様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　５ 年　 ６ 月　 １ 日現在

機関番号：３２６８６
研究種目：挑戦的研究（萌芽）
研究期間：2019～2022
課題番号：１９Ｋ２２８４７

研究課題名（和文）同種写像暗号に対する数理的技法による解読法の探求と計算量評価

研究課題名（英文）Exploration for mathematical attacks against isogeny-based cryptography and their complexity analysis

研究代表者
安田　雅哉（Yasuda, Masaya）

立教大学・理学部・教授

研究者番号：３０５３６３１３

交付決定額（研究期間全体）：（直接経費）　　5,000,000円

研究成果の概要（和文）：耐量子計算機暗号候補の1つである同種写像暗号の安全性を支える同種写像計算問題に対して，数理的技法による解読アルゴリズムを開発すると共に，実装結果を元に同種写像暗号への影響を評価した．具体的には，同種写像計算問題を連立代数方程式に帰着し，グレブナー基底計算アルゴリズムを用いて求解する解読法を開発し，同種写像暗号方式SIKEに対する解読時間を実装評価した．また，有限体上の超特異楕円曲線に関する構成的Deuring対応計算の高速化に成功した．さらに，超特異楕円曲線上の同種写像パス探索と同値な自己準同型環計算のアルゴリズムの開発と実装に成功した．

研究成果の学術的意義や社会的意義
本研究では，耐量子計算機暗号候補の1つである同種写像暗号の安全性を支える同種写像計算問題に対して，代数的手法に基づく解読実験によって多角的に安全性解析を行った．今回得られた解読手法と解析結果は，同種写像暗号における暗号方式として安全なパラメータの選択時に活用することができる．特に，本研究による多角的な安全性解析は，同種写像暗号がどの程度安全か評価するための学術的データを与えるため，耐量子計算機暗号としての同種写像暗号の標準化活動への貢献が期待できる．

研究成果の概要（英文）：Isogeny-based cryptography is one of the candidates for quantum-safe cryptography. In this research, we developed several mathematical attacks against isogeny problems that support the security of isogeny-based cryptography. We also analyzed their computational complexity based on implementation results. Specifically, we reduced the general isogeny problem to a system of algebraic equations, and solved the system using Groebner basis calculation algorithms. We also reported the running time for breaking SIKE by our method. Furthermore, we succeeded in speeding up the constructive Deuring correspondence calculation for supersingular elliptic curves over finite fields. We also developed and implemented an algorithm for computing the endomorphism ring of a supersingular elliptic curve, which is equivalent to solving the isogeny path-finding problem.

研究分野：暗号数理

キーワード：同種写像暗号　楕円曲線　同種写像問題　Deuring対応　耐量子計算機暗号　超特異楕円曲線　自己準同型環　四元数環

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

最も代表的な公開鍵暗号である RSA 暗号と楕円曲線暗号は SSL/TLS による暗号通信や電子政府での電子署名で広く普及している．しかし，これらの暗号の安全性はそれぞれ素因数分解や楕円曲線離散対数の数学問題の計算困難性に依存し，量子計算機で容易に解読できることが[Shor@FOCS1994]により示されている．将来の実用化が期待される量子計算機による既存暗号の危殆化に備え，2016 年 2 月に米国標準技術研究所 NIST は量子計算機を用いた解読に耐性のある耐量子計算機暗号の標準化計画を発表した．具体的な計画として，耐量子性を持つ暗号方式・電子署名・鍵交換方式を公募し，2017 年末の公募〆切後 3～5 年かけて提案方式の安全性と性能評価を行い，標準化方式を決定していく．実際，2017 年末に提出された方式は全 81 件で，2018 年 10 月の時点で 63 件の方式が残っている(安全性欠陥の理由で取り下げた方式が多数)．また，2016 年 7 月に米 Google 社が Web ブラウザ Chrome の実験版に耐量子計算機暗号技術を搭載すると発表するなど，米国を中心に耐量子計算機暗号への移行が急速に加速している．

