3.7.2 セキュリティ基盤研究室

室長　　盛合 志帆　ほか12名

IoTやプライバシー保護等の社会ニーズに応えるセキュリティ基盤技術

■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：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28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要素技術を精査し、それらを活用するための課題抽出・検討を行った。そのいくつかを紹介する。

安全・安心な社会システムの実現には様々な課題が存在する。クラウドなどに集められるユーザ情報を利活用するサービスが注目を集めているが、一方、プライバシーの問題が懸念される。プライバシーを保護したビッグデータの利活用のため、暗号文を復号せずに演算することが可能な「準同型暗号」において、特定のキーワードに関連した暗号文に対してのみ選択的に準同型演算を許し、別のキーワードの暗号文の誤演算混入を防ぐ新方式（図１）を提案し、情報処理学会コンピュータセキュリティシンポジウム2016において最優秀論文賞を受賞した。また、柔軟な鍵の取り扱いを可能とする、効率的な鍵失効機能を有するIDベース暗号の提案を行い、国際会議RSA Conference 2017にて発表した。その他、鍵共有方式FACEの公開鍵暗号（KEM）国際標準ISO/IEC 18033-2（AMD）掲載に向けた標準化活動を進めた。

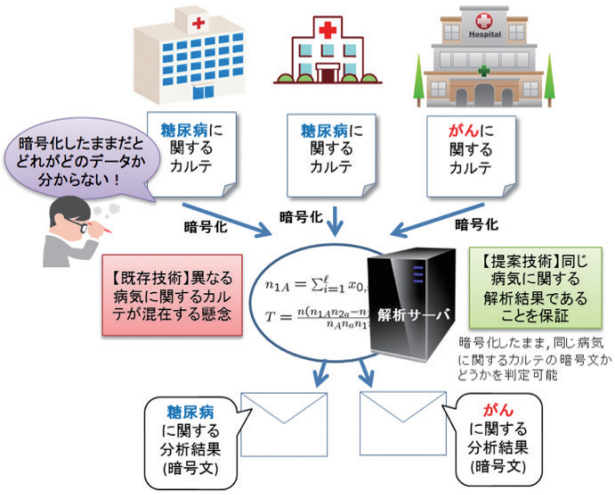

図1　暗号化したままデータ分析を行う際の課題を解決

また、大規模なシステムや複雑なアプリケーションを安全性と機能性を両立させながら実現するためには、モジュラー設計・構築が有用となる。モジュラー設計を可能にしつつ、安全で利便性の高い機能性暗号技術を実現する群構造維持暗号系の研究について、市村学術賞（功績賞）を受賞した。また、代数的構造のシンプルな対称ペアリング上で設計された暗号方式を、実装効率の優れた非対称ペアリング上の方式へと最適な変換を行う技術を提案し、暗号分野の世界最高峰の国際会議CRYPTO 2016にて採録された。

IoTシステムは急速な広がりを見せているが、リソースが限られ、従来の暗号技術を実装することが困難なIoTシステムが数多く存在する。IoT時代に適した軽量暗号の利用促進を図るため、軽量暗号を選択・利用する際の技術的判断に資する軽量暗号ガイドライン（日本語・英語版）をCRYPTREC軽量暗号WGにて作成した。また、軽量ハッシュ関数の国際規格ISO/IEC 29192-5の出版にエディタとして寄与した。

