戦略的国際共同研究プログラム(SICORP)
EIG CONCERT-Japan 共同研究
終了報告書　概要

1. 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. 研究期間：令和 3 年 4 月～令和 6 年 3 月
3. 主な参加研究者名：

日本側チーム

	氏名	役職	所属	研究分担
研究代表者	緒方　和博	教授	北陸先端科学技術大学院大学	日本側の担当する研究全般
研究参加者	Canh Minh Do	助教	北陸先端科学技術大学院大学	ツール作成・事例研究
研究参加者	Duong Dinh Tran	ポスドク	北陸先端科学技術大学院大学	ツール作成・事例研究
研究参加者	Thet Wai Mon	学生	北陸先端科学技術大学院大学	事例研究
研究期間中の全参加研究者数		4名		

相手側（スペイン・フランス・トルコ）チーム

	氏名	役職	所属	研究分担
研究代表者	Santiago Escobar	教授	Technical University of Valencia	研究全般
主たる共同研究者	Sedat Akleylek	准教授	Ondokuz Mayis University	ポスト量子暗号の調査研究
主たる共同研究者	Ayoub Otmani	教授	University of Rouen Normandie	ポスト量子暗号の調査研究
研究参加者	Víctor García	学生	Technical University of Valencia	事例研究
研究参加者	Kubra Seyhan	学生	Ondokuz Mayis University	ポスト量子暗号の調査研究
研究期間中の全参加研究者数		5名		

4. 国際共同研究の概要

実用規模量子コンピュータが現れると、今の公開鍵暗号方式（PKC）のほぼすべてが安全安心に利用できなくなる。Shor のアルゴリズムのためである。米国立標準技術研究所は、2031 年までに RSA-2048 が破られる可能性を 50%と見立てている。数年残っているが、「今は暗号文を収集し、後に解読する」という攻撃が知られている。この攻撃による影響をなるべく小さくするにはなるべく早くに量子コンピュータに耐性のある PKC（PQ-PKC）に切替えるべきであると周知すると共に PQ-PKC の標準化を定める手続きを進めている。本研究では、まず、PQ-PKC の理解を深めることを目的に、標準化の候補である Kyber や Saber 等の形式仕様を Maude で作成し、認証機能を有していなければ中間者攻撃を受け得ることをモデル検査により再確認した。続いて Maude-NPA や CafeOBJ を用いて PQ-PKC と従来の PKC とを併用することで耐量子性を持たせた上位のセキュリティプロトコルである Transport Layer Security（TLS）と Secure Shell（SSH）を対象に形式仕様を作成し所望のセキュリティに関する性質を有することの形式検証を実施した。2 つの方式を併用するそのようなプロトコルを PQ TLS と PQ SSH と呼ぶ。PQ SSH の形式検証では、認証性を有していないことを発見、改定案を提案、改定案が認証性を含めすべての性質を有していることを形式検証した。事例研究をとおして PQ セキュリティプロトコルの形式仕様作成・形式

検証実施のための手順を方法論としてまとめた。Maude-NPA による形式検証を高速化するために並列化したり、CafeOBJ による形式検証（証明スコア法）をより自動化するためのツールも開発した。MaudeやCafeOBJは代数仕様言語に分類されると共に姉妹言語であり、Maude-NPA は Maude を拡張することで開発されたプロトコル解析・検証用ツールである。

5. 国際共同研究の成果

5-1 国際共同研究の学術成果および実施内容

日本側と欧州側＜スペイン＞を中心に、欧州側＜トルコ＞＜フランス＞にも協力してもらい、Kyber や Saber 等の NIST の標準化の候補として残っている耐量子公開鍵暗号方式の形式仕様（形式モデル）を代数仕様言語である Maude を用いて作成し、Maude のモデル検査機能を用いて、耐量子であったとしても認証の機能を持っていなければ中間者攻撃を受け得る可能性があることを確認した。Maude を拡張することで開発されたセキュリティプロトコル形式解析・検証ツールである Maude-NPA の弱みである実行性能改善のため Maude-NPA の並列版を開発し実行性能改善に貢献できたことを確認した。PQ-PKC と従来の PKC を併用する SSH（PQ SSH）と TLS（PQ TLS）の形式仕様を、量子コンピュータを利用可能な攻撃者を仮定し、CafeOBJ で作成し、証明スコア法と呼ばれる定理証明法により所望の性質も満たすことを形式検証した。形式検証では、補題発見を除き証明スコア法を自動化する（本研究内で開発した）支援ツール IPSG を用いた。形式検証の結果、PQ SSH は認証性を満たさないことが分かった。理由は、ハッシュ値を求めるのにサーバとクライアントの識別子を用いていないためだった。用いるように改訂した PQ SSH は他の所望の性質に加え認証性も満たすようになったことが証明スコア法により明らかになった。

