Key Length Estimation of Pairing-based Cryptosystems using η_T Pairing

Naoyuki Shinohara[1], Takeshi Shimoyama[2], Takuya Hayashi[3], and Tsuyoshi Takagi[3]

[1] National Institute of Information and Communications Technology,
[2] FUJITSU LABORATORIES Ltd.,
[3] Kyushu University.

Abstract. The security of pairing-based cryptosystems depends on the difficulty of the discrete logarithm problem (DLP) over certain types of finite fields. One of the most efficient algorithms for computing a pairing is the η_T pairing over supersingular curves on finite fields whose characteristic is 3. Indeed many high-speed implementations of this pairing have been reported, and it is an attractive candidate for practical deployment of pairing-based cryptosystems. The embedding degree of the η_T pairing is 6, so we deal with the difficulty of a DLP over the finite field $GF(3^{6n})$, where the function field sieve (FFS) is known as the asymptotically fastest algorithm of solving it. Moreover, several efficient algorithms are employed for implementation of the FFS, such as the large prime variation. In this paper, we estimate the time complexity of solving the DLP for the extension degrees $n = 97, 163, 193, 239, 313, 353, 509$, when we use the improved FFS. To accomplish our aim, we present several new computable estimation formulas to compute the explicit number of special polynomials used in the improved FFS. Our estimation contributes to the evaluation for the key length of pairing-based cryptosystems using the η_T pairing.

Keywords: pairing-based cryptosystems, discrete logarithm problem, finite field, key length, suitable values

1 Introduction

Pairing-based cryptosystems such as identity-based encryption [9] have recently become one of the main research topics in cryptography. Their security is based on the intractability of the discrete logarithm problem (DLP) over certain types of finite fields. Once the underlying DLP is broken, the pairing-based cryptosystems are no longer secure. Therefore, evaluating the intractability of a DLP is an important task.

One of the most efficient algorithms for computing a pairing is the η_T pairing defined over supersingular curves on finite fields whose characteristic is 3 [7]. Many high-speed implementations of the η_T pairing have been reported in previous literature [4, 8, 15, 16, 22], and there are many efficient algorithms for Tate pairing over finite fields whose characteristic is 3 [6, 11, 12, 17, 24, 28]. The timings reported in the literature are appealing for using the η_T pairing in practices; therefore in this paper we deal with the DLP over finite fields whose characteristic is 3. Moreover, since the embedding degree of the η_T pairing is 6, we are interested in finite fields $GF(3^{6n})$ for some integers n.

In this paper, we try to estimate the time complexity of solving the DLP over $GF(3^{6n})$ for extension degrees $n = 97$, 163, 193, 239, 313, 353, 509, using the following background facts. In 2010, Hayashi et al. solved a 676-bit DLP (over $GF(3^{6\cdot 71})$) [18]. Joux and Lercier estimated that the time complexity of solving the DLP over $GF(3^{6\cdot 97})$ is around 2^{71} [21]. And Smart et al. showed that the difficulty of solving the DLP over $GF(3^{6\cdot 193})$ is roughly equivalent to that of factoring a 1024-bit RSA key (80-bit security) [30]. NIST recommended using a key size of more than 80 bits after 2011 [5]. Ahmadi et al. assumed that the DLP with $n = 509$ has the security level of 128 bits [4].

To estimate the time complexity, we consider an efficient algorithm to solve a DLP over $GF(3^{6n})$. Adleman proposed the function field sieve (FFS) to practically solve a DLP over finite fields whose characteristic is small [1, 3]. The time complexity of the FFS for a DLP over $GF(3^{6n})$ is asymptotically

$$L_{3^{6n}}[1/3, (32/9)^{1/3}] = \exp(((32/9)^{1/3} + o(1))(\log 3^{6n})^{1/3}(\log\log 3^{6n})^{2/3}),$$

Table 1. Estimation of the time complexity of solving DLP over $GF(3^{6n})$

n	97	163	193	239	313	353	509
$\log_2 C_{sieve}$	52.79	68.17	71.90	78.14	90.04	94.42	111.35

n: extension degree of the field $GF(3^{6n})$ over its base field $GF(3^6)$.
C_{sieve}: computational cost of the sieving step of the improved FFS
(In this paper, we ultimately regard C_{sieve} as the time complexity of solving the DLP over $GF(3^{6n})$.)

for $n \to \infty$. In 2002, Joux and Lercier proposed a practical improvement of the FFS called JL02-FFS [20], and in 2006 another new variant of the FFS (JL06-FFS) for $GF(q)$, where the characteristic is small and q is a medium-sized prime power [21]. Hayashi et al. reported that JL06-FFS has an advantage over JL02-FFS when we try to solve a DLP over $GF(3^{6n})$ [18]. Additionally, there are well-known efficient algorithms for implementation of JL06-FFS: the large prime variation [26], the lattice sieve [27], the filtering [10], the Galois action [18] and the free relation [18]. Thus, we estimate the time complexity of solving a over $GF(3^{6n})$ by JL06-FFS with these efficient algorithms. We call this FFS "the improved FFS" in this paper.

There is an elemental parameter $(\kappa, d_H, d_m, B, R, S)$ commonly-utilize in JL06-FFS (FFS) and the improved FFS. There is also an advanced parameter (λ, θ, β) for the improved FFS, where λ is for the large prime variation, θ for the lattice sieve, and β for the filtering. For our estimation of the time complexity, we require the value of the parameter $(\kappa, d_H, d_m, B, R, S, \lambda, \theta, \beta)$, such that the computational cost of the improved FFS is almost minimum, when the extension degrees n are fixed. In this paper, such values are called the "suitable values" of $(\kappa, d_H, d_m, B, R, S, \lambda, \theta, \beta)$. To find suitable values for the fixed extension degrees n, we performed an experiment via a personal computer with an Intel Quad-Core (2.8 GHz) CPU and 8 GB RAM, and it took roughly 57 hours. Specifically, we checked certain computable criteria to solve a DLP with the improved FFS, changing the values of $(\kappa, d_H, d_m, B, R, S, \lambda, \theta, \beta)$. The criteria are checkable by using our new formulas (22), etc., which are extended from Granger's formula [13]. (Section 5 provides details on our experiment.)

Through the experiment we obtained Table 3 of the suitable values, and were able to eventually regard the computational cost C_{sieve} of the sieving step of the improved FFS as the time complexity of solving the DLP over $GF(3^{6n})$. On the strength of the costs C_{sieve}, we present Table 1 of the time complexity estimation of solving the DLP over $GF(3^{6n})$.

The hardness of the DLP over $GF(3^{6 \cdot 509})$ was estimated to be equivalent to 128-bit security [4], however, the DLP over $GF(3^{6 \cdot 509})$ actually accomplishes only about 111-bit security. To safely utilize a cryptographic schemes with η_T pairing over $GF(3^n)$, we must be aware of this fact.

2 Outline of function field sieve

This section briefly explains the importance of the discrete logarithm problem (DLP) of $GF(3^{6n})$ where n is prime. It is well known that a function field sieve (FFS) is the most efficient method for solving a DLP of a finite field, so we provide an overview of it.

2.1 DLP and η_T pairing

We first refer to a discrete logarithm (DLP) over the multiplicative group $GF(3^{6n})^*$. Let g be a generator of the multiplicative group $GF(3^{6n})^*$ and $A \in \langle g \rangle$. We then try to solve the DLP over $\langle g \rangle$; namely, we compute the smallest positive integer $\log_g A$ such that $g^{\log_g A} = A$.

It is expected that the η_T paring over the supersingular curve on $GF(3^n)$ realizes practical pairing-based cryptosystems. The safety of these cryptosystems is based on the difficulty of the DLP over $GF(3^{6n})$, since the map η_T is a bilinear map from $G_1 \times G_2$ to $GF(3^{6n})$, where G_1 and G_2 are cyclic groups. For example, let α be a secret integer such that $v_1 = [\alpha]v_2$ for given $v_1, v_2 \in G_1$. We then prepare arbitrary $w \in G_2$ and compute $\eta_T(v_1, w), \eta_T(v_2, w)$. Since $\eta_T(v_1, w) = \eta_T([\alpha]v_2, w) = \eta_T(v_2, w)^\alpha \in GF(3^{6n})^*$, we can obtain α by solving the DLP over $GF(3^{6n})^*$.

2.2 FFS

There are several variants of FFS. Adleman proposed the first FFS in 1994 [1], and Adleman and Huang later proposed a practical FFS [3]. Joux and Lercier proposed two more practical FFS's; JL02-FFS [20] and JL06-FFS [21]. Hayashi et al. reported that JL06-FFS has an advantage over JL02-FFS in solving a DLP over $GF(3^{6n})$ [18], so we introduce JL06-FFS. From this section, FFS means JL06-FFS.

We begin with an overview of the FFS, and suppose that we try to obtain $\log_g A$ in this section. This consists of four steps: polynomial selection, sieving, linear algebra, and individual logarithm. The parameter $(\kappa, d_H, d_m, B, R, S)$ of FFS is called the elemental parameter of the FFS.

