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　１５　日現在

機関番号：　１２６０１
研究種目：　基盤研究(B)（一般）
研究期間：　2013～2017
課題番号：　２５２８００４８

研究課題名（和文）ペアリング暗号の大規模解読実験による安全性解析

研究課題名（英文）Security Evaluation of Pairing-Based Cryptography via Large-Scale Cryptanalysis

研究代表者
高木　剛（Takagi, Tsuyoshi）

東京大学・大学院情報理工学系研究科・教授

研究者番号：６０４０４８０２

交付決定額（研究期間全体）：（直接経費）　　11,500,000円

研究成果の概要（和文）：ペアリング暗号は、従来の公開鍵暗号では実現が困難であった暗号プロトコルを構成できるため、クラウドコンピューティング時代に適した暗号として研究開発が活発に行われている。本研究課題では、ペアリング暗号の安全性の根拠となる拡大体上の離散体問題の困難性の考察を行なった。特に、拡大体上の離散対数問題の高速解法となる数対篩法exTNFSに対して、固定した鍵長に関する計算量の考察を行ない、ペアリング暗号で用いられる楕円曲線のパラメータの安全性を評価した。また、ペアリングを利用した暗号プロトコルの研究も進め、鍵漏洩に耐性のある階層的IDベース暗号、鍵の失効が可能なIDベース署名付き暗号などを考察した。

研究成果の概要（英文）：Pairing-based cryptography provides us new cryptographic protocols, which cannot be constructed by the conventional public-key cryptosystems. In this research project, we investigated the hardness of solving the discrete logarithm problem (DLP) over extension fields which is used for the security estimation of pairing-based cryptography. In particular, we evaluated the secure parameters of elliptic curves used for the pairing-based cryptography by considering the extended TNFS which is the asymptotically fastest algorithm for solving the DLP over extension fields. Moreover, we proposed several pairing-based cryptographic protocols such as anonymous hierarchical IBE with continual-key-leakage tolerance, revocable identity-based signcryption scheme, and so on.

研究分野：　情報セキュリティ

キーワード：　暗号・認証等　公開鍵暗号　ペアリング暗号　離散対数問題　大規模計算

１．研究開始当初の背景

次世代暗号として注目されているペアリング暗号は、従来の公開鍵暗号では実現が困難であった暗号プロトコルを構成できるため、クラウドコンピューティング時代に適した暗号として研究開発が活発に行われている。

本研究課題では、大規模な計算機解読実験によりペアリング暗号の安全性を解析評価する。特に、大きな標数 p の拡大体 GF(p^n)上のペアリング暗号が、実システムで安全に利用できるための鍵サイズをより正確に評価する。

２．研究の目的

本研究課題では、ペアリング暗号の安全性評価の研究を進めている。特に、拡大体上の離散対数問題の困難性を評価することを目的として数体篩法の計算量の見積もりを行っている。以下の問題に取り組む。

(1)現在のペアリング暗号の解読世界記録を超える鍵サイズの離散対数問題の解読を目指す。
(2)ペアリング暗号で利用される鍵サイズの拡大体上の離散対数問題の解読計算時間を解析する。
(3)RSA 暗号に対する解読実験との比較を行い、安全なペアリング暗号の鍵サイズを見積もる。

３．研究の方法

大きな標数 p の拡大体 GF(pn)に対する NFS 法は、次の 3 段階に大別することができる。

(a)多項式選択ステップ(Polynomial selecting)
(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拡大体 GF(p^n)の特徴を考察した高速化を検討し、GF(p^n)上の離散対数問題の解読世界新記録を目指す。また、解読結果に基づき GF(p^n)上のペアリング暗号の安全性を解析評価して、実用化されている RSA 暗号と同等の安全性を持つ鍵サイズを検討する。