5-2 国際共同研究による相乗効果

2名の暗号の専門家と2名の形式手法の専門家が専門性をいかして研究を遂行したことが功を奏したと言える。日本国内のみでも同様の研究チームを組むことも不可能では無いと思うが、日本国内の研究者数と世界の研究者数とでは絶対数に大きな差がある。世界の研究者を対象に目的を共有した研究者同士でチームを組み研究を遂行したほうが研究を成功に導く可能性は大きくなるであろう。

5-3 国際共同研究成果の波及効果と今後の展望

日本側の研究参加者である Canh Minh Do は、本研究開始当時博士後期課程の学生であったが、本研究期間中に博士（情報科学）を取得し、ポスドク研究者を経由し、北陸先端科学技術大学院大学の助教に就くことができた。今後サイバーセキュリティの価値は益々重要になり、セキュリティプロトコルが所望の性質を満たすことを担保する技術も一層重要になることは技術革新や社会情勢からして自然な流れである。北陸先端科学技術大学院大学と Technical University of Valencia は、セキュリティプロトコルの形式解析・検証の世界的拠点である。両大学が切磋琢磨することでこの分野のより高みを目指すことが可能になる。このため、Santiago Escobar との協同研究や Technical University of Valencia との交流は継続したいと望んでいると共に新たな国際共同研究を提案していくようにする。

Strategic International Collaborative Research Program (SICORP)
EIG CONCERT-Japan Joint Research Program
Executive Summary of Final Report

1. Project title：Formal Analysis and Verification of Post-Quantum Cryptographic Protocols
2. Research period：April 2021 ～ March 2024
3. Main participants：

Japan-side

	Name	Title	Affiliation	Role in the research project
PI	Kazuhiro Ogata	Professor	Japan Advanced Institute of Science and Technology	All aspects of the research by Japan-side
Collaborator	Canh Minh Do	Assistant Professor	Japan Advanced Institute of Science and Technology	Tool development & case studies
Collaborator	Duong Dinh Tran	Postdoc	Japan Advanced Institute of Science and Technology	Tool development & case studies
Collaborator	Thet Way Mon	Student	Japan Advanced Institute of Science and Technology	Case studies
Total number of participants throughout the research period： 4				

Partner（Spain, France, Turkey）-side

	Name	Title	Affiliation	Role in the research project
PI	Santiago Escobar	Professor	Technical University of Valencia	All aspects of the research in the joint project
Co-PI	Sedat Akleylek	Associate Professor	Ondokuz Mayis University	Investigation of post-quantum cryptography
Co-PI	Ayoub Otmani	Professor	University of Rouen Normandie	Investigation of post-quantum cryptography
Collaborator	Víctor García	Student	Technical University of Valencia	Case studies
Collaborator	Kubra Seyhan	Student	Ondokuz Mayis University	Investigation of post-quantum cryptography
Total number of participants throughout the research period： 5				

4. Summary of the international joint research

When practical-scale quantum computers (QCs) emerge, almost all current public-key cryptosystems (PKCs) will no longer be able to be used securely. This is due to Shor's algorithm. NIST estimates that there is a 50% chance that RSA-2048 will be broken by 2031. Although several years remain, there is a known attack that harvests ciphertexts now and decrypts them later, and to minimize its impact, it is necessary to develop PKCs (PQ-PKCs) that are resistant to QCs ASAP, and NIST has been standardizing PQ-PKCs. In this research, to comprehend PQ-PKCs, we first formally specified in Maude some PQ-PKCs,

such as Kyber and Saber, and reconfirmed with model checking that they are subject to man-in-the-middle attacks. We next used Maude-NPA and CafeOBJ to formally specify quantum-resistant upper-level security protocols, such as Transport Layer Security (TLS) and Secure Shell (SSH), which use both PQ-PKCs and conventional PKCs, and formally verified that they enjoy desired properties. In the formal verification of PQ SSH, we found that it does not enjoy authentication properties, proposed a revised version of PQ SSH, and formally verified that the revised version enjoys authentication properties as well as all desired properties. We then came up with a methodology with which PQ security protocols can be formally specified and verified. We have also parallelized Maude-NPA to speed it up, and developed a tool called IPSG that almost automates the formal verification technique called the proof score method in CafeOBJ. Maude and CafeOBJ are algebraic specification languages and sibling languages, and Maude-NPA is a protocol analysis and verification tool developed by extending Maude.

