者計算などの多くの暗号学的応用をもつ基本プロトコルであり、既に世の中で多用されている。最も顕著な例が Trusted Computing Group(TCG)に採用され、Trusted Platform Module(TPM)の関数のひとつとして実装されている Direct Anonymous Attestation(DAA)である。しかし、ZK-PoK は暗号や署名に比べて幾分複雑なため、暗号技術に明るくない開発者が実装すると、演算時間が大きくなったり、誤実装が起こりがちである。本研究グループでは自動生成した健全な ZK-PoK プロトコルによる ZK-PoK の実現と、暗号およびセキュリティ技術者の利用を簡易化する研究を行っている。この目的の為、ZK-PoK プロトコルの安全で効率的な実装の自動設計と自動生成をサポートするプロトコルおよびコンパイラを開発している。

http://eprint.iacr.org/2008/471.pdf

On the Data Complexity of Statistical Attacks Against Block Ciphers [Eurocrypt 2009 poster]
Céline Blondeau, Benoît Gérard

繰り返しブロック暗号に対する多くの攻撃が沢山の平文/暗号文ペアを使って暗号の何らかの部分をランダム置換から識別する統計的な考察に依存している。そうした識別攻撃に必要な平文/暗号文ペアの量を見積もる簡単な数式を提案する。この数式はいろいろなシナリオ(線形解読, 差分線形解読, 差分/切詰差分/不能差分攻撃)に適用可能である。従って、これらの攻撃の漸近的なデータ計算量が導かれる。さらに、データ計算量を正確に計算する効率的なアルゴリズムを与える。

http://eprint.iacr.org/2009/064.pdf

Anonymity from Asymmetry: New Constructions for Anonymous HIBE [Eurocrypt 2009 poster]
Dan Boneh, Leo Ducas

階層型 ID ベース暗号(HIBE)は、もし暗号文が公開鍵に関する如何なる情報も与えないなら匿名(anonymous)であるという。安全な HIBE を構成する方法はたくさんあるが、匿名 HIBE を与える方法はそれよりずっと少ない。本研究は IBE と HIBE の構成方法のある大きな族を匿名 IBE および HIBE 系に変換する非対称ペアリングの使用方法を示す。そのうちの一つは委任可能秘匿ベクトル暗号(delegatable hidden vector encryption)に拡張可能である。

http://www.eleves.ens.fr/home/ducas/publi/ahibe/

Pairing with Supersingular Trace Zero Varieties Revisited [Eurocrypt 2009 poster]
Emanuele Cesena

トレース零多様体(Trace Zero Varieties, TZV)は超楕円 C/F_q 上の因子類群の特別な部分群で、定義

体の小次数拡大 F_q^r 上有理である。TZV は、高速算術および群構成に活用できるので暗号応用上大変興味深い。さらに、超特異 TZV を使うと超特異楕円曲線より高い bit 当たりの MOV 安全性を実現できるので、ペアリングに基づく暗号においても興味深い。本研究では q-フロベニウスの作用を利用した超特異 TZV 上の Tate ペアリングの新しいアルゴリズムを提案している。また、標数 2 の体上定義された超特異 TZV の実験結果を示している。

http://eprint.iacr.org/2008/404.pdf

Odd-Char Multivariate Hidden Field Equations [Eurocrypt 2009 poster]
Ming-Shing Chen, Jintai Ding, Chia-Hsin Owen Chen, Fabian Werner, Bo-Yin Yang

本研究では、新しい多変数公開鍵暗号(MPKC)を提案している。この MPKC は、秘密の非線形写像(hidden central map)に少数の小奇標数中サイズ有限体上ランダム二次式を採用しており、(本質的に幾つかの変数を 0 に固定する)追加"埋め込み"修正子(extra "embedding" modifier)を持っている。これら既知のアイディアを組み合わせ、他のどの MPKC よりも効率的でスケーラビリティのある MPKC を構成した。奇標数への切り替えが、攻撃者の方程式の使い方に影響する。グレブナー基底アルゴリズムを使って HFE や関係する MPKC を攻撃する時、この事が特に大きい違いをもたらす。

http://eprint.iacr.org/2008/543.pdf

Finding Good Linear Approximations of Block Ciphers and its Application to Cryptanalysis of Reduced Round DES [Eurocrypt 2009 poster]
Rafal Fourquet, Pierre Loidreau, Cédric Tavernier

本研究では、m-変量 Boolean 関数の与えられた bias 内の線形近似リストを決定するアルゴリズムを設計した。松井によって得られた最良 bias と同じオーダーの bias を持つ 8 ラウンドの DES の多重近似を見つけるために、このアルゴリズムをどう適用するか示した。結果として、一次 Reed-Muller 符号の軟判定復号(soft decision decoding)の技法に基づく大変効率的な新しい攻撃を提案する。

http://ced.tavernier.free.fr/index_fichiers/Articles/Linear_Approximations.pdf

Public Key Cryptography on Modern Graphics Hardware [Eurocrypt 2009 poster]
Owen Harrison, John Waldron

近年 GPUs(Graphics processing units)を汎用用途に使用する事例が増えている。本研究では、RSA のような公開鍵暗号の核ともいえる、大きな整数の冪乗剰余を DirectX 10 準拠 GPU 上で実装する方法を提案している。DirectX 10 準拠は GPU の最新世代アーキテクチャであり、柔軟なプログラミングが可能で、整数演算も使用可能である。標準的な位取り記数系(radix number system)および剰余記数系(residue number system)の両方の整数表現に基づく演算効率の高い冪乗剰余の実装法を提案している。そして 1024-bit RSA 復号関数において、同じレベルの CPU 実装に対して 4 倍もの性能を達成する GPU 実装の構築方法を示す。それから、位取り記数系および剰余記数系の両モジュールを含む GPU 実装が、総合性能で最上の結果を与えるようなモジュールの適応的選択方法を与える。また GPU を使って公開鍵暗号の演算性能を改善するのに必要な基準を明らかにした。

https://www.cs.tcd.ie/~harrisoo/publications/PKonGPU_eurocrypt.pdf

Statistical Tests for Key Recovery Using Multidimensional Extension of Matsui's Algorithm 1 [Eurocrypt 2009 poster]
Miia Hermelin, Joo Yeon Cho, Kaisa Nyberg

松井のアルゴリズム 1 において 1 鍵ビットの正しさの判定に対し、本質的にただ 1 つの二項分布統計量、バイアスあるいは相関が存在する。多次元(multidimension)の場合は正しい鍵の候補を探すための異なる統計的アプローチが利用可能である。本研究の目的は理論的あるいは実際にそうした判定の効率

を調べ、多次元線形近似(multidimensional linear approximation)に基づく分布を用いた新しい鍵クラス順位統計量(key class ranking statistic)および Selçuk により提案された順位統計量の一般化を提案することである。

http://www.tcs.hut.fi/Publications/mhermeli/dags-unif-alg1.pdf

The Key-Dependent Attack on Block Ciphers [Eurocrypt 2009 poster]

Xiaorui Sun and Xuejia Lai (Shanghai Jiao Tong University, P.R.China)

本研究では鍵依存攻撃(key-dependent attack)と呼ばれる、鍵依存性(key-dependent property)を用いた攻撃系を定式化する。この攻撃では分布が鍵に依存する中間変数に着目する。中間変数の統計的仮説の判定によって鍵が正しいか否かを決定する。鍵依存攻撃の時間およびデータ計算量についても議論する。そして、ラウンド縮小 IDEA に対して鍵依存攻撃を適用した。攻撃は Biryukov-Demirici 方程式の内のいくつかの項目の鍵依存分布に基づいている。5.5 ラウンド修正 IDEA に対する攻撃は 2^{21} の選択平文と $2^{112.1}$ 回の暗号化を必要とする。6 ラウンドの場合は 2^{49} の選択平文と $2^{112.1}$ 回の暗号化を必要とする。従来の攻撃と比較して、どちらの攻撃もそれぞれ最小の時間およびデータ計算量を持つ。

On Privacy Losses in the Trusted Agent Model [Eurocrypt 2009 poster]

Paulo Mateus, Serge Vaudenay

耐タンパデバイス(tamper-proof devices)はかなり強力な暗号学的仮定であり、それを使うと(耐タンパ仮定が破られない限り)大抵のセキュリティアプリケーションが簡単に構成できる。しかし、デバイスが悪意を持って利用されると、プライバシーが必要なアプリケーションで幾つかの性質が(仮に出来たとしても)実現困難となる。本研究では、否認可能性、無証拠性、匿名性が破られる例を取り上げている。

http://eprint.iacr.org/2009/286.pdf

Solving Low-Complexity Ciphers with Optimized SAT Solvers [Eurocrypt 2009 poster]

Karsten Nohl, Mate Soos

安くて、秘密仕様の暗号関数が RFID チケット、携帯電話、盗難防止などの組込アプリケーションで広く使用されている。こうした暗号には、しばしば統計的あるいは代数的攻撃が見つかる。代数的攻撃は拡散の非線形性が十分でないような暗号の脆弱性を見つけるのに強力な道具である。SAT solver はそうした脆弱性を見つける自動暗号解析ツールとなり得る。本研究では SAT solver の挙動と暗号の表現の両方を繰り返し調整し、暗号の攻撃を行った。その結果 MiFare Classic の Crypto-1、eSTREAM Portfolio の Trivium の簡易化版 Bivium でベストアタックを更新した。また、フィリップス社 RFID の HiTag2 の攻撃にはじめて成功した。

http://planete.inrialpes.fr/~soos/publications/Low-complexity-poster.pdf

A Geometric Approach on Pairings and Hierarchical Predicate Encryption [Eurocrypt 2009 poster]

Tatsuaki Okamoto, Katsuyuki Takashima

述語暗号(predicate encryption, PE)の概念は、ID ベース暗号、隠れベクトル暗号(hidden-vector encryption, HVE)、属性ベース暗号を含む一般化概念として Katz, Sahai, Waters によって提案された。Katz らの方式は既知の方式の中で最も記述能力の高い属性秘匿述語暗号であるが、委任機能(delegation functionality)を持ってない。Shi, Waters は述語暗号のあるクラスに対して委任機構(delegation mechanism)を提案したが、適用可能な述語が HVE の等価性のみで、Katz らの内積述語(inner-product predicate)に対しては適用できなかった。本研究ではペアリングに関する新しい幾何的アプローチに基づいてこの問題に取り組み以下の結果を得た。

- 内積述語に対する階層型述語鍵カプセル化機構(hierarchical predicate KEM, HPKEM)の提案

- 双ペアリングベクトル空間(dual pairing vector space, DPVS)に対する汎用モデル(generic model)での HPKEM の安全性証明

Generic Attacks on Feistel Networks with Internal Permutations [Eurocrypt 2009 poster]
Jacques Patarin, Joana Treger

本研究では内部関数に置換を用いている Feistel network に対する汎用的な攻撃を与える。この攻撃では置換はランダムであると仮定される。Twofish, Camellia, DEAL のような、いくつかの現実的な Feistel 暗号が実際に内部関数に置換を用いているにもかかわらず、そうした暗号はそれほど研究されてない。それらはいつも一般の Feistel network のように挙動する訳ではない。(既知平文あるいは選択平文)攻撃はときどき(即ち 3, 6, 9,…ラウンドの時)非効率的になる。この結果は驚くべき事で、置換を用いた Feistel network に対する汎用攻撃は、特別の注意深い解析を要する事を示している。2n bit サイズの平文に対してラウンド数が 5 段以下の時、攻撃計算量は 2^{2n}より純粋に小さい。また、ラウンド数 k が大きい時、k-ラウンド Feistel network とランダム置換の識別が可能となる攻撃を記述する。この結果は同名のタイトルで AFRICACRYPT 2009 にて発表された。

Could The 1-MSB Input Difference Be The Fastest Collision Attack For MD5? [Eurocrypt 2009 poster]
Tao Xie, Dengguo Feng, Fanbao Liu

2004 年に Wang らは、どのブロックにも 3-bit の入力差分がある MD5 の 2 ブロック衝突差分を発見した。2007 年に Xie らも、同じ性質をもつ別の 2 ブロック衝突差分を発見している。これらの差分は後にそれぞれ 1 分および 30 分以内にデスクトップ PC 上で衝突が発見出来るよう改良されたが、他の衝突差分、あるいは、より効率の良い衝突アルゴリズムが課題として残されていた。本研究では、1MSB 入力差分(ワード境界の MSB に差分があること)しか持たない新しい衝突差分を提案し、詳細に解析し、完全衝突差分特性を示した。この方法で衝突を生成するのには、まだ 2 ブロックメッセージが必要ではあるが、第一ブロックは 1MSB 差分しか持たず、第二ブロックは全く同じである(疑衝突)。新しい差分特性は明らかに計算困難であるが、衝突探索効率を劇的に改善する分割統治戦略を提案している。結果として、平均計算量が $2^{20.96}$(単位 MD5 圧縮計算)の衝突攻撃アルゴリズムが得られた。これは、現在最速の攻撃であり、任意のランダムな初期値に対して一般的な PC 上で 1 秒以内に衝突を発見でき、妥当な確率で 1/1000 秒以内に衝突が見つかるとのこと。現実的なプロトコルの実行中の攻撃に使用することが出来る。

http://eprint.iacr.org/2008/391.pdf

1.5. Pairing 2009 の発表

1.5.1. Pairing 2009 の発表(1 日目)

Boneh-Boyen signatures and the Strong Diffie-Hellman problem [Pairing 2009/ECC 2009]
David Jao and Kayo Yoshida

Boneh-Boyen 署名は偽造不可能性が標準モデルで q-Strong Diffie-Hellman 仮定へ帰着可能なペアリングに基づく署名であるが、今まで q-Strong Diffie-Hellman 仮定が破れる時 Boneh-Boyen 署名が敗れるか否かは分かっていなかった。本論文では、これを証明し、Boneh-Boyen 署名の偽造が q-Strong Diffie-Hellman 問題の求解と真に等しい事を示した。また、この等価性と q-Strong Diffie-Hellman 問題に対する良く知られた指数時間攻撃(Cheon の攻撃) を使って、大抵のペアリング向け曲線上で Boneh-Boyen 署名の秘密鍵を、時間計算量 $O(p^{2/5+\varepsilon})$、照会計算量 $O(p^{1/5+\varepsilon})$にて回復するアルゴリズムを示し、このアルゴリズムと Pollard の λ 法や ρ 法のような古典的な離散対数アルゴリズムの性能を比較する実装結果を示した。可能な対策として、鍵サイズを大きくする事は署名サイズや効率の点で望ましくなく、上記の攻撃が適用できない曲線を選択できればそれが望ましいが、出来ない場合は q-Strong Diffie-Hellman への帰着はなるべく避けた方が実用上賢明とのこと。

Security of Verifiably Encrypted Signatures and a Construction Without Random Oracles [Pairing 2009]
Markus Ruckert and Dominique Schroder

検証可能暗号化署名 (Verifiably Encrypted Signatures) とは、信頼された第三者(TTP)の公開鍵で暗号化された署名であり、署名者は、署名と暗号化が正しく行なわれた事を検証者に証明できる署名系である。Verifiably Encrypted Signatures の安全性は Boneh ら(Eurocrypt 2003) によって偽造不可能性(unforgeability)と不透明性(opacity)の 2 つの定式化が行われたが、検証可能暗号化署名の Optimistic Fair Contract Exchange への応用を考えると、この定式化では不十分であり、この論文では検証可能暗号化署名の 2 つの新しい基本的要件，即ち抽出可能性(extractability)および悪用不可能性(abuse-freeness) を提案している。抽出可能性とは TTP が正規の検証可能暗号化署名からいつでも正規の署名を抽出可能である事が保証される事であり、悪用不可能性とは TTP と結託した敵性署名者が検証可能暗号化署名を偽造できない事が保証されることである。本論文では、Boneh らのモデルがどちらの性質も捉えていない事を示した。さらに Lu ら(Eurocrypt 2006)の結果より効率的な検証可能暗号化署名を提案し、電子署名における強偽造不可能性の意味で強化した偽造不可能性と不透明性の定義も提案している。

Multisignatures as Secure as the Diffie-Hellman Problem in the Plain Public-Key Model [Pairing 2009]
Duc-Phong Le, Alexis Bonnecaze, and Alban Gabillon

多重署名を使うと、複数の署名者が協力して、共通の文書に対して小さいサイズの署名を生成する事が出来る。多重署名の長さは、署名方式の安全性パラメタのみに依存し、含まれる署名者の数には依存しない。従来の多準署名は、非現実的なセットアップ仮定を使うか、緩い安全性帰着しか持たないか、あるいは非効率的な署名検証しか実現できていなかった。本論文ではランダムオラクルモデルで CDH あるいは DDH に帰着する 2 つの多重署名を提案し、これらの問題をすべて解決したとのこと。本論文の講演は直前にキャンセルされた。

Short Programs for functions on Curves [Pairing 2009 Invited Talk]
Victor Miller

本講演では、最初の多項式時間 Pairing 計算アルゴリズムであり、あらゆる Pairing based cryptography の基礎となっている Miller のアルゴリズムについて Victor Miller 本人による解説が行われた。内容は、1986 年に原稿が完成したにもかかわらず 2004 年 にジャーナル化されるまで unpublished manuscrypt として散々参照された有名な論文“Short Programs for functions on Curves”に概ね従い、楕円曲線、Weil Pairing、Divisor などの数学的な基礎に始まり Addition Chain により Miller Algorithm が構成される事などが示された。その他 Tate Pairing、楕円離散対数問題から乗法群の離散対数問題への帰着、

ランダムな楕円曲線ではペアリングの埋め込み次数が大きくこの帰着が困難なこと、楕円曲線の群構造の決定への応用などの話題が概説された。

On the Security of Pairing-Friendly Abelian Varieties over Non-Prime Fields [Pairing 2009]
Naomi Benger, Manuel Charlemagne, and David Mandell Freeman

A を素数位数 r の部分群に関して埋め込み次数 k を持つ非素体 F_q 上のアーベル多様体とする。本論文では r に関する A の最小埋め込み体が F_{q^k}である q,k および r に関する厳密な条件を与えた。これらの条件が成立する時、埋め込み次数 k は A を用いるペアリングに基づく暗号系の安全性レベルの良い基準となる。本論文の定理を超特異楕円曲線および超特異種数 2 曲線に適用し、各々の場合で最小埋め込み体が F_{q^k} でなくてはならない最大 ρ -値(ペアリングの計算効率を測る一つの指標)を計算した。この結果は、超特異多様体に対する Rubin と Silverberg の結果よりも強く、より多くのアーベル多様体がペアリングに基づく暗号に利用可能である事を保証している。また、この定理は超特異多様体だけでなく一般のアーベル多様体に対しても成立するが、このセッティングでの非超特異曲線の構成に関しては未解決との事。

Generating Pairing-Friendly Curves with the CM Equation of Degree 1 [Pairing 2009]
Hyang-Sook Lee and Cheol-Min Park

非超特異なペアリング適応楕円曲線の族を与える Brezing-Weng 法を基礎とした様々なペアリング適応曲線構成法が提案されている。これらの方法を、基底行列の変更と次数 1 の CM 方程式を持つ円分体の基底の分類を通して再訪する。そして、この分類を用いて、次数 1 の CM 方程式を持つ、新しいペアリング適応曲線生成アルゴリズムを提案する。また、新しいより大きい判別式を持つ曲線の族を示す。

1.5.2. Pairing 2009 の発表(2 日目)

On the Final Exponentiation for Calculating Pairings on Ordinary Elliptic Curves [Pairing 2009]
Michael Scott, Naomi Benger, Manuel Charlemagne, Luis J. Dominguez Perez, and Ezekiel J. Kachisa

ペアリングの計算過程は主に 2 つの段階、即ち Miller ループおよび最終冪から構成される。Miller ループの部分の演算量削減が、R-ate ペアリングのようなループ打ち切りペアリングの発見とともに非常に良く進展した結果として、最終冪が計算全体の中でより重要な部分となって来ている。本研究では、偶数埋め込み次数を前提として、既存の様々なペアリング向け非超特異楕円曲線に対して、最終冪に必要な計算の加算連鎖の効率化を研究し、BN 曲線、Freeman 曲線、KSS 曲線についてそれぞれ結果を示した。

Faster Pairings on Special Weierstrass Curves [Pairing 2009]
Craig Costello, Huseyin Hisil, Colin Boyd, Juan Gonzalez Nieto, and Kenneth Koon-Ho Wong

ペアリングの高速化の技法は、概ね Miller Iteration の内部の高速化、曲線の選択による高速化、Miller Loop の短縮による高速化、の 3 つのカテゴリに分類されるが、各カテゴリに対して様々な技法が提案されている。ペアリングの高速な実装を得るには、これらの技法を様々な組み合わせを実現する必要がある。本論文では、j-不変量が 0 の特殊な楕円曲線 y^2 = c x^3 + 1 を用いて、これらの様々な技法を取り入れた効率的な公式を提案している。さらに、暗号の実装に使用可能な楕円曲線の例を示した。

Fast Hashing to G2 on Pairing Friendly Curves [Pairing 2009]
Michael Scott, Naomi Benger, Manuel Charlemagne, Luis J. Dominguez Perez, and Ezekiel J. Kachisa

非超特異楕円曲線を使用するペアリングに基づく暗号プロトコルを設計する際に、拡大体側(あるいはツイスト側)の巡回群上に値域を持つハッシュ関数が必要となることがある。素朴な方法を用いると拡大体上の点のスカラー倍演算が必要となり演算コストが大きい。本発表ではフロベニウス写像(あるいは類似の写像)を用いてこのスカラー倍の高速化を研究し、MNT 曲線、BN 曲線、Freeman 曲線、KSS 曲線の各々の場合について結果を報告した。

Pairing-Based Techniques for Zero Knowledge [Pairing 2009 Invited Talk]
Amit Sahai

17 年間未解決であった 非対話完全ゼロ知識証明 (non-interactive perfect zero-knowledge proof)を肯定的および構成的に解決した Groth, Ostrovsky, Sahai の“Perfect non-interactive zero knowledge for NP” [GOS06] と、あらゆる NP に対する数論的仮定の下での非対話証拠識別不能 (non-interactive witness indistinguishable) を実現した Groth, Sahai の“Efficient non-interactive proof systems for bilinear groups” [GS08] (通称 GS-proof) の解説講演。これらの結果は既に数多くの論文に参照され、多数のアプリケーションが提案されている。

Compact E-Cash and Simulatable VRFs Revisited [Pairing 2009]
Mira Belenkiy, Melissa Chase, Markulf Kohlweiss, and Anna Lysyanskaya

効率的非対話零知識証明は沢山の暗号学的問題を解決する為の強力なツールである。Groth および Sahai は最近ペアリングの積等式(pairing product equation)に対する Groth-Sahai 証明系 (GS-proof) を提案したが、本論文では次の 2 つの暗号学的問題に対して GS-proof を応用した。

- compact e-cash (Eurocrypt 2005)
- シミュレーション可能検証可能ランダム関数(simulatable verifiable random functions, sVRF) (CRYPTO 2007)

署名の所有、疑似乱数性、範囲証明(range proof)に対する効率的な GS-proof を構成することにより、ランダムオラクルに依存しない効率的な compact e-cash を初めて実現したとのこと。

Proofs on Encrypted Values in Bilinear Groups and an Application to Anonymity of Signatures [Pairing 2009]

Georg Fuchsbauer and David Pointcheval

本論文では、Boneh-Goh-Nissim 暗号系と Groth, Ostrovsky, Sahai らによる一連の非対話零知識証明を使って、双線形群における暗号系を、リンク不能匿名化する汎用的方法論を与える。最近、グループ署名と代理署名の機能と安全性概念を統一する新しい暗号プリミティブ、匿名代理署名が提案されている。本論文では匿名代理署名のはじめての(標準モデルでの)具体例を与える事により、この技法の使い方を例示する。この系を構成する為に、様々な効率的非対話零知識および証拠識別不能証明および条件を緩和したシミュレーション健全性の概念を使用した。

Identity Based Group Signatures from HIBE [Pairing 2009]

Nigel P. Smart and Bogdan Warinschi

本論文では、WIBE (Wildcarded IBE) と Naor の IBE から署名への変換を利用して、ID ベースグループ署名を構成する汎用的な方法論を提案し、Boneh,Boyen,Goh (Eurocrypt 2005)の HIBE/WIBE を使って具体的なプロトコルの構成を示した。この構成はランダムオラクルモデルでしか安全性が証明されていないが、非常に効率的で実用的である。ランダムオラクルを排除する事は CRS モデルの非対話ゼロ知識証明を使用し、標準的な技法で恐らく実現可能であろうとの事。

Forward-Secure Group Signatures from Pairings [Pairing 2009]

Toru Nakanishi, Yuta Hira, and Nobuo Funabiki

Forward-Security を持つグループ署名は従来 RSA に基づく方法が Song によって提案されていたが、この方式は鍵更新可能な最大回数 T に対して署名生成・検証、あるいは鍵更新に O(T)の計算量を必要とするものであった。本研究ではRSAではなくペアリングに基づく新しい Forward-Secureグループ署名系を提案している。この方式では署名生成、検証、鍵更新のいずれもO(log T)の計算量しか必要とせず、効率的である。O(1)署名生成・検証、ランダムオラクルの除去および実装が課題であるとのこと。

Efficient Traceable Signatures in the Standard Model [Pairing 2009]

Benoit Libert and Moti Yung

Traceable 署名とは匿名性(anonymity)の管理と撤回(revocation)の機構を追加した Group 署名の拡張概念で、Kiayias, Tsiounis, Yung (Eurocrypt 2004) により提案された。この機構を用いると、他のユーザーが作った署名の anonymity に深刻な影響を与えずに不正なユーザーの作った全ての署名の追跡が可能となる。標準モデルで安全性が証明されたTraceable署名は存在しなかったが、本論文ではそれを実現したとの事。使用している計算量的仮定は , HSDH (hidden SDH) などの強い仮定に依存している。効率の改善とより古典的な仮定での実現が課題とのこと。

1.5.3. Pairing 2009 の発表（3 日目）

Efficient Implementation of Pairings [Pairing 2009 Invited Talk]
Tanja Lange

本講演では Tate pairing, R-ate pairing 等の基本的な pairing アルゴリズム、円上の加法定理、エドワーズ曲線上の加法定理などの入門的な内容の紹介が行われた後、エドワーズ曲線上でのペアリングアルゴリズムとその幾何学的解釈について、延々と解説が行われた。従来、エドワーズ曲線上でペアリング計算を実現する為には、ワイエルシュトラス曲線上のアルゴリズムを、そのままエドワーズ曲線上に変換する方法などが検討されていたが、この方法は既知のワイエルシュトラス曲線上のアルゴリズムよりも大変非効率であることが分かっていた。幾何学的解釈を再考察する事により、エドワーズ曲線上でもワイエルシュトラス曲線上のアルゴリズムに匹敵するペアリング計算アルゴリズムが得られたとのこと。以下の論文の解説講演。

http://eprint.iacr.org/2009/155

Strongly Secure Certificateless Key Agreement [Pairing 2009]
Georg Lippold, Colin Boyd, and Juan Gonzalez Nieto

本論文では、証明書不要認証鍵交換（certicateless authenticated key exchange, CL-AKE）プロトコルの形式的モデルを提案し、ID ベース AKE プロトコルと公開鍵ベース AKE プロトコルの自然な組み合わせは、この強い安全性を満足しない事を示した。そして、ランダムオラクルモデルで証明付き安全な初めての 1 ラウンド CL-AKE を与えている。提案法は各参加者が最低 1 つの危殆化してない秘密を持つ限り安全で、たとえ鍵生成センターが両参加者の一時的秘密を学習してもこの系は安全である。

Universally Composable Adaptive Priced Oblivious Transfer [Pairing 2009]
Alfredo Rial, Markulf Kohlweiss, and Bart Preneel

電子的な店舗（shop）に対して顧客の個人情報が守られるような匿名購入プロトコル(Anonymous Purchase)を考えると電子マネーのような特別な決済方法が必要となり、制約が非常に大きい。紛失購入(Oblivious Purchase) は、匿名購入よりも制約の緩い電子購入プロトコルで、顧客が購入した商品の品目を秘匿することを目標としている。本研究では紛失購入を実現するための基本部品となる適応的価格つき紛失通信 (addaptive priced oblivious transfer)の設計を行い、ランダムオラクルモデルで汎用結合可能安全な具体的プロトコルを提案している。通信前の事前設定のラウンド計算量はメッセージの数に対して線形、紛失通信自体の計算量は定数ラウンドとのこと。

Conjunctive Broadcast and Attribute-Based Encryption [Pairing 2009]
Nuttapong Attrapadung and Hideki Imai

属性ベース暗号とは ID ベース暗号の拡張で、暗号化あるいは秘密鍵生成を行う際、ID の代わりに属性またはポリシーを指定し、属性とポリシーが一致する受信者だけが復号可能な暗号文を生成可能な暗号系である。本研究では、この属性ベース暗号の拡張である同報(放送用)属性ベース暗号の概念を提案し、具体的構成を示している。従来の鍵更新可能な属性ベース暗号では revocation を行う際に全受信者が鍵更新を行う必要があったが、同報属性ベース暗号ではそうしたステップを経由せずに revocation が可能であるとの事。

