4-6 Solving a Discrete Logarithm Problem via Function Field Sieve (FFS)

SHINOHARA Naoyuki, WANG Lihua, and MATSUO Shin'ichiro

Pairings is used to construct many cryptographic systems for which no other efficient implementation is known, such as identity based encryption. Especially, the η_T-paring on supersingular curves over a finite field $GF(3^n)$ is efficiently implementable. The security of cryptosystems using such η_T-parings is based on the difficulty to solve Discrete Logarithm Problem (DLP) in $GF(3^n)$. Therefore, in the collaborative research of National Institute of Information and Communications Technology (NICT) and Future University-Hakodate, we successfully set a new record for solving the DLP in $GF(3^{6\cdot 71})$ of 676-bit size. In this paper, we remark about the collaborative research.

Keywords
Finite field, Discrete Logarithm Problem (DLP), Index calculus method, Function Field Sieve (FFS)

1 Preface

In the current information systems, an increasing amount of confidential information is used, e.g. for online shopping or Internet banking. In addition, various cryptographic technologies are used for the current information systems in terms of information security. Therefore, the assessment of cryptographic technology to constantly ensure security against progress of deciphering ability of malicious attackers is required. The important role in this assessment is to ensure that the calculation of the mathematical problem which cryptographic technology is based on is difficult using the capabilities of current computers, or even those of future potential computers.

Recently, pairing based cryptosystems, used to construct many cryptosystems for which no other efficient implementation for the traditional public key encryption is known, such as identity based encryption, are actively researched. As pairing based cryptosystems are based on the difficulty to solve the Discrete Logarithm Problem (DLP) in a finite field, verification and assessment of computable bit count are required to accurately assess security.

Especially, the η_T-pairing on supersingular curves over a finite field $GF(3^n)$ is known to be efficiently implementable. Although the security of cryptosystems using such η_T-pairings is based on the difficulty to solve the Discrete Logarithm Problem (DLP) in $GF(3^n)$, few computational experiments related to the Discrete Logarithm Problem (DLP) in $GF(3^n)$ have been reported.

In April 2009, National Institute of Information and Communications Technology (NICT) and Future University-Hakodate started the collaborative research on the security of cryptosystems using such η_T-pairings, i.e. effective solution of the Discrete Logarithm Problem (DLP) in $GF(3^n)$. As a result, they succeeded in calculating a discrete logarithm in $GF(3^{6\cdot 71})$. This means that the Discrete Logarithm Problem (DLP) in a finite field of 676 bit length was solved. This result can be a technical base for estimating secure key size when adopting pairing based cryptosystems.

Various groups in the world have traditionally challenged the calculation of the Discrete Logarithm Problem (DLP) in a finite field. Regarding key groups which consist of a group from mathematics research institute of The University of Bonn in Germany, Department of Defense of France, a group from Rennes mathematics research institute, National Institute of Information and Communications Technology (NICT), and Future University-Hakodate, bit counts for which calculations have succeeded can be compared as Fig. 1 below.

The composition of this paper is as follows. Firstly, the Discrete Logarithm Problem (DLP) in a finite field is described in **2**. Secondly, Function Field Sieve (FFS) is described as an effective solution of the Discrete Logarithm Problem (DLP) in a finite field. The solution was also used in the collaborative research of National Institute of Information and Communications Technology (NICT) and Future University-Hakodate. As Function Field Sieve (FFS) is one of the index calculus methods, the index calculus method is described in **3**. In **4**, an overview of reference [15], i.e. the Function Field Sieve (FFS) which was used to solve the Discrete Logarithm Problem (DLP) in a finite field of 676 bit length is described. In addition, key points of ingenuity and calculation results are stated in **5**, and the feelings with regard to the collaborative research are summarized in **6**.

