WEAKNESS OF $\mathbb{F}_{3^{6\cdot 1429}}$ AND $\mathbb{F}_{2^{4\cdot 3041}}$ FOR DISCRETE LOGARITHM CRYPTOGRAPHY

GORA ADJ, ALFRED MENEZES, THOMAZ OLIVEIRA,
AND FRANCISCO RODRÍGUEZ-HENRÍQUEZ

Abstract. In 2013, Joux and then Barbulsecu et al. presented new algorithms for computing discrete logarithms in finite fields of small characteristic. Shortly thereafter, Adj et al. presented a concrete analysis showing that, when combined with some steps from classical algorithms, the new algorithms render the finite field $\mathbb{F}_{3^{6\cdot 509}}$ weak for pairing-based cryptography. Granger and Zumbrägel then presented a modification of the new algorithms that extends their effectiveness to a wider range of fields.

In this paper, we study the effectiveness of the new algorithms combined with a carefully crafted descent strategy for the fields $\mathbb{F}_{3^{6\cdot 1429}}$ and $\mathbb{F}_{2^{4\cdot 3041}}$. The intractability of the discrete logarithm problem in these fields is necessary for the security of pairings derived from supersingular curves with embedding degree 6 and 4 defined, respectively, over $\mathbb{F}_{3^{1429}}$ and $\mathbb{F}_{2^{3041}}$; these curves were believed to enjoy a security level of 192 bits against attacks by Coppersmith's algorithm. Our analysis shows that these pairings offer security levels of at most 91 and 129 bits, respectively, leading us to conclude that they are dead for pairing-based cryptography.

1. Introduction

Let $\mathbb{F}_q$ denote a finite field of order q, and let E be an elliptic curve defined over $\mathbb{F}_q$ with $\#E(\mathbb{F}_q) = cr$ where r is prime with $\gcd(r, q) = 1$ and $c \ll r$. Let k be the embedding degree of E, i.e., the smallest positive integer satisfying $r \mid q^k - 1$. The Weil and Tate pairings can be used to reduce the discrete logarithm problem (DLP) in the order-r subgroup of $E(\mathbb{F}_q)$ to the discrete logarithm problem in the order-r subgroup of $\mathbb{F}_{q^k}^*$ [8, 15]. Hence, the security of cryptosystems implemented using elliptic curves with small embedding degrees is dependent on the intractability of the DLP in (the multiplicative group of) $\mathbb{F}_{q^k}$.

Elliptic curves having small embedding degree k have been used to implement pairing-based protocols [3, 5]. In this paper, we are interested in the $k = 4$ supersingular elliptic curves $Y^2 + Y = X^3 + X$ and $Y^2 + Y = X^3 + X + 1$ defined over characteristic-two finite fields, and the $k = 6$ supersingular elliptic curves $Y^2 = X^3 - X \pm 1$ defined over characteristic-three finite fields.

The security of these elliptic curves has been severely tarnished due to the recent algorithms of Joux [11], Göloğlu et al. [9], and Barbulescu et al. [2]. More precisely, Joux developed an $L_Q[\frac{1}{4} + o(1), c]$ DLP algorithm in $\mathbb{F}_Q$, where $Q = q^n$ is a power of 2, and q and n are balanced in the sense that $q \approx m$ where $n = 2m$. Here, $L_Q[\alpha, c]$ with $0 < \alpha < 1$ and $c > 0$ denotes the expression

$$\exp\left((c + o(1))(\log Q)^{\alpha}(\log\log Q)^{1-\alpha}\right)$$

Date: November 9, 2013.

This work was done while the first, third and fourth authors were visiting the University of Waterloo.

that is subexponential in $\log Q$. Shortly thereafter, Barbulescu et al. presented a new DLP algorithm which, for many choices of field sizes, is asymptotically faster than all previous algorithms. In particular, in the case where q is a power of 2 or 3 with $q \approx n$ and $n \leq q+2$, the DLP in $\mathbb{F}_{q^{2n}} = \mathbb{F}_Q$ can be solved in quasi-polynomial time

$$(\log Q)^{O(\log \log Q)}.$$

While the new algorithms are asymptotic in nature, Adj et al. [1] showed that, when combined with some steps from classical algorithms, they can have a considerable impact on the security of pairing-based protocols in practice. Let E denote the supersingular elliptic curve $Y^2 = X^3 - X + 1$ over $\mathbb{F}_{3^{509}}$. Then $\#E(\mathbb{F}_{3^{509}}) = 7r$ where r is an 804-bit prime. The finite field $\mathbb{F}_{3^{6\cdot 509}}$ offers approximately 128 bits of security against attacks on the DLP by Coppersmith's algorithm [6] (see [13]). However, the concrete analysis in Adj et al. demonstrates that the order-r subgroup of the multiplicative group of this field offers at most 74 bits of security against the new attacks of Joux and Barbulescu et al.

The setup in Joux's algorithm imposes some restrictions on the algorithm parameters which limits the range of fields on which the algorithm is effective. Suppose that one wishes to compute logarithms in $\mathbb{F}_{q^{2n}}$,[1] where q is the power of a small prime and n is prime. Joux's algorithm represents $\mathbb{F}_{q^{2n}}$ as $\mathbb{F}_{q^2}[X]/(I_X)$, where I_X is a degree-n irreducible factor of $h_1X^q - h_0$ in $\mathbb{F}_{q^2}[X]$, and $h_0, h_1 \in \mathbb{F}_{q^2}[X]$ have small degree (say, 2); hence, one must have $n \leq q + 2$. For example, logarithms in $\mathbb{F}_{3^{6\cdot 509}}$ can be computed by first embedding the field in the quadratic extension $\mathbb{F}_{(3^6)^{2\cdot 509}}$; one can take $q = 3^6 = 729$ and $n = 509$. However, if one wishes to compute logarithms in $\mathbb{F}_{3^{6\cdot 1429}}$, then the smallest extension that meets the setup criteria is $\mathbb{F}_{(3^9)^{2\cdot 1429}}$; this field is too large for the new attacks to be effective.

At ECC 2013, Granger and Zumbrägel [10] presented a modification of the new algorithms that alleviates the aforementioned restrictions. Their idea is to select I_X as a degree-n irreducible factor of $h_1(X^q)\cdot X - h_0(X^q)$, where $h_0, h_1 \in \mathbb{F}_{q^2}[X]$ have small degree (say, 2); the condition on q and n is then relaxed to $n \leq 2q + 1$. While this modification does not affect the asymptotic run time of the new algorithms, it is very successful in increasing the effectiveness of the new algorithms in practice. For example, the $k = 4$ elliptic curve $E : Y^2 + Y = X^3 + X$ over $\mathbb{F}_{2^{1223}}$ has $\#E(\mathbb{F}_{2^{1223}}) = 5r$ where r is a 1221-bit prime. The finite field $\mathbb{F}_{2^{4\cdot 1223}}$ offers approximately 128 bits of security against attacks on the DLP by Coppersmith's algorithm. However, by embedding $\mathbb{F}_{2^{4\cdot 1223}}$ in $\mathbb{F}_{(2^{10})^{2\cdot 1223}}$, Granger and Zumbrägel reported that the order-r subgroup of the multiplicative group of $\mathbb{F}_{2^{4\cdot 1223}}$ offers at most 95 bits of security against the new attacks. As a second example, one can embed $\mathbb{F}_{3^{6\cdot 1429}}$ in $\mathbb{F}_{(3^6)^{2\cdot 1429}}$ and then the condition $n \leq 2q + 1$ is satisfied with $q = 3^6$ and $n = 1429$.

The purpose of this paper is to show that the new algorithms of Joux and Barbulescu et al., as modified by Granger and Zumbrägel, can have a drastic impact on the security of the $k = 4$ and $k = 6$ supersingular elliptic curves at higher security levels. More precisely, we consider the $k = 6$ elliptic curve $E_1 : Y^2 = X^3 - X - 1$ over $\mathbb{F}_{3^{1429}}$ and the $k = 4$ elliptic curve $E_2 : Y^2 + Y = X^3 + X$ over $\mathbb{F}_{2^{3041}}$. We have $\#E_1(\mathbb{F}_{3^{1429}}) = cr$ where r is a 2223-bit

[1] In general, one wishes to compute logarithms in $\mathbb{F}_{p^{\ell n}}$ where p is a small prime and n is prime. To accomplish this, one embeds $\mathbb{F}_{p^{\ell n}}$ in $\mathbb{F}_{(p^b)^{cn}}$ where $c > 1$ and $\ell \mid bc$. In this paper, we will only consider the case $c = 2$.

prime and c is a 43-bit cofactor, and $\#E(\mathbb{F}_{2^{3041}}) = r$ where r is a 3041-bit prime. Whereas the finite fields $\mathbb{F}_{3^{6\cdot 1429}}$ and $\mathbb{F}_{2^{4\cdot 3041}}$ offer approximately 192 bits of security against attacks on the DLP by Coppersmith's algorithm, our concrete analysis shows that the order-r subgroups of the multiplicative groups of these fields offer, respectively, at most 91 and 129 bits of security against the new attacks.

