A Subexponential Algorithm for Discrete Logarithms over All Finite Fields

Leonard M. Adleman and Jonathan DeMarrais

Department of Computer Science, University of Southern California, Los Angeles CA 90089

Abstract. There are numerous subexponential algorithms for computing discrete logarithms over certain classes of finite fields. However, there appears to be no published subexponential algorithm for computing discrete logarithms over all finite fields. We present such an algorithm and a heuristic argument that there exists a $c \in \Re_{>0}$ such that for all sufficiently large prime powers p^n, the algorithm computes discrete logarithms over GF(p^n) within expected time:

$$e^{c(\log(p^n)\log\log(p^n))^{1/2}}$$

1 Introduction

Given α, β in a finite field, the discrete logarithm problem is to calculate an $x \in Z_{\geq 0}$ (if such exists) such that:

$$\alpha^x = \beta$$

Interest in the discrete logarithm problem first arose when Diffie and Hellman proposed a public key cryptographic system based on the complexity of this problem[DH]. Additional systems using discrete logarithms have since been proposed, including ElGamal's crypto-system[El1]. Recently the goverment has proposed using a system of this type as a standard. These present systems are based on finite fields of special form for which subexponential algorithms already exist. However, it is likely that these systems can be generalized to work with arbitrary finite fields. Previously, no subexponential algorithms existed for all such fields. We present such an algorithm along with a heuristic argument that there exists a $c \in \Re_{>0}$ such that for all sufficiently large prime powers p^n, the algorithm computes discrete logarithms over GF(p^n) within expected time:

$$e^{c(\log(p^n)\log\log(p^n))^{1/2}}$$

There exist several algorithms which for all primes $p \in Z_{>0}$ compute discrete logarithms over GF(p) in time subexponential in p (e.g. [Ad1, Go1]). Further, for all primes $p \in Z_{>0}$, there exists algorithms which for all $n \in Z_{>0}$ computes discrete logarithms over GF(p^n) in time subexponential in p^n (for $p = 2$, this was first shown by Hellman and Reyneri [HR] and improved by Coppersmith [Co]; however, these approaches appear to generalize to an arbitrary prime p).

D.R. Stinson (Ed.): Advances in Cryptology - CRYPTO '93, LNCS 773, pp. 147-158, 1994.

ElGamal [El2] has given an algorithm which for all primes $p \in Z_{>0}$ compute discrete logarithms over $\mathrm{GF}(p^2)$ in time subexponential in p^2. Previously, the most general subexponential algorithm appears to be that of Lovorn [Lo] which computes discrete logarithms in $\mathrm{GF}(p^n)$ for $\log(p) \leq n^{0.98}$.

Our subexponential method for all finite fields actually consists of two algorithms. They both may be described as 'index calculus' methods [WM, Od]. The first algorithm is for the case $n < p$. Here, $\mathrm{GF}(p^n)$ is represented by $O/(p)$ where O is a number ring and (p) is the prime ideal generated by p. An element of $O/(p)$ is considered 'smooth' iff when considered as an element of O, the ideal it generates factors into prime ideals of small norm. The second algorithm is for the case $n \geq p$. Here, $\mathrm{GF}(p^n)$ is represented by $(Z/pZ[x])/(f)$ where $f \in Z/pZ[x]$ is irreducible. An element of $(Z/pZ[x])/(f)$ is considered 'smooth' iff when considered as an element of $Z/pZ[x]$ it factors into irreducible polynomials of small degree. The second algorithm is rather 'routine'. The first algorithm makes use of the notions of singular integers and character signatures which were introduced in the context of integer factoring [Ad2]. The first algorithm can be thought of as reducing the computation of discrete logarithms in $\mathrm{GF}(p^n)$ to the computation of discrete logarithms in several fields of the form $\mathrm{GF}(p')$ where $p' \in Z_{>0}$ is prime.

2 Preliminaries

In this section some basic facts are presented.

2.1 Singular Integers and Character Signatures

Here, some notions about presented in [Ad2] about integer factoring are generalized.

Definition: For all number fields K with ring of integers O, for all $s \in Z_{>0}$, and for all $\sigma \in O$, σ is an s-singular integer (with respect to O) iff there exists an ideal $I \subseteq O$ such that $(\sigma) = I^s$.

Let K be a number field with ring of integers O, unit group E and ideal class group C. Let $s \in Z_{>0}$ and let σ, τ be s-singular integers. Define $\sigma \approx \tau$ iff there exists $\alpha, \beta \in O$ such that $\alpha^s \sigma = \beta^s \tau$. "$\approx$" is an equivalence relation on s-singular integers, and the set of equivalence classes form a group $G(s)$ of exponent dividing s with identity $I(s) = \{\alpha^s | \alpha \in O\}$ under the operation:

$$[\alpha][\beta] \mapsto [\alpha\beta]$$

There is a homomorphism ψ from $G(s)$ onto the group $C(s) = \{c | c \in C \ \& \ c^s = [(1)]\}$.

$$[\alpha] \stackrel{\psi}{\mapsto} [I]$$

where $(\alpha) = I^s$.

