$\mathrm{GF}(3^6)$ の n 次拡大体における関数体篩法の実装実験

林 卓也　　白勢 政明　　高木 剛

公立はこだて未来大学大学院 システム情報科学研究科
041-8655 北海道函館市亀田中野町 116-2

あらまし $\mathrm{GF}(3^{6n})$ 上の離散対数問題 (DLP) は，高速実装が可能な $\mathrm{GF}(3^n)$ 上の超特異楕円曲線における η_T ペアリングを用いたペアリング暗号において安全性の根拠となる重要な問題の一つである．2006 年に Joux らによって提案された関数体篩法は, $\mathrm{GF}(q^n)$ において q が中程度（$q \approx n^{\sqrt{n}}$）の有限体上の DLP に対して有効なアルゴリズムである．また，$\mathrm{GF}(3^{6n})$ 上の DLP に対して漸近的な計算量では従来の関数体篩法と同等であるが，上記の条件とは異なる n に対して従来の関数体篩法と比較して数倍程効率的である可能性がある．本稿では Joux, Lercier が提案した関数体篩法の $\mathrm{GF}(3^{6n})$ 上での実装を行い，従来の関数体篩法との計算実験による比較を行った．その結果，従来の関数体篩法よりも高速に計算可能な拡大次数 n（$n = 19, 61$ など）が存在することを確認した．

Implementation of the Function Field Sieve in the Medium Prime-power Case over $\mathrm{GF}(3^{6n})$

Takuya Hayashi　　Masaaki Shirase　　Tsuyoshi Takagi

Graduate School of Systems Information Science, Future University Hakodate,
116-2, Kamedanakano-cho Hakodate Hokkaido, 041-8655, Japan

Abstract The discrete logarithm problems (DLP) over $\mathrm{GF}(3^{6n})$ is one of the most important problems which is the security basis of the pairing-based cryptosystems using the η_T pairing on supersingular curves over $\mathrm{GF}(3^n)$. In 2006, Joux and Lercier proposed the new function field sieve algorithm which is efficient for solving the DLP over $\mathrm{GF}(q^n)$ $(q = p^k)$ when q is a medium-sized prime-power. The new function field sieve has the same asymptotic complexity as traditional one for solving the DLP over $\mathrm{GF}(3^{6n})$. However, it may be more efficient than traditional one in some n. In this paper, we implemented the new function field sieve over $\mathrm{GF}(3^{6n})$ and compared with traditional one by practical experiments. As a result, we confirmed that the new function field sieve is more efficient than traditional one for solving the DLP over $\mathrm{GF}(3^{6n})$ such as $n = 19, 61$.

1　はじめに

ペアリング暗号では，ID を公開鍵として利用可能な ID ベース暗号 [5] などの従来の公開鍵暗号方式では実現が困難であった様々な暗号プロトコルが提案されている．また，高速な実装が可能なペアリングとして知られる標数 3，拡大次数 n の有限体 $\mathrm{GF}(3^n)$ 上の超特異楕円曲線を用いた η_T ペアリング [3] は，ソフトウェアやハードウェアなどで多くの実装が発表されている [4, 8]．この際，n は 97, 163, 193, ... などの素数が用いられているため [14]，以下特別な断

りがない限り n は素数であるとする．

有限体 $\mathrm{GF}(3^{6n})$ 上の離散対数問題 (DLP) は，$\mathrm{GF}(3^n)$ 上の η_T ペアリングを利用したペアリング暗号の安全性の根拠の一つである．この問題の漸近的に最も効率的な解法として関数体篩法が知られている．関数体篩法の計算量は鍵長に対して準指数関数時間であり，$\mathrm{GF}(q^n)$ 上の DLP に対し，

$$L_{q^n}[\frac{1}{3}, c] = \exp((c+o(1))(\log q^n)^{\frac{1}{3}}(\log\log q^n)^{\frac{2}{3}})$$