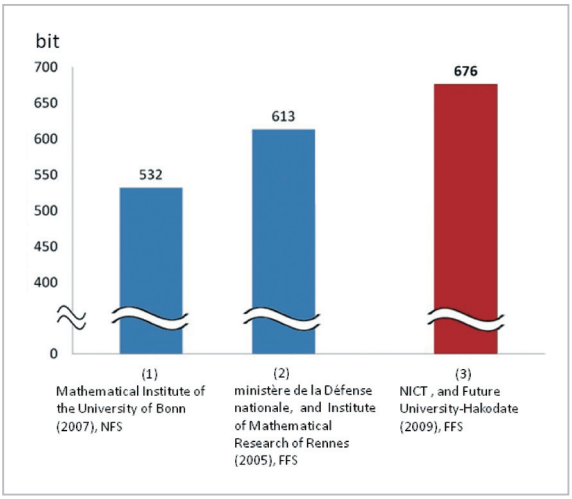

Fig.1 Current records

2 The Discrete Logarithm Problem (DLP) in a finite field

Firstly, the Discrete Logarithm Problem (DLP) in a finite field is described. The reduced residue class group of $GF(p^n)$, where p is characteristic and n is degree of field extension, is a cyclic group. Thus, a generator $g \in GF(p^n)^*$ exists and $GF(p^n)^* = < g >$ holds. Provided that:

$$< g > = \{g, g^2, ..., g^{p^n-1}(=1)\}$$

the "Discrete Logarithm Problem (DLP) in a finite field" is a problem asking to "find the integer number $e \in [1, p^n-1]$ which satisfies $X = g^e$ against given $X \in GF(p^n)^*$ and generator g." As the progression $\{g, g^2, ..., g^{p^n-1}\}$ acts like a random number sequence, its solution is difficult. The degree of calculation required for a Function Field Sieve (FFS) which is one of the actual effective methods is $L_{p^n}[1/3, c]$ where the constant number c exists.

Example 1)

$$GF(3^2)^* = (GF(3)[x]/(x^2+1))^*$$
$$= \{1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2\}$$

Where $x+1$ is generator. Given that $g = x+1$,

$$\{g, g^2, ..., g^8\} = \{x+1, 2x, 2x+1, 2, 2x+2, x, x+2, 1\}$$

holds.

Given that the defining polynomial of the quadratic extension field is x^2+1 and generator is $x+1$, the discrete logarithm $\log_{x+1}(2x+2)$ of $2x+2$ are 5. As the cycle of $GF(3^2)^*$ is 8, this means that the Discrete Logarithm Problem (DLP) of 4 bits has been solved.

In this paper, the solution of the Discrete Logarithm Problem (DLP) for $GF(3^{6\cdot71})$, i.e. the Discrete Logarithm Problem (DLP) of 676 bits is mainly discussed.

3 Index calculus method

One of the index calculus methods, a Function Field Sieve (FFS), is a method to solve the Discrete Logarithm Problem (DLP) effectively. Thus, the index calculus method is described in this section. Additionally, in this section,

let the finite field be a prime field $GF(p)$ of characteristic p which is an easier field and not required to be denoted by a polynomial ring. Therefore, the Discrete Logarithm Problem (DLP) is given by the following equation giving that g is generator $X \in GF(p)^*$:

$$g^e \equiv X \pmod{p}$$

3.1 Policy of index calculus method

Policy of index calculus method is described. As for $X \in GF(p)^*$, X can be considered to be an integer number. So, we assume that X is factorized into the product of prime number ρ_i which is not over an integer number B, and the prime factorization is known:

$$X = \prod_{\rho_i \le B} \rho_i^{e_i}$$

An integer number whose prime divisors are not over B is called a B-smooth integer number. In addition, we also assume a discrete logarithm z_i of each prime number ρ_i which is not over B, i.e. an integer number $0 \le z_i \le p-1$ which satisfies $\rho_i \equiv g^{z_i} \bmod p$ is known. This leads to

$$X = \prod_{\rho_i \le B} \rho_i^{e_i} \equiv \prod_{\rho_i \le B} g^{z_i e_i} \equiv g^{\sum_{\rho_i \le B} z_i e_i} \pmod{p}$$

and

$$e \equiv \sum_{\rho_i \le B} z_i e_i \pmod{(p-1)}$$

holds against discrete logarithm e of X. As e_i, z_i is known, e is given.

As stated earlier, there are two assumptions for the index calculus method. The first assumption that X is B-smooth can be solved by transforming the Discrete Logarithm Problem (DLP), i.e. given that $X' = g^a X \pmod{p}$ is B-smooth against an integer number g^a which is randomly generated, the discrete logarithm $a+e$ of X' can be obtained by the index calculus method, and e can be obtained as a is known. Another assumption is that the discrete logarithm of the factor base is known, and its calculus method will be described in **3.2**.