４．研究成果

平成 25 年度は、Joux らは CRYPTO 2006 において、拡大体上の離散対数問題の漸近的に最も高速な手法として数体篩法 JLSV06-NFS を提案した。また、素体上の離散対数問題に対する現在漸近的に最速の解法として数体篩法 JL03-NFS が知られている。論文[1]では、JL03-NFS において用いられる 2 次元格子篩を、3 次元へ拡張した格子篩法の構成方法を検討した。特に、2 次元の格子篩法において格子点を効率的に列挙できる Franke-Kleinjung 法を、3 次元の格子篩法に拡張して基底の生成方法および効率的な列挙アルゴリズムの提案を行った。

w	Computational cost (M)	time (s)	memory (bits)
–	99342	2.125	0
2	89497	1.920	4104
3	85761	1.835	16416
4	83190	1.787	41040
5	81415	1.751	90288
6	80252	1.719	188784
7	**79683**	**1.715**	385776
8	79872	1.717	779000
6 $(2\cdot 3)$	79304	1.699	4104
12 $(2^2\cdot 3)$	78889	1.692	16416
18 $(2\cdot 3^2)$	76289	1.634	28728
24 $(2^3\cdot 3)$	78398	1.664	41040
36 $(2^2\cdot 3^2)$	75214	1.618	65664
48 $(2^4\cdot 3)$	76960	1.650	90288
54 $(2\cdot 3^3)$	73586	1.577	102600
72 $(2^3\cdot 3^2)$	75215	1.617	139536
96 $(2^5\cdot 3)$	76664	1.649	188784
108 $(2^2\cdot 3^3)$	73829	1.590	213408
162 $(2\cdot 3^4)$	**72727**	**1.569**	324218

図１：Window 幅 w に対する計算時間の比較

論文[2]では、合成数位数のペアリング暗号の高速演算に関して、2 進 3 進混合形式(w-HBTF)を用いた Window 法ベースの Miller's Algorithm の高速化アルゴリズムを提案した。超特異楕円曲線上の Tate ペアリングを用いて、Window 法ベースの Miller's Algorithm の既存方式と比較したところ、提案アルゴリズムは 80 ビットの安全性レベルで約 11%の高速化が実現できた(図 1)。

また、ペアリングを利用した暗号プロトコルの考察を行い、署名付き ID ベース暗号化方式に対して、標準モデルにおいて決定 BDH 仮定の下で IND-CCA2 及び計算 DH 仮定で EUF-CMA と安全性が証明可能となる方式を提案した[3]。複数の受信者を持つ効率的な匿名暗号化方式を考察し、受信者の ID のプライバシとメッセージの秘匿性を同時に達成する方式を提案した[4]。

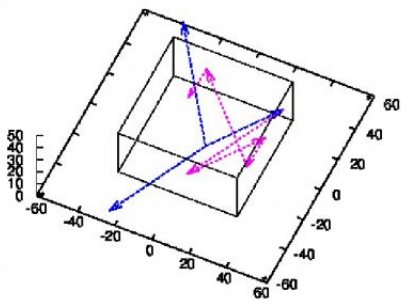

図 2：3 次元の Franke-Kleinjung 格子基底の例

平成 26 年度は、3 次元領域内の全ての格子点を高速に計算できる条件を考察し、基底の向きやサイズを特定することにより 3 次元の格子点を単純な演算により列挙できることを証明した(図 2)。本成果は、平成 26 年 10 月 22 日～24 日に札幌コンベンションセンター

で開催された情報処理学会コンピュータセキュリティシンポジウム CSS2014 において学生論文賞を受賞した。また、昨年度までに研究会や国際会議で発表してきた論文 3 編を、ジャーナル論文化した (IEICE Transactions[5], JSIAM Letters[6,7])。

一方、ペアリングを利用した暗号プロトコルも考察した。階層的な ID ベース暗号において、鍵漏洩攻撃に耐性のある方式を提案した。直交部分空間を用いたデュアルシステム暗号化を拡張することにより、128 ビットセキュリティにおいて 40-70%の漏洩に対して耐性がある方式を提案した[8]。また、匿名性を持つ空間暗号化方式 (Spatial Encryption)を考察した。提案方式は、メッセージ秘守、適応的安全性、受信者匿名性、部分順序代理、短い暗号文などの性質を有する。また、合成数位数のペアリングを利用した方式と、それを用いて素数位数ペアリングベースの方式への変換方法も議論した[9]。

