様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

# 科学研究費助成事業　　研究成果報告書

平成 ２８ 年　 ４ 月 １９ 日現在

機関番号：１７１０２
研究種目：挑戦的萌芽研究
研究期間：2013～2015
課題番号：２５５４００４７

研究課題名（和文）楕円曲線暗号のグレブナ基底による安全性解析

研究課題名（英文）Security Analysis of Elliptic Curve Cryptography using Groebner Basis

研究代表者
高木　剛（Takagi, Tsuyoshi）

九州大学・マス・フォア・インダストリ研究所・教授

研究者番号：６０４０４８０２

交付決定額（研究期間全体）：（直接経費）　　3,000,000円

研究成果の概要（和文）：本研究課題では、楕円曲線暗号に対する新しい攻撃法として、グレブナ基底を用いた多変数多項式による求解アルゴリズムを考察した。Semaev多項式の対称性を利用した高速化手法に注目し、グレブナ基底の計算の途中で多項式の次数が増大しない拡大体の基底表現によりメモリ量を削減する高速化を提案した。その結果、拡大次数29次の標数2の有限体上で定義される楕円曲線の離散対数問題を、計算代数ソフトウェアMagmaを用いてAMD Opteron 6276(メモリ512GB)において約34日で解くことができた。この解読実験データにより、想定される攻撃者の計算能力限界をより正確に評価できるようになった。

研究成果の概要（英文）：In this research, we have investigated some algorithms using Groebner basis for solving the discrete logarithm problem over elliptic curve of characteristic 2. From the symmetric structure of Semaev polynomial we proposed an efficient algorithm that reduces the complexity and memory during the computation of Groebner basis. The proposed algorithm enables us to solve the discrete logarithm problem over elliptic curve of finite field of extension degree 29 in about 34 days using computer algebra software Magma on AMD Opteron 6276 with 512GB memory. From this cryptanalysis data we are able to estimate the computational over-limit of the expected attackers more precisely.

研究分野：暗号理論

キーワード：暗号・認証等　公開鍵暗号　楕円曲線暗号　離散対数問題　グレブナ基底

## １．研究開始当初の背景

楕円曲線暗号は、IEEE や ISO などで既に国際標準化され実用化し、広く利用されている。また、日本でも CRYPTREC により電子政府推奨暗号に認定されており、楕円曲線暗号の安全性が評価・監視されている。

国際会議 Eurocrypt2012 において Faugere-Perret-Petit-Renault は、楕円曲線暗号に対してグレブナ基底を用いた新しい攻撃方法（FPPR 攻撃法）を提案した。Asiacrypt 2012 において、Petit-Quisquater は、FPPR 攻撃法の計算時間は準指数時間と評価している。FPPR 攻撃法は、楕円曲線暗号の歴史で初めて指数時間の限界を破るアルゴリズムであるため、その理論的正当性と攻撃の実用性が議論され始めている。

## ２．研究の目的

本研究課題では、楕円曲線暗号の安全性評価を目的として、FPPR 攻撃法およびその改良版を考察し、以下の問題に取り組む。

① FPPR 攻撃法で用いられたグレブナ基底に関する数学的な仮定を理論的に再検証する。
② FPPR 攻撃法で核となる Semaev 多項式の代数構造を再考察し、攻撃法の高速化を検討する。
③ 改良 FPPR 攻撃法をプログラム実装し、計算機解読実験により安全な鍵サイズを見積もる。

## ３．研究の方法

楕円曲線暗号に対する FPPR 攻撃法は、次の 3 段階に大別することができる。

(a) 因子基底選択ステップ (Factor Basis definition)
(b) 関係探索ステップ (Collection of relations)
(c) 線形代数ステップ (Linear algebra)

本研究では、各ステップに関して $GF(2^n)$ 上の楕円曲線の代数的構造を考察し、FPPR 攻撃法の理論的検証とアルゴリズムの高速化を目指す。また、改良 FPPR 攻撃法を汎用計算機で実装することにより標準化されている鍵サイズ n に対する解読計算量を求め、楕円曲線暗号の安全性を評価する。

