2021年度共同利用研究報告書

2022年03月31日

所属・職名 横浜国立大学先端科学高等研究院・特任助教
Jo Hyungrok

		整理番号		20210008	
1.研究計画題目	ラマヌジャン・グラフの整数論による耐量子計算機暗号へのアプローチ				
2.新規・継続	新規				
3.種別	若手研究				
4.種目	短期共同研究				
5.研究代表者	氏名	Jo Hyungrok			
	所属部局名	横浜国立大学先端科学高等研究院	職名	特任助教	
6.研究実施期間	2021年08月30日(月曜日)～2021年09月02日(木曜日)				
	2021年12月13日(月曜日)～2021年12月17日(金曜日)				
7.キーワード	耐量子計算機暗号、ラマヌジャン・グラフ、同種写像暗号				
8.参加者人数	58人				

9.本研究で得られた成果の概要

耐量子計算機暗号（Post-Quantum Cryptography）とは、量子アルゴリズムを実現する大規模な量子計算機が出現しても安全な暗号技術である。耐量子計算機暗号の有力な候補である同種写像暗号は、ラマヌジャン・グラフの一種である超特異楕円曲線の同種写像グラフの経路探索問題の困難性に基づいている。

本研究の目的は二つであった。まず、一つ目の目的は同種写像暗号の安全性を、その背後にある整数論の観点から評価することであった。一環として、組織委員と非公開セミナー２の参加者はコンパクトな鍵サイズと既存の同種写像ベース署名方式より更なる効率性を持つSQISign(Short Quaternion and Isogeny Signature)の構成やその安全性についてしっかり理解することを目指し、SQISignの数学および情報理論的な背景（四元数代数、KLPTアルゴリズム、ゼロ知識証明など）を適切に分担し、講演会を行った。非公開セミナー２（講演会）から得られた今後の課題は以下の通りである。

１．SQISignを用いた高機能暗号化への応用は可能か。
２．SQISignの定数時間アルゴリズムは実現可能か。
３．数学的なアプローチによりSQISignのアルゴリズムの改良は可能か。(KLPTアルゴリズムの改良によるSQISignの実行時間の短縮など)

二つ目の目的は、数学や暗号学の専門家の横断的なチームを構成することで、暗号学の観点のみでは得られなかった知見から新たな暗号方式の提案を目指すことであった。その一環として、非公開セミナー１の講演者の一人である熊本大学の佐竹翔平氏との共同研究で、大きい内周を持つ3正則グラフ（Triplet graphs, Sextet graphs）の上でハッシュ関数を構成した。この共同研究結果[1]は国内研究集会「2022年情報とセキュリティシンポジウム」で講演し、査読付国際会議に論文を投稿予定である。

最近では、暗号学に使われている数学の範囲が大きく広がっている。整数論だけではなく、代数的グラフ理論、組合せ論、代数幾何学などの様々な数学分野の専門家の活躍により、多様な観点から既存の暗号方式の安全性を評価することが望まれる。本研究の意義として、同種写像暗号の安全性を調査・研究するのは暗号技術の開発や分析に貢献すると共に、様々な数学の専門家の暗号研究への新規参入を促し新たな暗号方式の開発などを目指すきっかけとなることがあげられる。

[1] H. Jo and S. Satake, “Cryptographic hash functions based on Triplet and Sextet graphs,” Proceedings of the 39th Symposium of Cryptography and Information Security (SCIS2022), 2022.

A number theoretic approach for Post-Quantum Cryptography related to Ramanujan graphs

Hyungrok Jo *

Yokohama National University, IAS

Contents

1 Introduction

This is a report of *"2021 IMI Joint research program - young researcher - short period joint workshop"*.