平成 27 年度は、以下の研究を行なった。大きな標数を持つ拡大体上の離散対数問題を高速に解くアルゴリズムとして数体篩法が知られているが、2015 年になり数体篩法の計算量が大幅に改良されてきた。実際、Asiacrypt 2015 において、Barbulescu らは Tower Number Field Sieve (TNFS)を再考し、ペアリング暗号の高速実装で利用される特殊な形の標数 p に対して従来より計算量が低下することを示した。その後、Kim らは標数のサイズが medium となる場合にも計算量が低下する Extended Tower Number Field Sieve (exTNFS)を発表した。本年度は、これらの拡大体に対する数体対篩法の計算量の改良状況をサーベイ論文としてまとめ、2016 年 1 月に熊本で開催された 2016 年暗号と情報セキュリティシンポジウム(SCIS2016)で発表した。また、昨年度までに提案した 3 次元の高速な格子篩法に関する論文を IACR ePrint に投稿した。

一方、ペアリングを利用した暗号プロトコルの研究も進め、漏洩に耐性のある関数型暗号(The Computer Journal [10])、鍵の失効が可能となる ID ベース署名付き暗号化方式 (International Journal of Network Security)などを考察した[11]。

平成 28 年度は、ペアリングフレンドリ曲線 BLS-24, KSS-32, KSS-36, BLS-42, BLS-48 に対して、Kim らの手法に従って 256 ビット安全性を実現するペアリング暗号の鍵長を評価した。ペアリング暗号が 256 ビット安全性を持つためには、およそ 26,000 ビット以上の鍵長が必要であることが判明し、従来 256 ビット安全性に必要とされていた 14,000 ビットの鍵長よりも、10,000 ビット以上大きい値となった。更に、昨年度に IACR ePrint で発表した 3 次元版の Franke-Kleinjung 格子篩法を実装し、通常の線篩法および格子篩法との速度比較を行なった。これらの結果は、2017 年暗号と情報セキュリティシンポジウム SCIS 2017 で 3 件の論文として発表した。一方、ペアリングを利用した暗号プロトコルの研究も進め、鍵の失効が可能となる強偽造不可能な ID ベース署名(Security and Communication Networks [12])、効率的な否認認証暗号方式とその電子メールへの応用 (IEEE Transactions on Information Forensics and Security [13])などを考察した。

	BLS-24	KSS-32	KSS-36	BLS-42	BLS-48
$\mathrm{len}(p^k)$	25,990	27,410	28,280	28,150	27,410

図 3：256 ビット安全性を有するパラメータの鍵長

平成 29 年度は、ペアリング暗号で用いられる楕円曲線のクラス(BLS-24, KSS-32, KSS-36, BLS-42, BLS-48)に対して、256 ビットの安全性を有するパラメータの鍵長を評価した (図 3)。これらの結果は金沢で開催された国際会議 ACNS2017 で発表した[14]。一方、群の代数的演算を用いた代数的群モデルにおいて、ペアリング暗号の安全性根拠となる Diffie-Hellman 問題系と離散対数問題の計算量的関係を考察した。実際、代数的群モデルにおいて、Bilinear Diffie-Hellman 問題と離散対数問題の計算量的等価性を証明し、2018 年電子情報通信学会総合大会において発表した。更に、ペアリング暗号の安全性評価を目的として、有限体の標数が小さい場合の安全性に関して議論を行なった。特に、関数体篩法とその改良による解読世界記録に関するサーベイ論文を、電子情報通信学会論文誌で発表した[15]。

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 15 件）

[1] Kenichiro Hayasaka, Kazumaro Aoki, Tetsutaro Kobayashi, Tsuyoshi Takagi, “An Experiment of Number Field Sieve for Discrete Logarithm Problem over GF(p^{12})”, Number Theory and Cryptography, LNCS 8260, pp.108-120, 2013.
DOI: 10.1007/978-3-642-42001-6_8

