2024年度共同利用研究報告書

2024年11月29日

所属・職名 東京電機大学 理工学部 理工学科 情報システムデザイン学系・助教
橋本 侑知

		整理番号	2024a026	
1.研究計画題目	同種写像暗号の安全性に関する帰着効率の検討			
2.新規・継続	新規			
3.種別	若手・学生研究			
4.種目	短期研究員			
5.開催方法	対面開催			
6.研究代表者	氏名	橋本 侑知		
	所属 部局名	東京電機大学 理工学部 理工学科 情報システムデザイン学系	職名	助教
7.研究実施期間	2024年08月22日(木曜日)～2024年08月30日(金曜日)			
8.キーワード	暗号理論, 圏論, 同種写像暗号			
9.参加者人数	2人			

10.本研究で得られた成果の概要

同種写像暗号は、ある2つの楕円曲線が与えられたとき、その間の同種写像を見つけることが困難である事を安全性の根拠としている暗号である。楕円曲線は通常曲線と超特異曲線に分類され、同種写像暗号では主に超特異曲線が用いられる。そのため、同種写像暗号のパラメータ設定の際や楕円曲線のデータを送付し合う際に、楕円曲線が超特異曲線であるかどうかの判定(超特異性判定)が効率的に出来ることが望ましい。

本研究の当初の研究計画では、同種写像暗号の安全性に関する帰着効率を改善するアプローチで同種写像の効率化を進める予定であったが、決定的超特異性判定アルゴリズムの効率化の観点から同種写像暗号の効率化に関する成果を出した。効率的な決定的超特異性判定アルゴリズムは、Sutherlandにより提案された2-同種写像グラフを用いたアルゴリズムである。2-同種写像グラフを用いた超特異性判定アルゴリズムの計算効率は、2次拡大体上の通常曲線の同型類を頂点とする2-同種写像グラフ(2-volcanoグラフ)の高さのboundや2-同種写像計算のコストに依存している。本研究では、素体と2次拡大体上のvolcanoグラフの高さのboundの改善し、その結果を利用することにより、超特異性判定アルゴリズムの計算コストを約半分に削減した。またこのアルゴリズムに関して計算機実験を行い、実測値の観点からも計算コストが約半分に削減されていることを確かめた。詳しくは、reprint (arXiv:2409.00505) [1] を参照。

[1] Y. Hashimoto and K. Nuida. Bounds on heights of 2-isogeny graphs in ordinary curves over F_p and F_{p^2} and its application. arXiv:2409.00505 preprint, 2024.

IMI共同利用報告書
同種写像暗号の安全性に関する帰着効率の検討

橋本 侑知

1 概要

現在広く利用されている RSA 暗号や楕円曲線暗号は大型の量子コンピュータにより危殆化してしまう。このことから、量子コンピュータにも耐性のある暗号 (耐量子計算機暗号) の設計やその効率化が重要な研究分野となっている。その耐量子計算機暗号の有力候補の 1 つとして、同種写像暗号が提案されている。同種写像暗号は、ある 2 つの楕円曲線が与えられたとき、その間の同種写像を見つけることが困難である事を安全性の根拠としている暗号である。楕円曲線は通常曲線と超特異曲線に分類され、同種写像暗号では主に超特異曲線が用いられる。そのため、同種写像暗号のパラメータ設定の際や楕円曲線のデータを送付し合う際に、楕円曲線が超特異曲線であるかどうかの判定 (超特異性判定) が効率的に出来ることが望ましい。

本研究の当初の研究計画では、同種写像暗号の安全性に関する帰着効率を改善するアプローチで同種写像の効率化を進める予定であったが、超特異性判定アルゴリズムの効率化の観点から同種写像暗号の効率化に関する成果を出した。

