戦略的創造研究推進事業　CREST
研究領域「Society 5.0 を支える革新的
コンピューティング技術」
研究課題「耐量子計算機性秘匿計算に基づく
セキュア情報処理基盤」

研究終了報告書

研究期間　2019年10月～2025年03月

研究代表者：本間　尚文
（東北大学　電気通信研究所　教授）

§1 研究実施の概要

(1)実施概要

本研究では，耐量子計算機性暗号に基づくセキュアコンピューティング技術の確立を目指して，理論から実装までの技術レイヤーを融合したセキュア情報処理基盤の研究開発を推進した．具体的には，チームを構成する 4 つの研究グループがそれぞれ(1)耐量子計算機暗号に基づく高効率秘匿計算技術（本間グループ），(2)同暗号の耐タンパー性セキュアシステム実装技術（林グループ），(3)同暗号に基づく秘匿推論コンピューティング技術（橋本グループ）および(4)秘匿プロセッシング技術（佐藤グループ）の研究開発を行うとともに，全グループ協働によりエッジおよびクラウド応用を想定した統合プラットフォームの開発を推進した．エッジ向けプラットフォームとしては，主に(1)と(2)の成果を統合し，耐量子計算機性暗号の耐タンパー性実装設計・評価を可能とするプラットフォームを開発し，国内外に展開した．また，並行して同暗号に基づく高効率秘匿演算および同暗号の耐タンパー化技術の理論を構築し，同プラットフォーム・クラウド上にてその有効性を実証した．クラウド向けプラットフォームとしては，主に(3)と(4)の連携により，データおよびモデル・プログラムを秘匿したまま機械学習等の多様な処理を実行可能な秘匿汎用プロセッシング技術を提唱し，その基盤ソフトウェアを開発・公開した．さらに，秘匿汎用プロセッシング技術向けのハードウェアアクセラレータの研究開発も実施した．特に膨大で複雑なメモリアクセスと数論変換を効率よく実行する世界初となる専用ハードウェア開発に成功した．

本研究において得られた主要な成果を下記にまとめる．

- 研究項目（1）：耐量子計算機性暗号による確率的秘匿演算手法の開拓・実証
  耐量子計算機性準同型暗号と確率的演算を組み合わせる確率的秘匿演算手法を提案するとともに，そのハードウェアアクセラレータを開発し，従来比 2 桁の性能向上を達成した．また，商用クラウド（Amazon AWS）上でその動作を実証・デモンストレーションした．
- 研究項目（2）：耐量子計算機性暗号 HW 設計・評価プラットフォームの開発・展開
  大規模な暗号化回路を実装可能，かつ，高精度なサイドチャネル攻撃および故障注入攻撃評価可能な Side-channel Attack Standard IMplementation and evaluatIon (SASIMI) ボードを開発し，同ボードを中心とした耐量子計算機性暗号 HW 設計・評価プラットフォームの開発・動作実証に成功するとともに，国内外の有力な関係機関へと展開した．
- 研究項目（1）・（2）：耐量子計算機性暗号の耐タンパー化理論の開発と実証
  米国標準方式を含む主要な耐量子計算機性暗号方式のほとんどに適用可能なサイドチャネル攻撃および故障注入攻撃の脅威を発見するとともに，上記プラットフォームによりその実現可能性を実証した．また，同攻撃に対する効率的な対策手法を明らかにした．
- 研究項目（3）：データとモデル保護を両立する秘匿推論プロトコルの開発
  モデルとデータの両方を保護する耐量子計算機性暗号に基づく秘匿推論プロトコルを提案・開発した．BGV および TFHE という 2 種類の先端的準同型暗号方式を適用して実装および性能評価を行い，その有効性を実証した．
- 研究項目（4）：秘匿汎用プロセッシング技術の提唱と基盤ソフトウェアの開発
  トーラス型完全準同型暗号 TFHE による暗号化論理ゲートを用いて，実行されるプログラムと内部パラメータ，入出力データを全て秘匿しながら任意の計算を実行できる秘匿汎用プロセッシング技術の概念を提唱し，その基盤ソフトウェアを開発・公開した．
- 研究項目（4）：秘匿汎用プロセッシングのハードウェアアクセラレーション・応用展開
  上記で開発した TFHE 暗号化論理ゲート評価を高速化するため，FPGA と ASIC によるハードウェアアクセラレータを設計・開発し，更なる高性能化を達成した．特に，ASIC は，一連の膨大かつ複雑なメモリアクセスと数論変換を効率よく実行するハードウェアを ASIC として世界で初めて実現した．
- 研究項目（3）・（4）：高安全・高信頼な秘匿推論方式の開発
  項目（3）で開発したデータとモデル保護を両立する秘匿推論プロトコルに項目（4）で開発したトーラス型完全準同型暗号 TFHE の基盤ソフトウェアを適用し，モデルパラメータに加えてモデル種別までも秘匿可能な秘匿推論方式を開発した．また，高信頼化に向けて秘匿推論時のソフトエラーの影響を実験により明らかにした．