である．ただし，c は定数，$o(1)$ は $n \to \infty$ に対し $o(1) \to 0$ となる関数である．実装上最も高速な関数体篩法の一つとして知られる Joux, Lercier の関数体篩法は $c = (32/9)^{1/3}$ である [11]. Joux らはこの関数体篩法を用いて標数 2 の有限体上の DLP の計算世界記録となる $\mathrm{GF}(2^{613})$ 上の DLP の計算に成功した [10]．一方，2006 年に Joux, Lercier によって新たな関数体篩法が提案された [12]．従来の関数体篩法は小さな標数の有限体に対してのみ効率的であるのに対し，新たな関数体篩法では，関係探索の範囲を削減することにより中程度の大きさの標数の有限体 (medium prime case) に対しても効率的に計算が可能である．同様にして，小さな標数 p のべき $q = p^k$ が中程度の大きさの有限体 (medium prime-power case) に対しても効率的に計算が可能である．$q = 3^6$ として $\mathrm{GF}(3^{6n})$ 上の DLP に適用する場合，漸近的には従来の関数体篩法と同等の計算量であるが[1]，特定の拡大次数 n に対しては従来の関数体篩法と比較して数倍程度効率的である可能性がある．しかし，新たに提案された関数体篩法と従来の関数体篩法について，計算実験等による比較は行われていない．

本稿では，文献 [12] で提案された関数体篩法の $\mathrm{GF}(3^{6n})$ における実装を行い，従来の関数体篩法 [11] との計算実験による比較を行った．各関数体篩法の探索範囲の違いにより，パラメータ B に対し $(B+1)\log(3^6) \geq \sqrt{n/B}\log(n/B)$ を満たす最大の拡大次数 n において，文献 [12] の関数体篩法がより高速に計算可能であることが予想され，実際に，計算実験によって上記の式を満たす拡大次数 $n = 19, 61$ において，従来の関数体篩法よりも数倍程度高速に計算可能であることを確認した．

[1] n が合成数の場合，関数体篩法の計算量 $L_{q^n}[\frac{1}{3}, c]$ において $c = 3^{1/3}$ となる可能性がある．しかし，本稿では n を素数に限定するためこのような場合は扱わず，$c = (32/9)^{1/3}$ である．

2 関数体篩法

本節では関数体篩法の概要について説明する．関数体篩法は次の 4 ステップ

1. 多項式選択 (Polynomial selection)
2. 関係探索 (Collection of relations)
3. 線形代数 (Linear algebra)
4. 特定の元の離散対数計算 (Individual logarithm)

に大別される．

$\mathrm{GF}(3^{6n})$ 上の DLP に対し関数体篩法を適用することを考える．$k \in \{1, 2, 3, 6\}$ とし，$\mathrm{GF}(3^{6n})$ を $\mathrm{GF}(3^k)$ の $N = 6n/k$ 次拡大体として表現する．$f \in \mathrm{GF}(3^k)[x]$ を N 次モニック既約多項式とすると，$\mathrm{GF}(3^{6n}) \simeq \mathrm{GF}(3^k)[x]/(f)$ である．多項式選択ステップでは，Adleman によって示された条件 [1] を満たす y に関する次数 d の二変数多項式 $H(x, y) \in \mathrm{GF}(3^k)[x, y]$ を選択し，$H(x, m) \equiv 0 \bmod f$ となる $m \in \mathrm{GF}(3^k)[x]$ を計算する．関係探索ステップでは，パラメータ B に対して次数が B 次以下で互いに素な $a, b \in \mathrm{GF}(3^k)[x]$ に対し，

$$N_R(a, b) = a + bm \quad (1)$$
$$N_A(a, b) = (-b)^d H(x, -a/b) \quad (2)$$

がともに B-smooth（全ての既約因子の次数が B 次以下）となる (a, b) を探索し，因子基底の離散対数の関係 (relation) を十分な個数集める．線形代数ステップで関係から得られる線形方程式を解き，各因子基底の元の離散対数を計算し，それらを基に特定の元の離散対数計算ステップで任意の元の離散対数の計算を行う．各ステップの詳細については文献 [1, 7, 11] 等を参照されたい．

従来の関数体篩法 [11]（以下，[JL02] と表記）は小さな標数の有限体上の DLP を効率的に解

くアルゴリズムである．$k = 2, 3, 6$ とし計算を行うことも可能であるが，$k = 1$ と比較して高速にはならないため [7]，$k = 1$ の場合についてのみ扱い，$\mathrm{GF}(3^{6n})$ を $\mathrm{GF}(3)$ の $6n$ 次拡大体として表現する．一方，新しく提案された関数体篩法 [12]（以下，[JL06] と表記）では 3^k が中程度の大きさのときに効率的に計算できる．このため [JL06] では $k = 6$ とし，$\mathrm{GF}(3^{6n})$ を $\mathrm{GF}(3^6)$ の n 次拡大体として表現する．[JL02] と [JL06] とで異なる点は多項式選択ステップおよび関係探索ステップにおける探索範囲であるため，以下，多項式選択ステップおよび探索範囲について説明する．

