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 ２７ 年　 ６ 月　 ４ 日現在

機関番号：１３３０２
研究種目：挑戦的萌芽研究
研究期間：2011～2014
課題番号：２３６５０００６

研究課題名（和文）楕円曲線上の離散対数問題の安全性に関する研究

研究課題名（英文）Study on the security of elliptic curve discrete logarithm problems

研究代表者
宮地　充子（Miyaji, Atsuko）

北陸先端科学技術大学院大学・情報科学研究科・教授

研究者番号：１０３１３７０１

交付決定額（研究期間全体）：（直接経費）　　2,900,000円

研究成果の概要（和文）：楕円曲線上の離散対数問題（ECDLP)は利用する楕円曲線E/F(p)により安全性が異なるため，安全性を何らかの手法で評価できることが望ましい．E/F(p)上のECDLPはE/F(p)から有限体F(p)の拡大体上のF(p＾k)上への写像により，有限体上の離散対数問題(DLP)へ帰着する．この結果E/F(p)上のECDLPが拡大体F(p＾k) 上のDLPと等価の安全性となる．本研究では，超楕円曲線上のHittによるアプローチを楕円曲線上に応用し，楕円曲線の元の個数に新たなパラメータr, L を導入し，このパラメータで楕円曲線E/F(p)のトレースと元の個数，拡大次数を記述することに成功した．

研究成果の概要（英文）：An elliptic curve cryptosystem is based on elliptic curve discrete logarithm problem (ECDLP).An elliptic curve is uniquely determined by mathematical parameters such as j-invariant, trace, etc.The security of ECDLP is different from each elliptic curve, and there exist some ECDLP whose security is extremely low compared with others.This is why it is very important to find relation between mathematical parameters of elliptic curve and security level of ECDLP.However, only a few elliptic curves can explicitly give their security level by using their mathematical parameters.Recently, Hitt proves relations between security level and mathematical parameters of hyper elliptic curve.Hirasawa and Miyaji applied Hitt's approach to ECDLP and presented new relations between mathematical parameters and embedding degrees.In this research, we further extended their conditions and found new explicit relations between elliptic-curve parameters and embedding degrees.

研究分野：情報セキュリティ

キーワード：暗号・認証等　楕円曲線暗号　安全性評価

１．研究開始当初の背景

楕円曲線上の離散対数問題（ECDLP)は利用する楕円曲線 E/F(p)により安全性が異なるため，安全性を何らかの手法で評価できることが望ましい．楕円曲線 E/F(p)上の ECDLP の安全性を評価する方法が 楕円曲線 E/F(p)を有限体 F(p)の拡大体上の F(p＾k)上への写像により，有限体上の離散対数問題(DLP)へ帰着する方法であり，この結果 E/F(p)上の ECDLP が F(p)の拡大体上の F(p＾k)の DLP と等価の安全性となる．この拡大次数 k が現状利用可能な安全性の指標となる．

しかしながら，拡大次数 k と楕円曲線 E/F(p)のパラメータであるトレース t ，元の個数＃E(Fp) = h・l（l が安全性に関与する素数）などとの関係が明らかになる楕円曲線は限られており，例えば埋め込み次数 k が 6 以下では研究者が提案した MNT 曲線に限定されることがわかっている．

２．研究の目的

本研究は楕円曲線上の離散対数問題(ECDLP) の安全性の指標となる埋め込み次数を数学的な性質であるトレースなどを用いて明示的に記述することを目的とする．

３．研究の方法

本研究では，超楕円曲線上の Hitt によるアプローチを楕円曲線上に応用し，楕円曲線の元の個数に新たなパラメータを導入することで，埋め込み次数と楕円曲線の元の個数との関係を明らかにした．