The kernel of ψ, $\mathrm{Ker}(\psi) = \{[u] | u \in E\}$ and consequently $\mathrm{Ker}(\psi) \cong E/E^s$. Hence

$$(*) \quad G(s) \cong E/E^s \bigoplus C(s)$$

Definition: For all number fields K with ring of integers O, for all $s \in Z_{>0}$, for all prime ideals $P_1, P_2, \ldots, P_z \subset O$, for all $l_1, l_2, \ldots, l_z \in O$ and for all $\sigma \in O$: if for $i = 1, 2, \ldots, z$, $(\sigma) + P_i = (1), s | (N(P_i) - 1)$ and $l_i + P_i$ is a primitive s^{th} root of unity in O/P_i^*, then the s-character signature of σ with respect to $< P_1, l_1 >, < P_2, l_2 >, \ldots, < P_z, l_z >$ is: $< e_1, e_2, \ldots, e_z >$ where for $i = 1, 2, \ldots, z$, $\sigma^{(N(P_i)-1)/s} \equiv l_i^{e_i} \bmod P_i$ and $e_i \in Z_{\geq 0}^{<s}$.

Now assume that K is Abelian over Q, then it follows from the Čebotarev density theorem that for all $s \in Z_{>0}$, for all prime ideals $P_1, P_2, \ldots, P_z \subset O$, and for all $c \in G(s)$, there exists a $\sigma \in O$ such that $[\sigma] = c$ and for $i = 1, 2, \ldots, z$, $(\sigma) + P_i = (1)$. For $< P_1, l_1 >, < P_2, l_2 >, \ldots, < P_z, l_z >$ as above, let the map θ take c to the s-character signature of σ with respect to $< P_1, l_1 >, < P_2, l_2 >, \ldots, < P_z, l_z >$. θ is well defined on $G(s)$ and is a group homomorphism into $\bigoplus_{i=1}^{z} Z_s$.

2.2 Subfields of cyclotomic fields

Let $q \in Z_{>0}$ be prime and let $n | q - 1$, then there exists a unique field $K_{q,n} \subseteq Q(\zeta_q)$, the q^{th} cyclotomic field, such that $[K_{q,n} : Q] = n$. The following are well known [Ed]:

1. The ring of integers of $K_{q,n}$, $O_{q,n} = Z[\eta_0, \eta_1, \ldots, \eta_{n-1}]$, where for $i = 0, 1, \ldots, n-1$, $\eta_i = \eta_{q,n,i} = \sum \zeta_q^a$, where the sum is taken over the set of $a \in Z_{>0}^{\leq q-1}$ such that $ind(a) \equiv i \bmod n$ where $ind(a)$ denotes the index of a in Z/qZ^* with respect to a fixed generator.
2. $K_{q,n} = Q(\eta_0)$ (however, there exist q, n such that $O_{q,n} \neq Z[\eta_0]$).
3. The minimum polynomial for η_0 over Q is $f = f_{q,n} = \prod_{i=0}^{n-1} (x - \eta_i)$
4. If $p \in Z_{>0}$ is prime and p is inert in $K_{q,n}$, then $O_{q,n}/(p)$ is a finite field with p^n elements and

$$R = R_{q,n,p} = \{\sum_{i=0}^{n-1} a_i \eta_i | a_i \in Z_{\geq 0}^{\leq p}, i = 0, 1, \ldots, n-1\}$$

is a complete set of representatives.

Arithmetic in $K_{q,n}$ may be done as follows (our description is essentially that of Edwards [Ed] which in turn is derived from Kummer).

Elements in $O_{q,n}$ will be represented in terms of the integer basis $\eta_0, \eta_1, \ldots, \eta_{n-1}$.

First, for $i, j, k \in Z_{\geq 0}^{\leq n-1}$ calculate $c_{i,j,k} \in Z$ such that:

$$\eta_i \eta_j = \sum_{k=0}^{n-1} c_{i,j,k} \eta_k$$

then multiplication in $O_{q,n}$ is straightforward.

Prime ideals of $O_{q,n}$ will be represented as follows. Let $s \neq q$ be a rational prime and let f be the order of s in Z/qZ^*. Let $e = (q-1)/f$, then the splitting field of s is $K_{q,e}$. Let $g = (e,n)$, then s splits into g distinct prime ideals of residue class degree n/g in $O_{q,n}$.

Let $h \in Z/sZ[x]$ be an irreducible factor of $f_{q,q-1} = x^{q-1} + \ldots + x + 1$ (the q^{th} cyclotomic polynomial) and let σ be a generator for $\mathrm{GAL}(Q(\zeta_q)/Q)$ (the construction which follows produced the correct outcome for all choices of σ).

For $i = 1, 2, \ldots, g$, let $\tilde{S}_i \subseteq O_{q,q-1}$ be the prime ideal generated by s and $(h(\zeta_q))^{\sigma^i}$, and let $S_i = \tilde{S}_i \cap O_{q,n}$. Then $(s) = \prod_{i=1}^{g} S_i$ is the prime decomposition of s in $O_{q,n}$.

For $i = 1, 2, \ldots, g$, $j = 0, 1, \ldots, e-1$, calculate $u_{i,j} \in Z_{\geq 0}^{<s}$ such that

$$u_{i,j} \equiv \eta_{q,e,j} \bmod \tilde{S}_i$$

(such $u_{i,j}$ always exist [Ed]). Let $U = \{u_{i,j} | j = 0, 1, \ldots, e-1\}$ (U is the set of roots of $f_{q,e}$ mod s and is independent of i). Let $\psi_i = \prod_{j=0}^{e-1} \prod_{u \in U, u \neq u_{i,j}} (u - \eta_{i,j})$. For $i = 1, 2, \ldots, g$, $< s, \psi_i >$ will represent the prime ideal S_i of $O_{q,n}$ lying above s.