3 多項式選択ステップと関係探索の範囲

多項式選択ステップでは，Adleman により示された条件 [1] を満たす $H(x, y) \in \mathrm{GF}(3^k)[x, y]$ を選択する必要がある．文献 [11] より，以下の条件を満たす $m \in \mathrm{GF}(3^k)[x]$ が存在する $H(x, y)$ を C_{ab} 曲線から選択すればよい．

$$H(x, m) \equiv 0 \bmod f$$

多項式 $H(x, y)$ の具体的な構成方法として，[JL02] の多項式選択法，[JL06] の多項式選択法について説明し，それらによって定まる関係探索ステップにおける必要な探索範囲について説明する．

3.1 [JL02] の多項式選択と探索範囲

[JL02] では，$\mathrm{GF}(3^{6n})$ を $\mathrm{GF}(3)$ の $6n$ 次拡大体として表現する．$H(x, y)$ の y に関する次数を d とし，次数が $\lfloor 6n/d \rfloor$ となる $u_1, u_2 \in \mathrm{GF}(3)[x]$ をランダムに選択する．$f = u_2^d H(x, -u_1/u_2)$ が $6n$ 次既約多項式であるとき，$m = -u_1/u_2$ とすると明らかに $H(x, m) \equiv 0 \bmod f$ である．このとき，式 (1) を $au_2 - bu_1$ と式変形する必要がある．

パラメータ B, d は，

$$\begin{aligned} B &= \lceil (4/9)^{\frac{1}{3}} (6n)^{\frac{1}{3}} (\log_3 6n)^{\frac{2}{3}} \rfloor \\ d &= \lceil \sqrt{6n/(B+1)} \rfloor \end{aligned}$$

とする．このとき，$H(x, y)$ の x に関する次数を c とすると，

$$\begin{aligned} \deg(N_R(a, b)) &\leq B + \lfloor 6n/d \rfloor \\ \deg(N_A(a, b)) &\leq d \cdot B + c \end{aligned}$$

となる．また，a, b ともに B 次以下の $\mathrm{GF}(3)[x]$ の元であることから，探索範囲は $3^{B+1} \cdot 3^{B+1}$ である．

3.2 [JL06] の多項式選択と探索範囲

[JL06] では，$\mathrm{GF}(3^{6n})$ を $\mathrm{GF}(3^6)$ の n 次拡大体として表現する．

$$(B+1)\log(3^6) \geq \sqrt{n/B}\log(n/B) \quad (3)$$

を満たす最小の B，$d' \approx \sqrt{Bn}$, $d \approx \sqrt{n/B}$ であり，$dd' \geq n$ となる d, d' を選択する．d' 次の $m \in \mathrm{GF}(3^6)[x]$，$d$ 次の $g(y) \in \mathrm{GF}(3^6)[y]$ をランダムに選択する．$H(x, y) = g(y) + x$ とし，$f | H(x, m)$ となる f が n 次既約多項式であるとき，$H(x, m) \equiv 0 \bmod f$ を満たす．このとき，

$$\begin{aligned} \deg(N_R(a, b)) &\leq B + d' \\ \deg(N_A(a, b)) &\leq d \cdot B + 1 \end{aligned}$$

となる．

次に探索範囲について考察する．(a, b) に対し，$N_R(a, b)$, $N_A(a, b)$ が共に B-smooth であるとする．このとき，

$$\begin{aligned} N_R(a, b) &= c_1 \prod p_i^{e_i} \\ N_A(a, b) &= c_2 \prod p_j^{e_j} \end{aligned}$$

となる $c_1, c_2 \in \mathrm{GF}(3^6)^*$ が存在する．ここで，関係探索ステップで探索する因子基底の離散対数の関係式は $(3^{6n}-1)/(3^6-1)$ を法とするため，$\mathrm{GF}(3^6)^*$ の元は計算上無視して良い．このため，c_1, c_2 が異なる関係式であっても，$\prod p_i^{e_i}$, $\prod p_j^{e_j}$ が等しければ同じ関係式として計算できる．よって，重複する関係式を明示的に除去するために，c_1, c_2 を固定することを考える．c_1, c_2 は $N_R(a, b)$, $N_A(a, b)$ の最高次係数であるため，それぞれ bm, $(-b)^d x$ の最高次係数とほぼ一致する．m, x は固定であるため，b の最高次係数を

