SICORP　EIG CONCERT-Japan

「レジリエント、安全、セキュアな社会のためのICT**」領域　事後評価報告書**

1　共同研究課題名

「将来社会を支える次世代 IoT のための有機的レジリエント・セキュア無線ネットワーク」

2　日本－相手国研究代表者名（研究機関名・職名は研究期間終了時点）：

日本側研究代表者

石橋 功至（電気通信大学･教授）

ドイツ側研究代表者

ジュゼッペ・アブレウ（ジェイコブス大学ブレーメン･教授）

スペイン側研究代表者

ルイス・エルナンデス＝エンシナス（スペイン国立研究所･上級研究員）

トルコ側研究代表者

カヤ・デミル（トルコ科学技術研究会議･上級研究員）

3　研究概要及び達成目標

本研究は、身の回りのあらゆるデバイスが無線通信によって発信する情報を活用することで、社会や生活の質を向上させる次世代 IoT 時代に向け、レジリエントで安全な無線ネットワークの実現を目指す。今後、きたるべき社会では、量子計算機といった技術の発展により、計算量に依存した既存のセキュリティー技術の安全性を維持できない可能性がある。そこで、量子計算機が普及したポスト量子時代においても安定して高い安全性を実現するために、計算量に依存しない軽量暗号技術、無線通信の特性を活用した物理層セキュリティー、分散型無線アーキテクチャーによるセキュリティーの 3 つを技術的な柱とした研究開発を行なう。ドイツおよび日本側研究者が無線信号処理と分散型アーキテクチャー、トルコおよびスペイン側研究者がポスト量子暗号とハードウェアを中心に担当し、それぞれの知見を有機的に組み合わせることによって、次世代 IoT 技術の脆弱性を解決する。

4　事後評価結果

4.1 研究成果の評価について

4.1.1 研究成果と達成状況

主要な 5 つの課題（WP2～WP5）の内、WP2 のポスト量子・軽量暗号技術、WP3 のセキュアな無線信号処理、WP4 の分散セキュア無線アーキテクチャーに関しては、当初の目標をほぼ達成できたと判断する。WP5 の暗号解読法・トレードオフ解析に関しては、性能面での検討はされたが、安全性解析についての報告がない。

具体的には、WP2 では当初予定していたカオス MIMO 通信方式を再評価し問

題点を明らかにし、新たに非コヒーレント隠ぺい通信技術を提案しその優位性を示すと共に、送信アンテナのランダムホッピングによる情報攪乱を用いたセキュアな通信方式を提案した。WP3 では、セルフリー大規模 MIMO における正規通信者に対して極限までビーム精度を高め、盗聴者に対する信号の漏洩を防ぐプリコーディング手法を検討し、セキュアな通信に加え高い周波数利用効率を達成可能なことを明らかにした。さらに MIMO 通信路において通信路の時間相関と空間相関をマハラノビス距離によって測ることで認証を行う技術を開発した。WP4 では、連合機械学習において学習済みモデルへ雑音を付加することでユーザプライバシ漏洩量の抑制が可能なことに注目し、プライバシレベルと学習精度のトレードオフの改善に向けた学習モデルの適応的合成法を提案し、高信頼化と高速化に向けた改善も提案した。

これらの成果が評価の高い学術論文誌や国際会議において積極的に公表された点は高く評価できる。

一方で、日本側とドイツ側の物理層セキュリティー技術の研究と、スペインのポスト量子暗号、分散鍵配送プロトコルの研究とが相互に連携することでどのような新しい知見に繋がったのかが明らかでない点が惜しまれる。

物理層のセキュリティー技術は特許化に適していることから、特許出願が皆無なのは残念である。

4.1.2 国際共同研究による相乗効果

日本チームとドイツチームは共に無線の物理層セキュリティー技術の研究グループであり、両者間での連携は成果として共著論文に結実しており高く評価できる。

一方において、研究計画申請時より期待されていたのは、ポスト量子暗号における分散鍵配送プロトコルの研究を行ってきたスペインチームと物理層セキュリティーの研究を行ってきた日本とドイツの 2 チームとが、分野に跨った連携を行うことによりもたらされる相乗効果であった。しかし、プロジェクトのワークショップがスペインチームによって 2022 年に開催されたこと以外に、研究面での連携や人材交流の形跡が無く、スペインチームの個別の成果はあるものの、本プロジェクトの目標、並びに物理層セキュリティーとの関連性は希薄である。

トルコチームに関しては、ハードウェア実装と評価・解析が役割であったが、連携の痕跡や成果が報告されていない。

4.1.3 研究成果が与える社会へのインパクト、我が国の科学技術協力強化への貢献

IoT の無線通信の安全性の担保は極めて重要な社会課題である。この課題に、①計算量に依存しない暗号、②無線通信の特性を利用した物理層セキュリティー、③分散型プロトコルによるセキュリティーの 3 つの観点から取り組み、その成果を有機的に組み合わせることで、安定して高い安全性を実現する次世代の IoT 技術基盤を提案することを目指した本プロジェクトは申請時より大きく

期待された。
　無線通信の物理層セキュリティーに関しては、日本とドイツの 2 チームの連携により、優れた成果を多数発表しており、これらは今後、我が国の IoT を用いた社会インフラ等のセキュリティー技術の発展に貢献すると期待できる。提案手法を共有し広く評価に資するために、これらの一部を実装し GitHub に公開したことは高く評価できる。
　一方で、ポスト量子暗号の分散鍵配送プロトコルが IoT 通信とどのように関連し新しい技術展開をもたらし得るのかに関して大きな期待があったが、スペインチームとの連携が不十分であったことから期待に見合う成果を得るには至っていない。別途、日本とドイツのチームが連携して、量子アルゴリズムの新提案論文を準備中であるが、これは上記の課題とは別の問題を扱っている。

4.2 相手国研究機関との協力状況について

　4.1.2 と 4.1.3 にも述べたように、ドイツチームと日本チームは研究内容が類似していることから期間中並びに終了後も良好に連携し効果を上げている。
　ワークショップの開催と人材交流は、コロナ禍の影響が否めないが、充分とは言えない。オンラインでの開催や打ち合わせなど、工夫すべき点があったと考える。
　スペインチームとの連携は、スペインでのワークショップ開催に繋がったが、個別に研究が行われた感があり、分野に跨る連携による相乗効果が得られていない。トルコチームの貢献の成果が伺えない点は残念である。

4.3 その他

　特になし