４．研究成果

本研究では，超楕円曲線上の Hitt によるアプローチを楕円曲線上に応用し，楕円曲線の元の個数に新たなパラメータを導入することで，埋め込み次数と楕円曲線の元の個数との関係を明らかにした．具体的には，#E(Fp) = h・l とするとき，①L=qη(q は素数，η は奇数)とし，l=((t-1)＾(L2＾r+1)/λ((t-1)＾(η2＾r)+1)かつ(t-1)≠ 0 かつ(t-1)＾(η2＾r)≠-1 (mod l)となるときに，拡大次数 k = 2＾(r+1)L となること，②L=2β(β≧2)，l=((t-1)＾(β2＾r+1)/λかつ(t-1)≠ 0，かつ以下いずれかの条件を満たす時

- t>1 かつλ>0
- t<1 かつβが偶数でλ>0
- t<1 かつ r>0 でλ>0
- t<1 かつ r=0 でλ<0

に拡大次数 k = 2＾rL となることを示した．本研究の主要なアイデアは新たなパラメータ r，L を導入し，この共通のパラメータで楕円曲線 E/F(p)のトレースと元の個数と安全性の指標となる拡大次数を表したことにある．右表は本成果で判明した楕円曲線の候補数である．また，以下に Hitt の結果との比較表を示す．

k	r	L	#curves
6	0	3	17138
8	1	4	41640
10	0	5	22916
12	1	3	72974
14	0	7	34185
16	1	8	33261
18	0	9	32490
20	1	5	54842
22	0	11	56300
24	2	3	121913
26	0	13	170618
28	1	7	169781

	Hitt	本成果
種数	2	1
標数 q	2^m	p^m
#Jc(F2^m)，#E(Fp^m)の最大素因子	2^(L2^r)+1/(2^2^r+1)	(t-1)＾(L2＾r+1)/λ((t-1)＾(η2＾r)+1)
トレース t	-1,2^m+2^(2^m+2^(2m-L2^r))	|t|≦q^(1/((L-1)2^r))
ρ-value	4L/(3(L-1))≦ρ≦2-2/(2^r(L-1))	1

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 32 件）

1. Atsuko Miyaji and Kazumasa Omote, Self-healing Wireless Sensor Networks, Concurrency and Computation: Practice and Experience, 査読有, 2015, DOI: 10.1002/cpe.3434

2. Ryoma Ito, and Atsuko Miyaji, How TKIP downgrades security of generic RC4, The 20th Australasian Conference on Information Security and Privacy (ACISP 2015), Lecture Notes in Computer Science, Springer-Verlag, 査読有, 2015, 印刷中.

3. Ryoma Ito, and Atsuko Miyaji, New Linear Correlations related to State Information of RC4 PRGA using Ⅳ in WPA, The 22nd International Workshop on Fast Software Encryption (FSE 2015), Lecture Notes in Computer Science, Springer-Verlag, 査読有, 2015, 印刷中.

4. Atsuko Miyaji and Mazumder Rashed,

A new (n, 2n) Double Block Length Hash Function based on Single Key Scheduling, The 29th IEEE International Conference on Advanced Information Networking and Applications (AINA2015), IEEE, **査読有**, 2015, pp.546-570.

5. Jiageng Chen, Shoichi Hirose, Hidenori Kuwakado, and Atsuko Miyaji, A Collision Attack on a Double-Block-Length Compression Function Instantiated with Round-Reduced AES-256, The 17th International Conference on Information and Security Cryptology, ICISC 2014, , Lecture Notes in Computer Science, Springer-Verlag, **査読有**, 8949, 2015, pp.271-285.

6. Atsuko Miyaji and Mazumder Rashed, A new (n; n) blockcipher hash function using Feistel Network: Apposite for RFID Security, International Conference on Computational Intelligence in Data Mining (ICCIDM 2014), Lecture Notes in Computer Science, Springer-Verlag, **査読有**, Volume 33, 2015, pp.519-528.