表 1: 有限体 $\mathrm{GF}(3^{6n})$ における各パラメータ

n	ビット長	[JL02] の多項式選択法 [11]（$k=1$）					[JL06] の多項式選択法 [12]（$k=6$）					
		N	B	d	関係が得られる確率	探索範囲	N	B	d	d'	関係が得られる確率	探索範囲
19	181	114	10	3	1.6×10^{-5}	3.1×10^{10}	19	1	5	4	4.9×10^{-5}	3.9×10^{8}
31	295	186	12	4	1.6×10^{-6}	2.5×10^{12}	31	2	4	8	3.7×10^{-7}	2.1×10^{14}
47	447	282	15	4	1.8×10^{-7}	1.9×10^{15}	47	2	5	10	1.8×10^{-9}	2.1×10^{14}
61	581	366	17	5	4.0×10^{-8}	1.5×10^{17}	61	2	6	11	2.7×10^{-11}	2.1×10^{14}
79	752	474	19	5	6.9×10^{-9}	1.2×10^{19}	79	3	5	16	1.1×10^{-9}	1.1×10^{20}
97	923	582	21	5	1.4×10^{-9}	9.9×10^{20}	97	3	6	17	2.7×10^{-11}	1.1×10^{20}

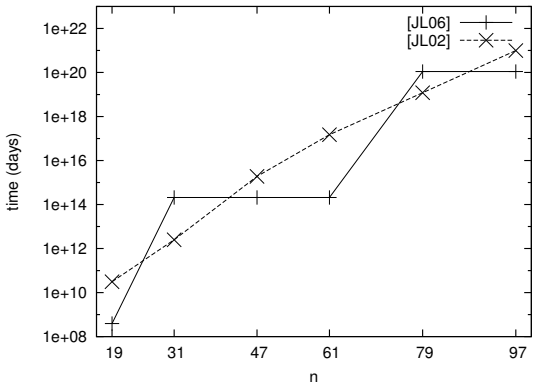

図 1: 拡大次数 n に対する探索範囲の見積もり

固定すればよい．b をモニック多項式に固定すると (a,b) の探索範囲はおよそ $(3^6)^{B+1}\cdot(3^6)^B$ となり，b の最高次係数を固定しない方法と比べ探索範囲をおよそ $1/(3^6)$ に削減できる．

3.3 多項式選択法の比較

表 1 に [JL02] および [JL06] において，各 n に対し算出したパラメータおよび関係が得られる確率，関係探索における探索範囲を示す．各パラメータおよび探索範囲は 3.1，3.2 節で示した方法で算出した．また，関係が得られる確率は，文献 [11] より次数 δ の多項式が B-smooth である確率は $\delta^{1/100}\le B\le\delta^{99/100}$ に対し漸近的に $(B/\delta)^{\delta/B}$ であることを用いて[2]，3.1，3.2 節で示した $N_R(a,b)$, $N_A(a,b)$ の次数から算出した．

[2] $B=1$ については上記の範囲を満たさないため，δ 次の多項式が δ 個の根を持つ確率が漸近的に $1/(\delta!)$ であることを用いた．

[JL02] の多項式選択法では，n が大きくなるとともに関係が得られる確率が小さくなっており，このため探索範囲をより大きく取る必要がある．一方，[JL06] の多項式選択法では，n が大きくなるとともに関係が得られる確率が小さくなっているが，$n=31, 47, 61$ や $n=79, 97$ において探索範囲の大きさは変わらない．これは，[JL06] では B が大きくなるとともに探索範囲が $(3^6)^2\approx530,000$ 倍の大きさになり，探索範囲の大きさの詳細な調整を行うのが困難なためである．このため，$n=31, 47$ や $n=79$ などでは [JL06] の多項式選択法の探索範囲は過大である可能性がある．

図 1 に各 n に対する探索範囲の大きさをグラフで示す．$n=19, 47, 61, 97$ において，[JL02] の多項式選択法と比較して [JL06] の多項式選択法がより探索範囲が小さい．探索範囲が小さいほど関係探索ステップの計算量は小さくなるため，[JL06] が [JL02] と比較して高速に計算できる可能性がある．

