戦略的創造研究推進事業　CREST
研究領域「イノベーション創発に資する
人工知能基盤技術の創出と統合化」
研究課題「安全な秘匿化データ処理を実現する
汎用依頼計算技術」

# 研究終了報告書

研究期間　2016年12月～2019年3月

研究代表者：花岡　悟一郎
（産業技術総合研究所
サイバーフィジカルセキュリティ
研究センター　研究チーム長）

## §1 研究実施の概要

(1)実施概要

データを収集・解析し、実社会に役立てる技術に期待が集まっているが、データ収集には常にプライバシ侵害のリスクがつきまとう。そのリスクを解消するための秘匿データ処理技術がこれまで数多く提案されてきたが、いずれも個別ケースに対する専用設計であり、高い開発コストが実用化を阻害する要因となっていた。本研究では低コストで実施可能かつ汎用性の高い「汎用秘匿化依頼計算技術」の実現に向け、暗号理論設計グループと応用分野実装グループが連携しながら、計画に沿って以下の通り研究を進めた。

まず、秘匿依頼計算技術の要素技術(関数暗号・準同型暗号・マルチパーティ計算)やそのアプリケーションに関する動向調査を行った。この動向調査を通じて、効率性や適用範囲を考慮すると、多項式回の加法に加えて 1 回の乗算を暗号空間で効率的に実行できるレベル2準同型暗号、および秘密分散技術を用いたマルチパーティ計算(特にクライアントが事前計算を補助するもの)が秘匿依頼計算の要素技術として有望であることが明らかになったため、これらの技術を理論・実践の両面から高度化していく方針で研究・開発を進めることとした。また、求められる演算に関して検討した結果、最大値を求める max、最大値のインデックスを求める argmax を秘匿計算上で実行できるようにすることで秘匿計算の適用範囲が広がることがわかり、それらの関数の中心的な構成要素は大小比較関数であることが判明したため、その効率化に注力することとした。

次に、秘匿データ処理システムの設計を行った。暗号理論グループでは複数の企業からの技術要求に応じた設計を行い、秘匿状態でユークリッド距離を計算できる検索可能暗号や秘匿大小比較の高度化、秘匿コンテンツ配信システムなどを構築した。応用分野実装グループではゲノム情報の秘匿化を扱い、Burrows-Wheeler 変換と紛失通信、加法準同型暗号を用いた高速な秘匿文字列検索手法の構築、それを日本語テキストなど大きなアルファベットサイズに適用するための Wavelet Matrix に基づく拡張を行った他、差分プライバシとマルチパーティ計算による薬剤感受性予測性能の向上にも成功した。

ここまでで得られた知見を基に、秘匿計算の汎用性向上と実装に取り組んだ。秘匿化依頼計算技術の汎用性向上のためには、高速で扱いやすいレベル2準同型暗号の設計と実装、複数の暗号技術を有機的に結合して取り扱えるフレームワーク(MAYBE フレームワーク)、及びその上で効率的に動作する秘匿化依頼計算ツール群が重要であることが判明しており、それらの実現に向けて研究を進めた。

- レベル2準同型暗号に関しては、Lifted-ElGamal 暗号と非対称素数位数ペアリングを組み合わせることにより高速処理が可能な方式を設計し、C++及び WebAssembly のライブラリを実装した。また、このライブラリを活用して、(1)SNS 会話を秘匿して高価値広告の表示、(2)カレンダーの内容を秘匿して日程調整、(3)遺伝病リスクや個人の嗜好を秘匿したお見合い、(4)回答内容を秘匿したアンケート集計や電子投票、などの社会実装に近い応用アプリケーション群を開発し、汎用性の高さを示した。このアプリケーション群に関するデモは、国内最大級会議である2018年コンピュータセキュリティシンポジウム(CSS2018)において最優秀デモンストレーション賞を受賞した。
- MAYBEフレームワークはこれまで知られているマルチパーティ計算の基盤ツール(秘密分散、ガーブルド回路、準同型暗号)を統合して扱えるフレームワークであり、実用面・学術面のいずれにおいても画期的な新技術であると言える。現在は基本部分の検討を終了し、論文を準備中である。秘匿化依頼計算ツール群に関しては、頻繁に用いられる大小比較に特に注目し、必要な通信回数が最も少ないプロトコルを構成した。他にも最大値抽出や算術除算などの効率化に成功した。得られた成果の多くは査読付き国際会議・論文誌に採録されており、国際的に高い評価を受けている。また、構築した秘匿化依頼計算ツール群を実装し、統計処理やゲノム距離計算といったアプリケーションの秘匿化を通じて、構築したツール群の有用性を示した。このツール群を提案した論文は CSS(PWS)2018 において優秀論文賞を受賞した。

(2)顕著な成果

＜優れた基礎研究としての成果＞

1． 効率的な追跡及び無効化が可能な暗号方式

概要：コンテンツ配信などの商用サービスにおいて有用な「追跡可能暗号」において、ユーザの無効化が可能かつ追跡が容易で効率の良い構成を世界で初めて提案し、セキュリティ分野のトップ会議であるACM CCS 2017に採録された。本研究では高機能暗号の一種である関数暗号から要件を満たす追跡可能暗号方式への一般的かつ効率的な変換法を提案しており、提案技術を既存の結果と組み合わせることで、上記性質を満たす追跡可能暗号方式が多数得られる。

