公開

研 究 終 了 報 告 書

「楕円曲線を用いた耐量子計算機暗号の安全性解析と高効率化」

研究期間： 2020 年 11 月～2023 年 3 月
研 究 者： 相川　勇輔

1．　研究のねらい

情報ネットワークで繋がった高度な情報化社会を実現していくためには、情報セキュリティ技術によって通信の安全を保障する必要がある。そのような情報セキュリティ技術は、様々な技術の複合体として構成されるが、根幹を成す技術として暗号技術である。本研究は公開鍵暗号技術をターゲットとし、その高安全および高効率化に寄与することを狙った。

公開鍵暗号はその安全性の根拠として数学的問題の計算量的困難性を利用するため、安全性の解析にはそのような問題を解くアルゴリズムの開発およびその効率化が重要である。一方で、暗号アルゴリズムは様々な数学的演算を用いて構成されるため、暗号の効率性については、これらの演算を効率的に実行するアルゴリズムの構成や、それらの演算の効率性の限界を知る必要がある。

現在、主に利用されている公開鍵暗号は RSA 暗号と楕円曲線暗号である。これらは素因数分解問題や群の離散対数問題の計算量的困難性に安全性の根拠を置く。そのため、これらの問題を効率的に解くアルゴリズムが発見された場合、RSA 暗号や楕円曲線暗号は危殆化する。

現在量子コンピュータの開発が世界中で盛んに進められているが、量子コンピュータで動くアルゴリズムに Shor のアルゴリズムがある。このアルゴリズムはこれらの問題を多項式時間で解くことが知られている。このことは、十分な規模の量子コンピュータが実現した社会においては、RSA 暗号や楕円曲線暗号はもはや安全でなくなることを意味する。従って、量子コンピュータによる暗号解読に対しても安全な暗号、すなわち耐量子計算機暗号の研究開発が急務である。

本研究では耐量子計算機暗号の重要な候補である同種写像暗号を研究ターゲットとした。同種写像暗号は超特異楕円曲線の同種写像問題の計算量的困難性にその安全性の根拠を置く暗号で、鍵サイズや暗号文サイズ等のデータサイズが耐量子計算機暗号候補の中で最も小さいという利点を持つ。一方で、2010 年ごろから研究がはじまった比較的新しい暗号であり、その安全性への信頼を高める必要がある。さらに、暗号アルゴリズム内部で楕円曲線のスカラー倍や同種写像計算を週十回～数百回程度実行するため計算量が重いという欠点がある。そこで本研究では、現状では同種写像問題を解く新たなアルゴリズムの構成および、同種写像計算の高効率化を図ることで、同種写像暗号の高安全および高い効率化をねらった。

2. 研究成果

(1)概要

本研究では、耐量子計算機暗号の数学的手法による安全性解析および効率性に関する研究を実施した。

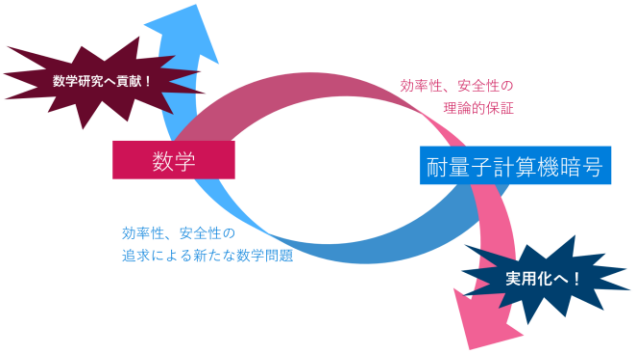


図 1

現在主に利用されている公開鍵暗号である RSA 暗号や楕円曲線暗号は、大規模な量子コンピュータが実現した場合、危殆化することが知られている。そこで、暗号の安全性の根拠を与える数学的問題(素因数分解問題および群の離散対数問題)を刷新することによって、未来に実現することが予想される量子情報化社会における情報通信の安全性を確保するために、量子コンピュータによる解読にも耐えうる暗号技術の研究開発が進められている。そのような暗号を総称して耐量子計算機暗号とよぶ。実際、実用化へ向けて 2016 年より NIST(アメリカ国立標準技術研究所)による耐量子計算機暗号の標準化方式の選定が進められている。