[2] Yutaro Kiyomura, Tsuyoshi Takagi, “Efficient Algorithm for Tate Pairing of Composite Order”, The 8th International Workshop on Security, IWSEC 2013, LNCS 8231, pp.01-216, 2013.
DOI: 10.1007/978-3-642-41383-4_13

[3] Fagen Li, Tsuyoshi Takagi, “Secure Identity-Based Signcryption in the Standard Model”, Mathematical and

Computer Modelling, Vol.57, No.11-12, pp. 2685-2694, 2013.
DOI: 10.1016/j.mcm.2011.06.043
[4] Mingwu Zhang, Tsuyoshi Takagi, “Efficient Constructions of Anonymous Multireceiver Encryption Protocol and Their Deployment in Group E-mail Systems With Privacy Preservation”, IEEE Systems Journal, Vol.7, No.3, pp.410-419, 2013.
DOI: 10.1109/JSYST.2012.2221893
[5] Kenichiro Hayasaka, Kazumaro Aoki, Tetsutaro Kobayashi, Tsuyoshi Takagi, “An experiment of number field sieve for discrete logarithm problem over GF(p^n)”, JSIAM Letters, Vol.6, pp.53-56, 2014.
DOI: 10.14495/jsiaml.6.53
[6] Yutaro Kiyomura, Tsuyoshi Takagi, “Efficient Algorithm for Tate Pairing of Composite Order2014”, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol.97-A, No.10, pp.2055-2063, 2014.
DOI: 10.1587/transfun.E97.A.2055
[7] Takumi Tomita, Tsuyoshi Takagi, “Efficient System Parameters for Identity-Based Encryption using Super-singular Elliptic Curves”, JSIAM Letters, Vol.6, pp.13-16, 2014.
DOI: 10.14495/jsiaml.6.13
[8] Mingwu Zhang, Bo Yang, Chunzhi Wang, Tsuyoshi Takagi, “Unbounded anonymous hierarchical IBE with continual-key-leakage tolerance”, Security and Communication Networks, Vol.7, pp.1974-1987, 2014.
DOI: 10.1002/sec.912
[9] Mingwu Zhanga, Bo Yang, Tsuyoshi Takagi, “Anonymous spatial encryption under affine space delegation functionality with full security”, Information Sciences, Vol. 277, pp.715-730, 2014.
DOI: 10.1016/j.ins.2014.03.012
[10] Mingwu Zhang, Chunzhi Wang, Tsuyoshi Takagi, Yi Mu, “Functional Encryption Resilient to Hard-to-Invert Leakage”, The Computer Journal, Vol.58, No.4, pp. 735-749, 2015.
DOI: 10.1093/comjnl/bxt105
[11] Xiangsong Zhang, Zhenhua Liu, Yupu Hu, Tsuyoshi Takagi, “Revocable Identity-based Signcryption Scheme Without Random Oracles”, International Journal of Network Security, Vol.17, No.2, pp.110-122, 2015.
http://ijns.femto.com.tw/contents/ijns-v17-n2/ijns-2015-v17-n2-p110-122.pdf
[12] Zhenhua Liu, Xiangsong Zhang, Yupu Hu, and Tsuyoshi Takagi, “Revocable and Strongly Unforgeable Identity-based Signature Scheme in the Standard Model”, Security and Communication Networks, Vol.9, No.14, pp.477-2486, 2016.
DOI: 10.1002/sec.1513
[13] Fagen Li, Di Zhong, and Tsuyoshi Takagi, “Efficient Deniably Authenticated Encryption and Its Application to E-Mail”, IEEE Transactions on Information Forensics and Security, Vol.11, No.11, pp. 2477-2486, 2016.
DOI:10.1109/TIFS.2016.2585086
[14] 高木剛, 下山武司, 篠原直行, 林卓也, "ペアリング暗号解読の世界記録とその安全性評価", 電子情報通信学会論文誌, Vol.J100-B, No.9, pp.582-592, 2017.
DOI:10.14923/transcomj.2016SHI0003
[15] Yutaro Kiyomura, Akiko Inoue, Yuto Kawahara, Masaya Yasuda, Tsuyoshi Takagi, Tetsutaro Kobayashi, "Secure and Efficient Pairing at 256-bit Security Level", The 15th International Conference on Applied Cryptography and Network Security, ACNS 2017, LNCS 10355, pp.59-79, 2017.
DOI: 10.1007/978-3-319-61204-1_4