超特異性判定アルゴリズムには確率的な判定法と決定的な判定法があり、確率的な判定法は決定的な判定法と比べて計算効率は良いが、誤判定をする可能性がある。一方で、決定的な判定法は確実に与えられた曲線が超特異曲線であるかどうかを判定出来る。効率的な決定的超特異性判定アルゴリズムは、Sutherland により提案された 2-同種写像グラフを用いたアルゴリズム [3] である。2-同種写像グラフは、頂点を楕円曲線の同型類として辺をその間の 2-同種写像とするようなグラフである。このアルゴリズムの計算量は $\tilde{O}(n^3)$ であり、支配的な計算コストは 2 次拡大体上の平方根計算である。現在では、この支配的な計算コストを約半分に削減したアルゴリズム [1] も提案されている。

2 本研究の成果

2-同種写像グラフを用いた超特異性判定アルゴリズムの計算効率は、2 次拡大体上の通常曲線の同型類を頂点とする 2-同種写像グラフ (2-volcano グラフ) の高さの bound や 2-同種写像計算のコストに依存している。本研究では、素体と 2 次拡大体上の volcano グラフの高さの bound の改善し、その結果どの程度超特異性判定アルゴリズムの計算速度が向上したかを計算機実験を通して明らかにした。詳しくは、preprint (arXiv:2409.00505) [2] を参照。また、本成果をまとめたこの論文は現在、査読付き論文誌に投稿中である。

2.1 bound の改善

p を素数とし、$\mathbb{F}_{p^2}$ を 2 次拡大体とする。また、2-volcano グラフの高さを h とする。既存の $\mathbb{F}_{p^2}$ 上の 2-volcano グラフの高さの bound である $h \leq \lfloor \log_2 p \rfloor + 1$ に対して、我々はその約半分の bound である $h \leq \left\lfloor \frac{1}{2} \lfloor \log_2 p \rfloor \right\rfloor + 2$ に改善した。また、既存の $\mathbb{F}_p$ 上の 2-volcano グラフの高さの bound である $h \leq \log_2 \sqrt{4p}$ に対して、以下のような bound に改善出来ることを示した。

1. $p \equiv 3 \pmod 4$ のとき、$h \leq 1$。
2. $p \equiv 5 \pmod 8$ のとき、$h \leq 2$。

また、$p \equiv 1 \pmod 8$ のときは、個々の素数 p に対して、高さ h の bound を計算するアルゴリズムを提案した。そのアルゴリズムを用いた計算結果は以下の通りである。

表 1: 素数 $p \equiv 1 \pmod 8$ を満たす 100 個の素数 p に対し、$\mathbb{F}_p$ 上定義された 2-volcano グラフの高さ h に対する upper bound h_1 の平均を表に記している。ただし、b は p のビット長を表し、h_2 は自明な upper bound $h_2 = \left\lfloor \frac{\lfloor \log_2 p \rfloor}{2} \right\rfloor + 2 = \left\lfloor \frac{b-1}{2} \right\rfloor + 2$ を表すものとする。

b	Average of Bounds h_1	Bound h_2
64	18.12	33
128	34.20	65
192	50.21	97
256	66.17	129
320	82.22	161
384	97.98	193
448	114.25	225
512	130.18	257
576	146.23	289
640	162.16	321
704	178.24	353
768	194.10	385
832	210.17	417
896	225.98	449
960	242.13	481
1024	258.05	513

2.2 超特異性判定アルゴリズム

超特異性判定アルゴリズムの計算効率は、$\mathbb{F}_{p^2}$ 上の 2-volcano グラフの高さの bound に依存している。より具体的には、既存の bound である $h \leq \lfloor \log_2 p \rfloor + 1$ に対して、同種写像グラフを用いた超特異性判定アルゴリズムでは、1 ステップで 3 方向の同種写像を計算するような繰り返し計算が $\lfloor \log_2 p \rfloor + 2$ 回必要となる。本研究ではこの bound を約半分の

$h \leq \left\lfloor \frac{1}{2} \lfloor \log_2 p \rfloor \right\rfloor + 2$ に改善したことにより、超特異性判定アルゴリズムにおける繰り返し計算回数も約半分の $\left\lfloor \frac{1}{2} \lfloor \log_2 p \rfloor \right\rfloor + 3$ 回で判定出来ることが分かった。また、実際の実行時間を Magma を用いて実験した。その結果は以下の通りであり、超特異性判定アルゴリズムの実行時間も約半分になっていることが分かった。

