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

平成　３０　年　　６　月　　６　日現在

機関番号：　３２６４１
研究種目：　基盤研究(C)（一般）
研究期間：　2015～2017
課題番号：　１５Ｋ００００２２

研究課題名（和文）被覆攻撃に対する楕円・超楕円暗号系の安全性に関する研究

研究課題名（英文）Security Analysis of Elliptic/Hyperelliptic Curve Cryptosystems Against Cover 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

交付決定額（研究期間全体）：（直接経費）　　3,500,000円

研究成果の概要（和文）：拡大体上に定義される楕円・超楕円曲線暗号は、素因数分解や離散対数に基づく暗号方式に比べて格段に安全であるのみならず、コンパクトな高速実装に適しているため、IoT暗号の候補として注目されている。しかし、拡大体上の楕円・超楕円暗号に対して、GHS 攻撃が知られているが、Freyによりそれをさらに一般的な被覆攻撃に拡張されており、その安全性解析は殆ど行われていない。本研究では、被覆攻撃は楕円・超楕円暗号に対して極めて危険であることを示し、さらにその数学的構造の解明によって、攻撃される曲線の分類手法を確立し、弱い曲線すべてを列挙した。さらに、各種攻撃可能性の検討を行い、安全性確保の方策を明らかにした。

研究成果の概要（英文）：Elliptic curve and hyperelliptic curve based cryptosystems are the most secure systems available now comparing with those based on factorization and discrete logarithm. Moreover using the definition fields as finite extensions of finite fields, fast and compact implementation of these systems become possible, which are then expected to play an important role in IoT technology. On the other hand, aiming at curves over extension fields, the GHS attack was proposed by Frey first then generalized to cover attack. This research present the first and complete security analysis on cover attack and GHS attack. We show that these attacks are very powerful. By a systematic analysis of the mathematical structure, we proposed algorithms to mathematically classify all curves which are subjected to these attacks. Then we obtain a complete list of all weak curves which will be useful in system design. We also discuss variations of these attacks and methodology to build a secure cryptosystem.

研究分野：　暗号理論と情報セキュリティ

キーワード：　Cryptography　Elliptic Curve　Security Analysis　GHS attacks　Cover Attakcs　IoT Cryptosystems　Hardware Implementation　Extension Fields