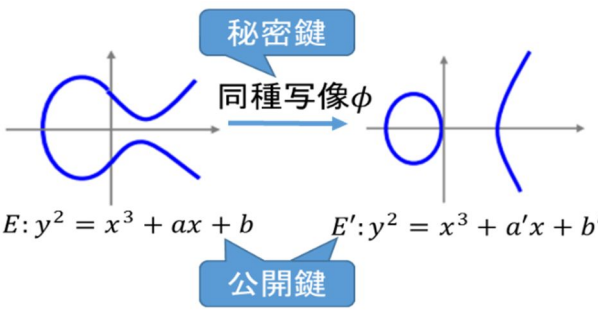
２．研究の目的

耐量子計算機暗号の候補として格子暗号・符号暗号・多変数多項式暗号・同種写像暗号などがある[NISTIR8105]．特に同種写像暗号は[Couveignes@ePrint2006]で初めてそのアイデアが示され，2010 年前後に具体的なハッシュ関数・暗号方式が提案されるなど非常に新しい研究対象である．2017 年末にはカナダ Waterloo 大・米マイクロソフトを含む合同チームが，[Jao-De Feo@PQCrypto2011]の同種写像ベースの鍵交換方式を基にしたアルゴリズム(SIKE: https://sike.org/)を NIST に提出し，耐量子計算機暗号の有力候補の１つとして注目されている．一方，同種写像暗号の安全性は同種写像計算問題と呼ばれる数学問題の計算困難性に依存するが，解読アルゴリズムの開発・解読実験を含めた安全性解析が不十分で，今後の標準化に向けた最重要課題となっている．実際，既存の解読法はグラフ構造を利用した一般の衝突探索法で，同種写像計算問題に特化した方法ではない．そこで，本研究では

(1) 同種写像が持つ代数的性質を利用した新しい解読アルゴリズムの探究と開発を行う．
(2) さらに解読実験による計算量評価を行い，同種写像暗号の安全パラメータ選択の指針を示す．

３．研究の方法

標数 2，3 を除く体上の楕円曲線は方程式 $E: y^2 = x^3 + ax + b$ で表され，その曲線上の点の全体集合は群をなす．同種写像は 2 つの楕円曲線間の群構造を保存する写像で，同種写像で結ばれる 2 つの楕円曲線は同種であるという．楕円曲線 E とその有限部分群 C が与えられたとき，その部分群を核とする同種写像 $\phi: E \to E' = E/C$ は Velu の公式で容易に計算できる．逆に，同種な 2 つの楕円曲線が与えられた時，それらの曲線を結ぶ同種写像を求めることは一般に難しく，これを同種写像計算問題という．右図のように，同種写像暗号では同種な 2 つの楕円曲線を公開鍵，2 つの曲線を結ぶ同種写像を秘密鍵として利用する．そこで，本研究では以下の 2 つの課題に取り組む：



(1) 数理的技法による新しい解読アルゴリズムを探求する．
(2) 上記の解読アルゴリズムを実装し，解読実験を行う．また，実験と理論の両面から計算量評価を行う．

４．研究成果

【同種写像問題に対する代数的解読アルゴリズムの開発と解読実験】

まず，同種写像暗号の安全性を支える数学的な計算問題の 1 つである同種写像パス探索問題に対して，楕円曲線が持つ代数的性質を利用した新しい解読法を開発すると共に，同種写像暗号方式 SIKE に対して実際の計算機による解読実験を行い，解読可能性を検証した．より具体的には，同種写像パス探索問題を同種写像計算に関する Velu の公式から得られる連立代数方程式に帰着し，グレブナー基底計算アルゴリズムにより，その連立代数方程式を求解する解読法を開発した[1]．また，Schoof らによる楕円曲線の位数計算法の一部の処理を同種写像計算問題の解読に適用した新しい代数的攻撃法も開発した．さらに，同種写像パス探索問題に対して現在最良の中間一致攻撃法と今回提案した代数的な攻撃法を組み合わせたハイブリッド型の解読法を数式処理システム Magma 上で実装し，SIKE 方式に対する解読実験を行った．実験結果としては，同種写像の次数が 3^{15} 程度までは今回のハイブリッド攻撃で SIKE 方式を解読できることを示すことができた[2].（特に，下図のように同種写像の次数が 3^{20} なら 1 日以内で SIKE 方式を解読することに成功した.）

