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 30 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の検討を行った。

(1) プライバシーを保護したまま解析可能な暗号方式の実証と外部連携

データマイニング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つつ、データ解析結果の妥当性を向上させるために、NICTでは暗号化したまま演算可能な準同型暗号において誤データ混入防止機能を持つ方式を開発研究している。これを用いて、暗号化した医療データの中身を見ることなく、また、解析対象外データの混入を防止しながらカイ二乗検定を行う手法（図１）の実証実験を、筑波大学と共に行った（７月プレスリリース）。この暗号方式では、解析中にデータの中身を見ることが許されない医療データに対して、解析対象外のデータが混在した場合でも高速に検出することができ、その解析結果に対象外のデータが混入していないことを暗号理論的に証明することで、解析結果の妥当性を向上させることが可能になった。さらに、パーソルキャリア

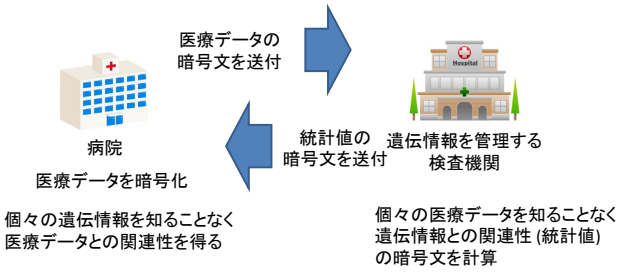

図1　暗号化した医療データの中身を見ることなく、解析対象外データの混入を防ぐ解析手法

株式会社 ミイダスカンパニー（現ミイダス株式会社）のデータ活用事業に対し、解析手法の技術支援（平成31年２月お知らせ）や、検索可能暗号における公開鍵暗号との併用時の安全性向上技術を東海大学と提案して開発するなど、暗号技術の社会還元に向けた様々な研究開発を推進している。

(2) 暗号方式の速度評価や効率化に向けた技術と外部連携

ペアリング暗号方式を用いた暗号方式の処理速度を実装せずに擬似コードレベルで評価可能なツールを、NTTと連携して提案した成果が、暗号分野の国内最大のシンポジウム SCIS2018にてイノベーション論文賞を受賞した（360件中２件受賞）。また、群構造維持ディジタル署名（SPS）について、高い安全性を持つ SPS として世界最小の署名サイズとなる方式を提案し、暗号分野世界３大会議の１つ国際会議 ASIACRYPT[*1] 2018にて採録された。さらに、情報理論的安全な秘密分散について、情報開示量を自由に制御し最適化する方式を大阪大学と連携し提案し、論文誌 IEEE Transactions on Information Theory に採録された。さらに、国際会議ISITA2018にて発表したカードを用いたセキュアな多数決投票プロトコルの論文が IEEE Information Theory Society Japan Chapter Young Researcher Best Paper Award を受賞し、国内会議CSS 2018にて発表した弱い計算量仮定に基づくしきい値暗号の論文がCSS2018優秀論文賞を受賞した。また、インターステラテクノロジズ株式会社と法政大学との産官学連携で、小型人工衛星や打上げ用小型ロケットとの通信において、現在利用可能な低コスト電子デバイスを用いて、情報理論的安全性を達成できること

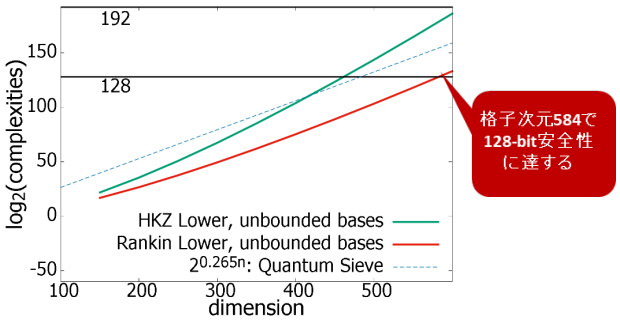

図2　格子暗号の安全性評価

を明らかにし、本安全性に基づく通信技術を提案するなど、暗号技術の社会還元に向けた様々な研究開発を推進している。

(3) 安全な暗号技術の標準化

NICTの研究成果である鍵共有方式（KEM）FACEが採択された公開鍵暗号国際標準 ISO/IEC18033-2（AMD）が発行され、エディタ貢献による国際規格開発賞を受賞した。