This research mainly studies on Isogeny-based cryptography which is one of main candidates in post-quantum cryptography. Moreover, we aim to suggest new cryptosystems which cannot be obtained by the existing cryptographic views, via organizing the crossing team of experts who specialized in various kinds of pure/applied mathematics and cryptography at university and industries. Comparing to other candidates of post-quantum cryptography such as Lattice-based cryptography, from the fact the key sizes of Isogeny-based cryptography are relatively smaller, it is expected in the near future that it is applicable to the devices which has the limitation of their memory. So, several large-sized enterprises (Microsoft, Mitsubishi electrics, etc) actively study on Isogeny-based cryptography for its usages in a real world. However, the historical record of Isogeny-based cryptography is short (about a decade), it has not undergone to analyze its security enough. A security of Isogeny-based cryptography is guaranteed by the hard problem of finding paths in the supersingular isogeny graphs which is known as one of the explicit Ramanujan graphs. Against this path-finding problem, the best way to find solutions so far is essentially a brute-force attack to find all possible paths. Actually, in this attack, it has not been considered the algebraic or number theoretical structure of supersingular isogeny graph, it seems reasonable to try to analyze a security of Isogeny-based cryptography by using these kinds of approaches. Therefore, in this research, we study on the elliptic curve theory, number theory, and algebraic graph theory related to the background of supersingular isogeny graphs. As a result, we aim to suggest much more safe security parameters and new cryptosystem. Moreover, we also encourage many experts who investigates on various

*jo-hyungrok-xz@ynu.ac.jp

mathematics related to this research to participate in the works on cryptography, for which affect the active collaborations with industries, universities, and governments.

1.1 Organizers

This joint research program is supported and accomplished by following committee members.

- Yusuke Aikawa (Mitsubishi Electric Corporation, Researcher)
- Yasuhiko Ikematsu (Kyushu University, Institute of Mathematics for Industry, Assistant Professor)
- Hyungrok Jo (Yokohama National University, Institute of Advanced Sciences, Assistant Professor)
- Noboru Kunihiro (University of Tsukuba, Faculty of Engineering, Information and Systems, Professor)
- Tomoki Moriya (Department of Mathematical Informatics, The University of Tokyo, Doctoral course 2nd year)
- Hiroshi Nozaki (Aichi University of Education, Department of Mathematics Education, Associate Professor)
- Hiroshi Onuki (Department of Mathematical Informatics, The University of Tokyo, Project Research Associate)
- Yoshinori Yamasaki (Ehime University, Graduate School of Science and Engineering, Professor)

1.2 Related work

Isogeny-based cryptography From the first suggestion of Couveignes [4] in 1997, which is republished in 2006, Isogeny-based cryptography has developed as one of promising candidates for post-quantum cryptography. Charles et al. [5] suggested cryptographic hash functions (CGL hash function) based on the explicit constructions of Ramanujan graphs, which is an optimal expander graphs in a spectral sense. The security of the schemes relies on the hardness of finding a path in the ℓ-isogeny supersingular graph between two given vertices. Especially, one of graphs from Pizer in CGL hash function, it is known that the graphs [18] have Ramanujan properties and also can be represented as supersingular elliptic curves and isogenies by the graph method [16]. It is well-explained in Déchène's work [6] for a beginner. A few years later, De Feo, Jao and Plût [8] proposed a Diffie-Hellman-like key exchange protocol based on supersingular isogeny graphs. In 2015, NIST (National Institute of Standards and Technology) announced a contest to standardize cryptographic algorithms (on PKE/KEM, DS) that are not known to be broken by quantum computers. Now in its third round, SIKE (`https://sike/org/` based on supersingular isogeny graphs) is considered as "alternate" for a next generation of public key exchange standard.