The remainder of the paper is organized as follows. In §2 we review the DLP algorithms of Joux and Barbulescu et al. as modified by Granger and Zumbrägel. Our concrete analyses for $\mathbb{F}_{3^{6\cdot 1429}}$ and $\mathbb{F}_{2^{4\cdot 3041}}$ are then presented in §3 and §4.

2. New DLP algorithm of Joux and Barbulescu et al.

The DLP algorithm we describe is due to Joux [11], with a descent step from the quasi-polynomial time algorithm (QPA) of Barbulescu et al. [2], and a polynomial representation (selection of h_0 and h_1) due to Granger and Zumbrägel [10]. For lack of a better name, we will call this algorithm the "new DLP algorithm". The description of the algorithm closely follows the description in [1]; the most important changes are the incorporation of the polynomial selection of Granger and Zumbrägel, the use of lattices in the classical descent stage, and the use of Wiedemann's algorithm for performing linear algebra.

Let $\mathbb{F}_{q^{2n}}$ be a finite field where $n \leq 2q+1$. The elements of $\mathbb{F}_{q^{2n}}$ are represented as polynomials of degree at most $n-1$ over $\mathbb{F}_{q^2}$. Let $N = q^{2n}-1$. Let g be an element of order N in $\mathbb{F}^*_{q^{2n}}$, and let $h \in \mathbb{F}^*_{q^{2n}}$. We wish to compute $\log_g h$. The algorithm proceeds by first finding the logarithms of all degree-one (§2.2) and degree-two (§2.3) elements in $\mathbb{F}_{q^{2n}}$. Then, in the *descent stage*, $\log_g h$ is expressed as a linear combination of logarithms of degree-one and degree-two $\mathbb{F}_{q^{2n}}$ elements. The descent stage proceeds in several steps, each expressing the logarithm of a degree-D element as a linear combination of the logarithms of elements of degree $\leq m$ for some $m < D$. Four descent methods are used; these are described in §2.4–§2.7. The cost of each step is given in Table 1.

Finding logarithms of linear polynomials (§2.2)	
Relation generation	$6q^2 \cdot S_{q^2}(1,3)$
Linear algebra	$q^5 \cdot A_N$
Finding logarithms of irreducible quadratic polynomials (§2.3)	
Relation generation	$q^{16}/N_{q^2}(1,6) \cdot S_{q^2}(1,6)$
Linear algebra	$q^7 \cdot A_N$
Descent (Degree D to degree m)	
Continued-fraction (§2.4)	$\{D = n-1\}$ $(q^{n-1}/N_{q^2}(m,(n-1)/2))^2 \cdot S_{q^2}(m,(n-1)/2)$
Classical (§2.5)	$q^{2(t_1-D+t_2)}/(N_{q^2}(m,t_1-D)N_{q^2}(m,t_2)) \cdot \min(S_{q^2}(m,t_1-D), S_{q^2}(m,t_2))$
	$q^{2(t_1+t_2-D)}/(N_{q^2}(m,t_1)N_{q^2}(m,t_2-D)) \cdot \min(S_{q^2}(m,t_1), S_{q^2}(m,t_2-D))$
QPA (§2.6)	$q^{6D+2}/N_{q^2}(m,3D) \cdot S_{q^2}(m,3D) + q^5 \cdot A_N$
Gröbner bases (§2.7)	$G_{q^2}(m,D) + q^{6m-2D}/N_{q^2}(m,3m-D) \cdot S_{q^2}(m,3m-D)$

Table 1. Estimated costs of the main steps of the new DLP algorithm for computing discrete logarithms in $\mathbb{F}_{q^{2n}}$. A_N and M_{q^2} denote the costs of an addition modulo N and a multiplication in $\mathbb{F}_{q^2}$. See §2.5 for the definitions of t_1 and t_2. The Gröbner basis cost $G_{q^2}(m,D)$ is defined in §2.7.

Notation. $N_{q^2}(m,n)$ denotes the number of monic m-smooth degree-n polynomials in $\mathbb{F}_{q^2}[X]$, $A_{q^2}(m,n)$ denotes the average number of distinct monic irreducible factors among

all monic m-smooth degree-n polynomials in $\mathbb{F}_{q^2}[X]$, and $S_{q^2}(m,d)$ denotes the cost of testing m-smoothness of a degree-d polynomial in $\mathbb{F}_{q^2}[X]$. Formulas for $N_{q^2}(m,n)$, $A_{q^2}(m,n)$ and $S_{q^2}(m,n)$ are given in [1]. For $\gamma \in \mathbb{F}_{q^2}$, $\overline{\gamma}$ denotes the element γ^q. For $P \in \mathbb{F}_{q^2}[X]$, $\overline{P}$ denotes the polynomial obtained by raising each coefficient of P to the power q. The cost of an integer addition modulo N is denoted by A_N, and the cost of a multiplication in $\mathbb{F}_{q^2}$ is denoted by M_{q^2}. The projective general linear group of order 2 over $\mathbb{F}_q$ is denoted $\mathrm{PGL}_2(\mathbb{F}_q)$. $\mathcal{P}_q$ is a set of distinct representatives of the left cosets of $\mathrm{PGL}_2(\mathbb{F}_q)$ in $\mathrm{PGL}_2(\mathbb{F}_{q^2})$; note that $\#\mathcal{P}_q = q^3+q$. A matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathcal{P}_q$ is identified with the quadruple (a,b,c,d).

2.1. **Setup.** Select polynomials $h_0, h_1 \in \mathbb{F}_{q^2}[X]$ of small degree so that

$$X \cdot h_1(X^q) - h_0(X^q) \tag{1}$$

has an irreducible factor I_X of degree n in $\mathbb{F}_{q^2}[X]$; we will henceforth assume that $\max(\deg h_0, \deg h_1) = 2$. Note that

$$X \;\equiv\; \frac{h_0(X^q)}{h_1(X^q)} \;\equiv\; \left(\frac{\overline{h}_0(X)}{\overline{h}_1(X)}\right)^q \pmod{I_X} \tag{2}$$

The field $\mathbb{F}_{q^{2n}}$ is represented as $\mathbb{F}_{q^{2n}} = \mathbb{F}_{q^2}[X]/(I_X)$ and the elements of $\mathbb{F}_{q^{2n}}$ are represented as polynomials in $\mathbb{F}_{q^2}[X]$ of degree at most $n-1$. Let g be a generator of $\mathbb{F}_{q^{2n}}^*$.

2.2. **Finding logarithms of linear polynomials.** Let $\mathcal{B}_1 = \{X + a \mid a \in \mathbb{F}_{q^2}\}$, and note that $\#\mathcal{B}_1 = q^2$. To compute the logarithms of $\mathcal{B}_1$-elements, we first generate linear relations of these logarithms. Let $(a,b,c,d) \in \mathcal{P}_q$. Substituting $Y \mapsto (aX+b)/(cX+d)$ into the systematic equation

$$Y^q - Y = \prod_{\alpha \in \mathbb{F}_q} (Y - \alpha), \tag{3}$$

and then multiplying by $(cX+d)^{q+1}$ yields

$$\begin{aligned}(aX+b)^q(cX+d) - (aX+b)(cX+d)^q \\ = (cX+d) \cdot \prod_{\alpha \in \mathbb{F}_q} [(a-\alpha c)X + (b - \alpha d)].\end{aligned} \tag{4}$$

Replacing X by $(\overline{h}_0/\overline{h}_1)^q$ in the linear terms $aX+b$ and $cX+d$ occurring in the left side of (4) and then clearing denominators yields

$$\begin{aligned}\Big((aX+b)(\overline{c}\overline{h}_0 + \overline{d}\,\overline{h}_1) - (\overline{a}\overline{h}_0 + \overline{b}\,\overline{h}_1)(cX+d)\Big)^q \\ \equiv \overline{h}_1^q \cdot (cX+d) \cdot \prod_{\alpha \in \mathbb{F}_q} [(a-\alpha c)X + (b-\alpha d)].\end{aligned} \tag{5}$$

If the polynomial on the left side of (5) is 1-smooth, then taking logarithms of both sides of (5) yields a linear relation of the logarithms of $\mathcal{B}_1$-elements and the logarithm of $\overline{h}_1$. The probability that the left side of (5) is 1-smooth is $N_{q^2}(1,3)/q^6 \approx \frac{1}{6}$. Thus, after approximately $6q^2$ trials one expects to obtain (slightly more than) q^2 relations. The cost of the relation generation stage is $6q^2 \cdot S_{q^2}(1,3)$. The logarithms can then be obtained by using Wiedemann's algorithm for solving sparse systems of linear equations [16]. The

expected cost of the linear algebra is $q^5 \cdot A_N$ since each equation has approximately q nonzero terms.