5. Outcomes of the international joint research

5-1 Scientific outputs and implemented activities of the joint research

The Japan side and the EU side (Spain), together with the EU sides (Turkey and France), formally specified in Maude some post-quantum (PQ) public-key cryptosystems, such as Kyber and Saber, and reconfirmed with model checking that they are subject to man-in-the-middle attacks. Maude-NPA is an extension of Maude to formally verify security protocols. One weakness is to take time to formally verify large protocols. To mitigate it, Maude-NPA has been parallelized. The Japan side and the EU side (Spain) also formally specified in CafeOBJ PQ SSH and TLS in which both PQ key exchange mechanisms and classical key-exchange ones are used, and formally verified with the proof score method in CafeOBJ that they enjoy desired properties. The formal verification used a tool called IPSG (developed within this research), which automates the proof score method except for lemma conjecture. In the formal verification of PQ SSH, it was fund that PQ SSH does not enjoy authentication properties. PQ SSH was revised. The formal verification was successfully carried out, showing that the revised version enjoys authentication properties as well as all other security properties with IPSG and CafeOBJ.

5-2 Synergistic effects of the joint research

The research was successful because two cryptographic experts from Turkey and France and two formal methods experts from Japan and Spain played their own roles. It might be possible to form a similar research team within Japan. Because there is a big difference between the number of researchers in Japan and the one of those in the world, however, research will be much more likely to be successful if researchers from all over the world with a shared goal form a team to conduct the research.

5-3 Scientific, industrial or societal impacts/effects of the outputs

Canh Minh Do, a research participant on the Japan side, was a doctoral student at the start of this research. He took a doctoral degree in Information Science from JAIST, worked as a postdoc researcher for the research, and finally became an assistant professor of JAIST during the research period. JAIST and Technical University of Valencia are world-class centers for formal analysis and verification of security protocols. Both universities will be able to aim for greater heights in this field by working hard together. Therefore, we hope to continue our collaboration with Santiago Escobar and our exchange with the Technical University of Valencia from a JAIST point of view, and will also propose new international joint research projects.

国際共同研究における主要な研究成果リスト

1. 論文発表等

＊原著論文（相手側研究チームとの共著論文）発表件数：計 11 件
・査読有り：発表件数：計 10 件

[1] Canh Minh Do, Adrián Riesco, Santiago Escobar and Kazuhiro Ogata: Parallel Maude-NPA for Cryptographic Protocol Analysis, 14th International Workshop on Rewriting Logic and its Applications (WRLA 2022), Springer LNCS 13252, pp.253-273
10.1007/978-3-031-12441-9_13

[2] Duong Dinh Tran, Kazuhiro Ogata, Santiago Escobar, Sedat Akleylek, Ayoub Otmani: Formal specification and model checking of Saber lattice-based key encapsulation mechanism in Maude, 34th International Conference on Software Engineering & Knowledge Engineering (SEKE 2022), pp.382-387 (Open Access)
10.18293/SEKE2022-097

[3] Víctor García, Santiago Escobar, Kazuhiro Ogata: Modeling and verification of the post-quantum key encapsulation mechanism KYBER using Maude, International Workshop on Formal Analysis and Verification of Post-Quantum Cryptographic Protocols 2022 (FAVPQC 2022), CEUR Workshop Proceedings 3280, pp.32—49 (Open Access)
ceur-ws.org/Vol-3280/paper3.pdf

[4] Duong Dinh Tran, Canh Minh Do, Santiago Escobar and Kazuhiro Ogata: Hybrid Post-Quantum TLS formal specification in Maude-NPA - toward its security analysis, International Workshop on Formal Analysis and Verification of Post-Quantum Cryptographic Protocols 2022 (FAVPQC 2022), CEUR Workshop Proceedings 3280, CEUR-WS.org, pp.50--64 (Open Access)
ceur-ws.org/Vol-3280/paper4.pdf

[5] Duong Dinh Tran, Canh Minh Do, Santiago Escobar and Kazuhiro Ogata: Hybrid Post-Quantum TLS formal specification in Maude-NPA - toward its security analysis, International Workshop on Formal Analysis and Verification of Post-Quantum Cryptographic Protocols 2022 (FAVPQC 2022), CEUR Workshop Proceedings 3280, CEUR-WS.org, pp.50—64 (Open Access)
ceur-ws.org/Vol-3280/paper4.pdf

