3.7.2 セキュリティ基盤研究室

室長　　盛合 志帆　ほか11名

IoT時代のデータ利活用に資するセキュリティ・プライバシー保護技術

■概要

本研究室では、第４期中長期計画のサイバーセキュリティ分野における「暗号技術」に示されている下記の３つの課題の研究開発に取り組んでいる。

1．機能性暗号技術：IoTの展開に伴って生じる新たな社会ニーズに対応するため、新たな機能を備えた機能性暗号技術や軽量暗号・認証技術の研究開発に取り組む。
2．暗号技術の安全性評価：現在使われている暗号技術や次世代の暗号技術の安全性評価を実施し、新たな暗号技術の普及・標準化に貢献するとともに、安心・安全なICTシステムの維持・構築に貢献する。
3．プライバシー保護技術：パーソナルデータの利活用に貢献するためのプライバシー保護技術の研究開発を行い、適切なプライバシー対策を技術面から支援する。

■平成29年度の成果

1．機能性暗号技術

現在のセキュリティシステムの課題やIoTシステムの展開により新たに生じる社会ニーズを解決する機能を実現する暗号技術の検討を行った。

①複数の暗号要素技術を組み合わせ可能とする群構造維持暗号系

ネットワーク上で利用される情報の中には、プライバシー情報や機密性の高いデータが多く含まれており、これらの情報を守り、ネットワーク上のセキュリティを保証するために、様々な暗号要素技術が利用されている。これらの暗号要素技術を単純に組み合わせるだけで容易に暗号アプリケーションを実現することができ、高い安全性と相互接続性を実現できる群構造維持暗号系方式（図１）を世界で初めて、日本電信電話株式会社（NTT）とドイツのカールスルーエ工科大学との研究協力で開発した（2017年７月 プレスリリース）。この群構造維持署名方式は、従来の群構造維持署名と比較して、利用者数が増加しても鍵長を伸ばすことなく従来と同程度の安全性を達成できる特性も併せ持っている。本方式は、暗号に関する最難関国際会議CRYPTO2017で採択された。

②暗号化したまま演算可能な準同型暗号方式

理化学研究所との共同研究では、暗号化された情報に関する統計情報処理において、統計結果に演算対象としない情報が混在してしまうことを防止するため、同じキーワードに関連した暗号文に対してのみ準同型演算を許可する新しい準同型暗号の演算制御方式を提案し、情報処理学会の2017年度山下記念研究賞を受賞した。また、演算の正しさを保証できる乗算可能な秘密分散方式に関する成果が、情報理論的安全性に関する国際会議ICITS 2017に採録された。さらに、鍵共有方式（KEM）

