2023 年度年次報告書
Society 5.0 を支える革新的コンピューティング技術
2019 年度採択研究代表者

本間 尚文

東北大学 電気通信研究所
教授

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

主たる共同研究者:
佐藤 高史（京都大学 大学院情報学研究科 教授）
橋本 昌宜（京都大学 大学院情報学研究科 教授）
林 優一（奈良先端科学技術大学院大学 先端科学技術研究科 教授）

研究成果の概要

本年度は，各研究開発項目について，下記の研究成果を得た．

(1) 耐量子計算機性準同型暗号に基づく高効率秘匿情報処理技術：

格子暗号に基づく確率的秘匿計算ハードウェアアクセラレータの開発を推進し，開発したアクセラレータをセキュア秘匿計算プラットフォームのコアとなる評価ボードに搭載し，その性能を評価した．それと並行して，開発した確率的秘匿計算を佐藤グループが開発した準同型評価エンジンに適用し，初期評価によりレイテンシが大幅に向上することを示した．

(2) 物理攻撃に対して頑健なセキュアシステム実装技術

耐量子計算機準同型暗号への物理攻撃モデル及び，物理攻撃評価手法の高精度化を進めるとともに，セキュア秘匿計算プラットフォームのコアとなる評価ボードの開発を継続した．また，同評価ボードを国内外研究機関に配布し，同機関との研究連携を強化した．さらに，上記プラットフォームを用いたテストベッド環境を構築した．

(3) 秘匿推論コンピューティング技術

論理解読攻撃に対する耐性を維持しつつ，秘匿計算の実行時間を最小とする秘匿計算向け論理回路設計技術の検討を進めた．具体的には，論理難読化に利用する LUT をどこにどれだけ利用すれば，論理解読攻撃に耐える最小の論理回路となるのかを明らかにした．また，放射線の照射実験により秘匿推論の信頼性を評価し，論理回路の冗長化による誤りの検出法を検討した．

(4) 秘匿プロセッシング技術

暗号化論理ゲートを高速に評価する論理回路を設計し，FPGA を用いてプロトタイピングしその性能を評価した．また，その結果に基づき，暗号化論理ゲートをハードウェアで評価する ASIC の設計を推進した．さらに，CPU，GPU，FPGA，ASIC が混在する環境で，暗号化論理回路をスケーラブルに評価する環境の方式を検討した．

(5) 技術統合・高度化・展開

上記技術を統合した耐量子性・耐タンパー性セキュア秘匿計算プラットフォームを構築した．また，秘匿プロセッシング技術の応用展開をチーム内外で推進した．

【代表的な原著論文情報】

1) Y. Tanaka, R. Ueno, K. Xagawa, A. Ito, J. Takahashi, and N. Homma, “Multiple-Valued Plaintext-Checking Side-Channel Attacks on Post-Quantum KEMs,” IACR Transactions on Cryptographic Hardware and Embedded Systems, 2023(3), pp.473–503, 2023.
2) H. Nishiyama, D. Fujimoto, and Y. Hayashi, “Remote Fault Injection Attack against Cryptographic Modules via Intentional Electromagnetic Interference from an Antenna,” 2023 Workshop on Attacks and Solutions in Hardware Security, pp. 93-102, 2023.
3) K. Suemitsu, K. Matsuoka, T. Sato and M. Hashimoto, "Logic Locking over TFHE for Securing User Data and Algorithms," ACM/IEEE Asia and South Pacific Design Automation Conference, pp. 600-605, 2024.
4) K. Matsuoka, S. Bian, and T. Sato, “HOGE: Homomorphic gate on an FPGA,” ACM/IEEE Asia and South Pacific Design Automation Conference, pp. 325-332, 2024.