# 3.4.3　ネットワークセキュリティ研究所　セキュリティ基盤研究室

室長　　盛合志帆　ほか 11 名

## セキュリティ基盤技術の研究とプライバシー保護への応用

### 【概　要】

本研究室では、情報通信ネットワークを誰もが安心・安全に利用できるためのセキュリティ基盤技術の研究開発を行っており、中期計画において下記の 4 つの研究テーマを掲げ、現代暗号理論から量子セキュリティまで、実用性を重視した次世代暗号技術の確立を目指し、研究開発を推進している。

1. **量子セキュリティ技術：** 量子 ICT 技術と現代暗号技術を融合した、情報理論的安全性を持つセキュリティネットワーク構築のための研究
2. **長期利用可能暗号技術：** 量子計算機が出現しても安全性を維持できる次世代公開鍵暗号など、長期にわたり高い安全性を維持できる長期利用可能暗号技術に関する研究
3. **実用セキュリティ技術：** プライバシー情報を含むビッグデータのセキュリティ処理に関する研究や秘密漏えいに対する耐性を備えた実用的暗号技術の研究
4. **暗号安全性評価技術の高度化：** 我が国の電子政府推奨暗号の継続的な安全性評価と、CRYPTREC（電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクト）を通じた将来の暗号技術移行指針への安全性評価結果の反映

平成 26 年度は、これまで研究を進めてきたセキュリティ基盤技術を深化させるとともに、そのプライバシー保護への応用展開において、多くの成果を挙げることができた。

### 【平成 26 年度の成果】

#### 1. 量子セキュリティ技術

量子セキュリティネットワークの構築に向けて、量子ネットワーク上でパスワード認証機能付き秘密分散機能を備えたセキュアな外部ストレージシステムの試作を行った。本システムはセキュリティ基盤研究室が東京工業大学とともに検討した方式を未来 ICT 研究所 量子 ICT 研究室等と連携して試作したもので、秘匿と認証の両方の観点で情報理論的安全性が保証されたシステムの世界初の試作である。これはクラウド上の複数サーバにデータを分散して保存する際に、パスワードを持たないユーザが複数のサーバ管理者と結託しても、結託者数が決められたしきい値以下であればデータやパスワードの漏えいがなく、プライバシー保護が実現できることが情報理論的に証明されている。本成果について論文にまとめるとともに、ISO/IEC JTC 1 /SC27 にて国際標準化提案に向けた活動を開始した。

#### 2. 長期利用可能暗号技術

機械学習の分野で難しい問題とされている「LWE（Learning with errors）仮定」を安全性の根拠としたプロキシ再暗号化技術を活用して、暗号化したまま暗号強度の変更と、暗号化したまま加算と乗算が可能なSecurity-updatable Public-key Homomorphic Encryption with Rich Encodings（SPHERE）という世界初の技術を開発した（図 1）。これにより、100 年以上の長期間の保護が求められる遺伝子データ等の安全性確保が可能になり、プライバシーを保護したデータマイニングが可能になる。具体的には、暗号化したデータに対する線形回帰計算で従来比 100 倍の高速化を達成した。本方式について特許出願を行い、報道発表を行った。

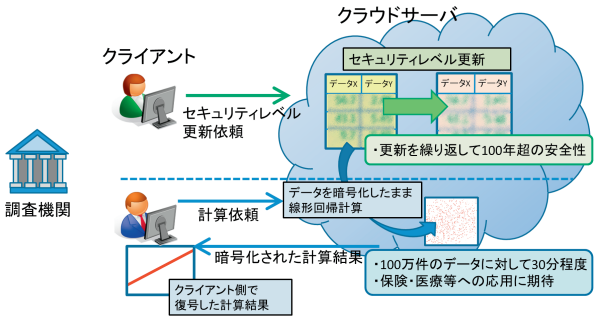


図 1　暗号化したままセキュリティレベルの更新と演算ができる格子理論ベースの準同型暗号方式

格子暗号の安全性の評価も進め、格子の最短ベクトル問題の評価について、フランスの INRIA と連携して評価アルゴリズムを大規模実験により検証した。また、九州大学と共同でドイツダルムシュタット工科大学主催の安全性評価コンテスト “Lattice Challenge” の複数の課題において世界記録を更新した。