3.2 Calculus method of discrete logarithm of factor base

The calculation of the discrete logarithm of the factor base is a relation exploration and simultaneous linear congruence equations which are given by the relation exploration. Firstly, the relation exploration is described.

In the relation exploration, an integer number $g^{a_j} \pmod{p}$ is generated randomly and what is to be B-smooth is collected. Note that

$$g^{a_j} = \prod_{\rho_i \le B} \rho_i^{e_{i,j}} \equiv \prod_{\rho_i \le B} g^{z_i e_{i,j}} \equiv g^{\sum_{\rho_i \le B} z_i e_{i,j}} \pmod{p}$$

holds, and by this relation, the congruence equation

$$a_j \equiv \sum_{\rho_i \le B} e_{i,j} z_i \pmod{p-1}$$

is given. As $a_j, e_{i,j}$ is known, the discrete logarithm of factor base z_i can be obtained by solving simultaneous linear congruence equations to be configured.

3.3 Outline of index calculus method

In this section, algorithms of index calculus method are organized.

Parameter selection phase: Set parameter B so that the overall calculation cost is minimized.
(For the Function Field Sieve (FFS) in the next section, this applies to the polynomial selection phase.)

Relation exploration phase: Generate an integer number $g^{a_j} \pmod{p}$ randomly, collect those that are B-smooth, and generate a sufficient number of the following congruence equations:

$$a_j \equiv \sum_{\rho_i \le B} e_{i,j} z_i \pmod{p-1}$$

Linear algebra phase: Find the discrete logarithm of all factor bases by solving simultaneous congruence equations.

Discrete logarithm calculation phase: Generate an integer number g^a randomly against a given integer number X, and find what leads $X' = g^a X \pmod{p}$ to be B-smooth. Calculate the discrete logarithm of X using the discrete logarithm of the factor base and a.

4 Function Field Sieve (FFS)

In this section, an overview of the Function Field Sieve (FFS) is described (see reference [15] for more information). This method consists of four phases, i.e. polynomial selection phase (parameter selection phase), relation exploration phase, linear algebra phase, and discrete logarithm calculation phase. Let a given finite field have a form of $GF(3^{6\cdot n})$. In addition, let g be a generator of reduced residue class groups, and consider finding the discrete logarithm $\log_g X$ of $X \in < g >$.

Polynomial selection phase: At this phase, parameter values $d_H, \deg m, B, R, S$ related to the calculation cost of the Function Field Sieve (FFS) which is described below is determined. Thus, we evaluate the later total calculation amount and calculate $d_H, \deg m, B, R, S$ to minimize the value.

Next, select an n^{th}-order polynomial $f(x)$ which is irreducible and monic in $GF(3^6)$. Note that a finite field $GF(3^{6\cdot n})$ can be denoted by $GF(3^6)[x]/(f)$. Then, find a 2-variable polynomial $H(x,y) \in GF(3^6)[x,y]$ which satisfies the eight conditions in [1]. In fact, a form of

$$H(x,y) = x + y^{d_H}$$

was selected. Note that a surjective homomorphism

$$\begin{aligned} \Phi : GF(3^6)[x,y]/(H) &\to GF(3^{6n}) \cong GF(3^6)[x]/(f) \\ y &\mapsto m \end{aligned}$$

exists. However, let $m \in GF(3^6)[x]$ satisfy both $H(x,m) \equiv 0 \bmod f$ and $\deg m \cdot d_H \geq n$. Next, select a smoothness bound B and select the factor base $F_R(B)$ of the rational side and the factor base $F_A(B)$ of the algebra side as follows:

$$\begin{aligned} F_R(B) = \{&\rho \in GF(3^6)[x] \mid \deg(\rho) \leq B, \\ &\rho \text{ is irreducible}\} \end{aligned}$$

$$\begin{aligned} F_A(B) = \{&< \rho, y - t > \in Div(GF(3^6)[x,y]/(H)) \mid \\ &\rho \in F_R(B),\ t \equiv m \bmod \rho\} \end{aligned}$$

However, let $Div(GF(3^6)[x,y]/(H))$ be a factor group of $GF(3^6)[x,y]/(H)$.