耐量子計算機暗号の有望な候補として主に、格子暗号、符号暗号、多変数多項式暗号および同種写像暗号が知られている。これらはその構成の土台とする数学が異なるために、その暗号としての特徴も異なる。格子暗号や符号暗号は計算効率性の高い方式である、その歴史も比較的古く、その安全性への信頼は高い。しかしながら、暗号文サイズや鍵サイズが大きいという欠点がある。多変数多項式暗号は、比較的データサイズの小さい署名方式の構成が可能であるが、近年著しく安全性解析が進展しており、安全性に関しては注視していく必要がある。そのような中で、同種写像暗号はデータサイズの小さい暗号方式を作ることができ、将来的には組み込み機器等のメモリ環境のシビアな状況での実装が期待されている。そこで、そのようなユースケースを見越し、本研究では同種写像暗号を研究ターゲットとする。

しかし、同種写像暗号の研究が本格的に始まったのが 2010 年頃と新しい方式であり、安全性解析の研究を進める必要がある。また、暗号アルゴリズム内部で楕円曲線のスカラー倍演算と同種写像演算を数十～数百回実行する必要があるために効率性にも課題を抱える。一方で、同種写像暗号の特徴として、その暗号学としての研究の中から新たな数学問題が多く掘り出されている。

そこで、本研究では数学的手法で同種写像暗号のこれらの課題解決を通しその実用化に向けて貢献するとともに、同種写像暗号の研究の中から新たな数学問題を定式化し、その解決を目指した(図1)。より具体的に、本研究では最終的に次の研究テーマを実施し、成果を挙げた(成果文献番号は本項(2)詳細の下部より):

1. 四元数代数を用いた同種写像問題の解読アルゴリズムの開発:[1],[2]
2. 同種写像計算を含む楕円曲線上の演算の効率性に関する研究:[4]
3. 超特別アーベル多様体の同種写像グラフのスペクトラルギャップの研究:[5]

また、本研究期間中に同種写像暗号のサーベイ論文の執筆を行い採択されている[3]。

（2）詳細

研究テーマ1：四元数代数を用いた同種写像問題の解読アルゴリズムの開発

超特異楕円曲線が二つ与えられたとき、それらの間の同種写像を求める問題を同種写像問題とよぶ。同種写像暗号はこの問題に帰着される問題の計算量的困難性に安全性の根拠を置く暗号のことである。つまり、同種写像問題を効率的に解くことができれば、同種写像暗号は危殆化したことになる。そのため、同種写像問題の困難性を解析することは同種写像暗号の安全性の解析に直結するため、この問題の求解アルゴリズムの理論的構成や、その実装実験の知見を蓄えることは、暗号の社会実装を行っていく上で必須の研究課題である。

しかしながら、同種写像問題に対するジェネリックな求解アルゴリズムは本質的に全数探索しか知られていない。そこで、本研究では、全数探索とは異なる整数論を用いた安全性解析手法の開発を目的とした。より具体的には、超特異楕円曲線の自己準同型環が四元数代数の極大整環と同型であることを利用し、四元数代数側で同種写像問題の類似問題を解くことで、同種写像問題のインスタンスに対する同種写像を復元する、というアイデアから求解アルゴリズムの開発を目指した（図2）。