SQISign (Short Quaternion Isogeny Signature Scheme) The ℓ-isogeny path problems and their variants are considered as the underlying hard problems of Isogeny-based cryptography, one of the main candidates in Post-Quantum Cryptography. In ANTS2014, Kohel, Lauter, Petit, and Tignol [15] presented a probabilistic polynomial algorithm (in short, KLPT algorithm) to a mirror-side of ℓ-isogeny path problems in terms of quaternion algebras under the Deuring correspondence. In ASIACRYPT 2017, Galbraith et al. [13] presented two public key signature schemes whose security relies on computational assumptions relating to supersingular isogeny grpahs. Their second scheme is an identification protocol which relies on the difficulty of the problem of computing the endomorphism ring of a supersingular elliptic curve (i.e., computing an isogeny between two given elliptic curves), so that the public key is a supersingular

elliptic curve and the secret key is the endomorphism of the supersingular elliptic curve. The main key-idea of the scheme is to use the powersmooth version of KLPT algorithm to compute a "pseudo-canonical" isogeny which is independent of a given isogeny as the private key in the phase of the proof. In ASIACRYPT 2020, De Feo et al. [9] suggested a new interactive identification protocol and the signature scheme "SQI:Sign (for Short Quaternion and Isogeny Signature)" based on a generalized KLPT algorithm, which means to be suited for their signature scheme, efficiently. It gives the instantiation of the protocol, along with parameters targeting the NIST-1 level of post-quantum security.

Cryptographic applications based on algebraic graph and group theory Nowadays, many of cryptographic schemes are using certain properties of finite groups, it is fair to say they are mostly number theoretic in nature. Besides, only a few schemes make use of advanced group-theoretic tools[20] . One of the attempts to exploit group- or graph-theoretic problems for cryptographic constructions is from expander graphs which are actively used in network theory. Especially, Ramanujan graphs are known as optimal structures in the spectral aspect of expander graphs, which are good candidates for cryptographic usages. As mentioned before, CGL hash functions are based on the explicit constructions of Ramanujan graphs and their security lie on the path-finding problem in each graph. For a deep security analysis on these kinds of schemes, it is necessary to study the based group- or graph- knowledge such as elliptic curve theory, algebraic graph theory, group theory and so on.

1.3 A progress of program

This joint research is done with three separated parts as *open workshop, closed workshop 1* and *closed workshop 2*. The work progress is appeared in the table as below:

Date	**Summary**
Apr. 19	Organizing committee Kick-off meeting
Jul. 15	Organizing committee meeting
Aug. 30	Open workshop (zoom online)
Aug. 31 - Sep. 2	Closed workshop 1 (zoom online)
Dec. 13 - Dec. 17	Closed workshop 2 (on-site)

Open workshop
"Isogeny theory and its cryptographic applications"

We invited the following speakers from university and corporations for studying various fields related to isogeny theory. This workshop is recorded and can be watched via Youtube `https://youtu.be/sxTus5L_IG4`.

- Toshiyuki Katsura (The University of Tokyo)

  Title: *Decomposed Richelot isogenies of curves of genus* 3

- Yuta Kambe (Sugakubunka/Rikkyo University)

  Title: *Solving the constructive Deuring correspondence via the Kohel-Lauter-Petit-Tignol algorithm*

- Kenta Kodera (Mitsubishi Electric Corporation/Osaka University)

  Title: *Efficient algorithm for isogeny computation in CSIDH*

Closed seminar 1 (Remote)
"A number theoretic approach for Post-Quantum Cryptography related to Ramanujan graphs"

Figure 1: An academic exchange using a RPG-style meta-verse platform (gather.town)

- Yusuke Aikawa (Mitsubishi Electric Corporation, Researcher)

  Title: 同種写像暗号の進展:実用化へ向けて

- Tomoki Moriya (Department of Mathematical Informatics, The University of Tokyo, Doctoral course 2nd year)

  Title: イデアル類群を用いた同種写像暗号プロトコル

- Hiroshi Onuki (Department of Mathematical Informatics, The University of Tokyo, Project Research Associate)

  Title: 同種写像の計算公式について

- Momonari Kudo (Department of Mathematical Informatics, The University of Tokyo, Assistant Professor)

  Title: 種数4, 5の超特別曲線および超特異曲線の(非)存在性に関する最近の話題

- Hiroshi Nozaki (Aichi University of Education, Department of Mathematics Education, Associate Professor)