Let $\alpha \in O_{q,n}$, and let $a \in Z_{\geq 0}$. Then:

$$\begin{gathered} S_i^a | (\alpha) \\ \text{iff} \\ S_i^a O_{q,q-1} | \alpha O_{q,q-1} \\ \text{iff} \\ \tilde{S}_i^a | \alpha O_{q,q-1} \\ \text{iff} \\ p^a | \psi_i^a \alpha \end{gathered}$$

The penultimate statement follows from Galois theory by noting that $\alpha \in K_{q,n}$. The last statement is essentially the first proposition of section 4.10 [Ed]. Hence there is a computationally efficient method for determining the power of S_i which divides (α).

Next consider singular integers and character signatures in $K_{q,n}$. Let $s \in Z_{>0}$. By Dirichlet's unit theorem, E/E^s can be written as the direct sum of at most n cyclic groups. Because the class number of $K_{q,n}$ is less than or equal to the class number of $Q(\zeta_q)$ ([Wa], Thrm 10.1), which is less than or equal to q^{q^3} [Ne], it follows that $C(s)$ can be written as the direct sum of at most $q^3 \log_2(q)$ cyclic groups. By (*) above, $G(s)$ can be written as the direct sum of at most $n + q^3 \log_2(q)$ cyclic groups. Let $H = n + q^3 \log_2(q) + 1$. If $\sigma_1, \sigma_2, \ldots, \sigma_H$ are s-singular integers then there exist $\delta \in O_{q,n}$ and $b_1, b_2, \ldots, b_H \in Z_{\geq 0}^{<s}$ such

that $\mathrm{GCD}(b_1, b_2, \ldots, b_H) = 1$ and $\prod_{j=1}^{H} \sigma_j^{b_j} = \delta^s$. Further, if $\theta_1 = \theta(\sigma_1), \theta_2 = \theta(\sigma_2), \ldots, \theta_H = \theta(\sigma_H)$ are the s-signatures of $\sigma_1, \sigma_2, \ldots, \sigma_H$ with respect to some $< P_1, l_1 >, < P_2, l_2 >, \ldots, < P_z, l_z >$ then $\sum_{j=1}^{H} b_j \theta_j = 0$. Finally, given the prime factorization of s and given the s-signatures $\theta_1, \theta_2, \ldots, \theta_H$, it can be shown that there exists an algorithm to calculate a sequence of b_j's, such that $\sum_{j=1}^{H} b_j \theta_j = 0$. This algorithm requires time at most $O(H^2 z \log^3(s))$.

2.3 Smooth numbers

For all $\gamma \in \Re_{>0}^{<1}$ and $\delta \in \Re_{>0}$, $L_x[\gamma, \delta]$ denotes the set of functions from $\Re$ to $\Re$ of the form [CEP]:

$$e^{(\delta + o(1))(\log(x))^{\gamma}(\log\log(x))^{1-\gamma}} \quad x \to \infty$$

It will be helpful in the running time analyses which follow to note that for all $\gamma \in \Re_{>0}^{<1}$, $\delta \in \Re_{>0}$, $L \in L_x[\gamma, \delta]$ and $c \in Z_{>0}$:

$$(\log(x)^c) L \in L_x[\gamma, \delta]$$

For all $\alpha, \gamma \in \Re_{>0}^{<1}$ with $\alpha < \gamma$, for all $\beta, \delta \in \Re_{>0}$, $L_0 \in L_x[\gamma, \delta]$ and $L_1 \in L_x[\alpha, \beta]$, there exists an $L_2 \in L_x[\gamma - \alpha, (\gamma - \alpha)\delta/\beta]$ such that for all $N \in \Re_{>0}$, the probability that a positive integer less than or equal to $L_0(N)$ is $L_1(N)$-smooth is at least $1/L_2(N)$ ($L_1(N)$-smooth means all positive prime divisors are less than or equal to $L_1(N)$.

Notation

For all $p, n \in Z_{>0}$ with p prime, if we write $f \in Z/pZ[x]$ then it will be assumed that $f = \sum_{i=0}^{n} a_i x^i$ where for $i = 1, 2, \ldots, n$, $a_i \in Z_{\geq 0}^{<p}$.

3 Algorithm I

This algorithm will be used for discrete logarithms over $\mathrm{GF}(p^n)$ when $p > n$.

First, the discrete logarithm problem over $\mathrm{GF}(p^n)$ will be reduced to the discrete logarithm problem over special finite fields of the form $O_{q,n}/(p)$ (see Preliminaries section).

Let $p \in Z_{>0}$ be prime and $f_1 \in Z/pZ[x]$ irreducible, monic of degree n. Then $(Z/pZ[x])/(f_1)$ is a finite field with p^n elements. Let $\alpha_1, \beta_1 \in Z/pZ[x]$ of degree less than n such that $[\alpha_1]$ generates $(Z/pZ[x])/(f_1)^*$ and $\beta_1 \not\equiv 0 \bmod f_1$. (If α_1 is not a generator, randomly choose one, and solve for both α_1 and β_1.) Hence there exists an x such that $0 \leq x \leq p^n - 1$ and $\alpha_1^x \equiv \beta_1 \bmod f_1$. Assume that $p, f_1, \alpha_1, \beta_1$ are given and x is sought. Then one may proceed as follows:

Using the construction in [AL] find an $f \in Z/pZ[x]$ irreducible of degree n in random time polynomial in $\log(p)$ and n (assuming ERH). Hence $(Z/pZ[x])/(f) \cong (Z/pZ[x])/(f_1)$. Using [Le] calculate α_2 and $\beta_2 \in Z/pZ[x]$ of degree less than n such that $[\alpha_2]$ is the image of $[\alpha_1]$ and $[\beta_2]$ is the image of $[\beta_1]$ under

this isomorphism. Hence our original problem is reduced to the problem: given p, f, α_2, β_2 with $[\alpha_2]$ generating $(Z/pZ[x])/(f)^*$ and $\beta_2 \not\equiv 0 \bmod f$, calculate x such that $0 \leq x \leq p^n - 1$ and $\alpha_2^x \equiv \beta_2 \bmod f$.

