2022年度共同利用研究報告書

2022年11月03日

所属・職名 三菱電機株式会社　情報技術総合研究所・研究員
相川 勇輔

		整理番号	2022a015	
1.研究計画題目	セキュアな量子情報活用に向けた次世代暗号の数理			
2.新規・継続	新規			
3.種別	プロジェクト研究			
4.種目	短期共同研究			
5.研究代表者	氏名	相川 勇輔		
	所属 部局名	三菱電機株式会社　情報技術総合研究所	職名	研究員
6.研究実施期間	2022年08月01日(月曜日)～2022年08月05日(金曜日)			
7.キーワード	量子計算、量子暗号プロトコル、耐量子計算機暗号、格子暗号、多変数多項式暗号、同種写像暗号			
8.参加者人数	318人			

9.本研究で得られた成果の概要

量子コンピュータの強力な計算能力は現在利用されている公開鍵暗号を危殆化させることが知られている。つまり、現在の公開鍵暗号の多くがその安全性の根拠としている素因数分解問題や離散対数問題をShorのアルゴリズムによって効率的に解く。したがって、大規模な量子コンピュータの実現に先駆けて、その解読にも耐えうる耐量子計算機暗号の研究開発および実用化が重要な課題となっている。実際、2016年よりNISTはその標準化を進めており産業的ニーズも高く、研究を進めると同時に、その知見について社会で共有することも重要である。一方では、Mahadevによるブレークスルーにより耐量子計算機暗号の量子情報処理への応用という新たな研究が進展している。しかしながら、これらの多くは分野ごとに研究が進展しており、それぞれの知見の共有はあまり試みられてこなかった。

そこで本研究では、これらの多様な知見を一か所に集め、基礎知識から最先端研究までの情報を広く共有することを目指した。公開型ワークショップ「耐量子計算機暗号と量子情報の数理」では、格子暗号、多変数多項式暗号、符号暗号、同種写像暗号、量子情報理論および計算量理論の分野に対し、組織委員に加え各分野で優れた成果を挙げておられる招待講演者も招き講演を実施した。その結果、318名という多数の参加者にも恵まれ目的が達成された。全ての講演スライドおよび動画は誰もが利用できる形で公開した。

さらに、組織委員のみによる非公開議論では同種写像に関する仮定からTrapdoor claw-free関数の構成を試み、同種写像暗号の量子情報への応用を検討した。SIDHベースの一方向性関数に楕円曲線の自己準同型をトラップドアとして利用するというアイデアでTrapdoor claw-free関数の構成を目指したが、本研究実施直前に発表されたCastryck-DecruによるSIDHの鍵復元攻撃を考えると、この方針では安全な関数の構成が困難であることがわかった。

成果報告書

プロジェクト研究-短期共同研究

「セキュアな量子情報活用に向けた次世代暗号の数理」

■ 実施概要

・ 組織委員
相川勇輔（三菱電機株式会社　情報技術総合研究所・研究員）[研究代表者]
池松泰彦（九州大学マス・フォア・インダストリ研究所・助教）
小貫啓史（東京大学大学院情報理工学系研究科・特任助教）
高安敦（東京大学大学院情報理工学系研究科・講師）
竹内勇貴（日本電信電話株式会社コミュニケーション科学基礎研究所・研究員）廣政良（三菱電機株式会社　情報技術総合研究所・研究員）
古江弘樹（東京大学大学院情報理工学系研究科・博士学生）
水谷明博（三菱電機株式会社　情報技術総合研究所・研究員）
守谷共起（東京大学大学院情報理工学系研究科・博士学生）

・ プロジェクトウェブサイト
https://joint1.imi.kyushu-u.ac.jp/research_chooses/view/2022a015

・ 研究実施期間
2022 年 8 月 1 日（月）～8 月 5 日（金）
うち
公開型ワークショップ：8 月 1 日（月）13:30～8 月 4 日（木）12:30
非公開型議論：8 月 4 日（木）13:30～8 月 5 日（金）12:30