１．研究開始当初の背景

(1)近年、情報通信技術のモバイル化、クラウド化及びソーシャルネットワークそして IoT、仮想通貨などの新しい技術における急激な進展を背景に、ネット犯罪やプライバシー侵害などは深刻な社会問題となりつつある。そのために情報セキュリティとりわけ暗号技術の個人情報やプライバシー保護における役割が大きく期待されている。現在公開鍵暗号やセキュリティプロトコールの根底をなしている暗号学一方向性関数は、準指数時間の複雑さをもつ素因数分解及び有限体上の離散対数問題、そして指数時間の複雑さを持つ楕円･超楕円曲線上の離散対数が知られている。 前者に比べて後者は本質的に難しい問題であるため、コンパクトなサイズでもより高い安全性を実現することができる。そのため、認証基盤から始めボロックチェンなどの仮想通貨まで利用されている。また、現在 1024 ビットないし 2048 ビットの鍵長を要するのに対して、 楕円･超楕円暗号の鍵長は 160 ビットであるため、情報機器の軽量化、小型化そして省エネルギー化に有利とされている。特に、有限体の拡大体上に定義されている DH 鍵共有方式や ElGamal 暗号､DSA 署名方式、そして楕円曲線・超楕円曲線版の拡張は、IoT 基盤においては、コンパクト化で高速なハードウェア実装が可能であるため、IoT 暗号方式として有望視されている。
(2)一方、有限体の拡大体の特有の構造を利用して、暗号方式に関する攻撃も最近新しい進展を見せている。有限体上の離散対数に関する攻撃が、medium size field つまり拡大次数 n と標数 p がほぼ同程度の有限体上の離散対数を関数体ふるい法による解読記録が 6120 ビットに上ったと報告され、特殊な場合とはいえ、有限体上の離散対数に対する信頼感が揺るがされたことは間違いない。そのために、より安全な楕円･超楕円暗号はさらに重要性が増してくると思われる。
(3)一方、楕円・超楕円暗号については、近年拡大体の構造を利用して準指数時間のアルゴリズムを目指す研究が話題となっている。最近、Semaev をはじめとして、Gaudry, Diem により、拡大体 Fp^n 上に定義される楕円曲線の構造に注目して、Fp 有理点を因式基底とする index calculus 法が研究された。特に、拡大体 Fq, q=p^n 上定義された楕円曲線に対して、n^2=log p という条件で、つまり、ADH の条件における種数を拡大次数に置き換えた場合、index calculus 法が準指数時間であることを証明した。しかし、それは上記 medium size field 攻撃同様に、準指数時間攻撃の可能性が標数 p と拡大次数 n という二つのパラメータ平面つまり 2D 空間の中で、密度ゼロの 1-パラメータファミリのみに存在すると意味するもので、むしろ Lenstra が期待していた、整数論的な構造を楕円曲線に転用することで、有限体上と同様に準指数時間攻撃を開発することは、極く特殊なクラスの曲線を除けば、殆ど望めないことを実証することとなり、即ち、楕円曲線或いは低種数超楕円曲線は、有限体上の離散対数よりはるかに強いことを示すこととなった。さらにこの攻撃は漸近的な意味合いしか持たず、有限体のサイズが 3000 ビット以上でないと、Pollard のロー法や、ラムダ法などの平方根オーダのアルゴリズムよりも遅く、楕円曲線の実用標準化は 160 ビットであることを考えると、現実的な脅威はほとんど与えられないことが明らかである。
しかし､2012 年以降 Semaev, Gaudry, Diem, Nagao による Weil descent と Semaev summation 多項式を併用して Grobner 基底で解くアルゴリズムは、拡大体上の楕円曲線離散対数問題は準指数時間になる証明、例えば Petit–Quisquater(2012), Semaev(2015), Karabina (2015)により発表され一時注目されたが、その後その証明に使われる FFD(first fall degree)条件などの成立が疑問視され、現在はその準指数性は認められておらず、楕円暗号の安全性は依然完全指数時間のままである。
(4)同様に拡大体の特徴を利用しているが、すべての曲線ではなく、その中で特殊な数学構造を持つ楕円・超楕円曲線を狙い撃ちする攻撃として、GHS 攻撃が知られている。具体的に、Frey の楕円暗号に Weil descent を適用するアイデアを逆用して、拡大体 Fp^n 上の楕円曲線の離散対数問題を Fp 上の超楕円曲線のヤコビ多様体へ変換して攻撃する方法である。 しかしながらこの変換は常にできるわけでなく、曲線の方程式の形や、変換された曲線の種数、 Frobenium 自己準同形写像の位数、そして conorm-norm 写像による離散対数の変換可能性などの条件が必要であった。楕円・超楕円曲線の構造を利用した新しい攻撃の可能性を覗かせた意味が大きいが、例題により示された攻撃のシナリオはアトホック的感が否めない。
また、Diem は奇標数楕円曲線から変換された曲線の種数の下界を評価して、それが拡大次数に従って指数的に増大、 例えば 11 次拡大以上の Galois 閉包の種数が 5000 以上となり攻撃が不可能になることを示した。一方、低い次数の拡大体においては、 攻撃例を示すことのみに止めた。 従って、 GHS 攻撃に破れる曲線があったとしても特殊で極わずかなもので、現実的な脅威をなさないと信じられるようになった。
(5) 一方、我々のグループは、同種条件のもとで、GHS 攻撃に対して組織的な解析を行うことで、その脅威を徐々に明らかにしてきた。例えば 3 次拡大体での楕円暗号の鍵長が 160 ビットと設計されていても、GHS 攻撃に対する強度は 107 ビットしかなく、現在楕円暗号の解読記録は 112 ビットであることを考えると、全く安全性を持たないこと

が分かる。さらにこのような曲線は、奇標数拡大体では、曲線全体の半分以上である証明を発表し、また、偶標数 3 次拡大体では破れる曲線がさらに多く全体の 4 分の 3 以上存在することを証明した。従って、ランダムな曲線を選ぶなどの対策では到底回避できなく、GHS 攻撃は、楕円暗号、超楕円暗号に対して最も現実的に危険であることは明らかである。 その結果は代表者が楕円暗号国際学会 ECC2007 の招待講演で公表していた。
⑹さらに、G. Frey が代数幾何的なアプローチにより、GHS というアトホックな攻撃を一般化した。具体的に、楕円・超楕円曲線を射影曲線 P1 上の 2 次被覆とみなしたとき、 これらを覆う P1 上の新たな被覆曲線が存在すれば、 離散対数問題を被覆曲線上へ写像して攻撃する「被覆攻撃」を 2003 年に発表した。この攻撃は、GHS 攻撃そして Weil descent 攻撃を特殊な場合として含んでおり、今まで最も一般的な攻撃シナリオを示すものである。
しかしながら、有限体の拡大体上に定義される楕円曲線・超楕円曲線暗号への被覆攻撃に対する暗号系の安全性解析は殆ど進んでいないのは現状である。