  Title: 固有値または内周が与えられた正則グラフの頂点数に対する線形計画限界

- Shohei Satake (Kumamoto University, Faculty of Advanced Science and Technology, Research Fellow)

  Title: 大きな内周とlocalizedな固有ベクトルをもつnear-Ramanujan graphの明示的構成に関して

- Hyungrok Jo (Yokohama National University, Institute of Advanced Sciences, Assistant Professor)

  Title: ラマヌジャン・グラフの明示的構成とその暗号への応用

- Shingo Sugiyama (Nihon University, Department of Mathematics, College of Science and Technology, Assistant Professor)

  Title: グラフ上の後戻りのない道の個数の非可換化と極限定理

- Yasuhiko Ikematsu (Kyushu University, Institute of Mathematics for Industry, Assistant Professor)

  Title: 同種写像パス探索問題に対するMITM攻撃について

Figure 2: Closed seminar 2 in Kyushu University IMI

Closed seminar 2 (On-site)
"Studies on SQISign"

Since SQISign is one of main interests of Isogeny-based cryptography in the late of 2020 and is also not easy to understand even its mathematical backgrounds and the relation between its security and construction, our committee members and attenders assigned each section of SQISign to ourselves, and we present our charged parts as follows:

- Yusuke Aikawa (Mitsubishi Electric Corporation, Researcher)

  Title: 準備　[SQISign論文の2章]

- Yasuhiko Ikematsu (Kyushu University, Institute of Mathematics for Industry, Assistant Professor)

  Title: シグマプロトコルについて

- Yota Maeda (Kyoto University, Department of Mathematics, Ph.D. course 1st year)

  Title: 四元代数の基礎[SQISign論文の4章]

- Tomoki Moriya (Department of Mathematical Informatics, The University of Tokyo, Doctoral course 2nd year)

  Title: KLPTアルゴリズム[KLPT2014]について

- Hyungrok Jo (Yokohama National University, Institute of Advanced Sciences, Assistant Professor)

  Title: Identification protocol [GPS2017]とその困難問題[EHL+2018]について

- Hiroshi Onuki (Department of Mathematical Informatics, The University of Tokyo, Project Research Associate)

  Title: 一般化されたKLPTアルゴリズム[SQISign論文の5,6章]とJuliaを用いた実装について

- Yusuke Aikawa (Mitsubishi Electric Corporation, Researcher)

  Title: ゼロ知識[SQISign論文の7章]について

- Hiroshi Onuki (Department of Mathematical Informatics, The University of Tokyo, Project Research Associate)

  Title: 効率性[SQISign論文の8章]について

2 Results and after the joint research program

We discussed about the security assumption and construction of signature scheme of SQISign mainly in closed seminar 2. We suggest the future works using SQISign or improving the efficiency of SQISign.

On the other hand, through closed seminar 1, as a cowork with Shohei Satake in Kumamoto University, we discussed about the possibility to build "Crytptographic hash functions based on Triplet graphs and Sextet graphs" which result is presented in SCIS2022 [14]. These works are supported by IMI Collaborative Research and undergoing in provided circumstances.

2.1 Result 1 : Thoughts on SQISign with Isogeny group

We raised up some future works related to SQISign.

(1) Is it possible to apply it to high functional cryptosystems?

(2) How could it be realized the constant time algorithms for SQISign?

(3) Are there any possibilities to improve its execution time or memories in mathematical treatments? (Improving generalized KLPT algorithms?)

For **(1)**, it seems make sense that build some kinds of high functional cryptosystems, especially signature schemes (such as aggregate signatures, ring signatures or group singnatures and so on.) if it guarantees that their security assumption lies on computational endomorphism ring problems well.

For **(2)**, it could be a good contribution for the efficiency of SQISign if it realizes. However, it means that it is necessary to specify constant time algorithm of KLPT's, it is a quite bit of challenging task.