## ４．研究成果

平成 25 年度は、FPPR 攻撃の計算量と使用メモリ量を削減する手法を考察した。特に、合成数の拡大次数に対して提案された Semaev 多項式の対称性を利用した既存の高速化手法に注目し、それを素数次拡大に適応する方法を提案して、理論的な計算量の見積もりと計算機実験による評価を与えた。提案方式では、グレブナ基底の計算の途中で多項式の次数(degree of regularity)が増大しない拡大体の基底表現を利用することにより計算量とメモリ量を削減している。改良アルゴリズムにより、拡大次数 29 次の標数 2 の有限体上で定義される楕円曲線の離散対数問題を、計算機代数ソフトウェア Magma を用いて AMD Opteron 6276(メモリ 512GB)において約 34 日で解くことができた。

| $n$ | $\#E_{\alpha,\beta}$ | FPPR (sec) | *ThisWork* (sec) |
|---|---|---|---|
| 7 | 4*37 | 1.574 | 0.864 |
| 11 | 4*523 | 8.625 | 6.702 |
| 13 | 4*2089 | 49.698 | 31.058 |
| 17 | 4*32941 | 2454.470 | 1364.742 |
| 19 | 4*131431 | 22474.450 | 9962.861 |
| 23 | 4*2098553 | N/A | 66703.400 |
| 29 | 4*134229259 | N/A | 2953043.698 |

*It is the product symbol which denoted the order of the EC group.

図１：拡大次数 n に対する解読時間の比較

一方、変数の個数 n が方程式の個数 m よりも大きいの場合の多変数 2 次多項式の求解問題を考察し、$n \geqq m(m+3)/2$ の場合に多項式時間で解くことができるアルゴリズムを提案した。グレブナ基底を用いた解読計算量が 2 の 80 乗であると言われている m=28,n=504 に対して、Magma により標準的な PC を用いて 78.8 秒で解くことができた。更には、RSA 暗号の安全性も考察し、高速実装可能な multi-prime RSA (MPRSA)に対する評価を行った。MPRSA は公開鍵 n が複数の素数の積 $n = p_1 p_2 \cdots p_r$ $(r > 2)$で鍵生成される RSA 暗号の変形版であり、素数の差 $\Delta$ ($\Delta = p_r - p_1, p_1 < p_2 < \cdots < p_r$)が小さい場合に多項式時間となる新しい低指数攻撃を提案した。

平成 26 年度は、楕円曲線暗号に対する新たな攻撃法として、有限体上の多変数多項式の求解問題の解法アルゴリズムを考察している。この問題の難しさは、変数の個数 n、多項式の個数 m、有限体の位数 q などにより変化する。昨年度、PQCrypto2013 において、変数の個数 n と方程式の個数 m が関係式 $n \geqq m(m+3)/2$ を満たし、更に有限体の標数が偶数の場合に、多項式時間で動作する効率的なアルゴリズムを提案した。今年度は、この方式の適用範囲を拡大し、標数が奇数である場合でも検索法の多層木構造化により、多項式時間で解くことが可能なアルゴリズムを構築した。本成果は、2014 年 10 月にトロントで開催された国際会議 PQCrypto2014 において発表した。

また、昨年度までに研究会や国際会議で発表した論文 4 編をジャーナル論文化した(電子情報通信学会英文論文誌 2 編、情報処理学会論文誌など)。特に、国際会議 IWSEC 2013

において発表した楕円曲線暗号の FPPR 攻撃に対する安全評価の論文は、大規模な計算機実験により安全性解析を詳細に考察した Full Paper として、Pacific Journal of Mathematics for Industry において発表した。

平成 27 年度は、2015 年 4 月 3 日に米国の Washington D.C.で開催されたワークショップ NIST Workshop on Cybersecurity in a Post-Quantum World において、有限体上の多変数多項式求解問題の困難性を評価するための解読コンテスト MQ Challenge を発表した。また、多変数多項式の求解問題を含むポスト量子暗号の研究動向に関する招待講演を 2 件行った(3rd ESTI Workshop on Quantum-safe Cryptography at Seoul, Future Cryptographic Technology Forum: Cryptographic Technologies in the Era of Quantum Computation at Seoul National University)。
また、H27 年度から参加した分担者の伯田は、多変数多項式を用いた Matsumoto-Imai 暗号の Tame 性に関する研究を進め、ジャーナル論文 1 編を Advances in Mathematics of Communications において発表した。