4 実装実験

本節では文献 [11] の関数体篩法（[JL02]），文献 [12] の関数体篩法（[JL06]）の実装および計算実験の結果を示す．

4.1 関係探索ステップの実装

関係探索ステップにおける篩処理は [JL02] では格子篩 [15] を実装した．この際，次数が 1 や 2 などの小さな次数の因子基底については，篩処理のコストが大きいことや篩処理の精度への

影響が小さいことなどを考慮し，篩処理を行っていない．実装の詳細については文献 [9] を参照されたい．

一方，[JL06] では b がモニック多項式といった制限から格子篩が有効ではないため，多項式篩 [6, 9] を実装した．[JL06] の篩処理では，全ての因子基底について篩処理を行い，篩処理で得られた候補のほぼ全てが関係となるようにした．このため，[JL06] では候補に対して B-smooth テストは行わずに既約分解を行っている．

4.2 線形代数ステップの実装

線形代数ステップでは，前処理として Structured Gaussian Elimination (SGE) [13, 16] を実装し，線形方程式の解法として反復法の一つである Lanczos 法を実装した．Lanczos 法は並列構造として文献 [2] と同様の構造を実装した．

4.3 比較実験

多項式選択法の違いにより，[JL02] と [JL06] の関係探索ステップの計算量が異なることから，実験は関係探索ステップの計算のみ行った．$n = 19, 31, 47, 61$ について行い，各パラメータは表 1 を参照している．$n = 79, 97$ については実験に数週間以上かかることが予想されたため実験は行っていない．実験環境は Intel Quad-Core Xeon E5440 (2.83GHz) × 2 CPU, 16GB RAM を搭載したノード 5 台，Intel Quad-Core Xeon X5355 (2.66GHz) × 2 CPU, 16GB RAM を搭載したノード 1 台，Intel Quad-Core Xeon L5420 (2.33GHz) × 1 CPU, 4GB RAM を搭載したノード 12 台の計 18 台（96 コア）である．

図 2 に各関数体篩法の関係探索ステップに要する時間を示す．ただし，1 時間以上かかる計算については 1 時間の計算の振る舞いから，全ての探索範囲を探索する時間を見積もっている．

図 2 では，図 1 と比較して [JL02] のグラフが全体的に下がっているのが分かる．これは，[JL02] の実装では篩処理に格子篩を用いているためであると考えられる．格子篩では special-q と呼ばれる因子基底の元で割り切れる点のみを篩処理の対象とするため，多項式篩と比較して

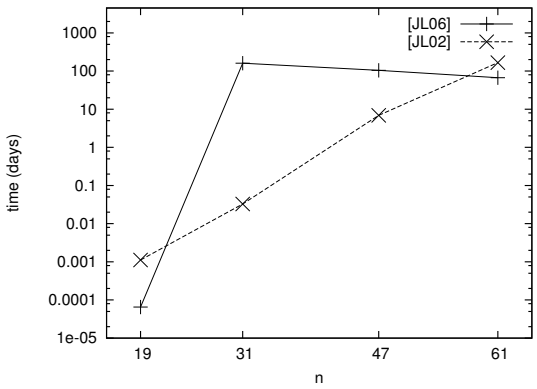

図 2: n に対する関係探索ステップの計算時間の見積もり

探索範囲が小さくなる．このため，関係探索に要する時間が全体的に短くなり，$n = 47$ においては図 2 と図 1 では結果が逆となっている．

$n = 19, 61$ において [JL06] の実装が [JL02] の実装よりも計算時間が短い結果となっており，実際に [JL06] が $\mathrm{GF}(3^{6n})$ 上の離散対数問題に対して有効である n が存在することが示された．特に，$n = 61$ では [JL02] の実装では約 165 日かかる見積もりに対し，[JL06] の実装では約 66 日でありおよそ 2.5 倍高速である．また，$n = 19$ は $B = 1$ について式 (3) を満たす最大の拡大次数 n，$n = 61$ は $B = 2$ について式 (3) を満たす最大の n であるため，ある B に対して式 (3) を満たす最大の n となる $\mathrm{GF}(3^{6n})$ 上の DLP に対しては，[JL06] が [JL02] よりも数倍程度高速である可能性がある．