・ 公開型ワークショップ参加人数
318 名

■ 本プロジェクトの背景

2022 年現在、量子コンピュータの開発が世界中で加速している。量子コンピュータは、古典コンピュータでは効率的に解くアルゴリズムの未だ知られていない特定の計算問題を高速に解くことが理論的に示されており、このことから次世代の強力な計算資源として様々な科学技術分野への応用が期待されている。

一方で、その強力な計算能力は現在利用されている公開鍵暗号を危殆化させることも知られている。公開鍵暗号はその安全性の根拠として一方向的な計算困難性を持つことが期待される数学的問題を利用する。例えば、RSA 暗号では巨大な素数（2022 年現在では 1024 ビット以上の素数の利用が推奨されている）のペア(p,q)を秘密鍵に、それらの積$N=p\cdot q$を公開鍵の一部の情報とすることで公開鍵暗号の原理を実現している。ここで重要なことは、素数の積を取ることは効率的に計算可能であるのに対し、巨大な合成数を素因数分解することは現状では一般に計算量的に困難であるという非対称性があるということである。この事実は、公開されている合成数から攻撃者が秘密鍵(p,q)の情報にアクセスすることを困難にしている。

上記の「量子コンピュータが公開鍵暗号を危殆化させる」とは、すなわち、量子コンピュータはその計算能力が素因数分解問題や離散対数問題のような暗号の安全性に直結する数学的問題を効率的に解くことが可能であることを意味する。それを実行するアルゴリズムが Shor のアルゴリズム[S]であり、大規模な量子コンピュータの実現は現代の情報化社会における安全を脅かすことになる。

そこで公開鍵暗号の研究は、その安全性を支える計算量仮定を刷新することで、量子コンピュータの登場に備えるという方向に大きく進展している。このように量子コンピュータを利用しても解くことが困難であることが期待される計算問題に安全性の根拠を置いた暗号方式群を耐量子計算機暗号という。以上のような背景から、耐量子計算機暗号の研究は産業的な観点からも重要な意味を持ち、その研究動向や知見を社会で広く共有することが重要である。実際、NIST は 2016 年より耐量子計算機暗号の標準化を進めており、現行システム内で利用されている既存暗号の耐量子計算機暗号への置き換え時期として 2030 年をマイルストンとして掲げている。

耐量子計算機暗号の主な候補として

- 格子問題に基づく格子暗号
- 多変数多項式方程式の求解問題に基づく多変数多項式暗号
- 誤り訂正符号技術に基づく符号暗号
- 楕円曲線間の同種写像問題に基づく同種写像暗号

がある。これらの暗号はそれぞれ使っている数学が大きく異なり、それゆえ研究手法だけでなく暗号技術としての特性も得手・不得手が大きくことなる。そのため産業ニーズとして、将来的にユースケースに応じた使い分けを柔軟に行うことが期待されている。そのため、これら暗号方式群について総合的に知見を蓄えておくことは学術的研究のみならず、暗号の実利用という観点からも重要である。

しかしながら、これらの暗号はその多様性のみならず使用する数学的技術が多岐に渡ることから、国内では分野ごとに研究者コミュニティが分かれてしまう傾向にあり、最新研究動向や研究手法の詳細に関する知識が散らばってしまっているという課題がある。

一方で、耐量子計算機暗号は従来利用してきた公開鍵暗号の耐量子化という目的のみな

らず、Mahadev のブレークスルー[M]によって量子情報処理への応用も見出された。それ以降、BQP の対話型アーギュメント、量子性の検証、QMA のゼロ知識アーギュメント、セルフテストなどといった量子情報技術は耐量子計算量仮定の下で古典コンピュータのみで達成できることが示され、現在も著しく研究が進展している。しかしながら、これら一連の研究は耐量子計算機暗号と量子情報のコミュニティを接近させた一方で、現状では LWE 仮定を利用した格子暗号の応用のみが知られているという状況であり、それ以外の耐量子性を持つ計算量仮定の適用可能性に関する知見は現段階では得られていない。