〔学会発表〕（計 12 件）

① 早坂健一郎, 青木和麻呂, 小林鉄太郎, 高木剛, “3 次元格子篩において用いられる格子点計算法の評価”, コンピュータセキュリティシンポジウムCSS2014, 平成 26 年 10 月 22 日, 札幌コンベンションセンター.
② Tsuyoshi Takagi, “A thrilling encounter with Johannes Buchmann”, A conference in honour of Johannes Buchmann's 60th birthday, 招待講演, 2014 年 11 月 22 日、Darmstadt, Germany.
③ 高木剛, “格子問題の困難性評価”, 電子情報通信学会 2015 年総合大会, 招待講演, 2015 年 3 月 10 日, 立命館大学.
④ 高木剛, “公開鍵暗号の安全性評価”, 最適モデリングセミナー, 招待講演, 2014 年 11 月 25 日, 東京大学本郷キャンパス.
⑤ 高木剛, “インターネットは安全？-数学と暗号の不思議な関係”, 数学・数理科学４研究拠点合同市民講演会, 万物共通の言葉「数学」, 招待講演, 2015 年 12 月 12 日, 明治大学中野キャンパス.
⑥ 井上明子, 林卓也, 高木剛, “拡大体上の離散対数問題に対する数体篩法について”, 2016 年暗号と情報セキュリティシンポジウム SCIS 2106, 2016 年 1 月 20 日, ANA クラウンプラザホテル熊本ニュースカイ.
⑦ 井上明子, 安田雅哉, 高木剛, 清村優太郎, 川原祐人, 小林鉄太郎, “256 ビット安全性を持つペアリング暗号の鍵長見積もり”, 2017 年暗号と情報セキュリティシンポジウム SCIS2017, 2017 年 1 月 24 日, ロワジールホテル那覇.
⑧ 清村優太郎, 川原祐人, 小林鉄太郎, 井上明子, 安田雅哉, 高木剛, “ペアリング

暗号を効率的に実装可能な 256 ビット安全性を持つペアリングフレンドリ曲線”，2017 年暗号と情報セキュリティシンポジウム SCIS2017，2017 年 1 月 24 日，ロワジールホテル那覇．

⑨ Wang Kun，林 卓也，高木 剛，“A Comparison of Three-Dimensional Sieve Methods for Number Field Sieve over GF(p^6)”，2017 年暗号と情報セキュリティシンポジウム SCIS2017，2017 年 1 月 26 日，ロワジールホテル那覇．

⑩ Tsuyoshi Takagi，“Security Evaluation of Post-Quantum Cryptography”，ChinaCrypt 2016，招待講演，2016 年 9 月 22 日，Hangzhou Institute of Technology，China．

⑪ 高木剛，“暗号の安全性はどのように評価するか？”，Computer Entertainment Developers Conference，CEDEC 2016，招待講演，2016 年 8 月 25 日，横浜パシフィコ．

⑫ 水出大河，高安敦，高木剛，“代数的群モデルにおける双線型 Diffie-Hellman 問題の困難性証明”，2018 年電子情報通信学会総合大会，2018 年 3 月 22 日，東京電機大学．

〔その他〕
ホームページ等
東京大学大学院情報理工学系研究科
数理情報第 1 研究室(高木研究室)
http://crypto.mist.i.u-tokyo.ac.jp/

６．研究組織

(1)研究代表者
高木 剛（TAKAGI TSUYOSHI）
東京大学・大学院情報理工学系研究科・教授
研究者番号：60404802

(2)研究分担者
安田 貴徳（YASUDA TAKANORI）
岡山理科大学・工学部・准教授
研究者番号：00464602