様式 C-19

科学研究費補助金研究成果報告書

平成 23 年 4 月 30 日現在

機関番号：32641
研究種目：基盤研究(C)
研究期間： 2008 ～ 2010
課題番号：20560370
研究課題名（和文）楕円曲線暗号と超楕円曲線暗号のベィユデセント攻撃に対する安全性に関する研究
研究課題名（英文）Study on Security Analysis of Elliptic and Hyperelliptic Cryptosystems against Weil Descent Attack
研究代表者
趙 晋輝 （ CHAO JINHUI ）
中央大学 理工学部 教授
研究者番号：60227345

研究成果の概要（和文）：

本研究は、公開鍵暗号の中で最も安全とされている楕円と超楕円暗号系の、最近提案された Weil descent GHS 攻撃に対する安全性を解明することが目的である。楕円曲線と超楕円曲線の GHS 攻撃に破れる可能性のある曲線をすべて割り出す弱い曲線の分類を行い、Weil descent GHS 攻撃に破れる楕円・超楕円曲線の完全分類と曲線の同型類の数を厳密に評価した。特に３次拡大体上の楕円曲線は半数以上が攻撃されることを明らかにした。

研究成果の概要（英文）：

This research is to analyze security of elliptic and hyperelliptic cryptosystems, which are supposed to be the safest cryptosystems, against the recently developed Weil descent GHS attack. In particular, we will show a complete classification of all elliptic and hyperelliptic curved used in the cryptosystems which are weak against the Weil descent GHS attack, find the number and classes of these weak curves and algorithms to test if a random curve is safe or not. These results then provide a full understanding on risk and damage of the cryptosystems again the GHS attack.

交付決定額

（金額単位：円）

	直接経費	間接経費	合 計
２００８年度	1,300,000	390,000	1,690,000
２００９年度	1,100,000	330,000	1,430,000
２０１０年度	1,100,000	330,000	1,430,000
総 計	3,500,000	1,050,000	4,550,000

研究分野：暗号理論
科研費の分科・細目：
キーワード：暗号理論、楕円暗号、超楕円暗号、安全性解析、Weil decent 攻撃

１．研究開始当初の背景

IT 技術によって支えられる安全･安心な高度化情報社会の実現に当たっては、個人認証や電子署名などの情報セキュリティ技術は最も重要なインフラであり、これらの認証署名技術の基礎を成している公開鍵暗号の高度な安全性を確保することは、情報セキュリティ技術の最中心課題であることは言うまでもない。

現在の暗号やプロトコールが基づいている暗号学一方向性関数は、基本的には、3 種類しか知られていない。その中では、RSA や ElGamal 暗号は安全性の根拠としている、素因数分解問題や有限体上の離散対数問題は、準指数時間で解読できる困難さを持つことが知られている。素因数分解と離散対数の解読記録は年々更新して、今年年始には、すでに 1000 ビットの素因数分解記録が報告されている。これは最近話題になった「2010RSA 問題」である。準指数関数と指数関数の差も指数的に広がることから、今後さらに頻繁にしかも大幅に鍵長を増加することが避けられない。

一方では、楕円暗号は、楕円曲線上の離散対数問題に基づいており、この離散対数問題は、完全指数時間であるため、以上のような心配がない。具体的に、RSA や ElGamal 暗号の鍵長が 1024 ビットである今日では、楕円暗号は、160 ビットという数倍も小さいサイズで、同じ安全性を保っている。さらに、今後 RSA や ElGamal 暗号の鍵長が倍増しても、楕円暗号はほぼ微増程度で済むことも知られている。従って、RSA や ElGamal 暗号に比べて、より難しい問題に基づく楕円暗号は、本質的に優れているのである。

さらに、近年の電子技術の進歩により携帯電話や IC カード等小型情報機器が急速に普及し、これら小型機器を利用した個人認証等が安全･安心な高度情報化社会のキー技術となると広く考えられている。RSA 暗号や、ElGamal 暗号など準指数時間の困難さに基づく公開鍵暗号に比べて、楕円曲線に基づく公開鍵暗号は鍵長が大幅に短縮できるため、コンパクト化に適している。また、楕円曲線の一般化である超楕円暗号では、計算機の語長をさらに短縮することが可能である。