[6] Duong Dinh Tran, Kazuhiro Ogata, Santiago Escobar, Sedat Akleylek, Ayoub Otmani: Kyber, Saber, and SK-MLWR Lattice-Based Key Encapsulation Mechanisms Model Checking with Maude, IET Information Security 2023: 9399887 (1-17), Hindawi (2023) (Open Access)
10.1049/2023/9399887

[7] Víctor García, Santiago Escobar, Kazuhiro Ogata: Modelling and verification of post-quantum key encapsulation mechanisms using Maude. PeerJ Comput. Sci. 9: e1547 (2023) (Open Access)
10.7717/peerj-cs.1547

[8] Duong Dinh Tran, Canh Minh Do, Santiago Escobar, Kazuhiro Ogata: Hybrid post-quantum Transport Layer Security formal analysis in Maude-NPA and its parallel version. PeerJ Comput. Sci. 9: e1556 (2023) (Open Access)
10.7717/peerj-cs.1556

[9] Víctor García, Santiago Escobar and Kazuhiro Ogata: Formal specification of the post-quantum signature scheme FALCON in Maude, 2nd International Workshop on Formal

Analysis and Verification of Post-Quantum Cryptographic Protocols (FAVPQC 2023), JAIST Press, pp.1-16, (2023) (Open Access)
hdl.handle.net/10119/18811

[10] Duong Dinh Tran, Kazuhiro Ogata and Santiago Escobar: A formal analysis of OpenPGP's post-quantum public-key algorithm extension, 2nd International Workshop on Formal Analysis and Verification of Post-Quantum Cryptographic Protocols (FAVPQC 2023), JAIST Press, pp.17-35, (2023) (Open Access)
hdl.handle.net/10119/18811

[11] Duong Dinh Tran, Kazuhiro Ogata, Santiago Escobar, Sedat Akleylek, Ayoub Otmani: Formal analysis of Post-Quantum Hybrid Key Exchange SSH Transport Layer Protocol, IEEE Access 12: 1672-1687, IEEE, (2024) (Open Access)
10.1109/ACCESS.2023.3347914

・査読無し：発表件数：計 0 件
該当無し

＊原著論文（相手側研究チームを含まない日本側研究チームの論文）：発表件数：計 6 件
・査読有り：発表件数：計 6 件

[12] Thet Wai Mon, Dang Duy Bui, Duong Dinh Tran, Canh Minh Do, Kazuhiro Ogata、Graphical Animations of the NS(L)PK Authentication Protocols, Journal of Visual Language and Computing 、 2021、2、39-51、 2021 (Open Access)
10.18293/JVLC2021-N2-005

[13] Thet Wai Mon, Dang Duy Bui, Duong Dinh Tran, Kazuhiro Ogata、 Graphical Animations of the NSLPK Authentication Protocol、 Proceedings of 27th International DMS Conference on Visualization and Visual Languages (DMSVIVA 2021)、29-35、2021 (Open Access)
10.18293/DMSVIVA2021-005

[14] Thet Wai Mon, Shuho Fujii, Duong Dinh Tran, Kazuhiro Ogata: Formal verification of IFF & NSLPK authentication protocols with CiMPG, Proceedings of 33rd International Conference on Software Engineering and Knowledge Engineering (SEKE 2021)、120-125, 2021 (Open Access)
10.18293/SEKE2021-037

[15] Duong Dinh Tran, Kazuhiro Ogata: IPSG: Invariant Proof Score Generation, 5th International Workshop on Advances in Artificial Intelligence and Machine Learning (AIML 2022): Towards Trustworthy AI, IEEE, pp.1050-1055 (2022)
0.1109/COMPSAC54236.2022.00164

[16] Duong Dinh Tran, Kazuhiro Ogata: Formal verification of TLS 1.2 by automatically generating proof scores, Computers & Security 123: 102909 (1 - 15), Elsevier, (2022) (Open Access)
10.1016/j.cose.2022.102909

[17] Duong Dinh Tran, Thet Wai Mon, Kazuhiro Ogata: Transport Layer Security 1.0 handshake protocol formal verification case study: How to use a proof script generator for existing large proof scores, PeerJ Computer Science 9:e1284 (1-25) PeerJ, (2023) (Open Access)
10.7717/peerj-cs.1284