Remark 1. (*running time of Wiedemann's algorithm*) Let B be the matrix obtained after the relation generation stage. Note that B is a matrix over $\mathbb{Z}_N$. However, the entries of B are coefficients of the discrete logarithms of linear polynomials that occur in the relations. Thus the vast majority of these entries are expected to be 0, 1, and -1, with the remaining entries (corresponding to repeated factors) being a number that is small in absolute value (e.g. ± 2). Wiedemann's algorithm treats B as a black box, and uses it only to perform matrix-vector multiplication with vectors over $\mathbb{Z}_N$. Since the nonzero entries of B are very small in absolute value, and since B has approximately q nonzero entries per row, the expected cost of each matrix-by-vector multiplication is $q^3 \cdot A_N$. Finally, since the block version of Wiedemann's algorithm [7] requires no more than q^2 such matrix-by-vector multiplications, the overall running time is $q^5 \cdot A_N$.

2.3. **Finding logarithms of irreducible quadratic polynomials.** Let $u \in \mathbb{F}_{q^2}$, and let $Q(X) = X^2 + uX + v \in \mathbb{F}_{q^2}[X]$ be an irreducible quadratic. Define $\mathcal{B}_{2,u}$ to be the set of all irreducible quadratics of the form $X^2 + uX + w$ in $\mathbb{F}_{q^2}[X]$; one expects that $\#\mathcal{B}_{2,u} \approx (q^2-1)/2$. The logarithms of all elements in $\mathcal{B}_{2,u}$ are found simultaneously using one application of QPA descent (see §2.6). More precisely, one first collects relations of the form (13), where the left side of (13) factors as a product of linear polynomials (whose logarithms are known). The expected number of relations one can obtain is $\frac{N_{q^2}(1,6)}{q^{12}} \cdot (q^3+q)$. Provided that this number is significantly greater than $\#\mathcal{B}_{2,u}$, the matrix $\mathcal{H}(Q)$ is expected to have full (column) rank. One can then solve the resulting system of linear equations to obtain the logarithms of all irreducible translates $Q + w$ of Q. This step is repeated for each $u \in \mathbb{F}_{q^2}$. Hence, there are q^2 independent linear systems of equations to be solved.

For each $u \in \mathbb{F}_{q^2}$, the cost of relation generation is $q^{14}/N_{q^2}(1,6) \cdot S_{q^2}(1,6)$, while the linear algebra cost is $q^5 \cdot A_N$.

2.4. **Continued-fraction descent.** Recall that we wish to compute $\log_g h$, where $h \in \mathbb{F}_{q^{2n}} = \mathbb{F}_{q^2}[X]/(I_X)$. We will henceforth assume that $\deg h = n-1$. The descent stage begins by multiplying h by a random power of g. The extended Euclidean algorithm is used to express the resulting field element h' in the form $h' = w_1/w_2$ where $\deg w_1, \deg w_2 \approx n/2$ [4]; for simplicity, we shall assume that n is odd and $\deg w_1 = \deg w_2 = (n-1)/2$. This process is repeated until both w_1 and w_2 are m-smooth for some chosen $m < (n-1)/2$. This gives $\log_g h'$ as a linear combination of logarithms of polynomials of degree at most m. The expected cost of this continued-fraction descent step is approximately

$$\left(\frac{q^{n-1}}{N_{q^2}(m,(n-1)/2)}\right)^2 \cdot S_{q^2}(m,(n-1)/2). \tag{6}$$

The expected number of distinct irreducible factors of w_1 and w_2 is $2A_{q^2}(m,(n-1)/2)$. In the analysis, we shall assume that each of these irreducible factors has degree exactly m. The logarithm of each of these degree-m polynomials is then expressed as a linear combination of logarithms of smaller degree polynomials using one of the descent methods described in §2.5, §2.6 and §2.7.

2.5. **Classical descent.** Let p be the characteristic of $\mathbb{F}_q$, and let $q = p^\ell$. Let $s \in [0, \ell]$, and let $R \in \mathbb{F}_{q^2}[X, Y]$. For the sake of simplicity, we will assume in this section that $h_1 = 1$. Then

$$\left[R(X, \overline{h}_0^{p^{\ell-s}})\right]^{p^s} = R'(X^{p^s}, \overline{h}_0^{p^\ell}) = R'(X^{p^s}, h_0(X^{p^\ell})) \equiv R'(X^{p^s}, X) \pmod{I_X},$$

where R' is obtained from R by raising all its coefficients to the power p^s. Hence

$$\left[R(X, \overline{h}_0^{p^{\ell-s}})\right]^{p^s} \equiv R'(X^{p^s}, X) \pmod{I_X}. \tag{7}$$

Let $Q \in \mathbb{F}_{q^2}[X]$ with $\deg Q = D$, and let $m < D$. In the Joux-Lercier descent method [12], as modified by Göloğlu et al. [9], one selects $s \in [0, \ell]$ and searches for a polynomial $R \in \mathbb{F}_{q^2}[X, Y]$ such that (i) $Q \mid R_1$ where $R_1 = R(X, \overline{h}_0^{p^{\ell-s}})$; (ii) $\deg R_1/Q$ and $\deg R_2$ are appropriately balanced where $R_2 = R'(X^{p^s}, X)$; and (iii) both R_1/Q and R_2 are m-smooth. Taking logarithms of both sides of (7) then gives an expression for $\log_g Q$ in terms of the logarithms of polynomials of degree at most m.

A family of polynomials R satisfying (i) and (ii) can be constructed by finding a basis $\{(u_1, u_2), (v_1, v_2)\}$ of the lattice

$$L_Q = \{(w_1, w_2) \in \mathbb{F}_{q^2}[X] \times \mathbb{F}_{q^2}[X] \ : \ Q \mid (w_1(X) - w_2(X)\overline{h}_0(X)^{p^{\ell-s}})\}$$

where $\deg u_1$, $\deg u_2$, $\deg v_1$, $\deg v_2 \approx D/2$. The points (w_1, w_2) in L_Q can be sampled to obtain polynomials $R(X, Y) = w_1(X) - w_2(X)Y$ satisfying (i) and (ii) by writing

$$(w_1, w_2) = a(u_1, u_2) + b(v_1, v_2) = (au_1 + bv_1, au_2 + bv_2)$$

with $a \in \mathbb{F}_{q^2}[X]$ monic of degree δ and $b \in \mathbb{F}_{q^2}[X]$ of degree $\delta - 1$. The number of lattice points to consider is therefore $(q^2)^{2\delta}$. We have $\deg w_1, \deg w_2 \approx D/2 + \delta$, so $\deg R_1 = t_1 \approx (D/2 + \delta) + 2p^{\ell-s}$ and $\deg R_2 = t_2 \approx (D/2 + \delta)p^s + 1$. In order to ensure that there are sufficiently many such lattice points to generate a polynomial R for which both R_1/Q and R_2 are m-smooth, the parameters s and δ must be selected so that

$$q^{4\delta} \gg \frac{q^{2(t_1-D)}}{N_{q^2}(m, t_1 - D)} \cdot \frac{q^{2t_2}}{N_{q^2}(m, t_2)}. \tag{8}$$

Ignoring the time to compute a balanced basis of L_Q, the expected cost of finding a polynomial R satisfying (i)–(iii) is

$$\frac{q^{2(t_1-D)}}{N_{q^2}(m, t_1 - D)} \cdot \frac{q^{2t_2}}{N_{q^2}(m, t_2)} \cdot \min(S_{q^2}(m, t_1 - D), S_{q^2}(m, t_2)). \tag{9}$$

The expected number of distinct irreducible factors of R_1/Q and R_2 is $A_{q^2}(m, t_1 - D) + A_{q^2}(m, t_2)$. In the analysis, we shall assume that each of these irreducible factors has degree exactly m.