1.5.4. Pairing 2009 Hot Topicsの発表

Verifiable Random Functions from Identity-Based Key Encapsulation [Pairing 2009 Hot Topics]
Michel Abdara

本発表では、VRF suitable と呼ばれる性質を持つ ID ベース鍵カプセル化機構(IB-KEM)を検証可能ランダム関数(VRF)に変換する VRF の新しい構成法が紹介された。VRF suitable は、一意復号(unique decryption)および疑似ランダムカプセル化解除(pseudorandom decapsulation)なる 2 つの性質が満たされる事を意味している。一意復号とは、同じ ID に対応する任意の秘密鍵がその ID とは無関係の暗号文に対しても同一の復号結果を持つ事を意味し、疑似ランダムカプセル化解除とは、任意の ID に関し、その ID に関する秘密鍵で、その ID と無関係の暗号文を復号すると結果として出力される値が多項式限界の観測者にとってランダムに見える事を意味する。境-笠原 KEM のような良く知られた IB-KEM は大体これらの性質を持つ。この方法論は理論的にも実用的にも大変興味深く、一見無関係そうに見える IB-KEM と VRF の関係を確立しただけに留まらず、従来法で利用されてきた非効率な Goldreich-Levin 変換を避け、直接的な変換を実現しており効率が良い。新しい VRF suitable な IB-KEM の構成が Open problem とのこと。同じ研究グループから同内容の発表が Eurocrypt 2009 にて行われている。

Functional Encryption [Pairing 2009 Hot Topics]
Amit Sahai

ID ベース暗号の拡張である、属性ベース暗号(Attribute Based Encryption) [Sahai-Waters Eurocrypt 05] あるいは述語暗号 (Predicate Encryption) [Katz-Sahai-Waters Eurocrypt 08] といった概念を統一的に捉える Functional Encryption について解説が行われた。公開鍵暗号の研究は、鍵交換→公開鍵→IBE といった進歩を遂げてきた。しかし、クラウド上で暗号化されたデータが共有される未来を考えると、何らかの属性によりアクセス権限が定義され、暗号化されたままデータの加工を行う、といった自然な要求を、これらの公開鍵暗号の枠組みだけでは十分に満足することが出来ず、複雑なアクセスコントロール基盤が必要となってしまう。こうした視点で暗号化について再考した結果、データへのアクセスポリシーと暗号化メカニズムが統一された Functional Encryption (属性ベース暗号) が生まれた。現在の Functional Encryption を取り巻く状況は、マルチパーティ計算の黎明期の状況と非常に良く似ているとのこと。

Adaptive Oblivious Transfer [Pairing 2009 Hot Topics]
Susan Hohenberger

紛失通信(Oblivious Transfer)とは、送信者が N 個のメッセージを送信し、受信者がその内 k 個を選んで受信できる二者間のプロトコルである。送信者は受信者がどのメッセージを選んだのか知ることが出来ない。また受信者は選択してないメッセージの内容を知ることが出来ない。適応的(adaptive)紛失通信とは受信者がどのメッセージを受信するかを適応的に(選んだメッセージの内容を確認しながら)決定できる紛失通信のことである。本発表では CNS07, GH07, GH08, JL09, RKP09 等の一連の研究の流れ、および話者らの最新の研究成果が紹介された。標準モデルで単純仮定(q-Strong DH のような照会仮定では無こと)の元、効率的で完全シミュレーション可能な紛失通信プロトコルを実現したとのこと。

http://eprint.iacr.org/2010/109/

Sub-linear Size Non-Interactive Zero Knowledge Proof [Pairing 2009 Hot Topics]
Jens Groth

本発表では、CRS model で完全完備性(perfect completeness)、完全零知識、計算量的(補)健全性((co-)soundness)を持つ回路充足性問題および算術回路に対する sub-linear サイズの非対話零知識証明(arguments)を構成したと報告された。双線形群を用い、安全性は一般群モデル(generic group model)で証明しているが、ランダムオラクルには依存していない。ランダムオラクルに依存しない sub-linear サイズの構成は初めてとのこと。この方式では、検証は非常に効率的であるが、証明は super-linear の計算が必要であるとのこと。

Secure ID-based Encryption with Efficient Revocation [Pairing 2009 Hot Topics]

Vipul Goyal

ID ベース暗号(IBE)は公開鍵基盤(PKI)の要らない公開鍵暗号の代替手段として期待されている。しかし PKI にせよ IBE にせよ、いずれのシステムにも利用者アカウントを失効(revocation)させる手段が必要となるであろう。伝統的な PKI の設定では効率的な失効手続きが良く研究されている。しかし IBE の設定では失効を実現する機構の研究はほとんど行われていない。最も現実的な解は、送信者が暗号化の際、鍵として使用する ID に有効期間を含める事である。この方法では、全ての受信者が(鍵が漏洩してるかどうかに拘わらず)信頼機関と通信して秘密鍵を定期的に更新する必要がある。そして、利用者の数が増大すると鍵更新が律速段階となり、規模をあまり大きくすることが出来ない。そこで発表者は利用者の効率を下げずに、信頼機関の鍵更新効率を(利用者数の線形計算量から対数計算量へ)著しく改善する IBE 方式を提案したとのこと。

1.6. SAC 2009 の発表

1.6.1. SAC 2009 の発表(1 日目)

Practical collisions for SHAMATA-256 [SAC 2009]
Tal Moran; Moni Naor; Gil Segev

SHAMATA は SHA-3 の Round 1 候補のハッシュ関数であり、AES の構成要素を使ったストリーム暗号に類似の構造を持ち、処理速度は最も速い部類に属する。著者らの解析の結果、SHAMATA はメッセージ挿入や状態更新に弱点があり、メッセージの延長や非線形部分の状態更新でハッシュ値を普遍に保つメッセージ差分を見つけることが可能である。この方法を適用したところ、ハッシュ長が 256 ビットの SHAMATA-256 では圧縮関数 2^{96} 回分の計算量で、また、ハッシュ長が 512 ビットの SHAMATA-512 では圧縮関数 2^{110} 回分の計算量でこのような差分が求まると評価できた。さらに、効率的な guess-and-determine 法を利用することでさらなる効率化が可能で、SHAMATA-256 の差分経路探索の計算量を 2^{40} まで削減できる。

Improved cryptanalysis of the reduced Grøstl compression function, ECHO permutation and AES block cipher [SAC 2009]
Florian Mendel and Thomas Peyrin and Christian Rechberger and Martin Schla¨ffer

この論文ではハッシュ関数の攻撃法として最近開発されたリバウンド攻撃を改良・拡張したものを SHA-3 候補である Grøstl と ECHO、ブロック暗号 AES に適用した。Grøstl-256 では semi-start-collision が 10 段中 7 段まで探索可能であり、AES に対しては 7 段まで既知鍵に対する識別攻撃が可能であることが分かった。AES は ECHO の内部関数として利用されている。

Cryptanalyses of Narrow-Pipe mode of operation in AURORA-512 hash function [SAC 2009]
Yu Sasaki

SHA-3 候補の AURORA-512 に対する衝突攻撃と第2原像攻撃、HMAC-AURORA-512 に対する攻撃可能性を示す。AURORA-512 の narrow-pipe モードでは Double-Mix Merkle-Damgard(DMMD)構造が利用され、そこでは2組の 256 ビット連鎖変数が並列で更新され、最後に 512 ビットを出力する。DMMD 構造自体に弱点があり、圧縮関数がランダム・オラクルと見なせても、攻撃は可能である。攻撃に必要な計算量は、衝突探索では AURORA-512 計算の 2^{236} 回分で必要メモリは 2^{236}*512 ビット。第2原像計算は与えられるすべてのメッセージに対して有効で、計算量は 2^{290} 回分、必要メモリは 2^{288}*512 ビットである。また、HMAC-AURORA-512 に対する 512 ビット鍵の復元では、2^{257} 回の質問と 2^{259} 回分の off-line 計算が必要で、メモリは無視できる程度しか必要としない。AURORA-384 に対しても同様に、HMAC-AURORA-384 に対する鍵復元攻撃は可能である。

More on Key wrapping [SAC 2009]
Matthias Krause and Dirk Stegemann

共通鍵を別の共通鍵で暗号化する key-wrapping は任意の暗号スキームに対して使えるが、key-wrapping に使えるが、実際の利用を考えるときには様々な制約が課せられる。この方向のアプローチは Eurocrypt 2006 の Rogaway- Shrimpton で発展し、決定論的認証つき暗号(DAE)という概念が定義された。DAE は制約のない AE よりも安全性は弱いが、key wrapping の場合は十分であると考えられる。この論文では、さらに安全性は弱いものの、実用上十分な安全性概念を追求した。具体的には、暗号化されるものが攻撃者が選ぶものではなくランダムであるという以外は通常の共通鍵暗号の要件を満たすだけというものである。

Information-theoretically secure multi party set intersection revisited [SAC 2009]
Arpita Patra and Ashish Choudhary and C. Pandu Rangan

Li,R.-Wu,C.は ACNS 2007 において、情報理論的設定における Multipartyset intersection(MPSI)のプ

ロトコルを提案し、n パーティ中 t(<n/3)パーティが無制限の計算能力を持つ攻撃者によって能動的に破壊されたとしても情報理論的安全性が保たれるというものである。その論文では、プロトコルは 6 ラウンドの通信と O(n^4m^2)個の field 要素との交信を行う。ここで各パーティは各々m 個の field 要素を含むセットを持つとしている。この論文では、実際には ACNS 2007 で書かれたより多くのラウンド数と交信回数が必要になること、プロトコルを改良することで、n>3t が満たされるとき、より少ないラウンド数と交信回数で済むことを示す。

Real traceable signatures [SAC 2009]
Sherman S.M. Chow

追跡可能署名方式は、グループ署名において匿名性管理機能を強化するように拡張する。グループ管理者は追跡用の落とし戸を計算でき、その落とし戸によって誰でも不正者による署名であるか否かを調べることができる。一方、これをグループ署名で同様のことをするには、すべての署名者の署名を明らかにするしかない。しかし、これは厳密な意味での追跡とは言えない。この論文ではより効率の良い追跡法を提案する。そこでは追跡用の落とし戸は不正者の署名を一意的に特定できるタグの再構成を可能する。全部で N'個の署名のうち N(<<N')個の署名を特定するには、N 個の小さなタグを計算し、それを署名の保持者に送るだけで良い。

Cryptanalysis of the LANE hash function [SAC 2009]
Shuang Wu and Dengguo Feng and Wenling Wunp

共通鍵を別の共通鍵で暗号化する key-wrapping は任意の暗号スキームに対して使えるが、実際の利用を考えるときには様々な制約が課せられる。この方向のアプローチは Eurocrypt 2006 の Rogaway-Shrimpton で発展し、決定論的認証つき暗号(DAE)という概念が定義された。DAE は制約のない AE よりも安全性は弱いが、key wrapping の場合は十分であると考えられる。この論文では、さらに安全性は弱いものの、実用上十分な安全性概念を追求した。具体的には、暗号化されるものが攻撃者が選ぶものではなくランダムであるという以外は通常の共通鍵暗号の要件を満たすだけというものである。

Practical pseudo-collisions for hash functions ARIRANG-224/384 [SAC 2009]
Jian Guo and Krystian Matusiewicz and Lars R. Knudsen and San Ling and Huaxiong Wang

ARIRANG は SHA-3 公募の Round 1 候補のハッシュ関数である。設計の特徴は、AES の S-box と MixColumn、及び word 単位の回転を使用している点にある。ARIRANG では、差分ビットが全部 1 となる初期ベクタ(IV)の対によって近衝突が簡単に作れるという性質がある。この性質を利用し、フルスペックの ARIRANG-224 と ARIRANG-384 に対する擬似衝突攻撃が可能で、計算量は圧縮関数計算の 2^{23} 回分になることが分かった。

A more compact AES [SAC 2009]
David Canright and Dag Arne Osvik

AES の実装に必要なビット演算回数を減らす2つの方法について考える。一つは部分体を利用した複合体(composite field)による最適化を全段に及ぼすことであり、もう一つは、Mixcolumn と S-box の線形変換を結合することである。この2つを組み合わせることによって、1 ブロックの平文を暗号化するのに要するビット演算回数を従来より 9.0%減らした。復号も同様の手法によって、従来より 13.5%減らした。

Optimization strategies for hardware-based cofactorization [SAC 2009]
Daniel Loebenberger and Jens Putzka

最近の一般数体篩法(GNFS)の実装において、中間的な篩による結果を楕円曲線を使って分解する ECM が使うことが多く、これを cofactorization step と呼ぶ。本論文では、特定のビット長に特化した ECM モジュールの配分を最適化することによって cofactorization step の効率化を図り、最適化しない場合と比べ、速度は 17%～33%向上した。

More on the security of linear RFID authentication protocols [SAC 2009]

Matthias Krause and Dirk Stegemann

計算リソースが限られるRFID用の認証プロトコルを調べた結果、Juels-Weisが導入したHBファミリーが有望そうに見え、受動攻撃と一部の能動攻撃に対する安全性が証明できる。しかし、通信に要するビット数が多くなることと、実行可能な能動攻撃が存在するという欠点がある。HB ファミリーの代替として、Cicho-Klonowski-Kutylowski が導入したプロトコルがあり、その特殊形が線形(n,k,L)-プロトコルである。(n,k,L)-プロトコルに対する能動／受動攻撃が存在するが、改良した$(n,k,L)^{++}$-プロトコルではある種の能動攻撃に対して安全性が証明できる。(n,k,L)-プロトコルの安全性は、線形部分空間の結合を学習する問題(LUVS)の困難性に帰着する証拠を著者らは掴んだ。

Differential fault analysis of Rabbit [SAC 2009]

Aleksander Kircanski and Amr Youssef

Rabbitは欧州のストリーム暗号研究プロジェクトであるeSTREAMがSW向けの推奨暗号としてPortofolioに掲載した方式であり、ストリーム暗号の国際規格 ISO/IEC 18033-4:2005 にも採用されている。鍵は128 ビット、初期ベクタは 64 ビットである。この論文では、Rabbit に対する故障利用攻撃が示される。攻撃では内部状態のランダムに決まるビットが反転(故障)するが、故障の位置は制御できないことを仮定する。この攻撃によって内部状態を復元するには、128～256回の故障とサイズが$2^{41.6}$バイトの事前計算テーブル、及び、2^{36}回の状態更新が必要である。

An improved recovery algorithm for decayed AES key schedule images [SAC 2009]

Alex Tsow

Haldermanらは、メモリ上に展開されているノイズ入りの鍵を読み取り、鍵を推定するcold-boot攻撃を確立した。本論文では、cold-bootを改良し、AES-128に対してオリジナルの攻撃法の1000万倍の高速化を実現した。この攻撃は鍵スケジュールのビットが 70%崩壊していても成功した。また、AES-256 では鍵スケジュール・ビットの 65%崩壊まで適用できた。

1.6.2. SAC 2009 の発表(2 日目)

Cryptanalysis of the full MMB block cipher [SAC 2009]
Meiqin Wang and Jorge Nakahara Jr and Yue Sun

MMB は 1993 年に Daemen らが IDEA の代替として提案したブロック暗号である。本論文では、MMB の中心的演算である Z_2^32-1 上の剰余乗算における特異な性質に注目し、それを利用した、差分解読(DC)、SQUARE 攻撃、線形解読(LC)を示した。
DC では、フルラウンドの 6 段を破ることができ、 必要な選択平文は 2^{118} 個、計算量は暗号化 $2^{95.91}$ 回分、2^{64} のカウンター。SQUARE 攻撃では、4 段縮小版の 128 ビット鍵が求まり、必要な選択平文 2^{34} 個、暗号化 $2^{126.34}$ 回分、メモリ・ブロック 2^{64} 個。LC では、3 段縮小版が攻撃でき、必要な既知平文 $2^{114.56}$ 個、暗号化 2^{126} 回分。これらの攻撃は、従来と異なり、暗号化鍵が弱鍵であるという条件を必要としない。

Weak Keys of the Block Cipher PRESENT for Linear Cryptanalysis [SAC 2009]
Kenji Ohkuma

PRESENT は実装サイズが極めて小さくなるように設計された 64 ビットブロック暗号である。設計者による自己評価では、線形解読法における特性確率(単経路)評価で 28 段で線形偏差が 2^-43 以下となるので、フルラウンドの 31 段では安全としている。本論文では、4 段以上では同じ線形マスクに対する単経路が複数存在するため、特性確率による評価では不十分てあることに着目し、複数経路効果を解析した。その結果、PRESENT とその縮小版では 32%の弱鍵で複数経路効果が顕著となること、弱鍵の場合、28 段の線形偏差が $2^{-39.3}$ と自己評価の結果を上回ることを示した。また、具体的な鍵回復攻撃を構成し、弱鍵に対して 24 段が攻撃可能で、必要平文数は既知平文 $2^{63.5}$ 個、計算量は暗号化 $2^{63.5}$ 回分と評価した。

Improved integral attacks on MISTY1 [SAC 2009]
Xiaorui Sun and Xuejia Lai

MISTY1 は電子政府推奨暗号とブロック暗号の国際規格 ISO/IEC 18033-3 に採用された 64 ビットブロック暗号である。MISTY1 に対して今までに最も成功した攻撃は、FL 関数付きの MISTY1 に対する積分攻撃で 8 段中 6 段までである。本論文では、鍵スケジュールの弱点を利用した攻撃の改良を行った。その結果、5 段縮小版し対し、2^{34} 個の選択平文を使ったとき、計算量(単位は暗号化 1 回分)を従来の 2^{46} 回から $2^{29.6}$ 回に削減した。また、6 段では、2^{32} 個の.選択暗号文で暗号化 $2^{126.1}$ 回分の計算量で攻撃できることを示した。これらの結果は今まで最も少ない計算量を達成している。

New results on impossible differential cryptanalysis of reduced-round Camellia-128 [SAC 2009]
Hamid Mala and Mohsen Shakiba and Mohammad Dakhil-alian

Camellia は電子政府推奨暗号とブロック暗号の国際規格 ISO/IEC 18033-3 に採用された 128 ビットブロック暗号である。本論文で、Camellia は 128 ビット鍵で FL 関数なしのとき、不能差分攻撃によって 18 段中 12 段まで破れることを初めて示した。Camellia に対する不能差分攻撃ではこの発表と同じ条件で 12 段まで破れるとする CT-RSA 2008 での Lu らの研究があるが、この発表ではその計算量が鍵全数探索より大きいことを示し、12 段の不能差分攻撃に選考したのはこれが初めてであると主張している。

Format-preserving encryption [SAC 2009]
Mihir Bellare and Thomas Ristenpart

Format Preserving Encryption (FPE)は、特定のフォーマットを持った平文を同じフォーマットの暗号文に暗号化する方式で、正当なクレジットカードの番号を正当なクレジットカード番号に暗号化するといった応用がある。しかし、FPE は十分一般的かつ厳密に扱われていなかった。本論文では、FPE を形式的に定義し、安全性のゴールを設定する。それに続け、FPE を複雑なドメインで実現するアプローチと“rank-then-encipher”によるアプローチについて調べ、FPE で何が出来、何が出来ないか追求する。ここでは、非対称の Feistel ネットを使った2種類の FPE 実現法を示す。

BTM: A single-key, inverse-cipher-free mode for deterministic authenticated encryption [SAC 2009]
Tetsu Iwata and Kan Yasuda

ブロック暗号を使った確定論的な認証付き暗号化(DAV)として、Eurocrypt 2006 で Rogaway-Shrimpton が提案した SIV と、FSE 2009 で著者らが発表した HBS がある。本論文では両アルゴリズムの性質を改良した BTM (Bivariate Tag Mixing)が提案された。BTM はブロック暗号鍵の1個だけしか必要とせず、鍵2個が必要な SIV より優れ、また使用するブロッ暗号の復号を必要としないので、HBS より優れている。BTM は認証用のハッシュに 2 変数多項式を利用するので、動的次元を持つベクトル入力を処理できる。

On repeated squarings in binary fields [SAC 2009]
Kimmo U. Ja¨rvine

二乗算の繰り返し問題は、楕円曲線暗号などで重要であり、有限体上の逆元計算や Koblitz 曲線上のスカラー倍算などの効率化に使われる。本論文では、二乗算の繰り返し問題において、参照テーブル(LUT)を使って、FPGA 実装での実装サイズや遅延を減らすことを目標に調べた。その結果、最適な構成は LUT のサイズに依存することが分かった。さらに新規アーキテクチャを提案し、それによって計算速度が大幅に向上し、サイドチャネル攻撃耐性も改善することを示す。

Highly regular m-ary powering ladders [SAC 2009]
Marc Joye

暗号計算向きの新しい冪乗計算法を提案である。提案法はいわゆる Montgomery ladder の m 進展開への一般化と見なせ、right-to-left と left-to-right の両方に対応する。提案法は Montgomery ladder と同様、同じ命令を同じ順序で繰り返し、ダミー処理は入らないので、実装(サイドチャネル)攻撃に対する自然な形の防御になっている。提案法は実装性能を向上し、柔軟性にも優れている。

An efficient residue group multiplication for the eta pairing over F3m [SAC 2009]
Yuta Sasaki and Satsuki Nishina and Masaaki Shirase and Tsuyoshi Takagi

最も高速なペアリングの一つである η_T ペアリングに対する高速実装の提案。SAC 2007 で Gorla らが提案した η_T ペアリングの実装は、$F_{3^{\{2m\}}}$ 上での乗算が 5 回、つまり、F_{3^m} 上の乗算が 15 回で済み、これは乗算回数の理論下限に達した。今回、剰余類群で計算することにより、この理論限界を超える方法を提案した。F_{3^m} 上での乗算回数は、m→∞の極限で 12 回となる。

Compact McEliece keys from Goppa codes [SAC 2009]
Rafael Misoczki and Paulo S. L. M. Barreto

Goppa 符号を使った McEliece 暗号の鍵サイズを縮小する提案。元々の McEliece 暗号は Goppa 符号上に構成され、未だに破られていないが、公開鍵サイズが非常に大きくなるという欠点がある。McEliece 暗号の鍵サイズを小さくする研究の多くは、別の符号クラスを使うことに集中しているが、それらのほとんどは安全性に欠陥があり、誤り訂正能力も半減するといった欠点を伴なう。本論文の提案法では、Goppa 符号のサブクラスを使うことにより、鍵サイズを大幅に下げるとともに実装効率を上げながら、誤り訂正能力を維持することに成功した。

Herding, second preimage and trojan message attacks beyond Merkle-Damgaard [SAC 2009]
Elena Andreeva and Charles Bouillaguet and Orr Dunkelman and John Kelsey

ハッシュ値とメッセージの接頭辞(prefix)を固定した原像攻撃の一種である herding 攻撃を Merkle-Damgard 構造以外の連接型(concatenated)ハッシュ関数や同じメッセージを複数回処理するハッシュ関数に拡張する内容。この手法を用いた、同じメッセージを2回繰り返した入力や特定の接尾辞(suffix)を持つメッセージ入力に対する第2原象を示す。

Cryptanalysis of Dynamic SHA(2) [SAC 2009]
Jean-Philippe Aumasson and Orr Dunkelman and Sebastiaan Indesteege and Bart Preneel

Dynamic-SHA と Dynamic-SHA2 は SHA-3 公募の Round 1 で評価されたハッシュ関数であり、ブロック暗号の RC5 などと同様データ依存ビット回転が主要な設計要素となっている。本論文では回転に着目した攻撃により、Dynamic-SHA に対する衝突攻撃、原像攻撃、第２原象攻撃が可能であり、Dynamic-SHA2 に対しては衝突攻撃が可能であることを示した。
・Dynamic-SHA-256 の3種類の攻撃に必要な計算量は各々、2^21、2^216、2^225
・Dynamic-SHA-512 の3種類の攻撃に必要な計算量は各々、2^22、2^256、2^262
・Dynamic-SHA2-256 の衝突攻撃に必要な計算量は 2^52
・Dynamic-SHA2-512 の衝突攻撃に必要な計算量は 2^85

A new approach for FCSRs [SAC 2009]
Franc,ois Arnault and Thierry Berger and Ce'dric Lauradoux and Marine Minier and Benjamin Pousse

Feedback with Carry Shift Register (FCSR)は LFSR を変形したものであり、非線形性と良い統計的性質を兼ね備えている。しかし、FCSR に対する最近提案された表現法を利用することで、暗号で利用される FCSR に弱点があることが分かった。本論文はこの弱点を解消するため、FCSR における新規の"リング"表現を提案する。リング表現はガロア表現とフィボナッチ表現を拡張した行列で定義され、両表現の統計的性質を保ちつつ、弱点を回避する。さらに、リング表現は、より速い拡散性とより良い実装性能を実現している。具体的応用例とし、ストリーム暗号 F-FCSR に新バージョンを示す。

New cryptanalysis of irregularly decimated stream ciphers [SAC 2009]
Bin Zhang

不規則に生成ビットを破棄する機構を用いたストリーム暗号に適用可能な、新規の相関攻撃を提案。従来より高い相関確率を得ることに成功している。この相関攻撃を、4種類のストリーム暗号、Krawczyk のパラメータによる収縮生成器(shrinking generator)、LILI-II、DECIM^{v2}、DECIM-128。
上記の収縮生成器に対する攻撃は実際に実行可能であり、攻撃アルゴリズムを C 言語で書いて通常の PC に実装したところ、平均 10 分で初期状態が復元できた。LILI-II に対しては、$2^{24.1}$ビットの鍵ストリーム、$2^{74.1}$ビットのメモリ、$2^{72.5}$回分の計算量で攻撃可能。
DECIM ではフィルタと出力の廃棄に独自のアルゴリズム ABSG が使われるが、今回 ABSG の相関を示した。この相関を利用した攻撃アルゴリズムを組み立てたところ、次の縮小版に対する攻撃が可能だった。
・DECIM^{v2}: フルスペックの 160 ビットを 192 ビットにした縮小版
・DECIM-128: フルスペックの 288 ビットを 256 ビットにした縮小した縮小版
興味深いことに、DECIM の安全性は ABSG よりも使用している LFSR を長さにより強く依存していることが分かった。なお、DECIM^{v2}はストリーム暗号の国際規格、ISO/IEC 18033-4:2005 に採用されている。

1.7. Crypto 2009 の発表

1.7.1. Crypto 2009 の発表(1 日目)

Reconstructing RSA Private Keys from Random Key Bits [Crypto 2009]
Nadia Heninger, Hovav Shacham

DES や AES の拡大鍵や RSA の秘密鍵には冗長性があるので、その一部の鍵ビットが分かると鍵全体を再現できることを Halderman らが USENIX Security 2008 で示し、その具体的な適用例である cold boot 攻撃によってその有効性を示している。この論文では、Halderman らの RSA 暗号に対する攻撃を改良し、より少ない鍵ビットでより短時間で鍵復原が可能であることを理論及び計算機実験で示した。鍵復原能力が向上した理由は、復元のアルゴリズムを改良したことであり、さらに利用できる秘密鍵情報の種類を増やすことで解読効率は高まる。高い確率で効率的に鍵復原が実行できるために必要な鍵ビットの割合は次の通りである。

(1) 27% (秘密鍵: p,q,d,dp,dq)
(2) 42% (秘密鍵: p,q,d)
(3) 57% (秘密鍵: p,q)

ここで、dp,dq は CRT を用いた高速演算用の秘密べき指数である。
これらの結果は、ある Conjecture の下で理論的に示され、計算機実験で確からしさが検証されている。

Public-Key Cryptosystems Resilient to Key Leakage [Crypto 2009]
Moni Naor, Gil Segev

サイドチャネル攻撃や cold boot 攻撃のように、暗号化／復号中の内部データの漏えいが現実的な問題となっている。TCC 2009 において、Akavia らは秘密情報の一部が漏れたときの安全性を評価する枠組みを提案した。この論文では、秘密鍵をLビットとしたとき、決定 Diffie-Hellman 仮定(及び、d-線形変数)に基づく新しいハッシュ証明システムを開発し、L(1-o(1))ビットの漏洩に対して安全であることを示した。また、Crypto 2008 で Boneh らが提案した“circular-secure”な新しいスキームが L(1-o(1))ビットの漏洩に対して安全であることを証明した。さらに、この枠組みを選択暗号文攻撃における鍵漏洩にも拡張したとき、Naor-Yung paradigm にこの設定が適用できることを示し、付随する暗号スキームで、L(1-o(1))ビットの鍵漏洩に対して CCA2-安全であることを理論的に示した。また実用的には、本来の構成における Cramer-Shoup 暗号が、L/4 ビットの鍵漏洩に対し CCA1-安全であり、L/6 ビットの鍵漏洩に対し CCA2-安全であることを示した。

Leakage-Resilient Public-Key Cryptography in the Bounded-Retrieval Model [Crypto 2009]
Joel Alwen, Yevgeniy Dodis, Daniel Wichs