２．研究の目的

⑴本研究では、今まで蓄積してきた GHS、被覆攻撃の研究実績を元に、GHS 攻撃を含み、被覆攻撃の全貌を解明すべく、楕円・超楕円曲線暗号の安全性を体系的に解析し、その数学的構造の解明によって、攻撃される曲線の分類手法を確立すること、また、具体的に攻撃される楕円・超楕円曲線のすべてを列挙すると同時に、攻撃手法に関する手法を検討することによって被害範囲を明らかにしたい。
⑵特に今までの GHS 攻撃に対しては、同種条件つまり攻撃者にとって最も有利な条件のもとで安全性解析を行ってきたが、被覆攻撃に対して、同種条件なしのすべての攻撃対象となる楕円曲線と超楕円曲線の完全分類を目的とする。

３．研究の方法

(1)本研究は、 まず被覆攻撃の数学的構造を解析することで、 代数幾何学と Galois 表現理論に基づき、攻撃される楕円・超楕円曲線の内在特徴を解明し、それらの分類理論を確立し、分類アルゴリズムを開発することで、そのすべての列挙を目指した。そして、被覆曲線が存在するとき、それを実際に構築することで、攻撃の実装研究を行った。また、ブラックリストを作成すると同時に、安全な楕円・超楕円曲線を明示するホワイトリストも求める。
(2)従来の GHS 攻撃の安全性解析の最大の問題は、アットホークな方法で攻撃される曲線の具体例を挙げても、攻撃対象となる曲線全体が探し尽くせないことであった。被覆攻撃に対しても同様に攻撃される曲線全体を理解するためには、 まず拡大体 Fp^n 上定義される楕円・超楕円曲線の中で、F_p 上定義される P1 への被覆曲線を持つものの全体を分類する必要がある。
本研究は Galois 表現の理論を利用し、被覆曲線の代数幾何学的及び位相幾何学的構造を明らかにすることで分類理論を構築すると同時に、分類アルゴリズムを開発した。特に、被覆曲線自体の構造が大変複雑で多様で、解明するのは難しいため、今まではそのヤコビ多様体は離散対数を定義する曲線のそれと同種であるという「同種条件」の下で、また、同種写像の余次元が有限の場合について、分類研究を行ってきた。これは攻撃側にとっては最も有利なシナリオではあるが、被覆攻撃のすべての可能性をカバーするためには、同種条件や余次元制限を課すことなく、被覆曲線が存在する楕円・超楕円曲線全体の分類を示した。特に、標数 2 の場合においては、wild ramification という悪名高い複雑な分岐の解析が極めて困難であることが知られている。それに対処するために ordinary と non-ordinary の場合に対して、代数多様体の分岐群そして高次分岐理論を応用して、分岐構造を明らかにすることで、攻撃される曲線の完全分類と列挙を行った。
(3)同型写像による攻撃、つまり曲線そのものはブラックリストに入っていなくとも、それをある種の同型写像によって、弱い曲線に変換される可能性があるため、その脅威を検討しなければならない。今までの楕円暗号においては、このような攻撃を考えられてこなかったため、ここで、このような攻撃を、同型攻撃と呼ぶことにする。同型攻撃の解析をするためには、定義体のみならず、その代数拡大体上の同型写像も調べた。さらに、同種写像により攻撃も検討した。
(4)暗号攻撃の一つ重要な手段は、攻撃対象を具体化して、攻撃アルゴリズムを実装することである。被覆攻撃においても、実際に被覆曲線を構築することで、アルゴリズムを実装することが重要である。今までは、Diem の関数体を用いた手法と橋詰、百瀬、趙が同種条件の下で、奇標数 3 次拡大体上の楕円曲線の被覆曲線を構築することに成功した。 また、 橋本、 志村、 趙が奇標数の 3 次拡大体上種数 2 の超楕円曲線の被覆曲線を構築された。さらに、条件なしで一般的な拡大次数と高い種数の曲線の構築法を検討した。
(5) 研究体制としては、整数論の保型形式の専門家である志村真帆呂氏は連携研究者として協力して頂き、 楕円･超楕円暗号を専門とする光電（株）研究員の飯島努氏を研究協力者としてお願いした。