■ 本プロジェクトの目的

以上に述べた背景のもと、本プロジェクトでは以下の 3 点を目的として掲げる：

1. 耐量子計算機暗号の各分野の基礎知識および数学的技術の共有
2. 耐量子計算機暗号と量子情報の各分野の基礎知識および最新研究動向の知見の交換
3. LWE 仮定以外の計算量仮定の量子情報処理への応用を見出す

目的 1，2 を達成するために、本プロジェクトでは、組織員に加え招待講演者による各分野の知識の交換および議論の場を提供する。この場は、当分野の最先端の情報が集まる場であり、社会に広く公開することで、将来的な共同研究を円滑に進めることが可能となり分野の活性化に資することが期待される。そのため、公開型ワークショップという形で実施を行った。さらに、それらをもとに非公開型の議論では組織委員で目的 3 に取り組んだ。より具体的には Mahadev[M]にはじまる量子暗号の研究の中で中心的な役割を果たす Trapdoor claw-free 関数を LWE 仮定以外の耐量子性を持つ計算量仮定から構成することを目指した。

■ 本プロジェクトの成果

上で述べたように、本プロジェクトは公開型ワークショップと非公開型議論で構成される。ここでは、これらの実施結果をそれぞれまとめる。

- **公開型ワークショップ**

  本プロジェクトでは 8/1（月）～8/4(木)に公開型ワークショップ「耐量子計算機暗号と量子情報の数理」を開催した。組織委員による講演加え、以下の研究者を招待し講演いただいた。ワークショップへの参加登録者は 318 名であった。プログラムは本報告書末尾に記載し、ここでは分野ごとに共有された知見についてまとめる。

  招待講演者（五十音順）：國廣昇（筑波大学)、七島幹人（東京工業大学)、
  成定真太郎（KDDI 総合研究所)、安田雅哉（立教大学)、
  山川高志（NTT）

  - **暗号一般**

    本ワークショップへは、暗号分野を専門としない数学を専門とする方々や量

子情報を専門とする方々の参加が予想された。そのため、研究代表の相川による「数理暗号入門」と題した講演を行い、暗号学的な考え方や暗号の構成法、数学との関わりおよび本ワークショップのオーバービューを参加された方々と共有した。なお、暗号の暗号理論的な側面については組織委員の廣政氏の講演「格子暗号」の中で解説いただいた。

- **量子情報**

  量子情報理論に関しても、異分野から前提知識を所有しない方々の参加が想定されたため、組織委員の竹内氏による「量子情報基礎」および「量子計算基礎」と題する講演を用意し、メインターゲットである Mahadev 以降の量子情報処理の研究の進展の講演へ備えた。前者の講演では、量子情報処理の目的についてオーバービューが提供されたのち、量子状態、量子操作および量子測定という基本的な概念について解説がなされた。後者の講演では、量子回路や量子計算の計算量的側面および量子計算の検証の基礎事項の解説が行われた。

  竹内氏の講演に続き組織委員の水谷氏により「量子計算の古典検証」と題し、主に Mahadev による結果およびその手法[M]の詳細が解説された。さらに、水谷氏らの関連する成果として CCZ マジック状態の生成・測定機能の古典検証[MTH+]の紹介がされた。

  Mahadev 以降の研究の進展については、当該分野で世界的に大きな貢献をなされている山川氏（NTT）を招待し講演いただいた。講演では山川氏の成果[CCY]を含む Mahadev の量子計算の古典検証の改良の研究の現状について「計算量的安全な量子暗号の最近の進展」という題で講演頂いた。Mahadev の証明技法の様々な応用が見出されており、それらの研究についても講演いただいた。最後に量子性の古典検証をハッシュ関数のみから構成した最新の研究[YZ]についても解説いただいた。

