ON COMPUTING LOGARITHMS OVER FINITE FIELDS

TaherElGamal

Hewlett-Packard Labs
3172 Porter Dr., bldg 29U
Palo Alto CA 94304

ABSTRACT

The problem of computing logarithms over finite fields has proved to be of interest in different fields [4]. Subexponential time algorithms for computing logarithms over the special cases $GF(p)$, $GF(p^2)$ and $GF(p^m)$ for a fixed p and $m \to \infty$ have been obtained. In this paper, we present some results for obtaining a subexponential time algorithms for the remaining cases $GF(p^m)$ for $p \to \infty$ and fixed $m \neq 1, 2$. The algorithm depends on mapping the field $GF(p^m)$ into a suitable cyclotomic extension of the integers (or rationals). Once an isomorphism between $GF(p^m)$ and a subset of the cyclotomic field $\mathbb{Q}(\omega_q)$ is obtained, the algorithms becomes similar to the previous algorithms for $m = 1, 2$.

A rigorous proof for subexponential time is not yet available, but using some heuristic arguments we can show how it could be proved. If a proof would be obtained, it would use results on the distribution of certain classes of integers and results on the distribution of some ideal classes in cyclotomic fields.

H.C. Williams (Ed.): Advances in Cryptology - CRYPTO '85, LNCS 218, pp. 396-402, 1986.

1. INTRODUCTION

This paper gives some ideas for extending the Merkle - Adleman algorithm for computing discrete logarithms over $GF(p)$ [1,7,9] to higher order fields. Section 2 finds appropriate integral domains for extending the algorithm. The reader is refered to [8,11] for discussion on number fields and using integral domains to extend the algorithm. Section 3 gives some ideas regarding the running time of the algorithm.

2. FINDING THE ISOMORPHISM:

From the discussion in [8], it seems natural to use higher number fields to extend the algorithm to higher order finite fields. Unfortunately, higher algebraic number fields do not have all the properties of quadratic fields that were used in proving a subexponential running time in [8]. For example, the norm function is not as easy to find, and hence the proofs for the fraction of smooth elements are more difficult. So the discussion in this paper is restricted to using a certain class of algebraic number fields; namely, the cyclotomic fields. For a discussion of the properties of cyclotomic fields, the reader is refered to [11]. Cyclotomic fields are used because they possess some of the properties of quadratic fields that were needed in developing the algorithm for the case $GF(p^2)$. For example, the splitting of primes in cyclotomic extensions is easy to determine, which is not the case for general fields.

For simplicity, only "prime" cyclotomic fields will be used, i.e. the fields $\mathbf{Q}(\omega_q)$ where ω_q is a primitive qth root of unity, and q is a prime in $\mathbf{Z}$. The qth cyclotomic polynomial has the form

$$\Phi_q(D) = D^{q-1} + D^{q-2} + \cdots + D + 1.$$

Note that the general cyclotomic polynomial does not necessarily have this nice form. Hence, the qth cyclotomic field has degree $q-1 = \varphi(q)$. Some results on cyclotomic fields are needed to find the appropriate cyclotomic fields. The reader is refered to [11] for proofs.

Recall, from [11], the results on the splitting of primes in cyclotomic extensions (known as Kummer's theorm). For each prime $p \in \mathbf{Z}$

$$(p) = \prod_{i=1}^{g} (p, h_i(\omega_q)),$$

where

$$\Phi_p(D) = \prod_{i=1}^{g} h_i(D) \mod q.$$

The polynomials $h_i(D)$ all have degree f, where $fg = q - 1$, and f is equal to the order of $p \mod q$ (or the order of p in the multiplicative group in $GF(q)$, which is usually denoted by $(\mathbb{Z}/q)^*$). Hence the splitting of the ideal (p) in $\mathbb{Z}(\omega_q)$ depends on the factorization of the pth cyclotomic polynomial $\mod q$ which is easy to find (see [11]).

If $\mathbf{R}_i = (p, h_i(\omega_q))$, then $N(\mathbf{R}_i) = p^f$, where $N(\mathbf{R}_i)$ is the norm of the ideal $\mathbf{R}_i$.

The next lemma relates cyclotomic polynomials to the orders of elements in $(\mathbb{Z}/q)^*$.