４．研究成果

(1)奇標数素数次拡大体上に定義される楕円曲線に対して、(2,2,…,2)被覆曲線が存在するもの完全分類を行った。特に、従来仮定していた同種条件や種数の余次元制限をなくして、任意の楕円曲線暗号に対して、被覆攻撃によって攻撃される対象のすべてを明らかにした。これによって、GHS 攻撃を含め、被覆攻撃に対する楕円暗号の安全性解析の最終かつ完全な解答を与えた。
(2)奇標数素数次拡大体上に定義される種数 2 の超楕円曲線に対して、(2,2,…,2) 被覆曲線が存在するものの完全分類を行った。同様に今まで用いた同種条件と種数の余次元制限を仮定することなく、任意の超楕円曲線暗号の中で被覆攻撃の攻撃対象をすべて列挙できた。これによって、GHS 攻撃を含め、被覆攻撃に対する種数 2 超楕円暗号の安全性解析の最終かつ完全な解答を与えた。
(3)今までの解析では、定義体の有限体の拡大次数が、素数次数と仮定しており、合成数次数の拡大体の場合は、その素因数である各素数次拡大体の場合を足し合わせれば得られると考えられた。そこで我々は、奇標数合成数次数拡大体上の楕円曲線の完全分類をも行い、特に合成数のすべての素因数が拡大次数である素数次拡大体上の曲線に含まれない、合成数次数拡大体上にのみ存在する曲線クラスの存在を発見した。特に IoT 暗号における高速コンパクト実装にスムーズな低次数拡大体が利用されるため、実用的な意義が大きい。
(4)奇標数楕円曲線暗号に対して、定義体が素体の 3 次拡大であるとき、被覆曲線が種数 3 の超楕円曲線の場合と、種数 3 の非超楕円曲線のタイプ I とタイプ II と分類された場合に関して、被覆曲線を構築し実装攻撃を検討した。
(5)偶標数素数次拡大体上の被覆曲線の構成法として、単純拡大を用いる手法と Elliptic Involution を用いた手法により明示的に楕円曲線の超楕円曲線被覆を構築する手法を提案した。特に曲線を定義方程式により与えたため、実装攻撃の検討が可能となった。
(6)楕円暗号或いは超楕円暗号の曲線が、以上の完全分類のブラックリストに含まれていないが、楕円曲線或いは超楕円曲線の同種変換或いは同型変換によって、攻撃対象になるという同種攻撃、同型攻撃に対して解析を行い、安全な曲線の判別法について検討した。
(7)本研究の成果は、国内のみならず、スペインバルセロナ整数論ゼミナールでの招待講演も行った。

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には下線）

〔雑誌論文〕（計 14 件）

①小林龍平、飯島努、趙晋輝「被覆曲線を持つ奇標数合成次拡大体上の楕円曲線の分類」「SCIS2018　暗号と情報セキュリティシンポジウム」論文集、電子情報通信学会，査読無，2018，3B3-1.

②. Naoki Hashizume, Fumiyuki Momose, Jinhui Chao, ``On implementation of GHS attack against elliptic curve cryptosystems over cubic extension fields of odd characteristic", *“Number Theory Related to Modular Curves”,*Contemporary Mathematics, vol. 701, American Mathematics Society, 査読有, 2018, pp. 125-150.
DOI: https://doi.org/10.1090/conm/701

③小林 龍平、飯島 努、趙 晋輝，「GHS 攻撃の対象となる奇標数合成数次拡大体上の楕円曲線の分類」「SCIS2017　暗号と情報セキュリティシンポジウム」論文集、電子情報通信学会，査読無，2017，4B1-2.

④小林龍平、飯島　努、趙　晋輝 、「GHS 攻撃の対象となる奇標数合成数次拡大体上の楕円曲線の分類 その 2」暗号と情報セキュリティ研究会,電子情報通信学会、査読無、 信学技報、 vol．116，no．505，ISEC2016-95，2017，pp．41-48.

