4-6　関数体ふるい法による離散対数問題の解法

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

篠原直行　　王　立華　　松尾真一郎
SHINOHARA Naoyuki, WANG Lihua, and MATSUO Shin'ichiro

要旨

ペアリング暗号は、従来では実現困難だった、利便性が高く様々なサービスに応用可能なIDベース暗号などの基礎となることが知られている。特に有限体$GF(3^n)$上の超特異曲線を用いたη_Tペアリングは高速実装が可能な実用的なペアリングとして例にあげられる。η_Tペアリングを利用した暗号の安全性は、有限体$GF(3^n)$上の離散対数問題の解法困難性に根拠を置いている。そこで、NICTと公立はこだて未来大学は共同研究（2009年4月～2011年3月）で、有限体$GF(3^{6\cdot 71})$上の離散対数の計算に成功し、離散対数問題において676-bitの世界記録を達成した。本稿ではこの共同研究について解説する。

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 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.

[キーワード]
有限体，離散対数問題，指数計算法，関数体ふるい
Finite field, Discrete Logarithm Problem (DLP), Index calculus method, Function Field Sieve (FFS)

1　まえがき

ネットショッピングやネットバンキングなど、現代の情報システムでは機密情報を扱う場面が非常に多くなっている。また、現代の情報システムには、情報セキュリティの観点から様々な暗号技術が用いられている。そのため、悪意を持った攻撃者の解読能力の進歩に対して常に安全性を確保するための暗号技術の評価が必要になる。この評価において重要な役割を果たすのは、暗号技術のベースとなる数学的な問題で、その計算が、現在および将来にわたり想定しうるコンピュータの能力によっても、困難であることを確認することである。

近年、従来の公開鍵暗号では実現困難だった、利便性が高く様々なサービスに応用可能なIDベース暗号などの基礎となるペアリング暗号の研究が盛んに行われている。ペアリング暗号は有限体上の離散対数問題の難しさを安全性の根拠としているため、安全性を正確に評価するためには、計算可能なビット数の検証・評価を行う必要がある。

有限体$GF(3^n)$上の超特異曲線を用いたη_Tペアリングは高速実装が可能な実用的なペアリングとして知られている。η_Tペアリングを用いた暗号の安全性は有限体$GF(3^n)$上の離散対数問題の困難性を根拠としているが、$GF(3^n)$上の離散対数問題に関する計算実験の報告は少ない。

2009年4月、NICTと公立はこだて未来大学はη_Tペアリングを用いた暗号の安全性、即ち

$GF(3^n)$ 上の離散対数問題の効率的な解法について共同研究を開始した。その結果、$GF(3^{6\cdot71})$ 上の離散対数の計算に成功し、これは676 bit 長の有限体上の離散対数問題を解いたことを意味する。この成果は、ペアリング暗号を採用する際に安全な鍵のサイズを見積るための技術的根拠となる。

有限体上の離散対数問題の計算は、従来から世界各国の様々なグループが挑戦してきた。主要なグループである、ドイツのボン大学数学研究所のグループ、フランスの国防省およびレンヌ数学研究所のグループ、そしてNICT および公立はこだて未来大学について、計算に成功したビット数を比較すると次の図1のようになる。

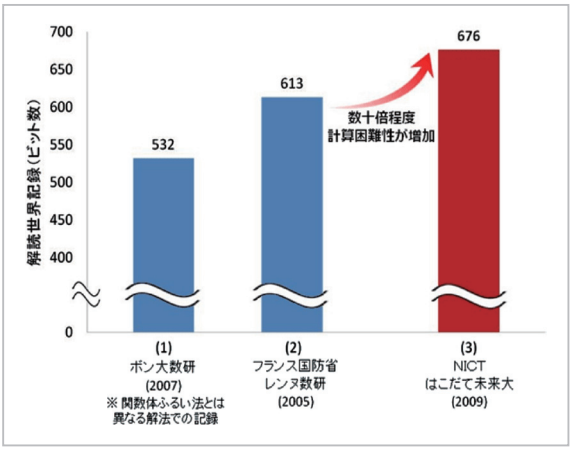

図1 世界の主要グループによる計算記録

本稿の構成は以下のとおりである。まず、**2** において有限体上の離散対数問題について説明する。次に、有限体上の離散対数問題を効率よく解く手法として関数体ふるい（Function Field Sieve：FFS）が挙げられ、NICT と公立はこだて未来大学の共同研究においても同様の手法を用いた。関数体ふるい法は指数計算法の1つであるため、**3** では指数計算法について説明する。**4** では文献[15]の概説、即ち676 bit 長の有限体上の離散対数問題を解く際に用いた関数体ふるい法について解説する。また、その工夫の要点と計算結果を **5** で述べ、**6** では共同研究をとおして感じたことをまとめる。