2．$NC^1$の計算制限ポリシーをサポートする計算機能制限可能疑似ランダム関数

概要：関数への入力値が所定のポリシーを満たさない場合にその関数値を計算できないよう機能制限された鍵を発行可能な「計算機能制限可能疑似ランダム関数」を、計算負荷の高い数学的ツールを用いずに初めて実現した結果が、暗号理論分野のトップ会議であるCRYPTO 2018に採録された。提案する関数は計算複雑性クラス$NC^1$をサポートしており、秘匿計算におけるアクセス制御や、暗号学的電子透かしなどの応用が期待されている。

3．高速な秘匿比較プロトコルの構成法

概要：秘密分散技術を用いて秘匿状態で整数の大小比較を行うプロトコルを提案し、セキュリティの有力会議ESORICS 2018に採録された。整数を木構造で表現して扱う手法などを駆使した結果、通信 5 ラウンド(既存の秘密分散ベース二者間秘匿計算において最小のラウンド数)で実行可能なプロトコルとなっている。大小比較は汎用依頼計算技術の設計において中心的な役割を果たすプロトコルであり、これを効率的に構成できた意義は極めて大きい。

＜科学技術イノベーションに大きく寄与する成果＞

1． 分散データ上での機械学習

概要：複数のパーティーが互いにデータを開示せずにモデル学習を行う手法を提案し、機械学習のトップ会議であるNIPS 2017に採録された。本研究では、差分プライバシとマルチパーティ計算を効果的に組み合わせることによって、分散したデータの保護に必要なノイズの分量を抑えている。薬剤感受性などのデータで検証したところ、単純にデータを分散させた場合よりも精度が大幅に向上することを確認した。本研究成果は複数の拠点に分散するデータの活用に貢献する。

2． 効率的なレベル2準同型暗号とその高速実装

概要：素数位数ペアリングを用いた簡潔で効率的なレベル2準同型公開鍵暗号を提案し、情報セキュリティ分野の有力会議ASIACCS 2018に採録された。提案手法は暗号文上での加算(多項式回)と乗算(1 回)をサポートしており、本研究と同様に素数位数ペアリングを用いた既存の構成と比較すると、暗号文サイズは同じであるもののより高速な処理が可能な方式であることを示している。また、C++に加えて WebAssembly 実装も行い、Web ブラウザから手軽に利用可能な技術となっている。

3． 秘匿アプリケーションの実装とデモ展示

概要：上記のレベル2準同型暗号を用いた秘匿データ処理のアプリケーションを多数実装し、国内最大級の情報セキュリティ会議 CSS2018 でデモ展示を行った。アプリケーションはチャットアプリにおける秘匿広告表示、秘匿スケジュール調整、秘匿アンケート集計、秘匿英語能力推定、不正検知機能付き秘匿電子投票など多岐に渡り、3 日間の展示で 100 人以上の観客を集め、秘匿計算の普及に大きく貢献した。また、最優秀デモストレーション賞を受賞した。

＜代表的な論文＞

1. Mikko Heikkilä, Eemil Lagerspetz, Samuel Kaski, Kana Shimizu, Sasu Tarkoma, and Antti Honkela: Differentially private Bayesian learning on distributed data, The 31st Annual Conference on Neural Information Processing Systems (NIPS 2017)
2. Nuttapong Attrapadung, Goichiro Hanaoka, Shigeo Mitsunari, Yusuke Sakai, Kana Shimizu, and Tadanori Teruya: Efficient Two-level Homomorphic Encryption in Prime-order Bilinear Groups and A Fast Implementation in WebAssembly, The 13th ACM ASIA Conference on Computer and Communications Security (ASIACCS 2018)
3. Hiraku Morita, Nuttapong Attrapadung, Tadanori Teruya, Satsuya Ohata, Koji Nuida, and Goichiro Hanaoka: Constant-Round Client-Aided Secure Comparison Protocol, The 23rd European Symposium on Research in Computer Security (ESORICS 2018)

## §2 研究実施体制

(1)研究チームの体制について

(1) 暗号理論設計グループ
① 研究代表者:花岡 悟一郎(産業技術総合研究所サイバーフィジカルセキュリティ研究センター 研究チーム長)
② 研究項目
・汎用秘匿化依頼計算アルゴリズムの理論設計

(2) 応用分野実装グループ
① 主たる共同研究者:浅井 潔(東京大学大学院新領域創成科学研究科 教授)
② 研究項目
・汎用秘匿化依頼計算技術に基づくアプリケーションとビジネスモデルの開発

(2)国内外の研究者や産業界等との連携によるネットワーク形成の状況について

民間企業 4 社と秘匿計算に関する共同研究を行っており、別資料の業績リストに示されているように査読付き国際会議へ論文が採択されている。また、本研究で中心的に扱っている秘密分散技術に基づく秘匿計算の研究開発を行っている NEC 社及び NTT 社とは、情報処理学会誌への寄稿や国内会議発表を行うなど、共同で秘匿計算技術の社会展開を推進している。