⑤久木埼聖矢、志村真帆呂、趙　晋輝、「単純拡大を用いた偶標数有限体上の楕円曲線の被覆曲線の構成」、暗号と情報セキュリティ研究会,電子情報通信学会、査読無、 信学技報、vol．116，no．505，ISEC2016-101，2017，pp．79-83.

⑥森下拓也、志村真帆呂、趙　晋輝、「偶標数素数次拡大体上の楕円曲線に基づく射影直線上の(2,...,2)型被覆の構成法に関する考察」暗号と情報セキュリティ研究会,電子情報通信学会、査読無、信学技報、vol．116，no．505，ISEC2016-102，2017，pp．85-89.

⑦ Ryutaro Ushigome, Takeshi Matsuda, Michio Sonoda and Jinhui Chao
“Examination of classifying hoaxes over SNS using Bayesian Network“ Proceedings of CANDAR 2017: The Fifth International

Symposium on Computing and Networking, 査読有、2017, pp. 606-608.
DOI 10.1109/CANDAR.2017.103

⑧飯島努、志村真帆呂、趙晋輝、「GHS 攻撃の対象となる楕円曲線の同型攻撃に関する考察」、「SCIS2016　暗号と情報セキュリティシンポジウム」論文集、電子情報通信学会，査読無，2016，4D1-2.

⑨小林 龍平、飯島 努、趙 晋輝、「GHS 攻撃の対象となる奇標数素数次拡大体上種数 2 の曲線の完全分類」、「SCIS2016　暗号と情報セキュリティシンポジウム」論文集、電子情報通信学会，査読無，2016，4D1-3.

⑩林 弘悦、趙 晋輝、“Fault attacks to elliptic curve cryptosystems with definition equation errors”、「SCIS2016 暗号と情報セキュリティシンポジウム」論文集、電子情報通信学会，査読無，2016，4D2-1.

⑪ Takuya Morishita、Jinhui Chao,
“ECM over dummy quadratic residue rings”「SCIS2016　暗号と情報セキュリティシンポジウム」論文集、電子情報通信学会，査読無，2016，4D2-5.

⑫飯島努、趙晋輝、「GHS 攻撃の対象となる奇標数素数次数拡大体上の楕円曲線 その 2」、「SCIS2015　暗号と情報セキュリティシンポジウム」論文集、電子情報通信学会，査読無，2015，1F2-1.

⑬飯島努、趙晋輝、「GHS 攻撃の対象となる奇標数素数次数拡大体上の楕円曲線 その 2」、「SCIS2015　暗号と情報セキュリティシンポジウム」論文集、電子情報通信学会，査読無，2015，1F2-1.

⑭細萱隆文、飯島努、志村真帆呂、趙晋輝、「GHS 攻撃の対象となる被覆曲線を持つ楕円曲線の同型類に関する考察」、暗号と情報セキュリティ研究会,電子情報通信学会、査読無、 信学技報、vol．114、 no．471、ISEC2014-89、2015，pp．89-95.

〔学会発表〕（計４件）

①Jinhui Chao, (Invited talk) "Recent Topics on elliptic and hyperelliptic cryptosystems" Catalonia Number Theory Seminar, Seminari Teoria de Nombres de Barcelona (UB-UAB-UPC) Aula Màster del Campus EPSEVG (UPC, Vilanova i la Geltrú) 2 June, 2017.

②森下 拓也、 趙 晋輝 「擬似的 2 次拡大環上の楕円曲線法」情報科学技術フォーラム講演論文集 14(4)，275-276，L-037，2015-08-24

③林 弘悦、趙 晋輝 「楕円曲線暗号における曲線パラメータに対する Fault 攻撃」情報科学技術フォーラム講演論文集、L-038，14(4)，277-278，2015-08-24

④久木崎 聖矢 , 松尾 和人 , 趙 晋輝 「サイドチャネル攻撃に安全な Granger-Scott 法」情報科学技術フォーラム講演論文集 14(4)，L-039，279-280，2015-08-24

６．研究組織

(1)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

(2)研究分担者
（　　）

研究者番号：

(3)連携研究者
志村　真帆呂（SHIMURA，Mahoro）
東海大学・理学部・准教授
研究者番号：　30308209

(4)研究協力者
飯島努（IIJIMA，Tsutomu）
光電株式会社・特機部・研究員