An alternative to the above method is to select $s \in [0, \ell]$ and search for $R \in \mathbb{F}_{q^2}[X, Y]$ such that (i) $Q \mid R_2$; (ii) $\deg R_1$ and $\deg R_2/Q$ are appropriately balanced; and (iii) both R_1 and R_2/Q are m-smooth. A family of polynomials R satisfying (i) and (ii) can be constructed by finding a basis $\{(u_1, u_2), (v_1, v_2)\}$ of the lattice

$$L_Q = \{(w_1, w_2) \in \mathbb{F}_{q^2}[X] \times \mathbb{F}_{q^2}[X] \ : \ Q \mid (w_1(X) - w_2(X)X^{p^s})\}$$

where $\deg u_1$, $\deg u_2$, $\deg v_1$, $\deg v_2 \approx D/2$. The points (w_1, w_2) in L_Q can be sampled as before to obtain polynomials $R(X,Y) = w_1''(Y) - w_2''(Y)X$ satisfying (i) and (ii) where w'' is obtained from w by raising all its coefficients to the power p^{-s}. We have $\deg w_1, \deg w_2 \approx D/2 + \delta$, so $\deg R_1 = t_1 \approx 2(D/2+\delta)p^{\ell-s} + 1$ and $\deg R_2 = t_2 \approx (D/2+\delta) + p^s$. In order to ensure that there are sufficiently many such lattice points to generate a polynomial R for which both R_1 and R_2/Q are m-smooth, the parameters s and δ must be selected so that

$$q^{4\delta} \gg \frac{q^{2t_1}}{N_{q^2}(m,t_1)} \cdot \frac{q^{2(t_2-D)}}{N_{q^2}(m,t_2-D)}. \tag{10}$$

Ignoring the time to compute a balanced basis of L_Q, the expected cost of finding a polynomial R satisfying (i)–(iii) is

$$\frac{q^{2t_1}}{N_{q^2}(m,t_1)} \cdot \frac{q^{2(t_2-D)}}{N_{q^2}(m,t_2-D)} \cdot \min(S_{q^2}(m,t_1), S_{q^2}(m,t_2-D)). \tag{11}$$

The expected number of distinct irreducible factors of R_1 and R_2/Q is $A_{q^2}(m,t_1) + A_{q^2}(m,t_2-D)$.

2.6. **QPA descent.** Let $Q \in \mathbb{F}_{q^2}[X]$ with $\deg Q = D$, and let $m \in [\lceil D/2 \rceil, D-1]$. Let $(a,b,c,d) \in \mathcal{P}_q$. Substituting $Y \mapsto (aQ+b)/(cQ+d)$ into the systematic equation (3) and multiplying by $(cQ+d)^{q+1}$ yields

$$(aQ+b)^q(cQ+d) - (aQ+b)(cQ+d)^q = (cQ+d) \prod_{\alpha \in \mathbb{F}_q} [(a-\alpha c)Q + (b - \alpha d)]. \tag{12}$$

Noticing that

$$cQ + d \equiv cQ\left(\left(\frac{\overline{h}_0}{\overline{h}_1}\right)^q\right) + d \equiv \left(\overline{c}\overline{Q}\left(\frac{\overline{h}_0}{\overline{h}_1}\right) + \overline{d}\right)^q \equiv \overline{h}_1^{-Dq}\left(\overline{c}\widetilde{Q} + \overline{d}\,\overline{h}_1^D\right)^q \pmod{I_X}$$

where $\widetilde{Q} = \overline{h}_1^D \cdot \overline{Q}(\overline{h}_0/\overline{h}_1)$, we obtain

$$\left((aQ+b)(\overline{c}\widetilde{Q} + \overline{d}\,\overline{h}_1^D) - (\overline{a}\widetilde{Q} + \overline{b}\,\overline{h}_1^D)(cQ+d)\right)^q \equiv \overline{h}_1^{Dq} \cdot (cQ+d) \cdot \prod_{\alpha \in \mathbb{F}_q} [(a-\alpha c)Q + (b-\alpha d)] \pmod{I_X}. \tag{13}$$

Note that the polynomial on the left side of (13) has degree $\leq 3D$. If this polynomial is m-smooth, then (13) yields a linear relation of the logarithms of some degree-m polynomials and logarithms of translates of Q. After collecting slightly more than q^2 such relations, one searches for a linear combination of these relations that eliminates all translates of Q except for Q itself. To achieve this, consider row vectors in $(\mathbb{Z}_N)^{q^2}$ with coordinates indexed by elements $\lambda \in \mathbb{F}_{q^2}$. For each relation, we define a vector v whose entry v_λ is 1 if $Q - \lambda$ appears in the right side of (13), and 0 otherwise. If the resulting matrix $\mathcal{H}(Q)$ of row vectors has full column rank, then one obtains an expression for $\log_g Q$ in terms of the logarithms of polynomials of degree $\leq m$. The number of distinct polynomials of degree $\leq m$ in this expression is expected to be $A_{q^2}(m,3D) \cdot q^2$; in the analysis we shall assume that each of these polynomials has degree exactly m.

Since the probability that a degree-$3D$ polynomial is m-smooth is $N_{q^2}(m, 3D)/(q^2)^{3D}$, one must have

$$\frac{N_{q^2}(m, 3D)}{q^{6D}} \cdot (q^3 + q) \gg q^2 \tag{14}$$

in order to ensure that $\mathcal{H}(Q)$ has $\gg q^2$ rows, whereby $\mathcal{H}(Q)$ can be expected to have full rank.

The expected cost of the relation generation portion of QPA descent is $q^{6D+2} \cdot S_{q^2}(m, 3D)/N_{q^2}(m, 3D)$, while the cost of the linear algebra is $q^5 \cdot A_N$.

2.7. **Gröbner bases descent.** Let $Q \in \mathbb{F}_{q^2}[X]$ with $\deg Q = D$, and let $m = \lceil (D+1)/2 \rceil$. In Joux's new descent method [11, §5.3], one finds degree-m polynomials $k_1, k_2 \in \mathbb{F}_{q^2}[X]$ such that $Q \mid G$, where

$$G = (k_1 \widetilde{k}_2 - \widetilde{k}_1 k_2) \bmod I_X$$

and where $\widetilde{k}_1 = \overline{h}_1^m \overline{k}_1(\overline{h}_0/\overline{h}_1)$ and $\widetilde{k}_2 = \overline{h}_1^m \overline{k}_2(\overline{h}_0/\overline{h}_1)$. We then have

$$\overline{h}_1^{mq} \cdot k_2 \cdot \prod_{\alpha \in \mathbb{F}_q} (k_1 - \alpha k_2) \equiv G(X)^q \pmod{I_X}$$

as can be seen by making the substitution $Y \mapsto k_1/k_2$ into the systematic equation (3) and clearing denominators. Note that $\deg(\widetilde{k}_1) = \deg(\widetilde{k}_2) = 2m$. Hence, if $3m < n$ then $G = k_1\widetilde{k}_2 - \widetilde{k}_1 k_2$ and so $G(X) = Q(X)R(X)$ for some $R \in \mathbb{F}_{q^2}[X]$ with $\deg R = 3m - D$. If R is m-smooth, we obtain a linear relationship between $\log_g Q$ and logs of degree-m polynomials by taking logarithms of both sides of the following:

$$\overline{h}_1^{mq} \cdot k_2 \cdot \prod_{\alpha \in \mathbb{F}_q} (k_1 - \alpha k_2) \equiv Q(X)R(X) \pmod{I_X}. \tag{15}$$

To determine (k_1, k_2, R) that satisfy

$$k_1\widetilde{k}_2 - \widetilde{k}_1 k_2 = Q(X)R(X), \tag{16}$$

one can transform (16) into a system of multivariate bilinear equations over $\mathbb{F}_q$. Specifically, each coefficient of k_1, k_2 and R is written using two variables over $\mathbb{F}_q$, the two variables representing the real and imaginary parts of that coefficient (which is in $\mathbb{F}_{q^2}$). The coefficients of $\widetilde{k}_1$ and $\widetilde{k}_2$ can then be written in terms of the coefficients of k_1 and k_2. Hence, equating coefficients of X^i of both sides of (16) yields $3m + 1$ quadratic equations. The real and imaginary parts of each of these equations are equated, yielding $6m + 2$ bilinear equations in $10m - 2D + 6$ variables over $\mathbb{F}_q$. This system of equations can be solved by finding a Gröbner basis for the ideal it generates. Finally, solutions (k_1, k_2, R) are tested until one is found for which R is m-smooth. This yields an expression for $\log_g Q$ in terms of the logarithms of approximately $q + 1 + A_{q^2}(m, 3m - D)$ polynomials of degree (at most) m; in the analysis we shall assume that each of the polynomials has degree exactly m.

Now, the number of candidate pairs (k_1, k_2) is $((q^2)^{m+1})^2 = q^{4(m+1)}$. Denote by $R(m, D)$ the expected number of distinct R obtainable. Then the condition

$$R(m, D) \gg \frac{q^{2(3m-D)}}{N_{q^2}(m, 3m - D)}, \tag{17}$$

can ensure that there exists a solution (k_1, k_2, R) for which R is m-smooth. The number $R(m, D)$ has not been determined and is best estimated experimentally.

It is difficult to determine the exact cost $G_{q^2}(m, D)$ of the Gröbner basis finding step. After the Gröbner basis is found, the cost to find an m-smooth R is $(q^2)^{3m-D}/N_{q^2}(m, 3m-D) \cdot S_{q^2}(m, 3m-D)$.