Polynomial selection : Let κ be the extension degree of the coefficient field of $GF(3^\kappa)[x]$, where $\kappa = 1, 2, 3, 6$. We select a monic irreducible polynomial $f \in GF(3^\kappa)[x]$, a polynomial $m \in GF(3^\kappa)[x]$, and a bivariate polynomial $H(x, y) = x + y^{d_H} \in GF(3^\kappa)[x, y]$ such that

$$H(x, m) \equiv 0 \pmod f, \ \deg f = 6n/\kappa. \tag{1}$$

Note that, by letting d_m be $\deg m$, the following property holds:

$$d_m \cdot d_H \geq \deg f. \tag{2}$$

Then the finite field $GF(3^{6n})$ is described as $GF(3^\kappa)[x]/(f)$. And $H(x, y)$ satisfies the eight conditions proposed by Adleman [1]. There is a surjective homomorphism

$$\Phi : \begin{cases} GF(3^\kappa)[x, y]/(H) & \rightarrow & GF(3^{6n}) \cong GF(3^\kappa)[x]/(f) \\ \qquad y & \mapsto & m. \end{cases}$$

Here we select the smoothness bound B and define a rational factor base $\bar{F}(B)$ and an algebraic factor base $\hat{F}(B)$ as follows:

$$\begin{aligned} \bar{F}(B) &= \{\mathfrak{p} \in GF(3^\kappa)[x] \mid \deg(\mathfrak{p}) \leq B, \, \mathfrak{p} \text{ is monic irreducible}\}, \\ \hat{F}(B) &= \{\langle \mathfrak{p}, y - t\rangle \in \mathrm{Div}(GF(3^\kappa)[x, y]/(H)) \mid \mathfrak{p} \in \bar{F}(B), \, H(x, t) \equiv 0 \pmod{\mathfrak{p}}\}, \end{aligned}$$

where $\mathrm{Div}(GF(3^\kappa)[x, y]/(H))$ is the divisor group of $GF(3^\kappa)[x, y]/(H)$ and $\langle \mathfrak{p}, y - t\rangle$ is a divisor generated by $\mathfrak{p}$ and $y - t$.

Sieving: For given positive integers R, S, we find pairs $(r, s) \in (GF(3^\kappa)[x])^2$ such that

$$\deg r \leq R, \, \deg s \leq S, \, \gcd(r, s) = 1, \, r \text{ is monic}, \tag{3}$$

$$rm + s = \prod_{\mathfrak{p}_i \in \bar{F}(B)} \mathfrak{p}_i^{a_i} \tag{4}$$

$$\langle ry + s\rangle = \sum_{\langle \mathfrak{p}_j, y - t_j\rangle \in \hat{F}(B)} b_j \langle \mathfrak{p}_j, y - t_j\rangle \tag{5}$$

by a sieving algorithm. The property (5) can be translated into the following equation:

$$(-r)^{d_H} H(x,\, -s/r) = (-r)^{d_H} x + s^{d_H} = \prod_{\langle \mathfrak{p}_j, y-t_j\rangle \in \hat{F}(B)} \mathfrak{p}_j^{b_j}. \tag{6}$$

Thus, in particular, we collect $(r,\, s)$ satisfying (3), (4) and (6). And such $(r,\, s)$ is called a B-smooth pair. Here, we assume $(3^{6n}-1)/(3^{\kappa}-1)$ is comprime to h which is the class number of the quotient field of $GF(3^{\kappa})(x)[y]/(H)$. Then, we obtain the following congruent:

$$\sum_{\mathfrak{p}_i \in \bar{F}(B)} a_i \log_g \mathfrak{p}_i \equiv \sum_{\langle \mathfrak{p}_j, y-t_j\rangle \in \hat{F}(B)} b_j \log_g \kappa_j \pmod{(3^{6n}-1)/(3^{\kappa}-1)}, \tag{7}$$

where $\kappa_j = \Phi(\lambda_j)^{1/h}$, $\langle \lambda_j \rangle = h\langle \mathfrak{p}_j,\, y-t_j\rangle$. The congruent (7) is called a *relation.* Let $\mathcal{R}_{sieve}$ be the number of relations obtained in the sieving step, and then we require the following criteria that

$$\mathcal{R}_{sieve} \geq (\#\bar{F}(B) + \#\hat{F}(B)). \tag{8}$$

Linear algebra: After generating a linear equation from relations, we translate it into a smaller linear equation by an algorithm such as the filtering. The smaller one is solved via an algorithm such as the Lanczos method [2, 25], and then we obtain

$$\log_g \mathfrak{p}_1, ..., \log_g \mathfrak{p}_{\#\bar{F}(B)}, \log_g \kappa_1, ..., \log_g \kappa_{\#\hat{F}(B)}.$$

Individual logarithm: Using the special-Q descent method [21], we compute integers e_i, f_j such that

$$\log_g A \equiv \sum_{\mathfrak{p}_i \in \bar{F}(B)} e_i \log_g \mathfrak{p}_i + \sum_{\langle \mathfrak{p}_j, y-t_j\rangle \in \hat{F}(B)} f_j \log_g \kappa_j \pmod{(3^{6n}-1)/(3^{\kappa}-1)}.$$

Then we obtain the discrete logarithm $\log_g A$.

3 Known evaluation methods

The computational cost of FFS is greatly influenced by the parameter selection of the FFS. For example, if we add only 1 to the value of the parameter R of the FFS given in equation (3), the computational cost of sieving increases 3^{κ}-fold. Therefore, the value of the parameter of the FFS must be meticulously selected.

The elemental parameter $(\kappa,\, d_H,\, d_m,\, B,\, R,\, S)$ of the FFS is given in section 2.2. For a fixed pair $(n,\, \kappa)$, there is a well known method for evaluating the value of the parameter, such that the computational cost of solving our DLP by FFS is estimated as approximately minimum. Such parameter values are called "suitable values" in this paper. (Note that it is difficult to identify the most suitable values, namely the value of parameters of FFS for which the cost is truly the minimum.) In general, an approximate suitable value is actually adopted to solve a DLP by FFS. However, we expect there might be more suitable values around the approximate one. For our aim, we introduce a sharp probability evaluation method in section 4.3 by extending Granger's method. Therefore, in this section, we explain how to compute the approximate suitable values, and Granger's method.

Table 2. Approximate suitable values of elemental parameter of FFS

n	97				163				193				239				313				353				509			
κ	1	2	3	6	1	2	3	6	1	2	3	6	1	2	3	6	1	2	3	6	1	2	3	6	1	2	3	6
d_H	6	6	6	6	7	7	7	7	7	7	7	7	8	8	8	8	8	8	8	8	9	9	9	9	10	10	10	10
d_m	97	49	33	17	140	70	47	24	166	83	56	28	180	90	60	30	235	118	79	40	236	118	79	40	306	153	102	51
B	18	9	6	3	23	11	7	4	24	12	8	4	27	13	9	4	30	15	10	5	31	16	10	5	37	18	12	6
R	18	9	6	3	23	11	7	4	24	12	8	4	27	13	9	4	30	15	10	5	31	16	10	5	37	18	12	6
S	18	9	6	3	23	11	7	4	24	12	8	4	27	13	9	4	30	15	10	5	31	16	10	5	37	18	12	6

n: extension degree of the field $GF(3^{6n})$ over its base field $GF(3^6)$
κ: extension degree of the coefficient field of $GF(3^\kappa)[x]$ such that $GF(3^{6n}) \simeq GF(3^\kappa)[x]/(f)$, where $f \in GF(3^\kappa)[x]$ is a monic irreducible polynomial of degree $6n/\kappa$
d_H: degree in y of the bivariate polynomial $H(x,y) = x + y^{d_H} \in GF(3^\kappa)[x,y]$ used for FFS
d_m: degree of the polynomial m in $GF(3^\kappa)[x]$ such that $H(x,m) \equiv 0 \pmod f$
B: smoothness bound for FFS
R: maximum degree of polynomial $r \in GF(3^\kappa)[x]$ used in the sieving step of FFS
S: maximum degree of polynomial $s \in GF(3^\kappa)[x]$ used in the sieving step of FFS

3.1 Asymptotic evaluation formulas

From asymptotic analysis in [21], when we solve a DLP over a finite field $GF(3^\kappa)[x]/(f)$ for given integers $\kappa, \deg f$ by FFS, the smallest positive integer satisfying (9) is generally selected as the value of B:

$$(B+1)\log 3^\kappa \geq \sqrt{\frac{\deg f}{B}} \log \frac{\deg f}{B}. \tag{9}$$

We then assume that $R = S = B$ and

$$d_H = \left\lceil \sqrt{\deg f / B} \right\rceil. \tag{10}$$

We also calculate the smallest integer d_m satisfying (2) for the given d_H and $\deg f$. We then have Table 2 of approximate suitable values of the elemental parameter of FFS.

3.2 Granger's evaluation formula

Granger proposed a sharp evaluation formula in (15) to estimate the running time of FFS. By extending ρ_1 in (15) we obtain our new functions ρ_2 and ρ_3 in section 4.3. Here we briefly explain Granger's method, and more detail is given in [13].

There is a problem about deciding on the smoothness bound B of factor bases $\bar{F}(B)$ and $\hat{F}(B)$. The numbers of factor bases increase exponentially, and take discrete values since B is an integer. To correct this problem, Granger naturally extends B-smooth to (B,β)-smooth with a new parameter $\beta \in (0,1]$. The new parameter β means the ratio of the number of polynomials in $\bar{F}(B)$ of degree B to that of all monic irreducible polynomials in $GF(3^\kappa)[x]$ of degree B.

In fact, factor bases $\bar{F}(B)$ and $\hat{F}(B)$ are extended to $\bar{F}(B,\beta)$ and $\bar{F}(B,\beta)$ such that

$$\bar{F}(B,\beta) = \bar{\Lambda} \sqcup \bar{F}(B-1),\ \hat{F}(B,\beta) = \hat{\Lambda} \sqcup \hat{F}(B-1),$$

where $\bar{\Lambda} \subset \bar{F}(B)$, $\hat{\Lambda} \subset \hat{F}(B)$ and the degree of an element in $\bar{\Lambda}$ or $\hat{\Lambda}$ is B. Elements of $\bar{\Lambda}$ and $\hat{\Lambda}$ are called large primes. We call a monic polynomial g in the rational side (B,β)-smooth if every prime factor of g is in the factor base $\bar{F}(B,\beta)$. In the same manner as the rational side, (B,β)-smooth is also introduced in the algebraic side. Therefore, B-smooth pair in section 2.2 can be naturally extended to (B, β)-smooth pair. In fact, a pair (r, s) is said to be a (B, β)-smooth pair if the (r, s) satisfies (3) and the following properties that

$$rm + s = \prod_{\mathfrak{p}_i \in \bar{F}(B-1)} \mathfrak{p}_i^{a_i} \prod_{\mathfrak{P}_j \in \bar{A}} \mathfrak{P}_j^{a_j}, \tag{11}$$

$$(-r)^{d_H} x + s^{d_H} = \prod_{\langle \mathfrak{p}_i, y-t_i \rangle \in \hat{F}(B-1)} \mathfrak{p}_i^{b_i} \prod_{\langle \mathfrak{P}_j, y-t_j \rangle \in \hat{A}} \mathfrak{P}_j^{b_j}, \tag{12}$$

which correspond to (4) and (6) respectively.

