2024年度共同利用研究報告書

2024年11月02日

所属・職名 東京大学大学院情報理工学系研究科・助教
相川 勇輔

		整理番号	2024a023	
1.研究計画題目	耐量子計算機暗号の社会実装に向けた数理基盤の研究			
2.新規・継続	新規			
3.種別	若手・学生研究			
4.種目	短期共同研究			
5.開催方法	ハイブリッド開催			
6.研究代表者	氏名	相川 勇輔		
	所属 部局名	東京大学大学院情報理工学系研究科	職名	助教
7.研究実施期間	2024年07月16日(火曜日)～2024年07月19日(金曜日)			
8.キーワード	耐量子計算機暗号，格子暗号，符号暗号，多変数多項式暗号，同種写像暗号，MPC-in-the-Head			
9.参加者人数	93人			

10.本研究で得られた成果の概要

耐量子計算機暗号の標準化活動が世界中で進行している．2022年には4つの方式が標準化方式として決まり，現在は暗号化方式4つおよび，追加で行われたデジタル署名公募に提出された40方式がふるいにかけられている（実施時点）．そこで，今回の共同利用研究ではこれらの方式にフォーカスし，その数理的側面の詳細を含め，その設計手法や安全性および研究動向について産学官で共有することを目的とした．

公開ワークショップを2日間，非公開の議論を2日間実施した．ハイブリッド開催された公開ワークショップでは計8つの1時間講演を行い，計93名の参加者を得た．非公開議論では，公開ワークショップで共有した知識や情報をもとに議論を実施した．その結果，いくつかの共同研究テーマを得ることができ，これらについては現在研究が進行中である．

成果報告書：
耐量子計算機暗号の社会実装に向けた
数理基盤の研究

開催概要

■開催日程　2024 年 7 月 16 日〜2024 年 7 月 19 日に実施．うち，7 月 16 日〜7 月 17 日には公開型のワークショップを実施．7 月 18 日〜7 月 19 日には非公開での議論を実施した．

■目的　量子情報時代におけるセキュリティ基盤技術として耐量子計算機暗号が期待されている．実際，2016 年より米国の NIST を中心として耐量子計算機暗号の標準化活動が進められており，2022 年には 4 つの方式が標準化された．また，4 つの暗号化方式が Round4 において依然ふるいにかけられている．

一方で，デジタル署名の候補方式の不足により 2023 年にデジタル署名を対象とした追加公募が行われた．その結果，新しく 40 方式が候補リストに加わった．これらの方式は実用化を目指すものであり，注意深く監視する必要がある．

そこで本共同研究では，格子暗号, 符号暗号などをはじめとした各方式カテゴリの専門家を集め，リストに加わった新方式を中心に標準化の現状に関する情報および研究課題を共有することを目的とする．

■期待される成果　上で述べた新方式の中には新たな計算量仮定のもとで設計された方式もある．その数理基盤をよく理解することは，暗号の安全性の解析をより厳密なものとし，量子情報社会における安心・安全を実現するために今後の重要な研究課題となると考えている．また，耐量子計算機暗号では従来方式に比較して効率性が劣ることが産業上の課題となっている．

本共同研究では，これらの課題を数理的な観点から分析し，有力な方式の洗い出し，およびその安全性および高効率化について議論を行った．これらの議論を通し，新方式の根幹をなす数理および諸問題を産業界とも広く共有することで，耐量子計算機暗号への将来的な移行が円滑なものとなることが期待できる．

公開型

公開型ワークショップでは，NIST の標準化活動に提出されている主なデジタル署名方式の数学的側面について，各々の専門家に講演いただき情報の共有を主なものとした．各講演の概要は以下の通りであった．

7 月 16 日

相川 勇輔（東京大学）：Deuring 対応の暗号応用：同種写像求解および署名設計

この講演では同種写像暗号について，まず四元代数を用いた安全性解析手法に関する研究成果が共有された．さらに，新たなデジタル署名方式である SQIsign に関する研究動向が議論された．

穴田 啓晃（明治学院大学）：耐量子ディジタル署名の対称鍵要素からの MPC-in-the-Head による構成について

デジタル署名の新たな設計手法として MPC-in-the-Head と呼ばれる手法があり，その安全性の高さから耐量子デジタル署名方式の候補として最も注目されているものの一つである．

この手法はマルチパーティ計算のプロトコルからゼロ知識証明のプロトコルを構成するものであり，本講演ではその手法の詳細が議論された．また，MPC-in-the-Head の代表的方式である Picnic 方式についても解説がなされた．

成定 真太郎（KDDI 総合研究所）：シンドローム復号問題の求解アルゴリズムの研究動向

符号暗号は NIST 標準化 Round4 において 3 つの暗号化方式が選ばれており，今後標準化される見込みの最も高い暗号である．その安全性はシンドローム復号問題（SDP）に基づいており，SDP の困難性の評価は最も重要な研究課題となっている．この講演では，SDP の求解法である Information Set Decoding について，その最新の研究動向が議論された．

相川 勇輔（東京大学）：符号理論に基づくデジタル署名の設計

符号理論にもとづくデジタル署名として新たな手法による設計が登場してきている．それらの中で最も有望と思われる WAVE 方式と LESS 方式について，その設計の数学的な側面を含め詳細に議論された．なお，これらの方式は NIST 標準化追加公募にも提出されており，今後の研究の進展が期待される．