2 有限体上の離散対数問題

まず、有限体上の離散対数問題について説明する。標数を p、拡大次数を n とする有限体 $GF(p^n)$ の既約剰余類群 $GF(p^n)^*$ は巡回群である。従って生成元 $g \in GF(p^n)^*$ が存在し $GF(p^n)^* = <g>$ が成り立つ。但し、

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

とする。

『有限体上の離散対数問題』とは「与えられた $X \in GF(p^n)^*$ と生成元 g に対して $X = g^e$ を満たす整数 $e \in [1, p^n-1]$ を求めよ」という問題である。数列 $\{g, g^2, ..., g^{p^n-1}\}$ は乱数列のようにふるまうのでその解法は困難であり、実際に効率の良い方法の1つである関数体ふるい法の計算量はある定数 c が存在して $L_{p^n}[1/3, c]$ である。

例1）

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

であり、$x+1$ は生成元である。実際に $g = x+1$ とすると

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

となる。この数列から、二次拡大体の定義多項式を x^2+1、生成元を $x+1$ としたときの $2x+2$ の離散対数 $\log_{x+1}(2x+2)$ は5である。$GF(3^2)^*$ の周期は8であることから、4-bit の離散対数問題を解いたことになる。

本稿では主に $GF(3^{6\cdot71})$ における離散対数問題、即ち676-bit の離散対数問題を解くことについて議論する。

3 指数計算法

離散対数問題を効率よく解く手法として、指数計算法の1つである関数体ふるい法が挙げられる。従って、**3** では指数計算法について説明する。また、ここでは有限体を、多項式環で表現する必要のない、より簡易な体である標数 p の基礎体 $GF(p)$ とする。従って離散対数問題は g を生成元、$X \in GF(p)^*$ として次式から与えられる：

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

3.1 指数計算法の方針

指数計算法の方針を説明する。まず $X \in GF(p)^*$ であるが X は整数と考えることもできる。そこで仮定として、X はある整数 B 以下の素数 ρ_i の積に因数分解され、その素因数分解が既知とする：

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

このように素因子が全て B 以下となる整数を B-smooth な整数という。さらにもう1つの仮定として、B 以下の各素数 ρ_i の離散対数 z_i、即ち

$$\rho_i \equiv g^{z_i} \bmod p$$

なる整数 $0 \le z_i \le p-1$ も既知とする。このとき

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

となり、X の離散対数 e に対して

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

が成り立つ。e_i, z_i は既知であることから e を得る。

先に述べたように指数計算法では仮定が2つあった。1つ目の、X が B-smooth であるという仮定は与えられた離散対数問題を変形させることで解決される。即ち、ランダムに生成した整数 g^a に対して $X' = g^a X \pmod{p}$ が B-smooth であれば指数計算法によって X' の離散対数 $a+e$ を得ることができ、さらに a が既知であることから e を得ることができる。もう1つの仮定は因子基底の離散対数を既知であることであり、その計算方法は **3.2** で説明する。

3.2 因子基底の離散対数の計算方法

因子基底の離散対数の計算は、関係（relation）探索とそれによって与えられる連立線型合同方程式を解くことである。まず、関係探索から説明する。

関係探索ではランダムに整数 $g^{a_j} \pmod{p}$ を生成し B-smooth となるものを集める。このとき

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

が成り立ち、この関係から合同方程式

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

が与えられる。$a_j, e_{i,j}$ は既知であることから、構成される連立線型合同方程式を解くことで因子基底の離散対数 z_i を得ることができる。

3.3 指数計算法の概要

ここでは指数計算法のアルゴリズムを整理する。

パラメータ選択段階：全体の計算コストが小さくなるようにパラメータ B を設定する。
（**4** の関数体ふるい法では多項式選択段階にあたる。）

関係探索段階：ランダムに整数 $g^{a_j} \pmod{p}$ を生成し B-smooth となるものを集め、次のような合同方程式を十分な数ほど生成する：

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

線形代数段階：連立合同方程式を解くことによって全ての因子基底の離散対数を求める。

離散対数計算段階：与えられた整数 X に対して、ランダムに整数 g^a を生成し、$X' = g^a X \pmod{p}$ が B-smooth となるようなものを求める。因子基底の離散対数と a から X の離散対数を計算する。