表 2: [1] における既存の upper bound である h_0 と、我々の改善した upper bound である h_2 に基づく平均実行時間を表す。ここで、$h_0 = \lfloor \log_2 p \rfloor + 1, \quad h_2 = \left\lfloor \frac{1}{2} \lfloor \log_2 p \rfloor \right\rfloor + 2$ とし、b は素数 $p = 4r + 1, p = 4r + 3\, r \in \mathbb{Z}$ のビット長を表し、実行時間はミリ秒単位の CPU 時間を表している。

b	h_0 $(p = 4r + 1)$	h_2 $(p = 4r + 1)$	h_0 $(p = 4r + 3)$	h_2 $(p = 4r + 3)$
64	18	10	12	8
128	66	37	51	27
192	158	84	126	67
256	315	165	249	132
320	537	278	430	225
384	880	453	694	359
448	1361	698	1072	554
512	2016	1032	1576	807
576	2897	1475	2230	1142
640	3822	1947	3006	1538
704	5157	2627	4012	2044
768	6716	3414	5275	2682
832	8738	4427	6734	3428
896	11229	5694	8594	4365
960	13879	7016	10720	5438
1024	17144	8679	13121	6639

参考文献

[1] Y. Hashimoto and K. Nuida. Improved supersingularity testing of elliptic curves using Legendre form. In F. Boulier, M. England, T. M. Sadykov, and E. V. Vorozhtsov, editors, *Computer Algebra in Scientific Computing - 23rd International Workshop, CASC 2021, Sochi, Russia, September 13-17, 2021, Proceedings*, volume 12865 of *Lecture Notes in Computer Science*, pages 121–135. Springer, 2021.

[2] Y. Hashimoto and K. Nuida. Bounds on heights of 2-isogeny graphs in ordinary curves over $\mathbb{F}_p$ and $\mathbb{F}_{p^2}$ and its application. *arXiv:2409.00505 preprint*, 2024.

[3] A. V. Sutherland. Identifying supersingular elliptic curves. *LMS Journal of Computation and Mathematics*, 15:317–325, 2012.

同種写像暗号の安全性に関する帰着効率の検討

整理番号	2024a026
種別	若手・学生研究-短期研究員
研究計画題目	同種写像暗号の安全性に関する帰着効率の検討
研究代表者	橋本 侑知（東京電機大学 理工学部 理工学科 情報システムデザイン学系・助教）
研究実施期間	2024年8月22日（木）～ 2024年8月30日（金）
研究分野のキーワード	暗号理論, 圏論, 同種写像暗号
目的と期待される成果	現代の情報化社会では、通信等の安全性を担保する暗号は必要不可欠になっている。現在提案されてい半は、ある数学的な計算量的困難性を持つ問題を安全性の根拠としている。すなわち、暗号方式の安全暗号方式の安全性を破るという問題を計算量的困難性を持つ問題に帰着させている。このとき、より効えることで暗号方式の安全性をより高い強度で保証でき、そのことは暗号方式の効率性向上にもつなが分野では数々の安全性証明技法が考案されてきたが、耐量子計算機暗号の一種である同種写像暗号の学的構造に基づく暗号技術にそうした既存の技法を適用するのは難しい状況である。そこで本研究では可能な安全性証明技法の確立を目指す。具体的には、圏論の応用として近年注目されているResource号方式の安全性証明に登場する「オラクル」や「攻撃者」などの概念の定式化を再考することで、圏論を用全性証明技法を探究する。また、同手法の適用例として具体的な同種写像暗号方式の安全性証明の改良の改良による個々の同種写像暗号方式の効率化を目指す。
組織委員(研究集会) **参加者(短期共同利用)**	橋本 侑知（東京電機大学・助教） 縫田 光司（九州大学・教授）