The criteria (8) is described as

$$\mathcal{R}_{sieve} \geq 2\#\bar{F}(B,\, \beta), \tag{13}$$

since $\bar{F}(B, \beta)$ and $\hat{F}(B, \beta)$ have almost the same cardinality in practice. For checking this criteria, Granger proposed two formulas to compute $\mathcal{R}_{sieve}$ and $\#\bar{F}(B, \beta)$. First, we discuss how to compute $\#\bar{F}(B, \beta)$. Let $I_q(k)$ be the number of monic irreducible polynomials in $GF(q)$ of degree k. $I_q(k)$ is computable by the equation $I_q(k) = \frac{1}{k} \sum_{d \mid k} \mu(d) q^{k/d}$, where μ is the *mobius function*. We then have the following formula:

$$\#\bar{F}(B, \beta) = \sum_{k=1}^{B-1} I_q(k) + \lfloor \beta I_q(B) \rfloor. \tag{14}$$

Next we consider $\mathcal{R}_{sieve}$, namely the number of (B, β)-smooth pairs (r, s) collected in the sieving step. Let $\rho_1(q,\, B, \beta, k)$ be the probability that a monic polynomial in $GF(q)[x]$ of degree k is (B, β)-smooth. For given non-negative integers $i,\, j$, let $\bar{a}_{i,j}$ be the number of pairs (r, s) satisfying (3). We denote $D_{NR}(i, j)$, $D_{NA}(i, j)$ by the degrees of $rm + s$ and $(-r)^{d_H} x + s^{d_H}$ respectively, where $i = \deg r$ and $j = \deg s$. Then $\mathcal{R}_{sieve}$ is described as

$$\sum_{i=0}^{R} \sum_{j=0}^{S} \rho_1(q,\, B, \beta, D_{NR}(i, j)) \rho_1(q,\, B, \beta, D_{NA}(i, j)) \bar{a}_{i,j}, \tag{15}$$

and the function $\bar{a}_{i,j}$ is given in Appendix A.

4 New evaluation formulas for efficient implementation of FFS

To solve the DLP over $GF(3^{6n})$ for $n \geq 97$, we employ several efficient algorithms for implementation of the FFS; the large prime variation [26], the lattice sieve [27], the filtering [10], the Galois action [18], and the free relation [18]. These algorithms are not considered in Granger's method. Especially, for the lattice sieve and the large prime variation, new parameters θ and λ are respectively introduced. We extend Granger's formula for the FFS with those efficient algorithms. (We call this FFS the "improved FFS.") Then the number $\mathcal{R}_{sieve}$ of the relations given by the sieving step of the improved FFS is computable by exchanging ρ_1 in (15) with our new formulas ρ_2 and ρ_3 in section 4.3. As mentioned in section 3.2, we also suppose that $\bar{F}(B, \beta)$ and $\hat{F}(B, \beta)$ have almost the same cardinality in this section.

4.1 Well-used efficient algorithms for FFS

This section provides brief explanations of efficient algorithms.

Large prime variation : the large prime variation is employed to reduce the computational cost of a sieving algorithm. To provide a simple explanation, we discuss only in rational side. On the algebraic side, the same discussion can be made.

In fact, we sieve with all factors $\mathfrak{p} \in \bar{F}(B,\beta)$ where $\deg \mathfrak{p} \le B-1$ not B; namely, we aim to effectively collect pairs (r,s) such that $rm+s$ is (B,β)-smooth with high probability. For a pair (r,s), $rm+s$ is separated into the two products $\mathcal{P}$ and $\mathcal{Q}$ such that $\mathcal{P} = \prod_{\deg \mathfrak{p}_i \le B-1} \mathfrak{p}_i^{a_i}$, $\mathcal{Q} = \prod_{\deg \mathfrak{q}_j \ge B} \mathfrak{q}_j^{a_j}$, where $\mathfrak{p}_i$, $\mathfrak{q}_j \in GF(3^\kappa)[x]$ are irreducible. We can compute $\deg \mathcal{Q} = \deg(rm+s) - \deg \mathcal{P}$ effectively since $\deg \mathcal{P}$ is easily computable by sieving. If $\deg \mathcal{Q}$ is small enough, the $rm+s$ is (B,β)-smooth with high probability. Therefore, we prepare a threshold value $\lambda B \in \mathbf{Z}$, and eliminate (r,s) for which $\deg \mathcal{Q}$ is larger than λB. Hence the most suitable value of λ is required.

Lattice sieve: Sieving in the lattice sieve is performed for only every (r,s) such that $rm+s$ (resp. $\langle ry+s \rangle$) is divisible by a fixed $Q \in \bar{\Lambda}$ (resp. $Q \in \hat{\Lambda}$). Such Q is called *special-Q*. It is usually chosen from $\hat{\Lambda}$ if $D_{NR}(R,S) < D_{NA}(R,S)$, where functions D_{NR} and D_{NA} are defined in section 3.2, and otherwise from $\bar{\Lambda}$. Let $\bar{\Theta}$ (resp. $\hat{\Theta}$) be the set of special-Q's on the rational side (resp. algebraic side). We then have that $\bar{\Theta} \subset \bar{\Lambda}$ and $\hat{\Theta} \subset \hat{\Lambda}$. Therefore, by letting θ be the ratio of the number of special-Q's to $\#(\bar{F}(B) \backslash \bar{F}(B-1))$ (resp. $\#(\hat{F}(B) \backslash \hat{F}(B-1))$), it holds that $0 < \theta \le \beta \le 1$. Moreover, the number of special-Q's is $\lfloor \theta I_{3^\kappa}(B) \rfloor$.

When we use the lattice sieve, (r,s) is represented as $c(r_1,s_1)+d(r_2,s_2)$, where $c,d,r_1,s_1,r_2,s_2 \in GF(3^\kappa)[x]$. Sieving is then performed on the c-d plane. The size of the c-d plane is roughly estimated at about $3^{\kappa(R+S+1-B)}$, since the degrees of r_1, s_1, r_2, and s_2 are about $B/2$ in most cases. The time complexity of the lattice sieve depends on the frequency of memory access, and the frequency is proportional to the size of the c-d plane. Therefore, we can assume that the complexity of sieving for one special-Q is almost the same as the size of c-d plane. Sieving is performed on both the rational side and algebraic side, so the complexity C_{sieve} of sieving in the lattice sieve is described as

$$2 \cdot 3^{\kappa(R+S+1-B)} \lfloor \theta I_{3^\kappa}(B) \rfloor. \tag{16}$$

In practice, to collect relations efficiently, sieving is performed with $\mathfrak{p} \in \bar{F}(B)$ and $\mathfrak{p} \in \hat{F}(B)$, not $\bar{F}(B,\beta)$ and $\hat{F}(B,\beta)$. After sieving, $\bar{F}(B)$ and $\hat{F}(B)$ are reduced to $\bar{F}(B,\beta)$ and $\hat{F}(B,\beta)$ via singleton and clique in the filtering described below.

Filtering: In the linear algebra step, the filtering [10] removes inessential variables and equations to solve the linear equation efficiently. It consists of three phases. The singleton phase removes an equation containing a variable whose frequency is one in the linear equation (such an equation is called *singleton.*) The clique phase deletes excess equations to produce more singletons. And the merge phase combines equations to produce singletons. The singleton phase and clique phase need little computation, and the merge phase needs a great deal. In order to produce many singletons in the clique phase, it is better to gather more relations. If we find many singletons, the number of variables in the linear equation can be reduced. Then the linear equation can be solved faster.

The explanation of the lattice sieve mentions that sieving is performed with $\bar{F}(B)$ and $\hat{F}(B)$. After that, we reduce variables in these factor bases by filtering. In most cases, a reduced variable corresponds to some large prime, so we estimate that the size of the matrix is $2\#\bar{F}(B,\beta)$.

Free relation: By using the free relation, we can obtain a relation virtually for free, without the sieving. Details of the method are discussed in [18], and the advantage is as follows. Let $\mathcal{R}_{free}$ be the number free relations. Then the following property holds:

$$\mathcal{R}_{free} \approx \begin{cases} \#\hat{F}(B)/d_H & \text{if } \gcd(d_H,3)=1 \\ \#\hat{F}(B)/2 & \text{if } d_H = 2,\ 6 \\ \#\hat{F}(B) & \text{if } d_H = 3,\ 9 \end{cases} \tag{17}$$

where $d_H \leq 10$. It seems that the suitable value of d_H is divisible by 3, so we check both cases where d_H is an approximate value and an integer divisible by 3. We therefore must pay attention to the selection of d_H.

Galois action: Via the Galois action, we can reduce the size of the matrix from $2\#\bar{F}(B,\beta)$ to $2\#\bar{F}(B,\beta)/\kappa$. Therefore, the computational cost C_{linear} of the linear algebra step is described as

$$C_{linear} = \left(\frac{2\#\bar{F}(B,\beta)}{\kappa}\right)^2. \tag{18}$$

In order to use the Galois action, a primitive polynomial $f \in GF(3^\kappa)[x]$ is selected so that all coefficients of f are in $GF(3)$. Then x is fixed by a function $\phi : x \mapsto x^{3^{6n/\kappa}}$ but $c \in GF(3^\kappa) \setminus GF(3)$ is not. This means that the logarithm of the element of the factor base $\mathfrak{p}$ that has at least one coefficient in $GF(3^\kappa) \setminus GF(3)$ corresponds to the logarithm of the other element of the factor base $\phi(\mathfrak{p})$ as $3^{6n/\kappa} \log_g \mathfrak{p} \equiv \log_g \phi(\mathfrak{p})$. Since the order of ϕ is κ, the number of variables in the linear algebra step can be reduced about $1/\kappa$ times itself.