### 3. 実用セキュリティ技術

車の各種センサー情報や位置情報に関するデータを活用した新たな高度道路交通システム（ITS）の実用化に向け、そのセキュリティやプライバシー確保が急務となっている。昨年度構築したセキュアストレージシステム PRINCESS を応用し、クラウドを介したセキュアな自動車情報共有システムを試作し、ITS ビッグデータの利活用を促進させる基盤技術開発を行った（図 2）。また、総務省で実証実験を進めている 700 MHz 帯を使った車車間／路車間通信及び、315 MHz 帯を使ったタイヤ空気圧検知システムによる車両特定可能情報等のプライバシー漏えいの可能性を検討するため、電波伝搬シミュレータによる解析を開始した。また、ネットワークにつながる車や ITS、IoT（Internet of Things）におけるセキュリティ確保のための軽量暗号技術の活用について、ITU（International Telecommunication Union）主催のワークショップ等で発表したほか、関連企業との共同検討を開始した。

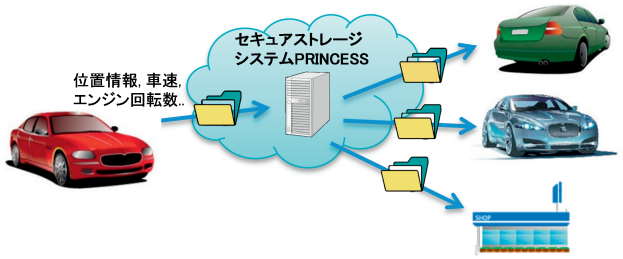


図 2　セキュアな自動車情報共有システム
PRINCESS を応用して実現。代理再暗号化技術により共有先を柔軟に設定でき、プライバシー漏えいのリスクを低減できる。

プライバシー保護技術として、サービスプロバイダがユーザを匿名で認証しつつ、サービス内容を暗号化することが可能なシステムを提案した。また、購入履歴等のログを匿名化することで、ログ漏えい時にもプライバシーを保護するとともに、問題発生時はユーザの特定が可能となるシステムを提案した。システム離脱時・鍵紛失時等に対応するための鍵失効機能についてユーザ削除時に公開するトークンサイズが削除ユーザ数に非依存な方式を提案し、鍵失効機能付き署名の更なる効率改善を図った。

また、パーソナルデータ利活用におけるプライバシー問題の解決に関する研究を立ち上げ、外部有識者を招いてワークショップを開催し、今後に向けて連携する体制作りを開始した。

ある種のペアリング上の暗号系で、実用的な設定における安全性に懸念が生じ始めている。これらの暗号系を安全なペアリング上で実行可能にする変換手法を提案した。また、大規模システムをモジュール的に構成するため、効率的かつ安全性を確保した最適な署名長の群構造維持署名を提案した。これらの成果はいずれも暗号分野において最も権威のある国際会議の 1 つである CRYPTO2014 で発表した。

公開鍵暗号を利用した鍵共有方式（Key Encapsulation Mechanism: KEM）において新方式を発表し、国際暗号標準 ISO/IEC 18033 -2 に採用されている方式よりも安全性・性能に優れていることを示し、ISO/IEC JTC 1 /SC27 にて国際標準化に向けた活動を開始した。

### 4. 暗号安全性評価技術の高度化

離散対数問題に基づく暗号方式の安全性評価の最新動向について調査を行い、電子政府推奨暗号への影響を含めて CRYPTREC に報告を行った。また、ペアリング暗号の安全性評価に対して電子情報通信学会業績賞を受賞した。

連立代数方程式の求解問題や離散対数問題に基づく公開鍵暗号方式の安全性評価を進めるために、立教大学と共同でグレブナー基底の計算アルゴリズムの有効性の検証を行った。また、九州大学と共同で、グレブナー基底を利用した楕円曲線暗号の攻撃法として、基本対称式の性質を利用した改良を提案した。

CRYPTREC 活動として、総務省・経済産業省・（独）情報処理推進機構（IPA）と連携し、暗号技術評価委員会及び暗号技術活用委員会を運営した。NICT は暗号技術の技術的信頼に関する検討を行う暗号技術評価委員会を主として担当し、暗号解析評価 WG 及び軽量暗号 WG で調査を進めた。最新の国際標準化動向や安全性解析状況を見据え、新しいハッシュ関数 SHA-3 等の追加など、CRYPTREC 暗号リストの小改定に向けた評価を行い、電子政府推奨暗号の技術的基盤を支える活動を行った。これらの活動内容は CRYPTREC Report 2014 として公開した。

昨年度構築した公開鍵の安全性検証システム XPIA（X.509 certificate Public-key Investigation and Analysis system）を一般財団法人日本情報経済社会推進協会（JIPDEC）に技術移転し、電子署名・認証制度に基づく認定認証業務において重要な役割を果たしている「認証局自身の電子証明書」について、脆弱性による危険（秘密鍵が推定される可能性）がないことを確認した。