7. Ryoma Ito, and Atsuko Miyaji, New Integrated Long-Term Glimpse of RC4, The 15th International Workshop on Information Security Applications (WISA 2014), Lecture Notes in Computer Science, Springer-Verlag, **査読有**, 8909, 2015, pp.137-149.

8. Jiageng Chen, Keita Emura, and Atsuko Miyaji, SKENO: Secret Key Encryption with Non-interactive Opening, Journal of Mathematical Cryptology, **査読有**, 2014, DOI: 10.1515/jmc-2014-0010

9. Keita Emura, Atsuko Miyaji, Mohammad Shahriar Rahman, and Kazumasa Omote, Generic Constructions of Secure-Channel Free Searchable Encryption with Adaptive Security, Wiley Security and Communication Networks, **査読有**, 2014, DOI: 10.1002/sec.1103

10. **宮地充子**, **ユビキタスネットワークにおけるセキュリティ技術－ 積極的利用を促すセキュリティ技術－**, **「電気評論」**, **査読有**, **夏季増刊号特集**, 2014, pp.12-15.

11. Atsuko Miyaji, Mazumder Rashed and Tsuyoshi Sawada, A new (n; n) Blockcipher based Hash Function for Short Messages, 2014 Ninth Asia Joint Conference on Information Security (ASIA JCIS), IEEE, **査読有**, 2014, pp.56-63.

12. Jiageng Chen, Atsuko Miyaji, and Chunhua Su, A Provable Secure Batch Authentication Scheme for EPCGen2 Tags, The 8th International Conference on Provable Security (Provsec 2014), Lecture Notes in Computer Science, Springer-Verlag, **査読有**, 8782, 2014, pp.103-116.

13. Jiageng Chen, Yuichi Futa, Atsuko Miyaji, and Chunhua Su, Improving impossible differential cryptanalysiswith concrete investigation of key schedulingalgorithm and its application to LBlock, The 8th International Conference on Network and System Security (NSS 2014) , Lecture Notes in Computer Science, Springer-Verlag, **査読有**, 8792, 2014, pp.184-197.

14. Mohammad Saiful Islam Mamun and Atsuko Miyaji, Secure VANET Applications with a rened Group Signature, 2014 Twelfth Annual International Conference on Privacy, Security and Trust (PST), **査読有**, 2014, pp.199-206.

15. Mohammad Saiful Islam Mamun, Atsuko Miyaji, and Hiroaki Takada, A multi-purpose Group Signature for Vehicular Network Security, 2014 17th International Conference on Network-Based Information Systems (NBiS), **査読有**, 2014, pp.511-516.

16. Cheng-Qiang Huangy, Atsuko Miyaji, Long-Hai Li, and Shang-Mei Xu, POND: A Novel Protocol for Network Coding based on Hybrid Cryptographic Scheme, 2014 IEEE International Conference on Computer and Information Technology (CIT), **査読有**, 2014, pp.373-380.

17. Jiageng Chen, Atsuko Miyaji, and Chunhua Su, Distributed Pseudo-Random Number Generation and its application to Cloud Database,

The 10th Information Security Practice and Experience Conference(ISPEC 2014) , Lecture Notes in Computer Science, Springer-Verlag, **査読有**, 8434、2014, pp.373-387.

18. Mohammad Saiful Islam Mamun and Atsuko Miyaji, A Scalable and Secure RFID Ownership Transfer Protocol, The 28th IEEE International Conference on Advanced Information Networking and Applications (AINA 2014), IEEE, **査読有**, 2014, pp.343-350.

19. Mohammad Saiful Islam Mamun and Atsuko Miyaji, RFID Path Authentication, Revisited, The 28th IEEE International Conference on Advanced Information Networking and Applications (AINA2014), IEEE, **査読有**, 2014, pp.245-252.

20. Jiageng Chen and Atsuko Miyaji, Differential Cryptanalysis and Boomerang Cryptanalysis of LBlock, Security Engineering and Intelligence Informatics, CD-ARES 2013 Workshops, Lecture Notes in Computer Science, Springer-Verlag, **査読有**, 8128, 2013, pp.1-5.