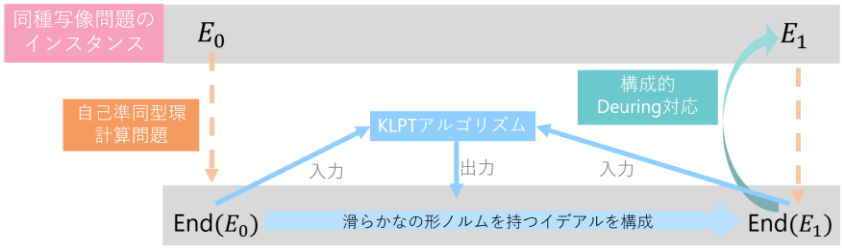


図 2

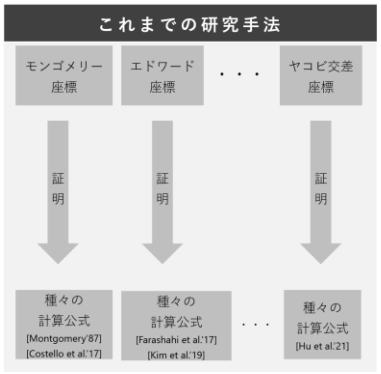
このとき重要な役割を果たすのが、KLPT アルゴリズム、構成的 Deuring 対応アルゴリズムおよび自己準同型環計算問題である。我々はまず KLPT アルゴリズムの改良の研究に取り組んだ。これは同種写像問題の四元数代数類似の求解アルゴリズムであり、入力されたイデアルに対し、それと同値なイデアルであって滑らかなノルムを持つイデアルを出力する。このアルゴリズムは Kohel らによって理論的な構成はされていたが、実装実験の数が少なく、さらに一般に出力サイズが大きくなるという欠点があった。KLPT アルゴリズムの出力サイズは、同種写像を復元するアルゴリズムである構成的 Deuring 対応アルゴリズムの計算量に直結するため大きな課題であった。そこで我々は KLPT アルゴリズムを詳細に解析し、出力に影響を与える因子を特定することによって改良を加えアルゴリズムの効率化に成功した。それに加え我々のアルゴリズムを実装し実験を行った。その結果、45 ビット標数における実装実験で、既存方式に比べ出力サイズを 16%削減するとともに実行時間を 65%削減することに成功した。本結果は国際会議 International Conference on Mathematics and Computing に採択されている[1]。

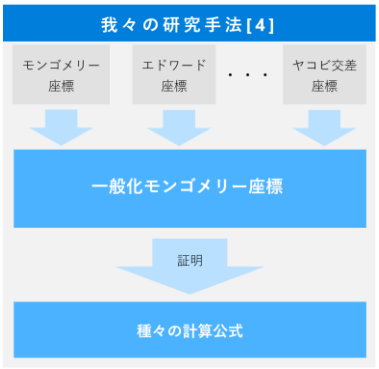
続いて我々は KLPT アルゴリズムによって出力されたイデアルから同種写像を復元するアルゴリズムである構成的 Deuring 対応アルゴリズムの研究に取り組んだ。このアルゴリズムについてはナイーヴな手法による 10 ビット標数程度の実験例しか与えられていない状況であった。実際、このアルゴリズムでは楕円曲線のねじれ点生成ステップにおける等分多項式計算がボトルネックとなっていた。そこで我々は[1]で得られた結果に加え、同種写像の Symbolic

Fomula を応用しアルゴリズムを改良することで、このステップの計算量削減に成功した。その結果、既存手法を大きく上回る 25 ビット標数に対する実装例を構成した。この結果は数理暗号の主要な国際会議である MathCrypt に採択され、国際雑誌 Mathematical Cryptology より出版された。

研究テーマ2：同種写像計算を含む楕円曲線上の演算の効率性に関する研究

同種写像暗号のアルゴリズムは、そのほとんどの方式が楕円曲線上のスカラー倍演算と同種写像演算を数十～数百回繰り返し行うことで構成される。スカラー倍演算は従来の楕円曲線暗号でも利用されているため研究が十分に進んでいる。そのため、同種写像暗号の計算効率性を理解するためには、同種写像演算の効率性を理解することが課題となっている。





同種写像演算でしばしば用いられる手法が、二つの座標を持つ楕円曲線上の点を射影直線上の点に変換し、一つの座標で計算公式を記述するものである。このように得られた公式を単一座標公式と呼ぶことにする。