一方、楕円暗号と超楕円暗号の安全性検証という肝要な問題については、暗号研究者の中では、当然重大な関心を寄せてきており、今までは、多大な努力が払われ続けてきた。実際に、世界で最も強力に楕円暗号の商品化を進めてきたマスターカードが創立した CERTICOM などは、7 千万円という破格の懸賞金を設けて、楕円暗号に対する攻撃を公募してきた。今までは、いくつかの攻撃法が開発されたが、結局、ごく特殊な曲線に対してのみ脅威をなす攻撃しか見出せなかった。具体的には、超特異曲線に対する MOV 攻撃は、楕円曲線上の離散対数問題を、有限体上の離散対数問題に変換して攻撃しているが、その変換が可能である楕円曲線の割合は非常に小さい。また、実際に楕円曲線のこの変換可能性は、筆者らが提案した B-smooth テストにより、簡単に判別する、従って避けることができるため、楕円暗号の安全性には現実的な脅威をなしているわけではない。トレース零の曲線と呼ばれる曲線に対する攻撃もほぼ同様である。また、その後発見された Anomalous 曲線の対する SSAV 攻撃は、大変強力な攻撃ではあるが、攻撃をうける曲線の数はさらに小さく、しかもそのような曲線の判別も極めて簡単に行える。実際に、今まで楕円暗号に対するほとんどの攻撃は、以上のように攻撃範囲、被害程度と対策が解明されており、楕円暗号の安全性は、不動なものであると思われるようになった。

一方、以上のようによく理解されておらず、安全性解析がほとんど進んでいない攻撃は、ただ一つだけ残されていた。この攻撃は、楕

円曲線の複雑な内部構造を利用した大変巧妙な方法で、谷山―志村予想の証明への貢献で知られているG.Frey教授により1998年に理論的に示唆され、2000 年 Gaudry, Hess, Smart によって提案されたものである。特にある有限体 Fq の拡大の上で定義されている曲線に対するもので、Fq の拡大体上の曲線上の離散対数を Fq 上の曲線上の離散対数問題へ変換する方法であるため、Weil descent GHS 攻撃と呼ばれている。この攻撃は、数学的に大変難解であるため、提案されて 10 年近く経ち、その実現や拡張そして解析が試みられてきたが、残念ながら攻撃される曲線の種類と数、さらに被害程度はほとんど分かっておらず、一般的には、仮にこのような曲線があっても非常にまれなケースであろうと信じられた。従って、この攻撃も楕円曲線暗号には脅威を与えないと思われてきた。

しかしながら、二年前に、提案されてから20年となる楕円暗号の安全性神話には、重大な試練が訪れることとなった。そのきっかけは、Frey の弟子である若手 Diem は、非超楕円曲線に対する非常に高速な攻撃法を発表したことである。

本研究グループでは楕円・超楕円暗号の開発と暗号化復号化アルゴリズムの高速化を精力的に進めてきた。一方では、国内外では超楕円暗号よりさらに一般的な例えば Cab 曲線のような、非超楕円曲線を用いる暗号を推進するグループも少なくない。その理由は、超楕円曲線よりも、非超楕円曲線のほうがより一般的であるため、より高い安全性を持つものは期待できるからである。しかし、Diem の結果はそのような期待を完全に打ち砕けた。さらに、この結果は、Weil descent GHS 攻撃にも大きなインパクトを与えた。具体的には、有限体 Fq の拡大体上に定義される楕円或いは超楕円曲線は、Fq 上の非超楕円曲線に変換されれば、楕円また超楕円暗号に対する強力な攻撃となるはず。

以上のような Diem の攻撃と Weil descent 攻撃と組み合わせる可能性は、理論的に存在するものの、実際にそれを解析或は実現することは大変困難で、実際に本研究グループのよき理解者協力者である Frey 先生によると、この攻撃を受ける弱い曲線の分類は”an extremely difficult problem” である。