21. Mohammad Saiful Islam Mamun and Atsuko Miyaji, A fully-secure RFID authentication protocol from exact LPN assumption, The 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom'13), IEEE, **査読有**, 2013, pp.102-109.

22. Keita Emura, Atsuko Miyaji and Mohammad Shahriar Rahman, Private Multiparty Set Intersection Protocol in Rational Model, The 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom'13), IEEE, **査読有**, 2013, pp.431-438.

23. Keita Emura, Atsuko Miyaji, and Mohammad Shahriar Rahman, Dynamic Attribute-based Signcryption without RandomOracles, International Journal of Applied Cryptography (IJACT), **査読有**, 2(3), 2012, pp.199-211.

24. Jiageng Chen and Atsuko Miyaji, Cryptanalysis of Stream Ciphers From a New Aspect: How to Apply Key Collisions to Key Recovery Attack, IEICE Trans., Fundamentals, **査読有**, E95-A(12), 2012, 2148-2159.

25. Tomoyuki Karasawa, Masakazu Soshi and Atsuko Miyaji, A Novel Hybrid IP Traceback Scheme with Packet Counters, The 5th International Conference on Internet and Dsitributed Computing Systems, IDCS 2012, Lecture Notes in Computer Science, Springer-Verlag, **査読有**, 7646, 2012, pp.71-84.

26. Atsuko Miyaji and Yiren Mo, How to Enhance the Security on the Least Significant Bit, The 4th International Symposium on Cyberspace Safety and Security , CANS 2012, Springer-Verlag, **査読有**, 7712, 2012, pp.263-279.

27. Atsuko Miyaji and Phuong V.X. TRAN, Constant-Ciphertext-Size Dual Policy Attribute Based Encryption, The 11th International Conference on Cryptology and Network Security, CSS 2012, Springer-Verlag, **査読有**, 7672, 2012, pp.400-413.

28. Mohammad S. I. Mamun and Atsuko Miyaji, An Optimized Signature Verification System for Vehicle Ad hoc NETwork, The 8th International Conference on Wireless Communications, Networking and Mobile Computing, WiCOM2012, IEEE, **査読有**, 2012, pp.1-8.

29. Mohammad S. I. Mamun and Atsuko Miyaji, A Secure and private RFID authentication protocol under SLPN problem, The 6th International Conference on Network and System Security NSS 2012, Springer-Verlag, **査読有**, 7645, 2012, pp.476-489.

30. Kazuya Izawa, Atsuko Miyaji, and Kazumasa Omote, Lightweight Integrity for XOR Network Coding in Wireless Sensor Networks, The 8th International Conference on Information Security Practice and Experience, ISPEC 2012, Lecture Notes in Computer Science, **査読有**,

7232, 2012, pp.245-258.

31. Raveen R. Goundar, Marc Joye, Atsuko Miyaji, Matthieu Rivain, andAlexandre Venelli, Scalar Multiplication on Weierstrass Elliptic Curves from Co-Z Arithmetic, Journal of Cryptographic Engineering (2011),Springer-Verlag, **査読有**, Vol. 1, 2011, pp.161-176.

32. Shoujirou Hirasawa and Atsuko Miyaji, New Concrete Relation between Trace, Definition Field, and Embedding Degree, IEICE Trans., Fundamentals, **査読有**, E94-A, 2011, pp. 1368-1374.

〔図書〕（計 1 件）

① 宮地充子，日本評論社，代数学から学ぶ暗号理論，2012，228 ページ．

〔その他〕

ホームページ等

６．研究組織

(1)研究代表者

宮地 充子(MIYAJI，Atsuko)
北陸先端科学技術大学院大学・情報科学研究科・教授
研究者番号：１０３１３７０１