4.2 Criteria for sufficient number of relations

In the same manner in section 3.2, we change criteria (8). In fact, (13) is changed for FFS with five efficient algorithms in section 4.1. First, since we use the free relation, (13) is translated into $\mathcal{R}_{sieve} + \mathcal{R}_{free} \geq 2\#\bar{F}(B,\beta)$. With consideration for the filtering, it is better to collect more relations[4], so we assume that the constraint property is that $\mathcal{R}_{sieve} + \mathcal{R}_{free} \geq 4\#\bar{F}(B,\beta)$. Finally, applying the Galois action, it is translated into

$$\mathcal{R}_{sieve} + \mathcal{R}_{free} \geq \frac{4\#\bar{F}(B,\beta)}{\kappa}. \tag{19}$$

To solve the DLP in our case, the values of parameters of the improved FFS must satisfy (19).

4.3 New evaluation formulas

New evaluation formulas enable us to estimate the complexity of the improved FFS by considering the parameters, κ, d_H, d_m in the polynomial selection step, B, R, S in the sieving step, λ for the large prime variation, θ for the lattice sieve, and β for the filtering. As discussed in section 3.2, Granger gave the evaluation formula ρ_1 to compute the number $\mathcal{R}_{sieve}$ of the relations. On the other hand, with consideration for the large prime variation and the lattice sieve, we introduce new evaluation formulas ρ_2 and ρ_3 for (B,β,λ)-smooth and (B,β,λ,Θ)-smooth, which are variants of (B,β)-smooth, respectively.

Granger considers a case employing the FFS with (B,β)-smooth, so he requires the number of (r,s) satisfying (3), (11), and (12). However, we consider the improved FFS. Therefore, if $D_{NR}(R,S) < D_{NA}(R,S)$, we require the number of (r,s) satisfying (3) and the following properties

$$rm + s = (\prod_{\mathfrak{p}_i \in \bar{F}(B-1)} \mathfrak{p}_i^{e_i})(\prod_{\mathfrak{P}_j \in \bar{\Lambda}} \mathfrak{P}_j^{e_j}),\ (\text{where } e_i, e_j \geq 0,\ \sum e_j \leq \lambda) \tag{20}$$

and

$$(-r)^{d_H} x + (-s)^{d_H} = (\prod_{\langle \mathfrak{p}_i, y-t_i \rangle \in \hat{F}(B-1)} \mathfrak{p}_i^{e_i})(\prod_{\langle \mathfrak{P}_j, y-t_j \rangle \in \hat{\Lambda} \backslash \hat{\Theta}} \mathfrak{P}_j^{e_j})(\prod_{\langle \mathfrak{P}_\ell, y-t_\ell \rangle \in \hat{\Theta}} \mathfrak{P}_\ell^{e_\ell}) \tag{21}$$

[4] In [23] for the factorization of RSA768, the authors collected about two time more relations than the number of factor base.

where at least one e_ℓ is larger than 0 and $e_i, e_j \geq 0$, $\sum e_j + \sum e_\ell \leq \lambda$. Such $rm + s$ and $(-r)^{d_H} x + (-s)^{d_H}$ are called (B, β, λ)-smooth and $(B, \beta, \lambda, \hat{\Theta})$-smooth respectively. Conversely, if $D_{NR}(R, S) \geq D_{NA}(R, S)$, we search (r, s) such that $rm + s$ and are $(B, \beta, \lambda, \bar{\Theta})$-smooth and (B, β, λ)-smooth. In this paper, $(B, \beta, \lambda, \Theta)$-smooth means $(B, \beta, \lambda, \hat{\Theta})$-smooth if $D_{NR}(R, S) < D_{NA}(R, S)$, otherwise $(B, \beta, \lambda, \bar{\Theta})$-smooth.

In the same manner as Granger's method, we introduce two new formulas ρ_2 and ρ_3 of the probabilities for (B, β, λ)-smooth and $(B, \beta, \lambda, \Theta)$-smooth. The details are given in Appendix B. Let $\rho_2(q,\, B,\, \beta,\, \lambda,\, k)$ be the probability that a monic polynomial in $GF(q)[x]$ of degree k is (B, β, λ)-smooth. Then ρ_2 is described as follows:

$$\rho_2(q,\, B,\, \beta,\, \lambda,\, k) =$$
$$\frac{1}{q^k} \left\{ N_q(k, B-1) + \sum_{\ell \geq 1}^{\lfloor k/B \rfloor} N_q(k - \ell B, B-1) \left\{ \sum_{i=1}^{\min\{\ell, \lambda\}} \binom{\lfloor \beta I_q(B) \rfloor}{i} \binom{\ell - 1}{\ell - i} \right\} \right\}.$$

Let $\rho_3(q,\, B,\, \beta,\, \Theta,\, \lambda,\, k)$ be the probability that a monic polynomial $g \in GF(q)[x]$ of degree k is $(B,\, \beta,\, \Theta,\, \lambda)$-smooth. Then ρ_3 is described as follows:

$$\rho_3(q,\, B,\, \beta,\, \lambda,\, \Theta,\, k) =$$
$$\frac{1}{q^k} \sum_{\ell=1}^{\lfloor k/B \rfloor} N_q(k - \ell B, B-1) \left\{ \sum_{\ell_Q=1}^{\ell} \sum_{\lambda_Q=1}^{\min\{\ell_Q, \lambda, \#\Theta\}} \binom{\#\Theta}{\lambda_Q} \binom{\ell_Q - 1}{\ell_Q - \lambda_Q} \tau_{B,\beta,\lambda,\Theta}(\ell, \ell_Q, \lambda_Q) \right\}$$

where

$$\tau_{B,\beta,\lambda,\Theta}(\ell, \ell_Q, \lambda_Q) = \begin{cases} \sum_{\lambda_t=1}^{Min} \binom{\lfloor \beta I_q(B) \rfloor - \#\Theta}{\lambda_t} \binom{\ell - \ell_Q - 1}{\ell - \ell_Q - \lambda_t} & (Min \geq 1) \\ 1 & (\ell = \ell_Q), \\ 0 & (\text{others}), \end{cases}$$
$$Min = \min\{\ell - \ell_Q, \lambda - \lambda_Q, \lfloor \beta I_q(B) \rfloor - \#\Theta\}.$$

Consequently, we obtain the following theorem:

Theorem 1 *By replacing ρ_1 in the formula (15) with ρ_2, ρ_3, we have that*

$$\mathcal{R}_{sieve} = \sum_{i=0}^{R} \sum_{j=0}^{S} \rho_v(q,\, B, \beta, D_{NR}(i,j)) \rho_w(q,\, B, \beta, D_{NA}(i,j)) \bar{a}_{i,j}. \tag{22}$$

where (ρ_v, ρ_w) is (ρ_2, ρ_3) if $D_{AR}(R, S) > D_{NR}(R, S)$, and (ρ_3, ρ_2) otherwise.

To find suitable values of parameters of the improved FFS, we check the criteria (19) for a given value of the parameter $(\kappa, d_H, d_m, B, R, S, \lambda, \theta, \beta)$. Namely, with changing the value of the parameter, we compute $\mathcal{R}_{sieve}$, $\mathcal{R}_{free}$ and $\#\bar{F}(B, \beta)$ many times, by using (22), (17), and (14). (Note that, since we supposed that $\#\bar{F}(B, \beta) = \#\hat{F}(B, \beta)$, the value of (17) is given by (14).) When κ is small and n is large, it takes a long time to compute (22). However, if $\kappa \neq 1$ and $n \leq 509$, we can actually compute it. For example, in our experiments, it takes roughly about 57 hours to make Table 3, using a PC with an Intel Quad-Core (2.8 GHz) × 1 CPU and 8 GB RAM.

5 Estimation of key length

In order to estimate the key length of pairing-based cryptosystems for the fixed extension degrees $n = 97,\ 163,\ 193,\ 239,\ 313,\ 353,\ 509$, we estimate the time complexity of solving the DLP over $GF(3^{6n})$

by the FFS (introduced in section 2.2) with the five efficient algorithms in section 4.1. (This FFS with efficient algorithms is called the "improved FFS" in this paper.) The improved FFS has two kinds of parameters: the elemental parameter $(\kappa, d_H, d_m, B, R, S)$ commonly utilized in the FFS without efficient algorithms, and the advanced parameter (λ, θ, β) for the efficient algorithms, where λ, θ, and β are used for the large prime variation, the lattice sieve, and, the filtering, respectively. For our estimation of the time complexity, we search the values of parameter $(\kappa, d_H, d_m, B, R, S, \lambda, \theta, \beta)$, such that the computational cost C_{sieve} of solving the DLP by the improved FFS is almost minimum. Such parameter values are called "suitable values" in this paper. (Note that it is not realistic to identify the most suitable value of the parameter for fixed extension degrees n, since there are infinitely many values of $(\kappa, d_H, d_m, B, R, S, \lambda, \theta, \beta)$.) To find suitable values of $(\kappa, d_H, d_m, B, R, S, \lambda, \theta, \beta)$ for the fixed extension degrees n, we performed an experiment to check the criteria (19) to solve the DLP, for many values of $(\kappa, d_H, d_m, B, R, S, \lambda, \theta, \beta)$. Criteria (19) is computable by using our new estimation formula (22) corresponding to the explicit number of the relations (defined in section 4.3), and so on. In this section, for the fixed extension degrees n, we present Table 5 of the suitable values of $(\kappa, d_H, d_m, B, R, S, \lambda, \theta, \beta)$ and the computational costs C_{sieve} when those suitable values are given. From Table 5, we obtain Table 1 meaning our estimation of the time complexity of solving the DLP over $GF(3^{6n})$, in section 1.