3. Computing discrete logarithms in $\mathbb{F}_{3^{6\cdot 1429}}$

We present a concrete analysis of the DLP algorithm described in §2 for computing discrete logarithms in $\mathbb{F}_{3^{6\cdot 1429}}$. In fact, this field is embedded in the quadratic extension field $\mathbb{F}_{3^{12\cdot 1429}}$, and it is the latter field where the DLP algorithm of §2 is executed. Thus, we have $q = 3^6 = 729$ and $n = 1429$.

As mentioned in §1, our main motivation for finding discrete logarithms in $\mathbb{F}_{3^{6\cdot 1429}}$ is to attack the elliptic curve discrete logarithm problem in $E_1(\mathbb{F}_{3^{1429}})$, where E_1 is the supersingular elliptic curve $Y^2 = X^3 - X - 1$ with $\#E_1(\mathbb{F}_{3^{1429}}) = cr$; here $c = 7622150170693$ is a 43-bit cofactor and $r = (3^{1429} - 3^{715} + 1)/c$ is a 2223-bit prime. The elliptic curve discrete logarithm problem in the order-r subgroup of $E_1(\mathbb{F}_{3^{1429}})$ can be efficiently reduced to the discrete logarithm problem in the order-r subgroup of $\mathbb{F}^*_{3^{12\cdot 1429}}$. In the latter problem, we are given two elements α, β of order r in $\mathbb{F}^*_{3^{12\cdot 1429}}$ and we wish to find $\log_\alpha \beta$. It can be readily seen that $\log_\alpha \beta = (\log_g \beta)/(\log_g \alpha) \bmod r$, where g is a generator of $\mathbb{F}^*_{3^{12\cdot 1429}}$. Thus, we will henceforth assume that h has order r and that we only need to find $\log_g h \bmod r$. An immediate consequence of this restriction is that all the linear algebra in the new algorithm can be performed modulo the 2223-bit r instead of modulo the 27179-bit N.

The parameters for each step of the algorithm were carefully chosen in order to balance the running time of the steps. We also took into account the degree to which each step could be parallelized on conventional computers. A summary of the parameter choices for the descent is given in Figure 1. The cost of each step is given in Table 2.

3.1. **Setup.** We chose the representations $\mathbb{F}_{3^6} = \mathbb{F}_3[U]/(U^6 + 2U^4 + U^2 + 2U + 2)$ and $\mathbb{F}_{3^{12}} = \mathbb{F}_{3^6}[V]/(V^2 + U^{365})$. We selected $h_0 = (U^{265}V + U^{236})X^2 + (U^{160}V + U^{24})X + (U^{628}V + U^{293}) \in \mathbb{F}_{3^{12}}[X]$ and $h_1 = 1$, and $I_X \in \mathbb{F}_{3^{12}}[X]$ to be the degree-1429 monic irreducible factor of $h_1(X^{3^6}) \cdot X - h_0(X^{3^6})$. The other irreducible factors have degrees 5, 5 and 19.

3.2. **Finding logarithms of linear polynomials.** The factor base $\mathcal{B}_1$ has size $3^{12} \approx 2^{19}$. The cost of relation generation is approximately $2^{30} M_{q^2}$, whereas the cost of the linear algebra is approximately $2^{48} A_r$.

3.3. **Finding logarithms of irreducible quadratic polynomials.** For each $u \in \mathbb{F}_{3^{12}}$, the expected cost of computing logarithms of all quadratics in $\mathcal{B}_{2,u}$ is $2^{39} M_{q^2}$ for the computation of $\mathcal{H}(Q)$, and $2^{48} A_r$ for the linear algebra.

3.4. **Continued-fraction descent.** For the continued-fraction descent, we selected $m = 79$. The expected cost of this descent is $2^{89} M_{q^2}$. The expected number of distinct irreducible factors of degree (at most) 79 obtained is $2A_{3^{12}}(79, 714) \approx 34$.

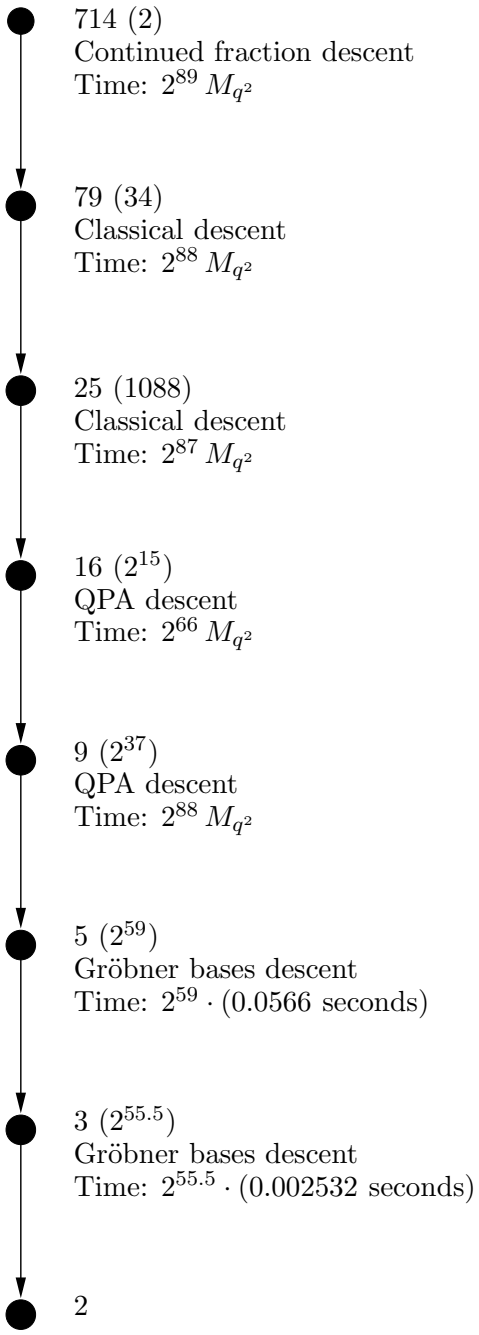

FIGURE 1. A typical path of the descent tree for computing an individual logarithm in $\mathbb{F}_{3^{12\cdot 1429}}$ ($q = 3^6$). The numbers in parentheses next to each node are the expected number of nodes at that level. 'Time' is the expected time to generate all nodes at a level.

Finding logarithms of linear polynomials		
Relation generation	$2^{30}M_{q^2}$	$2^{30}M_{q^2}$
Linear algebra	$2^{48}A_r$	$2^{51}M_{q^2}$
Finding logarithms of irreducible quadratic polynomials		
Relation generation	$3^{12}\cdot 2^{39}M_{q^2}$	$2^{58}M_{q^2}$
Linear algebra	$3^{12}\cdot 2^{48}A_r$	$2^{70}M_{q^2}$
Descent		
Continued-fraction (714 to 79)	$2^{89}M_{q^2}$	$2^{89}M_{q^2}$
Classical (79 to 25)	$34\cdot 2^{83}M_{q^2}$	$2^{88}M_{q^2}$
Classical (25 to 16)	$1088\cdot 2^{77}M_{q^2}$	$2^{87}M_{q^2}$
QPA (16 to 9)	$2^{15}\cdot(2^{49}M_{q^2}+2^{48}A_r)$	$2^{66}M_{q^2}$
QPA (9 to 5)	$2^{37}\cdot(2^{46}M_{q^2}+2^{48}A_r)$	$2^{88}M_{q^2}$
Gröbner bases (5 to 3)	$2^{59}\cdot(0.0566$ seconds)	$2^{85}M_{q^2}$
Gröbner bases (3 to 2)	$2^{55.5}\cdot(0.002532$ seconds)	$2^{77}M_{q^2}$

TABLE 2. Estimated costs of the main steps of the new DLP algorithm for computing discrete logarithms in $\mathbb{F}_{3^{12\cdot 1429}}$ ($q=3^6$). A_r and M_{q^2} denote the costs of an addition modulo the 2223-bit prime r and a multiplication in $\mathbb{F}_{3^{12}}$. We use the cost ratio $A_r/M_{q^2}=2^3$, and also assume that 2^{30} multiplications in $\mathbb{F}_{3^{12}}$ can be performed in 1 second (cf. §3.8).

3.5. **Classical descent.** Two classical descent stages are employed. In the first stage, which uses the alternative method described in §2.5, we have $D=79$ and select $m=25$, $s=5$, $\delta=2$, which yield $t_1=247$ and $t_2=284$. The expected cost of the descent for each of the 34 degree-79 polynomials is approximately $2^{58.7}\cdot S_{q^2}(25,205)$. The expected total number of distinct irreducible polynomials of degree (at most) 25 obtained is approximately 1088.