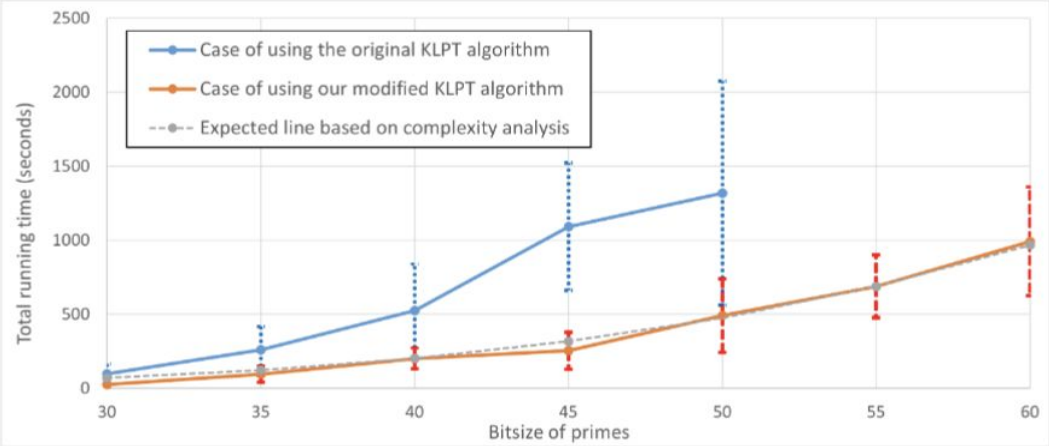
Isogeny degrees 3^e	Pure MITM (Section 3)			Our hybrid MITM (Section 4)	
	Using factorization of $\Phi_3(X, j)$	Using auxiliary torsion points	Algebraic approach	Using factorization of $\Phi_3(X, j)$	Using auxiliary torsion points
3^6	5.64 ($T_{e/2} \approx$ 4.5 KB)	0.75 ($T_{e/2} \approx$ 4.5 KB)	1.04	Same as algebraic approach	
3^8	16.12 (13.5 KB)	0.93 (13.5 KB)	1.61	Same as algebraic approach	
3^{10}	48.98 (40.5 KB)	1.5 (40.5 KB)	7.24	Same as algebraic approach	
3^{12}	150.48 (121.5 KB)	3.13 (121.5 KB)	175.63	44.94 ($T_d \approx$1.5 KB)	29.15 ($T_d \approx$1.5 KB)
3^{14}	466.81 (364.5 KB)	7.92 (364.5 KB)	5404.92	256.72 (4.5 KB)	129.56 (4.5 KB)
3^{16}	1593.41 (1.1 MB)	22.58 (1.1 MB)	> 1 day	2372.04 (13.5 KB)	880.12 (13.5 KB)
3^{18}	7719.86 (3.3 MB)	69.14 (3.3 MB)		16921.01 (40.5 KB)	5256.39 (40.5 KB)
3^{20}	60743.42 (10 MB)	230.07 (10 MB)		> 1 day	38082.70 (121.5 KB)
3^{22}	> 1 day	883.52 (30 MB)			>1 day
3^{24}		5375.75 (89 MB)			
3^{26}		46248.28 (266 MB)			

【構成的 Deuring 対応計算の高速化】

上述したように，同種写像暗号の安全性は，2 つの同種な楕円曲線を結ぶ同種写像の列を具体的に計算する同種写像計算問題の計算量困難性に依存する．一方，楕円曲線論において，有限体上の超特異楕円曲線の全体集合と四元数環における極大整環（maximal orders）全体集合が 1 対 1 に対応する Deuring 対応が知られている．近年，Deuring 対応計算による超特異楕円曲線の同種写像列を利用した電子署名方式 SQISign が提案されるなど，同種写像暗号における重要な計算技術の 1 つとして非常に注目されている．本研究では，超特異楕円曲線の Deuring 対応下における四元数環上の同種写像問題を効率的に解く Kohel-Lauter-Petit-Tignol(KLPT)アルゴリズムの高速実装に成功した．また，実装開発した KLPT アルゴリズムに加えて，超特異楕円曲線のねじれ点の高速探索法を提案し[3，4，5]，与えられたイデアルに Deuring 対応する超特異楕円曲線を求める構成的 Deuring 対応問題を実用的な処理時間で求解可能であることを示した[5].

（下図に示すように，KLPT アルゴリズムを改良することにより，構成的 Deuring 対応計算の高速化に成功した.）

Bitsizes of p	Original KLPT alg. Average	Original KLPT alg. Std. Dev.	Modified KLPT alg. Average	Modified KLPT alg. Std. Dev.	$T = \beta D^4 \log p$ ($\beta = 0.0015$)
30	98.201	66.304	26.087	18.494	68.766 ($D \approx 55$)
35	259.885	155.900	94.246	53.305	121.908 ($D \approx 61$)
40	523.616	314.720	200.884	71.164	201.710 ($D \approx 67$)
45	1091.260	430.645	252.944	124.920	316.207 ($D \approx 73$)
50	1318.407	757.091	490.048	248.837	474.628 ($D \approx 78$)
55	N/A	N/A	687.450	212.870	687.440 ($D \approx 84$)
60	N/A	N/A	991.315	366.778	966.384 ($D \approx 89$)



