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、第 3 期中長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**：多様な利用環境に合わせた安全性を提供する、実用的な暗号技術開発を目指す実用セキュリティの研究
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 27 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の実用化に向けた展開及びプライバシー保護への応用において、多くの成果を挙げることができた。

【平成 27 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実装を行った。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実装したもので、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実装である。ここでは、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できる認証機能付き秘密分散プロトコルを提案し活用している。本成果をまとめた論文は論文誌 Scientific Reports に掲載され、学術的にも高い評価を受けた。また、ISO/IEC JTC 1/SC27 にて国際標準化提案に向けた活動を行った。

2. 長期利用可能暗号技術

長期利用可能暗号技術については、格子理論に基づく方式の設計と安全性評価を進めた。格子理論に基づく方式の設計については、平成 26 年度に発表した、暗号化したままセキュリティレベルを変更でき、かつ暗号化したまま加算と乗算が可能な準同型暗号方式 SPHERE（Security-updatable Public-key Homomorphic Encryption with Rich Encodings）を高度化した。本方式は、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ている。この結果、ビッグデータ解析で活用されているロジスティック回帰分析を、データを暗号化したまま実用的な時間で計算可能とし、暗号化された 1 億件のデータを 30 分以内で複数グループに分類できることをシミュレーションで確認した（平成 28 年 1 月 14 日プレスリリー

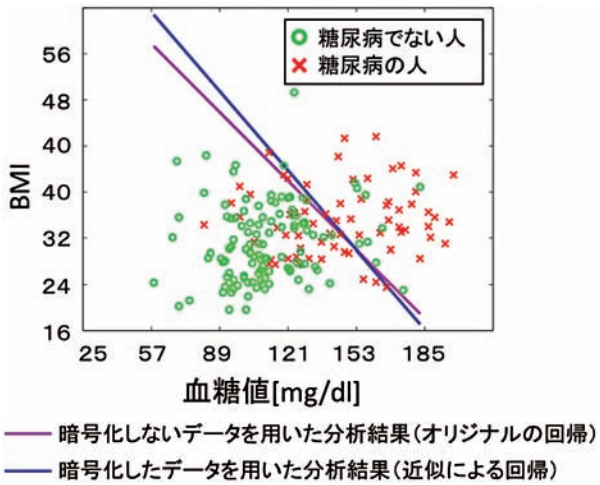

図 1　データを暗号化したままでのロジスティック回帰分析の性能評価の応用例

ス)。図1は、血糖値とBMIのデータから糖尿病であるかどうかを判定するロジスティック回帰分析に応用した例である。また、暗号化したままでの内積の計算方法も考案し、本方式の一連の権利化も進めた。

格子理論に基づく方式の安全性評価については、格子暗号の安全性の根拠である最短ベクトル問題の難しさを高速かつ正確に評価できるよう評価手法を改良し、その成果が暗号のトップカンファレンスのひとつであるEurocrypt2016に採録された。また、独ダルムシュタット工科大主催の安全性評価コンテスト“Lattice Challenge”のいくつかの次元の課題において世界記録を更新した。以上の成果は、九州大学、INRIA(フランス)、日本電気(株)等の外部研究機関と連携して実施したものである。

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。路車間通信において、位置情報のプライバシー保護を実現する軽量グループ署名の提案とシミュレーション解析を実施するほか、Raspberry Pi上で実装を行い、現実的な署名生成効率(数百msec)を実現していることを確認した(図2)。

図2　路車間通信におけるプライバシー保護
軽量グループ署名による実現。位置情報等を送り続けることによる、プライバシー漏えいのリスクを考慮

また、プライバシーに関する諸問題を検討する場として、有識者を交えた「プライバシー検討ワーキンググループ」を研究室内に立ち上げ、適切な同意取得やプライバシーリスク評価に関する議論を開始した。また、情報処理学会主催の第1回プライバシーワークショップ(PWS)にて開催されたPWS CUP(匿名加工処理や匿名加工データからの再識別処理を競うコンテスト)の運営に参画・貢献を行った(図3)ほか、ユーザのプライバシー意識を調査するアンケートシステムの構築を開始した。

第3期中長期目標期間における研究成果の国際標準化も進めた。新たに開発した鍵共有方式“FACE”が、現在、国際暗号標準ISO/IEC 18033-2に採用されている鍵共有方式(Key Encapsulation Mechanism: KEM)よりも安全性・性能に優れていることから、ISO/IEC JTC 1/SC27にて国際標準化に向けた検討を提案していたが、平成27年10月の会合で、ISO/IEC 18033-2への追補に記載する規格化作業を開始することで各国の合意が得られた。

図3　PWS CUPの模様

4. 暗号安全性評価技術の高度化

九州大学との共同研究等によりプライバシー保護に応用できる暗号技術の安全性評価技術の高度化を進めた。また、CRYPTRC暗号リスト掲載暗号MISTY1に対する新たな安全性解析手法の調査を実施した。これらはCRYPTRECにおける電子政府推奨暗号の今後の評価方針の指針として活用された。また、平成26年度に発表されたSSL/TLSに対する攻撃とその対応に関する理論的裏付けを国際会議及び論文誌にて発表した。

総務省及び経済産業省、独立行政法人情報処理推進機構(IPA)と連携してCRYPTRECを運営し、「CRYPTRECの在り方に関する検討グループ」「重点課題検討タスクフォース」にてCRYPTRECで今後扱うべき重点課題の取組方針のとりまとめに貢献した。また、暗号技術評価委員会及び暗号技術活用委員会の開催・運営を行った。特に、暗号アルゴリズムの脆弱性に関する情報発信フローの整備、CRYPTREC暗号リストへの新ハッシュ関数の追加方針の検討、軽量暗号に関する暗号技術ガイドラインの作成方針の検討、新技術に関する調査を実施した。これら一連の活動を通じて電子政府システムへの信頼性・安全性向上に貢献した。