2023 年度年次報告書
基礎理論とシステム基盤技術の融合による Society 5.0 のための基盤ソフトウェアの創出
2023 年度採択研究代表者

原 祐子

東京工業大学 工学院
准教授

Trustworthy IoT システム設計基盤の構築

主たる共同研究者:
岩本 貢（電気通信大学 大学院情報理工学研究科 教授）
崎山 一男（電気通信大学 大学院情報理工学研究科 教授）

研究成果の概要

既存の IP 保護技術は、専用回路の保護を前提（IP 保護のための鍵情報が 1 ビットでも誤れば IP 保護が成立することを前提）としており、汎用システムの IP 保護手法への展開については未検討であった。論文 1)では、汎用システム（組込みマイクロプロセッサ）の正規品をどのように設計すれば、過剰生産や非正規品のコピーなどを防ぐことができるかという新たな問題について取り組んだ。「保護」の定義を再検討することで汎用システムの IP 保護手法について問題提起し、さらに汎用システム上で処理されるアプリケーションへの影響と回路オーバヘッドを定量的に評価した初めての研究であると言う点において、基礎研究の発展に寄与する成果が得られたと考える。また、組込みマイクロプロセッサは IoT 市場において有力なプラットフォームであり、そのような製品の IP 保護は社会的・経済的に重要な課題である。これまで、組込みマイクロプロセッサのような汎用品の保護手法については十分に検討されていなかったが、本研究により一つの効果的かつ実用的な保護手法を提示できたと考えられ、社会・経済への波及効果が期待できる。

また、秘密計算の安全性概念については古くから研究が成されており、スタンダードな手法の一つとしてシミュレーションベース安全性と呼ばれる考え方が知られている。論文 2)では、シミュレーションベース安全性に関して、複数の等価な定式化を情報理論や理論統計の観点から明らかにした。この視点の有効性を明らかにするために、Ben-Or, Goldwasser Wigderson による古典的な秘密計算プロトコルに対して、まったく新しい安全性証明を示した。暗号理論やハードウェアセキュリティの知見を融合した学際的研究であり、安全性の定式化や証明技法についても様々なアプローチを用いる可能性がある。このような安全性証明手法に幅を持たせることで、様々な方向から証明可能安全性をもつ Logic locking の定式化・安全性証明にアプローチできるという点から基礎研究の発展に寄与する成果が得られたと考える。

【代表的な原著論文情報】

1) 一岡 知佑, タンビア アーメド, 原 祐子, "eFPGA を用いた組込みプロセッサの IP 保護," ハードウェアセキュリティ研究会, 2024 年 3 月.

2) M. Iwamoto, “Information-Theoretic Perspectives for Simulation-Based Security in Multi-Party Computation,” IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, E107-A, no. 3, pp. 360-371, 2024. (Invited paper)