研究課題別事後評価結果

１．研究課題名：　IoT 機器の長期的な安全性確保のためのビヨンド軽量暗号の開拓

２．個人研究者名

五十部　孝典（兵庫県立大学大学院応用情報科学研究科　教授）

３．事後評価結果

攻撃者が暗号化プログラムにアクセス可能な環境下においても、復号化プログラム生成と鍵盗難が困難であり、軽量実装と動的機能更新を可能とする共通鍵暗号技術の確立に挑戦する研究である。多種多様な IoT デバイスの安全性や安心性を低コスト（ソフトウェア）でかつ長期的・永久的に保証可能とする高機能軽量共通鍵暗号技術の確立と実環境での効果検証により、IoT セキュリティにおける根本課題の克服を目指した。

IoT 機器の長期的な安全性確保を実現する要素技術として、複製困難性を持つホワイトボックス暗号の設計理論と暗号アルゴリズムの開発に取り組み、当初目標である IoT 向けの軽量暗号の設計や安全性評価を構築し、特に標準暗号 AES の 1/10 遅延、世界最軽量の回路規模と低消費電力性能を実現した点は高く評価できる。更には、企業との共同研究や標準化活動を推進し、具体的な社会実装に向けた成果展開を推進・加速している点も特筆すべき成果である。

研究成果は国内外で評価され、特に暗号分野のトップ国際会議 5 つ（CRYPTO、ASIACRIYT、EUROCRYPT、FSE、CHES）全てへの論文採択、および FSE でのベストペーパ 2 年連続受賞は、世界が認める顕著な成果・業績であり、2023 年文部科学大臣表彰若手科学者賞の受賞を含め、情報セキュリティ・暗号分野のトップランナーとしての飛躍に繋がった。Beyond 5G/6G 向けに軽量暗号技術やホワイトボックス暗号技術の更なる低遅延化・低消費電力化に挑戦する大型研究プロジェクトの獲得・推進や、本さきがけプログラムの研究者と合同で申請・採択された 2024 年度 JST　AIP 加速課題の推進を通じて、研究成果の更なる発展と社会実装の加速化を期待する。