(2)顕著な成果

＜優れた基礎研究としての成果＞

1.　耐量子計算機性暗号による高効率確率的秘匿演算手法の開拓

概要：

耐量子計算機性暗号に基づく高効率な秘匿演算手法として，確率的秘匿演算手法を開発した．同手法は，確率的な数値表現および演算を利用することで，従来膨大な計算量を必要とした秘匿演算を効率的に実現できる．さらに，同演算手法向けの FPGA アクセラレータを開発し，更なる高性能化が可能なことを示すとともに，その有効性を Amazon AWS 上でデモンストレーションした．同手法を様々な多項式関数および機械学習における推論に適用した結果，従来比 2 桁の性能向上を達成した．上記手法は，その基本コンセプトの特許が日米欧で認定されており，暗号実装分野のトップジャーナルに採録されるなど，国内外で高く評価されている．

2. 耐量子計算機性暗号の耐タンパー化理論の開発と実証

概要：

主要な耐量子計算機性暗号のほとんどが対象となる物理攻撃手法の存在を発見し，その対策技術を提唱・実証した．具体的には，ほとんどの耐量子計算機性暗号に採用される FO（Fujisaki-Okamoto）変換に脆弱性があることを見出し，米国標準方式を含む代表的な耐量子計算機性暗号 9 種類中 8 種類に適用可能なサイドチャネル攻撃，9 種類中 7 種類に適用可能な故障注入攻撃を発見した．さらに，本プロジェクトで開発したプラットフォームによりそれを実証し，耐量子計算機性暗号実装技術の確立に向けて大きく貢献した．その成果は各々暗号理論のトップカンファレンスで採択され，被引用数 Top10％と国際的に高い注目を集めている．

3. 秘匿汎用プロセッシング技術の提唱と基盤ソフトウェアの開発

概要：

トーラス型完全準同型暗号 TFHE を用いてデータとプログラムの双方の暗号化・復号処理を実行するための基本ライブラリを構築し，任意の論理関数評価を可能とした．また，複数の論理関数の組み合わせからなる大規模な論理関数を効率よく評価するための実行エンジンを開発し，OSS ライブラリとして公開した．これらにより，任意の論理関数評価が可能となり多様な応用への展開が可能となった．さらに，暗号化仮想プロセッサの構成とそれがサポートする命令セットを定義し，それらを連動させることで入出力と内部パラメータ，実行されるプログラムの全てを秘匿する秘匿汎用プロセッシング技術が実現可能であることを示した．同成果はコンピュータセキュリティのトップカンファレンスに採録され，国際的に高く評価されている．