Relation exploration phase: At this phase, generate the congruence equation which is required to obtain the discrete logarithm of the factor base in the index calculus method.

Find the values of $F(\geq \#F_R(B) + \#F_A(B))$ of a pair (r,s) which satisfies the following conditions, and where r and s are prime numbers respectively, against $r, s \in GF(3^6)[x]$ whose order is not over B:

$$\begin{aligned} &\deg r \leq R,\ \deg s \leq S, \\ &rm + s = \prod_{\rho_i \in F_R(B)} \rho_i^{a_i} \\ &(-r)^{d_H} H(x, -s/r) = \prod_{<\rho_j, t_j> \in F_A(B)} \rho_j^{b_j} \end{aligned}$$

However, t_j is uniquely determined by ρ_j, r, s, and let r be monic. In other words, find a pair (r,s) which enables $rm+s, (-r)^{d_H} H(x, -s/r)$ to be factorized into a prime divisor which is not over B. Such (r,s) is called double B-smooth. Note that the following relation holds:

$$\sum_{\rho_i \in F_R(B)} a_i \log_g \rho_i \equiv \sum_{<\rho_j, t_j> \in F_A(B)} b_j \log_g \kappa_j \ (\bmod (3^{6n}-1)/(3^6-1))$$

However, for

$$\kappa_j = \Phi(\lambda_j)^h, < \lambda_j > = h < \rho_j, y - t_j >$$

let h be a class number of $GF(3^6)(x)[y]/(H)$.

Linear algebra phase: At this phase, find the discrete logarithm of the factor base by solving the linear equation given by the congruence equation generated in the relation exploration phase.

From F number of relations, the following matrix is obtained,

$$M = \begin{pmatrix} a_1^{(1)} \cdots a_{\#F_R(B)}^{(1)} & -b_1^{(1)} \cdots -b_{\#F_A(B)}^{(1)} \\ \vdots \quad\quad \vdots & \vdots \quad\quad \vdots \\ a_1^{(R)} \cdots a_{\#F_R(B)}^{(R)} & -b_1^{(R)} \cdots -b_{\#F_A(B)}^{(R)} \end{pmatrix}, \text{ vector}$$

$$v = \begin{pmatrix} \log_g \rho_1 \\ \vdots \\ \log_g \rho_{\#F_R(B)} \\ \log_g \kappa_1 \\ \vdots \\ \log_g \kappa_{\#F_A(B)} \end{pmatrix}$$

and linear equation

$$Mv \equiv 0 \ (\bmod (3^{6n}-1)/(3^6-1))$$

is to be solved.

Discrete logarithm calculation phase: At this phase, find the Discrete Logarithm Problem (DLP) for the given target using the discrete logarithm of the factor base found in the linear algebra phase.

Obtain the solution by finding integer numbers e_i, f_j which satisfy the following conditions:

$$\log_g X \equiv \sum_{\rho_i \in F_R(B)} e_i \log_g \rho_i + \sum_{<\rho_j, t_j> \in F_A(B)} f_j \log_g \kappa_j \pmod{(3^{6n}-1)/(3^6-1)}$$

5 About calculation of $GF(3^{6\cdot 71})$

For calculation of the Discrete Logarithm Problem (DLP) in a finite field addressed in reference [15], we succeeded in high-speed calculation in the relation exploration phase and the linear algebra calculation phase by using structural characters (Free-Relation and Galois Action) of $GF(3^{6\cdot 71})$.

5.1 Introduction of Free-Relations

At the relation exploration phase, a sufficient number of relations need to be generated so that a discrete logarithm of factor base can be obtained in the linear algebra phase, i.e. the generated linear equation has a solution.

Generally, the relation is generated by a sieve, and its calculation cost accounts for a large percentage of the calculation cost of a Function Field Sieve (FFS). On the other hand, a relation which is called "Free-Relation" and that can be obtained without using a sieve exists, and the cost of the sieve can be reduced by using it.

The number of relations depends on order d_H of y of $H(x, y)$ and the characteristic of a finite field. In fact, in many cases, approximately $\#F_A(B)/d_H$ number of Free-Relations exist, and the less the characteristic is the greater the number increases. In [15], we succeeded in obtaining $\#F_A(B)/2$ number of Free-Relations by selecting $H(x, y) = x + y^6$.