鍵漏洩に対して安全な公開鍵系の3つのプロトコルを開発した。ここでは、攻撃者が適応的な秘密鍵情報取得を何度でも繰り返せるが、取得できる情報の上限を l ビットに制限している。3つのプロトコルは具体的には次の通りである。

(1)最初の同定スキーム(ID)
(2)署名スキーム、
(3)認証付き鍵共有スキーム(AKA)

メインの結果は、提案する AKA が対話型の暗号スキームに利用でき、暗号文を見た攻撃者に対して安全ではない非対話型の暗号スキームより定性的に高いプライバシーを保証できることを示したことである。

さらに、これらのスキームは、制限想起モデル(Bounded-Retrieval Model)に拡張でき、任意の安全パラメータ λ、漏洩パラメータ l、相対漏洩パラメータ δ (1- δ が漏洩割合)に対し、鍵サイズを次のように設定することことで他の通信コストを掛けずに対応できる。

・秘密鍵サイズ　l(1+ δ)+O(λ)
・公開鍵サイズ　O(λ) … l には非依存
・通信複雑度　O(λ / δ) … l には非依存

・計算複雑度　O(λ / δ 2) … 秘密鍵の読み出し回数、l には非依存
最後に、これらのスキームは、固定の(秘密)マスター鍵に対し、(秘密)セッション鍵の見えない更新“invisible updates”に対し、l ビットの情報漏洩に対して安全性を保つことが可能である。

Short Chosen-Prefix Collisions for MD5, the Creation of a Rogue CA Certificate [Crypto 2009]
Marc Stevens, Alexander Sotirov, Jacob Appelbaum, Arjen Lenstra, David Molnar, Dag Arne Osvik, Benne de Weger

MD5 に対し、冒頭のビットを特定の値に固定した(chosen-prefix)ときの衝突の探索法を提案するとともに、この衝突探索法を利用して、偽造した証明書を作ることに成功した。正当なシリアル番号や有効期限を要求したとき、偽造証明書用の衝突を作るのに要する計算量は MD5 圧縮関数実行 2^{49} 回分だった。さらに実用的な単一ブロック衝突探索を MD5 圧縮関数実行 2^{16} 回分まで削減した。

Meet-in-the-Middle Preimage Attacks Against Reduced SHA-0, SHA-1 [Crypto 2009]
Kazumaro Aoki, Yu Sasaki

これまで、中間一致攻撃をハッシュ関数の原像攻撃に利用する方法は、メッセージ・スケジュールがビット置換であるハッシュ関数にしか適用されていなかったが、この論分ではメッセージ・スケジュールが線形変換の場合にも使えるように拡張し、SHA-0 と SHA-1 に適用した。その結果、SHA-0 では圧縮関数計算 $2^{156.6}$ 回で 52 ステップまで、SHA-1 では圧縮関数計算 $2^{159.3}$ 回で 48 ステップまで、原像攻撃可能であると評価した。これまでの最良の結果は、Crypto 2008 で De Canniere らが示した、SHA-0 が 49 ステップ、SHA-1 が 44 ステップであった。この論文では最近開発された補助的な手法である、slice-and-cut、partial-fixing、initial structure が利用されている。

Private Mutual Authentication and Conditional Oblivious Transfer [Crypto 2009]
Stanislaw Jarecki and Xiaomin Liu

この論文では、最初の実用的な Unlinkable Secret Handhake (SH)と最初の実用的な Ananymous Credential scheme (AC)を提案した。SH は、プライバシーが保護される双方向の認証とも言え、相手が認証ポリシーに合致しない場合にはパーティの情報が漏えいせず、双方が同じグループに属する場合は unlinkable となる相互認証方式である。また AC は、送受信者の認証ポリシーが一致することが、受信者が暗号化されたメッセージを復号できるための必要十分条件であるような封入(暗号化)方式である。提案されたこの2つのプロトコルは、Conditional Oblivious Transfer(COT)プロトコルの族という、新しい技術的なツールに依存している。COT とは、ある群要素の離散対数表現の上で、剰余演算による制約によって定義された言語に対し、決定 DH 仮定の下で安全かつ効率的な OT プロトコルを意味する。Strong DH 仮定と Decision Linear 仮定の下で安全な、2つの提案方式は、O(1)回の指数計算と双線形写像を用いて構成されている。

Randomizable Proofs and Delegatable Anonymous Credentials [Crypto 2009]
Mira Belenkiy and Jan Camenisch and Melissa Chase and Markulf Kohlweiss and Anna Lysyanskaya and Hovav Shacham

この論文では、効率的で委任可能な匿名信任状システム(delegatable anonymous credentials system)の構成を示した。委任可能な匿名信任状システムとは、ユーザが、元の authority から L レベル離れた(間に(L-1)人を介した)信任状を持っていることを証明でき、かつ、途中の(L-1)人の匿名性を保証する。提案方式では、セキュリティパラメータを k とすると、証明のサイズ(証明のための計算時間)は O(Lk)である。先行する唯一の構成は、Chase-Lysyanskaya が Crypto 2006 で示した NP 完全な言語に対する一般的な非対話証明に依存した方法であるが、匿名 credentials を構成するアプローチ全体を改良し、ランダム化可能な知識系のゼロ知識証明を中核の構成要素として設計した。ランダム化可能な非対話ゼロ知識証明の概念は、この論文でフォーマルに定義され、第3者による非対話ゼロ知識証明の制御された再ランダム化の最初の例として実現された。

Computational Differential Privacy [Crypto 2009]

Ilya Mironov and Omkant Pandey and Omer Reingold and Salil Vadhan

ICALP 2006 において Dwork は、差分プライバシー(differential privacy)の概念を提案した。この概念を直感的に言うと、攻撃者が一つの記録が存在するか否かを予想するときの成功確率がリスクの指標となる。ここで攻撃者が利用できるのは、予想対象の記録を除く、データベースの全記録である。Dwork のオリジナルの概念では、攻撃者の計算能力を無制限としていたが、そうすると対策のコストは非常に高くなる。この論文では、情報理論的安全性を計算量理論的な安全性へと条件を緩和し、攻撃者が効率的である(計算量に上限がある)とすることで、実用的な計算量で安全性を確保できる概念を提案した。そして、2つの概念が Reingold の pseudodense sets 理論との関連で関係づけられることを見出した。さらに、Reingold らによる dense model 理論を拡張して、計算量的 differential privacy の 2 つの定義、indistinguishability-based と simulatability-based の等価性を証明した。

Probabilistically Checkable Arguments [Crypto 2009]

Yael Tauman Kalai (Microsoft) and Ran Raz

この論文では、確率的にチェック可能な証明(PCP = probabilistically checkable proof)における健全性の情報理論的保証を計算量保証に緩和した概念である確率的にチェック可能な論証(PCA = probabilistically checkable argument)を定義し、多くの NP 言語において、witness のサイズに対して多項式サイズとなる PCA が存在することを示した。PCP の最小サイズでも instance のサイズに対する多項式サイズとなることから、PCA のサイズが小さいことが分かる。また、PCA の質問(queries)の数は、poly-logarithmic になる。これらの全結果における健全性は、PIR(Private-Information-Retrieval)スキームにおける指数時間困難性の仮定を根拠にしている。

On the Composition of Public-Coin Zero Knowledge Protocols [Crypto 2009]

Rafael Pass and Wei-Lung Dustin Tseng and Douglas Wikstrom

この論文では、並列の多項式回の繰り返しに対して安全な、public-coin かつ black-box のゼロ知識証明が可能なのは、BPP を満たす言語に限られることを示した。この結果は、plain model(set-up なし)と bare public-key model(証明者と検証者がともに登録された公開鍵を持つ)の両方に対して成立する。この結果を補強するものとして、a-priori に同時実行回数の上限か設定されているときに、public-coin かつ black-box のゼロ知識証明が存在することを示す。

On the Amortized Complexity of Zero-knowledge Protocols [Crypto 2009]

Ronald Cramer (CWI Amsterdam & Leiden University) and Ivan Damgaard

この論文では、単純な cut-and-choose 型のプロトコルが最も効率の良いような広いクラスの問題を根拠にするゼロ知識プロトコルに対し、複雑度を改良する一般的な手法を提案する。問題 instance を x、誤り確率を 2-n としたとき、cut-and-choose 型では O(|x|n)ビットであるのに対し、提案手法では O(|x|+n)ビットに削減できる。提案手法では、n 個の instance を同時に証明しており、いかなる計算量的仮定も利用していない。提案手法の適用例には、平方剰余に対する証明、部分群 membership や未知位数の群における離散対数の知識の証明、さまざまなタイプの準同型暗号スキームに対する平文の知識の証明、などがある。提案手法の一般性は、black-box 秘密分散スキームの意外な適用から生じている。

Linear Algebra with Sub-linear Zero-Knowledge Arguments [Crypto 2009]

Jens Groth

線形代数に関する statement に対する現実的な準線形サイズのゼロ知識の論証(argument)を提案する。有限体上の行列に対するコミットメントが与えられると、あるコミットされた行列が他の 2 つのコミットされた行列の積である、準線形サイズのゼロ知識論証を与えることができる。さらに、コミットされた行列が他の 2 つのコミットされた行列の Hadamard 積となるような準線形サイズのゼロ知識論証を与えることができる。これらのツールを使い、多くの新たな準線形サイズのゼロ知識論証を作ることができる。例えば、コミットされた行列が、上三角または下三角などといったものである。

1.7.2. Crypto 2009 の発表（2 日目）

New Birthday Attacks on Some MACs Based on Block Ciphers [Crypto 2009]
Zheng Yuan, Wei Wang, Keting Jia, Guangwu Xu, Xiaoyun Wang

ブロック暗号に基づく MACs の解読の新手法を提案する。MAC の構成法 ALRED の識別器と、AES に基づく実現 ALPHA-MAC を与える。ALRED 構成法については、一般的な識別攻撃を示す。これは、誕生日攻撃の計算量で直接偽造攻撃を行う。ALPHA-MAC の 2 ラウンド衝突差分パスが、約 $2^{65.5}$ 乗個の選択メッセージと $2^{65.5}$ 回のクエリの新しい識別器を構成するために用いられる。最も重要な結果は、この新しい識別器を用いて内部状態（ALPHA-MAC のサブ鍵と等価）の復元をことである。さらに、ALRED 構成法の識別器は、CBC や CFB 暗号モードに基づく MACs に適用できることである。
次に、MACs-PELICAN、MT-MAC-AES、PC-MAC-AES への不可能差分攻撃を初めて示す。誕生日攻撃を使って、ある特定の差分を持つ内部の近衝突を生み出すのに十分な数のメッセージ対が検出される。上に述べた MACs に対して 4 ラウンド AES への不可能差分攻撃が実行される。PELICAN については、提案する攻撃が、サブ鍵に等価な内部状態を復元する。MT-MAC-AES については、攻撃は直接にサブ鍵復元攻撃となることが分かる。これら 2 つの攻撃の計算量は、$2^{85.5}$ 乗個のメッセージと $2^{85.5}$ 乗回のクエリである。PC-MAC-AES については、その 256 ビット鍵を $2^{85.5}$ 個の選択メッセージと 2^{128} 回のクエリで復元する。

Distinguisher, Related-Key Attack on the Full AES-256 [Crypto 2009]
Alex Biryukov, Dmitry Khovratovich, Ivica Nikolic

Crypto 2009 において、ルクセンブルグ大の Dmitry Khovratovich らが、“Distinguisher and Related-Key Attack on the Full AES-256” のタイトルでフルラウンドの AES-256 に対する関連鍵攻撃の発表を行い、データおよび時間の複雑度 2^{131}、メモリ量 2^{65} で 2^{35} 個の関連鍵のうちの 1 つを鍵回復できるとの見積もりを示した。この結果は Eurocrypt 2009 のランプセッションで紹介されたものと同じである。
また、同研究グループはCrypto 2009 のランプセッションで、選択鍵のシナリオではなく全ての鍵に適用できる、4 個の関連鍵に対するブーメラン攻撃を使った関連鍵攻撃を発表し、フルラウンドのAES-256 に対してデータおよび時間複雑度 $2^{99.5}$、メモリ量 2^{77} で攻撃可能、フルラウンドのAES-192 に対してデータ複雑度 2^{123}、時間複雑度 2^{176}、メモリ量 2^{152} で攻撃可能と見積もった。この攻撃に関する成果はIACRの ePrint（http://eprint.iacr.org/2009/317）で公開されており、2009/07/01 に初稿が公開されて以降改訂が行われているが、AES-256 についてはデータおよび時間複雑度が改善している一方、AES-192 についての結果は変わっていない。
これらの結果が AES を直接使う現実的なアプリケーションに対して今すぐ脅威となることは無いが、AES を使用したハッシュ関数の理論的安全性に関しては何らかの影響を与える可能性はある。また、今回の結果は、関連鍵攻撃に関する AES-256 の理論的安全性が AES-128 より低いという逆転現象が起こっていることを意味し、長期的な安全性を目標とした暗号システムの要素としてブロック暗号を使用する場合、関連鍵攻撃のシナリオが有効であるなら、AES 以外の暗号を使う必要が生じる可能性も考えられる（使用方法により安全性レベルが逆転する事は、使用者の立場からは好ましい状況ではない）。今後も攻撃技術の進展を継続的に監視し続ける必要がある。

Cryptanalysis of C2 [Crypto 2009]
Julia Borghoff, Lars Knudsen, Gregor Leander, Krystian Matusiewicz

ブロック暗号 C2（DVDAudio ディスクや Secure Digital カードの暗号化に用いられる）に対するいくつかの攻撃を提案する。C2 は 56 ビット鍵と秘密の 8 ビット入力 8 ビット出力の S-box を持つ。攻撃者が鍵を選択することができるならば、S-box は 2^{24} 乗回の C2 暗号化によって復元できる。既知の S-box に対して 56 ビット鍵を攻撃することは、2^{48} 乗の計算量で行える。結局、8 入力 8 出力の秘密の S-box と 56 ビットの秘密鍵を持つ C2 の実装は、平均、$2^{53.5}$ 回の C2 暗号化により攻撃できる。

Message Authentication Codes from Unpredictable Block Ciphers [Crypto 2009]
Yevgeniy Dodis (NYU) and John Steinberger (Univ. of British Columbia)

ブロック暗号上の効率的な操作モード SS-NMAC を設計した。我々のモードは、以下の性質を持ち、ブロック暗号 f に適用された場合、可変長の鍵つきハッシュ関数 H となる。(1)MAC 保存:f が予測不可能ならば H はバースデイ安全なメッセージ認証子となる。(2)PRF 保存:f が擬似乱数ならば、H はバースデイ安全な擬似乱数関数となる。(3)サイドチャネル攻撃に対する安全性:ブロック暗号 f がその内部に関するサイドチャネル情報を攻撃者に漏らさないならば、H の残りの実装が情報を漏らしたとしても性質(1)(2)は成り立つ。

How to Encipher Messages on a Small Domain: Deterministic Encryption and the Thorp Shuffle [Crypto 2009]
Ben Morris and Phillip Rogaway and Till Stegers (UC Davis)

Thorp シャッフルもしくは最もアンバランスな Feistel ネットワーク(Maximally Unbalanced Feistel Network)の安全性を解析する。大雑把に言うと、Thorp シャッフルは N 枚のカードのうち任意の N^{1-1/r}枚を O(r lg N)ステップで混ぜる。対応して、n ビット列上の最もアンバランスな Feistel ネットワークに O(r)のパス(n ラウンド)を作ることにより 2^{n(1-1/r)}クエリに対する CCA 安全性を保証する。Markov 鎖のテクニックを使った我々の結果により、クレジットカード番号のような小さなスペースの暗号化のための実用的かつ証明可能安全なブロック暗号ベースのスキームを構成することができる。

How to Hash onto Elliptic Curves [Crypto 2009]
Thomas Icart (Sagem Securité, Univ. of Luxembourg)

有限体 GF(p^n)上定義された楕円曲線 E が与えられたとき、GF(p^n)の元を決定多項式時間 O(log^3{q})内に一定数の GF(p^n)演算で E に写像する新しい関数を明に与える。ただし p>3、p^n=2 mod 3 とする。関数は 3 乗根を計算する必要があり、応用として、楕円曲線への決定的かつ効率的なハッシュ関数の構成を 2 通り示す。はじめの構成は、ベースとなるハッシュ関数が一方向性であれば一方向となり、2 つ目の構成は、更にベースとなるハッシュ関数が衝突困難であれば衝突困難となる。

Batch Binary Edwards [Crypto 2009]
Daniel J. Bernstein (Univ. of Illinois at Chicago)

高い安全性を持つ Diffie-Hellman の計算、特に 251 ビット楕円曲線の変化するベースポイントのスカラー倍算に関して、ソフトウェアによるスピード新記録を達成した。200 ドルの Core 2 Quad Q6600 CPU 上の 1 秒の計算で、ソフトウェア BBE251 は、有限体 GF(2)[t]/(t^251+t^7+t^4+t^2+1)上定義された Edwards 曲線 d(x+x^2+y+y^2)=(x+x^2)(y+y^2)、d=t^57+t^54+t^44+1 上で、30000 回の 251 ビットスカラー倍算を実行する。本論文の体演算テクニックは、より一般の場合にも適用可能であるが、バイナリ Edwards 曲線の加算公式の完全性と特に効率的に作用する。

Solving Hidden Number Problem with One Bit Oracle and Advice [Crypto 2009]
Adi Akavia (IAS and DIMACS)

HNP(Hidden Number Problem)の目的は、p、g が与えられ、a の問合せに対して sg^a mod p の最上位 k ビットを返すオラクルへのアクセスができるときに、隠された数 s を見つけることである。p と g のみに依存するアドバイスが与えられたときに、HNP を解くアルゴリズムを示す。ただし、アドバイスの長さと実行時間は log p に関して多項式である。既存の HNP アルゴリズムに対して以下の点で優れている。(1)k>=1 は最適である。(2)ランダムな雑音に対して強い。(3)最上位 k ビットだけではなく、広い範囲の述語の族に対して成立する。新しいツールとして、Z/pZ 上定義された複素数値関数 f へのオラクルアクセスが与えられたときに、f の significant なフーリエ係数を出力するアルゴリズムを示す。

Computational Indistinguishability Amplification: Tight Product Theorems for System Composition [Crypto 2009]

Ueli Maurer and Stefano Tessaro (ETH Zurich)

計算量的識別不可性増幅(Computational indistinguishability amplification)は、効率的な区別者(distinguisher)のアドバンテージを押さえることにより安全性が定義される暗号プリミティブをより強くする問題である。例えば、擬似乱数生成器(PRG)、擬似ランダム関数(PRF)、擬似ランダム置換(PRP)などである。既存の文献は少なく、Yao の XOR 補題は、PRG の n ビット出力 S_i を n ビット列乱数とアドバンテージ δ 以上で識別する効率的な識別者がいないならば、m 個の独立な PRG の出力 S_1,…,S_m の XOR を n2^{m−1}δ^m 以上のアドバンテージで乱数と効率的に識別する識別者は存在しないことを意味する。我々は、この結果を 5 つの軸に沿って一般化し改良した。1 つ目はタイトな情報理論的なバウンド 2^{m−1}δ^m を与えた。2 つ目は対話型システム(PRF や PRP など)に関する結果を証明した。3 つ目は XOR だけでなく、中和的組合せ構成(neutralizing combination construction)のより一般的なクラスを考えた。4 つ目は、Myers の構成を特別な場合として含む、中和的組合せの部分クラスに対して強い安全性増幅を達成した。5 つ目は、より弱い仮定の下での強い安全性増幅を示した。

1.7.3. Crypto 2009 の発表(3 日目)

Merkle Puzzles are Optimal – an $O(n^2)$-Query Attack on Key-Exchange from a Random Oracle [Crypto 2009]
Boaz Barak and Mohammad Mahmoody-Ghidary (Princeton)

本論文では、オラクルに対し正直利用者が最大 n 照会の問い合わせを行うランダムオラクルモデルのあらゆる鍵交換プロトコルが、オラクルに対し O(n^2)照会の問い合わせを行う攻撃者によって破られる事を証明した。この結果は Impagliazzo と Rudich(STOC'89)が与えた $\Omega\tilde{}(n^6)$ 照会の攻撃を改善しており、彼らによって提案された未解決問題を解決している。Merkle (CACM'78) が $o(n^2)$ 照会攻撃者では解読不能の n 照会鍵交換プロトコルをこのモデルで与えているので、この限界は定数因子を除いて最適である。

Position Based Cryptography [Crypto 2009]
Nishanth Chandran and Vipul Goyal and Ryan Moriarty and Rafail Ostrovsky (UCLA)

いろいろな状況で、その人の居る場所がその人の ID を定義していることがある。たとえば、銀行の(防弾)窓口に居る金銭出納の担当行員は信用証明書を示さなくとも、単にその人の居る場所によって、その人の役割が認知されている。本論文では、参加者の ID がその地理上の位置から導かれる暗号プロトコルの研究を提案している。まず、このセッティングにおける中心的課題、即ちデバイスの位置の安全な検証について考察している。従来それを実現しようと試みる様々な研究が行われて来たが、本論文ではバニラモデル(あるいは標準モデル)でこの課題を実現する事は不可能であるとの結果を得た。この結果を受けて、研究方針を照会制限モデル(Bounded Retrieval Model, Bounded Storage Model の亜種) での実現に切り替え、以下の 2 つの基本課題(fundamental tasks)に対する情報理論的安全なプロトコルを定式化し構成した。

- 安全な位置決定
- 位置に基づく鍵交換

さらに、これらの処理(task)が実際この設定のもと汎用(universal)であること、即ち、安全な多者計算を実現するために、これらのツールをどう使うかを示す。この論文における主な寄与は次の 3 つである。

- 安全な位置決定の問題を健全な理論的土台の上に乗せた。
- この問題に対する従来の試みの危険性を示し、強い不可能性を証明した。
- 照会制限(bounded-retrieval)フレームワークが 位置に基づく暗号の基礎研究に対する"正しい"フレームワークの一つである事を示し、肯定的な結果を導いた。

Improving the Security of Quantum Protocols [Crypto 2009]
Ivan Damgard (Univ. of Aarhus) and Serge Fehr (CWI Amsterdam) and Carolin Lunemann and Louis Salvail (Univ. of Aarhus) and Christian Schaffner (Montreal University)

本論文では古典的なメッセージに続くランダムな BB84 量子ビットの送信で始まる 2 者量子プロトコルを考察している.そして、そうしたプロトコルの安全性を改善する汎用の"翻訳系"を示す。もしも元のプロトコルが"概正直(almost honest) "攻撃者に対して安全なら、翻訳されたプロトコルは任意の計算量的に制限された(量子)攻撃者に対して安全である。翻訳は定数因子を除き、送信された量子ビット数とラウンド数を保存する。また、翻訳系は量子格納制限モデル(bounded quantum strage model, BQSM)での安全性を保存する。即ち元のプロトコルが BQSM 安全であるなら、大きな量子記憶と大きな計算能力の両方を持つ攻撃者でなければ、翻訳されたプロトコルを破ることはできない。この事は攻撃者が期待以上の量子記憶を持つとき安全性が完全に毀損する既知の BQSM 安全なプロトコルとは対照的である。それから、この技法の量子本人認証(quantum identification)と紛失通信プロトコルへの適用方法を示す。

Practical Cryptanalysis of ISO 9796-2 and Europay-Mastercard-Visa Signatures [Crypto 2009]

Jean-Sebastien Coron (Univ. of Luxembourg) and David Naccache (ENS) and Mehdi Tibouchi (ENS) and Ralf-Philipp Weinmann (Univ. of Luxembourg)

1999 年 Coron, Naccache, Stern は RSA ベースのメッセージ回復型署名 ISO/IEC 9796-1 および 2 に対し存在的署名偽造を発見した。この攻撃を受けて、ISO/IEC 9796-1 は撤回され、ISO/IEC 9796-2 はメッセージダイジェストが最低 160 ビットとなるよう修正された。この修正版に対する上記の攻撃には 2^{61} 回の演算が必要である。本論文では、(現在有効な)修正版 ISO/IEC 9796-2 のどの法サイズに対しても攻撃可能な上記攻撃の改良アルゴリズムを提案している。RSA-2048 challenge modulus を使用して e = 2 の場合の現実的な偽造が Amazon EC2 グリッド上の 19 台のサーバーを用いて、たった 2 日で計算でき、偽造作成に費やした総費用は約 800 米ドルであったと報告された。一般には使用されない e = 2 を用いたのは、利用したソフトウェアの都合によるもので、奇指数の場合も原理的にはそんなに多くの時間がかかる訳ではないとのこと。新しい攻撃は Coron らの攻撃の漸近計算量を改善した訳ではないが、素因数分解で良く利用される様々なテクニックを使用し、従来手が届かないと思われていたパラメタ範囲での絶対計算量を大きく改善している。さらに、本論文では EMV 署名に対するこの攻撃の適用を検討している。EMV は ISO/IEC 9796-2 にいくらか冗長性を追加した形式であり、7 億 3 千万枚の EMV 決済カードが流通している。EMV の場合、運用方法の違いにより、この攻撃は現実的脅威では無いとのこと。

How Risky is the Random-Oracle Model [Crypto 2009]
Gaetan Leurent (DGA/ENS) and Phong Q. Nguyen (INRIA/ENS)

RSA-FDH およびランダムオラクルモデルで安全な多くの暗号系、署名系が標準的なサイズより大きい出力サイズのハッシュ関数を必要としている。本論文では、Bellare-Rogaway の 1993 年と 1996 年の提案、IEEE P1363 および PKCS に含まれるものなど、そういう場合に従来使用されてきたハッシュ関数の特殊なモード(ランダムオラクルの具体化)がランダムオラクルより弱いことを示す。例えば、1024-ビット要約に対する BR93 に関する 2^67 の原像攻撃を得た。次に、ROM 署名に対するハッシュ関数の欠陥による安全性へのインパクトを研究した。例えば、極端な例として Boneh らの ID ベース暗号(FOCS'07)の場合は、任意のハッシュの衝突により支配鍵(master key)が導出できる。tight security が証明されている Rabin-Williams 署名(EUROCRYPT 2008, Bernstein)の場合は、任意のハッシュの衝突により秘密鍵が暴露される。興味深いことに、どちらの系に対しても、簡単な修正で ROM 安全性を変更せずに、これらの攻撃を防ぐことが出来る。また RSA および Rabin/Rabin-Williams の場合、適切な PSS パディングの方が他の既知のパディングより頑強である証拠を与える。2008 年 10 月 20 日に IACR の ePrint に投稿された以下の論文と同一の内容。

http://eprint.iacr.org/2008/441

Abstraction in Cryptography [Crypto 2009 Invited Talk]
Ueli Maurer (ETH Zurich)

本講演では、暗号学における抽象化について講義が行われた。先ず、暗号の抽象化に関して、1.帰着(reduction)、2.抽象資源(abstract resouces)、3.抽象システム(abstract systems)、4.離散システム(discrete systems)、5.システム実装(system implementation)、6.物理モデル(physical model)の 6 つのレベルを導入し、抽象的な定義と証明の例がいくつか示された。そして、1-3 に関して、高い抽象レベルで構成的安全性パラダイムを捉えること、資源間の可能な最強の帰着を定義すること、および、汎用結合可能性(universal composability)や reactive simulatability や強識別不能性(indifferentiability)などの概念を統一的に捉えることを目標とした"抽象暗号(Abstract Cryptography)"の提案と解説が行われた。

Asymptotically Good Ideal Linear Secret Sharing with Strong Multiplication over Any Fixed Finite Field [Crypto 2009]
Ignacio Cascudo (University of Oviedo, Spain) and Hao Chen (East China Normal University) and Ronald Cramer (CWI Amsterdam & Leiden University) and Chaoping Xing (NTU Singapore)

本研究では、″多者計算適合(MPC-friendly)″線形秘密分散方式 (linear secret sharing schemes, LSSS), 即ち Cramer, Damgaard, Maurer によって導入された秘匿多者計算(secure multi-party computation, MPC)の基礎となる数学的基本関数(mathematical primitive)を取り扱っている。ChenとCramerは代数幾何から構築され、固定された有限体上の効率の良い秘匿多者計算を可能とする多者計算適合線形秘密分散方式の特殊な類(class)を提案した(CRYPTO 2006)。本論文はこの結果に対して、以下の 4 つの拡張を行った。第一に, 線形秘密分散系のこの類およびその(漸近的)性質を類型化(cast)し分析できる抽象符号理論的フレームワークを提案した。第二に、あらゆる有限体 F_q に対して、漸近的に以下の意味で良い F_q 上 LSSS の無限個の族(family)が存在する事を示した:

方式が"理想的(ideal) "である。理想的とは、即ち、各分散値が一個の F_q 元で構成され、方式が n 参加者に対して t-強乗算を持つという事である。(但し、n を無限大に漸近させると買収許容量 3t/(n-1) が $0<\nu(q)<1$ なる定数 $\nu(q)$に収束する事を仮定する。)さらに$|F_q|$が無限大に漸近する時, $\nu(q)$が最適値の 1 に収束する。

