

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

「ポスト量子暗号プロトコルの形式解析・検証」

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

緒方 和博（北陸先端科学技術大学院大学・教授）

スペイン側研究代表者

サンティアゴ・エスコバ（バレンシア工科大学・准教授）

フランス側研究代表者

アユブ・オトマニ（ルーアンノルマンディー大学・教授）

トルコ側研究代表者

スダット・アクアラク（オンドクズマユス大学・准教授）

3 研究概要及び達成目標

本研究は、ポスト量子時代を見据え、暗号システムの代数的特性を考慮可能な暗号セキュリティープロトコルの解析ツールである **Maude-NPA** を使用して、ポスト量子暗号プロトコルを形式解析する方法を考案することを目的とする。これまではポスト量子暗号プロトコルの形式解析ツールは知られておらず、ポスト量子暗号システムの形式解析についても深く研究されていない。本研究では、検索と決定問題、および代数的手法のさまざまな解釈に基づき、格子ベースとコードベースに基づくポスト量子暗号プロトコルの形式解析のため、**Maude-NPA** を適切に拡張する。本研究の成果は、本公募のスコープの **1** つであるサイバー攻撃の防止と回復を含む、ポスト量子時代を考慮したサイバーセキュリティに本質的に貢献する。

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

来たる量子コンピューティングの時代に向けて、相手側からポスト量子暗号の最新動向を入手し、日本側が形式手法でプロトコルを記述し論理的分析を効率的に実施し検証を達成するなど、当初計画に沿って国際的にも高い研究成果を挙げ、国際トップジャーナル等へ多くの論文を公表した点は高く評価できる。

標準化候補のプロトコルに形式検証を適用し、問題点の発見や改定案につなげた。形式検証の並列化による高速化にも取り組み、ツール開発も行った。これらの点も高く評価できる。

トップジャーナルを目指した故に期間内に査読が終了しなかった論文が複数ある点は残念であるがやむを得ないと考える。

特許の出願に関しては、成果のトップジャーナルへの公表に重点を置いたことから、現時点では計画されていない点が残念である。

以上の理由により、当初目標は十分に達成されたと判断する。

4.1.2 国際共同研究による相乗効果

相手側はポスト量子暗号プロトコルの研究を先導する研究グループであり、日本側は形式的に記述された仕様の解析・検証を行う形式手法の研究者である。前者が後者にポスト量子暗号プロトコルの最新動向をレクチャし、後者がこれを形式記述し解析検証するという役割分担で共同研究が行われた。前者にとっては形式検証の手法とツールを得ることができ、後者にとっては今後重要となるポスト量子暗号の分野に形式手法を適用し、当初のプロトコルの問題点を発見して改善を促し、その安全性を理論的に保証するという重要な貢献に繋がった。

このような連携を繰り返すことにより、ポスト量子暗号プロトコルの研究現場にどのような波及効果が生まれたかについてもより具体的な報告が望まれる。

それぞれの分野において国際的なトップランナーが、異なる分野に跨って連携することによって、このような今後の社会に重要な課題に対して、安全性の理論的保証を行う方法論の構築に重要な一步を踏み出したことは、本プログラムの趣旨を反映した相乗効果に繋がったと評価できる。

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

現在盛んに研究開発がなされている量子コンピュータが実用化されれば、現状では安全であるとして広く利用されている RSA 等の公開鍵暗号は安全ではなくなる。この重大な問題に答えるべく、ポスト量子暗号の研究が進められているが、そのプロトコルの安全性がどのように保証できるのかは重大な課題である。

本プロジェクトでは、ポスト量子暗号プロトコルの国際標準化にも携わる相手側チームが、日本の形式検証の専門家と組んで、ポスト量子暗号のプロトコルの安全性を形式検証手法に基づいて理論的に与える方法を先駆的に具体的に示した。量子コンピュータの実用化が迫っている現在の社会における最大の脅威の一つである暗号の安全性保証に関して、重要な第 1 歩の貢献となる成果をもたらしたと評価できる。

4.2 相手国研究機関との協力状況について

国際ワークショップを 2022 年と 2023 年にマドリードとブリスベンで開催し、国際学術誌と国際会議に共著論文を各々 4 報と 7 報出すなど、異なる分野の相手側チームとの連携による相乗効果が成果にも反映されている。一方で、コロナ禍の影響もあるが、相手側チームの日本チーム訪問や、相互の若手人材の短中期派遣の実績がないのは残念である。プロジェクト終了後も連携の継続が確認されており、予算獲得に向けて協力がなされている点は望ましいことで

ある。

4.3 その他

特になし