Lemma 1

Let q be a prime $\leq n$, and let $a \in \mathbb{Z}$. Then $q \mid \Phi_n(a)$ if and only if the order of a in $(\mathbb{Z}/q)^*$ is n.

Proof

First, if the order of $a \mod q$ is equal to n, then $a^n - 1 = 0 \mod q$ and n is the smallest such exponent. Hence, q divides one of the factors of the polynomial $D^n - 1$ evaluated at $D = a$. It is known that $D^n - 1 = \prod_{d \mid n} \Phi_d(D)$ (see [11]). Hence, q divides $\Phi_n(a)$ since, if it divides another factor of $a^n - 1$, then its order is less than n. Conversely, if q divides $\Phi_n(a)$ then $a^n - 1 = 0 \mod q$ since q divides one of the factors of the polynomial $D^n - 1$ evaluated at $D = a$, and n is the smallest such exponent (otherwise q would divide $\Phi_d(a)$ for some $d < n$ in which case the polynomial $D^n - 1$ has multiple roots which is never the case [11]). This proves Lemma 1.

This lemma provides an easy check for the order of $p \mod q$. That is, if the order of $p \mod q$ is equal to f, then q has to divide $\Phi_f(p)$.

Going back to the isomorphism, a cyclotomic field $\mathbf{Q}(\omega_q)$ is used to generate a finite field $GF(p^m)$, for p and m known (and m small). A field that is isomorphic to $GF(p^m)$ needs to be found from the ring of integers in a cyclotomic field similar to the isomorphisms that were found for the cases $m = 1, 2$.

One observation is that if the "residue classes" $\mathbf{Z}(\omega_q)/\mathbf{R}_i$ for some prime ideal $\mathbf{R}_i$ of norm p^m are constructed, then these residue classes form a finite field isomorphic to $GF(p^m)$. Let

$$\mathbf{R}_i = (p, h_i(\omega_q)),$$

and

$$\Phi_q(D) = \prod_{i=1}^{g} h_i(D) \bmod p,$$

where each $h_i(D)$ is irreducible $mod\ p$. Then $h_i(D)$ is a candidate for generating $GF(p^m)$.

Finding the appropriate field $\mathbf{Q}(\omega_q)$

The discrete logarithm problem is the following; given α, y and p^m, find x such that

$$\alpha^x = y \ \ in\ GF(p^m)$$

for some given irreducible polynomial $K(D)$ with degree m. First, as noted in [2,3,10], the choice of the irreducible $K(D)$ does not affect the running time of the algorithm since all representations of $GF(p^m)$ are isomorphic and only polynomial time is needed to find the corresponding logarithms in one representation if the logarithms are known in another representation.

From the above discussion, a prime ideal $\mathbf{R}$ that has norm equal to p^m needs to be obtained. That is equivalent to finding a prime q such that p has order $m \ \ mod\ q$.

Equivalently, to construct an appropriate field $\mathbf{Q}(\omega_q)$, a prime factor q of $\Phi_m(p)$ should be computed (see Lemma 1). This proves the existence of such q, which might be quite large (for example $O(p)$ or higher). In this case the obtained field cannot be used for our algorithm since just representing an integer takes $O(p)$ operations.

Fortunately, as p grows larger the probability that $\Phi_m(p)$ has at least one small factor is high if the number $\Phi_m(p)$ is assumed to be random, but for some given p and m no small divisor q may exist. The reason is that $p^m - 1$ should be chosen to have at least one large prime

factor, and hence $\Phi_m(p)$ (which is a factor of $P^m - 1$) is likely to be a prime, or not to have any large prime factor.

For the cases where $\Phi_m(p)$ does not have any small factors, $GF(p^m)$ could be embedded in $GF(p^{im})$ for some small $i \in \mathbf{Z}$. $\log y$ can be found as if y and α were elements in $GF(p^{im})$ and the results are transferred back to $GF(p^m)$ which is isomorphic to the subfield of order p^m in $GF(p^{im})$.

So in this case, a small divisor of $\Phi_{im}(p)$ for some $i \in \mathbf{Z}$ is needed. That increases the chance of finding an appropriate q, since the probability that one of the numbers $\Phi_{im}(p)$, $i = 1, 2, \cdots, l$ for some l, has at least one small prime factor grows with l.