5.2 Introduction of Galois Action

The linear algebra phase also accounts for a large percentage of the calculation cost of a Function Field Sieve (FFS). Thus, provided that the size of matrix and vector is reduced maintaining the condition to enable obtaining a discrete logarithm for all factor bases, i.e. the number of variables in the linear equation is reduced, the calculation cost can be reduced significantly.

Galois Action is a method to relate one factor base to another using the Frobenius map ϕ. For example, when a factor base ρ corresponds to another factor base ρ' by the Frobenius map ϕ,

$$\rho' = \phi(\rho) = \rho^{3^n}$$

holds. This means that

$$\log_g \rho' = 3^n \log_g \rho$$

holds, and with this, the variable which exists in congruence equation and corresponds to $\log_g \rho'$ can be eliminated. In addition, the value which corresponds to the eliminated variable can be calculated from $\log_g \rho$, the condition to enable discrete logarithms to be obtained for all factor bases is ensured.

Provided that a finite field is $GF(3^{6n})$, $6n/n = 6$ holds. Therefore, from one factor base, up to six factor bases (including the original one) can be related to many factor bases using the Frobenius map. This means that the number of variables can be reduced to 1/6, and as a result, the calculation cost of the linear algebra phase can be reduced to $1/6^2$.

5.3 Calculation result

We used 18 servers for calculation, 12 servers from National Institute of Information and Communications Technology (NICT) and 6 servers from Future University-Hakodate, and succeeded in calculation in approximately 33 days with 96 Xeon CPU cores. This corresponds to approximately 9 years of calculation time with 1 Xeon core (Fig. 2).

Hereinafter, each phase in calculation of [15] is stated.

Polynomial selection phase: This is an impor-

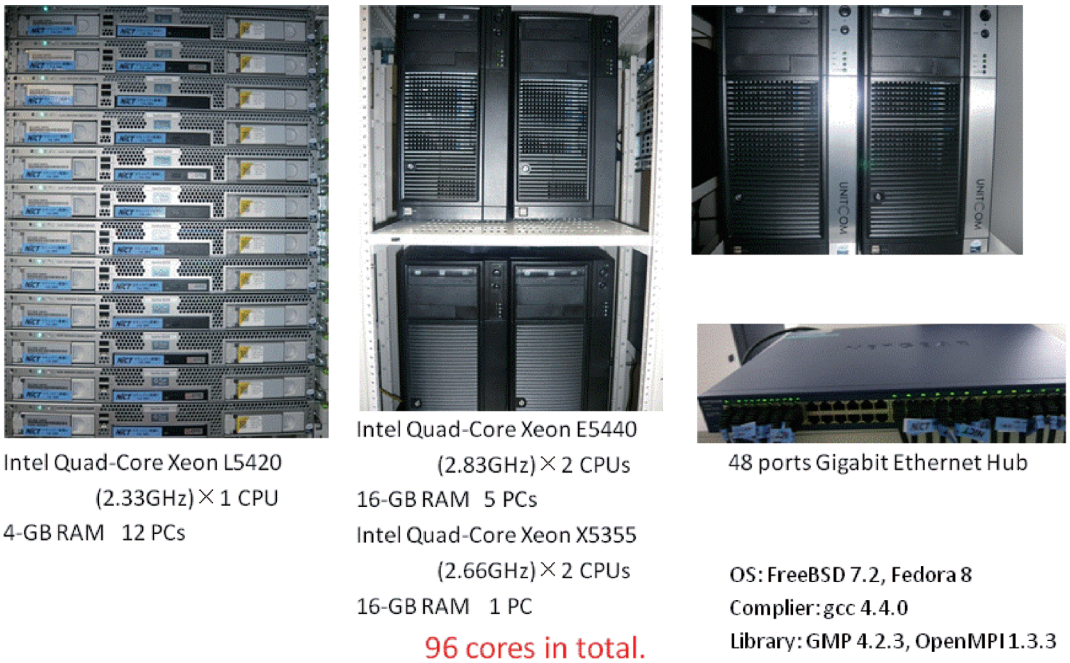

Fig.2 *Computational experiment environment (totally 96 core)*

tant phase to determine calculation amount of the remaining phases, however, as an effective selection method is proposed, calculation is scarcely required.