By the construction in [AL] (also see [BS]), there exists a $\tilde{c} \in Z_{>0}$ such that $f = f_{q,n}$ for some prime $q \in Z_{>0}$ with $q \leq \tilde{c}n^4(log(np))^2$ (assuming ERH). Since f is irreducible in $Z/pZ[x]$, it follows that p is inert in $K_{q,n}$. There exists the following isomorphism from $(Z/pZ[x])/(f)$ to $O_{q,n}/(p)$:

$$[\sum_{i=0}^{n-1} g_i x^i] \mapsto [\sum_{i=0}^{n-1} g_i (\sum_{j=0}^{n-1} d_{i,j}\eta_{q,n,j})]$$

where for $i = 0, 1, \ldots, n-1$, $\eta_{q,n,0}^i = \sum_{j=0}^{n-1} d_{i,j}\eta_{q,n,j}$, where $d_{i,j} \in Z$.

Calculate $\alpha_3, \beta_3 \in O$ such that $[\alpha_3]$ is the image of $[\alpha_2]$ and $[\beta_3]$ is the image of $[\beta_2]$ under this isomorphism. By reducing coefficients modulo p find $\alpha, \beta \in R_{q,n,p}$ such that $\alpha \equiv \alpha_3 \bmod p$ and $\beta \equiv \beta_3 \bmod p$. Hence the original problem becomes that of calculating x such that $0 \leq x \leq p^n - 1$ and $\alpha^x \equiv \beta \bmod p$.

Below, a family of algorithms $\{A_y\}_{y \in Z_{>0}}$ is presented. It will be argued that for sufficiently large y, A_y on all inputs q, n, p, α, β such that $p, q \in Z_{>0}$ are prime, $n < p$, $n|q-1$, $q \leq \tilde{c}n^4(log(np))^2$, p inert in $K_{q,n}$, and $\alpha, \beta \in R_{q,n,p}$ with $[\alpha]$ generating $O_{q,n}/(p)^*$ and $\beta \not\equiv 0 \bmod p$, outputs x such that $0 \leq x \leq p^n - 1$ and $\alpha^x \equiv \beta \bmod p$.

Let $L_0 \in L_x[1/2, \sqrt{1/2}]$.

Algorithm A_y

Stage 0 input q, n, p, α, β

Stage 1 Set $N = p^{yn}$. Set (the 'smoothness bound') $B = L_0(N)$. Set $H = n + q^3 \log_2(q) + 1$.

Stage 2 Calculate $T = \{I | I$ is a prime ideal of O, $q \notin I$ and I lies over a rational prime $< B\}$. Let $w = \#T$ and let $< I_1, I_2, \ldots, I_w >$ be an ordering of T.

Stage 3 Set $j = 1$. While $j \leq H$:

Stage 3(a) Set $z = 1$. While $z \leq w + 1$: Choose random r, s with $0 \leq r, s \leq p^n - 1$ and calculate $\gamma \in R_{q,n,p}$ such that $\gamma \equiv \alpha^r \beta^s \bmod (p)$. If $(\gamma) = \prod_{i=1}^{w} I_i^{e_i}$ (i.e. if the ideal generated by γ is B-smooth) then set $\gamma_{j,z} = \gamma$, $r_{j,z} = r$, $s_{j,z} = s$, $v_{j,z} =< e_1, e_2, \ldots, e_w >$ and $z = z + 1$.

Stage 3(b) Calculate $a_1, a_2, \ldots, a_{w+1} \in Z_{\geq 0}^{<p^n-1}$ such that GCD(a_1, a_2, $\ldots$, a_{w+1}) $= 1$ and $\sum_{i=1}^{w+1} a_i v_{j,i} \equiv < 0, 0, \ldots, 0 > \bmod p^n - 1$. Calculate $\sigma_j = \prod_{i=1}^{w+1} \gamma_{j,i}^{a_i}$. Set $j = j + 1$.

Stage 4 For $j = 1, 2, \ldots, H$, calculate θ_j the $(p^n - 1)$-signature of σ_j with respect to $< S_1, m_1 >, < S_2, m_2 >, \ldots, < S_{2H}, m_{2H} >$. For $j = 1, 2, \ldots, H$, $k = 1, 2, \ldots, 2H$, $S_k \subset O_{q,n}$ is a prime ideal such that $(\sigma_j) + S_k = (1)$, $(p^n - 1)|N(S_k) - 1$ and m_k is a primitive $(p^n - 1)^{th}$ root of unity in O/S_k.

Stage 5 Calculate $b_1, b_2, \ldots, b_H \in Z_{\geq 0}^{<p^n-1}$ such that $GCD(b_1, b_2, \ldots, b_H) = 1$ and $\sum_{j=1}^{H} b_j \theta_j \equiv < 0, 0, \ldots, 0 > \bmod (p^n - 1)$.