4 関数体ふるい法

ここでは関数体ふるい法の概要について説明する（詳細は文献[15]を参照）。この手法は4つの段階、即ち、多項式選択段階（パラメータ選択段階）、関係探索段階、線形代数段階、離散対数計算段階から構成される。また、与えられた有限体は $GF(3^{6 \cdot n})$ の形を持つものとする。さらに、g をその既約剰余類群の生成元とし、$X \in <g>$ の離散対数 $\log_g X$ を求めることを考える。

多項式選択段階：この段階では関数体ふるい法の計算コストに関する後述のパラメータ値 $d_H, \deg m, B, R, S$ を決定する。従って、以降の段階の総計算量を評価し、その値が小さくなるような $d_H, \deg m, B, R, S$ を算出する。

次に、$GF(3^6)$ 上既約でモニックな n 次多項

式 $f(x)$ を選ぶ。このとき有限体 $GF(3^{6\cdot n})$ は $GF(3^6)[x]/(f)$ と表すことができる。次に文献[1]にある8つの条件を満たす2変数多項式 $H(x,y)\in GF(3^6)[x,y]$ を求める。実際には

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

のような形を選んだ。このとき全射準同型

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

が存在する。但し $m\in GF(3^6)[x]$ は $H(x,m)\equiv 0 \bmod f$ かつ $\deg m\cdot d_H\geq n$ を満たすものとする。次に smoothness bound Bを選び、有理側の因子基底 $F_R(B)$ と代数側の因子基底 $F_A(B)$ を次のように選ぶ:

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

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

但し、$Div(GF(3^6)[x,y]/(H))$ は $GF(3^6)[x,y]/(H)$ の因子群とする。

関係探索段階: この段階では指数計算法における因子基底の離散対数を得るために必要な合同方程式を生成する。

次数が B 以下の $r,s\in GF(3^6)[x]$ に対して、互いに素かつ以下の条件を満たす組 (r,s) を $F(\geq \#F_R(B)+\#F_A(B))$ 個見つける:

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

但し、t_j は ρ_j, r, s によって一意に決定される。また、r はモニックであるとする。つまり $rm+s$, $(-r)^{d_H}H(x,-s/r)$ がともに B 次以下の素因子に因数分解される組 (r,s) を探し、またこのような (r,s) を double B-smooth と呼ぶ。このとき次のような関係(relation)が成り立つ:

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

但し、

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

で h は $GF(3^6)(x)[y]/(H)$ の類数とする。

線形代数段階: この段階では、関係探索段階で生成された合同方程式から与えられる線型方程式を解くことで、因子基底の離散対数を求める。

F 個の relation から次のような行列と

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

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

が得られ、線型方程式

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

を解く。

離散対数計算段階: この段階では、線形代数段階で求めた因子基底の離散対数を用いて、与えられた対象の離散対数問題を求める。

次の条件を満たす整数 e_i, f_j を求めることで解を得る:

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

5 $GF(3^{6\cdot 71})$ の計算について

文献[15]で扱った有限体上の離散対数問題の計算では、$GF(3^{6\cdot 71})$ の構造による性質(Free-Relation、Galois Action)を利用することで、関係探索段階、線形代数計算段階の2つの段階について高速に計算することに成功した。

5.1 Free-Relationの導入

関係探索段階では、線形代数段階で因子基底の離散対数を得られるように、即ち生成した線型方程式が解を持つように、十分な数のrelationを効率よく生成しなければならない。

一般にRelationはふるいによって生成され、その計算コストは関数体ふるい法の計算コストで大きな割合をしめる。一方でFree-Relationと呼ばれるふるいを用いずに得られるrelationが存在し、これを用いることでふるいのコストを削減することができる。

Relationの個数は$H(x,y)$のyの次数d_Hと有限体の標数に依存する。実際に、多くの場合で約$\#F_A(B)/d_H$個のFree-Relationが存在し、さらに標数が小さいほどその数は増加する。文献[15]では$H(x,y)=x+y^6$を選ぶことで$\#F_A(B)/2$個のFree-Relationを得ることに成功した。