We performed an experiment to develop Table 5, using a PC with an Intel Quad-Core (2.8 GHz) × 1 CPU and 8 GB RAM. As mentioned in section 1, for fixed extension degrees n, we suppose that if there are more suitable values than the approximate ones in Table 2, they are close to those in Table 2. Therefore, we select several values of (d_H, d_m, B, R, S) around each value in Table 2. For example, if $(n, \kappa) = (193, 6)$, then the approximate suitable value of (d_H, d_m, B, R, S) is $(7, 28, 4, 4, 4)$. We select values of (d_H, d_m, B, R, S) such as $(7, 28, 4, 4, 4)$, $(7, 28, 4, 3, 4)$, $(7, 28, 4, 4, 5)$ and so on. For such a single value, we change the values of λ, β, θ many times in that order. (We have empirically confirmed that this order has no impact on the estimation of suitable values.) Then, to check the property (19) we compute (22), (17), and (14) for given values of $(d_H, d_m, B, R, S, \lambda, \theta, \beta)$.

From now, the value of $(n, \kappa, d_H, d_m, B, R, S)$ is fixed. Through experiments, we obtain the fact that the cost C_{sieve} of sieving decreases if λ increases, and there exists an integer λ_0 such that C_{sieve} does not decrease for any $\lambda \geq \lambda_0$. Therefore, λ_0 is the most suitable value of λ. To find the integer λ_0, the value of λ is started from 1 and in steps of 1 in our computation.

For a fixed λ, we move β from 1 to 0 in parts per 10^3, and next θ is also moved from the given β to 0 in parts per 10^5, since $0 < \theta \leq \beta \leq 1$. As mentioned in section 4.1, our sieving is performed with $\beta = 1$, so the cost C_{sieve} of sieving is given by the formula (16), where θ is minimum number such that (19) holds for $\theta \leq \beta = 1$. Such θ is described as θ_{min} in Table 5.

Next, we consider the cost C_{linear} of the linear algebra step. This is evaluated by the formula (18), and $2\#\bar{F}(B, \beta)/\kappa$ means the size of the matrix appearing in the linear algebra step. As mentioned in section 4.1, by the filtering, the size is reduced from $2\#\bar{F}(B)$ to $2\#\bar{F}(B, \beta)$. Therefore, we compute C_{linear} given by (18) for β_{min}, where β_{min} is explained as follows. For the explanation of β_{min}, we consider the case in which filtering is not employed. In other words, in the sieving step, we set β as small as possible under the condition that (19) holds. If we reduce the β, then the relations given by sieving decrease since the numbers of the factor bases decrease. We therefore must collect more relations by performing the lattice sieve more times. This implies that larger θ is required, so there exists the minimum β satisfying (19) since $0 < \theta \leq \beta \leq 1$. The β_{min} is denoted by the minimum β. If we set β smaller than β_{min}, then (19) does not hold, and so we suppose that the filtering reduces the size of the matrix from $2\#\bar{F}(B)$ to $2\#\bar{F}(B, \beta_{min})$.

In Table 5, we omit the case of $\kappa = 1$ for the following reason. For each pair (n, κ) where $n = 71, 79, 89, 97$ and $\kappa = 1, 2, 3, 6$, we check (19) for many values of parameter $(d_H$, d_m, B, R, S, θ, λ, $\beta)$. Then, for every fixed n, there are no suitable values when $\kappa = 1$. In other words, for each

Table 3. Suitable values of parameter of improved FFS to solve DLP over $GF(3^{6n})$

n	κ	d_H	d_m	B	R	S	λ	θ_{min}	β_{min}	$\log_2 C_{linear}$	$\log_2 C_{sieve}$
97	2	6	49	9	9	9	7	0.08436	0.420	49.06	54.49
	3	6	33	6	6	6	6	0.01392	0.281	47.49	53.95
	6	6	17	3	3	3	6	0.00011	0.225	46.44	52.79
163	2	7	70	11	12	12	7	0.03787	0.296	60.42	72.06
	3	7	47	7	8	8	8	0.01358	0.424	57.60	72.82
	6	7	24	4	4	4	5	0.00001	0.003	53.91	68.17
193	2	7	83	12	12	12	7	0.26513	0.727	68.49	74.74
	3	7	56	8	8	8	7	0.03672	0.471	67.00	74.06
	6	7	28	4	4	4	7	0.00017	0.230	64.69	71.90
239	2	8	90	13	14	14	7	0.06879	0.421	73.33	85.36
	3	8	60	9	9	9	7	0.01221	0.22	74.31	81.81
	6	8	30	4	4	4	8	0.01147	0.668	67.75	78.14
313	2	8	105	15	15	15	7	0.24041	0.653	86.59	93.11
	3	9	79	10	10	10	8	0.02541	0.391	84.87	92.31
	6	9	35	5	5	5	7	0.00010	0.173	82.25	90.04
353	2	9	118	16	16	16	7	0.09357	0.414	91.70	98.18
	3	9	79	10	11	11	8	0.01749	0.416	85.03	101.2
	6	9	40	5	5	5	8	0.00214	0.484	85.20	94.42
509	2	9	170	18	19	19	8	0.12474	0.547	104.67	117.45
	3	9	114	12	12	12	10	0.25254	0.847	105.43	114.30
	6	9	57	6	6	6	8	0.00061	0.342	102.69	111.35

n: extension degree of the field $GF(3^{6n})$ over its base field $GF(3^6)$
κ: extension degree of the coefficient field of $GF(3^\kappa)[x]$ such that $GF(3^{6n}) \simeq GF(3^\kappa)[x]/(f)$, where $f \in GF(3^\kappa)[x]$ is a monic irreducible polynomial of degree $6n/\kappa$

d_H: degree in y of the bivariate polynomial $H(x,y) = x + y^{d_H} \in GF(3^\kappa)[x,y]$ used for FFS

d_m: degree of the polynomial m in $GF(3^\kappa)[x]$ such that $H(x,m) \equiv 0 \pmod f$

B: smoothness bound for FFS

R: maximum degree of polynomial $r \in GF(3^\kappa)[x]$ used in the sieving step of FFS

S: maximum degree of polynomial $s \in GF(3^\kappa)[x]$ used in the sieving step of FFS

λ: threshold value for the large prime variation

θ_{min}: minimal ratio of the required special-Q's to all monic irreducible polynomials in $GF(3^\kappa)[x]$ of degree B

β_{min}: minimal ratio of the required large primes to all monic irreducible polynomials in $GF(3^\kappa)[x]$ of degree B

C_{linear}: computational cost of the linear algebra step of FFS

C_{sieve}: computational cost of the sieving step of FFS

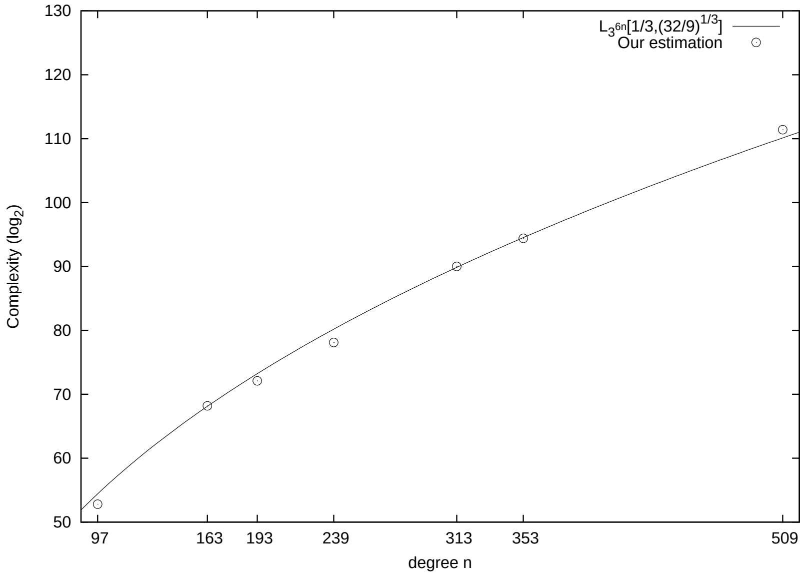

Fig. 1. Time complexity estimation of solving DLP over $GF(3^{6n})$ and $L_{3^{6n}}[1/3, (32/9)^{1/3}]$ with $o(1) = -0.18$

candidate of the suitable values when $\kappa = 1$, there exist more suitable values when $\kappa = 2$, 3, or 6. Therefore, we suppose that the same property holds for $n > 97$. Since the computational costs of (22) are very heavy when $\kappa = 1$ and $n \geq 163$, we omit the test for the condition.

Finally, for each fixed value of $(n, \kappa, d_H, d_m, B, R, S, \lambda)$ mentioned above, we have computed $\beta_{min}, \theta_{min}$, and obtained the costs C_{sieve}, C_{linear}. Comparing these costs where (n, κ) is fixed and $(d_H, d_m, B, R, S, \lambda)$ is changed, we obtain Table 5 of suitable values of $(d_H, d_m, B, R, S, \lambda, \theta, \beta)$ for each fixed (n, κ).

Notice that in Table 5, C_{sieve} for a fixed (n, κ) is larger than C_{linear} for the same (n, κ). Moreover, for each n, the C_{sieve} with $\kappa = 6$ is less than the C_{sieve} with $\kappa = 2, 3$. Therefore, we estimate that the time complexity of solving our DLP by the improved FFS is C_{sieve} with $\kappa = 6$, so we obtain Table 1 and Figure 1. For each pair $(n,\ \kappa,\ d_H,\ d_m)$ in Table 5, we have confirmed the existence of polynomials f, m, H satisfying (1), and these are given in Appendix D.

6 Conclusions

In this paper, we evaluated the security of pairing-based cryptosystems using the η_T pairing defined over finite fields whose characteristic is 3. For the evaluation, we consider the time complexity of solving the discrete logarithm problem (DLP) over the extension field $GF(3^{6n})$ of the embedding degree 6 by the asymptotically fastest function field sieve (FFS). The extension degree 6 allows us to improve the speed of FFS by efficient algorithms such as the large prime variation, the lattice sieve, the filtering, the Galois action, and the free relation. We therefore estimated the precise time complexity of solving our DLP by FFS with the efficient algorithms, called the "improved FFS" in this paper. By using our new formulas to count the explicit number of smooth polynomials used in the improved FFS, our experiment obtain the precise time complexity. Finally, we adapted the formulas to the degree n appeared in several studies in the literature, and then estimated that the time complexity of solving the DLP over $GF(3^{6n})$ for $n = 193$, 239, 509 is 2^{72}, 2^{78}, 2^{111}, respectively. Therefore, n must be larger than 239 to keep 80 bit security.