２．研究の目的

本研究は、この困難ではあるが、極めて重要である、楕円と超楕円暗号系の Weil descent 攻撃に対する安全性を完全に解明することを目的とするものである。具体的には、Weil descent 攻撃に弱い楕円曲線と超楕円曲線のすべてのパターンを発見、分類する、そしてこのような曲線の数と形を解明し、その判別法を示す、さらにこれらの曲線の定義方程式を見つけ、攻撃を実装することによって、攻撃されるときの被害度を解明することを目指すものである。

３．研究の方法

G. Frey は 1998 年楕円暗号に導入した Weil descent のアイデアは、楕円曲線 E の定義体がある有限体 Fq の d 次拡大であるとき、E 上の離散対数を、ある Fq 上に定義される、E の被覆と呼ばれる曲線 C 上の離散対数へ変換するというものであった。このアイデアは、具体的に、Gaudry, Hess, Smart によって発展され、その結果として、2000 年楕円暗号への GHS 攻撃が提案された。GHS 攻撃に対して数多くの研究がなされてきたが、その攻撃の手口から、攻撃可能な曲線を探すことに集中してきたためが、ほとんど成功していない。

その理由は、攻撃される場合の可能性が多岐にわたり、それらの可能性をすべて解析することは極めて困難なため、結局最も解析し

やすい場合に限定してしまい、結果としては、今まで解析してきた曲線のクラスの中では、GHS 攻撃によってその安全性が脅かされるような例はほとんど見つからなかった。

そのために、仮に GHS 攻撃によって破れる楕円曲線があったとしても、非常に特殊なもので、その数も少ないに違いないと信じるようになったと思われる。

一方では、本研究のアプローチが従来のアットホック的な手法と根本的に異なる点は、攻撃されそうな拡大体上の楕円曲線或いは超楕円曲線 C0 を探していくのではなく、初めから攻撃される被覆曲線 C が存在すると仮定して、C と C0 が満たすべき条件を逆に割り出すことである。この方針を用いているため、GHS 攻撃に弱い曲線のすべてのパターンを発見、分類することが可能である。

現在、楕円暗号に対しては、特殊な曲線を除いては、直接攻撃する方法は知られていない。楕円曲線の一般化である超楕円曲線の中では、種数 3 以上の超楕円曲線に対しては、現在最も強力な攻撃法は、Gaudry-Theriault-Thome-Diem アルゴリズムの Double-large-prime variation である。さらに、種数 3 以上の非超楕円曲線に対しては、Diem アルゴリズムの Double-large-prime variation は、最強力な攻撃法である。本研究では、前述のように、被覆曲線 C の存在のみならず、その曲線が超楕円曲線であるか、または非超楕円曲線であるかも含めて判断し、さらに具体的に、C が存在する拡大体上で定義される E を分類し、その定義方程式を示し、密度つまり同型類の数を厳密に評価した。そして、C の定義方程式の構成した上で、C0 上の離散対数を C 上へ変換して、上記 2 アルゴリズムによって攻撃することを実装して評価した。

研究体制について、本研究は、研究代表者と連携研究者という情報工学者と数学者の間の協力は重要不可欠である。また、本研究を推進するにあたっては、情報セキュリティ・暗号理論分野の権威である辻井先生によるより高い立場からの教示と、超楕円暗号の実装計算の専門家である松尾氏による高速算法に関する助言、そして、整数論の保型形式の専門家である志村氏による被覆曲線 C の構成法に関する助言を頂いた。

４．研究成果

定義体が奇標数の有限体の場合について、GHS 攻撃の適用条件と攻撃可能な曲線のクラスを完全に分類し、また密度解析を行うことにより、楕円・超楕円暗号の安全性を明らかにした。具体的に、まず以上の楕円曲線或いは超楕円曲線の被覆曲線のヤコビ多様体の様態は大変複雑であるが、まず GHS 攻撃にとっては、最も有利な攻撃状況、つまり C のヤコビ多様体が、C0 の Weil restriction に同種である場合を想定し、解析を行った。

