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」 2022 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（FAVPQC）
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
Duong Dinh Tran	北陸先端科学技術大学院大学・先端科学技術研究科・博士後期課程学生	ポスト量子 TLS の調査、ポスト量子 TLS の形式検証事例研究、侵入者に関する新たな仮定の発見
Canh Minh Do	北陸先端科学技術大学院大学・先端科学技術研究科・博士後期課程学生	Maude-NPA の並列化と並列化の有効性確認のため事例研究
Thet Wai Mon	北陸先端科学技術大学院大学・先端科学技術研究科・博士後期課程学生	ポスト量子 TLS の形式検証事例研究

2．日本側研究チームの研究目標及び計画概要

ポスト量子暗号プロトコルの解析・検証で用いることのできる（用いるべき）侵入者モデルを考案するための足掛かりを作ることが一番の目標である。それに向け、ポスト量子 TLS を調査し、従来の侵入者モデルに加え、従来の鍵交換方式を破ることができるという仮定を加え、ポスト量子 TLS が秘匿性等の性質を満たすことを形式検証する。欧州側と協力して追加すべき仮定を探し、その下で形式検証を行う。これにより妥当と思われる仮定

を絞り込む。複雑なポスト量子暗号プロトコルの解析・検証に備え Maude-NPA を並列化する。

3. 日本側研究チームの実施概要

暗号の専門家である欧州側（トルコ、フランス）のポスト量子暗号プロトコル（主にポスト量子 TLS）の調査結果等を基に、形式検証の対象とするポスト量子 TLS を選択し、形式仕様を作成可能になる程度に理解を深める。

TLS は、インターネットでの安心・安全な通信を担保するために広く使われている暗号プロトコルである。量子計算機実用化後にも安心・安全な通信を持続可能にするため、マイクロソフト社やアマゾンウェブサービス社等によりポスト量子 TLS の開発が進められている。ポスト量子 TLS に焦点をあてるのはこのような理由のためである。

量子計算機が実用化されるとディフィー・ヘルマン等の従来の鍵交換方式等の暗号の基本機能が解読可能になることが知られている。ポスト量子 TLS では、従来の TLS との互換性のため、ポスト量子鍵交換方式と従来の鍵交換方式が使われている。ポスト量子 TLS が秘密情報の秘匿性等の性質を満たすことの形式検証の際に、侵入者に関する従来の仮定（たとえば、ネットワークを流れるメッセージはすべて盗聴可能）に加え、従来の鍵交換方式は解読可能であるという仮定も考慮する。ディフィー・ヘルマンや RSA 等の公開鍵暗号が解読可能になるのは、ショアの考案した素因数分解を高速に解くことのできる量子アルゴリズムのためである。グローバーの考案した逆関数を高速に求めることのできる量子アルゴリズムを用いると、秘密鍵暗号の解読も高速に行える。

ただし、前者への対応は新たなポスト量子鍵交換方式を考案する必要があるが、後者には鍵の長さを 2 倍にすることで可能である。形式検証の際に、後者への対応ができない利用者がいるという仮定を置くことは、実世界で起きたこと（たとえば、SSL/TLS のダウングレード攻撃）を顧みると現実的ではない。このような仮定の下での意味のある問は、対応のできている利用者への悪影響の有無である。悪影響が無いことを性質として記述し、ポスト量子 TLS がこの性質を満たすことを形式検証する。

これまでに考案された量子アルゴリズムは、Quantum Algorithm Zoo というウェブサイトで公開されている。これを参考に、ポスト量子 TLS で使われている暗号の基本機能（たとえば、疑似乱数生成）を解読することを可能とする量子アルゴリズムが存在するかどうかを調べると共に、鍵の長さを 2 倍にする等の自明な対応方法の有無を調べる。この調査から、侵入者に関する新たな仮定と関連する意味のある問を見つけて形式検証を実施することを繰り返し行う。このように見つけた新たな仮定（と関連する意味のある問、あるいはその問から得られる性質）のあつまりが、ポスト量子暗号プロトコルの解析・検証で用いることのできる（用いるべき）侵入者モデルを考案するための足掛かりである。

ポスト量子暗号プロトコルは従来の暗号プロトコルより複雑であり、解析・検証により多くの時間を費やすことが容易に想像できる。このことに備え、欧州側（スペイン）で開発された暗号プロトコル解析・検証用ツールの Maude-NPA を並列化する。そのため、欧州側（スペイン）から実装の詳細情報等の提供を予定する。