この事実は"漸近的最適買収許容量"の尺度 $\hat{\tau}(q)$ に関する厳密な下界を導く。この結果は Chen と Cramer の結果と、専用の体降下法(dedicated field-descent method) を組み合わせる事によって得られた。特にF_2の場合は、n が無限大に向かう時 3t/(n-1) ≒ 2.86 % となり、1 ビットの秘密を持ち、各参加者に対してたった 1 ビットの分散値しか持たない 2 進 t-強乗法的理想線形秘密分散 (binary t-strongly multiplicative ideal LSSS) の族が存在する。従来そうした結果は q >= 49 の自乗の q に対してのみ示されていた。第三に代数幾何に依存せず、あらゆる有限体F_q上で機能するt-強乗法を持つ理想(線形秘密分散)系の無限個の族を示した。第四に買収許容量に関する改良された非漸近的上界を与えた。

The Round Complexity of Verifiable Secret Sharing Revisited [Crypto 2009]

Arpita Patra and Ashish Choudhary (IIT Madras) and Tal Rabin (IBM) and Pandu Rangan (IIT Madras)

対話プロトコルのラウンド計算量は最も重要な計算量尺度の一つである。従来、t 閾値 n= 3t + 1 参加者の検証可能秘密分散(VSS)において、秘密の再構築が確率 1 で成功する場合、ラウンド計算量の上界および下界が 3 である事が知られていた。本論文では、秘密の再構築に無視しうる確率の誤りを許容するモデルを使い以下の結果を得て、この下界が回避可能である事を示した。

1. n = 3t + 1 に対して効率的な 2-ラウンド VSS プロトコルが存在する。もし攻撃者が non-rushing(他者の出力を見てから自分の出力を決められない事)であると仮定するなら、1-ラウンド再構築が達成できる。
2. t = 1 かつ n > 3 に対して効率的な 1-ラウンド VSS が存在する。
3. 以下を示す事により、これらの結果が閾値(resilience)および共有ラウンドの数の点で最適である事を証明した。
   (a) n <= 3t に対して 2 ラウンド WSS(弱秘密分散)が(従って VSS も)存在しない事を示した。
   (b) t >= 2 and n >= 4 に対して 1-ラウンド VSS が存在しない事を示した。

Somewhat Non-Committing Encryption and Efficient Adaptively Secure Oblivious Transfer [Crypto 2009]

Juan Garay (AT&T Labs) and Daniel Wichs (NYU) and Hong-Sheng Zhou (Univ. of Connecticut)

本論文は、計算進行中に参加者を買収できる適応的攻撃者を許容する効率的な暗号プロトコルの設計について研究している。まず、静的安全より強く適応的安全より弱い準適応的安全性 (semi-adaptive security) なる概念を導入している。適応的安全性と準適応的安全性の主な違いは、準適応的安全性では一方の参加者が買収されてからプロトコルを開始し後にもう一方の参加者が買収される事は許されるが、両方の参加者が正直でプロトコルを開始して、後に両方買収されることは許されないという事である。準適応的安全性は完全な適応的安全性より達成がずっと容易である。次に、本論文では、任意の準適応的安全なプロトコルを完全適応的安全なプロトコルに変換する単純で汎用的なプロトコル翻訳系を与えている。この翻訳は、適応的安全性の問題を、別個に取り扱える 2 つの(より単純な)問題、即ち準適応的安全性の問題および、ある種の安全な通信路を実現する問題に効率的に分解する。本論

文では後者の問題を somewhat non-committing encryption なる新しい基本関数によって解決した。結果として (fully) non-committing encryption を使って安全な通信路を実現する標準的な方法に対して著しい効率の改善が得られた。somewhat non-committing encryption はequivocalityパラメタ l(暗号文が"open" されうる方法の数) および文書サイズ k の 2 つのパラメタを持つ。本論文の実装は小さい値の l に対しては、k が大きくても大変効率的である。この事実は、(bit-OT のような)小さい入出力領域の準適応的安全なプロトコルが完全適応的安全なプロトコルへ大変効率的に翻訳出来ることを意味している。本論文では Peikert らの静的買収安全な紛失通信にこの方法を適用し、効率的で適応的安全で合成可能な初めての紛失通信プロトコルを得た。この方法は 1 個の n-ビット文書を伝送するのに定数のラウンドと O(n) 公開鍵演算しか使わない。

Collusion-Free Multiparty Computation in the Mediated Model [Crypto 2009]

Joel Alwen (NYU) and Jonathan Katz (Univ. of MD) and Yehuda Lindell (Bar-Ilan University) and Giuseppe Persiano (Univ. of Salerno) and abhi shelat (Univ. of VA) and Ivan Visconti (Univ. of Salerno)

結託自由プロトコルとは参加者が水面下で通信を行う事を防ぐ為のプロトコルである(即ち、隠れ通信路が存在しない事を保証するプロトコルのこと)。標準的な通信モデルにおいては、もし一方向関数が存在するなら、あらゆる妥当な秘匿性を満たすプロトコルは、結託自由になり得ない。この不可能性を回避するため、Alwen, shelat, Visconti (CRYPTO 2008) は、あらゆる通信が調停者(mediator)を介してやり取りされる調停モデル(mediated model)を提案した。その目標は調停者が正直である限り結託自由が保障され、さらに調停者が正直でなくとも標準的な安全性が保障されるプロトコルを設計することである。このモデルにおいて、彼らは 2 者セッティングのコミットメントとゼロ知識証明の結託自由プロトコルの構成方法を与えた。本論文では Alwen らの定義を強化し、(調停モデルにおいて)任意の多者関数を計算する結託自由プロトコルを示すことによって、この分野における主たる未解決問題を解決したとのこと。

Privacy-Enhancing Auctions Using Rational Cryptography [Crypto 2009]

Peter Bro Miltersen and Jesper Buus Nielsen (Univ. of Aarhus) and Nikos Triandopoulos (Brown University)

本論文では、密封入札単一品目競売 (sealed-bid single-item auctions) だけでなく、汎用複数品目複数勝者競売 (general multi-item multi-winner auctions) も含む競売プロトコル(auction) のある大きな類型(class)に対する秘匿性(privacy)の強化を考察している。入札者はまず金銭上の利得を第一と考え、自分の型(値付け情報など)の漏洩および他者の型の学習に関してはその次に考えると仮定する。即ち入札者は“貪欲のち猜疑的(greedy then paranoid)”であるとする。ゲーム理論的文脈で秘匿性を厳密に取り扱うために、参加者の利得に金銭および情報(privacy)の両方の成分を考える新しいハイブリッド効用モデル(hybrid utility model)を提唱する。そして、参加者間の専用回線認証通信路(point-to-point authenticated channels) のみしか使用しない暗号プロトコルを介する、信頼調停者(trusted mediator)のない競売の、任意の与えられた“無暫定”個別厳密合理均衡 (“ex interim” individually strictly rational equilibrium)を、合理的暗号 (rational cryptography) を使って如何に近似的に実装するかを示す。“無暫定個別厳密合理”とは、型が与えられるなら、プロトコル開始前に各参加者はある厳密に正の期待効用を持つ事を意味している。“近似的実装”とは、暗号学的仮定のもと、プロトコルの実行が、元の均衡と無視しうるほど近い利得プロファイルを持つ計算量的ナッシュ均衡である事を意味している。

Utility Dependence in Correct and Fair Rational Secret Sharing [Crypto 2009]

Gilad Asharov and Yehuda Lindell (Bar-Ilan University)

近年、ゲーム理論的な意味で参加者が合理的であるという仮定の下での暗号学的プロトコルの研究が注目を集めている。特に合理的秘密分散については、少なからぬ研究が行われている。合理的秘密分散の目的とは、仮に各参加者が自分だけが秘密を得ようと行動しても、秘密の再構築段階で合理的参加者がプロトコルに協力するよう動機づけられる機構(メカニズム)を構築する事である。この問題はごく最近 Halpern と Teague によって提起されたものであるが、既に美しいアイディアを持つ沢山の研究結果が与えられている。しかしながら、いずれの結果も、参加者の実際の効用値(あるいは少なくともその限界)が事前に判明している必要がある。現実には参加者の効用というものは必ずしも公開される情

報ではなく、むしろ秘密にしておくべき情報であるから、この仮定は大きい問題となる。本研究では、この“実際の効用値への依存”が本当に必要であるか否かを考察している。そして、基本的セッティングでは、この依存性無しには合理的秘密分散が達成不可能であるという否定的な結果を証明した。肯定的な結果として、効用関数に関する標準的仮定を緩和することにより効用独立(utility independence)を達成可能な事も示した。これらの結果の他に、同時通信路（simultaneous channel）を仮定しない、既知の全ての合理的秘密分散プロトコルが、参加者の一人が原因で他の誰かが誤った値を出力してしまう問題を解決出来ない事を示した(この問題は、ある参加者が秘密を知り、他者が誤った値を得る時に高い効用が得られる場合に起こる)。そして、非同時通信路モデルにおいて、この攻撃により得られる参加者効用の実際の値が事前に分からない場合は、この問題は本質的に避けられないことを示した。

1.7.4. Crypto 2009 の発表(4 日目)

On Bounded Distance Decoding, Unique Shortest Vectors, and the Minimum Distance Problem [Crypto 2009, ECC2009]
Vadim Lyubashevsky (Tel-Aviv University) and Daniele Micciancio (UCSD)

格子ベース暗号が安全性の根拠とする、BDD(Bounded Distance Decoding)問題、uSVP(unique Shortest Vector Problem)問題、GapSVP 問題の多項式近似因子$\sqrt{}$(n/log n)内の等価性を示し、長年の未解決問題を解決した。これにより、Ajtai-Dwork 暗号や Regev 暗号は、従来 uSVP 問題に基づいていたが、それぞれ GapSVP_{O(nˆ2.5)}と GapSVP_{O(nˆ2)}に基づいていることが言えた。また、ほとんどの格子問題に関する等価性はほぼ 2 つのクラス(GapSVP, GapSIVP, SIVP, uSVP, BDD のクラスと SVP, CVP のクラス)になり、残るところ、SVP から GapSVP への帰着が示せれば、ほぼすべての格子問題の等価性がいえることになる。

Fast Cryptographic Primitives and Circular-Secure Encryption Based on Hard Learning Problems [Crypto 2009]
Benny Applebaum (Princeton) and David Cash (Georgia Tech) and Chris Peikert (SRI International) and Amit Sahai (UCLA)

LWE (Learning a linear function With Errors)問題は、見たところ困難な問題であり、いくつかの暗号スキームの根拠となっている。強い安全性の性質と高いレベルの効率性を持つ、更なる応用を示す。1 つ目は、KDM 攻撃(Key-Dependent Messages、攻撃者が任意のアフィン関数を通じて秘密鍵に依存するメッセージの暗号文を得ることができる)に対して安全であり、かつ、Circular 安全(任意のユーザーの秘密鍵が任意のユーザーの公開鍵で暗号化されてよいという鍵サイクルが存在しても安全)である、公開鍵および対象鍵暗号システムを構成する。どちらの場合も暗号文は平文より定数因子分のみ大きいだけであり、暗号化および復号のコストは、公開鍵の場合メッセージシンボルに対して n polylog(n)ビット演算であり、対称鍵の場合 polylog(n)ビット演算となる。2 つ目は、2 つの効率的な擬似ランダムオブジェクトを構成する。1 つは LPN(Learning Parity with Noise)の困難性をベースとした、サイズ O˜(n)のブール回路で計算される擬似乱数生成器であり、もう 1 つは RWPRF(Randomized Weak PseudoRandom Function)と呼ばれる、弱い擬似乱数性および検証可能性を持つ関数群である。

Dual System Encryption: Realizing Fully Secure IBE and HIBE under Simple Assumptions [Crypto 2009]
Brent Waters (Univ. of Texas Austin)

暗号システムの安全性を証明するための、新しい方法論、DSE(Dual System Encryption)を示す。この技術を用いて、IDE(ID ベース暗号)および HIBE(階層的 ID ベース暗号)の安全性を、単純かつ確立された決定双線型 Diffie-Hellman 仮定および決定線型仮定の下で安全であることを示すことができる。我々の IBE システムは一定数の群要素からなる暗号文、秘密鍵、公開パラメーターを持ち、単純な仮定および短いパラメーターからなる初めての HIBE および IBE システムである。DSE システムにおいては、暗号文と秘密鍵は、2 つの区別できない型のうち一つの型を取ることができる。秘密鍵または暗号文は、それぞれシステムの鍵生成または暗号化アルゴリズムにより生成されたとき normal であるという。更に、semi-functional という鍵および暗号文を定義する。semi-functional な秘密鍵は、すべての normal に生成された暗号文を復号するが、semi-functional な暗号文を復号しようとすると失敗する。同様に semi-functional な暗号文は、normal な秘密鍵によってのみ復号される。

The Group of Signed Quadratic Residues and Applications
Dennis Hofheinz and Eike Kiltz (CWI Amsterdam)

Signed Quadratic Residue (SQR)は平方剰余の変形版であり、次のように定義される。
QR_N^+:={ |x| : x=y if y∈QR_N ∧ y≦(N-1)/2,

x=-(y-N) if y∈QR_N ∧ y>(N+1)/2 }
SQR は素因数分解と同程度に計算困難(平方根を求めるのが困難)であるものの、決定問題(SQR の判定)が容易であるギャップ群(gap group)である。このため、素因数分解を困難とする仮定の下、SQR 上で SDH 仮定が成り立つことを示せる。つまり、SQR では DDH オラクルが存在しても、DH 問題が困難となる。これらの事実の有用性をハイブリッド・エルガマル暗号方式(DHIES)に適用し、使用するハッシュ関数が four-wise 独立であるとき、CCA 安全であることを示す。

Short and Stateless Signatures from the RSA Assumption

Susan Hohenberger (Johns Hopkins) and Brent Waters (Univ. of Texas Austin)

従来の、RSA 仮定に基づく、標準モデルで安全な短い署名では、より強い安全性仮定(強 RSA 仮定)や署名者が状態を保持するといった条件が付いている。本論文は、通常の RSA 仮定の下で標準モデルでの安全性が証明できる最初の短い状態なし署名法を実現した。公開鍵も短く、法 N、Z_N^*の要素 1 個、整数 1 個、擬似ランダム関数のシード 1 個だけである。提案された署名法の設計において、弱い署名法から十分強い(fully-secure)署名法を作る構成法とカメレオン・ハッシュ関数を利用した。

Smooth Projective Hashing for Conditionally Extractable Commitments

Michel Abdalla and Celine Chevalier and David Pointcheval (ENS)

平滑射影ハッシュ関数は Eurocrypt 2002 で Cramer-Shoup が提案したもので、ある言語に対するゼロ知識証明の特殊形と見なせる。平滑射影ハッシュ関数は最初、効率的で CCA 安全な公開鍵暗号方式の構成に使用されたが、それ以外にもパスワード・ベースの認証つき鍵交換や oblivious transfer などに応用されている。本論文では、平滑射影ハッシュ関数が存在することが知られている簡単な言語の分離や結合の記述によってより複雑な言語を構成する方法を示す。次に、より複雑な言語上の平滑射影ハッシュ関数をゼロ知識証明を使わずに、どのように extractable commitment schemes と効率的に関連付けるか説明する。最後に、これらの結果を使って、よく知られた2つの暗号学上の問題に対するより効果的な解を与える。

1.8. ECC 2009 の発表

1.8.1. ECC 2009 の発表(1 日目)

Security of compositions with implicit certificate schemes [ECC 2009]
Daniel Brown, ○Matthew J. Campagna, Scott Vanstone (Certicom Research)

OMC(Optimal Mail Certificate)証明書は、implicit タイプの証明書であり、従来の証明書と比較してサイズが小さいなどのメリットがある。ECDSA 署名と OMC との組合わせに対し、Qu により偽造攻撃が示されたため、それに対策を施した ECQV 証明書が開発された。ECDSA 署名と ECQV 証明書の組合わせに対しては、Qu の攻撃は有効とならず、受動攻撃に対して安全なことが示される。本技術に関しては、SEC 4、ZigBee Smart Energy Profile、ISA SP100.11a、CEN DPM Infrastructure Standard などで標準化が進められている。

Asymmetric Pairings [ECC 2009]
○Alfred Menezes, S. Chatterjee, D. Hankerson, E. Knapp (University of Waterloo)

2006 年に Galbraith、Paterson、Smart らは、Pairing を、対称的(定義域の 2 つの群 G1,G2 が同一)な Type 1(超特異)と、非対称的な Type 2、Type 3(通常)に分類した。G2 から G1 への効率的に計算可能な同型写像が存在する場合を Type 2、そうでない場合を Type 3 と呼ぶが、一般に Type 2 上のプロトコルから Type 3 上のプロトコルへの自然な変換が存在し、セキュリティ証明も成立し、パラメーターを適切に選択すれば処理性能も劣ることはない。従って、同型写像は暗号上メリットとはならず、Type 3 に対して、Type 2 を使うことのアドバンテージは、セキュリティ上も性能上も見当たらない。Type 1 上のプロトコルを Type 3 上のプロトコルに変換する場合は、処理性能に影響を与えるトレードオフが発生する可能性があるため、プロトコル設計者はトレードオフを分析する必要がある。

Boneh-Boyen signatures and the Strong Diffie-Hellman problem [Pairing 2009/ECC 2009]
○David Jao, Kayo Yoshida (University of Waterloo)

Boneh-Boyen 署名は偽造不可能性が標準モデルで q-Strong Diffie-Hellman 仮定へ帰着可能なペアリングに基づく署名であるが、今まで q-Strong Diffie-Hellman 仮定が破れる時 Boneh-Boyen 署名が敗れるか否かは分かっていなかった。本論文では、これを証明し、Boneh-Boyen 署名の偽造が q-Strong Diffie-Hellman 問題の求解と真に等しい事を示した。また、この等価性と q-Strong Diffie-Hellman 問題に対する良く知られた指数時間攻撃(Cheon の攻撃) を使って、大抵のペアリング向け曲線上で Boneh-Boyen 署名の秘密鍵を、時間計算量 $O(p^{2/5+\varepsilon})$、照会計算量 $O(p^{1/5+\varepsilon})$にて回復するアルゴリズムを示し、このアルゴリズムと Pollard の λ 法や ρ 法のような古典的な離散対数アルゴリズムの性能を比較する実装結果を示した。可能な対策として、鍵サイズを大きくする事は署名サイズや効率の点で望ましくなく、上記の攻撃が適用できない曲線を選択できればそれが望ましいが、出来ない場合は q-Strong Diffie-Hellman への帰着はなるべく避けた方が実用上賢明とのこと。

Loading the bases – some open problems associated with the use of multiple-base number systems in ECC [ECC 2009]
Vassil S. Dimitrov (University of Calgary)

DBNS(Double Base Number System)は、与えられた正整数 n を、二つの素数べきの積({p,q}整数と呼ぶ)の和または差で表すスキームのことを言う。DBNS は、様々な計算問題(行列の多項式計算、楕円曲線の点のスカラー倍算等)において、様々な自明でない上限や下限を与える。例えば Koblitz 曲線の τ に関して、$Z[\tau]$の元 k は、O(logN(k)/loglogN(k))個の(τ, $\tau-1$, $\tau^2-\tau-1$)クライン整数の和で表される。DBNS に関連する予想をいくつか述べる。
予想: $\pm 2^a 3^b = \pm 2^c 3^d = \pm 2^e 3^f = 4985$ は、整数解を持たない。
(x 個の符号付き{2,3}整数を必要とする最小の整数は、x=1 のときは 1、x=2 のときは 5、x=3 のときは 103 である。x=4 のときは、4985 と予想している。)

Computing Scalar Multiplication with Many Cores [ECC 2009]

○Chen-Mou Cheng (National Taiwan University, Taiwan), Daniel J. Bernstein (University of Illinois at Chicago, USA), Tanja Lange (Technische Universiteit Eindhoven, the Netherlands), Bo-Yin Yang (Academia Sinica, Taiwan)

プロセッサーのクロック周波数増加には様々な壁が出てきており、多数のコアを持つプロセッサを用いることがメインストリームとなってきているので、GPUを用いて楕円曲線のスカラー倍算高速化を図る。理想的な応用先としては、素因数分解の楕円曲線法(ECM)や Pollard の ρ 法への適用が考えられる。1024 ビット以上の数体篩法(NFS)による素因数分解においては、100-300 ビット整数の 30 ビット程度の素因子を見つける処理が重要となり、ECM の高速化により NFS の高速化が期待できる。NVIDIA GTX 295 を使用したシステムのコストパフォーマンスは、1880 USD で、192 ビットモジュラスの乗算剰余演算を 1 秒間に 13 億回行うことが可能である。

Fast Implementation of Elliptic Curve Cryptography and Pairing Computation for Sensor Networks [ECC 2009]

○Julio Lopez, Diego Aranha, Danilo Camara, Ricardo Dahab, Leonardo Oliveira, Conrado Lopes (University of Campinas, Brazil)

無線センサーネットワーク(WSN)のような計算能力や計算資源が限定された環境において、暗号を配備することは冒険的な仕事である。3 つの WSN プロセッサ(ATmega128L、MSP430、Intel PXA27x)においてペアリング計算および楕円曲線スカラー倍算の高速ソフトウェア実装を行った。具体的には、素体・2 べき体演算の高速化、ECDSA の高速実装(新記録)、WSN 向けペアリング計算の高速実装(新記録)を行った。例えば、ATmega128L における ECDSA の鍵生成・署名・検証の処理性能は、163 ビット Koblitz 曲線の場合各々0.29 秒、0.36 秒、0.63 秒、233 ビット Koblitz 曲線の場合各々0.66 秒、0.78 秒、1.39 秒、ランダムな 163 ビットバイナリ曲線の場合各々0.37 秒、0.45 秒、1.04 秒、ランダムな 233 ビットバイナリ曲線の場合各々0.94 秒、1.04 秒、2.55 秒であった。ATmega128L における F2 の 271 次拡大体上のペアリングフレンドリー超特異曲線:y^2+y=x^3+x 上での η T ペアリングの処理性能は、C 言語で 4.44 秒、アセンブラ言語で 2.06 秒であった。
(D.J.Bernsteinからソースコードは公開しているかと質問があり)ソースコードは現在は公開していないが、公開の準備をしている。

1.8.2. ECC 2009 の発表(2 日目)

Post-quantum cryptography [ECC 2009]

Dan Bernstein (University of Illinois, USA)

量子計算機に耐性を持つ暗号の候補の一つとして、符号理論ベースの暗号を集中的に取り上げ、McEliece 暗号や近年の hidden Goppa 符号構造などの話題を紹介する。量子計算機が実現されると、RSA、DSA、ECDSA、(一般の)ECC、(一般の)HECC、Buchmann-Williams、(一般の)類群はすべて破られるが、それ以外のハッシュベース暗号、符号ベース暗号、格子ベース暗号、多変数2次方程式暗号、秘密鍵暗号などは生き残る。McEliece 暗号において、公開鍵 K が GF(2)上のランダムな 500×1024 行列の場合、情報集合復号は 1988 年以来多くの改良がなされ、2008 年に Bernstein-Lange-Peters は、2^{58} Core 2 Quad サイクルを達成した。近年の McEliece 暗号は、より大きな(n/2)×n 行列(例えば 1800×3600)を用いることにより、システムを救っている。既存攻撃は、大雑把には $2^{n/2\lg n}$ 命令の計算量となってしまう。受信者は、hidden Goppa 符号構造を持つ公開鍵 K を生成する。即ち、K=SHP において、S は(n/2)×(n/2)可逆行列、H は (n/2)×n Goppa 行列、P は n×n 置換行列であり、この構造を見出すことは、ランダムな K の攻撃よりも困難に見える。

On Bounded Distance Decoding, Unique Shortest Vectors, and the Minimum Distance Problem [ECC 2009 / Crypto 2009]

○*Daniele Micciancio(University of California at San Diego, USA), Vadim Lyubashevsky(Tel Aviv Univ., Israel)*

格子ベース暗号が安全性の根拠とする、BDD(Bounded Distance Decoding)問題、uSVP(unique Shortest Vector Problem)問題、GapSVP 問題の多項式近似因子$\sqrt{}$(n/log n)内の等価性を示し、長年の未解決問題を解決した。これにより、Ajtai-Dwork 暗号や Regev 暗号は、従来 uSVP 問題に基づいていたが、それぞれ GapSVP_{$O(n^{2.5})$}と GapSVP_{$O(n^2)$}に基づいていることが言えた。また、ほとんどの格子問題に関する等価性はほぼ 2 つのクラス(GapSVP, GapSIVP, SIVP, uSVP, BDD のクラスと SVP, CVP のクラス)になり、残るところ、SVP から GapSVP への帰着が示せれば、ほぼすべての格子問題の等価性がいえることになる。

NICE Cryptanalyses [ECC 2009/ASIACRYPT2009]

Guilhem Castagnos (Université Bordeaux, France)

$N=pq^2$ 型の整数を素因数分解する二元二次形式に基づく新しいアルゴリズムを提案している．一般に，その実行時間は指数時間となるが，特殊な(算術的)ヒントが利用出来るときは多項式となる．90 年代末期に提案された二次体に基づく公開鍵暗号，いわゆる NICE ファミリーに対する攻撃がまさにこの場合に相当する．この暗号系には二次体の虚実に従って二種類の版が存在する．本論文のアルゴリズムは NICE のどちらの版に対しても機能し，多項式時間一般鍵回復攻撃を実現する．Castagnos と Laguillaumie は最近 虚-NICE の完全解読を与えたが，この攻撃は 実-NICE には適用できなかった．本論文のアルゴリズムは CL 攻撃と同様に 虚-NICE の公開鍵をヒントとして効率の良い素因数分解を与えるが，実-NICE の場合でも，二次体 Q($\sqrt{}$p)の単数規準が著しく小さいという知識を使って効率の良い素因数分解を与える事が出来る．一般的な $N=pq^2$ 型の素因数分解ではこのアルゴリズムは指数時間で，一般化(ESIGN の場合など)については未解決とのこと．

Isogeny computation in small characteristic [ECC 2009]

Luca De Feo (Ecole Polytechnique, France)

同種写像は楕円曲線の研究に重要なツールであり、楕円曲線暗号においても、位数計算、スカラー倍算高速化、離散対数困難性の証明、より簡単な曲線への離散対数変換、同種写像鎖への弱い曲線の隠蔽、ハッシュ関数の定義など様々な用途に使われる。Velu は、曲線が複素数体上定義されている場合に、二つの曲線間の同種写像を明に表す公式を与えた。これらの公式は、Morain、Atkin、Charlap-Coley-Robbins らにより、体の標数が同種写像の次数よりも大きい場合に拡張された。の高速計算アルゴリズムについて述べられた。体の標数が小さいときには、Couveignes、Lercier、Joux-Lercier、Lercier-Sirvent らのアルゴリズムが考えられたが、これらの戦略を見直し、Couveignes のアイディアを改良することにより高速なアルゴリズムを得た。数式処理システム SAGE に実装を進めている。

Encryption from the Diffie-Hellman assumption [ECC 2009]

Eike Kiltz (Centrum Wiskunde & Informatica, Holland)

通常の楕円曲線暗号システムでは Hybrid ElGamal スキーム DHIES がよく用いられているが、その安全性はランダムオラクルモデルにおける強 DH(Diffie-Hellman)問題が根拠となっている。強 DH(Diffie-Hellman)問題の安全性については研究が十分ではない面もあるため、DHIES の代替として、Twin ElGamal、HK07 各種暗号を紹介する。Cash-Kiltz-Shoup による Twin ElGamal では Twin DH 仮定を新たに導入し、強 TwinDH 仮定が DH 仮定と等価になることを示した。これによりランダムオラクルモデルの下で、DH 仮定に基づくスキームを構成することができるが、暗号化においてべき演算 1 回分のコストおよび公開鍵において 1 要素が増加する。2007 年の Hofheinz-Kiltz によるスキームは、標準も出るにおいて HDDH(Hashed Decesion DH)仮定のもとで安全性が示される。これはランダムオラクルモデルの下では、CDH(Computational DH)仮定に基づくことになる。Twin ElGamal と比較して暗号文において更に 1 要素が増加する。

Number Theory or Numerology? [ECC 2009 招待講演]

Richard K. Guy (University of Calgary, Canada)

特別招待講演。各種数列・数字遊びと、その背後にある数論との関係についての各種話題が述べられた。

1.8.3. ECC 2009 の発表(3 日目)

Computing modular polynomials with the Chinese Remainder Theorem [ECC 2009]
Andrew Sutherland (Massachusetts Institute of Technology, USA), Reinier Broker, Kristin Lauter (Microsoft Research, USA)