In the second classical descent stage, which uses the first method described in §2.5, we have $D=25$ and select $m=16$, $s=2$, $\delta=2$, which yield $t_1=176$ and $t_2=127$. The expected cost of the descent for each of the 1088 degree-25 polynomials is approximately $2^{54.4}\cdot S_{q^2}(16,127)$. The expected total number of distinct irreducible polynomials of degree (at most) 16 obtained is approximately 2^{15}.

3.6. **QPA descent.** Two QPA descent stages are employed. In the first stage, we have $D=16$ and select $m=9$. For each Q, the expected cost of relation generation is $2^{30.9}\cdot S_{q^2}(9,48)$ and the cost of the linear algebra is $2^{48}A_r$. Also for each Q, the expected number of distinct polynomials of degree at most 9 obtained is expected to be $A_{q^2}(9,48)\cdot q^2\approx 2^{22}$. Thus, the total number of distinct polynomials of degree at most 9 obtained after the first QPA descent stage is approximately 2^{37}.

In the second stage, we have $D=9$ and select $m=5$. For each Q, the expected cost of relation generation is $2^{30.5}\cdot S_{q^2}(5,27)$ and the cost of the linear algebra is $2^{48}A_r$. Also for each Q, the expected number of distinct polynomials of degree at most 5 obtained is expected to be $A_{q^2}(5,27)\cdot q^2\approx 2^{22}$. Thus, the total number of distinct polynomials of degree at most 5 obtained after the second QPA descent stage is approximately 2^{59}.

3.7. **Gröbner bases descent.** Two Gröbner bases descent stages are employed. The first stage has $D=5$ and $m=3$, and is expected to yield approximately 2^{69} polynomials

of degree (at most) 3. The second stage has $D = 3$ and $m = 2$ and is applied to all the $2^{55.5}$ monic irreducible cubics. Our experiments were run using Magma v2.19-7 [14] on a 2.9 GHz Intel core i7-3520M.

In the first stage, for each degree-5 polynomial Q we have to solve a system of 20 quadratic polynomial equations in 26 variables over $\mathbb{F}_q$ (cf. (16)). Since the ideal generated by these polynomials typically has dimension greater than 0, we randomly fix some of the variables in the hope of obtaining a 0-dimensional ideal. (More precisely, we added some linear constraints involving pairs of variables, one variable from k_1 and the other from k_2.) Each degree-4 R obtained from the variety of the resulting ideal is tested for 3-smoothness. If no 3-smooth R is obtained, we randomly fix some other subset of variables and repeat. We ran 100,000 Gröbner bases descent experiments with randomly-selected degree-5 polynomials Q. On average, we had to find 1.892 Gröbner bases for each Q. The average number of R's tested for 3-smoothness for each Q was 1.332. The average time to find each Gröbner basis was 0.0566 seconds. In total, the expected number of polynomials of degree at most 3 obtained is $2^{59}(q + 1 + A_{q^2}(3, 4)) \approx 2^{69}$.

For the second stage, we use the experimental results from §4.7 of [1].

3.8. **Overall running time.** The second column of Table 2 gives the running time estimates for the main steps of the new DLP algorithm in three units of time: A_r, M_{q^2}, and seconds. In order to assess the overall time, we make some assumptions about the ratios of these units of time.

First, we shall assume that $A_r/M_{q^2} = 2^3$. To justify this, we observe that a 2223-bit integer can be stored in 35 64-bit words. The X86-64 instruction set has an **ADD** operation that adds two 64-bit unsigned integers in one clock cycle. Hence integer addition can be completed in 35 clock cycles. Modular reductions comprises one conditional statement plus one subtraction (required in roughly half of all modular additions). One can use a lazy reduction technique that amortizes the cost of a modular reduction among many integer additions. All in all, the cost of A_r can be estimated to be 35 clock cycles. Unlike for 64-bit integer multiplication, there is no native support for $\mathbb{F}_{3^{12}}$ multiplication on an Intel Core i7 machine. However, we expect that a specially designed multiplier could be built to achieve a multiplication cost of 4 clock cycles. This gives us an A_r/M_{q^2} ratio of approximately 2^3.

Next, since a multiplication in M_{q^2} can be done in 4 clock cycles, we will transform one second on a 2.9 GHz machine (on which the Gröbner bases descent experiments were performed) into $2^{30}M_{q^2}$.

Using these estimates, we see from the third column of Table 2 that the overall running time of the new algorithm is approximately $2^{90.2}M_{q^2}$. We note that the relation generation, continued-fraction descent, classical descent, and Gröbner bases descent steps, and also the relation generation portion of QPA descent, are effectively parallelizable in the sense that one can essentially achieve a factor-C speedup if C processors are available. On the other hand, the linear system of equations for finding logarithms of linear polynomials, the $3^{12} \approx 2^{19}$ linear systems of equations for finding logarithms of irreducible quadratic polynomials, and the $2^{15} + 2^{37}$ linear systems of equations in QPA descent enjoy relatively modest benefits from parallelization on conventional computers.

3.9. **Comparisons.** The upper bound of $2^{90.2}M_{q^2}$ on the running time of the new algorithm for computing logarithms in $\mathbb{F}_{2^{6\cdot 1429}}$ convincingly demonstrates that this field offers

drastically less security than the 2^{192} resistance to attacks by Coppersmith's algorithm [6, 13]. The decrease in security is even more pronounced when one considers that Coppersmith's algorithm is not effectively parallelizable since a dominant step is the solution of a very large system of linear equations, whereas the new algorithm offers many avenues for parallelization.

Also striking is the relatively small difference between the $2^{90.2}M_{q^2}$ running time with the estimate of $2^{81.7}M_{q^2}$ for $\mathbb{F}_{3^{6\cdot 509}}$ [1] (in both cases, we have $q = 3^6$). The security levels for $\mathbb{F}_{3^{6\cdot 1429}}$ and $\mathbb{F}_{3^{6\cdot 509}}$ against Coppersmith's attack differ by $192-128 = 64$ bits. However, the security levels against the new attack differ by only 8.5 bits.

4. Computing discrete logarithms in $\mathbb{F}_{2^{4\cdot 3041}}$

We present a concrete analysis of the DLP algorithm described in §2 of [1] for computing discrete logarithms in $\mathbb{F}_{2^{4\cdot 3041}}$. Note that the algorithm employed in this section uses the original polynomial representation $h_1X^q - h_0$ of Joux [11]. As with the algorithm described in §2 of this paper, we employ lattices in the classical descent stages, and use Wiedemann's algorithm for performing linear algebra.

The field $\mathbb{F}_{2^{4\cdot 3041}}$ is embedded in the sextic extension $\mathbb{F}_{2^{24\cdot 3041}}$, and it is in the latter field where the DLP algorithm is executed. Thus, we have $q = 2^{12} = 2048$ and $n = 3041$.

As mentioned in §1, our main motivation for finding discrete logarithms in $\mathbb{F}_{2^{4\cdot 3041}}$ is to attack the elliptic curve discrete logarithm problem in $E_2(\mathbb{F}_{2^{3041}})$, where E_2 is the supersingular elliptic curve $Y^2+Y = X^3+X$ with $\#E_2(\mathbb{F}_{2^{3041}}) = r$ and $r = 2^{3041}-2^{1521}+1$ is a 3041-bit prime. The elliptic curve discrete logarithm problem in the order-r subgroup of $E_2(\mathbb{F}_{2^{3041}})$ can be efficiently reduced to the discrete logarithm problem in the order-r subgroup of $\mathbb{F}^*_{2^{4\cdot 3041}}$. We wish to compute $\log_g h \bmod r$, where g is a generator of $\mathbb{F}^*_{2^{4\cdot 3041}}$ and $h \in \mathbb{F}^*_{2^{4\cdot 3041}}$ has order r. Hence, all the linear algebra in the new algorithm is performed modulo the 3041-bit r.

A summary of the parameter choices for the descent is given in Figure 2. The cost of each step is given in Table 3.

4.1. **Setup.** We chose the representations $\mathbb{F}_{2^{12}} = \mathbb{F}_2[U]/(U^{12}+U^7+U^6+U^5+U^3+U+1)$ and $\mathbb{F}_{2^{24}} = \mathbb{F}_{2^{12}}[V]/(V^2 + U^{152}V + U^{3307})$. We selected $h_0 = (U^{1515}V + U^{3374})X^2 + (U^{3690}V + U^{2704})X + (U^{2440}V + U^{142}) \in \mathbb{F}_{2^{24}}[X]$ and $h_1 = X + U^{2339}V + U^{807}$, and $I_X \in \mathbb{F}_{2^{24}}[X]$ to be the degree-3041 monic irreducible factor of $h_1 \cdot X^{2^{12}} - h_0$. The other irreducible factors have degrees 5, 7, 69, 110, 293 and 572.