7 月 17 日

上村 周作（KDDI 総合研究所）：Lattice Isomorphism Problem に基づく署名方式と安全性評価

NIST 標準化追加公募に提出された格子ベースのデジタル署名として有望なものに HAWK がある．この方式の安全性は新たな計算量仮定である Lattice Isomorphism Problem(LIP) に基づいており，関心を集めている．本講演では LIP の詳細からはじまり，LIP に基づき HAWK をどのように設計するのかについて詳細に議論された．

廣瀬 勝一（福井大学）：ハッシュ関数を用いたデジタル署名方式

2022 年に決定された標準化方式の一つである SPHINCS+ はハッシュ関数に基づく設計を持つ．本講演では，ハッシュ関数の基礎知識からはじまり，ハッシュ関数からデジタル署名を設計っする手法について詳細に議論された．

池松 泰彦（九州大学）：UOV 署名方式とその改良について

NIST 標準化追加公募で最も注目を集める方式として多変数多項式暗号の一つである UOV がある．本講演では，UOV の設計手法およびその改良方式のアイデアが議論された．また，追加公募に応募されている多変数多項式暗号の最新の研究動向について詳細に共有された．

古江 弘樹（NTT）：剰余環構造を用いた UOV 署名方式の効率化について（QR-UOV）

UOV の改良方式の一つとして剰余環構造を用いる QR-UOV と VOX がある．本講演ではこれらの方式の設計の詳細が議論された．また，これらの方式に対する MinRank 攻撃の適用法も議論され，VOX の提案パラメータの安全性の不足が指摘された．

非公開議論

公開型ワークショップにおいて共有した知識や情報をもとに，今後の研究テーマの創出に向けて議論を行なった．その結果，NIST 標準化候補暗号の高効率化および，安全性解析に関していくつかのアイデアを得た．これらの研究テーマは現在進行中の未公開のものであり，詳細は割愛する．なお，非公開議論の参加者は以下の通りである．

■参加者　池松 泰彦（九州大学　マス・フォア・インダストリ研究所），石塚慶太（三菱電機），上村周作（KDDI 総合研究所），成定 真太郎（KDDI 総合研究所），古江 弘樹（日本電信電話），相川勇輔（東京大学）

九州大学 IMI 共同利用・短期共同研究　公開プログラム

ワークショップ：耐量子署名方式の設計と安全性の数理

Workshop on Mathematics of Post-Quantum Signatures and its Security

7月16日（火）

10:15-10:30
本勉強会の主旨説明

10:30-11:30
講演者：相川 勇輔（東京大学）
講演タイトル：Deuring 対応の暗号応用：同種写像求解および署名設計

13:00-14:00
講演者：穴田 啓晃（明治学院大学）
講演タイトル: 耐量子ディジタル署名の対称鍵要素からの MPC-in-the-Head による構成について

14:20-15:20
講演者：成定 真太郎（KDDI 総合研究所）
講演タイトル：シンドローム復号問題の求解アルゴリズムの研究動向

15:40-16:40
講演者：相川 勇輔（東京大学）
講演タイトル：符号理論に基づくデジタル署名の設計

7月17日（水）

10:30-11:30
講演者：上村 周作（KDDI 総合研究所）
講演タイトル：Lattice Isomorphism Problem に基づく署名方式と安全性評価

13:00-14:00
講演者：廣瀬 勝一（福井大学）
講演タイトル： ハッシュ関数を用いたデジタル署名方式

14:20-15:20
講演者：池松 泰彦（九州大学）
講演タイトル：UOV 署名方式とその改良について

15:40-16:40
講演者：古江 弘樹（NTT）
講演タイトル：剰余環構造を用いた UOV 署名方式の効率化について（QR-UOV）

※研究実施期間：2024 年 7 月 16 日(火)～7 月 19 日(金)
※公開日：2024 年 7 月 16 日(火)～7 月 17 日(水)

ＨＰ掲載用英文

Speaker:　Yusuke Aikawa (The University of Tokyo)
Title: Cryptographic Application of the Deuring Correspondence: Signature Schemes and Solving Isogeny Problem

Speaker:　Hiroaki Anada (Meiji Gakuin University)
Title: On the Constructions of Post-Quantum Digital Signatures from Symmetric-Key Primitives by MPC-in-the-Head

Speaker:　Shintaro Narisada (KDDI Research)
Title: Recent Advances on Decoding Algorithms for the Syndrome Decoding Problem

Speaker:　Yusuke Aikawa (The University of Tokyo)
Title:　Design of Signature Schemes based on Coding Theory

Speaker:　Shusaku Uemura (KDDI Research)
Title:　Signature scheme based on Lattice Isomorphism Problem and its security

Speaker:　Shoichi Hirose (University of Fukui)
Title:　Hash-based Digital Signature Schemes

Speaker:　Yasuhiko Ikematsu (Kyushu University)
Title:　UOV signature scheme and its variants

Speaker:　Hiroki Furue (NTT)
Title:　Efficient variant of UOV signature using quotient ring structure (QR-UOV)