Note that $\Phi_m(p)$ need not be factored completely because only a small divisor ($O(\log p)$ for example) is needed. Even if $\Phi(p)$ is factored completely, the asymptotic running time of algorithm will not increase since $\Phi_m(p) = O(p^{\varphi(m)})$ and factoring such a number also takes subexponential time in $\varphi(m) \log p$.

3. THE RUNNING TIME

This section sketches some ideas about the running time of the algorithm as desribed above.

A. The image of $GF(p^m)$ is $\mathbf{Z}(\omega_q)/\mathbf{A}$, which consists of the elements

$$\left\{ \sum_{j=0}^{m-1} a_j \omega^j , a^j \in \mathbf{Z} \text{ for all } j \right\},$$

and the norm of the ideal $\mathbf{A}$ is p^m.

B. All the elements in $\mathbf{Z}(\omega_q)/\mathbf{A}$ have norm less than

$$M = m^2 (p-1)^m .$$

This is a loose bound, since it is obtained by adding m^2 terms. (When computing the norm of any element in $\mathbf{Z}(\omega_q)$, m^2 are obtained, each has the value $(p-1)^m$ which is the maximum value of each term, since each a_i is less than p.)

C. The number of ideals in $\mathbf{Z}(\omega_q)$ with norm up to M is linear in M ($= kM$) for some constant k (see [8]).

The number of prime ideals in $\mathbf{Z}(\omega_q)$ with norm up to M is therefore equal to $O\left[\frac{M}{\log M}\right]$.

D. The number of principal prime ideals up to norm M is equal to the total number of prime ideals with norm up to $M^{1/h}$, where h is the class number of $\mathbf{Z}(\omega_q)$, because any ideal $\mathbf{A} \in \mathbf{Z}(\omega_q)$ raised to the hth power is principal.

E. The number of smooth principal ideals in $\mathbf{Z}(\omega_q)$ with norm up to M (smooth is defined with respect to some value for the maximum norm of small prime principal ideals $\mathbf{N}$) can be computed in a way similar to the computation in [6] for the case of $GF(p^2)$.

F. Assume that the smooth elements are uniformly distributed among the different subsets of elements with small norm. Then, the ratio of smooth elements in $\mathbf{Z}(\omega_q)/\mathbf{R}$ is of the same form as for the cases $GF(p)$ and $GF(p^2)$, and a subexponential running time could be obtained.

REFERENCES

[1] L. Adleman, "A Subexponential Algorithm for the Discrete Logarithm Problem with Applications to Cryptograpo be published.

[2] I. Blake, R. Fuji-Hara, R. Mullin, and S. Vanstone, "Computing Logarithms in Finite Fields of Characteristic Two", *to be published.*

[3] D. Coppersmith, "Fast Evaluation of Logarithms in Fields of Characteristic Two", *to appear in IEEE Transactions on Information Theory*, July 1984.

[4] W. Diffie and M. Hellman, "New Directions in Cryptography", *IEEE Transactions on Information Theory*, vol. IT-22 pp.644-654 Nov. 1976.

[5] W. Diffie and M. Hellman, "Privacy and Authentication: An Introduction to Cryptography", *Proceedings of the IEEE*, vol 67, No 3, March 1979.

[6] T. ElGamal, "A Subexponential-Time Algorithm for Computing Discrete Logarithms over $GF(p^2)$", *submitted to IEEE Transactions on Information Theory.*

[7] M. Hellman and J. Reyneri, "Fast Computation of Discrete Logarithms in $GF(p^m)$, "

Presented at Crypto 82 Conference Santa Barbara, CA August 1982.

[8] D. Marcus, *Number Fields*, Springer-Verlag.

[9] R. Merkle, *Secrecy, Authentication, and Public Key Systems*, Ph.D. Dissertation, Electrical Engineering Department, Stanford University June 1979.

[10] A. Odlyzko, "Discrete Logarithms in Finite Fields and Their Cryptographic Significance", *to be published. Journal of Number Theory* vol. 15 no. 2, October 1982.

[11] L. C. Washington, *Introduction to Cyclotomic Fields*, Graduate texts in mathematics 83, Springer - Verlag 1982.