まず、拡大体上に定義されている楕円曲線或いは種数 2、3 の超楕円曲線 C0 の Galois 閉包を考え、それによって定義される被覆曲線は、射影曲線 P^1 の(2,2,…,2)被覆となるため、そのような型の被覆の完全分類を行った。そのためには、拡大体上定義される曲線 C0 の被覆 C の被覆群に対する Galois 群の作用に注目し、Galois 表現を分類する手法を用いた。GHS の攻撃に弱い曲線のクラスの方程式を示し、その同型類の密度を明らかにした。このような被覆の密度に関して、特に、3 次拡大体上のルジャンドル正準形で表すランダムな楕円曲線の中では、2 分の 1 以上であることは、厳密に証明した。従って、GHS 攻撃はこのような楕円暗号系には大変危険であることを明らかにした。また、楕円暗号や超楕円暗号の設計を行う際、どの曲線は弱いかという判別を高速に行う弱い曲線判定法

を示した。

さらに、理論解析のみならず、以上のように発見できた弱い曲線 C0 に対して、具体的にその被覆曲線 C を構成して、さらに C0 上の離散対数問題を C 上へ変換して、攻撃を実装することも重要な課題である。そのためには、まず、正則埋め込みと Galois 作用を利用して射影空間における C のモデルを構築する手法を用いて、C の定義方程式を求めた。構成された曲線上に変換された離散対数に対して、Gaudry- Theriault-Thome-Diem の超楕円曲線に対する Double-large-prime variation 攻撃、または、Diem の非超楕円曲線に対する Double-large-prime variation 攻撃を適用し、現時点で暗号系に使われている楕円暗号・超楕円暗号に対する攻撃効果を評価した。

21 年度以降は、目標としていたのは、標数 2 の有限体上定義される楕円暗号と超楕円暗号の安全性解析である。

本研究は、ordinary の場合ついては、被覆における分岐群の分類を用いて、さらに、non-ordinary の場合については、分岐理論を用いて、標数 2 の有限体の拡大体上に定義される弱い楕円曲線・超楕円とその被覆の完全分類を行った。標数 2 の場合においては、GHS 攻撃を受ける曲線はさらに大量に存在することを、例えば 3 次拡大体上に定義される楕円曲線と超楕円曲線について、証明した。さらに、これらの曲線の被覆曲線を構築し、その攻撃される場合の等価的な鍵長の解析を行うと同時に、GHS 攻撃を実装することで、その安全性の厳密評価を行った。

特に、3 次拡大体上に定義される楕円暗号或いは超楕円暗号は、その半分ないし 3 分の 2 が攻撃されるという驚くべき事実を発見した。これほど大量な暗号系が攻撃されることは今まで公開鍵暗号の歴史の中でも見られなかった。その反響が大変大きく、例えば、世界で楕円暗号については最も権威のある学会 ECC2007 で研究代表者が招待講演に招かれて、本グループの研究成果は高い評価が受けた。また、フランスエコールポリテックやカナダトロント大学など海外の主な研究グループより講演の依頼も受けた。

さらに、2011 年 6 月に Ecole Polytechnique Fédérale de Lausanne, Switzerland が開催する ECDLP 国際ワークショップでは、本研究の成果を紹介する招待講演に招かれている。

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者は下線）

〔雑誌論文〕（計 11 件）

① M. Shimura, F.Momose, J.Chao "Elliptic curves with weak coverings over cubic extensions of finite fields with even characteristic II" Proceedings of SCIS2011, **「暗号と情報セキュリティシンポジウム」電子情報通信学会**, **査読無**, 2011, 2C1-3.

②H. Yoshimori, T.Iijima, J.Chao " Security Analysis of Elliptic/hyperelliptic Curves against GHS Attack without Isogeny Condition" Proceedings of SCIS2011, **「暗号と情報セキュリティシンポジウム」電子情報通信学会**, **査読無**, 2011, 2C1-2.

