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 8 名

セキュリティ基盤技術の実用化に向けた展開

【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サイドチャネル攻撃による秘密漏えいに対する耐性を備えた暗号技術の研究
4. **暗号安全性評価技術の高度化**: わ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反映

平成25年度は、中期計画でこれまで研究を進めてきたセキュリティ基盤技術の実用化に向けた展開において、多くの成果を挙げることができた。

【平成 25 年度の成果】

1. 量子セキュリティ技術: 認証機能付き秘密分散方式の機能拡張および世界初の実装

量子セキュリティネットワーク構築に向けて、パスワード認証機能付き秘密分散方式の機能拡張および安全性検証を行った。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閾値以下であれば、秘密情報の漏えいがないことを情報理論的に示すことができた（東京工業大学との共同研究）。さらに、上記パスワード認証機能付き秘密分散方式を、未来 ICT 研究所 量子 ICT 研究室等との連携プロジェクト「量子鍵配送を利用したセキュアネットワークの研究開発」にて試作を行った。本試作は、秘匿・認証ともに情報理論的安全性が保証された方式の世界初の実装となる。

2. 長期利用可能暗号技術: 格子理論に基づく新方式の設計と安全性評価

格子理論に基づく新しい暗号方式の設計を行った。機械学習の分野において難しい問題として知られている Learning with Errors （LWE） 仮定の下で安全性が証明され、暗号化・復号処理時間で優れた新しいプロキシ再暗号化方式を提案し、国際会議で発表した（オーストラリア Queensland Institute of Technology との共同研究）。さらに本方式を拡張して、暗号化後にセキュリティレベルを変更できる Security Updatable Encryption という新概念を世界で初めて創出し、特許を出願した。本方式は機能面だけでなく、処理速度においても優れており、従来方式のペアリングベースのプロキシ再暗号化方式と比較して、暗号化では 200 倍以上の処理速度となっている（表 1）。

また、格子暗号の安全性の根拠である最短ベクトル問題の評価を進めた（2013 年 暗号と情報セキュリティシンポジウム論文賞 受賞）。特に、BKZ 2.0 アルゴリズムにおける最適なパラメータを、スーパーコンピュータ TSUBAME2.0 を活用して事前計算して数表とし、実装性能を飛躍的に高めた。一連の改良は、上記の Security Updatable Encryption のパラメータ選定にも活用されている。

表 1　Security Updatable Encryption の処理速度（Core i7, 2GHz 上で測定）

	暗号化	復号	再暗号化	セキュリティレベル
提案方式	0.4 ms	0.045 ms	3.71 ms	135 bit
従来方式	112.3 ms	6.59 ms	352.4 ms	112 bit
高速化	約280倍	約146倍	約94倍	-

3. 実用セキュリティ技術

(1)　サイバーフィジカルシステムを支える暗号技術

センサのようなリソースの限られたデバイスに実装可能な「軽量暗号」の評価基盤の構築を開始した。センサおよびクラウドサーバ上でさまざまな実装性能評価を行い、軽量ブロック暗号の既存暗号に対する優位点を明確化した。センサ側の実装はハードウェア実装(45nm CMOS ASIC ライブラリ利用)および組込マイコン実装(16bit ルネサス RL78)、クラウドサーバ側の実装は Intel Haswell microarchitecture 上でビットスライス実装を行った。さらに、軽量暗号の活用が期待できるアプリケーションとして、自動車や制御システム、医療機器等でのニーズを調査した。特に自動車および ITS のセキュリティについて調査を行い、ワークショップを開催して関係者との意見交換を実施した。

また、ISO/IEC SC27 WG2 で行われている軽量ハッシュ関数の国際規格 ISO/IEC 29192-5 の規格化の開始に貢献した。

(2)　機密レベルに応じた処理が可能なセキュアストレージシステム PRINCESS (プリンセス) の開発

近年、多くのクラウドストレージサービスが普及しているが、サイバー攻撃や管理会社の運用ミス等で保管データの情報が漏えいする可能性がある。このようなリスクを下げるために、保管データの暗号化は有効な手段である。当研究室においてこれまで取り組んできたプロキシ再暗号化技術を応用し、利用者のプライバシや機密情報の取り扱いに配慮した暗号化ファイル共有システム PRINCESS (Proxy Re-encryption with INd-Cca security in Encrypted Storage System) を開発した(図 1)。

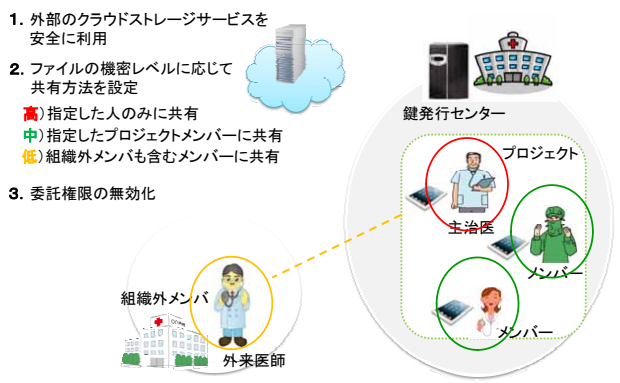

図 1　PRINCESS の医療データ管理への応用例
ファイルの機密レベルに応じた共有方法を設定でき、ストレージ上で暗号化したまま、指定メンバーと安全にファイルを共有できる。

4. 暗号安全性評価技術の高度化

(1)　離散対数問題ベースの公開鍵暗号の安全性評価

クラウドコンピューティング等でのプライバシ保護機能が期待されている次世代暗号「ペアリング暗号」の評価や楕円曲線上の離散対数問題に対してグレブナー基底理論を活用した高速化手法を研究し、2012 年の情報処理学会 喜安記念業績賞につづき、2013 年ドコモ・モバイル・サイエンス賞、IWSEC2013 Best Student Paper Award 各賞を受賞。また電子政府システムでも利用されている離散対数問題ベースの公開鍵暗号の安全性に関する最新動向を CRYPTREC を通じて公開し、電子政府システムの信頼性向上に貢献した。

(2)　SSL サーバ証明書公開鍵検証システム XPIA (エクスピア) の構築

インターネット上の SSL サーバの公開鍵証明書を収集し、サーバ認証に用いられている RSA 暗号の秘密鍵が複数で共有され、脆弱な状態になっている実態を把握するための可視化システム(図 2)を構築し、平成 25 年 10 月に報道発表した。約 400 万の X.509 公開鍵証明書を分析し、10 月時点で世界中で少なくとも 2,600 台を超える SSL サーバが脆弱な公開鍵を利用していることが把握できた。

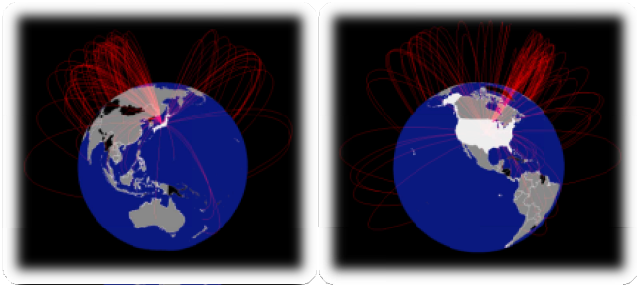

図 2　SSL サーバ証明書公開鍵検証システム XPIA
公開鍵証明書が共通の素因子を共有している SSL サーバ間を赤線で結んで可視化