For **(3)**, in recent (2022.Feb.23.), there is an improvement on KLPT algorithm which insists on accelerating SQISign twice [10]. There are some potentials to improve on KLPT algorithms by specific modifications of strong approximation step (solutions to diophantine norm equations of targeting elements in special order).

2.2 Result 2 : A proposal of a hash function based on arc-transitive graphs with Shohei Satake

In SCIS2022 [14], we propose new constructions of cryptographic hash functions based on two families of non-bipartite cubic graphs, namely, triplet graphs and sextet graphs. The main idea is to construct hash functions by choosing a walk in these graphs according to a given message, and define the output as the end vertex of the walk. Triplet and sextet graphs have some advantages as underlying graphs of hash functions. First triplet graphs have large girth, which positively effects to the (weak/strong) collision resistance of the proposed hash function. It is also conjectured that sextet graphs would have large girth as well, where small-size graphs in fact have large girth. Second we discussed the relationship between collision resistance of our proposed hash functions and group word problems and generic attacks (the birthday attack, the rho method) in the aspect of security analysis.

2.3 After the joint research program

One of main purposes of this joint research program is encouraging the mathematician in many fields to get in cryptography. For this purpose, Ramanujan graph is a good object which brings people together under beautiful mathematics even in cryptography. Seen from the resume of Isogeny-based cryptography, CGL hash functions play an important role in past even now.

A cryptographic hash function is a ubiquitous tool for various uses in cryptography such as digital signatures, public-key encryption, integrity verification, message authentication, password protection and key agreement protocols. If it is possible to develop a hash function based

on a mathematically difficult problem, various contributions can be expected in cryptography that is secure as a primitive. These studies are well worth not only providing the cryptographic primitives but also contributing security analysis using advanced mathematical tools.

References

[1] N. L. Biggs, "Graphs with large girth," *Ars Combin.*, vol. 25-C, pp. 73–80, 1988.

[2] N. L. Biggs, *Algebraic Graph Theory*, Second edition. Cambridge University Press, 1993.

[3] N. L. Biggs and M. L. Hoare, "The sextet construction for cubic graphs," *Combinatorica*, vol. 3, no. 2, pp. 153–165, 1983.

[4] J. M. Couveignes, "Hard Homogeneous Spaces", IACR Cryptol. ePrint Arch., 2006, 291.

[5] D. X. Charles, K. E. Lauter and E. Z. Goren, "Cryptographic hash functions from expander graphs," *J. Cryptol.*, vol. 22, no. 1, pp. 93-113, 2009.

[6] I. Déchène, I. "Quaternion algebras and the graph method for elliptic curves", Master's Thesis, *Department of Mathematics and Statistics, McGill University, Montreal*, 1998.

[7] M. Deuring, "Die typen der multiplikatorenringe elliptischer funktionenkörper", In Abhandlungen aus dem mathematischen Seminar der Universität Hamburg, 14(1), Springer-Verlag, pp: 197–272, 1941.

[8] L. De Feo, D. Jao, J. and Plût,"Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies,", *Journal of Mathematical Cryptology*, 8(3), pp. 209-247, 2014.

[9] L. De Feo, D. Kohel, A. Leroux, C. Petit and B. Wesolowski,"SQISign: compact post-quantum signatures from quaternions and isogenies", *ASIACRYPT2020*, `https://eprint.iacr.org/2020/1240.pdf`.

[10] L. De Feo, A. Leroux and B. Wesolowski, "New algorithms for the Deuring correspondence: SQISign twice as fast", `https://eprint.iacr.org/2022/234`

[11] K. Eisenträger, S. Hallgren, K. Lauter, T. Morrison and C. Petit, "Supersingular isogeny graphs and endomorphism rings: reductions and solutions," *In Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 329-368, Springer, Cham., 2018.

[12] E. Fuchs, K. E. Lauter, M. Litman and A. Tran, "A cryptographic hash function from Markoff Triples," arXiv preprint arXiv:2107.10906.