4.2. **Finding logarithms of linear polynomials.** The factor base $\mathcal{B}_1$ has size 2^{24}. The cost of relation generation is approximately $2^{35}M_{q^2}$, whereas the cost of the linear algebra is approximately $2^{60}A_r$.

4.3. **Finding logarithms of irreducible quadratic polynomials.** For each $u \in \mathbb{F}_{2^{24}}$, the expected cost of computing logarithms of all quadratics in $\mathcal{B}_{2,u}$ is $2^{44}M_{q^2}$ for the computation of $\mathcal{H}(Q)$, and $2^{60}A_r$ for the linear algebra.

4.4. **Continued-fraction descent.** For the continued-fraction descent, we selected $m = 123$. The expected cost of this descent is $2^{128.4}M_{q^2}$. The expected number of distinct irreducible factors of degree (at most) 123 obtained is $2A_{2^{24}}(123, 1520) \approx 44$.

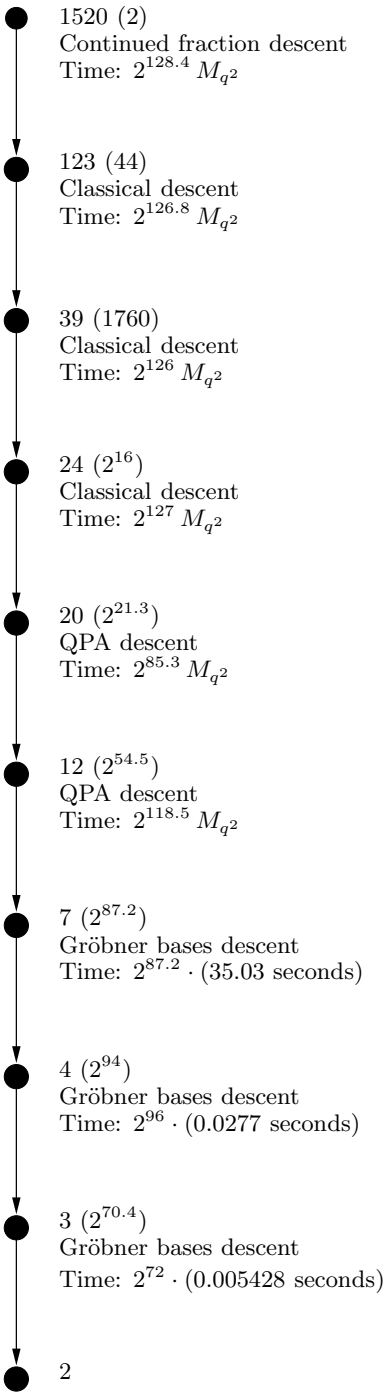

FIGURE 2. A typical path of the descent tree for computing an individual logarithm in $\mathbb{F}_{2^{24\cdot 3041}}$ ($q = 2^{12}$). The numbers in parentheses next to each node are the expected number of nodes at that level. 'Time' is the expected time to generate all nodes at a level.

Finding logarithms of linear polynomials		
Relation generation	$2^{35}M_{q^2}$	$2^{35}M_{q^2}$
Linear algebra	$2^{60}A_r$	$2^{64}M_{q^2}$
Finding logarithms of irreducible quadratic polynomials		
Relation generation	$2^{24}\cdot 2^{44}M_{q^2}$	$2^{68}M_{q^2}$
Linear algebra	$2^{24}\cdot 2^{60}A_r$	$2^{88}M_{q^2}$
Descent		
Continued-fraction (1520 to 123)	$2^{128.4}M_{q^2}$	$2^{128.4}M_{q^2}$
Classical (123 to 39)	$44\cdot 2^{121.3}M_{q^2}$	$2^{126.8}M_{q^2}$
Classical (39 to 24)	$1760\cdot 2^{115}M_{q^2}$	$2^{126}M_{q^2}$
Classical (24 to 20)	$2^{16}\cdot 2^{111}M_{q^2}$	$2^{127}M_{q^2}$
QPA (20 to 12)	$2^{21.3}\cdot(2^{54}M_{q^2}+2^{60}A_r)$	$2^{85.3}M_{q^2}$
QPA (12 to 7)	$2^{54.5}\cdot(2^{52}M_{q^2}+2^{60}A_r)$	$2^{118.5}M_{q^2}$
Gröbner bases (7 to 4)	$2^{87.2}\cdot$ (35.03 seconds)	$2^{120.3}M_{q^2}$
Gröbner bases (4 to 3)	$2^{94}\cdot$ (0.0277 seconds)	$2^{116.8}M_{q^2}$
Gröbner bases (3 to 2)	$2^{70.4}\cdot$ (0.005428 seconds)	$2^{90.9}M_{q^2}$

TABLE 3. Estimated costs of the main steps of the new DLP algorithm for computing discrete logarithms in $\mathbb{F}_{2^{24\cdot 3041}}$ ($q=2^{12}$). A_r and M_{q^2} denote the costs of an addition modulo the 3041-bit prime r and a multiplication in $\mathbb{F}_{2^{24}}$. We use the cost ratio $A_r/M_{q^2}=2^4$, and also assume that 2^{28} multiplications in $\mathbb{F}_{2^{24}}$ can be performed in 1 second (cf. §4.8).

4.5. **Classical descent.** Let $p=2$ and $\ell=12$. Let $s\in[0,\ell]$, and let $R\in\mathbb{F}_{q^2}[X,Y]$ with $\deg_Y R=e$. Then

$$h_1^e\cdot\left[R(X,X^{p^{\ell-s}})\right]^{p^s}=h_1^e\cdot R'(X^{p^s},X^{p^\ell})\equiv h_1^e\cdot R'(X^{p^s},h_0/h_1)\pmod{I_X}, \tag{18}$$

where R' is obtained from R by raising all its coefficients to the power p^s.

Let $Q\in\mathbb{F}_{q^2}[X]$ with $\deg Q=D$, and let $m<D$. One selects $s\in[0,\ell]$ and searches for a polynomial $R\in\mathbb{F}_{q^2}[X,Y]$ such that (i) $Q\mid R_1$ where $R_1=R(X,X^{p^{\ell-s}})$; (ii) $\deg R_1/Q$ and $\deg R_2$ are appropriately balanced where $R_2=h_1^e\cdot R'(X^{p^s},h_0/h_1)$; and (iii) both R_1/Q and R_2 are m-smooth. Taking logarithms of both sides of (18) then gives an expression for $\log_g Q$ in terms of the logarithms of polynomials of degree at most m.

A family of polynomials R satisfying (i) and (ii) can be constructed by finding a basis $\{(u_1,u_2),(v_1,v_2)\}$ of the lattice

$$L_Q=\{(w_1,w_2)\in\mathbb{F}_{q^2}[X]\times\mathbb{F}_{q^2}[X]\ :\ Q\mid(w_1(X)-w_2(X)X^{p^{\ell-s}})\}$$

where $\deg u_1$, $\deg u_2$, $\deg v_1$, $\deg v_2\approx D/2$. The points (w_1,w_2) in L_Q can be sampled to obtain polynomials $R(X,Y)=w_1(X)-w_2(X)Y$ satisfying (i) and (ii) by writing

$$(w_1,w_2)=a(u_1,u_2)+b(v_1,v_2)=(au_1+bv_1,au_2+bv_2)$$

with $a\in\mathbb{F}_{q^2}[X]$ monic of degree δ and $b\in\mathbb{F}_{q^2}[X]$ of degree $\delta-1$. We have $\deg w_1,\deg w_2\approx D/2+\delta$, so $\deg R_1=t_1\approx(D/2+\delta)+p^{\ell-s}$ and $\deg R_2=t_2\approx(D/2+\delta)p^s+2$. In order to ensure that the number of lattice points considered is enough to generate a polynomial R such that both R_1/Q and R_2 are m-smooth, the parameters s and δ must be selected

so that

$$q^{4\delta} \gg \frac{q^{2(t_1-D)}}{N_{q^2}(m, t_1 - D)} \cdot \frac{q^{2t_2}}{N_{q^2}(m, t_2)}. \tag{19}$$

Ignoring the time to compute a balanced basis of L_Q, the expected cost of finding a polynomial R satisfying (i)–(iii) is

$$\frac{q^{2(t_1-D)}}{N_{q^2}(m, t_1 - D)} \cdot \frac{q^{2t_2}}{N_{q^2}(m, t_2)} \cdot \min(S_{q^2}(m, t_1 - D), S_{q^2}(m, t_2)). \tag{20}$$

The expected number of distinct irreducible factors of R_1/Q and R_2 is $A_{q^2}(m, t_1 - D) + A_{q^2}(m, t_2)$. In the analysis, we shall assume that each of these irreducible factors has degree exactly m.

