2011 2014

Study on the security of elliptic curve discrete logarithm problem

Miyaji, Atsuko

2,900,000

(ECDLP)
E/F(p)   E/F(p)
E/F(p)   ECDLP E/F(p)   ECDLP E/F(p)   F(p)   F(p k)
(DLP)   E/F(p)   ECDLP   F(p k)   DLP
Htt
r, L   E/F(p)

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, Htt proves relations between security level and mathematical parameters of hyper elliptic curve. Hrasawa and Miyaji applied Htt'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.

(ECDLP)

E/F(p)

E/F(p)   ECDLP
E/F(p)
F(p)   F(p k)
(DLP)
E/F(p)
ECDLP F(p)   F(p k) DLP
k

k   E/F(p)
t

$E(Fp) = h \cdot l$ l   )

k   6
MNT

(ECDLP)

Htt

	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

	Htt	
	2	1
q	2^m	p^m
#Jc(F2^m), #E(Fp^m)	$2^{(L2^r)}+1/(2^{2^r}+1)$	$(t-1)(L2r+1)/((t-1)(2r)+1)$
t	$-1, 2^m 2^{(2^m-2^{(2m L2^r)})}$	$\lvert t \rvert$ $q^{(1/((L-1)2^r))}$
-value	$4L/(3(L-1))$ $2-2/(2^r(L-1))$	1

Htt

E(Fp)
$= h \cdot l$ $L=q$ (q
) $l=((t-1)(L2 r+1)/((t-1)(2 r)+1)$ (t-1) 0   (t-1)
(2 r) -1 (mod l)
k = 2 (r+1)L   L=2 (
2) l=((t-1)(2 r+1)/   (t-1) 0

● t>1   >0
● t<1   >0
● t<1   r>0   >0
● t<1   r=0   <0
k = 2 rL

r, L
E/F(p)

Htt
.

32

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

2. Ryoma Ito, and <u>Atsuko Miyaji</u>, 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,   , 2015,   .

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

4. <u>Atsuko Miyaji</u> 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, , 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, , 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, , 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, , 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, , 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, , 2014, DOI: 10.1002/sec.1103

10. _____,

, ,
, , 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, , 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, , 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, , 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), , 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), , 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), , 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, , 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, , 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, , 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, , 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, , 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, , 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), , 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, , 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, , 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, , 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, , 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, , 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, , 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, ,

7232, 2012, pp.245-258.

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

32. Shoujirou Hirasawa and <u>Atsuko Miyaji</u>, New Concrete Relation between Trace, Definition Field, and Embedding Degree, IEICE Trans., Fundamentals, , E94-A, 2011, pp. 1368-1374.

1

─────── ,   ,
, 2012, 228   .

(1)

(MIYAJI, Atsuko)