・査読無し：発表件数：計 0 件
該当無し

＊その他の著作物（相手側研究チームとの共著総説、書籍など）：発表件数：計 2 件
[18] Sedat Akleylek, Santiago Escobar, Kazuhiro Ogata, Ayoub Otmani: Proceedings of the International Workshop on Formal Analysis and Verification of Post-Quantum Cryptographic Protocols co-located with the 23rd International Conference on Formal Engineering Methods (ICFEM 2022), Madrid, Spain, October 24, 2022. CEUR Workshop Proceedings 3280, CEUR-WS.org, 2022. (Open Access)
ceur-ws.org/Vol-3280/

[19] Sedat Akleylek, Santiago Escobar, Kazuhiro Ogata, Ayoub Otmani: Proceedings of the 2nd International Workshop on Formal Analysis and Verification of Post-Quantum Cryptographic Protocols co-located with the 24th International Conference on Formal Engineering Methods (ICFEM 2023), Brisbane, Autoralia, November 21, JAIST Press, 2023. (Open Access)
hdl.handle.net/10119/18811

＊その他の著作物（相手側研究チームを含まない日本側研究チームの総説、書籍など）：発表件数：計 0 件
該当無し

2. 学会発表

＊口頭発表（相手側研究チームとの連名発表）
発表件数：計 6 件（うち招待講演：0 件）
[20] Canh Minh Do, Adrián Riesco, Santiago Escobar and Kazuhiro Ogata: Parallel Maude-NPA for Cryptographic Protocol Analysis, 14th International Workshop on Rewriting Logic and its Applications (WRLA 2022) (a satellite event of ETAPS 2022), April 2-3, Munich, Germany, Presented online by Canh Minh Do

[21] Duong Dinh Tran, Kazuhiro Ogata, Santiago Escobar, Sedat Akleylek, Ayoub Otmani: Formal specification and model checking of Saber lattice-based key encapsulation mechanism in Maude, 34th International Conference on Software Engineering & Knowledge Engineering (SEKE 2022), July 1 - July 10, 2022, Online, Presented by Duong Dinh Tran

[22] Víctor García, Santiago Escobar, Kazuhiro Ogata: Modeling and verification of the post-quantum key encapsulation mechanism KYBER using Maude, International Workshop on Formal Analysis and Verification of Post-Quantum Cryptographic Protocols 2022 (FAVQC 2022) (a satellite event of ICFEM 2022), Oct 24, 2022, Madrid, Spain, Presented in person by Santiago Escobar

[23] Duong Dinh Tran, Canh Minh Do, Santiago Escobar and Kazuhiro Ogata: Hybrid Post-Quantum TLS formal specification in Maude-NPA - toward its security analysis, International Workshop on Formal Analysis and Verification of Post-Quantum Cryptographic Protocols 2022 (FAVQC 2022) (a satellite event of ICFEM 2022), Oct 24, 2022, Madrid,

Spain, Presented in person by Canh Minh Do

[24] Víctor García, Santiago Escobar and Kazuhiro Ogata: Formal specification of the post-quantum signature scheme FALCON in Maude, 2nd International Workshop on Formal Analysis and Verficiation of Post-Quantum Cryptographic Protocols (FAVPQC 2023), Nov 21, 2023, Brisbane, Australia, Presented online by Víctor García

[25] Duong Dinh Tran, Kazuhiro Ogata and Santiago Escobar: A formal analysis of OpenPGP's post-quantum public-key algorithm extension, 2nd International Workshop on Formal Analysis and Verficiation of Post-Quantum Cryptographic Protocols (FAVPQC 2023) (a satellite event of ICFEM 2023), Nov 21, 2023, Brisbane, Australia, Presented in person by Duong Dinh Tran

＊口頭発表（相手側研究チームを含まない日本側研究チームの発表）

発表件数：計 6 件（うち招待講演：2 件）

[26] Thet Wai Mon, Dang Duy Bui, Duong Dinh Tran, Kazuhiro Ogata: Graphical Animations of the NSLPK Authentication Protocol、 Proceedings of 27th International DMS Conference on Visualization and Visual Languages (DMSVIVA 2021), June 29-30, 2021, Online, Presented by Thet Wai Mon

[27] Thet Wai Mon, Shuho Fujii, Duong Dinh Tran, Kazuhiro Ogata: Formal verification of IFF & NSLPK authentication protocols with CiMPG, Proceedings of 33rd International Conference on Software Engineering and Knowledge Engineering (SEKE 2021), July 1 - July 10, 2021, Online, Presented by Thet Wai Mon

