AIMaP 研究集会等実施報告書

(Part 1/4) 名称・重点テーマ・キーワード等

項目	内容
名称	International Symposium on Mathematics, Quantum Theory, and Cryptography (MQC 2019)
採択番号	2019A009
重点テーマ	ポスト量子暗号
キーワード	量子理論・暗号理論・最適化理論
主催機関	東京大学大学院情報理工学系研究科
運営責任者	東京大学　高木剛
開催日時(開始)	2019/09/25　13:00
開催日時(終了)	2019/09/27　17:30
開催場所	九州大学ウエスト 1 号館 D413 IMI オーディトリアム

(Part 2/4) 最終プログラム・参加者数

項目	内容
最終プログラム	**September 25** 11:30–13:00 Registration 13:00–13:15 Opening 13:15–14:15 Keynote Address 1 ・Sustainable Cryptography Johannes Buchmann (Technical University of Darmstadt) 14:20–15:50 Session 1 ・Quantum Random Numbers generated by a Cloud Superconducting Quantum Computer Yutaka Shikano (Keio University) ・Quantum Factoring Algorithm: Resource Estimation and Survey of Experiments Noboru Kunihiro (University of Tsukuba) 15:50–16:20 Coffee Break 16:20–17:50 Session 2 ・A Review of Secret Key Distribution Based on Bounded Observability Jun Muramatsu (NTT Communication Science Laboratories) ・Towards Constructing Fully Homomorphic Encryption without

Ciphertext Noise from Group Theory

Koji Nuida (The University of Tokyo)

September 26

9:45–10:45 Keynote Address 2

・What kind of insight provide analytical solutions of quantum models?

Daniel Braak (Max Planck Institute)

10:50–12:20 Session 3

・Number theoretic study in quantum interactions.

Masato Wakayama (Kyushu University)

・From the Bloch sphere to phase space representations with

the Gottesman–Kitaev–Preskill encoding

Laura Garcia Alvarez (Chalmers University of Technology),

Alessandro Ferraro (Queen's University Belfast), Giulia Ferrini (Chalmers University of Technology)

12:20–13:50 Lunch

13:50–15:20 Session 4

・Matroid Parity

Satoru Iwata (The University of Tokyo)

・Verified numerical computations and related applications

Shin'ichi Oishi (Waseda University)

15:20–15:50 Coffee Break

15:50–17:20 Session 5

・A Survey of Solving SVP Algorithms and Recent Strategies for Solving the SVP Challenge

Masaya Yasuda (Kyushu University)

・Recent developments in multivariate public key cryptosystems

Yasufumi Hashimoto (University of the Ryukyus)

September 27

9:45–10:45 Keynote Address 3

・Emerging ultrastrong coupling between light and matter observed

in circuit quantum electrodynamics

Kouichi Semba (NICT)

10:50–12:20 Session 6

・Securing Data by Noise–Disturbance in the Light of Quantum Sensing Device

Masao Hirokawa (Hiroshima University)

・Quantum optics with giant atoms – the first five years

Anton Frisk Kockum (Chalmers University of Technology)

12:20–13:50 Lunch

13:50–15:20 Session 7

	・Extended divisibility relations for constraint polynomials of the asymmetric quantum Rabi model Cid Reyes-Bustos (Tokyo Institute of Technology) ・Generalized group-subgroup pair graphs Kazufumi Kimoto (University of the Ryukyus) 15:20-15:50 Coffee Break 15:50-17:20 Session 8 ・Ramanujan graphs for post-quantum cryptography Hyungrok Jo (University of Tsukuba), Shingo Sugiyama (Nihon University), Yoshinori Yamasaki (Ehime University) ・Post-Quantum Constant-Round Group Key Exchange from Static Assumptions Katsuyuki Takashima (Mitsubishi Electric Corporation) 17:20-17:30 Closing
参加者数	数学・数理科学:43 人, 諸科学: 12 人, 産業界: 7 人, その他: 4 人

(Part 3/4) 論点・現状・今後の展開

項目	内容
当日の論点	量子計算機に耐性のあるポスト量子暗号(Post-Quantum Cryptography)の構築に関し、海外から指導的立場にある著名研究者とともにトップレベルの若手研究者を招聘し、暗号理論、量子理論、最適化理論などの分野を横断した交流を通して、どのように多角的な安全性評価ができるか議論を行った。
研究の現状と課題 (既にできていること、できていないことの切り分け)	大規模な量子計算機により素因数分解問題・離散対数問題は多項式時間で解読されることから、現在広く普及しているRSA暗号・楕円曲線暗号は危殆化することが知られている。 そこで、新しい数学問題を用いて量子計算機に耐性があるポスト量子暗号を研究開発することが注目を集めている。有力なポスト量子暗号の候補で用いられる数学問題としては、格子基底最短ベクトル問題(SVP)、有限体上の多変数多項式求解問題(MQ問題)、ラマヌジャングラフ上の同種写像問題などがある。現在これら数学問題の計算困難性に基づいた様々な方式が提案され、その安全性が研究されている。 新しい数学問題を用いた暗号の安全性をより深く考察するためには、最新の最適化数理モデリングによる評価は不可欠となる。また、数学者と理論・実験物理の専門家の共同研究による、量子計算機の基本素子となるラビ模型の数理モデリングの構築が必須である。
新たに明らかになった課題	ポスト量子暗号の研究に対しては、最適化モデリングによる暗号の安全性評価、量子相互作用による量子計算機の数理モデリング、新しい数学問題を用いた安全な暗号方式の構成など、様々な分野を横断した寄与が必要である。本シンポジウムには幅広い分野から多数の研究者が参加し、分野横断的に活発に議論が行われたことは大きな意義

	を持つが、これらの交流を継続していくことは新たな課題となる。
今後解決すべきこと、今後の展開・フォローアップ	量子計算機の実用化が見通されている現在、あらゆる通信の安全基準をそれに関わる数学研究の成果により担保していく必要がある。本シンポジウムを日本で開催した今、今後の安全基準の策定における中心的な研究を日本から発信できるようサポートしたい。その一環として、本シンポジウムでは、講演内容を論文形式でまとめた 250 ページ程度の簡易印刷予稿集を配布し、シンポジウム開催期間中の活発な議論を促した。そして開催後、投稿者にはそれらの議論や講演での様々なコメントを反映してもらうために再度原稿の修正を依頼し、最終原稿からなる査読付き論文集を Springer-Nature 社から Mathematics for Industry のシリーズとして出版する予定である。また、印刷出版するだけではなく、研究結果を国内外に広くアピールするためにオンラインフリーアクセスが可能な電子出版となるよう契約を進めている。 また、本シンポジウムでは純粋数学や産業界との新たな交流・連携を得ることも目的の一つであったが、AIMaP の持つ繋がりや取り組みによりそれを実現することが出来た。その一つに、MQC 2019 の開催を通して、ポスト量子暗号の有力候補である格子暗号の実装評価に関して、パナソニック様から九州大学へ共同研究の打診があり、2019 年 12 月から共同研究を開始した。

(Part 4/4) 写真

項目	内容
添付写真 1	

添付写真 2	
添付写真 3	

(20190614 Ver.)