Stage 6 Calculate $k = \sum_{j=1}^{H} \sum_{i=1}^{w+1} (r_{j,i} a_i b_j)$ and $l = \sum_{j=1}^{H} \sum_{i=1}^{w+1} (s_{j,i} a_i b_j)$. If $\alpha^k \beta^l \not\equiv 1 \bmod (p)$ then go to stage 3.

Stage 7 If $(l, p^n - 1) \neq 1$ then go to stage 3, Else calculate and output $x \equiv -k/l \bmod p^n - 1$ and halt.

4 Analysis of Algorithm I

In this section computational details of Algorithm I will be described and there will be an analysis of the expected number of steps required by the algorithm on all inputs q, n, p, α, β such that $p, q \in Z_{>0}$ are prime with $n < p$, $n | q - 1$, $q \leq \tilde{c} n^4 (log(np))^2$, p inert in $K_{q,n}$, and α, $\beta \in R_{q,n,p}$ with $[\alpha]$ generating $O_{q,n}/(p)^*$ and $\beta \not\equiv 0 \bmod p$. For convenience the argument will be for p^n sufficiently large.

To begin, consider the expected number of steps required by a single pass through each of the stages of the algorithm.

The time required for stages 0,1,6 and 7 are dominated by the time required by other stages.

Stage 2: Test all numbers less than or equal to B for primality. For each prime $s \neq q$ found, calculate the representatives $< s, \psi_i >$ of the prime ideals of $O_{q,n}$ lying above s and add them to T (see Preliminaries section).

Using random polynomial time primality testing [SS, AH] and random polynomial time finite field polynomial factorization [Be] and observing that because of the size constraints on q, orders can be computed naively, it follows that there exists an $L_1 \in L_x[1/2, \sqrt{1/2}]$ such that the expected number of steps for a pass through stage 2 is at most $L_1(N)$.

Further, since each rational prime has at most n primes lying over it in $O_{q,n}$, it follows that there exists an $L_2 \in L_x[1/2, \sqrt{1/2}]$ such that $w = \#T \leq L_2(N)$.

Stage 3(a): A γ will be tested for B-smoothness by the following method: First the norm of γ will be calculated and tested for B-smoothness. Those γ which have B-smooth norms will then be factored as ideals (see Preliminaries section).

A bound on the norm of γ will be needed.

$$\gamma = \sum_{i=0}^{n-1} g_i \eta_i,$$

where $0 \leq g_i \leq p - 1$ for $i = 0, 1, \ldots, n - 1$. Hence γ is the sum of $q - 1$ terms each of the form $g\zeta_q^c$ where $0 \leq g \leq p - 1$ and $c \in Z_{\geq 0}^{<q}$. This is also the form of the n conjugates of γ. Hence the norm of $\gamma = \prod_{\sigma \in Gal(K_{q,n}/Q)} \gamma^\sigma$ is the sum of $(q-1)^n$ terms, the largest of which has absolute value p^n. By the constraints on q and n, it follows that there exists a $y_0 \in Z_{>0}$ such that $N(\gamma) \leq p^{y_0 n} \leq N$ for all algorithms A_y with $y \geq y_0$. Henceforth assume that $y \geq y_0$.

Making the usual assumption [LLMP] that the probability that $N(\gamma)$ is B-smooth (the exception of the prime q is inconsequential) is equal to the probability that a random positive integer less than N is B-smooth, (see Preliminaries section) there exists an $L_3 \in L_x[1/2, \sqrt{1/2}]$ such that the probability that γ is

B-smooth is at least $1/L_3(N)$ (B-smooth means that all prime ideals dividing (γ) have norm less than or equal to B). Since w B-smooth γ's are needed, it follows that there exists an $L_4 \in L_x[1/2, \sqrt{2}]$ such that the expected number of γ's which must be generated and tested for B-smoothness is at most $L_4(N)$.

The norm of each γ may be tested for B-smoothness naively. Hence there exists an $L_5 \in L_x[1/2, 3/\sqrt{2}]$ such that the expected number of steps required for a single pass through stage 3(a) will be at most $L_5(N)$.

Stage 3(b) There must exist $a_1, a_2, \ldots, a_{w+1} \in Z_{\geq 0}^{<p^n-1}$ such that GCD(a_1, a_2, ..., a_{w+1}) = 1 and $\sum_{i=1}^{w+1} a_i v_{j,i} \equiv < 0, 0, \ldots, 0 > \bmod(p^n - 1)$. Further, there exists an algorithm which will find $a_1, a_2, \ldots, a_{w+1}$ in $O(w^3 \log^2(p^n))$ steps. Hence there exists an $L_6 \in L_x[1/2, 3/\sqrt{2}]$ such that the expected time for a single pass through stage 3(b) is at most $L_6(N)$.

Stage 4: Check numbers of the form $1 + a(q(p^n - 1))$ until primes s_1, s_2, ..., $s_{2H/n}$ are found. For $k = 1, 2, \ldots, 2H/n$, let $g_k \in Z_{\geq 0}^{<s_k}$ generate Z/s_kZ^* and let $g \in Z_{\geq 0}^{<q}$ generate Z/qZ^*. For $k = 1, 2, \ldots, 2H/n$, $l = 1, 2, \ldots, n$: Let $\tilde{S}_{k,l} \subseteq O_{q,q-1}$ be the prime ideal generated by s and $\zeta_q^{d_l} - c_k$, where $c_k \equiv g_k^{a(p^n-1))} \bmod s$ and $d_l \equiv g^l \bmod q$. Let $S_{k,l} = \tilde{S}_{k,l} \cap O_{q,n}$. $S_{k,1}, S_{k,2}, \ldots, S_{k,n}$ are the (distinct, residue class degree 1) prime ideals of $O_{q,n}$ lying above s_k. Since $s_k \equiv 1 \bmod q(p^n - 1)$, it follows that $(p^n - 1) | (N(S_{k,l}) - 1)$ and $N(S_{k,l}) > B$. Since for $j = 1, 2, \ldots, H$, (σ_j) is B-smooth, it follows that $(\sigma_j) + S_{k,l} = (1)$. Let $m_k = g_k^{aq} \bmod s_k$. Then the $2H$ pairs $< S_{k,l}, m_k >$ will be as required for stage 4.