モジュラー多項式は、位数計算(SEA アルゴリズム)、CM 法による構成、自己準同型群の計算など楕円曲線に関するアルゴリズム研究にとって重要な役割を占めるが、次数を n とすると、そのサイズは $O(n^3 \log n)$ビットと大きく、それを計算することはとても困難となる。同種写像および中国剰余定理を使ってモジュラー多項式を効率的に計算するアルゴリズムを得た。一般リーマン予想のもとで、計算量は $O(n^3(\log n)^{3+e}\log\log n)$となる。m を法とすると、$O(n^2 \log(mn))$となる。Weber の f-関数などにも適用可能である。扱える次数の記録としては、モジュラー多項式なら 5003 次、Weber の f-関数は 50021 次をそれぞれ 1 日以内、スピードの記録としては、モジュラー多項式 251 次なら 40 秒、Weber の f-関数 1009 次なら 3.2 秒で計算できる。

Generating Genus two Hyperelliptic Curves over Large Characteristic Finite Fields [ECC 2009]
Takakazu Satoh (Tokyo Institute of Technology, Japan)

素体上、$y^2=x^5+ux^3+vx$ という形の種数 2 の曲線に関する位数計算アルゴリズムにより、超楕円暗号に適した曲線をランダムに生成できる方法を与える。Furukawa-Haneda-Kawazoe-Takahashi は、$y^2=x^5+ax$、$y^2=x^5+a$ の形の超楕円曲線位数公式を明に与えたが、曲線の形は非常に特殊である。我々の方法は、$y^2=x^5+ux^3+vx$ の形の曲線の係数をランダムに生成し、位数が大きな素数を含む場合に、効率的にその位数を計算する。位数がそのような形でない場合は、計算を破棄し次の候補を試みる。曲線の形は、まだ特殊ではあるが、2 項式ほど特殊ではない。そのため、ある種の ECDLP の困難性との比較が可能となるが、更なる安全性に関する考察が必要である。実装に関しては、p が 86 ビット程度の素数の場合、ランダムに生成した 2000 本の曲線のうち 13 本が 2×素数の形の位数となった。1 曲線あたりの計算時間は 3 分から 20 分であった。ペアリングに適した曲線への適用については、David Mandell Freeman との共同研究が進行中であり、近い将来発表できる見込みである。

Cryptographic Aspects of Real Hyperelliptic Curves [ECC 2009]
○ *Mike Jacobson(University of Calgary, Canada), S.Erickson, J.Hammell, R.Scheidler, N.Shang, S.Shen, A.Stein*

超楕円曲線暗号に関する研究の多くは、超楕円曲線の所謂虚モデルにおけるヤコビアン群を用いており、因子のマンフォード表現は、群要素を表現し効率的な演算を与える。有限体上定義され、5 つ以上の要素を持つ虚モデルの超楕円曲線は、同じ基礎体上のある実モデル超楕円曲線に双有理同値となるが、体を拡大しなければ逆は必ずしも成立しないため、実モデルは虚モデルよりも一般的であるといえる。しかしながらヤコビアン群の演算が、より面倒かつ非効率的になると考えられているため、実モデルの暗号への適用はあまり研究されていなかった。本講演では、実モデルの超楕円曲線を用いた暗号への応用を概観する。Infrastructure といわれる因子のある種の構造における baby ステップという通常の演算よりも高速な演算に焦点をあてる。Infrastructure における鍵共有プロトコル、Infrastructure におけるスカラー倍算の Scheidler-Stein らによる改良、種数 2 の場合の因子演算の明なる公式について述べ、鍵共有の性能データを示す。実モデルの方が虚モデルよりも若干遅くなっている。Infrastructure の DLP に関しては、一般的な計算量は平方根オーダーである、種数が 1 の場合は ECDLP と等価、位数 R がスムースならば Pohlig-Hellman の方法が適用可能、∞1-∞2 により生成される部分群の離散対数と同じ、$g > \log q$ の場合は $O(L_{q^{\wedge}\{2g+2\}}[1.44+o(1)])$等々の結果が知られている。2008 年に Hammell は、Infrastructure の baby ステップを用いてランダムウォークを $O(g^2)$から $O(g)$に下げ関係式を高速に生成し、更に線型代数を改良することにより、ある仮定の下、指数計算法の計算量を $g > \log q$ の場合に、$O(L_{q^{\wedge}g}[2.45+o(1)])$と解析した。

1.8.4. ECC 2009 rump の発表

Batch Binary Edwards [ECC2009 rump]
Daniel Bernstein (University of Illinois at Chicago, USA)

F_2 の 251 次拡大体上での、2.4GHz Core 2 Quad による Diffie-Hellman 計算の新記録を達成した。
http://binary.cr.yp.to/

Pairings on Edward curves [ECC2009 rump]
Michael Naehrig (Technische Universiteit Eindhoven, Netherlands)

Tate ペアリングを計算するミラーアルゴリズムにおいて、高速化のための倍算および加算の新しい公式を提示した。
IACR ePrint Archive 2009/155

Recent ECC implementations [ECC2009 rump]
Peter Schnabe (Technische Universiteit Eindhoven, Netherlands)

PS3 上で、256 ビット楕円曲線のスカラー倍算を高速に実装した。
http://cryptojedi.org/crypto/

Scaler EC multiplication on x86 [ECC2009 rump]
Bo-Yin Yang (Academia Sinica, Taiwan)

Kleinjung の訪問を受け、x86-64 上の実装が速くないと指摘され、改良を加え、Kleinjung のデータを超えることができた。

A Diophantine Equation [ECC2009 rump]
Everett Howe (Caltech, USA)

Vassil Dimitrov の一般講演における予想を証明した。
http://alumnus.caltech.edu/~however/talks/Calgary.pdf

Appointed cryptanalysis, or how to win an iPhone [ECC2009 rump]
Tanja Lange (Technische Universiteit Eindhoven, the Netherlands)

ターゲットフレーズの SHA-1 値にハミング距離が最も近い SHA-1 値を持つフレーズを 30 時間で求めるプログラミングコンテストに応募し、賞品である iPhone を手に入れた。

1.9. FDTC 2009 の発表

1.9.1. FDTC 2009 の発表(1 日目)

Low voltage fault attacks on the RSA cryptosystem [FDTC 2009]
A. Barenghi, G. Bertoni, E. Parrinello and G. Pelosi

組込み用の汎用マイクロプロセッサである ARM9 用に実装された RSA 暗号に対し、電圧降下を利用した故障利用攻撃を提案し、有効性を確認した。ここで提案された攻撃法の特徴は、誤動作による命令の交換(swap)を利用する点であり、特殊な装置を必要としないため、非常に安上がりですむという長所がある。

Fault attack on Schnorr based identification and signature schemes [FDTC 2009]
P.A. Fouque, D. Masgana and F. Valette

指数演算を利用した公開鍵暗号系に対する DPA 対策として Coron は CHES 1999 において、指数をランダム化する対策を提案した。CHES 2008 において著者らは carry に注目した情報漏えいを利用することで RSA 暗号が攻撃できることを示した。この論文では carry に着目するアイデアを発展させ、DSA, ECDSA といった署名や Schnorr, GPS という認証・署名方式に対する非常に効率の良い故障利用攻撃を提案する。攻撃に必要なコストは秘密鍵を含んだ計算式の複雑度に依存する。

Protecting RSA against fault attacks: the embedding method [FDTC 2009]
M. Joye

モンゴメリ・ラダーを利用した RSA 暗号に対する故障利用攻撃の対策として、公開鍵指数を秘密鍵の一部として埋め込んでおき、計算の途中と最後に、正しい値からの誤りを検知する方法を提案する。この対策は既存のインフラに適合しており、実装のオーバーヘッドは小さく、特にオンボードの鍵生成を提供する Java Card に適している。

Securing AES implementation against fault attacks *[FDTC 2009]*
L. Genelle, C. Giraud and E. Prouff

故障攻撃への対策として回路を二重化する方法があるが、計算コストが大きい。この論文では、AESの操作の各々に対するダイジェストを計算し、独立にチェックすることにより、次の3つの条件を満たす防御法を実現した。1) 少なくとも、1 バイト誤作動モデルでの検出率が 100%2) 2 バイト誤作動モデルに対する二重化対策よりも検出率が高い 3) 1 バイト・モデル及び 2 バイト・モデルの二重化対策より効率が良い

WDDL is protected against fault attacks [FDTC 2009]
N. Selmane, S. Bhasin, S. Guilley, T. Graba and J.L. Danger

WDDL (Wave Dynamic Differential Logic)は、回路の二重化して電力消費を一定にする電力解析対策の一種であり、CMOSセルを使うので特殊なライブラリを必要としない。本論文では、AESのFPGA実装に対し、電圧を低下させることによってセットアップ時の誤動作を引き起こす故障攻撃を行った。その結果、WDDLが誤ったビットを暗号文において 0 ビットに置き換え、情報を漏洩しないことが確認できた。さらに、この結果を裏付ける理論モデルも示した。

Practical fault attack on a cryptographic LSI with ISO/IEC 18033-3 block ciphers [FDTC 2009]
T. Fukunaga and J. Takahashi

ブロック暗号の国際規格ISO/IEC 18033-3に記載された6種類の暗号AES, DES, Camellia, CAST-128, SEED, MISTY1 を、暗号専用LSIを搭載したサイドチャネル攻撃用標準評価ボード SASEBO-Rに実装し、クロック信号にグリッチを乗せることによって誤作動を希望する段で引き起こせることを確認した。

AESに関してはPiretの攻撃法を適用し、誤まった暗号文1個だけを用いて、鍵が復元できることを確認した。

A fault attack on ECDSA [FDTC 2009]
J.M. Schmidt and M. Medwed

ECDSAのdouble and adder、または、Montgomery ladderによる実装に対する新規の故障利用攻撃を提案した。この攻撃は、スキップ命令に関する誤作動を利用し、一時鍵の部分情報を入手し、それを使った格子攻撃によって署名鍵を求めるものである。さらに、射影Jacobi座標での展開を利用した故障検知による防御法も提案している。

Fault analysis of the stream cipher Snow 3G [FDTC 2009]
B. Debraize and I. Marquez Corbella

SNOW 3Gは、3GPPが決めた第3世代携帯電話技術UMTSでKASUMIが攻撃されたときのバックアップ用のストリーム暗号で、国際規格ISO/IEC 18033-4 に採用されたSNOW 2.0 の改良版である。この論文では、22 回の故障注入だけで秘密鍵の復元に成功した。

Using optical emission analysis for estimating contribution to power analysis [FDTC 2009]
S. Skorobogatov

この論文では、動作中のチップの発光を安価なCCDで検出し、それが電力波形と高い相関を持つことを示し、故障利用攻撃に利用出来る可能性を指摘している。発光測定は、0.9 μ mマイクロコントローラのSRAM、EEPROM、Flashに保存されたデータの復元に利用されており、0.13 μ mチップに対する適用可能性についても議論されている。発光測定単体の攻撃には限界があるが、部分的なリバースエンジニアで攻撃対象の部分を絞るなど、故障利用攻撃などを補強する技術として有望としている。

Differential fault analysis on SHACAL-1 [FDTC 2009]
R. Li, C. Li and C. Gong

SHACAL-1 はNESSIEの最終候補の一つだったブロック暗号で、SHA-1 を構成要素としている。そのため、S-boxと置換ではなく、混合と回転が処理の中心であるためか、故障利用の解析結果はほとんどなかった。この論文では、word単位の故障を仮定したモデルを利用し、理論解析と実験によって有効性を検証した。その結果、72 回のランダムな故障によって、512 ビットの鍵が確率 60%で復元できることと、120 回の故障によって、512 ビットの鍵が確率 99%で復元できることを示した。

1.10. CHES 2009 の発表

1.10.1. CHES 2009 の発表(1 日目)

Faster and Timing-Attack Resistant AES-GCM [CHES 2009]
Emilia Ka˝sper, Peter Schwabe

AES の CTR モードをビットスライスで実装することにより、キャッシュタイミング攻撃に対する耐性を持たせるとともに高速化を実現した。Core 2 では、従来より 25%高速な 7.59 cycles/byte を達成した。576-byte パケットでは、従来のヒットスライス実装より 2 倍以上高速化した。また、lookup-table に基づく GCM 認証では、従来より 30%高速な 10 cycles/byte を達成した。さらに、処理時間一定の AES-GCM を 21.99 cycles/byte という妥当な速度を実現し、タイミング攻撃に耐性のある authenticated encryption のフルセットを提供している。

Accelerating AES with Vector Permute Instructions [CHES 2009]
Mike Hamburg

AES の S-box 計算を高速化し、キャッシュタイミング攻撃耐性を持たせるため、F_2^8 を F_2^4 からの逐次拡大を利用し、ベクトル置換で実行する方法試した。その結果、Intel Core i7 920(Nehalem)では、一つ前の Ka'sper-Schwabe の実装に勝てなかったものの、Power PC G4 では、より少ない cycles/byte を実現した。

SSE Implementation of Multivariate PKCs on Modern x86 CPUs [CHES 2009]
Anna Inn-Tung Chen, Ming-Shing Chen, Tien-Ren Chen, Chen-Mou Cheng, Jintai Ding, Eric Li-Hsiang Kuo, Frost Yu-Shuang Li, Bo-Yin Yang

多変数公開鍵暗号システム(MPKC)は量子計算機後の暗号として有望視されているが、CPU の進歩に伴なう実装効率の改善が目覚しい楕円曲線暗号(ECC)に差を差をつけられつつあるように見える。
この論文では、現在広く普及した CPU 利用できる SSE2 を初めとするベクトル命令で多数の小さな整数演算を駆動することによって、MPKC の実装効率も改善することを示す。特に Rainbow 型の電子署名では、Intel の SSSE 命令を利用することによって、通常の SW 実装の 4 倍の高速化が実現する。比較的サイズの小さい奇素数体上の MPKC では、Intel 製及び AMD 製の 64 ビット CPU のほとんどで利用できる SSE2 命令を使って高効率実装が実現する。筆者らはここで開発された手法が FPGA にも適用可能であるとしている。

MicroEliece: McEliece for Embedded Devices [CHES 2009]
Thomas Eisenbarth, Tim Gu˝neysu, Stefan Heyse, Christof Paar

McEliece 暗号は未知の二進線形符号による復号が NP 完全であることに基づいており、素因数分解ベースや離散対数ベースの暗号と異なり、量子暗号でも効率的に解読できないと期待されている。この論文では、鍵サイズが大きい McEliece 暗号を組込み系で効率的に実装する方法を示す。著者らによると、低価格の 8 ビット AVR マイクロプロセッサと Xilinx Spartan-3AN FPGA に McEliece 暗号を実装したのはこれが最初である。

Practical Electromagnetic Template Attack on HMAC [CHES 2009]
Pierre-Alain Fouque, Gae˝tan Leurent, Denis Re'al, Fre'de'ric Valette

この論文では HMAC-SHA-1 に対する効率的な電磁波測定利用のテンプレート攻撃を示す。攻撃に利用するのは、攻撃者がデバイスにアクセスして設定できる profiling phase の後で、HMAC-SHA-1 の単独実行を観測することで秘密鍵を復元する。鍵の復元にはテンプレート攻撃が利用され、κ をワード(32 ビット)単位で表した鍵長とすると、計算量は圧縮関数 $2^{32}\,3^{\kappa}$ 回分である。この攻撃法は通常の組込み系の実装に対して有効であり、FPGA 上の NIOS プロセッサによる実装に対する実験によって、情報の漏えいを確認した。著者らはこの論文の結論が SHA-3 のサイドチャネル耐性の要件チェックに寄与することを

期待している。

First-Order Side-Channel Attacks on the Permutation Tables Countermeasure [CHES 2009]
Emmanuel Prouff, Robert McEvoy

SCN 2008 で Coron らはランダムな置換表を利用したサイドチャネル対策を提案した。この対策ではアルゴリズム実行中に、計算の途中の値がランダムな置換表に従って操作される。本論文では、SCN 2008 論文の対策による AES 実装のある操作が1次のサイドチャネル情報を漏洩することを示し、それを利用して、相関ベース及び相互情報量ベースの新しい攻撃法を提案する。これらの攻撃法の有効性は、計算機実験とスマートカード上での実装に対する攻撃で確認された。

Algebraic Side-Channel Attacks on the AES: Why Time also Matters in DPA [CHES 2009]
Mathieu Renauld, Franc,ois-Xavier Standaert, Nicolas Veyrat-Charvillon

最近提案された代数的サイドチャネル攻撃では、ターゲットとする暗号方式と物理的に漏洩した情報から over defined な連立方程式を導き、解くことにより、鍵を復元する。この攻撃法か最初に適用されたのは、代数的構造が単純なブロック暗号 PRESENT だった。この論文では、PRESENT に対する代数的攻撃における洞察の多くが8ビット・コントローラ上のサイドチャネル対策なしの AES 実装に対しても有効であることを実験的に示す。さらに、WISA 2005 で Oswald らが提案した $GF(2^4)^2$ へマスクする対策と、ACNS 2006 で Herbst らが提案した S-box の事前計算を利用する対策について解析し、比較した。その結果、後者の対策がより有効でありそうなことと、初段と最終段だけの対策は有効でないことが示された。

Differential Cluster Analysis [CHES 2009]
Lejla Batina, Benedikt Gierlichs, Kerstin Lemke-Rust

差分クラスタ解析という新規のサイドチャネル攻撃を提案した。これは衝突攻撃と DPA を組み合わせたもので、クラスタ解析で内部衝突を検知する。この手法は従来より一般的な漏洩を捉えるもので、アルゴリズムとしての衝突にも実装に依存した衝突に適用でき、本質的に多変数に対応している。適用範囲は広く、電力消費モデルの有無によらず、漏洩が単ビットでもマルチビットでも利用できる。この手法は実際に、AVR マイクロコントローラ上に実装した DES と AES の HW モジュールという2種類のプラットフォームで有効性を確認した。著者らの知る限り、この攻撃は高度に並列化されたプラットフォーム上に対する内部衝突攻撃としては初めてのものである。

Known-Plaintext-Only Attack on RSA-CRT with Mrontgomery Multiplication [CHES 2009]
Martin Hlava'c

この論文はモンゴメリべき乗法を利用した RSA-CRT に対する新しいサイドチャネル攻撃を提案するもので、既知平文に対するべき乗演算における最後の減算での漏洩情報を使って Hidden Number Problem(HNP)の方程式を立て、解くことによって、RSA のモジュラスの素因数分解を行う。既存の攻撃では選択平文が必要だったのに対し、既知平文で良い点に提案法の優位性がある。既存の攻撃法では電子パスポートで利用されている能動認証(AA)の安全性は破れなかったが、提案法では破れる。その際に必要なのは、7000 回の測定から選んだ 150 波形で、これらを使って立てた HNP を解くことで攻撃できる。一旦、AA で使われる秘密鍵が入手できると、RFID の全機能が再現できる。

A New Side-Channel Attack on RSA Prime Generation [CHES 2009]
Thomas Finke, Max Gebhardt, Werner Schindler

RSA 暗号における鍵生成の直接的な(straightforward)実装に対するサイドチャネル攻撃を提案し、解析した。この攻撃法では、個々の素数候補に対する試しの割り算の回数を求めるための電力情報を利用する。この攻撃の有効性は実験で確認され、対策法も提示提案された。現実的なパラメータ設定での攻撃成功確率は、10-15%である。

1.10.2. CHES 2009 の発表(2 日目)

An Efficient Method for Random Delay Generation in Embedded Software [CHES 2009]
Jean-Se'bastien Coron, Ilya Kizhvatov

ソフトウェア実装におけるサイドチャネル攻撃対策として、ランダムな遅延を入れる方法があり、坑道(pit)型分布を利用したBernoit-Tunstall 法が知られている。本論文では、矩形分布の平均値をランダムに動かす不動平均値法(Floating Mean)を提案し、CPA で鍵を推定するための波形数が Bernoit-Tunball の 6 倍必要となり、有効性が実証された。

Higher-order Masking and Shuffling for Software Implementations of Block Ciphers [CHES 2009]
Matthieu Rivain, Emmanuel Prouff, Julien Doget

ソフトウェア実装に対するDPA 対策とmaskingとshuffling(実行順序の入れ替え)の2つが主に用いられ、最近の研究では両方を組み合わせて使うことを提案している。しかしながら、masking に対しては高次(higher-order)DPA、shuffling に対しては積算型(Integrated) DPA が有効であり、両者を組み合わせることで、masking と shuffling を組み合わせた対策も破れる。本論文では、高次 masking と shuffling を組み合わせることによって、大幅に攻撃耐性が向上することを示した。

A Design Methodology for a DPA-Resistant Cryptographic LSI with RSL Techniques [CHES 2009]
Minoru Saeki, Daisuke Suzuki, Koichi Shimizu, Akashi Satoh

CMOS 標準セル上に暗号を実装した暗号モジュールの有効なDPA 対策として、RSL(Random Switching Logic)が提案されている。RSL で利用される独自の RSL-gate では、ランダムなマスクとグリッチの抑制が必要となる。本論文では標準セル・ライブラリによる一般的な論理ゲートを使って、同様の効果を実現する"pseudo RSL"を提案した。この有効性を検証するため 130-nm CMOS 標準セル・ライブラリで実装した。同じ条件で実装した既存の DPA 対策であるWDDL ではゲート数が 3 倍、速度が 1/4 になったのに対し、pseudo RSL では各々、2 倍、1/2 であり、実装性で優った。また、DPA 耐性にも優れていた。ただし、論文採録後、pseudo RSL を実装したものが、1 ビット DPA で攻撃可能であることが分かり、その原因が遅延に関する条件が満足されていないことが分かった。遅延に関する条件に合わせた修正は実施中。

A Design Flow and Evaluation Framework for DPA-resistant Instruction Set Extensions [CHES 2009]
Francesco Regazzoni, Alessandro Cevrero, Franc,ois-Xavier Standaert, Stephane Badel, Theo Kluter, Philip Brisk, Yusuf Leblebici, Paolo Ienne

CMOS における電力解析対策として、防御されたロジック様式(style)が提案されているが、サイズと電力消費量が非常に大きくなるので、補足的にしか使われない。本論文では、防御されたロジックによって、安全性と実装性能の両方を持った専用命令セットを備えたプロセッサを増やすことを提案し、その設計のために合成を自動化する標準の CAD ツールをベースに開発されたデザイン・フローについて述べた。軽量ブロック暗号 PRESENT にデザイン・フローを適用した例が紹介されたが、一般のアルゴリズムに適用可能である。

Based on Karatsuba-Ofman Multipliers [CHES 2009]
Jean-Luc Beuchat, Je're'mie Detrey, Nicolas Estibals, Eiji Okamoto, Francisco Rodri'guez-Henri'quez

標数 3 の supersingular 楕円曲線上の Tate ペアリングの計算を並列で高速化するためのデザインを開発した。Miller's loop はパイプライン化した Karatsuba-Ofman 乗算を利用した新しい HW 実装が提案されている。改良した Tate ペアリングのアルゴリズムでも最終の指数計算が必要となるが、これはコプロセッサで処理する。Xilinx FPGA で実装したところ、それまでに公開されたコプロセッサと比べ、計算時間とサイズ・時間トレードオフの両方で優位な結果が得られた。

Faster Fp-arithmetic for Cryptographic Pairings on Barreto-Naehrig Curves [CHES 2009]
Junfeng Fan, Frederik Vercauteren, Ingrid Verbauwhede

Barreto-Naehrig (BN)曲線での F_p 演算を高速化するため、F_p 乗算がより効率的になるように曲線を使ったアルゴリズムを提案した。提案アルゴリズムでは、Montgomery reduction と準メルセンヌ数を使った coefficient reduction を組み合わせて利用している。このアルゴリズムによるペアリング計算は、BN 曲線上だと現状のハードウェア環境で 5.4 倍高速になった。このアルゴリズムをハードウェア実装したところ、周波数 204MHz で 256 ビット BN 曲線上での ate ペアリングと R-ate ペアリングの計算に各々、4.22ms、2.91ms 掛かった。

Designing an ASIP for Cryptographic Pairings over Barreto-Naehrig Curves [CHES 2009]

David Kammler, Diandian Zhang, Peter Schwabe, Hanno Scharwaechter, Markus Langenberg, Dominik Auras, Gerd Ascheid, Rudolf Mathar

Barreto-Naehrig (BN)曲線での多様なペアリング計算に対応した、ASIP(アプリケーションに特化した命令セットプロセッサ)の設計空間(design-space)探索についての報告だった。130nm の標準セル・ライブラリで実装したところ、動作周波数 338MHz て。256 ビット BN 曲線上の Optimal-Ate ペアリング計算が 15.8ms だった。

KATAN & KTANTAN – A Family of Small and Efficient Hardware-Oriented Block Ciphers [CHES 2009]

Christophe De Cannie`re, Orr Dunkelman, Miroslav Knezevic'

KATAN と KTANTAN はハードウェア向けの軽量暗号であり、線形フィードバックシフトレジスタと AND と XOR で構成されている。ブロック長はともに3種類: 32, 48, 64 ビットが利用できが、KTANTAN では鍵がハードウェア的に固定され、鍵の変更はできない。ハードウェア実装した結果、性能は次の通りとなった。

・KTANTAN32 は 462GE で 12.5kbs(100MHz)
・RFID 用に推奨の KTANTAN48 は 588GE で 18.8kbs(100MHz)
・KTANTAN64 は 1054GE で 25.1kbs(100MHz)

Runtime Programmable and Parallel ECC Coprocessor Architecture: Tradeoffs between Area, Speed and Security [CHES 2009]

Xu Guo, Junfeng Fan, Patrick Schaumont, Ingrid Verbauwhede

楕円曲線暗号(ECC)に対しては多様なサイドチャネル攻撃と故障利用攻撃が有効であることが知られている。本論文では、安全性、実装性能、コストのトレードオフが調整でき、スケーラブルでプログラム可能である汎用の ECC 用コプロセッサのアーキテクチャを提案した。

Elliptic Curve Point Scalar Multiplication Combining Yao's Algorithm and Double Bases [CHES 2009]

Nicolas Me'loni, M. Anwar Hasan

楕円曲線上の点スカラー倍算のための二重基底数(double base number)システムの利用法の改良による効率化を試みる。Yao のアルゴリズムの修正版を使い、広く使われている二重基底鎖表現を一般化する。具体的には、整数 k を $\Sigma \hat{}_{n_i=1} 2^{b_i} 3^{t_i}$ で、b_i と t_i が単調減少なのに対し、提案方式では両方の最大値だけを与える。そして、異なる基底で最適パラメータを取ったときの効率を評価する。特にここでは整数の binary/Zecknedorf 表現の面白い結果を与える初めて与えた。最後に、多様な曲線の形と最近の点加算公式の速度向上を含んだ、現状の方法と提案法との分かりやすい比較を行う。

1.10.3. CHES 2009 の発表(3 日目)

The Frequency Injection Attack on Ring-Oscillator-Based True Random Number Generators [CHES 2009]
A. Theodore Markettos, Simon W. Moore

リング振動子を使った物理乱数生成器に対し、適切な周波数の波形を注入することにより、生成される乱数のエントロピーを減少させる攻撃法を考案した。この攻撃により、物理乱数生成器を使った安全なマイコンが作る鍵空間を 2^{64} から 3300 に収縮させ、2004 EMV payment card を攻撃することに成功した。EMV 支払システムに対する攻撃は、13 回の試行で 32 ビットの乱数を推定できた。

Low-Overhead Implementation of a Soft-Decision Helper Data Algorithm for SRAM PUFs [CHES 2009]
Roel Maes, Pim Tuyls, Ingrid Verbauwhede

PUF(物理的に複製不能な機能)では、固有のサブミクロンの構造から秘密鍵の生成されるが、実際に利用する際は、出力の曖昧さに対処するため HDA(補助データアルゴリズム)が必要になる。PUF と HDA の組み合わせは、不揮発性メモリに保存された秘密鍵よりもオーバーヘッドが小さい必要がある。本論文では、soft-decision information を使った最初の HDA を提案し、以前の提案よりもリソースが 44.8%小さいを設計した。この HDA はエントロピーの損失が小さいため、PUF のサイズを 58.4%にまで削減できた。

CDs Have Fingerprints Too [CHES 2009]
Ghaith Hammouri, Aykutlu Dana, Berk Sunar

CD に固有の fingerprint を作る方法を提案した。fingerprint は、CD 製造において異なる lands や pits を利用する。有効性の確認のため、100 枚の CD に対してどのように固有の fingerprint が付けられるか解析した。

Trojan Side-Channels: Lightweight Hardware Trojans through Side-Channel Engineering [CHES 2009]
Lang Lin, Markus Kasper, Tim Gu¨neysu, Christof Paar, Wayne Burleson

最近の半導体製造では設計と製造の分業が進み、信頼性の低い製造業者による半導体を使用するリスクが高まっている。本論文では、意図的にサイドチャネル情報を漏洩させるハードウェアによるトロイの木馬を提案し、トロイの木馬によるサイドチャネル(TSC)の2種類の小型実装法を示し、FPGA で有効性を検証した。その結果、軽量な TSC は通常の検出方法では発見が困難であることが確認できた。

MERO: A Statistical Approach for Hardware Trojan Detection [CHES 2009]
Rajat Subhra Chakraborty, Francis Wolff, Somnath Paul, Christos Papachristou, Swarup Bhunia

