# 研究課題別事後評価結果

１．研究課題名：　バッテリレス無線センサネットワークのためのポスト量子暗号計算技術

２．個人研究者名

上野　嶺（東北大学電気通信研究所　助教）

３．事後評価結果

今後の更なる普及が予想されるバッテリレス無線センサネットワークでの安全性を確保すべく、ポスト量子暗号計算（PQC）技術の確立を目指す研究である。PQC の中でも計算コストの大きい同種写像暗号と格子暗号において、効率的な実行を可能にするための新ハードウェアアルゴリズムを開発し、評価時点において最速となる結果を得たことは高く評価できる。また、PQC のうち鍵交換や認証などに用いられる鍵カプセル化メカニズム（KEM）の実装において、サイドチャネル攻撃により PQC KEM の秘密鍵を詐取できる脆弱性を発見した。NIST PQC 公募コンペティションでの KEM 候補のうち殆どの場合で秘密鍵詐取が可能であることを実験的に示しており、同分野における国際的貢献は極めて大きい。また、従来は実験的評価が主であった深層学習によるサイドチャネル攻撃を対象に、その攻撃能力の数理的解析を進めた。そして、攻撃に必要な波形数を示すなど、攻撃可能性分析に関する新しい方法論を築いた。これは、今後の暗号回路設計に大きな影響を与えるものであるとともに、様々なサイドチャネル攻撃を対象とした標準的な評価基盤への展開が期待できる。PQC のような長期セキュリティを実現する技術ならびにそのサイドチャネル攻撃評価解析は学術的・産業的インパクトが極めて大きく、今後のセキュア・コンピューティングにおける一つの方向性を見せてくれた研究である。当初のターゲットであったバッテリレス無線センサネットワークへの実装と統合を鑑みた場合、より厳しい消費電力制約を満たす必要があり、この観点からも暗号研究者を巻き込んだ大きな成果の創出を期待する。