日本―スペイン、トルコ、フランス 国際共同研究「レジリエント、安全、セキュアな社会のための ICT」 2021 年度　年次報告書	
研究課題名（和文）	ポスト量子暗号プロトコルの形式解析・検証
研究課題名（英文）	Formal Analysis and Verification of Post-Quantum Cryptographic Protocols (FAVPQC)
日本側研究代表者氏名	緒方　和博
所属・役職	北陸先端科学技術大学院大学・教授
研究期間	2021 年 4 月 1 日～2024 年 3 月 31 日

1．日本側の研究実施体制

氏名	所属機関・部局・役職	役割
緒方和博	北陸先端科学技術大学院大学 先端科学技術研究科 教授	研究全般

2．日本側研究チームの研究目標及び計画概要

本研究で使用予定の支援ツール Maude-NPA とポスト量子暗号の調査を実施する。ポスト量子暗号については、アメリカ国立標準技術研究所（NIST）により手続きが進められている標準化案に注視しつつ、最新動向について報告書としてまとめる予定である。Maude-NPA に関しては、初学者も Maude-NPA を使うことが可能になることを目指したチュートリアル資料を作成予定である。

3. 日本側研究チームの実施概要

主に 2021 年度は以下のことを実施した。: (1) 格子問題の困難さに基づく鍵交換方式（lattice-based KEM）の調査と Maude による形式仕様作成・モデル検査、(2) Maude-NPA の調査と並列化、(3) 認証プロトコルの CafeOBJ を用いた形式検証の再構築。
(1) アメリカ国立標準技術研究所が進めているポスト量子暗号プリミティブの標準化案の公募に応募されたポスト量子鍵交換方式の中で有力と思われている lattice-based KEM である Kyber、Saber、MLWR、BIKE について調査した。理解を深めること等を目的に、侵入者の存在を仮定すると共にこれらの lattice-based KEM の形式仕様を書換え論理に基づく形式仕様言語 Maude で作成し、2 者間で交換する鍵（秘密情報）が侵入者に漏れることがないかどうかについてのモデル検査を行った。モデル検査の結果、中間者攻撃により鍵が侵入者に漏れる可能性があることを再現することが出来た。漏れる理由は認証の機能を有していないためである。鍵が漏れること、理由が認証の機能を有していないことは既知であるが、形式仕様を作成しモデル検査で中間者攻撃を再現したことは新規である。このため、調査結果をまとめるに留まらず論文を執筆した。Kyber のモデル検査等についてまとめた論文は国際ワークショップ WRLA 2022 に work-in-progress 論文として、Saber のモデル検査等についてまとめた論文は国際会議 SEKE 2022 に short 論文として採録された。共に欧州側 <スペイン> <トルコ> <フランス> との国際共著論文である。
(2) 暗号プロトコルの解析・検証を目的とした支援ツールである Maude-NPA について調査すると共に並列化した。Maude-NPA は、解析・検証対象であるプロトコルの状態を表現する式（項）に変数を含むことを許し、無限の参加者やセッションを扱うことを可能とし、攻撃状態から出発し後ろ向きに（パタンマッチではなく）ユニフィケーションを用いる書換え（ナローイング）を用いて解析・検証を行う。解析・検証途中で一般に複数の項の各々に対し 1 ステップのナローイングを行う。複数の項を順番に処理するのではなく同時に処理することで並列化した。Maude-NPA を用いて解析・検証された暗号プロトコルに対し並列化 Maude-NPA を用いて解析・検証をすることで約 30%の処理速度の向上を図ることが出来ることが分かった。調査結果をまとめるに留まらず、並列化 Maude-NPA について論文としてまとめた。まとめた論文は WRLA 2022 に regular 論文として採録された欧州側 <スペイン> との国際共著論文である。WRLA 2022 の proceedings は Springer 社の Lecture Notes in Computer Science（LNCS）として出版される予定で論文はそこに収録される。Maude-NPA の開発チームである欧州側 <スペイン> によりチュートリアル論文が執筆されていると共に Maude-NPA による多数の暗号プロトコルの形式仕様及び解析・検証の事例を記載したウェブサイトが準備されたため、日本側ではチュートリアルを作成するのではなく上述した研究論文を執筆した。
(3) 認証プロトコル NSLPK（NSPK の Lowe による改善案）と TLS 1.0 が秘匿性などの所望の性質を満たすことの形式検証（定理証明）を代数仕様言語 CafeOBJ で証明の計画である証明スコアを記述することで再構築すると共に証明スコアの正しさを確認した。証明スコアは、プログラムを記述するのと同じように証明の計画を記述できるという柔軟性に優れている反面、ヒューマンエラーの影響を避けることが出来ないという弱点を有している。これを改善するため、CafeOBJ 用の証明支援系 CafeInMaude Proof Assistant (CiMPA)と証明生成系 CafeInMaude Proof Generator (CiMPG)が開発されている。CafeInMaude は、Maude を実装言語とする世界で 2 番目の CafeOBJ の処理系である。CiMPG は、証明スコアを入力とし、CiMPA 用の証明スクリプトを生成する。生成された証明スクリプトが CiMPA により証明を完了させることで証明スコアの正しさを確認する。NSLPK と TLS 1.0 が所望の性質を満たすことの形式検証を行うための証明スコアの正しさを CiMPG と CiMPA を用いて確認した。NSLPK に関する研究結果をまとめた論文は SEKE 2021 に short 論文として採録された。TLS 1.0 に関する研究結果をまとめた論文は国際学術誌に投稿予定である。形式検証（定理証明）で必要になる補題を探すことを目的に状態機械のグラフィカルアニメーション（GA）作成支援ツール SMGA が開発されている。NSLPK を形式化した状態機械の GA を SMGA で作成した。この研究成果をまとめた論文は国際会議 DMSVIVA 2021 に short 論文として採録されると共に拡張版は国際学術誌 JVLC に採録された。