【有限体上の超特異楕円曲線の自己準同型環の計算】

同種写像暗号の安全性を支える超特異楕円曲線上の同種写像パス探問題は，自己準同型環計算に帰着できることが知られている. 本研究では，素数 p の要素数を持つ有限体上の超特異楕円曲線の自己準同型環計算のために，超特異楕円曲線における同種写像グラフのサイクル探索と，サイクル探索が定める自己準同型写像の四元数環の元表現に関するアルゴリズムを整備した．また，数式処理システム SageMath 上での実装により，超特異楕円曲線の自己準同型環の計算に成功した.（下図に示すように，30 ビット程度の標数に対し，1.5 時間以内で自己準同型環を求めることに成功した.）

Bit-size of p	Upper bound D	Average running time (seconds) Finding cycles	Transformation	Total time	Average of #isogeny cycles
10	60	3.69	1.26	4.95	5.1
15	80	15.10	2.07	17.17	3.9
20	120	122.16	21.02	143.18	7.0
25	160	262.85	96.45	359.29	11.1
30	200	3842.54	124.61	3967.15	18.7

主な発表論文

[1] Yasushi Takahashi, Momonari Kudo, Ryoya Fukasaku, Yasuhiko Ikematsu, Masaya Yasuda, Kazuhiro Yokoyama, Algebraic approaches for solving isogeny problems of prime power degrees, Journal of Mathematical Cryptology, vol. 15, pp. 31–44, 2020.

[2] Ikematsu Yasuhiko, Fukasaku Ryoya, Kudo Momonari, Yasuda Masaya, Takashima Katsuyuki, Yokoyama Kazuhiro, “Hybrid meet-in-the-middle attacks for the isogeny path-finding problem”, APKC 2020, pp. 36–44, 2020.

[3] Masayuki Noro, Masaya Yasuda, Kazuhiro Yokoyama, Symbolic computation of isogenies of elliptic curves by Velu’s formula, Commentarii mathematici Universitatis Sancti Pauli, vol. 68, pp. 93–130, 2020.

[4] 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, vol. 1, pp. 10–24, 2021.

[5] Yuta Kambe, Yasushi Takahashi, Masaya Yasuda, Kazuhiro Yokoyama, “On the feasibility of computing constructive Deuring correspondence”, presented at NuTMiC 2021. (To appear in a special edition of the Banach Center Publications as post-proceedings of NuTMiC 2021.)

５．主な発表論文等

〔雑誌論文〕　計8件（うち査読付論文　7件／うち国際共著　0件／うちオープンアクセス　4件）

１．著者名 Kambe Yuta, Yasuda Masaya, Noro Masayuki, Yokoyama Kazuhiro, Aikawa Yusuke, Takashima Katsuyuki, Kudo Momonari	４．巻 1
２．論文標題 Solving the Constructive Deuring Correspondence via the Kohel-Lauter-Petit-Tignol Algorithm	５．発行年 2022年
３．雑誌名 Mathematical Cryptology	６．最初と最後の頁 10～24
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Kambe Yuta, Aikawa Yusuke, Kudo Momonari, Yasuda Masaya, Takashima Katsuyuki, Yokoyama Kazuhiro	４．巻 1412
２．論文標題 Implementation Report of the Kohel-Lauter-Petit-Tignol Algorithm for the Constructive Deuring Correspondence	５．発行年 2022年
３．雑誌名 Advances in Intelligent Systems and Computing, Springer	６．最初と最後の頁 953～966
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-981-16-6890-6_72	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Masayuki NORO, Masaya YASUDA, and Kazuhiro YOKOYAMA	４．巻 68
２．論文標題 Symbolic Computation of Isogenies of Elliptic Curves by Velu ' s Formula	５．発行年 2020年
３．雑誌名 COMMENTARII MATHEMATICI UNIVERSITATIS SANCTI PAULI	６．最初と最後の頁 93～130
掲載論文のDOI（デジタルオブジェクト識別子） 10.14992/00020348	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Ikematsu Yasuhiko、Fukasaku Ryoya、Kudo Momonari、Yasuda Masaya、Takashima Katsuyuki、Yokoyama Kazuhiro	４．巻 --
２．論文標題 Hybrid Meet-in-the-Middle Attacks for the Isogeny Path-Finding Problem	５．発行年 2020年
３．雑誌名 APKC20: Proceedings of the 7-th ACM Workshop on ASIA Public-Key Cryptography	６．最初と最後の頁 36～44
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3384940.3388956	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Yokoyama Kazuhiro、Yasuda Masaya、Takahashi Yasushi、Kogure Jun	4．巻 14
2．論文標題 Complexity bounds on Semaev’s naive index calculus method for ECDLP	5．発行年 2020年
3．雑誌名 Journal of Mathematical Cryptology	6．最初と最後の頁 460～485
掲載論文のDOI（デジタルオブジェクト識別子） 10.1515/jmc-2019-0029	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Takahashi Yasushi、Kudo Momonari、Fukasaku Ryoya、Ikematsu Yasuhiko、Yasuda Masaya、Yokoyama Kazuhiro	4．巻 15
2．論文標題 Algebraic approaches for solving isogeny problems of prime power degrees	5．発行年 2020年
3．雑誌名 Journal of Mathematical Cryptology	6．最初と最後の頁 31～44
掲載論文のDOI（デジタルオブジェクト識別子） 10.1515/jmc-2020-0072	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 安田雅哉	4．巻 CRYPTREC EX-3001-2020
2．論文標題 ディジタル署名EdDSAで使われている曲線の安全性に関する調査及び評価	5．発行年 2020年
3．雑誌名 CRYPTREC外部評価報告書	6．最初と最後の頁 1～47
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Yuta Kambe, Yasushi Takahashi, Masaya Yasuda, Kazuhiro Yokoyama	4．巻 --
2．論文標題 On the feasibility of computing constructive Deuring correspondence	5．発行年 2022年
3．雑誌名 NuTMiC 2021 (To appear in a special edition of the Banach Center Publications as post-proceedings of NuTMiC 2021)	6．最初と最後の頁 --
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計10件（うち招待講演　1件／うち国際学会　4件）