楕円曲線は様々なモデルを持つが、モデルごとに射影直線上の点への変換が異なる。既存研究ではそれらを用いることで、モンゴメリーモデル、エドワードモデル、ハフモデルおよびヤコビ交差モデルなどといった主要なモデルに対して単一座標公式が構成され、効率性の比較が論じられてきた。しかしながら、それらの研究が示すことは効率性の差が数%の差に収まるということであった。

そこで我々はこれらの単一座標構成が本質的に同じものであるという着想の下、これらの構成の一般化を行った。その結果得られたのが、一般の楕円曲線上で定義される座標としてしかるべき機能を有した関数である一般化モンゴメリー座標と名付けた概念である。我々はこの関数を利用し、スカラー倍演算や同種写像演算の公式を記述することで、既存手法の多くが本研究のフレームワークの中に入ることを示した（図3）。さらに、各モデル間の公式の差が一般化モンゴメリー座標に対する等分多項式から生じることを示し、効率性の差が高々この多項式の演算分しか生じないことを示した。

この結果をまとめた論文は数理暗号の主要な国際会議である MathCrypt に採択され、国際雑誌 Mathematical Cryptology より出版された。

研究テーマ3：超特別アーベル多様体の同種写像グラフのスペクトラルギャップの研究

超特異楕円曲線を利用した暗号方式の高次元類似を考えることで、超特別アーベル多様体の数論の研究が進展している。特に、Castryck らによる超特別アーベル多様体の同種写像グラフ（頂点が超特別アーベル多様体からなり、辺は同種写像で結ぶことで構成される）を利

用した暗号学的ハッシュ関数の構成によって、そのグラフの構造を理解することが重要な研究課題となった。

本研究では、ACT-X 一期生の田中亮吉氏（京大）との共同研究で、超特別アーベル多様体のスペクトラルギャップに関する研究を行った。これまでの研究では、Katsura らの研究によって同種写像グラフの各頂点からどのように辺が伸びているかという組み合わせ論的研究が進められており、さらに Jordan らによってグラフの連結性が証明されていた。しかしながら、Castryck らによるハッシュ関数の構成はグラフ上のランダムウォークを利用するものであるが、その終点の一様性については解答が得られていなかった。

そこで我々は超特別アーベル多様体の同種写像グラフを標数に関するグラフ族ととらえそれらのスペクトラルギャップの研究を実施した。その結果、スペクトラルギャップを抑える標数に依らない定数が存在することを証明し、その定数を明示的に与えた。このとこは超特別アーベル多様体の同種写像グラフ族がエクスパンダーグラフに類する族（有向多重グラフのため厳密にはエクスパンダーグラフとは言えない）となっているということであり、暗号応用上妥当な性質を持つことを意味する。

本結果をまとめた論文は現在国際雑誌に投稿中である。

文中で用いた成果番号：

[1] Kambe, Y., Aikawa, Y., Kudo, M., Yasuda, M., Takashima, K., Yokoyama, K. (2022). Implementation Report of the Kohel-Lauter-Petit-Tignol Algorithm for the Constructive Deuring Correspondence. In: Giri, D., Raymond Choo, KK., Ponnusamy, S., Meng, W., Akleylek, S., Prasad Maity, S. (eds) Proceedings of the Seventh International Conference on Mathematics and Computing . Advances in Intelligent Systems and Computing, vol 1412. Springer, Singapore.

[2] Yuta Kambe, Masaya Yasuda, Masayuki Noro, Kazuhiro Yokoyama, Yusuke Aikawa, Katsuyuki Takashima, Momonari Kudo, Solving the Constructive Deuring Correspondence via the Kohel-Lauter-Petit-Tignol Algorithm, Mathematical Cryptology, 1(2), 10-24.

[3] Yusuke Aikawa, Post-Quantum Cryptography from Supersingular Isogenies (Theory and Applications of Supersingular Curves and Supersingular Abelian Varieties), RIMS Kôkyûroku Bessatsu B90: 97-116, June, 2022.

[4] Tomoki Moriya, Hiroshi Onuki, Yusuke Aikawa, Tsuyoshi Takagi, The Generalized Montgomery Coordinate: A New Computational Tool for Isogeny-based Cryptography, Mathematical Cryptology, 2(1), 36-59.