③T. Iijima, F. Momose, J.Chao ”Elliptic and hyerelliptic curves with weak covering without isogeny condition” Proceedings of SCIS2010, **「暗号と情報セキュリティシンポジウム」電子情報通信学会**,**査読無**, 2010,2D2-1

④M. Shimura, F. Momose, J.Chao, "Elliptic curves with weak covering on cubic extension of finite fields with even characteristic" Proceedings of SCIS2009, **「暗号と情報セキュリ**

ティシンポジウム」電子情報通信学会,査読無, 2010, 1D2-2.

⑤趙晋輝、松尾和人、百瀬文之, 書評"R.Avanzi, C.Doche, T.Lange, K.Nguyen and F.Vercauteren：Handbook of hyperelliptic curve cryptography".「数学」, 日本数学会,査読有, 第61巻4号, 2009, 433－436.

⑥F. Momose, J. Chao "Elliptic curves with weak coverings over cubic extensions of finite fields with odd characteristics" IACR E-print Archive http://eprint.iacr.org/2009/236, 査読無, 2009, 1－56.

⑦T. Iijima, F. Momose, and J. Chao "Classification of elliptic/hyperelliptic curves with weak coverings against GHS attack without isogeny condition" IACR E-print Archive http://eprint.iacr.org/2009/613, 査読無, 2009, 1-32.

⑧T. Iijima, F. Momose, J. Chao "Classification of Weil Restrictions Obtained by (2,...,2) Coverings of P^1 without Isogeny Condition in Small Genus Cases" Proceedings of SCIS2009, 「暗号と情報セキュリティシンポジウム」電子情報通信学会, 査読無, 2009, 2C3-4.

⑨N. Hashizume and F. Momose and J. Chao "On Implementation of GHS Attack against Elliptic Curve Cryptosystems over Cubic Extension Fields of Odd Characteristics" IACR E-print Archive, http://eprint.iacr.org/2008/215, 査読無, 2008, 1-34.

⑩T. Iijima, F. Momose, J. Chao, "On Certain Classes of Elliptic/Hyper-elliptic Curves with Weak Coverings against GHS Attack" Proceedings of SCIS2008, 「暗号と情報セキュリティシンポジウム」電子情報通信学会, 査読無, 2008, 2D4-2.

⑪橋詰直紀、百瀬文之、趙晋輝「奇標数3次拡大体上の楕円曲線暗号に対するGHS攻撃の実装」Proceedins of SCIS2008,「暗号と情報セキュリティシンポジウム」電子情報通信学会, 査読無, 2008, 2D3-5.

〔学会発表〕（計４件）

①（招待講演）飯島努、趙晋輝“Elliptic and hyperelliptic curves with weak covering under isogeny condition”International workshop on ECDLP (Elliptic curve discrete logarithm problems) Ecole Polytechnique Fédérale de Lausanne Switzerland, 2011年5月26日-27日

②大川 一樹, 飯島 努, 趙晋輝「奇標数3次拡大体上の楕円曲線に対する B. Smith 変換を用いた攻撃」電子情報通信学会暗号と情報セキュリティ研究会、2011年3月3日, 大阪大学,

③原 弘幸, 飯島 努, 志村 真帆呂, 趙 晋輝「拡大体上の楕円曲線のnon-hyperelliptic被覆の構成法に関する考察」電子情報通信学会暗号と情報セキュリティ研究会, ISEC 2011年3月5日, 大阪大学.

④ (招待講演) 趙晋輝「楕円曲線上の公開鍵暗号」シンポジウム「数学的土壌の上に花開く暗号技術―楕円曲線と暗号理論」2009年9月29日, 中央大学駿河台記念館.

〔図書〕（計 １件）

辻井重男、笠原正雄、趙晋輝 共著、森北出版、「暗号理論と楕円曲線」2008 (p.52-114)

６．研究組織

(1)研究代表者

趙 晋輝（Jinhui Chao）

中央大学・大学院理工学研究科・教授

研究者番号：60227345

(2)連携研究者

百瀬 文之（Fumiyuki Momose）

中央大学・大学院理工学研究科・教授

研究者番号：80182187