集積回路を安心して使うためには、ハードウェアによるトロイの木馬を低コストで検出する方法が必要である。しかし、製造後の工程ではハードウェアのトロイの木馬検出には対応していない。本論文では、内部ノードにおいてまれな論理条件を多重に起こす試験パターン生成方法を提案する。この方法により、ハードウェアによるトロイの木馬を検出するために必要なテストベクタの数を劇的に減らすことが出来る。ISCAS のベンチマークでは、ランダムパターンを使用した場合と同等か優る検出率を、85%少ないパターンで実現した。

On Tamper-Resistance from a Theoretical Viewpoint [CHES 2009]
Paulo Mateus, Serge Vaudenay

耐タンパー(tamper resistant)な装置は強力であり、アプリケーションでより高い安全性を実現するのに有効である。本論文では、耐タンパー装置を普及しているプライバシー保護機構を破るという悪意のある

使い方に利用する可能性について検討する。
プログラム可能な安全なハードウェアを定式化するため、trusted agent の理論モデルを提案する。このモデルにより、tamper-proof 装置を使わないプロトコルでは、悪意のある認証者が trusted agent を使えるとき、否認不可は出来ないことを示す。否認不可能力は、強い鍵登録モデルによって復活できるが、鍵供託(key escrow)というコストを伴なう。応用として、否認不可署名における不可視性を破ったり、電子投票の票を売ったり、グループ／リング署名の匿名性を破ったりする方法を示す。最後に計算機器に境界を設ける能力によって、フル制御や個人情報の拡散を防ぐことが可能になることを示す。これは機器にシールをすることは、ある意味でプライバシーと両立しないことを意味する。

Mutual Information Analysis: How, When and Why? [CHES 2009]
Nicolas Veyrat-Charvillon, Franc,ois-Xavier Standaert

相互情報量解析(MIA)は CHES 2008 で提案された一般的なサイドチャネル攻撃用の識別子(distinguisher)である。本論文の MIA の実用に関する貢献は次の3つである。最初に強調したのは、MIA の原理が他の統計的攻撃法を含むツールボックスと見なせることである。この発想により、オリジナルの攻撃法の興味深い代案を導入する。次に、MIA が Pearson の相関係数を使った古典的な攻撃法より少ない測定データで鍵を正しく推定できる状況について議論する。最後に、ACNS 2009 で Prouff-Rivain が提案した相互情報量を使った攻撃法との関連性と相違について検討する。MIA が2つの(情報)漏洩デバイスが比較できるための十分条件は、攻撃者が使う離散モデルが物理的漏洩と完全に対応していることである。

Fault Attacks on RSA Signatures with Partially Unknown Messages [CHES 2009]
Jean-Se'bastien Coron, Antoine Joux, Ilya Kizhvatov, David Naccache, Pascal Paillier

1990 年代の終りに Boneh-DeMillo-Lipton は、CRT-RSA のハードウェア実装に対する故障利用攻撃を提案した。これらの攻撃では、パディングが決定論的であるとき、署名者の法を素因数分解することができる。しかし、これらの攻撃はメッセージが部分的に分からないときには適用できない。例えば、メッセージがある程度ランダムな誤りを含み、それらは正しい署名が検証された時だけ訂正されるようなときである。本論文では CRT-RSA に対する故障利用攻撃を拡張し、メッセージが部分的に分からない場合に広く適用できるようにした。提案する攻撃法では、多変数多項式の小さな解を見つけるための Coppersmith アルゴリズムを利用する。提案攻撃法は、国際規格 ISO/IEC 9796-2 に記載された署名法をランダム化したものに対する攻撃に成功し、署名とメッセージ・ダイジェストに 160 ヒットずつ誤りがあったとしても、2048 ビットの法を 1 分間以内で素因数分解できる。

Higher-order Masking and Shuffling for Software Implementations of Block Ciphers [CHES 2009]
Matthieu Rivain, Emmanuel Prouff, Julien Doget

ブロック暗号に対する差分型故障利用攻撃(DFA)は、通常最後の数段にだけを攻撃対象とする。のため、全段を防御する必要はないと考えられるが、安全性を損なうことを避けるために、最後の何段分を防御すれば良いか、慎重に決める必要がある。本論文では、防御を何段にするか決めるために、DES の中間段を対象に DFA を適用した。その結果、9,10,11,12 段の最後に DFA を適用して攻撃できたことが分かった。

1.11. SHARCS'09 の発表

1.11.1. SHARCS'09 の発表(1 日目)

3 Years of Evolution: Cryptanalysis with COPACOBANA [SHARCS'09]
Tim Güneysu, Gerd Pfeiffer, Christof Paar, and Manfred Schimmler

この論文はモンゴメリべき乗法を利用した RSA-CRT に対する新しいサイドチャネル攻撃を提案するもので、既知平文に対するべき乗演算における最後の減算での漏洩情報を使って Hidden Number Problem(HNP)の方程式を立て、解くことによって、RSA のモジュラスの素因数分解を行う。既存の攻撃では選択平文が必要だったのに対し、既知平文で良い点に提案法の優位性がある。既存の攻撃法では電子パスポートで利用されている能動認証(AA)の安全性は破れなかったが、提案法では破れる。その際に必要なのは、7000 回の測定から選んだ 150 波形で、これらを使って立てた HNP を解くことで攻撃できる。一旦、AA で使われる秘密鍵が入手できると、RFID の全機能が再現できる。

Sparse Boolean equations and circuit lattices [SHARCS'09]
Igor Semaev

連立ブール方程式は、各方程式が含む変数の個数が小さいとき、疎(sparce)と言う。この方程式系を解くことは、現代暗号の暗号解析において困難な問題となっている。一致アルゴリズム(Agreeing Algorithm)はこの問題を解くために設計された方法であるが、この論文ではアルゴリズムの数学的な記述が直接的に電気配線とスイッチに読み替えることが出来ることを示す。この方法の DES と Triple DES に対する適用について解析した結果、少なくとも理論的には、総当りによる高速鍵廃棄が COPACOBANA より速く実行できる結果となった。

Pollard Rho on the PlayStation 3 [SHARCS'09]
Joppe W. Bos, Marcelo E. Kaihara, and Peter L. Montgomery

素体上の離散対数問題(ECDLP)を解くための Pollard の ρ 法の PlayStation 3 を使った高効率実装について述べる。現在、標準的となっている 112 ビット素体上の ECDLP を解くのに必要な時間を見積もったところ、62.6 PS3 年となった。算術アルゴリズムは PS3 の SIMD アーキテクチャと計算ユニット用の豊かな命令セットに合わせて設計された。今回の実装は 112 ビット・モジュラスに特化したものだが、他の大きなモジュラスでも実装戦略のほとんどが利用可能である。

The Certicom Challenges ECC2-X [SHARCS'09]
Daniel V. Bailey, Brian Baldwin, Lejla Batina, Daniel J. Bernstein, Peter Birkner, Joppe W. Bos, Gauthier van Damme, Giacomo de Meulenaer, Junfeng Fan, Tim Gu¨neysu, Frank Gurkaynak, Thorsten Kleinjung, Tanja Lange, Nele Mentens, Christof Paar, Francesco Regazzoni, Peter Schwabe, Leif Uhsadel

Certicom challenges で出題されている標数 2 の拡大体 F_2^{131} と F_2^{163} 上の楕円離散対数問題を解くのに必要なコストを様々なプラットフォームで評価した。発表では Koblitz 曲線と非 Koblitz 曲線に対するステップ関数と識別点の選び方について詳しい説明があった。以前の Certicom Challenges で著者らは通常の PC 上での SW 実装だけを使ったが、今回は様々な ASIC, FPGA, CPU, Cell BroadbandEngine が使われた。有限体上での演算では、多項式表現と標準基底の両方を調べた。特に Koblitz 曲線の標準基底での challenges では、ASIC と FPGA による実装効率の高さが強く印象に残った。

1.11.2. SHARCS'09 の発表(2 日目)

FSBday: Implementing Wagner's Generalized Birthday Attack against the SHA-3 candidate FSB [SHARCS'09]
Daniel J. Bernstein, Tanja Lange, Ruben Niederhagen, Christiane Peters, and Peter Schwabe

FSB は SHA-3 の Round 1 候補のハッシュ関数であり、誤り訂正符号を使用した圧縮関数を持つ。
また、一般化誕生日攻撃とは、B ビット・ストリングのリストが 2^i-1 個あるとき、各リストから 1 個ずつストリングを選んで、それら全部の排他的論理和(XOR)が 0 となるようにすることである。
本論文では、FSB の設計者による縮小版である FSB_48 に対する一般化誕生日攻撃について詳細に記述する。これを 8GB の RAM と 700GB の HDD を持つ PC 8 台によるクラスターに実装した結果、約 19.5 日で一般化衝突を発見できた。

Cost analysis of hash collisions: will quantum computers make SHARCS obsolete? [SHARCS'09]
Daniel J. Bernstein

数体篩法のスケーラビリティは Shnor の量子アルゴリズムよりかなり劣るので、本格的な量子計算機が出来ると、素因数分解用専用ハードウェアは陳腐化する可能性が考えられる。本論文では量子計算機の性能について詳細に考察した。b ビットのハッシュ関数の衝突探索のコストは、Brassard-Hoyer-Tapp が提案した量子アルゴリズムを使えば $2^{b/2}$ から $2^{b/3}$ としばしば主張されている。そこで、Brassard らの量子アルゴリズムの具体的な実装形体を考察して計算コストを見積もったところ、楽観的に評価しても、Oorschot-Wiener の古典的衝突探索回路に劣る価格性能比にしかならないという結果が得られた。

Shortest Lattice Vector Enumeration on Graphics Cards [SHARCS'09]
Jens Hermans, Michael Schneider, Johannes Buchmann, Frederik Vercauteren, and Bart Preneel

格子基底縮約(lattice reduction)アルゴリズムが、並列化法 GUDA を使用した GPU である NVIDIA グラフィックカード上に実装が可能かどうか初めて解析した。GPU 上で高並列化する計算の有力候補として、BKZ 格子基底縮約アルゴリズムの計算フェーズを選び実装したところ、高い格子次元のとき計算時間を 50%以上削減できた。この結果は格子ベース暗号の安全性に対して影響を与える。

The Billion-Mulmod-Per-Second PC [SHARCS'09]
Daniel J. Bernstein, Hsueh-Chung Chen, Ming-Shing Chen, Chen-Mou Cheng, Chun-Hung Hsiao, Tanja Lange, Zong-Cing Lin, and Bo-Yin Yang

素因数分解のための楕円曲線法における最速記録を次のプラットフォーム上で達成した。
・GPU (NVIDIA GTX)
・x86 CPU with SSE2 (Intel Core 2 & AMD Phenom)
・Cell (PlayStation 3 & PowerXCell 8i)
この論文の特筆すべきことは、2000ドルの PC でどうやれば、192 ビットの剰余乗算を毎秒 100 万回以上実行できるか説明していることである。

Efficient FPGA Implementations of High-Dimensional Cube Testers on the Stream Cipher Grain-128 [SHARCS'09]
Jean-Philippe Aumasson, Itai Dinur, Luca Henzen, Willi Meier, and Adi Shamir

cube tester はストリーム暗号などの識別子(distinguisher)の設計に利用され、cube 攻撃と代数的性質の tester をベースにしている。本論文では、eSTREAM のポートフォリオに掲載されたストリーム暗号 Grain-v1 の変形版の1つである Grain-128 に対する cube tester の FPGA 実装について報告している。最良の結果は、Grain-128 の 237 段縮小版(フルスペックは 256 段)を 256*32 並列、2^{54} クロックで実行するものである。この結果から外挿すると、フルスペックの Grain-128 の識別に必要なクロック数は 2^{83} となり、

総当たり法の 2^{128} を下回る。

Cryptanalysis of KeeLoq with COPACOBANA [SHARCS'09]

Martin Novotny' and Timo Kasper

KeeLoq は自動車のドアのキーやガレージの開閉をリモート制御するシステム及びそこで使われるブロック暗号の名称である。KeeLoq の脆弱性はいくつか指摘されているが、本論文ではランダムな SEED を使って鍵を推定する方法を取り上げる。ランダムな SEED を使った総当たり攻撃は、普通の PC 1 台では能力不足であり、FPGA を使った暗号攻撃専用ハードウェア COPACOBANA を使った結果、32 ビットのシードでは 0.5 秒、48 ビットのシードでは 6 時間で鍵が求まった。この結果から外挿すると、KeeLoq のシード・サイズは COPACOBANA で 1011 日を要する 60 ビット以上であることが望ましい。ただし、この日数も COPACOBANA を多数利用することで縮めることが可能である。

1.12. Asiacrypt 2009 の発表

1.12.1. Asiacrypt 2009 の発表(1 日目)

Related-key Cryptanalysis of the Full AES-192 and AES-256 [Asiacrypt 2009]
Alex Biryukov and Dmitry Khovratovich

AES-256/192 のフルラウンドに対する関連鍵攻撃が発表された。ともに攻撃に必要な関連鍵は 4 個である。AES-256 では関連鍵ブーメラン攻撃が利用され、必要選択平文数・暗号化回数(計算量)ともに $2^{99.5}$、必要メモリは 2^{77}。AES-192 では関連鍵増幅型(amplified)ブーメラン攻撃が利用され、必要選択平文数 2^{123}、暗号化回数(計算量)2^{176}、必要メモリは 2^{152}。Crypto 2009 本セッションの発表では、AES-256 の関連鍵の一部しか特定できず、AES-192 はフルラウンドが解けていなかったが、今回の攻撃ではともに、4 個の関連鍵が全部求まる点が進歩している。今回の関連鍵攻撃には、最近開発されたハッシュ関数に対する攻撃テクニックと内部衝突が利用されており、今後の改良が注目される。

The Key-Dependent Attack on Block Ciphers [Asiacrypt 2009]
Xiaorui Sun and Xuejia Lai

ブロック暗号IDEAには、中間変数において、鍵に依存する偏った分布を持つ関係式が存在する。著者らは、このような鍵依存分布に着目し、追加段の拡大鍵推定と分布から導かれる鍵に関する制約式を使って全鍵ビットを推定する方法を鍵依存攻撃と名付けた。この攻撃法により、5.5 段縮小 IDEA が選択平文 2^{21} 個、暗号化 $2^{112.1}$ 回分の計算量で、6 段縮小 IDEA が選択平文 2^{49} 個、暗号化 $2^{112.1}$ 回分の計算量で攻撃可能だった。なお、IDEA のフルスペックは 8.5 段である。これらの結果は、従来研究の攻撃可能段数を伸ばしてはいないものの、解読効率は改善している。本攻撃法は IDEA に固有の性質(関係式)を利用しいるため、他の既存暗号に対して適用できる可能性は低い。ただし、新規にブロック暗号を設計する際は、同様の弱点が生じないよう留意する必要がある。

Cascade Encryption Revisited [Asiacrypt 2009]
Peter Gazi and Ueli Maurer

ブロック暗号の安全性低下への対策として、暗号化を繰り返し行うことにより安全性強化法がある。Rogaway と Shrimpton は Eurocrypt 2006 において、ゲーム理論を利用して、暗号化を 2 回繰り返しても安全性は大して向上せず、3 回繰り返すとによって安全性が大幅に改善することを示した。この発表では、Maurer のランダム系理論を拡張した識別不可能性に関するレンマを提案し、これを使って Bellare-Rogaway の証明戦略を理解しやすいように書き直した。その結果、より多くの段数での安全性が扱えるようになった。この結果を使うと、DES のように鍵長がブロック長より短い暗号では、暗号化を重ねることによって安全性がある一定の限界まで向上することが示せた。これは以前からの公開質問に対する部分的な回答となっている。

Quantum-Secure Coin-Flipping and Applications [Asiacrypt 2009]
Ivan Damgard and Carolin Lunemann

通常の古典論的(非量子論的)な暗号系における安全性証明を量子論に適用することは通常、困難である。この問題に対するアプローチとして、Watrous.J.は Siam Journal vol. 39.1(2009)において量子巻き戻しレンマ(Quantum Rewinding Lemma)を示し、それを使って、、グラフ同型のようなゼロ知識証明系における量子検証者の効率の良い量子シミュレータを構成した。この論文では Watrous のアイデアを応用し、量子的な攻撃者がいても古典的なコイン投げが安全であることを証明した。さらにこの証明の2つの応用を示した。一つは、コイン投げと非対話型ゼロ知識証明の組み合わせによる、非対話型ゼロ知識から対話型量子的ゼロ知識への簡単な変換である。もう一つは、Crypto 2009 で著者らが発表した量子プロトコルの安全性強化法への応用で、セットアップ時の仮定を必要としない実装法を可能にした。

On the Power of Two-Party Quantum Cryptography [Asiacrypt 2009]
Louis Salvail, Christian Schaffner and Miroslava Sotakova

2 パーティの古典的(非量子論的)プロトコルは実現不能であることが分かっており、量子論でそれらが可能になるかの研究が行われている。本論文では、正直なプレイヤから不正な利用者への情報漏洩を定量的に測る枠組みを与え、情報漏えい量(leakage)が個々のプロトコルに対し、プレイヤのプライバシの良い物差しになることを論じる。そして、正直なプレイヤが正しい結果を得られることを保証すると非自明なプロトコルでは必ず不正直なプレイヤに情報が漏洩することを示した。さらに、2人のプレイヤが TTP の助けを借りた場合の安全性を解析した結果、いかなるプリミティブでも安全性は改善しないことが明らかになった。以上の結果は、攻撃者が honest-but-curious であっても成立する。

Security Bounds for the Design of Code-based Cryptosystems [Asiacrypt 2009]
Matthieu Finiasz and Nicolas Sendrier

符号ベース暗号は、量子計算機完成以降(Post-Quantum)の数論ベース暗号の有望な代替の一つである。符号ベース暗号に対する効率的な攻撃法は少数であり、線形符号の復号アルゴリズムに基づいている。その中で主要なものは、Information Set Decoding (ISD)と Generalized Birthday Algorithm (GBA)である。これら2種類の攻撃法に対する攻撃コストを評価した研究は多いが、ほとんどが攻撃者の視点による上限を調べるもので、設計者の立場に立った評価は、Bernstein,D.J.らによる WCC 2009 での ISD に関する論文が唯一の例外だった。この論文では、設計者の立場に立った安全性評価用のツールを提供し、適切なパラメータを容易に選択することを可能にした。

Rebound Attack on the Full LANE Compression Function [Asiacrypt 2009]
Krystian Matusiewicz, Maria Naya-Plasencia, Ivica Nikoli?, Yu Sasaki and Martin Schlaffer

改良したリバウンド攻撃法を`SHA-3 公募の第 1 ラウンドで落ちたハッシュ関数候補 LANE に適用し、LANE-256 では圧縮関数 2^{96} 回の計算量と 2^{88} のメモリ、LANE-512 では圧縮関数 2^{224} 回の計算量と 2^{128} のメモリで、semi-free-start 衝突が見つけられることを示した。LANE は AES ベースのハッシュ関数で、圧縮関数には線形のメッセージ展開と 6 並列の処理(lanes)で構成されている。本論文のリバウンド攻撃では、疎な切詰差分経路を使うことでメッセージ展開と lanes の衝突を独立に解くことを可能にしている。さらに、並列の AES 状態の自由度を活用することで、入射バウンドを複数回起こすことに成功した。これらの攻撃技術の改良によって、フルスペックの LANE に対する semi-free-start 衝突発見攻撃が可能となった。

Rebound Distinguishers: Results on the Full Whirlpool Compression Function [Asiacrypt 2009]
Mario Lamberger, Florian Mendel, Christian Rechberger, Vincent Rijmen and Martin Schlaffer

Whirlpool は AES をベースとしたハッシュ関数で、AES の 4*4 のサブバイトを 8*8 に拡張した SPN 構造の圧縮関数を持つ。安全性と実装性能を高く評価され、2002 年に NESSIE の公募で推奨方式となり、2004 年に国際規格 ISO/IEC 10118-3 に採用された。本論文では、リバウンド攻撃をインバウンドを2重化することにより、攻撃可能段数を 2 段伸ばした。これにより、近衝突(near-collision)発見を 10 段中 9.5 段まで伸ばし、必要計算量は 2^{176} で、必要メモリ量は無視できる程度であった。さらに、計算量 2^{188} で圧縮関数に対する識別攻撃が可能となった。

MD5 is Weaker than Weak: Attacks on Concatenated Combiners [Asiacrypt 2009]
Florian Mendel, Christian Rechberger and Martin Schlaffer

異なるハッシュ関数の入力を共通とし、各々の出力の連接を出力とするハッシュ関数結合(hash function combiner)は、個々のハッシュ関数の安全性低下に対する対策として利用され、実際に MD5||SHA-1 の形の結合が SSL 3.0/TLS 1.0 と TLS 1.1 に採用されている。Joux,A.は Crypto 2004 においてハッシュ関数結合に対する攻撃法を示し、計算量が binrthday-bound を下回る攻撃法は可能かという問いを発し、それが今まで未解決の問題となっていた。この論文はこの問題に対する肯定的な回答を与えるもので、論文中で Type 3 と呼ばれる差分経路パターンに着目した衝突探索法を提案した。

The Intel AES Instructions Set and the SHA-3 Candidates [Asiacrypt 2009]
Ryad Benadjila, Olivier Billet, Shay Gueron and Matt Robshaw

Intel は 2010 に発表する CPU Westmere に AES の高速計算用命令セット AES New Instructions(AES-NI)を入れることを発表している。AES の構造をベースとする SHA-3 候補ハッシュ関数の提案者たちは、AES-NI によって自分たちの方式の実装性能が向上すると主張している。この論文では、AES-NI を使うことで、AES ベースの SHA-3 候補の実装性能がどの程度向上するか評価した結果を報告した。なお、Westmere プロセッサはまだ実際には利用できないので、既に広く利用されている Nehalem プロセッサを用いた emulation 法を開発し、実装性能を評価した。

Group Encryption: Non-Interactive Realization in the Standard Model [Asiacrypt 2009]
Julien Cathalo, Benoit Libert and Moti Yung

グループ暗号は Asiacrypt 2007 で A. Kiayias、M. Yung らが最初に提案したグループ署名の暗号版であり、メッセージの秘匿性と送信者の匿名性がともに CCA2 の安全性を持つ。ここで、送信者は特定の PKI グループに属する。Kiayias らの方式は、送信者が PKI グループに属することの証明に処理コストが大きい対話型証明が必要だった。この論文では、初めて非対話型証明のグループ暗号方式を実現した。今回の重要な構成要素は、新しい公開鍵証明方式であり、それは必要な対話を最小限に抑えている。

On Black-Box Constructions of Predicate Encryption from Trapdoor Permutations [Asiacrypt 2009]
Jonathan Katz and Arkady Yerukhimovich

predicate 暗号は、ID ベース暗号(IDE)、放送暗号、属性ベース暗号などを一般化したもので、authority がマスターの秘密鍵・秘密鍵ペアを作り、マスター秘密鍵でユーザ各人の秘密鍵を生成する。秘密鍵に対応する述語が暗号文の属性と対応したとき復号できる。predicate 暗号に関しては、例えば落とし戸置換といった一般的な構成要素をブラックボックスとして使った構成法が可能かという自然な質問が提起されていた。D. Boneh らは FOCS 2008 で IBE に限定した場合、ブラックボックス型の構成が不可能であるという否定的な結果を示した。この論文では、否定的と肯定的、両方の結果を導いている。否定的な結果は、述語と属性間の組み合わせに関する性質を導き、落とし戸置換を使ったブラックボックス構成が不可能であることを示した。この結果は Boneh らの結論の一般化である。肯定的な結果は、CPA 安全な暗号スキームに基づいた predicate 暗号の方式が可能となる条件を明らかにした。

Hierarchical Predicate Encryption for Inner-Products [Asiacrypt 2009]
Tatsuaki Okamoto and Katsuyuki Takashima

predicate 暗号は、ID ベース暗号(IDE)、隠れベクトル暗号(HVE)、属性ベース暗号(ABE)などを一般化したもので、秘密鍵に対応する述語が暗号文の属性と対応したとき復号できる。この論文では、新規の仮定に基づく標準モデルで安全性が保証できる、内積型の述語を使った階層型述語暗号(HPE)を初めて構成した。ここでの仮定は、非対話型であることと、攻撃者の質問数に上限があることである。提案された HPE で使われている独自技術は、線形空間上の双線形ペアリング群に基づいている。

Hedged Public-Key Encryption: How to Protect Against Bad Randomness [Asiacrypt 2009]
Mihir Bellare, Zvika Brakerski, Moni Naor, Thomas Ristenpart, Gil Segev, Hovav Shacham and Scott Yilek

公開鍵暗号における IND-CPA 安全性は、平文ごとに新鮮なランダム性を根拠としている。しかし、現実的には、平文はしばしばランダム性を欠く場合がある。この論文では、IND-CPA に代わる新しい安全性概念として、IND-CDA (Chosen Distribution Attack)を提案した。IND-CDA の具体例として、ランダムオラクル(RO)の仮定で、IND-CPA となる方式に最小限のソフトウェア改変を行うことで実用的な IND-CDA を実現する方法を示した。さらに、RO を仮定しないモデルで、損失の多い落とし戸関数(LTDFs)と決定論的暗号化の技術に基づく方式も構成した。

1.12.2. Asiacrypt 2009 の発表(2 日目)

Secure Two-Party Computation is Practical [Asiacrypt 2009]
Benny Pinkas, Thomas Schneider, Nigel P. Smart and Stephen C. Williams

多者計算 (secure multi-party computation) は暗号学において 20 年以上研究されている古い研究分野であるが, 最近まで純粋に理論的な分野と考えられてきた. 長い間, 汎用多者計算の実用的実装がほとんど利用できなかった為, 特定の応用に特化した最適化以外はあまり研究されて来なかった. しかし, 近年いくつかの実用的実装が利用可能となり, 汎用多者計算の最適化への関心が高まっている. 本論文では, semi-honest, covert, malicious の 3 つの攻撃者設定に関して, Yao の garbled 回路を使った汎用二者計算のいろいろな最適化を理論的および実験的に解析した. そして, 工学的に興味ある十分大きい回路の例として, AES-128 (平文を持つ者と鍵を持つ者が協力して, それぞれ鍵と平文を学習することなく,平文を持つ者が AES-128 の暗号文を得る回路) を実装し, 汎用二者計算の実用性を示した.

Secure Multi-party Computation Minimizing Online Rounds [Asiacrypt 2009]
Seung Geol Choi, Ariel Elbaz, Tal Malkin and Moti Yung

多者計算は入力を秘匿しつつ任意の関数を計算する重要な汎用手続きである. 本論文では汎用結合可能多者計算の事前計算による対話計算量の削減について研究している. 回路のゲート数に関する限界 k が既知であること以外は具体的な回路および入力に依存しない如何なる多項式時間事前計算も可能とする. この問題を研究するために, 先ず, [FH96, JJ00, CDN01, DN03] に示された多者秘匿データ計算 (multi-party computation on encrypted data, MP-CED) のモデルの定義を行った. このモデルでは, 参加者は先ず事前計算段階で閾値公開鍵を確立し, その後共有された公開鍵で暗号化された秘匿データが暴露される. 次に参加者は合意した計算回路を得て暗号化されたデータに関する回路を評価する. 本論文では, このモデルで対話効率の良い二つのプロトコルを提案する.

- 第一のプロトコルは事前計算段階で k 個の garbled gate を生成し, (対話時には) 2 ラウンドしか必要としない.
- 第二のプロトコルは事前計算段階でサイズ O(k log k) の garbled 汎用回路を生成し, (対話時に) 1 ラウンド(即ち自明な下界)しか必要とせず, 従って非同期実行が可能である.

どちらのプロトコルも任意の数の参加者を制御できる動的および静的攻撃者に対して安全である. 攻撃者が買収可能な参加者が半数以下の時, 攻撃者はプロトコルを強制終了させる事が出来ない. MP-CED モデルは汎用多者計算と強い関連があり, 実際, 互いに帰着可能である. 上記第一(第二)のプロトコルは 3 ラウンド(2 ラウンド)の敵性非適応的攻撃者に対して安全な(事前計算付き)汎用結合可能多者計算を自然に与える.

Improved Non-Committing Encryption with Applications to Adaptively Secure Protocols [Asiacrypt 2009]
Seung Geol Choi, Dana Dachman-Soled, Tal Malkin and Hoeteck Wee

本論文では non-committing encryption の新しい構成法を提案する. 従来の Canetti ら(STOC'96)および Damgard ら(Crypto 2000)の構成法と違って, 本構成法は以下の全ての性質を達成した.

- 最適対話計算量.
- 弱い仮定.
- 効率の改善.

結果として, 従来は CDH 仮定および RSA 仮定の元でしか実現できなかった non-committing 公開鍵暗号を、初めて素因数分解仮定および最悪ケース格子仮定の下で実現した. この結果を多者計算の既知の結果と組み合わせると, 従来より弱い仮定の下で, 任意の数の参加者を適応的買収できる敵性攻撃者に対して安全な多者計算のプロトコルを得る. 特に, 共通参照文字列ありの汎用結合可能設

定および単独設定の両方で素因数分解の困難性に基づく適応的安全な多者計算プロトコルを初めて得た.