Three classical descent stages are employed. In the first stage, we have $D = 123$ and select $m = 39$, $s = 3$, $\delta = 2$, which yield $t_1 = 575$ and $t_2 = 506$. The expected cost of the descent stage for each of the 44 degree-123 polynomials is approximately $2^{93.7} \cdot S_{q^2}(39, 452)$. The expected total number of distinct irreducible polynomials of degree (at most) 39 obtained is approximately 1760.

In the second classical descent stage we have $D = 39$ and select $m = 24$, $s = 4$, $\delta = 2$, which yield $t_1 = 277$ and $t_2 = 338$. The expected cost of the descent for each of the 1760 degree-39 polynomials is approximately $2^{90.2} \cdot S_{q^2}(24, 238)$. The expected total number of distinct irreducible polynomials of degree (at most) 24 obtained is approximately 2^{16}.

In the third classical descent stage we have $D = 24$ and select $m = 20$, $s = 4$, $\delta = 2$, which yield $t_1 = 270$ and $t_2 = 226$. The expected cost of the descent for each of the 2^{16} degree-24 polynomials is approximately $2^{86.9} \cdot S_{q^2}(24, 226)$. The expected total number of distinct irreducible polynomials of degree (at most) 20 obtained is approximately $2^{21.3}$.

4.6. **QPA descent.** Two QPA descent stages are employed. In the first stage, we have $D = 20$ and select $m = 12$. For each Q, the expected cost of relation generation is $2^{34.8} \cdot S_{q^2}(12, 60)$ and the cost of the linear algebra is $2^{60} A_r$. Also for each Q, the expected number of distinct polynomials of degree at most 12 obtained is expected to be $A_{q^2}(12, 60) \cdot q^2 \approx 2^{33.2}$. Thus, the total number of distinct polynomials of degree at most 12 obtained after the first QPA descent stage is approximately $2^{54.5}$.

In the second stage, we have $D = 12$ and select $m = 7$. For each Q, the expected cost of relation generation is $2^{35} \cdot S_{q^2}(7, 36)$ and the cost of the linear algebra is $2^{60} A_r$. Also for each Q, the expected number of distinct polynomials of degree at most 7 obtained is expected to be $A_{q^2}(7, 36) \cdot q^2 \approx 2^{32.7}$. Thus, the total number of distinct polynomials of degree at most 7 obtained after the second QPA descent stage is approximately $2^{87.2}$.

4.7. **Gröbner bases descent.** Three Gröbner bases descent stages are employed. The first stage has $D = 7$ and $m = 4$, and is expected to yield approximately $2^{99.2}$ polynomials of degree (at most) 4. The second stage has $D = 4$ and $m = 3$ and is applied to all the 2^{94} monic irreducible quartics over $\mathbb{F}_{2^{24}}$. The third stage has $D = 3$ and $m = 2$ and is applied to all the $2^{70.4}$ monic irreducible cubics over $\mathbb{F}_{2^{24}}$. Our experiments were run using Magma v2.19-7 [14] on a 2.9 GHz Intel core i7-3520M.

In the first stage, for each degree-7 polynomial Q we have to solve a system of 26 quadratic polynomial equations in 32 variables over $\mathbb{F}_q$ (cf. (16)). After fixing some variables, each degree-5 R obtained from the variety of the resulting ideal is tested for 4-smoothness.

If no 4-smooth R is obtained, we randomly fix some other subset of variables and repeat. We ran 10,000 Gröbner bases descent experiments with randomly-selected degree-7 polynomials Q. On average, we had to find 1.806 Gröbner bases for each Q. The average number of R's tested for 4-smoothness for each Q was 1.252. The average time spent on each Q was 35.03 seconds.

For the second and third stages, we use the experimental results from §A.7 of [1].

4.8. **Overall running time.** The second column of Table 2 gives the running time estimates for the main steps of the new DLP algorithm in three units of time: A_r, M_{q^2}, and seconds. In order to assess the overall time, we make some assumptions about the ratios of these units of time.

First, we shall assume that $A_r/M_{q^2} = 2^4$. To justify this, we observe that a 3041-bit integer can be stored in 48 64-bit words. As in §3.8, the cost of A_r can be estimated to be 48 clock cycles. Using the carry-less multiplication instruction PCLMULQDQ, a multiplication in $\mathbb{F}_{2^{24}}$ can be performed at a price of 3-4 clock cycles. This gives us an A_r/M_{q^2} ratio of approximately 2^4.

Next, since a multiplication in M_{q^2} can be done in 15 clock cycles, we will transform one second on a 2.9 GHz machine (on which the Gröbner bases descent experiments were performed) into $2^{28}M_{q^2}$.

Using these estimates, we see from the third column of Table 3 that the overall running time of the new algorithm is approximately $2^{129.3}M_{q^2}$.

4.9. **Comparisons.** The upper bound of $2^{129.3}M_{q^2}$ on the running time of the new algorithm for computing logarithms in $\mathbb{F}_{2^{4\cdot 3041}}$ convincingly demonstrates that this field offers drastically less security than the 2^{192} resistance to attacks by Coppersmith's algorithm [6, 13]. As with the case of $\mathbb{F}_{3^{6\cdot 1429}}$, this decrease in security is even more pronounced when one considers that Coppersmith's algorithm is not effectively parallelizable whereas the new algorithm offers many avenues for parallelization.

References

[1] G. Adj, A. Menezes, T. Oliveira and F. Rodríguez-Henríquez, "Weakness of $\mathbb{F}_{3^{509}}$ for discrete logarithm cryptography", *Pairing-Based Cryptography – Pairing 2013*, to appear; available at http://eprint.iacr.org/2013/446.

[2] R. Barbulescu, P. Gaudry, A. Joux and E. Thomé, "A quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic: Improvements over FFS in small to medium characteristic", available at http://eprint.iacr.org/2013/400.

[3] P. Barreto, H. Kim, B. Lynn and M. Scott, "Efficient algorithms for pairing-based cryptosystems", *Advances in Cryptology – CRYPTO 2002*, LNCS 2442 (2002), 354–368.

[4] I. Blake, R. Fuji-Hara, R. Mullin and S. Vanstone, "Computing logarithms in finite fields of characteristic two", *SIAM Journal on Algebraic and Discrete Methods*, 5 (1984), 276–285.

[5] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil pairing", *Journal of Cryptology*, 17 (2004), 297–319.

[6] D. Coppersmith, "Fast evaluation of logarithms in fields of characteristic two", *IEEE Transactions on Information Theory*, 30 (1984), 587–594.

[7] D. Coppersmith, "Solving homogeneous linear equations over $GF(2)$ via block Wiedemann algorithm", *Mathematics of Computation*, 62 (1994), 333–350.

[8] G. Frey and H. Rück, "A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves", *Mathematics of Computation*, 62 (1994), 865–874.

[9] F. Göloğlu, R. Granger, G. McGuire and J. Zumbrägel, "On the function field sieve and the impact of higher splitting probabilities: Application to discrete logarithms in $\mathbb{F}_{2^{1971}}$", *Advances in Cryptology – CRYPTO 2013*, LNCS 8043 (2013), 109–128.
[10] R. Granger and J. Zumbrägel, "On the security of supersingular binary curves", presentation at ECC 2013, September 16 2013.
[11] A. Joux, "A new index calculus algorithm with complexity $L(1/4+o(1))$ in very small characteristic", *Selected Areas in Cryptography – SAC 2013*, to appear; available at http://eprint.iacr.org/2013/095.
[12] A. Joux and R. Lercier, "The function field sieve in the medium prime case" *Advances in Cryptology – EUROCRYPT 2006*, LNCS 4004 (2006), 254–270.
[13] A. Lenstra, "Unbelievable security: Matching AES security using public key systems", *Advances in Cryptology – ASIACRYPT 2001*, LNCS 2248 (2001), 67–86.
[14] Magma v2.19-7, http://magma.maths.usyd.edu.au/magma/.
[15] A. Menezes, T. Okamoto and S. Vanstone, "Reducing elliptic curve logarithms to logarithms in a finite field", *IEEE Transactions on Information Theory*, 39 (1993), 1639–1646.
[16] D. Wiedemann, "Solving sparse linear equations over finite fields", *IEEE Transactions on Information Theory*, 32 (1986), 54–62.

Computer Science Department, CINVESTAV-IPN
E-mail address: gora.adj@gmail.com

Department of Combinatorics & Optimization, University of Waterloo
E-mail address: ajmeneze@uwaterloo.ca

Computer Science Department, CINVESTAV-IPN
E-mail address: thomaz.figueiredo@gmail.com

Computer Science Department, CINVESTAV-IPN
E-mail address: francisco@cs.cinvestav.mx