＜科学技術イノベーションに大きく寄与する成果＞

1. 耐量子計算機性暗号技術の安全性設計・評価プラットフォームの開発

概要：

耐量子計算機性暗号に代表される大規模な暗号を実装可能，かつ，高精度なサイドチャネル攻撃および故障注入攻撃が評価可能な Side-channel Attack Standard IMplementation and evaluatIon (SASIMI) ボードを開発し，同ボードを中心とした耐量子計算機性暗号 HW・SW 設計・評価プラットフォームの開発とその動作実証・デモンストレーションに成功するとともに，世界的な研究ネットワーク形成のため国内外の有力な関係機関へと展開した．

2. データとモデル保護を両立する秘匿推論プロトコルの開発

概要：

モデルオーナーが秘密鍵を持ち，準同型暗号で暗号化した決定木を送ることでモデルを秘匿したまま計算委託を可能とする秘匿推論プロトコルを提案・開発した．同プロトコルは，データオーナーに決定木の構造推測に有用な情報を与えず，また，モデルオーナーにデータの情報を一切与えないことを可能とし，データとモデル保護を両立する．BGV と TFHE の 2 種類の先

端的準同型暗号を適用した実装・性能評価を行い，その有効性・効率性を明らかにした．

3. トーラス型完全準同型暗号ハードウェアアクセラレータの開発

概要：

トーラス型完全準同型暗号による暗号化論理ゲートの評価を高速化する FPGA および ASIC をプラットフォームとするハードウェアアクセラレータを開発した．暗号化論理ゲートの演算ごとに増加するノイズを低減するブートストラップ演算が処理時間の大部分を占めることに着目し，その主要な処理である多項式乗算を，加減算とシフトのみで計算が可能なハードウェア実装に適する法を活用して高速化した．また，CPU に加えて FPGA や GPU 等のアクセラレータが混在する環境で，暗号化論理ゲートを高速評価できる実行エンジンを世界に先駆けて開発した．

＜代表的な論文＞

1. Rei Ueno, Keita Xagawa, Yutaro Tanaka, Akira Ito, Junko Takahashi, and Naofumi Homma, “Curse of Re-encryption: A Generic Power/EM Analysis on Post-Quantum KEMs,” IACR Transactions on Cryptographic Hardware and Embedded Systems, Vol. 2022, Issue 1, pp. 296–322, DOI:10.46586/tches.v2022.i1.296-322, November 2021.

概要：

本論文では，耐量子計算機性暗号 PQC 全般に脅威となる電力・電磁波解析攻撃の存在を明らかにしている．特に，FO 変換と呼ばれる PQC に必須の処理中のサイドチャネル情報（消費電力や放射電磁波）を観測することで現実的な時間で暗号解読が可能なことを初めて示し，米国標準技術研究所（NIST）の標準暗号候補 9 種類中 8 種類で暗号解読に成功することを実証している．また，同攻撃に対する効果的な対策も合わせて示している．本論文は，暗号実装に関するトップカンファレンス CHES に採択され，被引用数 Top10％と高い注目を集めている．

2. Kotaro Matsuoka, Ryotaro Banno, Naoki Matsumoto, Takashi Sato, and Song Bian, “Virtual Secure Platform: A Five-Stage Pipeline Processor over TFHE,” The 30th USENIX Security Symposium, pp. 4007—4024, August 2021.

概要：

本論文では，完全準同型暗号を用いて Virtual Secure Platform (VSP)と呼ぶ汎用プロセッシング技術を提案・開発した．VSP はデータと関数の双方を秘匿する必要のあるクラウド計算環境等において特に有効である．専用の命令セットアーキテクチャを定義することでゲート数を低減するとともに，パイプライン構成とすることで暗号化ゲート評価の並列性を向上している．オープンソースとして公開されている VSP は1命令を1秒以下で実行でき，既存の完全準同型暗号ベースのプロセッサに対し 1600 倍高速である．本論文は，コンピュータセキュリティのトップカンファレンスの一つ USENIX Security に採択され，そのコードを OSS として公開している．

3. Akira Ito, Rei Ueno, and Naofumi Homma, “On the Success Rate of Side-Channel Attacks on Masked Implementations: Information-Theoretical Bounds and Their Practical Usage,” The 29th ACM Conference on Computer and Communications Security (CCS 2022), pp.1521–1535, November 2022.