Many high-speed implementations of the η_T pairing have been reported, which have attracted us to achieve practical use of the η_T pairing. Our estimation in this paper contributes to evaluating the key length of the pairing-based cryptosystems using the η_T pairing.

References

1. L. M. Adleman, “The function field sieve,” ANTS-I, LNCS 877, pp. 108-121, (1994).
2. 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).
3. 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).
4. O. Ahmadi, D. Hankerson, and A. Menezes, “Software implementation of arithmetic in F_{3^m},” WAIFI 2007, LNCS 4547, pp. 85-102, (2007).
5. E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid, “Recommendation for key management - Part 1: General (Revised),” NIST Special Publication 800-57, (2007).
6. P. S. L. M. Barreto, H. Y. Kim, B. Lynn, and M. Scott, “Efficient algorithms for pairing based cryptosystems,” CRYPTO 2002, LNCS 2442, pp. 354-368, (2002).
7. 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).
8. 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).
9. D. Boneh and M. Franklin, “Identity based encryption from the Weil pairing,” SIAM J. Comput., vol.32, no.3, pp. 586-615, (2003).
10. S. Cavallar, “Strategies in filtering in the number field sieve,” ANTS-IV, LNCS 1838, pp. 209-231, (2000).
11. S. Galbraith, K. Harrison, and D. Soldera, “Implementing the Tate pairing,” ANTS 2002, LNCS 2369, pp. 324-337, (2002).
12. E. Gorla, C. Puttmann, and J. Shokrollahi, “Explicit formulas for efficient multiplication in $F_{3^{6m}}$,” SAC 2007, LNCS 4876, pp. 173-183, (2007).
13. R. Granger, “Estimates for discrete logarithm computations in finite fields of small characteristic,” Cryptography and Coding. LNCS 2898, pp. 190-206, (2003).
14. 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).
15. 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).
16. D. Hankerson, A. Menezes, and M. Scott, “Software implementation of pairings,” In Identity-Based Cryptography, pp. 188-206, (2009).
17. K. Harrison, D. Page, and N. P. Smart, “Software implementation of finite fields of characteristic three, for use in pairing-based cryptosystems,” LMS Journal of Computation and Mathematics 5, pp. 181-193, (2002).
18. T. Hayashi, N. Shinohara, L. Wang, S. Matsuo, M. Shirase, and T. Takagi, “Solving a 676-bit discrete logarithm problem in $GF(3^{6n})$,” PKC 2010, LNCS 6056, pp. 351-367, (2010).
19. 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)
20. A. Joux and R. Lercier, “The function field sieve is quite special,” ANTS-V, LNCS 2369, pp. 431-445, (2002).
21. A. Joux and R. Lercier, “The function field sieve in the medium prime case,” EUROCRYPT 2006, LNCS 4004, pp. 254-270, (2006).
22. Y. Kawahara, K. Aoki, and T. Takagi, “Faster implementation of η_T pairing over $GF(3^m)$ using minimum number of logical instructions for $GF(3)$-addition,” Pairing 2008, LNCS 5209, pp. 282-296, (2008).
23. T. Kleinjung, K. Aoki, J. Franke, A. K. Lenstra, E. Thomè, J. W. Bos, P. Gaudry, A. Kruppa, P. L. Montgomery, D. A. Osvik, H. J. J. T. Riele, A. Timofeev, and P. Zimmermann, “Factorization of a 768-Bit RSA Modulus,” CRYPTO 2010, LNCS6223, pp. 333-350, (2010).
24. T. Kerins, W. Marnane, E. Popovici, and P. S. L. M. Barreto, “Efficient hardware for the Tate pairing calculation in characteristic three,” CHES 2005, LNCS 3659, pp. 412-426, (2005).
25. C. Lanczos, ”Solution of systems of linear equations by minimized iterations,” J. Res. Nat. Bureau of Standards, vol.49, no.1, pp. 33-53, (1952).
26. A. K. Lenstra, H. W. Lenstra, Jr., M. S. Manasse, and J. M. Pollard, “The number field sieve,” LNIM 1554, pp. 43-49, (1993).
27. J. M. Pollard, “The lattice sieve,” LNIM 1554, pp. 43-49, (1993).
28. D. Page and N. P. Smart, “Hardware implementation of finite fields of characteristic three,” CHES 2002, LNCS 2523, pp. 529-539, (2003).

29. C. Pomerance and S.S. Wagstaff, Jr., "Implementation of the continued fraction integer factoring algorithm," Congress. Numer., vol. 37, pp. 99-118, (1983).
30. N. Smart, D. Page, and F. Vercauteren, "A comparison of MNT curves and supersingular curves," Applicable Algebra in Engineering, Communication and Computing, vol. 17, pp. 379-392, (2006).

A Function $\bar{a}_{i,j}$ used in Granger's formulas and our new formulas

This appendix gives the formula of $\bar{a}_{i,\,j}$ used in the formula (15) in section 3.2 and in Theorem 1 in section 4.3. In the same manner as Granger's method [13], $\bar{a}_{i,\,j}$ is described as

$$\bar{a}_{i,j} = \begin{cases} (q-1)^2 q^{i+j-1} & (i,\, j > 0) \\ (q-1)^2 q^{i} & (i = 0) \\ (q-1)^2 q^{j} & (j = 0). \end{cases} \tag{23}$$

This corresponds to the equation (3) in [13]. Note that we suppose that $0 \le i \le j$ in [13], but $0 \le i,\, j$ in this paper.

B Proof of formulas used in Theorem 1

This appendix gives proofs of formulas ρ_2 and ρ_3 used in Theorem 1 in section 4.3. Formulas ρ_2 and ρ_3 contain the formula $N_q(k, B)$ that means the number of monic polynomials g of degree k, such that g is factorized into irreducible polynomials whose degree is not larger than B. The details of the formula $N_q(k, B)$ are given in [13].

B.1 Proof of formulas ρ_2

$$\rho_2(q,\, B,\, \beta,\, \lambda,\, k) =$$
$$\frac{1}{q^k}\left\{ N_q(k, B-1) + \sum_{\ell \ge 1}^{\lfloor k/B \rfloor} N_q(k-\ell B, B-1) \left\{ \sum_{i=1}^{\min\{\ell,\lambda\}} \binom{\lfloor \beta I_q(B) \rfloor}{i} \binom{\ell-1}{\ell-i} \right\}\right\}$$

Proof . Let $g \in GF(q)[x]$ be a monic irreducible polynomial of degree k and (B, β, λ)-smooth.

First we consider that the case g does not have any large primes, namely g is $(B-1)$-smooth. Then the number of such polynomials of degree k is $N_q(k, B-1)$.

Next we suppose that g has at least one large prime. Let s be a $(B-1)$-smooth polynomial, and t_j a large prime factor of s. Then g is described as follows:

$$g = s \prod_{j=1}^{i} t_j^{e_j} \ (1 \le i \le \lambda,\ e_j \ge 1).$$

Since the degree of polynomial s is $k - \ell B$ where $\ell = \sum_{j=1}^{i} e_j$, there exist $N_q(k-\ell B, B-1)$ candidates of s for given B and ℓ. Here we consider the number of candidates of $\prod_{j=1}^{i} t_j(x)^{e_j}$. We select i distinct large primes $t_1, ..., t_i$ from the set Λ whose cardinality is $\lfloor \beta I_q(B) \rfloor$. Additionally, we select $\ell - i$ repeated polynomials from the set $\{t_1, ..., t_i\}$. Therefore, the number of candidates of $\prod_{j=1}^{i} t_j(x)^{e_j}$ is

$$\binom{\lfloor \beta I_q(B) \rfloor}{i} \binom{i + (\ell - i) - 1}{\ell - i} = \binom{\lfloor \beta I_q(B) \rfloor}{i} \binom{\ell - 1}{\ell - i}.$$

Consequently, since $1 \le i \le \lambda$ and $1 \le \ell \le \lfloor k/B \rfloor$, the number of candidates of g is

$$\sum_{\ell \ge 1}^{\lfloor k/B \rfloor} N_q(k - \ell B, B-1) \left\{ \sum_{i=1}^{\min\{\ell,\lambda\}} \binom{\lfloor \beta I_q(B) \rfloor}{i} \binom{\ell - 1}{\ell - i} \right\}$$

There are q^k monic polynomials of degree k, so we obtain that

$$\rho_2(q,\, B\,\beta,\, \lambda,\, k) = \\ \frac{1}{q^k} \left\{ N_q(k, B-1) + \sum_{\ell \ge 1}^{\lfloor k/B \rfloor} N_q(k - \ell B, B-1) \left\{ \sum_{i=1}^{\min\{\ell,\lambda\}} \binom{\lfloor \beta I_q(B) \rfloor}{i} \binom{\ell - 1}{\ell - i} \right\} \right\}$$

□

B.2 The proof of formulas ρ_3

$$\rho_3(q,\, B,\, \beta,\, \lambda,\, \Theta,\, k) = \\ \frac{1}{q^k} \sum_{\ell=1}^{\lfloor k/B \rfloor} N_q(k - \ell B, B-1) \left\{ \sum_{\ell_Q=1}^{\ell} \sum_{\lambda_Q=1}^{\min\{\ell_Q,\lambda,\#\Theta\}} \binom{\#\Theta}{\lambda_Q} \binom{\ell_Q - 1}{\ell_Q - \lambda_Q} \tau_{B,\beta,\lambda,\Theta}(\ell, \ell_Q, \lambda_Q) \right\}$$

where

$$\tau_{B,\beta,\lambda,\Theta}(\ell, \ell_Q, \lambda_Q) = \begin{cases} \sum_{\lambda_t=1}^{Min} \binom{\lfloor \beta I_q(B) \rfloor - \#\Theta}{\lambda_t} \binom{\ell - \ell_Q - 1}{\ell - \ell_Q - \lambda_t} & (Min \ge 1) \\ 1 & (\ell = \ell_Q), \\ 0 & (\text{others}), \end{cases}$$
$$Min = \min\{\ell - \ell_Q, \lambda - \lambda_Q, \lfloor \beta I_q(B) \rfloor - \#\Theta\}.$$

Proof. Let Θ' be the set $\Lambda \backslash \Theta$. Let g be a monic and $(B, \beta, \lambda, \Theta)$-smooth polynomial in $GF(q)[x]$ of degree k.