Relation exploration phase: This phase requires the largest number of calculations among the four phases. However, calculations can be performed faster by using many calculators as parallel calculation can be performed with little communication. By using Free-Relations, calculation in this phase could be performed approximately eight times as fast as before. Approximately 18 days were required for calculation of this phase.

Linear algebra phase: This phase also requires the largest number of calculations in the same way as in the relation exploration phase, however, as communications are required to perform parallel calculation, high-speed calculation cannot simply be performed using many calculators. By introducing Galois Action, we succeeded in performing calculation in this phase approximately thirty-six times as fast as before. This enabled calculations in approximately 12 hours in this phase which used to require calculations which were nearly equal to those of relation exploration.

Discrete logarithm calculation phase: At this final phase, same calculation as that in the relation exploration, however, not so many calculation amounts are required compared with the relation exploration. We succeeded in calculating discrete logarithm, which is to be a solution, in 14 days using only 6 servers from Future University-Hakodate.

6 Collaborative research of Future University-Hakodate and Kyushu University

The first half of the collaborative research was carried out with the Takagi research room of Future University-Hakodate. We went to a lot of trouble, including those of working at a distance, to show successful results. For the latter half, we carried out collaborative research with Kyusyu University along with a transfer of the Takagi research room, and conducted an internship. This internship significantly contributed to the efficiency of the research, and was meaningful.

7 Summary

We succeeded in calculating the Discrete Logarithm Problem (DLP) in a finite field $GF(3^{6\cdot 71})$ through collaborative research with the Takagi research room of Future University-Hakodate, and achieved a world record of 676 bits for the Discrete Logarithm Problem (DLP). We continue to carry out the collaborative research with Takagi research room even after it transferred to Kyushu University to pursue the establishment of a new record.

Acknowledgements

The results[15] described in this paper were achieved through collaborative research with professor TAKAGI Tsuyoshi and Mr. HAYASHI Takuya from Future University-Hakodate (currently, Kyushu University).

References

1 L. M. Adleman, "The function field sieve," ANTS-I, LNCS 877, pp. 108–121, 1994.

2 L. M. Adleman and M.-D. A. Huang, "Function field sieve method for discrete logarithms over finite fields," Inform. and Comput., Vol. 151, pp. 5–16, 1999.

3 K. Aoki, T. Shimoyama, and H. Ueda, "Experiments on the linear algebra step in the number field sieve," IWSEC 2007, LNCS 4752, pp. 58–73, 2007.

4 K. Aoki and H. Ueda, "Sieving using bucket sort," ASIACRYPT 2004, LNCS 3329, pp. 92–102, 2004.

5 P. S. L. M. Barreto, S. Galbraith, C. Ó hÉigeartaigh, and M. Scott, "Efficient pairing computation on supersingular abelian varieties," Des., Codes Cryptogr., Vol. 42, No. 3, pp. 239–271, 2007.

6 J.-L. Beuchat, N. Brisebarre, J. Detrey, E. Okamoto, M. Shirase, and T. Takagi, "Algorithms and arithmetic operators for computing the η_T pairing in characteristic three," IEEE Trans. Comput., Vol. 57, No. 11, pp. 1454–1468, 2008.

7 D. Boneh, D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," EUROCRYPT 2004, LNCS 3027, pp. 506–522, 2004.

8 D. Boneh and M. Franklin, "Identity based encryption from the Weil pairing," SIAM J. Comput., Vol. 32, No. 3, pp. 586–615, 2003.

9 D. M. Gordon, "Discrete logarithms in $GF(p)$ using the number field sieve," SIAM J. Discrete Math., Vol. 6, No. 1, pp. 124–138, 1993.

10 D. M. Gordon and K. S. McCurley,"Massively parallel computation of discrete logarithms," CRYPTO' 92, LNCS 740, pp. 312–323, 1992.

11 R. Granger, "Estimates for discrete logarithm computations in finite fields of small characteristic," Cryptography and Coding 2003, LNCS 2898, pp. 190–206, 2003.

12 R. Granger, A. J. Holt, D. Page, N. P. Smart, and F. Vercauteren, "Function field sieve in characteristic three," ANTS-VI, LNCS 3076, pp. 223–234, 2004.

13 R. Granger, D. Page, and M. Stam, "Hardware and software normal basis arithmetic for pairing-based cryptography in characteristic three," IEEE Trans. Comput., Vol. 54, No. 7, pp. 852–860, 2005.