概要：

本論文では，サイドチャネル攻撃対策としてマスキング実装が適用された際の攻撃成功率を情報理論の観点から解析するとともに同解析に基づく対策の実装法について明らかにした．特に，低次マスキング対策がなされた際のサイドチャネル情報の相互情報量もしくは機械学習により推定された秘密情報の条件付き確率から，高次マスキング対策の適用時にどこまで安全性が保証されるかを推定することを可能とした．これにより，対策に施すべき適切な次数を決定する指針を与えることに成功した．本論文は，コンピュータセキュリティのトップカンファレンスの一つ ACM CCS 2022 に採択されており，被引用数 Top10％と高い注目を集めている．

§2 研究実施体制

(1)研究チームの体制について

① 「秘匿計算基盤」グループ

研究代表者:本間 尚文(東北大学電気通信研究所 教授)

研究項目:

1-1. 耐量子計算機準同型暗号ハードウェア
1-2. 確率的秘匿演算アルゴリズム
1-3. 確率的秘匿演算による応用アプリケーション
2-2. 耐量子計算機準同型暗号への物理攻撃解析
5-1. 秘匿計算プラットフォームプロトタイプの開発
5-2. 秘匿計算プラットフォームの高機能化・集積化
5-3. 耐量子性・耐タンパー性秘匿計算技術の実証実験

② 「セキュアシステム実装」グループ

主たる共同研究者:林 優一(奈良先端科学技術大学院大学 教授)

研究項目:

2-1. 耐量子計算機準同型暗号への物理攻撃評価環境構築
2-2. 耐量子計算機準同型暗号への物理攻撃解析
2-3. テストベッド環境の構築とシステム実装技術の開発
5-1. 秘匿計算プラットフォームプロトタイプの開発
5-2. 秘匿計算プラットフォームの高機能化・集積化
5-3. 耐量子性・耐タンパー性秘匿計算技術の実証実験

③ 「秘匿推論コンピューティング」グループ

主たる共同研究者:橋本 昌宜(京都大学 教授)

研究項目:

3-1. 決定木秘匿推論プロトコルの CPU 実装
3-2. モデル種別も秘匿可能な秘匿推論方式の開発
3-3. 秘匿推論の信頼性評価
5-1. 秘匿計算プラットフォームプロトタイプの開発
5-2. 秘匿計算プラットフォームの高機能化・集積化
5-3. 耐量子性・耐タンパー性秘匿計算技術の実証実験

④ 「秘匿プロセッシング」グループ

主たる共同研究者:佐藤 高史(京都大学 教授)

研究項目:

4-1. 秘匿プロセッシング向け要素技術の開発
4-2. 秘匿プロセッシング技術の SW(CPU/GPU)実装
4-3. 秘匿プロセッシング技術の HW(FPGA/ASIC)実装
5-1. 秘匿計算プラットフォームプロトタイプの開発
5-2. 秘匿計算プラットフォームの高機能化・集積化
5-3. 耐量子性・耐タンパー性秘匿計算技術の実証実験

(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

国内外の研究機関と暗号ハードウェアの実装技術に関して研究開発で連携している. 特に, 海外では, SASIMI ボードを展開した 8 か国 10 機関の研究者らとネットワークを形成している. 民間企業とも実用化に向けた共同研究を実施している. また, 開発した汎用プロセッシングの基盤技術の応用について, CREST 数理的情報活用基盤 AI 集約的サイバーフィジカルシステムの形式的解析設計手法(研究代表者 末永幸平)と連携している.