[13] S. D. Galbraith, C. Petit and J. Silva, "Identification protocols and signature schemes based on supersingular isogeny problems," *In International Conference on the Theory and Application of Cryptology and Information Security*, pp. 3-33, Springer, Cham., 2017.

[14] H. Jo and S. Satake, "Cryptographic hash functions based on Triplet and Sextet graphs," *Proceedings of the 39th Symposium of Cryptography and Information Security (SCIS2022)*, 2022.

[15] D. Kohel, K. Lauter, C. Petit and J.P. Tignol, "On the quaternion l-isogeny path problem", *LMS Journal of Computation and Mathematics* 17(A), pp: 418–432, 2014.

[16] J. F. Mestre, A. T. Jorza, "The Method of Graphs. Examples and Applications", Notes, 2011.

[17] C. Peng, J. Chen, L. Zhou, K. K. R. Choo and D. He, "CsiIBS: A post-quantum identity-based signature scheme based on isogenies," *Journal of Information Security and Applications*, 54, 102504, 2020.

[18] A. K. Pizer, "Ramanujan graphs", AMS IP STUDIES IN ADVANCED MATHEMATICS, 7, pp: 159–178, 1998.

[19] S. Shaw and R. Dutta, "Identification Scheme and Forward-Secure Signature in Identity-Based Setting from Isogenies," *In International Conference on Provable Security*, pp. 309-326, Springer, Cham, 2021.

[20] M. I. G. Vasco and R. Steinwandt, "Group theoretic cryptography", (9). CRC Press, 2015.

九州大学 IMI 共同利用・短期共同研究　公開プログラム

同種写像理論とその暗号への応用
Isogeny theory and its cryptographic applications

日時：　2021年8月30日（月）13：00 〜 16：40
場所：　Zoomミーティングによるオンライン開催
代表者：　筑波大学　Jo Hyungrok

8月30日（月）

13：00-13：10　Opening remark

13：10-14：10
講演者　　：桂 利行（東京大学大学院数理科学研究科・特任教授）
講演タイトル：Decomposed Richelot isogenies of curves of genus 3

14：20-15：20
講演者　　：神戸 祐太（立教大学理学部数学科/すうがくぶんか・講師）
講演タイトル：Solving the constructive Deuring correspondence via the Kohel-Lauter-Petit-Tignol algorithm

15：30-16：30
講演者　　：小寺 健太（大阪大学大学院工学研究科/三菱電機情報技術総合研究所・研究員）
講演タイトル：同種写像暗号 CSIDH の高速化に向けた効率的な同種写像計算

16：30-16：40　Closing remark

※研究実施期間：2021 年 8 月 30 日(月)〜9 月 2 日（木）
8 月 31 日(火)〜9 月 2 日（木）は非公開

講演者　　：桂 利行（東京大学大学院数理科学研究科・特任教授）
講演タイトル：Decomposed Richelot isogenies of curves of genus 3
アブストラクト：
標数 p が 2 ではない代数的閉体 k 上の種数 3 の非特異射影代数曲線に対し、その Jacobian 多様体が分解する Richelot isogeny をもつための必要十分条件を与え、分解する場合の代数曲線の構造を明らかにする。

講演者　　：神戸 祐太（立教大学理学部数学科/すうがくぶんか・講師）
講演タイトル：Solving the constructive Deuring correspondence via the Kohel-Lauter-Petit-Tignol algorithm
アブストラクト：
素数 p について、E_0 を F_{pˆ2} 上の超特異楕円曲線とする。 このとき、 Deuring 対応と呼ばれる End(E_0)の左イデアル I と E_0 を定義域とする同種写像 ¥phi:E_0 → E_I の間の一対一対応が存在する。 タイトルにある構成的 Deuring 対応問題とは、与えられた左イデアル I に対して E_I の j-不変量を計算する問題である。
本講演では構成的 Deuring 対応問題の求解法として Kohel-Lauter-Petit-Tignol アルゴリズム（KLPT アルゴリズム）を用いた方法を紹介し、実際に 25 ビット程度の標数における計算例の紹介やデモンストレーションを行う。