[5]Yusuke Aikawa, Ryokichi Tanaka, Takuya Yamauchi, Isogeny graphs on superspecial abelian varieties: Eigenvalues and Connection to Bruhat-Tits buildings, preprint(arXiv:2201.04293).

3. 今後の展開

今後も引き続き同種写像暗号を軸とし、耐量子計算機暗号の社会実装に貢献していく。本研究実施期間中に、NIST 標準化ラウンド4まで進出していた有望な同種写像ベースの暗号化方式である SIKE(Supersingular Isogeny Key Encapsulation)方式が Casrtyck らによって

解読された。そのため標準化候補からの落選が NIST より今後発表される見込みである。さらに、その攻撃手法の威力により方式の修復も困難と思われる。

一方で、本研究実施期間中に同種写像ベースのデジタル署名方式である SQISign(Short Quaternion and Isogeny Signature)方式が De Feo らによって提案された。この方式は格子ベースの方式に比較すると署名生成効率が著しく悪いが（実時間の計測で 10,000 倍のオーダーで差がある）、一方で署名サイズが 204 バイト、秘密鍵サイズが 16 バイト、公開鍵サイズが 64 バイトとコンパクトな方式を実現している（1,000 倍のオーダーで差がある）。NIST は耐量子デジタル署名方式の不足から 2023 年に再公募をかけることを発表しており、SQISign 方式は応募される見込みである。

そこで、これまでの研究では特定の方式に依らないジェネリックな状況での研究を推進してきたが、今後は SQISign 方式の社会実装に向けた高安全パラメータ提案や効率化手法の研究を推進する。特に、SQISign 方式では特殊な入力パラメータに対する KLPT アルゴリズムや構成的 Deuring 対応が本質的な役割を果たしており、本研究で得られている（一般の入力に対する）これらアルゴリズムの知見を活かせるものと思われる。耐量子計算機暗号への切り替えのマイルストンが 2030 年であることから、2026 年を目途に高安全独自パラメータ生成、安全性解析および効率性の研究を中心に進め、その後は平行して 2028 年を目途に独自ライブラリの実装を行い、そこから社会への提供を目指す。

4. 自己評価

本研究では当初より同種写像暗号の安全性解析をメインテーマに据えていた。本テーマに関しては、自己準同型環計算アルゴリズムの研究の難しさから当初の計画よりも研究を進めることができなかったが、アイデアを共有できる共同研究者にも恵まれ査読付き論文 2 本（＋準備中論文 1 本）の形にまとめることができ着実に前進することができた。この研究では四元数代数の理論を暗号の安全性解析に応用するという数学/暗号双方の専門性を持つという独自性を出すことができた。

さらに、当初の計画には無かった研究ではあるが、ACT-X 内での交流から超特別アーベル多様体の同種写像グラフのスペクトラルギャップの評価という難問に取り組むことができ、最終的に解決することができた。スペクトラルギャップの評価は代数的グラフ理論の中心的問題であるだけでなく、この結果はアーベル多様体を利用した同種写像暗号の安全性の保障に一定の解答を与えるものであり、その影響力からプレプリント公開後に当該分野の国内外研究者から問い合わせをいただき研究者ネットワークの拡大につながった。さらに本研究は、異分野研究者間で知識を交換し合いながら議論を進めるという経験も得られた。

本研究期間中は、これらの研究が評価され、計 9 件の招待講演を行う機会も得ることができた。それらの機会を通して研究成果を社会に対し報告することができただけでなく、整数論や暗号のコミュニティだけでなくグラフ理論、計算量理論および量子情報の研究者コミュニティにもネットワークを形成することができた。

研究費執行について、20 年度は計画通り論文調査/作成用ラップトップおよびタブレット端末の購入等で執行できた。一方で、21 年度は研究費のほとんどを旅費として申請していたが、新型コロナウイルスの影響が想定以上に長引いたため計画通りの執行が行えなかっ