Assume that approximately the 'expected' number of primes will be found in an arithmetic progression: assume that for all $m, b \in Z_{>0}$, with $b > m \log(m)^3$: $\#\{a | 1 + am < b \ \& \ 1 + am \text{ prime}\} > b/m \log(b)^2$. Letting $v = 2H/n$ and $m = q(p^n - 1)$, then all of the v primes needed above can be found by checking less than $v \log(v)^3 \log(m)^3$ a's and each prime s found will be less than $mv \log(v)^3 \log(m)^3$. The constraints on n and q imply that there exists a $c_1, c_2 \in Z_{>0}$ such that $v \log(v)^3 \log(m)^3 < (n \log(p))^{c_1}$ and $mv \log(v)^3 \log(m)^3 < p^n (n \log(p))^{c_2}$. Hence the required primes can be found and tested for primality [AH, SS] in a negligible number of steps.

Generators for Z/s_kZ^* are abundant ([AH], Lemma 4). Checking a candidate g to determine whether it is a generator will be done by factoring $s-1$ and testing that for all primes $t | s - 1$, $g^{(s-1)/t} \not\equiv 1 \bmod s$. The factorization can be done using an '$L[1/2, 1]$' factoring method (e.g. [Le2]). A similar argument shows that a generator for Z/qZ^* can be found in a negligible number of steps.

$O_{q,n}/S_{k,l} \cong Z/s_kZ$ where the isomorphism is induced by $\zeta_q^{d_l} \mapsto c_k$. Hence the calculations of the $(p^n - 1)$-signatures of the σ_j's is a set of discrete logarithm problem over Z/s_kZ. Using the bounds on $2H$ and the primes s together with an '$L[1/2, 1]$' discrete logarithm algorithm for finite prime fields (e.g. [Po]), it follows that there exists an $L_7 \in L_x[1/2, 1]$ such that the expected number of steps required for a single pass through stage 4 is at most $L_7(N)$.

Stage 5: The required $b_1, b_2, \ldots, b_H$ can be shown to always exist and can be found in time $O(H^3 \log^3(p^n - 1))$. Using the bounds on q, it follows that the

number of steps required for a single pass through stage 5 is negligible.

It will next be shown that the expected number of passes through stages of the algorithm is negligible. Stages will be repeated only if required in stage 6 or stage 7.

Stage 6 will cause stages of the algorithm to be repeated only if $\alpha^k\beta^l \not\equiv 1 \bmod (p)$. One has:

$$\begin{gathered}\alpha^k\beta^l = \\ \prod_{i,j}\alpha^{r_{j,i}a_ib_j}\beta^{s_{j,i}a_ib_j} = \\ \prod_j(\prod_i(\alpha^{r_{j,i}}\beta^{s_{j,i}})^{a_i}))^{b_j} \equiv \\ \prod_j(\prod_i\gamma_{j,i}^{a_i})^{b_j} = \\ \prod_j\sigma_j^{b_j}\end{gathered}$$

By the construction, the σ_j's are (p^n-1)-singular integers. By the arguments in the Preliminaries section there exists a $\delta \in O_{q,n}$ and $b_1, b_2, \ldots, b_H \in Z_{\geq 0}^{<p^n-1}$ such that $\mathrm{GCD}(b_1, b_2, \ldots, b_H) = 1$ and $\prod_{j=1}^H \sigma_j^{b_j} = \delta^{p^n-1}$. $G(p^n-1)$ is a group of index dividing p^n-1 which is the direct product of at most $H-1$ cyclic groups (see Preliminaries section). The signature homomorphism θ maps $G(p^n-1)$ into a group which is the direct product of $2H$ cyclic groups of order p^n-1. It is reasonable to assume that this map is an embedding and hence that these $b_1, b_2, \ldots, b_H$ are the ones found in stage 5. It follows that:

$$\begin{gathered}\alpha^k\beta^l \equiv \\ \prod_j\sigma^{b_j} = \\ \delta^{p^n-1} \equiv \\ 1\end{gathered}$$

Stage 7 will cause stages of the algorithm to be repeated only if $(l, p^n-1) \neq 1$. However, $(l, p^n-1) = 1$ with probability $\phi(p^n-1)/(p^n-1) \geq 1/c\log p^n$ where $c \in \Re_{>0}$ is independent of p and n ([AH], Lemma 4). Briefly, this can be argued as follows: Since from stage 3(b) $\mathrm{GCD}(a_1, a_2, \ldots, a_{w+1}) = 1$ and from stage 5 $GCD(b_1, b_2, \ldots, b_H) = 1$ it follows that for all primes t dividing p^n-1, there exist $i \in Z_{>0}^{\leq w+1}$ and $j \in Z_{>0}^{\leq H}$ such that a_ib_j is relatively prime to t. Consider $\gamma_{j,i} \equiv \alpha^{r_{j,i}}\beta^{s_{j,i}}$, and observe that for all $s \in Z_{\geq 0}^{<p^n-1}$, there exists a unique $r \in Z_{\geq 0}^{<p^n-1}$ such that $\gamma_{j,i} \equiv \alpha^r\beta^s$. Hence $s_{j,i}$ is 'random' mod t and consequently $l = \sum_{j=1}^H\sum_{i=1}^{w+1}(s_{j,i}a_ib_j)$ is also 'random' mod t.