  量子情報処理のみならず、暗号と量子情報の関わりにおいて背景でも述べたように、公開鍵暗号の安全性を解析する上で量子アルゴリズムの研究を進めることも重要である。量子アルゴリズムについて知見をお持ちの國廣氏（筑波大）を招待し、「隠れ部分群問題から見る素因数分解, 離散対数問題」という題で講演いただいた。隠れ部分群問題に焦点をあて、それと関する様々な数学的問題に対する量子アルゴリズムの研究の進展について解説いただいた。

- **格子暗号**

  耐量子計算機暗号の有力候補である格子暗号についてはまず廣政氏に「格子暗号」と題する講演で解説いただいた。格子暗号は NIST の標準化においても暗号化方式 CRYSTALS-KYBER、デジタル署名方式 CRYSTALS-DELITHIUM, FALCON が標準化暗号として選出され、今後実用化に向けてますます重要性が増すトピックである。廣政氏の講演では、公開鍵暗号の基礎的な内容からはじめ

Regev 暗号、LWE 問題および完全準同型暗号について解説をいただいたのち、格子暗号の量子情報処理への応用として Noisy trapdoor claw-free 関数の構成について詳しく解説いただいた。

格子暗号の安全性解析については、近年では[NY]等の成果を挙げ知見をお持ちの安田氏（立教大）を招待し「格子基底簡約と LWE/NTRU 問題に対する格子攻撃」と題し講演いただいた。格子理論を用いた数学的な安全性解析のオーバービューの提供に加え、その実装コードの披露や実演を交えた講演をしていただいた。

- **多変数多項式暗号**

多変数多項式暗号は耐量子計算機暗号の候補の一つであったが、NIST の標準化では Round3 で全ての方式が落選してしまった。一方で、[FIKT]等の新たなデジタル署名方式が提案されるなど、依然として活発な分野である。

この暗号方式は、一般に署名長のコンパクトなデジタル署名の構成に優れるといわれている。そこで、2021 年にデジタル署名方式 QR-UOV[FIKT]の提案を行った組織委員の古江氏に「多変数多項式暗号 1：署名方式の構成」と題して、[FIKT]の成果含め、署名方式の構成について解説いただいた。Matsumoto-Imai 暗号からはじめ、HFE,UOV および NITS 標準化 Round 3 で重要な候補暗号であった Rainbow について解説いただいた。

続いて組織委員の池松氏に「多変数多項式暗号 2：安全性解析」と題し講演頂いた。多変数多項式暗号の安全性解析は近年進展が著しい分野であり、その知見に関するニーズはアカデミアのみならず産業でも高い。ここでは、近年の最も大きな成果である Beullens による Rainbow の安全性解析[B]の結果や、多変数多項式暗号の現状においては UOV が最も効率的で安全であるという認識が共有された。

- **符号暗号**

耐量子計算機暗号の有力な候補である符号暗号については、その解読実験で大きな成果[NFK]を挙げておられる成定氏（KDDI）を招待し、「符号暗号の高速求解手法の実装に向けて」と題し講演いただいた。符号暗号とシンドローム復号問題(SDP)の基礎からはじめ、線形代数や組み合わせ論に基づく SDP の解読アルゴリズムである ISD の研究動向やその実装について詳細に解説いただいた。また、近年の動向として量子 ISD についても解説いただいた。

- **同種写像暗号**

同種写像暗号は耐量子計算機暗号の候補であり、NIST の標準化でも Round 4 に SIKE が選出されている。世界的に研究の進んでいる分野ではあるが、楕円曲線や同種写像といった異分野には馴染みのない数学的概念を本質的に活用するため、その参入障壁の高さから国内では他分野に比して研究が活発でなかった。

そこで、今回は相川が「同種写像暗号 1：楕円曲線と同種写像グラフ」と題し、同種写像暗号を支える数学の基礎についてのチュートリアルを提供した。その中で最新の成果であるモンゴメリー座標の一般化[MOAT]や超特別アーベル多様体の同種写像グラフの代数的性質[ATY]についても紹介を行った。