Non-Malleable Statistically Hiding Commitment from Any One-Way Function [Asiacrypt 2009]
Zongyang Zhang, Zhenfu Cao, Ning Ding and Rong Ma

本論文では一方向関数の存在に基づく頑強統計的秘匿コミットメントの構成法を与える. 本構成法では近年 Haitner らによって提案された統計的秘匿コミットメント方式と特殊健全証拠識別不能証明を使用する. 安全性の証明は Dolev, Dwork, Naor のメッセージスケジューリング技法に依存しており, ブラックボックス技法しか必要としない.

Proofs of Storage from Homomorphic Identification Protocols [Asiacrypt 2009]
Giuseppe Ateniese, Seny Kamara and Jonathan Katz

記憶証明 (Proofs of Storage, PoS) とはサーバー (server) がファイルを忠実に保存している事をクライアント (client) が検証できる対話プロトコルである. 任意の準同型線形認証メッセージ (homomorphic linear authenticators, HLA) から記憶証明が構成出来る事が知られている. 準同型線形認証メッセージとは、大雑把に言って、複数の文書の任意の線形結合の'タグ'(認証メッセージ) を各文書の'タグ'の準同型結合により得ることの出来る署名/メッセージ認証のことである. 本論文ではある準同型性を満たす相手認証 (identification) プロトコルから公開鍵準同型線形認証メッセージを得るフレームワークを与える. そして任意の公開鍵準同型線形認証メッセージを通信量がファイルの長さと独立で無制限回の検証が可能な公開検証可能記憶証明に変換する方法を示す. Shoup の相手認証プロトコルの変種にこの変換を適用し、初めて素因数分解に基づく無制限回使用可能な記憶証明を (ランダムオラクルモデルで)得た.

Simple Adaptive Oblivious Transfer Without Random Oracle [Asiacrypt 2009]
Kaoru Kurosawa and Ryo Nojima

適応的紛失通信とは, 送信者が信頼できる第三者(TTP)に $M_1,\cdots,M_n$ を送信し, 受信者が TTP から $i = 1,2,\cdots,k$ に対して適応的に $M_{\sigma(i)}$ を受信するような理想世界をシミュレートする二者プロトコルである. 本論文では最初のペアリング無し 完全シミュレーション可能適応的紛失通信を示す. 本方式は, 動的仮定に依存しない初めての完全シミュレーション可能な方式でもある.

1.12.3. Asiacrypt 2009 の発表(3 日目)

Improved generic algorithms for 3-collisions [Asiacrypt 2009]
Antoine Joux and Stefan Lucks

関数の r-衝突とは出力が等しい r 個の異なる入力の組のことである．要素数 N の有限集合上ランダム写像の r-衝突発見には、逐次機械上で少なくともおよそ N^{(r-1)/r} の時間計算量を要する．r = 2 は良く研究されており，無視しうるサイズの領域計算量で効率よく並列化出来るアルゴリズムが知られている．本論文では r >= 3 の時，領域効率が良く並列化可能なアルゴリズムを研究している．こうした多衝突発見アルゴリズムは、ハッシュ関数の攻撃ツールとしての応用が知られており，本結果を利用して AURORA-512 の攻撃に必要な記憶領域の削減が可能とのこと．この論文は本会議の最優秀論文賞に選ばれた．主な結果は以下の通り．

1. $\alpha <= 1/3$ なるパラメタ α に対し,およそ N^{α} 記憶領域 $N^{1-\alpha}$ 時間の 3-衝突逐次アルゴリズム．特に $N^{1/3}$ 記憶領域が利用可能のとき $N^{2/3}$ 時間で 3-衝突を発見できる．
2. N^{1/3}演算器，毎演算器定数記憶領域，$N^{1/3}$ 時間の 1．の並列化．
3. 2．の r>=3 への一般化: s <= (r-2)/r なるパラメタ s に対し，N^{s} 演算器，毎演算器 $N^{((r-2)/r)-s}$ 記憶領域，$N^{((r-1)/r)-s}$ 時間の r-衝突アルゴリズム．

A Modular Design for Hash Functions: Towards Making the Mix-Compress-Mix Approach Practical [Asiacrypt 2009]
Anja Lehmann and Stefano Tessaro

本論文では，安全性のモジュール性および故障耐性なる概念を備えた暗号学的ハッシュ関数の構成法の提唱を行っている．単純なハッシュ関数 H および他の基本関数(例えばブロック暗号) F から，より完全なハッシュ関数 $C^{H,F}$ を構成するとする．そして $C^{H,F}$ の衝突困難は H のみに依存し，ランダムオラクルとの強識別不可能性は F の理想性のみに従う，といった構成を考察している．Ristenpart と Shrimpton (ASIACRYPT 2007) の MCM (Mix-Compress-Mix)法はハッシュ関数 H を 2 つの単射混合段の間に挟む方式で，こうした設計の最初の試みと考えることが出来る．しかし、この提案の具体例は大変に非効率的であり，出力されるハッシュ値は H よりも大きくなってしまう．本論文では，高速で出力長の短い効率的なモジュール化ハッシュ関数 (modular hash function) を初めて実現した．この方法の肝は、非常に弱い仮定にしか依存しない新しいブロック暗号に基づく MCM 手法の混合段の設計である: 最初の混合段は (基礎となる暗号が理想的であること以外) 如何なる計算量仮定にも依存しない．二番目の混合段は落し戸の無い一方向置換であることのみが必要とされる．それは単射ランダムオラクルの構成に必要な最小の仮定である事が証明できる．

How to Confirm Cryptosystems Security: The Original Merkle-Damgard is Still Alive! [Asiacrypt 2009]
Yusuke Naito, Kazuki Yoneyama, Lei Wang and Kazuo Ohta

Coron ら (Crypto 2005) は extension 攻撃の概念を示す事により、固定入力長ランダムオラクルを使った Merkle-Damgard ハッシュ関数(MDHF)がランダムオラクル RO と強識別不可能ではない事を示した．この結果は RO モデルでは安全であるが MDHF の下では安全でない暗号系が存在する事を示している．従って，MDHF の下で暗号系の安全性を証明する方法論を確立したい．本論文では，以下の手順に従って，暗号系の安全性証明を行う事を考える．

1. extension 攻撃を実現するのに必要な情報を漏らす RO の変種 RO~ を見つける．
2. MDHF が RO~ と強識別不可能である事を証明する．
3. 暗号系の安全性を RO~ モデルで証明する．

強識別不可能性のフレームワークより，RO~ 下の暗号系の安全性は MDHF 下の安全性でもある．従って，本論文では，まず RO より弱い RO~ を見つける事に専念する．そして初めに extension 攻撃が可能となる十分な情報を漏洩する traceable random oracle(TRO) を提案する．TRO を使って OAEP およびその変種の安全性を容易に確認できる．しかし，TRO を使って安全性が確認出来ない実用的

な暗号系がいくつか存在する（例えば RSA-KEM）．これは TRO が extension 攻撃と関係ない情報まで漏洩するからである．従って，次に extension 攻撃に必要な情報のみを漏洩する他の RO~，即ち extension attack simulatable random oracle (ERO) を提案する．ERO は MDHF に基づく暗号系の安全性を確認するのに必要十分であり，MDHF に基づく任意の暗号系の安全性は ERO モデルの下での安全性と等価である．本論文では ERO モデルの下で RSA-KEM の安全性を証明した．

On the Analysis of Cryptographic Assumptions in the Generic Ring Model [Asiacrypt 2009]
Tibor Jager and Jorg Schwenk

汎用環モデル（generic ring model）とは，暗号系で使用する環の代数構造を抽象化した攻撃環境モデルであり，素因数分解に基づく暗号系を考えるとき，攻撃者は法 N の剰余環の完全な代数構造を利用できるが，要素の表現から得られる情報は一切利用できない．Aggarwal ら（Eurocrypt 2009）は汎用環モデルで RSA の解読と素因数分解の等価性を証明した．この結果から，

『汎用環モデルでの証明を如何に解釈すべきか？』

という自然な疑問が生ずる．汎用モデルでの困難性が，計算の一般モデルでの困難性の証拠を与えると考えたくなるかも知れない．しかし,そう考えることは妥当であろうか？本論文では，ヤコビ記号の計算が汎用環モデルでは素因数分解と等価である事を証明する．簡単で効率的なヤコビ記号計算の非汎用アルゴリズムが存在するので，汎用モデルは計算問題の困難性への如何なる証拠も与えてない事となる．この否定的な結果にもかかわらず，本論文では汎用環モデルでの証明が何故重要であるかを議論し，平方剰余問題と部分群決定問題が汎用的に素因数分解と等価である事を示す．

Zero Knowledge in the Random Oracle Model, Revisited [Asiacrypt 2009]
Hoeteck Wee

Bellare-Rogaway (CCS'93) および Pass (Crypto 2003) によるランダムオラクルモデルにおける零知識の従来の定式化を再訪し，両方の定式化を含む零知識の階層を示す．ランダムオラクルのプログラム可能性に関する階層は Nielsen (Crypto 2002) により既に示されているが，本論文ではそれより微細な階層を示した．

- Bellare-Rogaway の定式化と弱い定式化の間で 3 つのランダムオラクルの変種，NPRO，EPRO，FPRO を定義し，EPRO と FPRO に基づく零知識の分離(separation)を示した．
- どの定式化に従った零知識(証明)も，逐次合成の下で保存しない事を示した．逐次合成に関して零知識性が閉じるよう，攻撃者がランダムオラクルに依存した補助入力を受け取れる強い定義を導入した．また，強い定義を満たす NP に対するラウンド数最適のプロトコルを示した．
- 知識証明に関しても研究し，オラクルに依存する補助入力を考慮したランダムオラクルモデルの下での知識証明の新しい定義を導入した．従来の定義で知識の零知識証明を達成するには 1 ラウンドの対話で十分であったが，この定義の下では 2 ラウンドの対話が必要十分である事を示した．
- 回路難読化（circuit obfuscation）に関しても研究し，ランダムオラクルモデルでの回路難読化の階層を示した．EPRO モデルでは零知識に対して非自明な構成があるのに回路難読化に対しては存在しない事を示した．

A Framework for Universally Composable Non-Committing Blind Signatures [Asiacrypt 2009]
Masayuki Abe and Miyako Ohkubo

一般的なブラインド署名では，署名者がブラインド署名を発行した後，署名依頼者が都合の良い文書をオープン出来ないよう，署名時に文書がコミットされる必要がある．安全な汎用結合可能(UC)コミットメントはプレインモデルでは実現できないので、UC ブラインド署名も(安全に)実現するのは不可能である．本論文では，たとえ非コミットブラインド署名であっても，プレインモデルでは(UC 安全に)実現するのは不可能であることを示す．そして，共通参照文字列(CRS)モデルでの適応的安全な UC 非コミットブラインド署名を，等価なスタンドアローンの安全性概念を示すことにより特徴づける．また，Fischlin のブラインド署名方式に基づく汎用構成法を示す．

Cryptanalysis of the Square Cryptosystems [Asiacrypt 2009]

Olivier Billet and Gilles Macario-Rat (Yannick Seurin gives the talk)

HFE および SFLASH が暗号解析されて以来，UOV および HFE-- 以外で重要な多変数多項式暗号系は残っていなかったが，最近二次内部変換 (quadratic internal transformation) に基づく高効率多変数多項式暗号系に関する2つの提案がなされた: 第一の提案は square-vinegar と呼ばれる署名系であり，第二の提案は square と呼ばれる暗号系で CT-RSA 2009 にて導入された．本論文では square-vinegar 署名系と square 暗号系の両方の完全解読を提案する．これらの暗号系の作者により提案された実用パラメタに対して，本攻撃の計算量はおよそ 2^{35} 演算である．本論文には Magma 計算代数システムで実装した攻撃の全ステップが記述してあり，実験的に評価することが出来る．

Factoring pq^2 with Quadratic Forms: Nice Cryptanalyses [Asiacrypt 2009]

Guilhem Castagnos, Antoine Joux, Fabien Laguillaumie and Phong Q. Nguyen

本論文では N=pq^2 型の整数を素因数分解する二元二次形式に基づく新しいアルゴリズムを提案している．一般に，その実行時間は指数時間となるが，特殊な(算術的)ヒントが利用出来るときは多項式となる. 90 年代末期に提案された二次体に基づく公開鍵暗号，いわゆる NICE ファミリーに対する攻撃がまさにこの場合に相当する．この暗号系には二次体の虚実に従って二種類の版が存在する．本論文のアルゴリズムは NICE のどちらの版に対しても機能し，多項式時間一般鍵回復攻撃を実現する．Castagnos と Laguillaumie は最近 虚-NICE の完全解読を与えたが，この攻撃は 実-NICE には適用できなかった．本論文のアルゴリズムは CL 攻撃と同様に 虚-NICE の公開鍵をヒントとして効率の良い素因数分解を与えるが，実-NICE の場合でも，二次体 $Q(\sqrt{p})$の単数規準が著しく小さいという知識を使って効率の良い素因数分解を与える事が出来る．一般的な $N=pq^2$ 型の素因数分解ではこのアルゴリズムは指数時間で，一般化(ESIGN の場合など)については未解決とのこと．

Attacking Power Generators Using Unravelled Linearization: When Do We Output Too Much? [Asiacrypt 2009]

Mathias Herrmann and Alexander May

本論文では，乱数種 $s_0 \in Z_N$ に対し各反復である特定量のビットを出力する反復冪擬似乱数生成器 (iterated power generators) $s_i = s_{i-1}^e \bmod N$ の暗号解析を行った．毎反復 $(1-1/e) \log N$ 上位ビットの出力により全擬似乱数列の効率的な回復が可能である事を，発見的方法によって示す．特に，このことは Blum-Blum-Shub 擬似乱数生成器は毎反復半分未満のビット，e=3 の RSA 擬似乱数生成器は毎反復 1/3 未満のビットの出力で利用すべきである事を意味する．本論文では，格子に基づく(多項式方程式の)線形化と，多項式方程式の小さい根を求める Coppersmith の方法を組みあわせた，unravelled linearization なる技法を提案し，これに基づき上記の限界を得た．

Security Notions and Generic Constructions for Client Puzzles [Asiacrypt 2009]

Liqun Chen, Paul Morrissey, Nigel P. Smart and Bogdan Warinschi

本論文では，解を得るのに資源(演算処理装置のサイクル,記憶領域，あるいはその両方) を必要とする適度に難しい計算量的問題を計算量的パズル (computational puzzle) と呼ぶ．パズルはセキュリティの分野で様々な応用が見付かっている．本論文では クライアントパズル (client puzzle，サービス拒否(DoS)攻撃への防御として利用されるパズル) を研究し，クライアントパズルの安全性の形式的モデルを与えている．そして，クライアントパズルが提供すべき入出力仕様を分類し，パズルに対する 2 つの安全性概念 (puzzle-unforgeability と puzzle-difficulty) を与えた．二つの性質のうちどちらか一方を破ると即サービス拒否攻撃が成功する.本論文では従来提案されたパズルの構成に対する攻撃を示し，この点を明らかにする．また，この安全性定義に適合するクライアントパズルの汎用的な構成法を示す．

Foundations of Non-Malleable Hash and One-Way Functions [Asiacrypt 2009]

Alexandra Boldyreva, David Cash, Marc Fischlin and Bogdan Warinschi

頑強性(Non-malleability) は暗号，コミットメントおよび零知識証明のような基本関数に対しては広く研究されてきた．一方，一方向関数およびハッシュ関数の頑強性は重要な性質として浮上して来ているにもかかわらず，広く取り扱われているとは到底言い難い．本論文ではそんな頑健関数の研究を開始したい．まず，適切な安全性の定義の設計を行う．それから，完全一方向ハッシュ関数およびシミュレーション健全非対話零知識知識証明を使った理論的構成を示して，頑強ハッシュおよび一方向関数が実現可能である事を示す．また，その計算量についても議論する．特に，そうした関数は完全一方向性を含意することを示し，さらに一方向置換と頑健関数とのブラックボックス分離を与える．そして ，Bellare-Rogaway の IND-CCA 暗号系の 2 つのランダムオラクルのうちの一つを安全に置き換えるのに，あるいは クライアント-サーバーパズル（client-server puzzle）の安全性を向上するのに，頑強性が必要十分である事を示し，この定義の暗号学的応用における有用性を例証する．

A New Approach on Bilinear Pairings and Its Applications [Asiacrypt 2009]
Tatsuaki Okamoto

一般に暗号学の分野においてペアリングが広く認識されるようになったのは，1990 年に楕円曲線に対する MOV 攻撃が発表されて以降の事であるが，本公演の前半では，誰が最初に暗号学にペアリングを導入したかに関して，Burt Kaliski の 1988 年の PhD thesis の紹介が行われた．後半は講演者と三菱電機の高島氏との共同研究の内容紹介が行われた．ペアリング群の直積によって構成される，豊富な代数構造を持つ N-次元ベクトル空間について，その和とスカラー倍，標準基底と標準基底上の元の表現，双対性，直交性，基底変換，自己双対などの概念が解説され，その抽象化である，双対ペアリングベクトル空間（DPVS, dual pairing vector space）の定義およびその構成方法が紹介された．また DPVS 内での 3 つの困難問題，

- ベクトル分解問題(VDP, vector decomposition problem),
- ベクトル分解判定問題(DVDP, decisional VDP),
- 部分空間判定問題(DSP, decisional subspace problem),

についての解説が行われ，多変数準同型暗号，内積述語暗号などの暗号学的応用が紹介された．

1.12.4. Asiacrypt 2009 の発表(4 日目)

Improved Cryptanalysis of Skein [Asiacrypt 2009]
Jean-Philippe Aumasson, Cagdas Calik, Willi Meier, Onur Ozen, Raphael C.-W. Phan and Kerem Varici

Skein は SHA-3 の Round 2 に進んだ有望なハッシュ関数であり、ブロック暗号 Threefish を主要な構成要素としている。この論文では、Threefish-512(フルスペックは 72 段)に対し、次の各項を発見した。

- 17 段の近衝突
- 21 段の不能差分
- 34 段の関連鍵ブーメラン識別子(distinguisher)
- 35 段の既知関連鍵ブーメラン識別子(distinguisher)
- 32 段までの鍵復元攻撃

これらの結果から、Skein で使用する Threefish-512 は、少なくとも 36 段以上は必要であると結論づけた。

Linearization Framework for Collision Attacks: Application to CubeHash and MD6 [Asiacrypt 2009]
Eric Brier, Shahram Khazaei, Willi Meier and Thomas Peyrin

ハッシュ関数の衝突探索に圧縮関数の線形化を利用する攻撃法は、Crypto 1998 で F.Chabaud と A.Joux が発表した SHA-0 に対する解析が最初で、その後、V.Rijmen と E.Oswald が SHA-1 を解析した CT-RSA 2005 の発表などがそれに続いた。Rijmen-Oswald では、圧縮関数の線形化と線形符号の組み合わせが利用されており、加算・XOR・ビット回転(AXR)をベースに設計されたハッシュ関数に対して有効な攻撃法である。この論文では、線形化と差分経路のより具体的で分かりやすい関係を示した。そこでは、差分に対する依存テーブルを使った解析を行っており、中立ビットに加え、確率的中立も考慮することで探索を効率化する。この手法を SHA-3 候補である CubeHash と MD6 に適用した。
CubeHash は、連鎖値のバイト長 b と繰返し段数 r の2つのパラメータを持ち、CubeHash-r/b と表される。SHA-3 への投稿では CubeHash-8/1 であり、これは破れなかったが、ずっと弱い CubeHash-3/64 と CubeHash-4/48 では実際に衝突を発見した。また、より安全性の高い CubeHash-6/16 と CubeHash-7/64 の衝突探索コストは各々、$2^{222.6}$ と $2^{203.0}$ と総当たり攻撃より低く、ハッシュ長が 512 ビットの CubeHash-6/4 に対する第2原像攻撃の計算コストはハッシュ値が一つだけ与えられたとき、確率 2^{-478} で成功することが分かった。また、推奨段数が 80 から 168 段の MD6 では、16 段での衝突が発見されている。

Preimages for Step-Reduced SHA-2 [Asiacrypt 2009]
Kazumaro Aoki, Jian Guo, Krystian Matusiewicz, Yu Sasaki and Lei Wang

SHA-2 ファミリーは NIST が SHA-1 の後継としたハッシュ関数であり、今まで衝突探索の研究は比較的進んでおり、SHA-256 に対しては、Nicolic,I.と Biryukov.A による FSE 2008 の論文、および、Indesteege,S.らによる SAC 2008 の論文で、64 段中 24 段まで衝突攻撃が提案されている。一方、原像攻撃の論文は少なく、筆者らの知る限り、Isobe.T と Shibutani,T.が FSE 2009 で示した 24 段という結果だけだった。
この論文では、中間一致を利用した原像攻撃を SHA-2 族に適用した次の結果が報告された。

- SHA-224 は擬似衝突探索が 43 段まで可能で計算量 $2^{219.9}$
- SHA-256 は衝突及び擬似衝突の探索が 43 段まで可能で、計算量は各々 $2^{254.9}$ と $2^{251.9}$
- SHA-384 は擬似衝突探索が 43 段まで可能で、計算量は 2^{366}
- SHA-512 は衝突及び擬似衝突の探索が 46 段まで可能で、計算量は各々 2^{509} と $2^{511.5}$

Fiat-Shamir With Aborts: Applications to Lattice and Factoring-Based Signatures [Asiacrypt 2009]
Vadim Lyubashevsky

著者らは効果的な数論ベースの ID スキームと署名スキームで使われている枠組みをとのようにすれば格子ベースに移植できるかを示した。この移植により、理想格子における最悪ケースでの困難性に基づく安全性を持つ ID スキームと署名スキームで最も効率的なものが実現できた。特に、ID スキームでは通

信複雑度が約 65,000 ビット、署名スキームでは署名長、約 50,000 ビットを達成した。従来の格子ベースの ID/署名スキームでは、通信量や署名長が数百万ビットもしていた。
これらの安全性は近似最短ベクトルを $\tilde{O}(n^2)$ で発見することの困難性をベースとしており、ID スキームでは標準モデル、署名スキームではランダムオラクル・モデルを利用している。また、両スキームの計算時間は $\tilde{O}(n)$ である。この論文の技術を使うと数論ベースのスキームを改良するのにも利用できる。Eurocrypt 1990 で Girault が発表した素因数分解ベースの電子署名スキームに適用すると、安全性を落とさずに署名サイズを短縮することが可能である。

Efficient Public Key Encryption Based on Ideal Lattices [Asiacrypt 2009]

Damien Stehle, Ron Steinfeld, Keisuke Tanaka and Keita Xagawa

この論文では、理想格子上の近似最短ベクトル問題解法の最悪ケースでの困難性に基づいて安全性が証明できる公開鍵暗号スキームを提案している。ベースとなる問題を解くことが、量子計算機を使っても指数関数的に困難であるという仮定の下に、準指数的攻撃に対する CPA 安全性と(準)最適な漸近的性能を達成した。安全性パラメータを n とすると、公開鍵と秘密鍵のサイズが $\tilde{O}(n)$ で、暗号化・復号の 1 ビット当たりの計算コストが $\tilde{O}(1)$ である。この構成法は、Gentry らが STOC'08 で発表した構造化格子に対する誤差付き学習問題をベースとする落とし戸付き一方向性関数を採用している。著者らが主に使った技術的ツールは、ICALP 1999 で発表された Ajtai の落とし戸鍵生成アルゴリズムと、Regev による制限距離復号問題と最短格子ベクトルサンプリング問題の間の量子的帰着関係の再解釈である。

Smooth Projective Hashing and Password-Based Authenticated Key Exchange Based on Lattices [Asiacrypt 2009]

Jonathan Katz and Vinod Vaikuntanathan

安全性の根拠をランダムオラクル・モデルによらない、パスワードベースの認証付き鍵交換プロトコル(PAKE)を最初に提案したのは、Goldreich-Lindell(J.Cryptology 19(3), 2006)だった。しかし、この方式は効率が悪く、同じパーティによる同時実行に対して安全でなかった。この問題点を解決したのが、Eurocrypt 2001 で Katz-Ostrovsky-Yung が提案した方式だが、common reference string(CRS)を利用する点に不満が残った。これらの問題を解決する手段として格子ベースの構成が検討されたが、その実現には、まだ出来ていない CCA 安全な暗号化が必要であった。
この論文では、(一種の)スムーズな projective hashing を認めたとしても選択暗号文攻撃(CCA)に対する安全性が保証できる格子ベースの公開鍵暗号スキームを提案した。ここで、安全性は誤差付き学習問題(LWE)の困難性を根拠としている。この暗号スキームを利用することで、LWE 仮定の下で標準モデルによる安全性が証明可能な PAKE を構成することが可能になった。

PSS is Secure against Random Fault Attacks [Asiacrypt 2009]

Jean-Sebastien Coron and Avradip Mandal

RSA 暗号の CRT を使った実装に対する故障利用攻撃の代表的なものにランダムな誤動作を利用する Bellcore 攻撃がある。RSA 暗号以外にも、FDH や ISO/IEC 9796-2 の Scheme 1 に対して有効であることが知られている。この論文では、確率的なアルゴリズムである RSA-PSS を対象とした。解析の結果、RSA の復号が困難と仮定し、ランダムオラクル・モデルを使うと、PSS は Bellcore 攻撃に対して安全であることを証明した。

Cache-Timing Template Attacks [Asiacrypt 2009]

Billy Brumley and Risto Hakala

従来のキャッシュタイミング攻撃はサイドチャネル情報として計算時間を利用していたが、この論文では電力波形を利用する。解析では、CHES 2002 で Oswald が導入した隠れマルコフモデルに、ベクトル量子化を組合せることにより、キャッシュタイミングを推定する手法が使われている。この解析手法を OpenSSL(0.9.8k)の楕円曲線計算部分に適用したところ、ECDSA の長期秘密鍵が数時間で求まった。観測したのは、キャッシュタイミング、署名、メッセージである。

Memory Leakage-Resilient Encryption based on Physically Unclonable Functions [Asiacrypt 2009]
Frederik Armknecht, Roel Maes, Ahmad-Reza Sadeghi, Berk Sunar and Pim Tuyls

最近、メモリを直接読み出す攻撃法が現実的脅威であることが明らかになり、秘匿情報の一部が漏れても安全性が保証できる暗号方式の研究が盛んになっているが、漏洩情報がしきい値を超えると安全性が保証できないという問題点がある。ここでは、これに対する解決策として、Physically Unclonable Functions(PUF)を利用して擬似乱数を生成する暗号プリミティブ PUF-PRF を提案している。さらに、情報漏えいがあっても安全性が証明できる、PUF-PRF ベースのブロック暗号を提案した。また、PUF-PRF の実現方法としては、効率的で安全性の高い SRAM を使った方式を提案している。

Signature Schemes with Bounded Leakage Resilience [Asiacrypt 2009]
Jonathan Katz and Vinod Vaikuntanathan

近年、秘密鍵の任意のビットが漏洩しても、漏洩ビット数が上限を越さなければ、安全性が保証できる漏洩耐性暗号方式(leakage-resilient cryptosystem)が提案されている。しかし、それらのほとんどは秘匿性を保証するもので、唯一の例外は、認証性(authenticity)を保証した方式は、Crypto 2009 で Allen.J らが提案した方式だけだった。Allen らの漏洩耐性を持つ署名方式は、ランダムオラクル・モデルを使った数論的仮定に基づくものだった。
この論文では、標準モデルを使い、一般的な仮定の下で漏洩耐性を保証できる1個の署名方式と2個の一時(one-time pad)署名方式を提案した。今、秘密鍵をnビットとすると、これら3個の署名方式は次の性質を持つ。
(1)署名方式標準モデルにおける一般的な仮定の下で、選択メッセージ攻撃に対し、存在論的に偽造不能。任意の $\varepsilon > 0$ に対し、準指数時間の困難性の仮定では $n - \omega(\log n)$ ビットの情報漏洩まで耐性がある。
(2)t-time 署名方式
標準モデルにおいて、一方向性の最小限の仮定の下で、任意の $\varepsilon > 0$ に対し、$(1/4 - \varepsilon)\omega \cdot n$ ビットの情報漏洩まで耐性がある。
(3)one-time 署名方式
標準モデルにおいて、種々の具体的な仮定の下で、任意の $\varepsilon > 0$ に対し、$(1/2 - \varepsilon)\omega \cdot n$ ビットの情報漏洩まで耐性がある。また、$\Theta(n/t)$ ビットの情報漏洩まで耐性がある t-time 署名方式。

1.12.5. Asiacrypt 2009 rumpの発表

A Practical-Time Attack on the Encryption Algorithm Used in Third Generation Telephony [Asiacrypt 2009 rump]
Orr Dunkelman, Nathan Keller, and Adi Shamir