4.4 $\mathrm{GF}(3^{6\cdot 61})$ 上の DLP の計算

上記の実験の結果，パラメータ $B = 2$ で計算可能な DLP については我々の実装で計算可能であるので，$B = 2$ で計算できる最大の n である $n = 61$ において，$\mathrm{GF}(3^{6n})$ 上の DLP の計算を行った．本稿投稿時（2009 年 9 月 4 日）には関係探索ステップの計算のみ終了しており，線形代数ステップの計算は終了していない．このため，線形代数ステップについては終了する日数を以下に見積もった．

関係探索ステップの計算環境は 4.3 節と同様

である．この計算では全ての探索範囲を探索せず，必要な個数の関係を得られた時点で関係探索を終了した．およそ 24 日間の計算を行い，必要な関係の個数 531,806 個に対し 549,530 個の関係が得られた．

線形代数ステップの計算は Intel Quad-Core Xeon E5440 (2.83GHz) × 2 CPU, 16GB RAM を搭載したノード 4 台（32 コア）を Gigabit Ethernet で接続した環境で行った．$549,530 \times 531,806$ の行列に対し前処理として SGE を行い，$531,512 \times 531,512$ に削減した．この線形方程式を Lanczos 法を用いて計算を行っている．Lanczos 法の 1 回の反復におよそ 3.5 秒を要し，反復回数の最大値は行列の列数のため，線形代数ステップ全体では最大 21 日程度かかると予想される．

5 まとめ

本稿では，高速実装が可能な η_T ペアリングで用いられる $\mathrm{GF}(3^{6n})$（n: 素数）において，2006 年に Joux, Lercier によって提案された新たな関数体篩法 [12] の実装を行い，従来の関数体篩法 [11] との計算実験による比較を行った．結果，パラメータ B に対し $(B+1) \geq \sqrt{n/B}\log(n/B)$ を満たす最大の n（$n = 19, 61$ など）において，従来の関数体篩法よりも数倍程度高速に離散対数問題の計算が可能であることを確認した．

謝辞: 本研究の一部は，CRYPTREC(`http://www.cryptrec.go.jp`) の支援を受け，NICT セキュリティ基盤グループとの共同研究の一環として実施された．

参考文献

[1] L. M. Adleman. The function field sieve. *ANTS-I*, *Lecture Notes in Comput. Sci.*, Vol. 877, pp. 108–121, 1994.

[2] K. Aoki, T. Shimoyama, and H. Ueda. Experiments on the linear algebra step in the number field sieve. *IWSEC2007*, *Lecture Notes in Comput. Sci.*, Vol. 4752, pp. 58–73, 2007.

[3] 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.

[4] 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.

[5] D. Boneh and M. Franklin. Identity based encryption from the weil pairing. *SIAM J. Comput.*, Vol. 32, No. 3, pp. 586–615, 2003.

[6] D. M. Gordon and K. S. McCurley. Massively parallel computation of discrete logarithms. *CRYPTO' 92*, *Lecture Notes in Comput. Sci.*, Vol. 740, pp. 312–323, 1992.

[7] R. Granger, A. J. Holt, D. Page, N. P. Smart, and F. Vercauteren. Function field sieve in characteristic three. *ANTS-VI*, *Lecture Notes in Comput. Sci.*, Vol. 3076, pp. 223–234, 2004.

[8] 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.

[9] 林卓也，白勢政明，高木剛．$\mathrm{GF}(3^n)$ 上の関数体篩法における篩処理の実装実験． *SCIS2009*, 3F1-1, 2009.

[10] A. Joux, et al. Discrete logarithms in $\mathrm{GF}(2^{607})$ and $\mathrm{GF}(2^{613})$. 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.

[11] A. Joux and R. Lercier. The function field sieve is quite special. *ANTS-V*, *Lecture Notes in Comput. Sci.*, Vol. 2369, pp. 431–445, 2002.

[12] A. Joux and R. Lercier. The function field sieve in the medium prime case. *EUROCRYPT 2006*, *Lecture Notes in Comput. Sci.*, Vol. 4004, pp. 254–270, 2006.

[13] B. A. LaMacchia and A. M. Odlyzko. Solving large sparse linear systems over finite fields. *CRYPTO' 90*, *Lecture Notes in Comput. Sci.*, Vol. 537, pp. 109–133, 1991.

[14] 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.

[15] J. Pollard. The lattice sieve. In *The Development of the Number Field Sieve*, *Lecture Notes in Math.*, Vol. 1554, pp. 43–49, 1991.

[16] 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.