Recalling that in algorithm A_y, $N = p^{y^n}$, it follows that there exists a $c_I \in \Re_{>0}$ and an $L_I \in L_x[1/2, c_I]$ such that for all sufficiently large y, the expected number of steps required by Algorithm A_y is $L_I(p^n)$ on all inputs q, n, p, α, β such that $p, q \in Z_{>0}$ are prime, $n < p$, $n|q-1$, $q \leq \tilde{c}n^4(log(np))^2$, p inert in $K_{q,n}$, and α, $\beta \in R_{q,n,p}$ with $[\alpha]$ generating $O_{q,n}/(p)^*$ and $\beta \not\equiv 0 \bmod p$. Hence there exists a $c_I \in \Re_{>0}$ such that the expected number of steps required by Algorithm I (when $n < p$) is:

$$e^{c_I(\log(p^n)\log\log(p^n))^{1/2}}$$

Finally, it is clear from stages 6 and 7 that the output of the algorithm is x such that $\alpha^x \equiv \beta \bmod p$.

5 Algorithm II

This algorithm will be used for discrete logarithms over GF(p^n) when $p \leq n$.

Algorithm II is a generalization of the algorithm for GF(2^n) by Hellman and Reyneri discussed in Coppersmith [HR, Co].

It is assumed that the inputs to the algorithm are p, f, α, β such that $p \in Z_{>0}$ is prime, $f \in Z/pZ[x]$ is monic, irreducible of degree $n \geq p$, and $\alpha, \beta \in Z/pZ[x]$ of degree less than n with $[\alpha] \in (Z/pZ[x])/(f)$, and $[\alpha]$ a generator of the multiplicative group and $\beta \not\equiv 0 \bmod f$.

For purposes of brevity, we have not included analysis of Algorithm II. Lovorn [Lo] gives detailed analysis of a similar algorithm.

Algorithm II

Stage 0 input f, p, α, β

Stage 1 Set n =degree of f, $m = \lfloor \sqrt{n} \rfloor$

Stage 2 Calculate $T = \{f_i | f_i \in Z/pZ[x],\ deg(f_i) \leq m,\ f_i$ irreducible and monic$\}$. Let $w = \#T$ and let $< f_1, f_2, \ldots, f_w >$ be an ordering of T.

Stage 3 Set $z = 1$, While $z \leq w+1$: Choose random r, s with $0 \leq r, s \leq p^n - 1$ and calculate $\gamma \in Z/pZ[x]$, of degree less than n such that $\gamma \equiv \alpha^r \beta^s \bmod f$. If $\gamma = \widetilde{\gamma} \prod_{i=1}^{w} f_i^{e_i}$ where $\widetilde{\gamma}$ is the leading coefficient of γ (i.e. if γ is m-smooth) then set $\gamma_z = \gamma$, $r_z = r$, $s_z = s$, $v_z =< e_1, e_2, \ldots, e_w >$ and $z = z + 1$.

Stage 4 Calculate $a_1, a_2, \ldots, a_{w+1} \in Z_{\geq 0}^{<p^n-1}$ such that GCD(a_1, a_2f, ..., a_{w+1}) $= 1$ and $\sum_{i=1}^{w+1} a_i v_i \equiv < 0, 0, \ldots, 0 > \bmod (p^n - 1)$.

Stage 5 Calculate $k = \sum_{i=1}^{w+1} (r_i a_i)$ and $l = \sum_{i=1}^{w+1} (s_i a_i)$. Calculate $s \in Z_{>0}^{<p}$ such that $s \equiv \alpha^k \beta^l \bmod f$.

Stage 6 Calculate $y \in Z_{\geq 0}^{<p-1}$ such that $\alpha^{y((p^n-1)/(p-1))} \equiv s \bmod f$.

Stage 7 If $(l, p^n - 1) \neq 1$ then go to Stage 3, Else calculate and output $x \equiv (y((p^n - 1)/(p - 1)) - k)/l \bmod p^n - 1$ and halt.

Acknowledgments

We would like to thank Dennis Estes and Bob Guralnick for their help. Research supported by NSF CCR-9214671.

Discussion

Little effort was made to 'optimize' the algorithm presented here. It is possible to improve the running time in several ways. Sparse matrix methods can be used to find some dependencies[Wi]. A better bound on q in Algorithm I can

be argued heuristically. Smoothness of norms can be tested using the 'elliptic curve methods' [Le]. The integer factoring done in various parts can probably be avoided if necessary or 'L[1/3]' methods can be used (e.g. [AH, LLMP]). The use of Algorithm II can perhaps be avoided altogether by adopting Algorithm I to a more general setting. Alternatively the 'L[1/3,c]' method of Coppersmith [Co] might be adapted for the case $n \geq p$.