第3世代携帯電話規格の一つである WCDMA で利用されている KASUMI は、MISTY1 をベースに設計された 64 ビット・ブロック暗号である。この発表では、KASUMI に対して関連鍵ブーメラン攻撃を提案した。攻撃に関するデータは次の通り。
・関連鍵: 4 個
・データ複雑度: 2^{26} 個の選択平文
・空間複雑度(メモリ): 2^{36} バイト(=1 ギガバイト)
・時間複雑度(計算量): 2^{32}(回分の暗号化)

http://eprint.iacr.org/2010/013

1.13. FSE 2010 の発表

1.13.1. FSE 2010 の発表(1 日目)

Cryptanalysis of the DECT Standard Cipher [FSE 2010]
Karsten Nohl, Erik Tews, and Ralf-Philipp Weinmann

DECT Standar Cipher (DSC)はワイヤレス電話の通話を秘匿するために広く利用されている proprietary な 64 ビットのストリーム暗号であり、クロックが不規則な複数の LFSR と非線形出力コンバイナによって構成されている。この論文では、カスタム・ファームウェアと特許の明細を利用して、HW から DSC をリバースエンジニアする方法を述べ、続いて DSC に対する実用的な攻撃法を提案した。この攻撃法は、DSC ではセッション鍵が入力されてから鍵ストリームが出力されるまで、40 ラウンドしか状態更新しないという設計上の弱点に着目したもので、2^{16} の鍵ストリームを使うと、標準的な PC で数時間以内で 75%の確率で攻撃に成功する。

Improving the Generalized Feistel [FSE 2010]
Tomoyasu Suzaki and Kazuhiko Minematsu

Type-II の一般化 Feistel 構造(GFS)は実装上いくつかの長所を持つものの、拡散性が低いため、十分な安全性を達成するために多くの段数を必要とする欠点がある。この論文では、Type-II GFS の拡散性を改善するため、巡回シフトを別の置換に入れ替えた構造を提案した。サブブロック数が 2 のべき乗のとき、de Bruijin グラフに基づく高効率なブロック置換を使うことによって、安全性と段数のトレードオフが大幅に改善することを示した。

Nonlinear Equivalence of Stream Ciphers [FSE 2010]
Sondre R?njom and Carlos Cid

LFSR と F2 上のフィルター生成器を組合せたストリーム暗号間の非線形等価性について調べた。LFSR が n ビットとすると、このストリーム暗号が生成する鍵ストリームの周期は 2^{n-1} の約数となり、非線形の等価クラスに分類できる。解析の結果、同じ等価クラスの中で、代数攻撃に対する耐性や非線形性は不変でないことが明らかになった。このことから、ストリーム暗号の安全性を議論する場合、同じ非線形等価クラスの中で最も弱い暗号を決めることが必要であることが分かった。しかし、実用的な例における等価クラスのサイズは非常に大きいので、このような作業の実行は非常に困難である。

The Survey of Cryptanalysis on Hash Functions [FSE 2010]
Xiaoyun Wang

ハッシュ関数の攻撃研究のサーベイで、ハッシュ関数の構成、攻撃の歴史、SHA-3 公募に関する話題を簡潔に紹介した。講演後の質問で SHA-3 の有力候補を訪ねられたが、答えは「No idea」だった。また、SHA-1 の衝突探索の計算量も質問され、普通に探索すると 2^{63} で、メッセージ調整などの工夫をすると 2^{61} まで減らせると回答した。この数値は既に発表されているものだが、その後の進展がないことが確認できた。

Lightweight Privacy Preserving Authentication for RFID Based on a Stream Cipher [FSE 2010]
Olivier Billet, Jonathan Etrog, and Henri Gilbert

プライバシを保護する RFID 用の認証プロトコルを軽量ストリーム暗号を利用して構成した。この認証プロトコルの満たすべき要件は、既存のプロトコルと比べ、forward privacy、安全性、DoS 攻撃耐性、計算効率(タグとリーダの両方)をより現実的なバランスで実現することである。forward privacy とは、攻撃者が RFID をタンパーでき、それまでの交信を記録していたとしても、それ以降のデータアクセスとの関連付けができない性質のことである。この論文では、ストリーム暗号が安全であるとき、提案プロトコルの安全性が標準モデルで証明できるこどを示した。実際には、ここで利用されるストリーム暗号は HW 実装が非常に軽量であることが要求される。

Fast Software AES Encryption [FSE 2010]
Dag Arne Osvik, Joppe W. Bos, Deian Stefan, and David Canright EPFL, Switzerland, EPFL, Switzerland, The Cooper Union, USA, and Naval

共通鍵ブロック暗号 AES の 128 ビット鍵に対する高速ソフトウェア実装を 4 種類の環境(8 ビット AVR、32 ビット ARM、Cell、NVIDIA で行い、全環境で処理速度の記録を更新した。ただし、速度の伸びは目覚しいほどではなく、今後、同じ環境で実装性能が大幅に伸びる可能性は低いと感じた。

Attacking the Knudsen-Preneel Compression Functions [FSE 2010]
Onur Özen, Thomas Shrimpton, and Martijn Stam

Knudsen-Preneel(KP)圧縮関数は両者が Asiacrypt'96 と Crypto'97 で提案したハッシュ関数用の圧縮関数である。wide-pipe 構造は線形誤り訂正符号を使って設計され、ブロック暗号は Davies-Meyer モードで利用されたる。この論文では、KPl 圧縮関数の原像耐性を公開ランダム関数の枠組みで解析した。解析の結果、KP 圧縮関数に対する新しい非適応的原像攻撃に成功した。これは query に関して最適な攻撃である。さらに、この攻撃は、提案者が活性要素の個数に基づいて得た直感的な安全性限界の評価が間違っていることを示した。原像攻撃の query 複雑度を形式的に解析したところ、多くの具体的な誤り訂正符号に対し、著者らの攻撃法は計算量(time complexity)が最小になることが分かった。

Finding Preimages of Tiger Up to 23 Steps [FSE 2010]
Lei Wang and Yu Sasaki

FSE 1996 で Anderson と Biham が提案したハッシュ関数 Tiger(ハッシュ長 192 ビット)に対する原像攻撃耐性を評価した。その結果、計算量が圧縮関数 2^{181} 回分で、24 段中 23 段の擬似原像(pseudo-preimage)攻撃が構成できた。これは 24 段中 23 段の原像攻撃及び第2原像攻撃に変換することができ、必要な計算量は各々、$1.4*2^{189}$ と $2^{187.5}$ だった。これらの攻撃に必要なメモリは 2^{22} words である。擬似原像攻撃では、圧縮関数を独立な2つの部分に分割し、中間一致攻撃を適用することによって計算量を削減している。また、攻撃可能段数を最大化するために、鍵スケジュールとステップ関数両方の弱点を利用し、Tiger 圧縮関数を
分割する際のより大きな自由度を得た。

Cryptanalysis of ESSENCE [FSE 2010]
Maria Naya-Plasencia, Andrea Röck, Jean-Philippe Aumasson, Yann Laigle-Chapuy, Gaëtan Leurent, Willi Meier and Thomas Peyrin

ESSENCE は、SHA-3 に応募されたハッシュ関数で、HW 実装に適し、高い並列度を誇る設計になっている。以前の解析では、圧縮関数の非ランダム性は示されたものの、具体的な攻撃には至ってなかった。設計者らは標準的な差分攻撃には耐性があると主張していたが、この論文では、手計算で見つけた差分特性と進化した探索アルゴリズムによって、ESSENCE-256 と ESSENCE-512 の各々に対し、複雑度 $2^{67.4}$ と $2^{134.7}$ の衝突攻撃を見つけた。さらに、HMAC-ESSENCE-256 と HMAC-ESSENCE-512 に対し、各々衝突攻撃と同じ計算量の偽造ペア(メッセージと MAC)を作れることを示した。

1.13.2. FSE 2010 の発表(2 日目)

Domain Extension for Enhanced Target Collision-Resistant Hash Functions [FSE 2010]

Ilya Mironov (Microsoft Research, Silicon Valley Campus)

鍵付きハッシュ関数の安全性概念である enhanced target collision resistance(eTCR)を満たす領域拡張(domain extension)を実現する既存の方式では、鍵長がメッセージ長の増加に対して線形で増加するものしかなく、FSE 2009 で Reyhanitabar は鍵長がメッセージ長の準線形で抑えられる方式の有無を未解決の問題としていた。この論文では、鍵長が準線形となる新たな領域拡張方式を提案し、一方向性関数が存在することがこの方式が eTCR となるための必要十分条件であることを証明した。

Security Analysis of the Mode of JH Hash Function [FSE 2010]

Rishiraj Bhattacharyya, Avradip Mandal, and Mridul Nandi (Indian Statistical Institute, Kolkata, India, University of Luxembourg, Luxembourg, and National Institute of Standards and Technology and George Washington University, USA)

SHA-3 候補として Round 2 に残っているハッシュ関数 JH は、2n ビットの固定置換に基づく圧縮関数(ハッシュ長: n ビット)と、独自のパディングを持つ chopMD 型領域拡張を使う。この論文では、JH の indifferentiability と原像攻撃耐性に関する次の解析結果が述べられている。・JH で使われている 2n ビット置換がランダム置換だと仮定すると、2n-s ビットの出力はランダムオラクルと indifferentiable であって、識別子の利得(advantage)は $O(q^2 \sigma /2^s+q^3/2^n)$で抑えられる・JH のパディング規則は不可欠であり、n ビットを出力する際のメッセージ長を反映したパディングがなければ、単純な indiffirentiability の識別子が構成できる。・JH の出力の際の切り出し方(chopping)を少し改良するだけで、計算効率が同じで、スポンジ構造と同様の安全性限界を保証するハッシュ関数が構成できる。・順逆両方向の多重衝突(multicollisions)を利用することにより、原像攻撃の効率を既存のものより改善した。n=s=512 の原像を得るのに必要な queries は 2^{507} に減った。

Enhanced Security Notions for Dedicated-Key Hash Functions: Definitions and Relationships [FSE 2010]

Mohammad Reza Reyhanitabar, Willy Susilo, and Yi Mu (University of Wollongong, Australia)

Halevi-Krowczyk は Crypto 2006 で鍵付きハッシュ関数の安全性概念 eTCR を提案した。一方、Rogaway-Shrimpton は FSE 2004 でハッシュ関数に関する 7 つの安全性概念 Coll, Sec, aSec, eSec, Pre, aPre, ePre を導入したが、この中には eTCR は入っていない。この論文ではこのような状況を踏まえ、ハッシュ関数の安全性の定義とそれらの間の帰着関係について再考し、次の2つの成果を得た。
・強化された(enhanced)安全性概念 6 個の導入
・上記 6 個と既存の 7 個を合わせた、13 個の間の帰着関係の決定

A Unified Method for Improving PRF Bounds for a Class of Blockcipher based MACs [FSE 2010]

Mridul Nandi (National Institute of Standards and Technology and George Washington, University, USA)

既存のブロック暗号ベースの MAC の大多数では、ブロック暗号への入力が直前のブロック暗号の出力のアフィン変換として決定論に与えられる。この論文では、このような MAC の領域拡張のクラス ADEs(affine domain extensions)と、そのサブクラスとして SADEs(secure ADEs)を導入した。SADEs とはベースとなるブロック暗号をランダム置換と仮定したとき安全性が保証できる ADEs であり、既存の MAC では、CBC-MAC, GCBC*, OMAC, PMAC が含まれる。著者はこれらの SADEs が全部、擬似ランダム関数としての advantage が $O(tq/2^n+N(t,q)/2^n)$で抑えられることを証明した。ここで、t は全部で q 個の query を処理するのに必要なブロック暗号の計算回数であり、N(t,q)はこの論文中で定義されている。この他にも SADEs のいくつかの安全性のバウンドと、CBC-MAC と GCBC*については既存のバウンドより厳密に良いことが示された。

How to Thwart Birthday Attacks against MACs via Small Randomness [FSE 2010]

Kazuhiko Minematsu(NEC Corporation, Japan)

初期ベクタ(IV)をランダム化した MAC の安全性限界(security bound)は従来 O(q^2/2^n)だった。ここで、n は IV のビット長、q は MAC を生成するメッセージ数。本論文では、入力が 2n ビットの擬似ランダム関数と n ビット出力のユニバーサル・ハッシュ関数を組み合わせることで、おおよそ $O(q^3/n^2)$の安全性限界を達成する MAC の構成を提案し、ブロック暗号を使った例を示す。

Constructing Rate-1 MACs from Related-Key Unpredictable Block Ciphers: PGV Model Revisited [FSE 2010]
Liting Zhang, Wenling Wu, Peng Wang, Lei Zhang, Shuang Wu, and Bo Liang(Chinese Academy of Sciences, China)

ブロック暗号ベースの MAC のほとんどで、安全性が元となるブロック暗号の擬似乱数性に帰着されるように設計されているが、2・3 の例外では擬似乱数性より厳密に弱い安全性概念である予測可能性に安全性を帰着させる設計になっている。後者は前者に比べて実装性能は低い。本論文では、関連鍵の意味で予測不能なブロック暗号から構成した rate-1 の MAC の安全性を解析した。最初に、ある種の関連鍵予測不能ブロック暗号を使って設計された rate-1 の MAC が必ず安全でないことが判明した。この攻撃が可能となる条件は、攻撃者が全ての連鎖値を観測できることである。この仮定の下に、鍵付き PGV の rate-1 MAC の 64 タイプを解析した結果、次の結果が得られた。
1) 15 個は無意味
2) 25 個は 3 種類の攻撃が適用可能
3) 24 個は関連鍵予測不能ブロック暗号の仮定の下で安全性が証明可能

Higher Order Differential Attack on Step-Reduced Variants of Luffa v1 [FSE 2010]
Dai Watanabe, Yasuo Hatano, Tsuyoshi Yamada, and Toshinobu Kaneko (Hitachi, Ltd., Japan, Hitachi, Ltd., Japan, Tokyo University of Science, Japan, and Tokyo University of Science, Japan)

Luffa は SHA-3 候補として提案されたハッシュ関数で、Round 2 に進むにあたり、仕様を変更している。仕様の変更前と変更後のバージョンを区別するため、各々を Luffa v1、Luffa v2 と呼ぶことにする。本論文では変更前の Luffa v1 に対する高階差分攻撃を適用した結果、2^{216} 個のメッセージを使い、8 段中 7 段まで攻撃可能であることが示された。Luffa v2 では、終了プロセスで入力なしの(blank)段を利用しているため、この攻撃は適用できない。

Rebound Attack on Reduced-Round Versions of the JH [FSE 2010]
Vincent Rijmen, Deniz Toz, and Kerem Varici (Katholieke Universiteit Leuven, Belgium)

JH は SHA-3 公募の Round 2 に進んだハッシュ関数である。本論文では、JH に対してリバウンド攻撃を適用した結果が示される。メッセージブロックのサイズを 2^d とするとき、提案方式では d=8 であるが、まず d=4 で JH ファミリーに対するリバウンド攻撃がどう適用出来るかを示す。次に d=8 に対する解析を行い、全てのハッシュ長に対し、準自由開始(semi-free-start)衝突が 35.5 段中 16 段まで攻撃可能であり、攻撃に必要な圧縮関数呼出が $2^{179.24}$ 回であると評価した。さらに、1008 ビットの semi-free-start 近衝突が 35.5 段中 19 段まで攻撃可能であり、攻撃に必要な圧縮関数呼出が $2^{156.77}$ 回で、必要メモリ量が $2^{143.70}$ バイトであると評価した。

Pseudo-cryptanalysis of the Original Blue Midnight Wish [FSE 2010]
Soren S. Thomsen (DTU Mathematics, Technical University of Denmark, Denmark)

Blue Midnight Wish (BMW)は SHA-3 公募の Round-2 に進んだハッシュ関数である。BMW は Round 2 に進む際に仕様を変更している。本論文では、仕様変更前のオリジナル版に対する衝突攻撃、原像攻撃、第2原像攻撃の適用結果が示されている。これらの攻撃では、擬似(pseudo-)攻撃、つまり、初期値(IV)を攻撃者が選べる変形版も含まれる。以下では、ハッシュ値のサイズを n ビットとする。近衝突攻撃に必要な計算複雑度(単位は圧縮関数 1 回の計算量)は 2^{14}、擬似衝突攻撃では $2^{3n/8}+1$、擬似(第2)原像攻撃では $2^{3n/4}+1$ である。上記の攻撃はメモリを殆ど必要とせず、BMW の安全性パラメータの影響もあまり受けない。

Differential and Invertibility Properties of BLAKE [FSE 2010]

Jean-Philippe Aumasson, Jian Guo, Simon Knellwolf, Krystian Matusiewicz, and Willi Meier (Nagravision SA, Switzerland, NTU, Singapore, FHNW, Switzerland, DTU, Denmark, and FHNW, Switzerland)

BLAKE は SHA-3 公募の Round 2 に進んだハッシュ関数であり、ハッシュ長に応じて BLAKE-32(224/256 bits)と BLAKE-64(384/512 bits)の2種類がある。BLAKE の内部関数にはストリーム暗号 ChaCha が使われており、BLAKE-32 と BLAKE-64 の推奨段数は各々、10 段、14 段である。BLAKE の内部関数 G の差分特性に基づき、段関数が置換になることと、効率的な逆算アルゴリズムが存在することが示せる。このような性質を使い、1.5 段ではそれまでの攻撃法より速く原像計算ができる。また、発見された性質を使って、BLAKE の内部置換 2 段に対する広いクラスの不能差分が多数見つけられる。また、限られたクラスの不可能差分は、BLAKE-32／BLAKE-64 の各々に対し、5 段／6 段まで導かれる。さらに、線形かつ回転無しモデルを使って、圧縮関数 4 段に対する近衝突が求めることができる。

1.13.3. FSE 2010 の発表(3 日目)

Rotational Cryptanalysis of ARX [FSE 2010]
Dmitry Khovratovich and Ivica Nikolic(University of Luxembourg, Luxembourg)

本論文では、剰余加算、回転、排他的論理和(XOR)を使ったシステムを ARX と名付け、その安全性を解析する。この解析には、理論的な安全性の評価と現実的な攻撃の両方を含む。ARX に対しては、回転攻撃(rotational cryptanalysis)が非常に有効である。回転攻撃は、SHA-3 の Round 2 候補の一つ Skein のコアとして使われるブロック暗号 Threefish の縮小版に対する最も効果的な攻撃法であり、次のような鍵回復攻撃攻撃に関する結果が得られている。
・Threefish-256: 72 段中 39 段
・Threefish-512: 72 段中 42 段
・Threefish-1024: 80 段中 43.5 段
さらに、定数を伴なう ARX は機能的に完全、つまり、いかなる関数も実現できることを証明する。

Another Look at Complementation Properties [FSE 2010]
Charles Bouillaguet, Orr Dunkelman, Gaëtan Leurent, and Pierre-Alain Fouque (École normale supérieure, France and Weizmann Institute of Science, Israel)

DES の弱鍵の間には相補性があるが、本論文では、これを一般化してスライド攻撃と関連鍵攻撃に適用する。第1の結果は、SHA-3 公募の Round 1 候補だったハッシュ関数 Lesamnta であり、スライド／関連鍵攻撃を防ぐために段定数が導入されているにも関わらず、1 回の query だけでフルスペックの圧縮関数に対する識別子が構成できる。第2の結果は、ブロック暗号に対する攻撃で、XTEA、ESSENCE、PURE などの縮小版に対する鍵回復攻撃を示した。

Super-Sbox Cryptanalysis: Improved Attacks for AES-like Permutations [FSE 2010]
Henri Gilbert and Thomas Peyrin Orange Labs, France and Ingenico, France

AES の 2 段は、大きな S-box(Super-Sbox、接続のある 8 個の S-box を含む)4 個で構成される 1 段と見なせる。この性質を使い、AES ベースの SHA-3 候補であるハッシュ関数 Grostl と ECHO に対する攻撃を試みた。その結果、次の攻撃が可能であった。
・Grostl-256 の圧縮関数に対し、10 段中 7 段の擬似衝突攻撃(計算複雑度 2^{120})
・ECHO(512 ビット)の内部関数に対し、10 段中 8 段の識別攻撃(計算複雑度 2^{768})
さらに AES の既知鍵に対する識別子が 128 ビット鍵に対し、初めて 8 段に達した。

1.14. その他

Official comment on MD6 (2009/07/03) [その他]
Ronald L. Rivest 他

MD6 の仕様調整(段数削減など)に関する NIST の依頼に対し、設計者の公式回答が 2009/07/01 に hash-forum@nist.gov へ寄せられた。この回答により、MD6 の SHA-3 への公募が事実上取り下げられたとの認識が広がったが、必ずしもそうでは無い旨の注意が以下で行われている。

http://groups.csail.mit.edu/cis/md6/

112-bit prime ECDLP solved (2009/07/10) [その他]
Joppe W. Bos, Marcelo E. Kaihara, Thorsten Kleinjung, Arjen K. Lenstra, Peter L. Montgomery

200 台の PlayStation3 のクラスタを使って半年かけて 112 bit 素体楕円離散対数問題を実際に解いた。必要な計算時間は 3.5 ヶ月程度。この結果は SHARCS 2009 にて発表予定とのこと。

http://lacal.epfl.ch/page81774.html

SHA-3 Second Round Candidates (2009/07/24) [その他]
NIST

SHA-3 Competition の round 2 Candidates として次の 14 候補が発表された.BLAKE, Blue Midnight Wish, CubeHash, ECHO, Fugue, Grøstl, Hamsi, JH, Keccak, Luffa, Shabal, SHAvite-3, SIMD, Skein

http://csrc.nist.gov/groups/ST/hash/sha-3/Round2/submissions_rnd2.html

GSM-SRSLY? (2009/12/27) [26C3]
Karsten Nohl, Chris Paget

A5/1 ストリーム暗号のリアルタイム攻撃を目的とする、公開事前計算テーブル(レインボーテーブル)作成プロジェクトに関する解説および計算資源募集の発表。この講演が契機となり、携帯電話の通話秘匿用暗号に対する懸念が数多く報道された。A5/1 および、その鍵長を制限した A5/2 は 20 年以上前に設計され世界中で使用されているが、国内の携帯電話網では基本的に採用していない。GSM で使用する A5/1 の鍵長は実質的に 54 bit であり、現在では汎用的攻撃が十分現実的であると考えられている。

Factorization of a 768-bit RSA modulus (2010/01/07) [ePrint 2010/006]
Thorsten Kleinjung and Kazumaro Aoki and Jens Franke and Arjen Lenstra and Emmanuel Thomé and Joppe Bos and Pierrick Gaudry and Alexander Kruppa and Peter Montgomery and Dag Arne Osvik and Herman te Riele and Andrey Timofeev and Paul Zimmermann

RSA factoring challenge の 768 ビット(10 進 232 桁)合成数 RSA-768 の素因数分解に成功した(これまでの世界記録は、663 ビット、10 進 200 桁)という報告が IACR ePrint Archive(2010/006)に掲載された。スイス連邦工科大学ローザンヌ校、日本電信電話株式会社、ドイツ・ボン大学、フランス・国立情報学自動制御研究所、アメリカ・マイクロソフト研究所、オランダ・国立情報工学・数学研究所らの共同研究により、一般数体篩法を用いて約 2 年間で達成された。計算量の支配的なステップは以下の処理である。

篩処理:Opteron 2.2GHz 換算で 1500 年
線型代数処理:Opteron 2.2GHz 換算で 155 年

CRYPTREC Report 2006 における評価では、768 ビット篩処理の計算量を Athlon 64 2.2GHz 換算で 1108 年と見積もっており、評価の妥当性を示す実験結果と言える。

http://eprint.iacr.org/2010/006

楕円曲線暗号とRSA暗号の安全性比較 (2010/01/19) [SCIS 2010]

○下山武司 (富士通株式会社) 伊豆哲也 (富士通株式会社) 小暮淳 (富士通株式会社) 安田雅哉 (富士通株式会社)

素因数分解問題や楕円離散対数問題の実用的パラメタにおける困難さの理解が進んだ. 従来 1024 bit の RSA は 160 bit の楕円曲線暗号と同等の強度と認識されていたが、この評価によると 136 ～ 142 bit の楕円曲線暗号と同等の強度しか持たない. 他のパラメタの評価については以下の通り.

表 2 現実的計算量の等価なパラメタサイズの見積もり(単位 bit)

共通鍵暗号 (全数探索)	素因数分解 (RSA)	楕円離散対数 (素体)	楕円離散対数 (2の拡大体)	楕円離散対数 (Koblitz 曲線)
56	696	105	104	110
60	768	113	111	117
64	850	121	119	125
72	1024	137	136	142
80	1219	151	150	156
92	1536	176	174	181
108	2048	205	203	210
112	2206	213	212	219
128	2832	244	243	250
192	6281	370	369	376
256	11393	596	495	503

Constructing New Differential Paths and Implementing Algebraic … for Full-SHA-1 (2010/01/20) [SCIS 2010]

○杉田 誠 (NTT未来ねっと研究所,産業技術総合研究所) 川添 充 (大阪府立大学) 今井 秀樹 (中央大学,産業技術総合研究所)

SHA-1 の衝突探索の計算量評価としては、McDonald,C.らが Eurocrypt 2009 のランプセッションで示した 2^{52}(回分の圧縮関数計算)が最小であるが、本論文は発表されていない。この発表では、McDonald らの方法をグレブナー基底に基づいて定式化し直し、disturbance ベクトルから差分経路と十分条件を自動的に導く方法や新しい手法(段ごとの準中立ビット、広域ブーメラン、適応的増幅ブーメラン)を適用した。その結果、McDonald らによる新しい disturbance ベクトルに基づくフルスペックの SHA-1 に対する十分条件を導くことに成功した。この結果に基づいて評価した、衝突探索に必要な計算量は 2^{60} 程度ということである。

Experimental Results on Cheon's Algorithm (2010/01/21) [SCIS 2010]

Tetsuya Izu, Masahiko Takenaka, Masaya Yasuda

q-SDH 問題のように、一般の DLP の攻撃者よりも攻撃者に有利な設定で高速に DLP の求解が可能な Cheon 攻撃を GF(3^{127})上定義された超特異楕円曲線上の DLP に対して実装し、実験を行った。使用した計算環境は 3GHz の Core2Quad 1 core で、計算の第一ステップには 8 時間の計算量と 38 Mbyte のデータ領域を要し、第二ステップには 6 時間の計算量と 23 Mbyte のデータ領域を要したとのこと。

GF(3^(6・71))上の離散対数計算実験(676 ビットの解読) (2010/01/22) [SCIS 2010]

◎林 卓也 (公立はこだて未来大学大学院) 篠原 直行 (独立行政法人 情報通信研究機構) 王 立華 (独立行政法人 情報通信研究機構) 松尾 真一郎 (独立行政法人 情報通信研究機構) 白勢 政明 (公立はこだて未来大学) 高木 剛 (公立はこだて未来大学)

関数体篩法により、GF(3)の 6×71 次拡大体(676 ビット)における離散対数計算に成功し、世界記録を更新した(これまでの記録は GF(2)の 613 次拡大)。関係探索ステップでは 96 コアの計算機で約 18 日、線型代数ステップでは 80 コアで約 0.5 日、特定の元の離散対数計算ステップでは 48 コアで約 14 日を費

やした。

On the Security of 1024-bit RSA and 160-bit Elliptic Curve Cryptography (2009/08/15) [IACR ePrint]
Joppe W. Bos, Marcelo E. Kaihara, Thorsten Kleinjung, Arjen K. Lenstra, Peter L. Montgomery

1024 ビット RSA 暗号と 160 ビット楕円曲線暗号との安全性を比較。1024 ビット RSA 暗号は、少なくとも 2014 年までに解読される危険は小さいであろう。160 ビット楕円曲線暗号は、もう少し長く安全に使用できると思われる。2020 年までに解読される可能性はとても小さいと思われる。

http://eprint.iacr.org/2009/389

Breaking ECC2K-130 (2009/11/08) [IACR ePrint]
Daniel V. Bailey et al.

楕円離散対数問題の厳密な強度を理解する為 Certicom は様々なサイズの問題を出題している。本論文では並列化した Pollard の ρ 法を使った Certicom が出題した問題の一つである ECC2K-130 に対する攻撃を記述している。幾つかの普通の計算機クラスター、PlayStation 3 クラスター、GPU および FPGA を使った計算機などが攻撃に貢献している。Eurocrypt より前には攻撃が完了する見込みとのこと.

http://eprint.iacr.org/2009/541

発行日　2010年 5月 28日　第1版第1刷
発行者
・〒184-8795
東京都小金井市貫井北四丁目2番1号
独立行政法人 情報通信研究機構
（情報通信セキュリティ研究センター セキュリティ基盤グループ）
NATIONAL INSTITUTE OF
INFORMATION AND COMMUNICATIONS TECHNOLOGY
4-2-1 NUKUI-KITAMACHI,KOGANEI
TOKYO,184-8795 JAPAN

・〒113-6591
東京都文京区本駒込二丁目28番8号
独立行政法人 情報処理推進機構
（セキュリティセンター 暗号グループ）
INFORMATION-TECHNOLOGY PROMOTION AGENCY JAPAN
2-28-8 HONKOMAGOME,BUNKYO-KU
TOKYO,113-6591 JAPAN