続いて組織委員の守谷氏に「同種写像暗号 2 ：鍵交換方式 SIDH と CSIDH」と題して、最も重要な同種写像暗号プリミティブである SIDH[DJP], [JD]と CSIDH[CLM+]について紹介を行っていただいた。さらに、守谷氏の提案した CSIDH ベースの暗号化方式である SiGamal[MOT]についても紹介いただいた。

組織委員の小貫氏には同種写像分野において近年の最も大きな成果の一つであるデジタル署名方式 SQISign[DKL+]について「同種写像暗号 3：デジタル署名方式 SQISign」と題した講演で紹介いただいた。この方式は今後 NIST 標準化でのデジタル署名再公募に応募されると目されている方式であるため、その情報を共有しておくことは産業的ニーズも高い。実際、公開鍵長および署名長が格子暗号による NIST 標準化方式 Falcon に比べそれぞれ 1/14、1/3 程度のサイズという著しくコンパクトな性能を有している。一方で数学的な構成が複雑であり、その安全性解析が困難という課題もある。最近小貫氏は SQISign の公開鍵の安全性に関して成果[O]を挙げておられるので、その結果についても共有いただいた。

最後に、本ワークショップ開催直前の 7 月末に Castryck と Decru による SIDH 方式への鍵復元攻撃[CD]が提案された。この攻撃は、最も安全性レベルの高い NIST level 5 のパラメータに対しても 20 時間 37 分で鍵を復元するという著しく強力なものであり、SIDH をベースとした鍵カプセル化方式 SIKE が NIST 標準化 Round 4 に選出されているという影響力の大きさから、緊急でこの論文の内容を紹介する講演を用意した。論文の内容をワークショップ開催中に相川、守谷氏および小貫氏で検討を行い、その結果を小貫氏に「同種写像暗号 SIDH への鍵復元攻撃について」と題する講演で共有いただいた。この攻撃は、暗号方式設計のために補助情報を公開するという SIDH の特性を利用したものであり、全ての同種写像暗号に効くわけではない（例えば現段階では CSIDH には適用できない）という重要な事実を、論文[CD]が公開されて数日後に共有することができた。

- **計算量理論**

計算量理論から暗号へのアプローチの研究も、コルモゴロフ複雑度の計算問題の観点からアルゴリズム的[HN]、暗号学的[LP]研究が進んでいる。当該分野で成果[HN]を挙げておられる七島氏を招待し、「コルモゴロフ複雑度とそのアルゴリズム/暗号理論的恩恵」と題し、その進展やメタ計算量理論による研究手法について解説いただいた。

本プロジェクトの成果物として、多くの最新の結果を含む上記講演全ての講演資料および動画を誰もが利用できる形で公開した。それらは全て以下の HP より利用が可能である：https://joint.imi.kyushu-u.ac.jp/post-5123/

- **非公開型議論**

非公開型議論では議論のテーマを「同種写像に関する安全性仮定から Trapdoor claw-free 関数を構成」とし、議論を行った。今回、SIDH ベースでの暗号化方式である Séta[DSF+]を事前に調査し、この構成を参考に SIDH 型の一方向性関数にトラップドアとして楕円曲線の自己準同型を利用することで Trapdoor claw-free 関数の構成を目指した。議論の中で構成の技術的課題を明確にすることができたが、それ以上に今回の構成は SIDH と同様に補助情報を利用しているため[CD]の攻撃の適用可能性が重要な検討事項であった。本共同研究実施中は、パラメータを慎重に設定することで回避できるかもしれないという認識であったが、後日発表された論文[R]によって（もしこの論文の主張が正しければ）この方針では安全な Trapdoor claw-free 関数が作れないことが明らかになった。

■ 参考文献

[ATY] Y.Aikawa, R. Tanaka, T.Yamauchi, Isogeny graphs on superspecial abelian varieties: Eigenvalues and Connection to Bruhat-Tits buildings, arXiv:2201.04293.