た。22 年度も同様にほとんどを旅費として計画していたが、当該年度は新型コロナウイルスの影響も前年度に比較して小さく、ほぼ計画通りに執行できる見込みである。

5. 主な研究成果リスト

（1）代表的な論文（原著論文）発表

研究期間累積件数：4件

1. Kambe, Y., Aikawa, Y., Kudo, M., Yasuda, M., Takashima, K., Yokoyama, K. (2022). Implementation Report of the Kohel-Lauter-Petit-Tignol Algorithm for the Constructive Deuring Correspondence. In: Giri, D., Raymond Choo, KK., Ponnusamy, S., Meng, W., Akleylek, S., Prasad Maity, S. (eds) Proceedings of the Seventh International Conference on Mathematics and Computing . Advances in Intelligent Systems and Computing, vol 1412. Springer, Singapore.
同種写像問題の安全性解析における重要なアルゴリズムに KLPT アルゴリズがある。これは四元代数の極大オーダーの左イデアル I が与えられたときに、I に同値な左イデアル J であって滑らかなノルムを持つものを出力する。このアルゴリズムは出力サイズが大きくなる傾向があった。本研究ではアルゴリズムを改良することによって、45 ビット標数での実験において、既存手法より出力サイズを 16%削減するとともに実行時間を 65%削減することに成功した。相川はアルゴリズムの改良パートを主導した。
2. Yuta Kambe, Masaya Yasuda, Masayuki Noro, Kazuhiro Yokoyama, Yusuke Aikawa, Katsuyuki Takashima, Momonari Kudo, Solving the Constructive Deuring Correspondence via the Kohel-Lauter-Petit-Tignol Algorithm, Mathematical Cryptology, 1(2), 10-24.
同種写像問題の安全性解析における重要なアルゴリズムに構成的 Deuring 対応アルゴリズムがある。このアルゴリズムは、ねじれ点を取りながら逐次的に同種写像を計算していくため、一般に演算を行う体が拡大していくことがボトルネックとなる。本研究では、論文 1.の結果および同種写像の Symbolic Formula を応用することで、アルゴリズムの効率化に成功し、10 ビット程度の実装例しかなかった本アルゴリズムに対し、25 ビットの実装例を構成した。相川はアルゴリズムの改良パートを主導した。
3. Tomoki Moriya, Hiroshi Onuki, Yusuke Aikawa, Tsuyoshi Takagi, The Generalized Montgomery Coordinate: A New Computational Tool for Isogeny-based Cryptography, Mathematical Cryptology, 2(1), 36-59.
楕円曲線には様々なモデルが存在し、それぞれのモデルに対して同種写像計算公式が構成され性能比較が行われてきた。その時によく利用される手法が楕円曲線上の点を射影直線上の座標に圧縮し、その座標で公式を構成する方法である。本研究では、モデルに依らない任意の楕円曲線上にそのような関数（一般化モンゴメリー座標）が存在することを示し、その関数を用いて同種写像計算を含む基礎演算公式を導いた。

（2）特許出願

研究期間全出願件数：0 件

（3）その他の成果（主要な学会発表、受賞、著作物、プレスリリース等）

1. [招待講演]同種写像暗号の数理, 九州大学 IMI 暗号学セミナー, 2021 年 7 月 14 日
2. [招待講演]量子コンピュータ社会における次世代暗号技術, 愛媛大学　データサイエンス研究セミナー, 2021 年 9 月 28 日
3. [招待講演]超特異楕円曲線を用いた耐量子計算機暗号の数理とその進展, 東京大学大学院数理科学研究科　情報数学セミナー　,2022 年 1 月 27 日
4. [招待講演]整数論で守るポスト量子社会のセキュリティ, JST 数学関連3領域連携 WS「情報科学と拓く新しい数理科学」, 2022 年 9 月 12 日
5. [招待講演]Mathematics of Post-Quantum Cryptography, 理研 iTHEMS　数学セミナー, 2022 年 11 月 18 日

ほか招待講演 4 件および査読なし国内会議発表 5 件あり