[28] Duong Dinh Tran, Kazuhiro Ogata: IPSG: Invariant Proof Score Generation, 5th International Workshop on Advances in Artificial Intelligence and Machine Learning (AIML 2022) (a satellite event of COMPSAC 2022), June 27 - July 1, 2022, Online, Presented by Duong Dinh Tran

[29] Kazuhiro Ogata: A proof score approach to security protocol formal verification, Vietnam-JapanAutumn School on Cyber Security, Academy of Cryptography Techniques, Hanoi, Oct. 15-17, 2023, presented by Kazuiro Ogata (invited)

[30] Kazuhiro Ogata: Security Protocol Model Checking based on Algebraic Specifications, 1st International Conference on Intelligent Systems and Data Science (ISDS 2023), November 11 – November 12, Can Tho, Vietnam, Presented by Kazuhiro Ogata (an invited keynote speech)

[20] Kazuhiro Ogata: An overview of FAVPQC achievements (Opening of FAVPQC 2023), 2nd International Workshop on Formal Analysis and Verification of Post-Quantum Cryptographic Protocols (FAVPQC 2023) (a satellite event of ICFEM 2023), Nov 21, 2023,

Brisbane, Australia, Presented in person by Kazuhiro Ogata

＊ポスター発表（相手側研究チームとの連名発表）
発表件数：計 0 件

＊ポスター発表（相手側研究チームを含まない日本側研究チームの発表）
発表件数：計 0 件

3. 主催したワークショップ・セミナー・シンポジウム等の開催
[1] International Workshop on Formal Analysis and Verification of Post-Quantum Cryptographic Protocols 2022 (FAVPQC 2022)、主催者：Sedat Akleylek, Santiago Escobar, Kazuhiro Ogata, Ayoub Otmani、Oct 24, 2022, Madrid, Spain, Universidad Complutense de Madrid、参加人数 15 名程
https://favpqc2022.gitlab.io/

[2] International Workshop on Formal Analysis and Verification of Post-Quantum Cryptographic Protocols 2023 (FAVPQC 2023)、主催者：Sedat Akleylek, Santiago Escobar, Kazuhiro Ogata, Ayoub Otmani、Nov 21, 2023, Brisbane, Australia, Novotel Brisbane South Bank、参加人数 10 名程
https://favpqc2023.gitlab.io/

4. 研究交流の実績（主要な実績）
【合同研究打ち合わせ】
・2022 年 11 月 24 日～28 日：スペインマドリッドで開催された国際会議 ICFEM 2023 の参加の合間を縫って Santiago Escobar, Kazuhiro Ogata, Canh Minh Do, Duong Dinh Tran の 4 名でスペインマドリッドにおいて研究打ち合わせを実施した。
・４ヶ国（日本、スペイン、フランス、トルコ）のチームメンバーを交えて Webex でオンラインミーティングを開催した（初年度 5 回、2 年度 3 回、3 年度 1 回）。

【研究者受入】
・2023 年 1 月 16 日～18 日：Kazuhiro Ogata, Canh Minh Do, Duong Dinh Tran との合同研究打ち合わせのため Santiago Escobar を北陸先端科学技術大学院大学に受け入れた。

5. 特許出願
研究期間累積出願件数：0 件

6. 受賞・新聞報道等
該当無し

7. その他
【オープンサイエンスにかかる取組み】
・原著論文のほぼすべて（原著論文[1, 14] 以外すべて）をオープンアクセスとして出版した。
・PQ Hybrid SSH の形式仕様・形式検証で用いたファイルを以下のウェブサイトで公開した：

https://github.com/duongtd23/PQSSH
発表論文（原著論文[11]）に明記することで研究に興味を持った方に上記ファイルを入手出来るようにした。
・不変性を形式検証するための証明スコア自動生成ツール（のソースコード）を以下のウェブサイトで公開した：
https://github.com/duongtd23/ipsg-tls
発表論文（原著論文[16]）に明記することで研究に興味を持った方に上記ファイルを入手出来るようにした。
・並列化 Maude-NPA（のソースコード）を以下のウェブサイトで公開した：
https://github.com/canhminhdo/parallel-maude-npa
発表論文（原著論文[1]）に明記することで研究に興味を持った方に上記ファイルを入手出来るようにした。
・Maude-NPA と並列化 Maude-NPA で実施した PQ Hybrid TLS の形式仕様・形式検証で用いたファイルを以下のウェブサイトで公開した：
https://github.com/duongtd23/PQSSH
発表論文（原著論文[8]）に明記することで研究に興味を持った方に上記ファイルを入手出来るようにした。