2．暗号技術の安全性評価

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）において、現在利用されている暗号及び

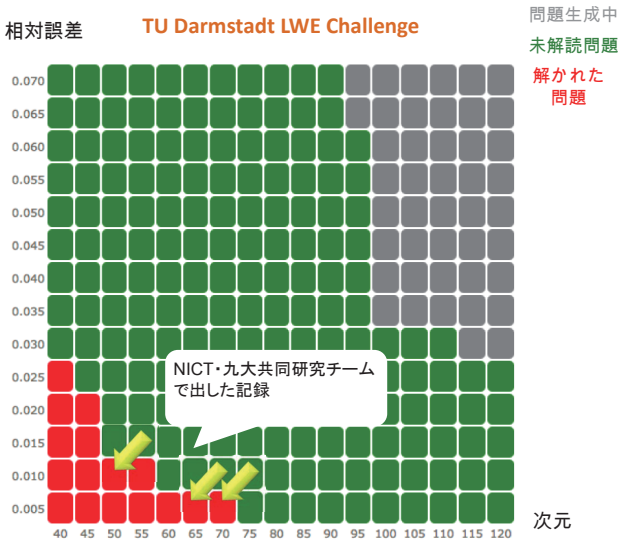

図2　格子暗号の安全性評価で世界記録を更新
https://www.latticechallenge.org/

今後の利用が想定される暗号の安全性評価と監視活動を実施している。楕円曲線暗号の安全評価において、既存の攻撃方法であるρ法の計算効率と、新たな攻撃方法であるECDLPに対する指数計算法の計算効率を比較する必要が生じている。なぜならば、楕円曲線暗号の安全な鍵長は最も効率のよい攻撃方法の計算効率から算出される必要があるからである。上記の２つの攻撃方法の計算効率性について調査し、現時点ではρ法で安全な鍵長を見積もる必要があることを、CRYPTRECレポートで公開した。また、ハッシュ関数SHA-1において衝突発見が報告されたことから、SHA-1の安全性低下を警告し、より安全なハッシュ関数（SHA-256等）への移行を推奨する速報をCRYPTREC Webページにて公開した。

現在、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暗号（耐量子計算機暗号）の研究が世界的に進められている。一方で、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暗号として準同型暗号が注目されている。格子暗号は耐量子計算機暗号及び準同型暗号の双方の性質を持つ暗号であり、実用化に向けて研究が進められている。格子暗号の安全性評価において、世界最高の解読速度と正確な解読時間評価を両立したアルゴリズムを開発し、国際会議Eurocrypt 2016で発表した。さらに、暗号解読をめぐって世界中の暗号研究者が参加するドイツDarmstadt工科大学（TU Darmstadt）主催のLearning with Errors（LWE）Challengeに参加した。LWE Challengeは問題を構成するノイズと次元が大きいほど、その問題の困難性が高まる。図２が示すように、ノイズの割合が0.005で次元が70の場合を含む３つの場合で解読実験に成功することで、Eurocrypt2016で発表したアルゴリズムの有効性を数値実験的に証明した。

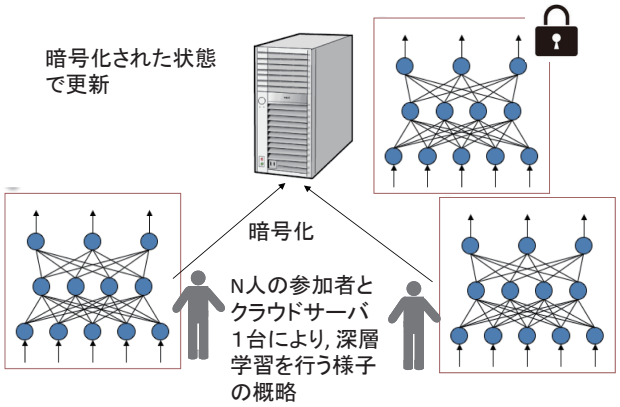

図3　プライバシー保護深層学習システム

３．プライバシー保護技術

本プロジェクトでは、個人情報及びプライバシーの保護を図りつつ、パーソナルデータの利活用に貢献するために、（A）準同型暗号や代理再暗号化技術等を活用し、データを暗号化したまま様々な解析を可能とする技術等の研究開発を行うこと、また、（B）パーソナルデータ利活用におけるプライバシー保護を技術支援するためのポータルサイト作成を目標としている。

（A）として、多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（分散協調学習）を提案した（図３）。さらに、「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」の研究課題がJST CRESTに採択された。本課題においては、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に取り組む。本技術を金融分野における、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の２つの課題の解決に活用することを目標としている。

（B）として、匿名加工技術の有用性指標、安全性指標の設計及び開発を行い、提案した指標を情報処理学会主催のPrivacy Workshop匿名加工・再識別コンテストPWS CUPに導入し、同コンテストのルール及びシステムの設計に貢献して有効性を実証した。またプライバシー保護技術で守るべきプライバシー情報の調査を行い、仮名化データのリスク評価ツールの試作を行った。さらに、プライバシー保護の基本技術である確率的応答方式について差分プライバシーを用いて定量的に安全性評価を行い、いくつかの有用だとされてきた方式が安全ではないことが判明した。これら一連の研究成果については、国際会議などで発表した。