1．発表者名
高橋康，神戸祐太，安田雅哉，横山和弘

2．発表標題
適切な素数選択によるKLPTアルゴリズムを利用した同種写像構成計算

3．学会等名
2022年暗号と情報セキュリティシンポジウム（SCIS2022）

4．発表年
2022年

1．発表者名
神戸祐太，高橋康，相川勇輔，工藤桃成，安田雅哉，高島克幸，横山和弘

2．発表標題
SIKEに対するvOW法の内部関数の新計算手法

3．学会等名
2022年暗号と情報セキュリティシンポジウム（SCIS2022）

4．発表年
2022年

1．発表者名
Takahashi Yasushi, Kambe Yuta, Yasuda Masaya, Yokoyama Kazuhiro

2．発表標題
Selection of primes in the KLPT algorithm for construction of fast isogeny (poster)

3．学会等名
IWSEC2021（国際学会）

4．発表年
2021年

1．発表者名
Kambe Yuta, Yasuda Masaya, Noro Masayuki, Yokoyama Kazuhiro, Aikawa Yusuke, Takashima Katsuyuki, Kudo Momonari

2．発表標題
Solving the Constructive Deuring Correspondence via the Kohel-Lauter-Petit-Tignol Algorithm

3．学会等名
MathCrypt2021（国際学会）

4．発表年
2021年

１．発表者名
Masaya YASUDA, Kazuhiro YOKOYAMA

２．発表標題
Introduction to algebraic approaches for solving isogeny path-finding problems

３．学会等名
RIMS Conference on Theory and Applications of Supersingular Curves and Supersingular Abelian Varieties（招待講演）（国際学会）

４．発表年
2020年

１．発表者名
神戸祐太 ， 安田雅哉 ， 横山和弘

２．発表標題
Kohel-Lauter-Petit-Tignolアルゴリズムのsageにおける実装報告

３．学会等名
日本応用数理学会2020年度年会

４．発表年
2020年

１．発表者名
神戸祐太、相川勇輔、工藤桃成、安田雅哉、高島克幸、横山和弘

２．発表標題
Kohel-Lauter-Petit-Tignolアルゴリズムの構成的Deuring対応への適用

３．学会等名
2021年暗号と情報セキュリティシンポジウム（SCIS2021）

４．発表年
2021年

１．発表者名
高橋康、工藤桃成、池松泰彦、安田雅哉、横山和弘

２．発表標題
Algebraic approaches for solving isogeny problems of prime power degrees

３．学会等名
MathCrypt 2019（国際学会）

４．発表年
2019年

１．発表者名 池松泰彦、深作亮也、工藤桃成、安田雅哉、高島克幸、横山和弘
２．発表標題 同種写像パス探索問題に対する中間一致攻撃のハイブリッド手法
３．学会等名 2020年暗号と情報セキュリティシンポジウム（SCIS2020）
４．発表年 2020年

１．発表者名 高橋康、工藤桃成、池松泰彦、安田雅哉、横山和弘
２．発表標題 同種写像問題に対する代数的求解法の解析と計算量評価
３．学会等名 日本応用数理学会2019年度年会：「数論アルゴリズムとその応用」（JANT）セッション
４．発表年 2019年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	高島　克幸 (Takashima Katsuyuki) (70723964)	早稲田大学・教育・総合科学学術院・教授 (32689)	

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関