First we suppose that g has at least one prime factor in Θ', so g is described as

$$g = s \left(\prod_{i=1}^{\lambda_t} t_i^{e_i} \right) \left(\prod_{j=1}^{\lambda_Q} Q_j^{e_j} \right) \quad (t_i \in \Theta',\ Q_j \in \Theta), \tag{24}$$

where λ_t, e_i, λ_Q, $e_j \ge 1$ and s is a $(B-1)$-smooth polynomial. Let ℓ_t, ℓ_Q be $\sum_{i=1}^{\lambda_t} e_i$, $\sum_{j=1}^{\lambda_Q} e_j$, respectively. Then, there are $N_q(k - B(\ell_t + \ell_Q), B-1)$ such polynomials s since $\deg s = k - B(\ell_t + \ell_Q)$. Here we consider the number of such $\prod_{j=1}^{\lambda_Q} Q_j(x)^{e_j}$. We first select λ_Q distinct polynomials $Q_1, ..., Q_{\lambda_Q}$ from Θ, and then $\ell_Q - \lambda_Q$ polynomials are additionally selected from the set $\{Q_1, ..., Q_{\lambda_Q}\}$. In this way, the product $\prod_{j=1}^{\lambda_Q} Q_j(x)^{e_j}$ are constructed, so the number of such product is

$$\binom{\#\Theta}{\lambda_Q} \binom{\lambda_Q + (\ell_Q - \lambda_Q) - 1}{\ell_Q - \lambda_Q} = \binom{\#\Theta}{\lambda_Q} \binom{\ell_Q - 1}{\ell_Q - \lambda_Q}. \tag{25}$$

In a similar way, the number of such $\prod_{i=1}^{\lambda_t} t_i(x)^{e_i}$ is

$$\binom{\lfloor \beta I_q(B) \rfloor - \#\Theta}{\lambda_t} \binom{\ell_t - 1}{\ell_t - \lambda_t}.$$

The number of such g is described as

$$\sum_{\ell=2}^{\lfloor k/B\rfloor} N_q(k-\ell B, B-1)\left\{\sum_{\ell_Q=1}^{\ell-1}\sum_{\lambda_Q=1}^{\min\{\ell_Q,\lambda-1,\#\Theta\}}\binom{\#\Theta}{\lambda_Q}\binom{\ell_Q-1}{\ell_Q-\lambda_Q}\tau_{B,\beta,\lambda,\Theta}(\ell,\ell_Q,\lambda_Q)\right\}, \tag{26}$$

where

$$\tau_{B,\beta,\lambda,\Theta}(\ell,\ell_Q,\lambda_Q)=\sum_{\lambda_t=1}^{Min}\binom{\lfloor\beta I_q(B)\rfloor-\#\Theta}{\lambda_t}\binom{\ell-\ell_Q-1}{\ell-\ell_Q-\lambda_t}$$
$$Min=\min\{\ell-\ell_Q,\lambda-\lambda_Q,\lfloor\beta I_q(B)\rfloor-\#\Theta\}.$$

Since g is a (B,β,λ,Θ)-smooth polynomial, at most λ distinct polynomials can be selected from $\Lambda=\Theta\cup\Theta'$ for the product $\left(\prod_{i=1}^{\lambda_t}t_i^{e_i}\right)\left(\prod_{j=1}^{\lambda_Q}Q_j^{e_j}\right)$. Thus we have that $2\le\lambda_Q+\lambda_t\le\lambda$, so $1\le\lambda_Q\le\min\{\ell_Q,\lambda-1,\#\Theta\}$. By letting $\ell=\ell_Q+\ell_t$, we obtain that $2\le\ell\le\lfloor k/B\rfloor$ and $1\le\ell_Q\le\ell-1$. Here we consider the product $\left(\prod_{i=1}^{\lambda_t}t_i^{e_i}\right)$. Notice that $\ell_t=\ell-\ell_Q$, and in a similar way as above, we obtain the properties for $1\le\lambda_t\le Min$.

Then, we consider the case that g has no factor in Θ': namely g is factorized as

$$g=s\left(\prod_{j=1}^{\lambda_Q}Q_j^{e_j}\right)\quad(Q_j\in\Theta). \tag{27}$$

By extending (24) to the case that $\lambda_t=\ell_t=0$, we can obtain the number of such g. Notice that $\ell=\ell_Q$ and $1\le\lambda_Q\le\lambda$. There are $N_q(k-B\ell,B-1)$ such polynomials s, and the number of $\prod_{j=1}^{\lambda_Q}Q_j(x)^{e_j}$ is (25). Thus, the number of such g is

$$\sum_{\ell=1}^{\lfloor k/B\rfloor}N_q(k-\ell B,B-1)\left\{\sum_{\lambda_Q=1}^{\min\{\ell,\lambda,\#\Theta\}}\binom{\#\Theta}{\lambda_Q}\binom{\ell-1}{\ell-\lambda_Q}\right\}. \tag{28}$$

(28) is translated into

$$\sum_{\ell=1}^{\lfloor k/B\rfloor}N_q(k-\ell B,B-1)\left\{\sum_{\ell_Q=\ell}^{\ell}\sum_{\lambda_Q=1}^{\min\{\ell_Q,\lambda,\#\Theta\}}\binom{\#\Theta}{\lambda_Q}\binom{\ell_Q-1}{\ell_Q-\lambda_Q}\right\}. \tag{29}$$

By adding (26) to (29), we want to describe the number of g as

$$\sum_{\ell=1}^{\lfloor k/B\rfloor}N_q(k-\ell B,B-1)\left\{\sum_{\ell_Q=1}^{\ell}\sum_{\lambda_Q=1}^{\min\{\ell_Q,\lambda,\#\Theta\}}\binom{\#\Theta}{\lambda_Q}\binom{\ell_Q-1}{\ell_Q-\lambda_Q}\tau_{B,\beta,\lambda,\Theta}(\ell,\ell_Q,\lambda_Q)\right\}$$

Therefore, we define that $\tau_{B,\beta,\lambda,\Theta}(\ell,\ell_Q,\lambda_Q)=1$ when $\ell=\ell_Q$. The terms when $\ell_Q<\ell$ and $\lambda_Q=\lambda$ are in excess, and we have $Min=0$ and $\ell\ne\ell_Q$ under the property. Hence, by extending $\tau_{B,\beta,\lambda,\Theta}(\ell,\ell_Q,\lambda_Q)$ to

$$\tau_{B,\beta,\lambda,\Theta}(\ell,\ell_Q,\lambda_Q)=\begin{cases}\sum_{\lambda_t=1}^{Min}\binom{\lfloor\beta I_q(B)\rfloor-\#\Theta}{\lambda_t}\binom{\ell-\ell_Q-1}{\ell-\ell_Q-\lambda_t} & (Min\ge1)\\ 1 & (\ell=\ell_Q)\\ 0 & (\text{others})\end{cases},$$

we obtain the theorem. □

C Free relation in section 4.1

This appendix explains the number $\mathcal{R}_{free}$ (in section 4.1) of free relations. It is known that there exist about $\#\hat{F}(B)$ free relations roughly [18]. However, if d_H is divisible by 3, we obtain more free relations.

Let a, b be nonnegative integers such that $d_H = 3^a b$ and $\gcd(3, b) = 1$. We suppose that $q = 3^\kappa$ and $\mathfrak{p} \in \bar{F}(B)$ of degree d. Then, for any $t_i \in GF(q)[x]/(\mathfrak{p})$, there exists an element $t_{i+1} \in GF(q)[x]/(\mathfrak{p})$ such that $t_i = t_{i+1}^3$. Therefore, we obtain that

$$H(x, y) = y^{3^a b} + x = y^{3^a b} + t_1^3 = (y^{3^{a-1} b} + t_1)^3 = \cdots = (y^b + t_a)^a.$$

Thus, the number of free relations is $\#\hat{F}$ if $b = 1$.

Next we consider the case $b = 2$. If there exist T_1, T_2 satisfying that

$$y^2 + t_a \equiv (y - T_1)(y - T_2) \pmod{\mathfrak{p}}, \tag{30}$$

then we obtain one free relation. The property (30) holds if and only if $-t_a$ is quadratic residue in $GF(q)[x]/(\mathfrak{p})$. Notice that the cardinality of $GF(q^d)^*$ is even. Since exactly half of the elements in $GF(q^d)^*$ are quadratic residue, the probability that a random element in $GF(q^d)^*$ is quadratic residue is 1/2. However, the probability for the fixed element $-t_a$ is required. We check (30) for every $\mathfrak{p}$, so we guess that $-t_a$ behaves as a random element. Thus there are about $\#\hat{F}(B)/2$ free relations, and this fact is confirmed experimentally.

D Polynomials f and m used for function field sieve in section 2.2

This appendix gives example polynomials f and m described in section 2.2 for the extension degrees n and κ appearing in Table 3. The polynomials are represented by hexadecimal numbers in which "3" is substituted for the univariate polynomials f and m over $GF(3^\kappa)$ whose all coefficients are in $GF(3)$. For example, the number `0x11327af4` (which is equal to 288520948 in the decimal number) of the polynomial $m \in GF(3^6)[x]$ at the row of $n = 97, \kappa = 6$ means the univariate polynomial $2x^{17} + 2x^{15} + 2x^{12} + 2x^{11} + 2x^{10} + x^8 + x^6 + x^5 + 1$.