講演者　　：小寺 健太（大阪大学大学院工学研究科/三菱電機情報技術総合研究所・研究員）
講演タイトル：同種写像暗号 CSIDH の高速化に向けた効率的な同種写像計算
アブストラクト：
近年、耐量子暗号と呼ばれる、量子計算機を用いた攻撃に耐えうる暗号の研究が盛んに行われている。耐量子暗号の候補の 1 つの同種写像暗号がある。例えば 2018 年に Castryck らによって提案された CSIDH は、公開鍵長が非常に短いという特長がある一方で実行時間に課題がある。そこで本研究では CSIDH の主要な計算である同種写像の計算手法を改良し、高速化を目指す。
一般に同種写像の計算には核に含まれる点の座標が必要となる。既存の手法では加法公式を用いて核の点のうち約半数の座標を計算していた。本研究では加法公式を元に核の点における関係式を導出し、より少数の点の座標から同種写像を計算する手法を提案する。

九州大学 IMI 共同利用・短期共同研究　非公開講演会

ラマヌジャン・グラフの整数論による耐量子計算機暗号へのアプローチ

A number theoretic approach for Post-Quantum Cryptography related to Ramanujan graphs

日時：　2021年8月31日（火）から9月2日（金）まで、10：00 〜 16：00
場所：　Zoomミーティングによるオンライン開催
代表者：　筑波大学　Jo Hyungrok

8 月 31 日（火）

10：00-11：00
講演者　　：相川 勇輔（三菱電機株式会社情報技術総合研究所・研究員）
講演タイトル：同種写像暗号の進展：実用化へ向けて

11：00-11：30　討議

13：00-14：00
講演者　　：守谷 共起（東京大学大学院情報理工学系研究科数理情報学専攻・博士課程 2 年）
講演タイトル：イデアル類群を用いた同種写像暗号プロトコル

14：00-14：30　討議

14：30-15：30
講演者　　：小貫 啓史（東京大学大学院情報理工学系研究科数理情報学専攻・特任研究員）
講演タイトル：同種写像の計算公式について

15：30-16：00　討議

9 月 1 日（水）

10：00-11：00
講演者　　：工藤 桃成（東京大学大学院情報理工学系研究科・助教）
講演タイトル：種数 4，5 の超特別曲線および超特異曲線の(非)存在性に関する最近の話題

11：00-11：30　討議

13：00-14：00
講演者　　：野崎 寛（愛知教育大学数学教育・准教授）
講演タイトル:固有値または内周が与えられた正則グラフの頂点数に対する線形計画限界

14：00-14：30　討議

14：30-15：30
講演者　　：佐竹 翔平（熊本大学 大学院先端科学研究部・特別研究員）
講演タイトル：大きな内周と localized な固有ベクトルをもつ near-Ramanujan graph の明示的構成に関して

15：30-16：00　討議

9月2日（木）

10：00-11：00
講演者　　：Jo Hyungrok（筑波大学システム情報系・研究員）
講演タイトル：ラマヌジャン・グラフの明示的構成とその暗号への応用

11：00-11：30　討議

13：00-14：00
講演者　　：杉山真吾（日本大学理工学部数学科・助手）
講演タイトル：グラフ上の後戻りのない道の個数の非可換化と極限定理

14：00-14：30　討議

14：30-15：10
講演者　　：池松 泰彦（九州大学マス・フォア・インダストリ研究所・助教）
講演タイトル：同種写像パス探索問題に対する MITM 攻撃について

15：10-15：30　討議

ＨＰ掲載用英文

Speaker: Yusuke Aikawa (Mitsubishi Electric)
Title: Development of isogeny-based cryptography: toward practical use

Speaker: Tomoki Moriya (The Univ. of Tokyo)
Title: Isogeny based cryptosystems via ideal class groups

Speaker: Hiroshi Onuki (The Univ. of Tokyo)
Title: On formulas for computing isogenies