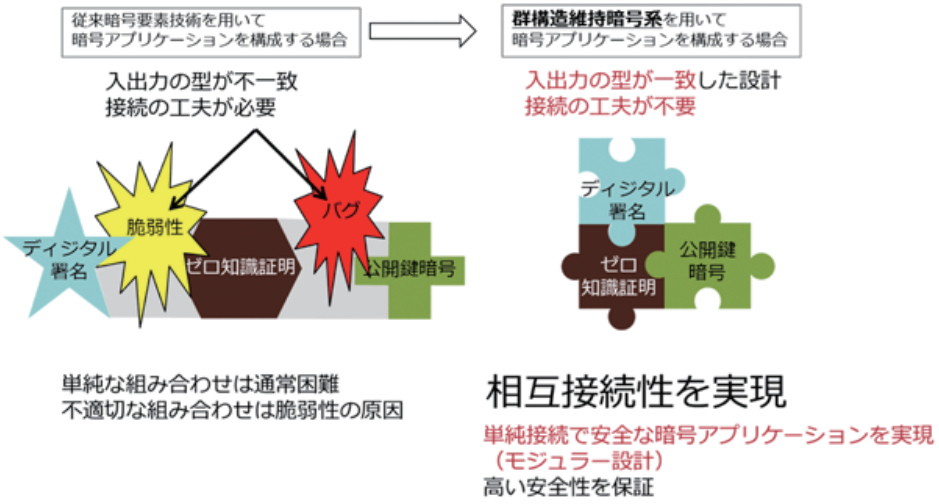

図1　群構造維持暗号技術のコンセプト

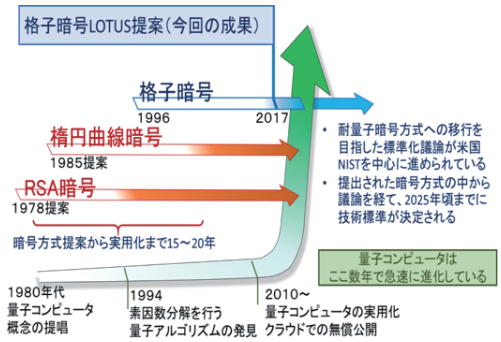

図2　公開鍵暗号の変遷

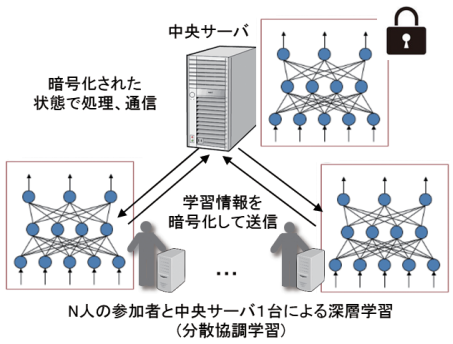

図3　プライバシー保護深層学習システム（Deep Protect）の概念

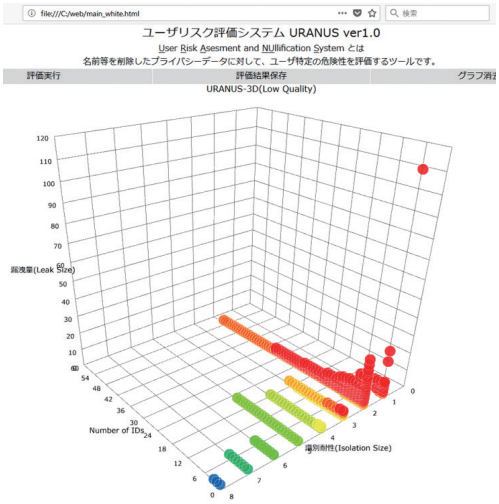

図4　プライバシーリスク評価システム（URANUS）

FACEが公開鍵暗号国際標準ISO/IEC 18033-2（AMD）として採用された。

③IoT機器に実装可能な軽量暗号

IoT時代に向けた軽量暗号の利用促進を図るため、国際会議FSE2017、ITU Workshop、Cyber Secure Car Japan 2017、情報セキュリティ調査専門委員会（JEITA）、組込み技術／IoT Technology2017等で講演を行うとともに、総務省、経済産業省及び独立行政法人情報処理推進機構（IPA）と連携して運営している暗号技術評価プロジェクトCRYPTREC（Cryptography Research and Evaluation Committees）にて軽量暗号ガイドライン（日英語版）を発行・公開した。またCRYPTRECシンポジウムにて、米国国立標準技術研究所（National Institute of Standards and Technology：NIST）の招待講演を実施した。さらに、スマートメータ等で利用可能な、公開検証可能なプライバシー保護時系列データ統計計算方式が国際会議ACISP 2017に採録され、その実装に関する発表が国際会議IWSEC 2017 ベストポスター賞を受賞した。

2．暗号技術の安全性評価

CRYPTRECの暗号解析評価ワーキンググループにおいて、量子計算機が実用化されても安全性が保てることが見込まれる耐量子計算機暗号の安全性評価に関する動向調査を開始した。調査結果は、次年度のCRYPTREC Reportにおいて公開する予定である。

耐量子計算機暗号の１つである格子暗号は、プライバシー保護に適した秘匿計算機能の実現が期待される準同型暗号の性質も持つ暗号であり、実用化に向けて研究が進められている。この格子暗号の安全性評価において、解析が不十分だったSchnorrのRandom Samplingアルゴリズムの再評価に成功し、その成果を国際会議Eurocrypt 2017にて発表した。さらに、量子コンピュータでも解読が困難な格子理論に基づく新暗号方式LOTUS（ロータス）を開発し、現在の公開鍵暗号を置き換える耐量子計算機暗号を世界中から公募するNIST PQC（Post-Quantum Cryptography）標準化プロジェクト（図２）に提案した（2018年１月 プレスリリース）。

3．プライバシー保護技術

AIを活用したプライバシー保護データ解析技術として、複数の参加者が持つデータセットを互いに秘匿したまま深層学習を行うプライバシー保護深層学習システム（Deep Protect）（図３）の実装を行い、実用性検証を行った。

JST CREST研究領域にて採択された研究課題「複数組織データ利活用を促進するプライバシー保護データマイニング」の研究開発を連携研究機関と進めている。パーソナルデータを保護しつつ、機械学習アルゴリズムを活用して、高速に分類・予測・異常検知を行うセキュアなビッグデータ解析技術の研究開発を進め、金融分野における、インターネットバンキング不正送金の検知、顧客データを活用した融資時の適正利率の導出等の社会問題の解決を目指す。

また、個人情報保護法改正に伴って導入された「匿名加工情報」の技術支援として、仮名化によるプライバシーリスク評価システム（URANUS）（図４）を開発した。