14 D. Hankerson, A. Menezes, and M. Scott, "Software implementation of pairings," In Identity-Based Cryptography, pp. 188–206, 2009.

15 Takuya Hayashi, Naoyuki Shinohara, Lihua Wang, Shin'ichiro Matsuo, Masaaki Shirase, and Tsuyoshi Takagi, "Solving a 676-bit Discrete Logarithm Problem in $GF(3^{6n})$," 13th International Conference on Practice and Theory in Public Key Cryptography, PKC 2010, LNCS 6056, pp. 351–367, 2010.

16 A. Joux et al., "Discrete logarithms in $GF(2^{607})$ and $GF(2^{613})$," Posting to the Number Theory List, available at

http://listserv.nodak.edu/cgi-bin/wa.exe?A2=ind0509&L=nmbrthry&T=0&P=3690, 2005.
17 A. Joux and R. Lercier, "The function field sieve is quite special," ANTS-V, LNCS 2369, pp. 431–445, 2002.
18 A. Joux and R. Lercier, "Improvements to the general number field sieve for discrete logarithms in prime fields. A comparison with the Gaussian integer method," Math. Comp., Vol. 72, No. 242, pp. 953–967, 2002.
19 A. Joux and R. Lercier, "The function field sieve in the medium prime case," EUROCRYPT 2006, LNCS 4004, pp. 254–270, 2006.
20 A. Joux, R. Lercier, D. Naccache, and E. Thome, "Oracle-assisted static Diffie-Hellman is easier than discrete logarithms," Cryptography and Coding 2009, LNCS 5921, pp. 351–367, 2009.
21 A. Joux, R. Lercier, N. P. Smart, and F. Vercauteren, "The number field sieve in the medium prime case," CRYPTO 2006, LNCS 4117, pp. 326–344, 2006.
22 T. Kleinjung et al., "Discrete logarithms in $GF(p)$ - 160 digits," Posting to the Number Theory List, available at
http://listserv.nodak.edu/cgi-bin/wa.exe?A2=ind0702&L=nmbrthry&T=0&P=194, 2007.
23 B. A. LaMacchia and A. M. Odlyzko, "Solving large sparse linear systems over finite fields," CRYPTO' 90, LNCS 537, pp. 109–133, 1991.
24 R. Matsumoto, "Using C_{ab} curves in the function field sieve," IEICE Trans. Fundamentals, Vol. E82-A, pp. 551–552, 1999.
25 A. J. Menezes, T. Okamoto, and S. Vanstone, "Reducing elliptic curve logarithms to logarithms in a finite field," IEEE Trans. Inform. Theory, Vol. 39, No. 5, pp. 1639–1646, 1993.
26 D. Page, N. P. Smart, and F. Vercauteren, "A comparison of MNT curves and supersingular curves," Appl. Algebra Engrg. Comm. Comput., Vol. 17, No. 5, pp. 379–392, 2006.
27 J. Pollard, "The lattice sieve," In The Development of the Number Field Sieve, pp. 43–49, 1991.
28 C. Pomerance and J. W. Smith, "Reduction of huge, sparse matrices over finite fields via created catastrophes," Experiment. Math., Vol. 1, No. 2, pp. 89–94, 1992.
29 O. Schirokauer, "The special function field sieve," SIAM J. Discrete Math., Vol. 16, No. 1, pp. 81–98, 2003.
30 G. Wambach and H. Wettig, "Block sieving algorithms," Technical Report 190, Informatik, Universität zu Köln, 1995.
31 D. H. Wiedemann, "Solving sparse linear equations over finite fields," IEEE Trans. Inform. Theory, Vol. 32, No. 1, pp. 54–62, 1986.

(Accepted June 15, 2011)

SHINOHARA Naoyuki, *Ph.D.*

Expert Researcher, Security Fundamentals Laboratory, Network Security Research Institute

Computer Algebra

WANG Lihua, *Ph.D.*

Expert Researcher, Security Fundamentals Laboratory, Network Security Research Institute

Cryptographic Theory, Information Security

MATSUO Shin'ichiro, *Ph.D.*

Director, Security Architecture Laboratory, Network Security Research Institute

Cryptographic Protocol