- $n = 97$, $\kappa = 2$, $d_H = 6$, $d_m = 49$

m: 0x39964dda99f4afdc4b5a

f: 0x3f31f11476f4d1f90974a848f7a230e0f58abf660c549f80140176fe8eb6cf4c60f72a4fa07b11f5b589953b5f9b8627b71fd169a4d0c5937495

- $n = 97, \kappa = 3, d_H = 6, d_m = 33$

m: 0x2bb4276d9b04a6

f: 0x1631a97eb594a8efc51f327df6b0ce76fd036bf6b34e6b9309d1ec2f3f56410e7e301d77f68d70

- $n = 97, \kappa = 6, d_H = 6, d_m = 17$

m: 0x11327af4

f: 0x4d31960ccaf29169980134a47469d224a84f489

- $n = 163, \kappa = 2, d_H = 7, d_m = 70$

m: 0x8e3f3c5cb849b6a9f1baa5dc021c

f: 0x10594fc2d06a45c0980736ce3d3f8d111bde1a984e87690d6e91ec6cc9e4ad1aea205407ea29478c5d2bebc2734417994f267992465a74837712662e2c1cdfe4b35a191147aa06eb37c2cbd054b5e2017f8055ae53c3b8d06f5b20a6ebd88057060

- $n = 163, \kappa = 3, d_H = 7, d_m = 47$

m: 0x9670f0eb1b14b846a60

f: 0x266f4241d517bbb4ed2e65c9e7dc9c4a0537a8a9c75297ac57f9a16784ce63ac591015d0937ea0b095ddc52b9bdebc58a7e78cc1b1107bd54f4d3cd623761a0f67

- $n = 163, \kappa = 6, d_H = 7, d_m = 24$

m: 0x72e1099b86

f: 0x96b90dd695d79212e2ff1b2ea804a6f49a615cd53ff16674bbf271457d6f4056e

- $n = 193, \kappa = 2, d_H = 7, d_m = 83$

m: 0x17c5831113b42a6951b76f9cb4afbdda9a

f: 0x3ae84fba553a71c0d63f23ac129cef4b3908f5fc5332eb2e9d47f3a028ff4403632585d9e2d90d3725c00f2d8898a56db64f148916647df2e474aef89bdb1e24e2bfa6895471812a5474de67149b3048034fabbe08a4bdc4cde32db9d88458f369d3a5f2f5ab9e070bf0cddb8577667f346bdd

- $n = 193, \kappa = 3, d_H = 7, d_m = 56$

m: 0x4345d8983748633fa31bdb4

f: 0x191dd6323aa7ac2e93aaec774dfe0c05a10e281f5954c0ab86afa23c5daf333aca704f131a634a26106398b65ad92dfa370780f3f000759ef2d60ea145101fe95a1a86d7c2383e5b00982b75e9

- $n = 193, \kappa = 6, d_H = 7, d_m = 28$

m: 0x1ef3e12ae074

f: 0x5d10818cea67e0a5bd896a111e6a29af1cd1a4fbaf3c65638c00679732179454dda79852def62

- $n = 239, \kappa = 2, d_H = 8, d_m = 90$

m: 0x120758d4f8d47aca740b362c5a6d7d7dce858

f: 0x184cfc7460bab501388fde6826845bbdef023294c436aa97190038b3a09f8df41572b0b9873cb988ed4acb1a287270c75b71a6e7ae09f9cdf841fb3e7dd1dcdff1fa41148b997cfe9bfa636226eae48e9e032da7b72815f25e1b2804ca8a1d49af17f6a9daf6a172ad01537a0f0445720291ce565aea27dbdca8ffafaf8fa239be5f6a67867b99f8c7819b3914583

- $n = 239, \kappa = 3, d_H = 8, d_m = 60$

m: 0x18bd6e17a060c429b5078f40f

f: 0x3be4d85c45e866a2446f06d8a393f68596cc41cb491c29d8b06ce94c2f5165e8fda191c059eb1039b54f091f1311c49dd84f173d2cfc1280e4d138e46e5f22e2aff3bdb111a3222fdb812016925b3ba587cc52fc506eab4d826c0da116ed06

- $n = 239, \kappa = 6, d_H = 8, d_m = 30$

m: 0xc55d20ceaebd

f: 0x7c161894e37f675847384d657397d87bc1f27b3b673bea716d58cbd4ec61d9102fb575905bd5dd0c0f5386715adbd4e

- $n = 313, \kappa = 2, d_H = 8, d_m = 118$

m: 0x15b85b97c176e38a10e628fce756e29066d2699d78940788

f: 0x24d68c68a19d0d7841ade22df4ede00dee0da9b3815e3866f7a6b9b00615c0d06b201a236d362cc1aa6a8badb1d92a376d060a14325a8e1327f9c7c8774c6b2e49c7d0a469139560f7a232ce4ef2e709e855546deb74886e27978afbb56cce283ef73173c9331e1e40955c57e3209d66b46cc58db526cad3ff26b57ddfdb9ca7327a8fdd8da43c093f7e6852986b14deb28125c9e134dd86bac944bc87c5fe0808d296f2ad352384bd22b8aa6556f7faf63ba4233c60721d6aca8

- $n = 313, \kappa = 3, d_H = 9, d_m = 79$

m: 0x5655d29bdb485085208fd978abd42def

f: 0x20eb9bb0e7e0b2f97bdc7a49e4ea4f72ed4faa1ac9fccab08ed1468b2e1c387274874b3a1a7fc07999f6f8f6a4d02d1c84a8673c9d0470ebc92d368e6aea4ffbaef34bd175a0f1bfe809d6f0a169b885eba260a24ae9fe122308a6fcc9b9940f3fce20be814fbf9fa9793b9ceb21d67587325d84d6b7e5eeaea7a9a68

- $n = 313, \kappa = 6, d_H = 9, d_m = 35$

m: 0x12b946308a71c98

f: 0x20c25be993cf520cfe972d4aa5b9f8f6fabafb0ee95c12f4ee748090eff153a9615e8167c2cc652e4aa95be03a5bd77095cb412791e82cb71f3ae019593d8

- $n = 353, \kappa = 2, d_H = 9, d_m = 118$

m: 0x16968ca44e6ebff0cd072d643f88d9eb89b922eef48e6378

f: 0xa23742483db4f40824d9b2a7dabe6ff07ec5f15aa0d02deb59d0ed4d685f69c0942e1690b6fa452445320dbb0577ef57d2721d7195154c3dcf0699b298fdb81fd4924d7c89c9e2eec93d65e03c53cafe11320c47f8d8cf45ea0950c63889e523cdf10fb01f1385ed2e0d45dfb9393269db19265374d129d8e7a9c5e5f67f78d2072a9a9a0aa98448c3d22bf29cdba283080fb9bff4ba8e2309a2de1174be45221f9a2baf13bfc71dfc639d98c1521d523f829cbf0bdec5f74cebac4bd5e17c9b4de51d9d3522efbe4e579592a8b745b64144

- $n = 353, \kappa = 3, d_H = 9, d_m = 79$

m: 0x368258f92e30a5a9f4385ac2543ba51c

f: 0x926ef1ee517c3cc5abfa767e929f5a4ec894381704939bdc27eb267e5411f6de25ef587c755220205763be7331660f915182d8a291ff6c7fc1a5efcc45c4c1806d702ac1214510a293cb674df27ff775e413a651ca9043097c0a817c424869bbdfcb59d2f30c68084993ec0b6b7813e2f962e1711c39370555080eb85a7a272e05ebefaf13292cd8b7731212

- $n = 353, \kappa = 6, d_H = 9, d_m = 40$

m: 0x1544ad320c2775609

f: 0x159f625b2865ae374f202a8edeb3c5e715434d553dcfb0c211aff94b7c88395766aaa2da8903274f099f8a34088ebc1ce5574e7eb2eeca724530eb0de477ca546c29304b01f51

- $n = 509, \kappa = 2, d_H = 9, d_m = 170$

m: 0x637b0ddbb456ce4ca9c52bb1eba3060e2c8a560cd54e78caa05c37dcc331dbd1b22d

f: 0x197830517df44aa2772514e71875163887a269479f0fcb261ed5240c8bddb77db6b7e4d48ecf2c3b91895b3fff9e77bd225082cfe5f8edb1ab8ae20394fd824f883b28edd5c04dfac56e7f4a00402d37c1bc40395787e126d5906d91705e1dcd7848f4caccd4c96c63eab14e27671c1f47239f2cac87394971083610ecc082f9d7e2011a0f8ff09dc01ed94e201ad89efd0ca6e3c410a1d6940cdc5faf8287d35178b5d94d1ea3b2b0fb4afc90e0c91ecaafd4133a4420616b1bcb35b8632a4b8d6f6efa9a8160e1b9f1927da7d91a90338e72ea11643faabc0762d8d36ef3b4bb5ff8364a2284e88eb1cfcd0de4af34741618accf9c5a2c2d9b9abb7d1364d69d77d6a7d2b0558942c34fb38bc9856dc5947a0f9a8b5e36b070d6975585b6b5b8977540b00f106be205c7407c040d

- $n = 509, \kappa = 3, d_H = 9, d_m = 114$

m: 0x1f34758909ee31a9e4666c6ab3d268a272e6abffd434f6

f: 0x5225d1ea2d9c5173cd7956accba48d7d0c00b321883dab86178ea0291ffc16c86cb68753e1b743d1117ad2a328a5565eb6b8ba4c141fe67bc3380d842d8f2703ac8e7d3afddbaf66e88bc753bce09c47236f3907526d3bef3be36910ed61e723143c81dc14142c9b190a311a1ca0835353de681ec18c301ee6394ccd702b1f2b904363e8e82176327a6e563410104d707ade6c1f58a98aced56103f113b814498d56c755ca0da8ab1b5be29c6db7ef6624beb0bf545efe0b222c6a455369d4c56b7fcf1bbff942d8a144

- $n = 509, \kappa = 6, d_H = 9, d_m = 57$

m: 0x759368a35ffb3865a07a4aa

f: 0x8ee700ea09b1007d18ffa4d10d58fc687ded81e10918e4d8625ed67a57d60a8518ab23a33e818987c3d53e3fab0409865c108784b9515b6609946fde9c87ed003761593713056b98c7e375754eb847c14e321c1d04a22eb5b9d5e8f40387e4c45bf79334de