It terms of running time there appear to be several natural open problems:

- Do there exist a $c \in Z_{>0}$ and an algorithm for discrete logarithms over $\mathrm{GF}(p^n)$ with provable expected running time in $L_x[1/2, c]$?
- Does there exist an algorithm for discrete logarithms over $\mathrm{GF}(p^n)$ with heuristic expected running time in $L_x[1/2, 1]$?
- Does there exist an algorithm for discrete logarithms over $\mathrm{GF}(p^n)$ with provable expected running time in $L_x[1/2, 1]$?
- Do there exist a $c \in Z_{>0}$ and an algorithm for discrete logarithms over $\mathrm{GF}(p^n)$ with heuristic expected running time in $L_x[1/3, c]$?

References

[Ad1] Adleman L.M., A subexponential algorithm for discrete logarithms with applications to cryptography. *Proc. 20th IEEE Found. Comp. Sci. Symp.* 1979, pp. 55-60.

[Ad2] Adleman L.M., Factoring numbers using singular integers, *Proc. 23rd Annual ACM Symposium on Theory of Computing*, 1991, pp. 64-71.

[AH] Adleman L.M. and Huang M., *Primality Testing and Abelian Varieties Over Finite Fields*, Lecture Notes In Mathematics 1512, Springer-Verlag, 1992.

[AL] Adleman L.M. and Lenstra H.W. Jr., Finding irreducible polynomials over finite fields. *Proc. 18th Annual ACM Symposium on Theory of Computing*, 1986, pp. 350-355.

[Be] Berlekamp E., Factoring polynomials over large finite fields. *Math. Comp.* 24, 1970. pp. 713-735.

[BS] Bach E. and Shallit J., Factoring with cyclotomic polynomials. *Proc. 26th IEEE Found. Comp. Sci. Symp.* 1985, pp. 443-450.

[CEP] Canfield E.R., Erdös P. and Pomerance C., On a problem of Oppenhiem concerning "Factorisatio Nemerorum". *J. Number Theory*, 17, 1983 pp. 1-28.

[Co] Coppersmith D., Fast Evaluation of Logarithms in Fields of Characteristic Two. *IEEE Trans on Information Theory*, vol IT-30, No 4, July 1984, pp. 587-594.

[COS] Coppersmith D., Odlyzko A.M. and Schroeppel R., Discrete logarithms in *GF(p)*, *Algorithmica*, v. 1, 1986, pp 1-15.

[DH] Diffie W. and Hellman M.E., New Directions in Cryptography, *IEEE Trans. Inform Theory*, vol IT-22, pp 644-654, 1976

[Ed] Edwards H.M., *Fermat's Last Theorem*, Graduate Texts in Mathematics 50, Springer-Verlag, 1977.

[El1] ElGamal T., A public key cryptosystem and a signature scheme based on discrete logarithms, *IEEE Trans. Info. Theory*, vol IT-31 pp. 469-472, 1985

[El2] ElGamal T., A subexponential-time algorithm for computing discrete logarithms over $\mathrm{GF}(p^2)$,*IEEE Trans. Info. Theory*, vol IT-31 pp. 473-481, 1985

[Ga] Gauss K.F., *Disquisitiones Arithmeticae*, translation A.C. Clarke, S.J., Yale University Press, 1966.

[Gol] Gordon D.M., Discrete logarithms in GF(p) using the number field sieve, manuscript, April 4, 1990.

[HR] Hellman M. E., Reyneri J. M. Fast computation of discrete logarithms in GF(q). *Advances in Cryptography: Proceedings of CRYPTO '82*, pp. 3-13

[Le] Lenstra H.W. Jr., Finding isomorphisms between finite fields. *Math Comp* 56, 1991, pp. 329-347.

[Le2] Lenstra H.W. Jr., Factoring integers with elliptic curves. *Ann. of Math.* 126, 1987, pp. 649-673.

[LLMP] Lenstra A.K., Lenstra H.W., Jr., Manasse M.S. and Pollard J.M. The number field sieve. *Proc. 22nd STOC*, 1990, pp. 564-572.

[Lo] Lovorn R., Rigorous, subexponenial algorithms for discrete logarithms over finite fields, PhD Thesis, University of Georgia, May 1992

[Ne] Newman M., Bounds for class numbers, *Proc. Sympos. Pure Math.* American Mathematics Society, Vol. VIII, 1965, pp 70-77.

[Od] Odlyzko A. M., Discrete Logarithms in Finite Fields and their Cryptographic Significance, *Proceedings of Eurocrypt '84*, Lecture Notes in Computer Science, Springer-Verlag. 1985. pp. 224-314.

[Po] Pomerance C. Fast, rigorous factorization and discrete logarithms, *Discrete Algorithms and Complexity*. ED. Johnson D.S., Nishizeki T., Nozaki A. and Wilf H.S. Academic Press, 1987. pp. 119-144.

[RA] Rabin M. O., Probabilistic Algorithms in Finite Fields. *SIAM Journal of Computing*, Vol 9, No 2, May 1980, pp. 273-280

[SS] Solovay R. and Strassen V., A fast Monte-Carlo test for primality. *Siam Journal of Computing* 6, 1977. pp. 84-85.

[Wa] Washington L.C., *Introduction to Cyclotomic Fields*, Graduate Texts in Mathematics 83, Springer-Verlag, 1982.

[Wi] Wiedermann D. Solving sparse linear equations over finite fields. *IEEE Trans. Inform. Theory*. IT-32, pp. 54-62

[WM] Western A.E. and Miller J.C.P., *Tables of Indices and Primitive Roots*, Royal Society Mathematical Tables, vol. 9., Cambridge University Press, 1968.