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７件）


① Yun-Ju Huang, Christophe Petit, Naoyuki Shinohara, Tsuyoshi Takagi, Improvement of Faugere et al.'s Method to Solve ECDLP, The 8th International Workshop on Security, IWSEC 2013, LNCS 8231, pp.115-132, 2013. DOI: 10.1007/978-3-642-41383-4_8

② Hiroyuki Miura, Yasufumi Hashimoto, Tsuyoshi Takagi, Extended Algorithm for Solving Underdefined Multivariate Quadratic Equations, Fifth International Conference on Post-Quantum Cryptography, PQCrypto 2013, LNCS 7932, pp.118-135, 2013. DOI: 10.1007/978-3-642-38616-9_8

③ Hui Zhang, Tsuyoshi Takagi, Attacks on Multi-Prime RSA with Small Prime Difference, 18th Australasian Conference on Information Security and Privacy, ACISP 2013, LNCS 7959, pp.41-56, 2013. DOI: 10.1007/978-3-642-39059-3_4

④ Chen-Mou Cheng, Yasufumi Hashimoto, Hiroyuki Miura, Tsuyoshi Takagi, A Polynomial-Time Algorithm for Solving a Class of Underdetermined Multivariate Quadratic Equations over Fields of Odd Characteristics, 6th International Workshop on Post-Quantum Cryptography, PQCrypto 2014, LNCS 8772, pp.40-58, 2014. DOI: 10.1007/978-3-319-11659-4_3

⑤ 鷲見拓哉，石黒司，清本晋作，三宅優，小林透，高木剛，Web Workers を用いた多変数公開鍵暗号 Rainbow の並列実装，情報処理学会論文誌，Vol.55, No.9, pp.2061-2071, 2014.

⑥ Yun-Ju Huang, Christophe Petit, Naoyuki Shinohara, Tsuyoshi Takagi, Improvement of FPPR method to solve ECDLP, Pacific Journal of Mathematics for Industry, Vol. 7-1, pp.1-9, 2015. DOI: 10.1186/s40736-015-0012-6

⑦ Keisuke Hakuta, Hisayoshi Sato, Tsuyoshi Takagi, On tameness of Matsumoto-Imai central maps in three variables over the finite field F2, Advances in Mathematics of Communications, Vol.10, No.2, pp.221-228,2016. DOI:10.3934/amc.2016002


〔学会発表〕（計 6 件）


① Tsuyoshi Takagi, MQ challenge: hardness evaluation of solving multivariate quadratic problems, DIMACS Workshop on The Mathematics of Post-Quantum Cryptography,招待講演, 2015 年 01 月 14 日, Rutgers University, USA

② 高木 剛, 多変数多項式暗号の安全性評価, 第 6 回暗号フロンティア研究会, 招待講演, 2015 年 03 月 18 日, 北陸先端科学技術大学院大学

③ Takanori Yasuda, Xavier Dahan, Yun-Ju Huang, Tsuyoshi Takagi, Kouichi Sakurai, MQ Challenge: Hardness Evaluation of Solving Multivariate Quadratic Problems, NIST Workshop on Cybersecurity in a Post-Quantum World, 2015 年 4 月 3 日, Washington D.C, USA

④ Tsuyoshi Takagi, Security Analysis of Quantum-Safe Cryptography, 3rd ESTI Workshop on Quantum-safe Cryptography, 招待講演, 2015年10月7日, Seoul, Korea

⑤ Tsuyoshi Takagi, Recent Developments of Post-Quantum Cryptography, Future Cryptographic Technology Forum: Cryptographic Technologies in the Era of Quantum Computation, 招待講演, 2016年1月14日, Seoul National University, Korea

〔その他〕
ホームページ
九州大学マス・フォア・インダストリ研究所
高木研究室
http://imi.kyushu-u.ac.jp/~takagi/

## ６．研究組織

(1)研究代表者
高木 剛（TAKAGI TSUYOSHI）
九州大学・マス・フォア・インダストリ研究所・教授
研究者番号：60404802

(2)研究分担者
伯田　恵輔（HAKUTA KEISUKE）
島根大学・総合理工学研究科・助教
研究者番号：90587099