5.2 Galois Actionの導入

線形代数段階も関数体ふるい法の計算コストで大きな割合を占める。従って、全ての因子基底に対して離散対数が得られる条件を保ったまま、行列とベクトルの大きさを小さくする、即ち線型方程式の変数の数を減らすことができれば計算コストを大きく削減することができる。

Galois Actionは、Frobenius map ϕを使って、ある因子基底と他の因子基底を関係づける手法である。例えば、因子基底ρがFrobenius map ϕによって別の因子基底ρ'に対応すると

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

が成り立つ。従って、

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

が成り立ち、このことから合同方程式に現れる変数で$\log_g \rho'$に対応するものを消去することができる。また、消去された変数に対応する値は$\log_g \rho$から計算できるため、全ての因子基底に対して離散対数が得られるという条件は保証されている。

有限体が$GF(3^{6n})$の場合$6n/n=6$であることから、多くの因子基底に対して、1つの因子基底からそれ自身を含めて6個の因子基底をFrobenius mapで関係づけることができる。これは変数の数を約1/6に削減できることを意味しており、その結果として線形代数段階の計算コストを$1/6^2$倍に抑えることができた。

5.3 計算結果

使用した計算機はNICTのサーバー12台、公立はこだて未来大学のサーバー6台の計18台で、

Intel Quad-Core Xeon
L5420(2.33GHz)× 1 CPU
4 GB RAM 12台 (NICT)

Intel Quad-Core Xeon E5440
(2.83GHz)× 2 CPU
16 GB RAM 5台
Intel Quad-Core Xeon X5355
(2.66GHz)× 2 CPU
16 GB RAM 1台

48port Gigabit Ethernet Hub(NICT)

図2 計算実験環境(計96コア)

Xeon 96コア分のCPUコアにより、およそ33日間で計算に成功した。これは、Xeon 1コアで約9年の計算時間に相当する(図2)。

以下、文献[15]の計算における各段階について述べる。

多項式選択段階：この段階は残りの段階の計算量を決める重要な段階であるが、効率的な選択手法が提案されているため、計算をほとんど必要としない。

関係探索段階：この段階は4つの段階中最も多くの計算を必要とする。しかし、ほとんど通信を行わずに並列計算が可能であるため、多くの計算機を利用することでより高速に計算を行うことができる。Free-Relationを利用することでこの段階の計算を従来のおよそ8倍高速に行うことができた。この段階の計算に約18日を必要とした。

線形代数段階：この段階も関係探索段階と同様に多くの計算を必要とするが、並列計算を行う際には通信を行う必要があるため、単純に多くの計算機を利用するだけでは高速に計算を行うことができない。Galois Actionを導入することで、この段階の計算を従来のおよそ36倍の高速で行うことに成功した。これにより、従来は関係探索と同程度の計算が必要だったこの段階を、およそ12時間の計算で行うことができた。

離散対数計算段階：この最後の段階では、関係探索段階と同様の計算を行うが、関係探索段階と比較すると計算量はさほど必要としない。公立はこだて未来大学のサーバー6台のみを利用し、14日かけて、解となる離散対数を計算することに成功した。

6 公立はこだて未来大学、九州大学との共同研究

共同研究の前半は公立はこだて未来大学の高木研究室と進めてきた。距離的な問題もあり苦労しながらも成果を上げることができた。後半は、高木研究室の移籍に伴い、国立九州大学と共同研究を進めており、インターンシップも行った。このインターンシップによる研究の効率は大きく、有意義なものとなった。

7 まとめ

公立はこだて未来大学の高木研究室との共同研究において、有限体 $GF(3^{6\cdot71})$ 上の離散対数の計算に成功し、離散対数問題において676-bitの世界記録を達成した。高木研究室が国立九州大学に移籍した後も更なる記録の更新を目指し共同研究を行っている。

謝辞

本稿で解説した成果[15]は公立はこだて未来大学(現在は国立九州大学)の高木剛教授、林卓也氏との共同研究によるものである。

参考文献

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.

（平成 23 年 6 月 15 日 採録）

篠原直行（しのはら なおゆき）
ネットワークセキュリティ研究所
セキュリティ基盤研究室専攻研究員
博士（数理学）
計算機代数学

王　立華（Lihua Wang）
ネットワークセキュリティ研究所
セキュリティ基盤研究室専攻研究員
博士（工学）
暗号プロトコル

松尾真一郎（まつお しんいちろう）
ネットワークセキュリティ研究所
セキュリティアーキテクチャ研究室室長　博士（工学）
暗号プロトコル