Speaker: Momonari Kudo (The Univ. of Tokyo)
Title: Recent developments on the study of the (non-)existence of superspecial curves and supersingular curves of genera four and five

Speaker: Hiroshi Nozaki (Aichi Univ. of Education)
Title: Linear programming bounds on the order of a regular graph given eigenvalues or girth

Speaker: Shohei Satake (Kumamoto Univ.)
Title: On explicitly constructing high-girth near-Ramanujan graphs with localized eigenvectors

Speaker: Hyungrok Jo (Univ. of Tsukuba)
Title: Explicit constructions of Ramanujan graphs and their cryptographic applications

Speaker: Shingo Sugiyama (Nihon Univ.)
Title: A non-commutative version of the number of non-backtracking paths on a graph and its limit theorem

Speaker: Yasuhiko Ikematsu (Kyushu Univ. IMI)
Title: Hybrid meet-in-the-middle attacks for the isogeny path-finding problem

九州大学 IMI 共同利用・短期共同研究 第２弾非公開セミナー

ラマヌジャン・グラフの整数論による耐量子計算機暗号へのアプローチ

A number theoretic approach for Post-Quantum Cryptography related to Ramanujan graphs

日時：　2021年12月13日（月）から12月17日（金）まで、10：00 〜 17：00
場所：　九州大学伊都キャンパス理学部
代表者：　横浜国立大学先端科学高等研究院　Jo Hyungrok

研究概要：
本研究では、近年注目を集めている同種写像ベースの電子署名方式 SQISign の勉強会を行うことで、その構成や安全性および効率性について参加者全員が深く理解し、同種写像問題に基づいた電子署名方式の新たな研究テーマを探索する。
[https://eprint.iacr.org/2020/1240.pdf]

12 月 13 日（月）

14：00-15：00
講演者　：相川 勇輔（三菱電機株式会社情報技術総合研究所・研究員）
講演内容　：準備　[SQISign 論文の 2 章]

15：00-17：00　討議（アイデアの共有と課題点の模索）
予想内容：
- 既存のSQISignスキームのパート別の改良（KLPTアルゴリズムの高速化など）
- 他の同種写像問題基盤スキームを新たに提案
- 同種写像ベース計算困難問題に集中

12 月 14 日（火）

10：00-12：00
講演者　：池松 泰彦（九州大学マス・フォア・インダストリ研究所・助教）
講演内容　：シグマプロトコルについて
[https://cs.au.dk/~ivan/Sigma.pdf]

13：30-14：00　自由討論

14：00-17：00
講演者　：前田 洋太（ソニーグループ株式会社 R&D センター 先端研究部・研究員）
講演内容　：四元代数の基礎[SQISign 論文の 4 章]

12 月 15 日（水）

10：00-12：00
講演者　　：守谷 共起（東京大学大学院情報理工学系研究科数理情報学専攻・博士課程 2 年）
講演内容　：KLPT アルゴリズム[KLPT2014]について

14：00-16：00
講演者　　：Jo Hyungrok（横浜国立大学先端科学高等研究院・特任助教）
講演内容　：Identification protocol [GPS2017]とその困難問題[EHL+2018]について

16：00-17：00　自由討論

12 月 16 日（木）

10：00-12：00
講演者　　：小貫 啓史（東京大学大学院情報理工学系研究科数理情報学専攻・特任助教）
講演内容　：一般化された KLPT アルゴリズム[SQISign 論文の 5,6 章]と Julia を用いた実装について

14：00-16：00
講演者　　：相川 勇輔（三菱電機株式会社情報技術総合研究所・研究員）
講演内容　：ゼロ知識[SQISign 論文の 7 章]について

16：00-17：00　自由討論

12 月 17 日（金）

10：00-11：30
講演者　　：小貫 啓史（東京大学大学院情報理工学系研究科数理情報学専攻・特任助教）
講演内容　：効率性[SQISign 論文の 8 章]について

11：30-12：30　まとめ（研究報告書）