[B] W. Beullens, (2022). Breaking Rainbow Takes a Weekend on a Laptop. In: Dodis, Y., Shrimpton, T. (eds) Advances in Cryptology – CRYPTO 2022. CRYPTO 2022. Lecture Notes in Computer Science, vol 13508. Springer, Cham. https://doi.org/10.1007/978-3-031-15979-4_16

[CCY] NH. Chia, KM. Chung, T. Yamakawa, (2020). Classical Verification of Quantum Computations with Efficient Verifier. In: Pass, R., Pietrzak, K. (eds) Theory of Cryptography. TCC 2020. Lecture Notes in Computer Science(), vol 12552. Springer, Cham. https://doi.org/10.1007/978-3-030-64381-2_7

[CD] W.Castryck, T.Decru, An efficient key recovery attack on SIDH (preliminary version), IACR Cryptol. ePrint Arch. 2022/975. https://eprint.iacr.org/2022/975.pdf

[CLM+] W. Castryck, T. Lange, C. Martindale, L. Panny, J. Renes, (2018). CSIDH: An Efficient Post-Quantum Commutative Group Action. In: Peyrin, T., Galbraith, S. (eds) Advances in Cryptology – ASIACRYPT 2018. ASIACRYPT 2018. Lecture Notes in Computer Science(), vol 11274. Springer, Cham. https://doi.org/10.1007/978-3-030-03332-3_15

[DJP] L. De Feo, D. Jao, J. Plût, "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies" *Journal of Mathematical Cryptology*, vol. 8, no. 3, 2014,

pp. 209-247. https://doi.org/10.1515/jmc-2012-0015
[DKL+] L. De Feo, D.Kohel, A.Leroux, C.Petit, B. Wesolowski, (2020). SQISign: Compact Post-quantum Signatures from Quaternions and Isogenies. In: Moriai, S., Wang, H. (eds) Advances in Cryptology – ASIACRYPT 2020. ASIACRYPT 2020. Lecture Notes in Computer Science(), vol 12491. Springer, Cham. https://doi.org/10.1007/978-3-030-64837-4_3
[DSF+] L. De Feo, *et al.* (2021). Séta: Supersingular Encryption from Torsion Attacks. In: Tibouchi, M., Wang, H. (eds) Advances in Cryptology – ASIACRYPT 2021. ASIACRYPT 2021. Lecture Notes in Computer Science(), vol 13093. Springer, Cham. https://doi.org/10.1007/978-3-030-92068-5_9
[FIKT] H.Furue, Y.Ikematsu, Y.Kiyomura, T.Takagi (2021) A New Variant of Unbalanced Oil and Vinegar Using Quotient Ring: QR-UOV. In: Tibouchi M., Wang H. (eds) Advances in Cryptology – ASIACRYPT 2021. ASIACRYPT 2021. Lecture Notes in Computer Science, vol 13093. Springer, Cham.
[HN] S. Hirahara and M. Nanashima, "On Worst-Case Learning in Relativized Heuristica," *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)*, 2022, pp. 751-758, doi: 10.1109/FOCS52979.2021.00078.
[JD] D. Jao, L. De Feo, (2011). Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies. In: Yang, BY. (eds) Post-Quantum Cryptography. PQCrypto 2011. Lecture Notes in Computer Science, vol 7071. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-25405-5_2
[LP] Y. Liu and R. Pass, "On One-way Functions and Kolmogorov Complexity," *2020 IEEE 61st Annual Symposium on Foundations of Computer Science (FOCS)*, 2020, pp. 1243-1254, doi: 10.1109/FOCS46700.2020.00118.
[M] U. Mahadev, "Classical Verification of Quantum Computations," *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)*, 2018, pp. 259-267, doi: 10.1109/FOCS.2018.00033.
[MOAT] T.Moriya, H.Onuki, Y.Aikawa, T.Takagi, "The Generalized Montgomery Coordinate: A New Computational Tool for Isogeny-based Cryptography", 4th International Workshop on Mathematical Cryptology, MathCrypt2022, 2022.
[MOT]T.Moriya, H.Onuki, T.Takagi, (2020) SiGamal: A Supersingular Isogeny-Based PKE and Its Application to a PRF. In: Moriai S., Wang H. (eds) Advances in Cryptology – ASIACRYPT 2020. ASIACRYPT 2020. Lecture Notes in Computer Science, vol 12492. Springer, Cham.
[MTH+] A.Mizutani, Y.Takeuchi, R.Hiromasa, Y.Aikawa, S.Tani, Computational self-testing for entangled magic states, Phys. Rev. A, 106, L010601, 2022, Jul.
[NFK] S. Narisada, K. Fukushima and S. Kiyomoto, "Fast GPU Implementation of Dumer's