2．暗号技術の安全性評価

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）と連携して行っているCRYPTREC[*2] の暗号解析評価ワーキンググループにおいて、大規模量子コンピュータ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」の研究動向調査報告書を平成31年３月31日までに完成した。平成31年４月にはCRYPTREC Webページに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１つであり、実用化に向けて研究が進められている。量子コンピュータでも解読が困難な格子理論に基づき開発した新暗号方式LOTUS[*3]（ロータス）を、米国NIST[*4] が進めるNIST PQC（Post-Quantum Cryptography）標準化プロジェクトのRound １候補（69方式）の１つとしてNIST PQC標準化ワークショップにて発表した。さらに、LOTUSなど格子暗号の安全性評価に用いる格子点探索アルゴリズムの計算量について、量子版の厳密な評価を行いASIACRYPT 2018で採録された。この評価を古典版探索アルゴリズムの計算量の下限評価（図２）（CRYPTO[*1] 2018に採録）と組み合わせることで、長期的な運用に向けたパラメータ設定が可能になった。

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）の研究開発を継続して行っており、銀行の実取引データを用いた不正取引検知の実証実験を神戸大学、株式会社エルテスと共に開始した（平成31年２月プレスリリース）。この研究の一部は、平成28年度採択のJST CREST[*5] 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（課題番号 JPMJCR168 A、研究代表者: NICT セキュリティ基盤研究室 盛合 志帆）」の下で行われた。

プライバシーポリシーのユーザ理解支援ツール設計に向けた検討を進め、プライバシーポリシー解析用の機械学習用データセット拡充やGDPR[*6]（EU一般データ保護規則）施行後に改訂されたプライバシーポリシーの調査を行った。また、ユーザにとって理解しやすいプライバシーポリシー表示方法をWebアンケートにより調査し、その結果をSCIS2019において発表した。

*1 ASIACRYPT: 暗号分野における世界３大会議の１つ、他にCRYPTO、EUROCRYPTがある
*2 CRYPTREC: Cryptography Research and Evaluation Committees、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
*3 LOTUS: Learning with errOrs based encryption with chosen ciphertexT secUrity for poSt quantum era
*4 NIST: National Institute of Standards and Technology
*5 JST CREST：国立研究開発法人科学技術振興機構（JST）が行う戦略的創造研究推進事業
*6 GDPR：General Data Protection Regulation、EU一般データ保護規則

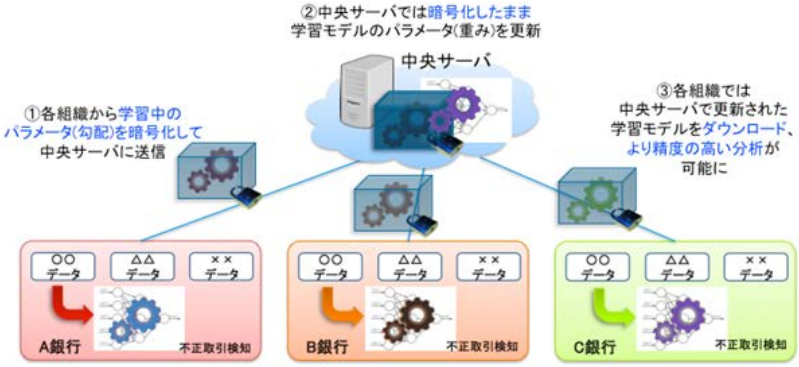

図3　複数の組織が持つデータを外部に開示することなく協調して深層学習を行えるプライバシー保護深層学習システム「DeepProtect」