Algorithm Solving the Syndrome Decoding Problem," *2021 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom)*, 2021, pp. 971-977, doi: 10.1109/ISPA-BDCloud-SocialCom-SustainCom52081.2021.00136.

[NY] S.Nakamura, M. Yasuda (2021). An Extension of Kannan's Embedding for Solving Ring-Based LWE Problems. In: Paterson, M.B. (eds) Cryptography and Coding. IMACC 2021. Lecture Notes in Computer Science(), vol 13129. Springer, Cham. https://doi.org/10.1007/978-3-030-92641-0_10

[O] H. Onuki, "On the key generation in SQISign", Number-Theoretic Methods in Cryptology, NuTMiC2021, 2022.

[R] D.Robert, Breaking SIDH in polynomial time, IACR Cryptol. ePrint Arch. 2022/1038. https://eprint.iacr.org/2022/1038.pdf

[S] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 1994, pp. 124-134, doi: 10.1109/SFCS.1994.365700.

[YZ]T.Yamakawa, M.Zhandry, Verifiable Quantum Advantage without Structure, arXiv:2204.02063, to appear in FOCS'22.

九州大学 IMI 共同利用・短期共同研究　公開プログラム

耐量子計算機暗号と量子情報の数理

Mathematics of Post Quantum Cryptography and Quantum Information Theory

8月1日（月）

13:30-14:30
講演者：相川勇輔（三菱電機）
講演タイトル：暗号数理入門

14:50-15:50
講演者：竹内勇貴（NTT）
講演タイトル：量子情報基礎

16:10-17:10
講演者：廣政良（三菱電機）
講演タイトル：格子暗号

８月２日（火）

9:30-10:30
講演者：竹内勇貴（NTT）
講演タイトル：量子計算基礎

10:50-11:50
講演者：水谷明博（三菱電機）
講演タイトル：量子計算の古典検証

13:30-14:30
講演者：相川勇輔（三菱電機）
講演タイトル：同種写像暗号１：楕円曲線と同種写像グラフ

14:50-15:50
講演者：守谷共起（東京大学）
講演タイトル：同種写像暗号２：鍵交換方式 SIDH と CSIDH

16:10-17:10
講演者：小貫啓史（東京大学）
講演タイトル：同種写像暗号３：デジタル署名方式 SQISign

８月3日（水）

9:30-10:30
講演者：安田雅哉（立教大学）
講演タイトル：格子基底簡約と LWE/NTRU 問題に対する格子攻撃

10:50-11:50
講演者：國廣昇（筑波大学）
講演タイトル：隠れ部分群問題から見る素因数分解，離散対数問題

13:30-14:30
講演者：成定真太郎（KDDI 総合研究所）
講演タイトル： 符号暗号の高速求解手法の実装に向けて

14:50-15:50
講演者：七島幹人（東京工業大学）
講演タイトル：コルモゴロフ複雑度とそのアルゴリズム/暗号理論的恩恵

16:10-17:10
講演者：山川高志（NTT）
講演タイトル：計算量的安全な量子暗号の最近の進展

８月4日（木）

9:30-10:30
講演者：古江弘樹（東京大学）
講演タイトル：多変数多項式暗号１：署名方式の構成

10:50-11:50
講演者：池松泰彦（九州大学）
講演タイトル：多変数多項式暗号 2 ：安全性解析

12:00-12:30
講演者：小貫啓史（東京大学）
講演タイトル：同種写像暗号 SIDH への鍵復元攻撃について