A Subexponential-Time Algorithm for Computing Discrete Logarithms over GF(p^2)

TAHER ELGAMAL, MEMBER, IEEE

Abstract—**An algorithm for computing discrete logarithms over GF(p^2), where p is a prime, in subexponential time is described. The algorithm is similar to the Merkle–Adleman algorithm for computing logarithms over GF(p), but it uses quadratic fields as the appropriate algebraic structure. It also makes use of the idea of a virtual spanning set due to Hellman and Reyneri for computing discrete logarithms over GF(p^m), for m growing and p fixed.**

I. Introduction

THE DISCRETE LOGARITHM problem, namely finding x given α, y, and q such that $\alpha^x = y$ over GF(q), is of great interest in public key cryptography [8], because it appears to be a one-way function. The reason is that exponentiation mod p takes polynomial time in the number of bits in p (or $\log_2 p$). However, the best known algorithm for the case $q = p$, a prime, runs in subexponential time and was developed independently by Western and Miller [16], [23], Merkle [15], [21], and Adleman [1]. Adleman proved that the algorithm runs in subexponential time. A subexponential extension of this algorithm was developed by Hellman and Reyneri [11], and modified by Blake *et al.* [5], Coppersmith [7], and Odlyzko [20] for the case $q = p^m$ for p fixed and m growing. However, no subexponential algorithm is known for any case where $q = p^m$ for a fixed $m > 1$ and $p \to \infty$. In this paper we present a subexponential algorithm for the first such case, namely $q = p^2$. The proof for the running time depends on a hypothesis about the distribution of prime ideals in quadratic fields. This algorithm provides more evidence that a subexponential algorithm exists for any GF(q).

In the Appendix, we present an overview of quadratic fields. They will be used throughout the algorithm instead of the field of quotients that was used in the case GF(p). In Section II we describe the algorithm giving the necessary conditions that have to be satisfied by a quadratic field to be suitable for the algorithm. In Section III, we prove a subexponential running time for the algorithm. In Section IV, we give some conclusions and remarks.

Manuscript received December 16, 1983; revised December 19, 1984. This work was supported by the National Security Agency under the contract MDA904-81-C-0414 and by the Joint Services Electronics Program under contract DAAG29-81-0057. The material in this paper was partially presented at Crypto '83, Santa Barbara, CA, August 1983.

The author was with the Information Systems Laboratory, Stanford University, Stanford, CA. He is now with Hewlett-Packard Laboratories, 1501 Page Mill Road, Palo Alto, CA 94304, USA.

Notation: For $n \in \mathbf{Z}^+$, let $\mathbf{Z}_n = \mathbf{Z}/n\mathbf{Z}$ = the integers modulo n = the set $\{0, 1, \cdots, n-1\}$. If $x = a \bmod n$, then a denotes the remainder after dividing x by n.

II. Description of the Algorithm

An element of GF(p^2) is represented as a polynomial of degree ≤ 1 with coefficients from GF(p), with multiplication of elements taken modulo a second degree irreducible polynomial [4].

For example, over GF(17), the polynomial $k(D) = D^2 + D + 6$ is irreducible. Let $y_1 = 4D + 5$ and $y_2 = 3D + 10$. Then

$$y_1 y_2 = 12D^2 + 55D + 50.$$

Reducing modulo $k(D)$,

$$\begin{aligned} y_1 y_2 &= 12(-D - 6) + 55D + 50 \\ &= 43D - 22. \end{aligned}$$

Then taking each coefficient mod 17,

$$y_1 y_2 = 9D + 12, \qquad \text{over GF}(17^2).$$

The Merkle–Adleman algorithm for computing logarithms over GF(p) relies on finding small primes and elements that factor completely into small primes (i.e., smooth elements [1]). By considering quadratic fields, we define similar notions. We do so by finding a mapping (see Theorem 1 below)

$$f: \text{GF}(p^2) \to \boldsymbol{I}(\sqrt{m})/(p), \qquad \text{for a suitable } m. \quad (1)$$

Remark: For computing logarithms in GF(p), f is the identity mapping, since GF(p) is isomorphic to the set $\mathbf{Z}_p$. In the case of GF(p^2), we shall establish a similar isomorphism between GF(p^2) and $\boldsymbol{I}(\sqrt{m})/(p)$, where $\boldsymbol{I}(\sqrt{m})/(p)$ denotes the residue classes modulo the ideal (p) in $\boldsymbol{I}(\sqrt{m})$.

The next theorem establishes the isomorphism required in the algorithm.

Theorem 1: Let m be a quadratic nonresidue mod p. Then $\boldsymbol{I}(\sqrt{m})/(p)$ is isomorphic to GF(p^2).

Proof: This result is a generalization of the known result that $\mathbf{Z}/p$ is isomorphic to GF(p). Consider the set of residue classes $\boldsymbol{I}(\sqrt{m})/(p)$, where (p) is a principal prime ideal in $\boldsymbol{I}(\sqrt{m})$. We can generalize the Euler φ function to the quadratic case (and to higher fields also).

0018-9448/85/0700-0473$01.00

Let $\phi(A)$ be the number of residue classes mod A that are relatively prime to A, where A is a prime ideal in $I(\sqrt{m})$. Then it can be shown that $\phi(A) = N(A) - 1$, where $N(A)$ is the norm of the ideal A. In our case $A = (p)$ and hence its norm is equal to $N(p) = p^2$.

The proof is divided into two parts. First, we shall show that $I(\sqrt{m})/(p)$ contains p^2 elements. The second part shows that $I(\sqrt{m})/(p)$ is a field. We shall denote each residue class mod (p) by a representative $a + b\sqrt{m}$ for some $0 \le a, b \le p - 1$, and $a, b \in Z$. First, any two elements

$$\{\alpha_i = a_i + b_i\sqrt{m},\ i = 1, 2\}$$

in the set

$$M = \{a + b\sqrt{m} \mid 0 \le a, b \le p - 1,\ a, b \in Z\}$$

are distinct since $\alpha_j - \alpha_k$ for any j, and k cannot be divisible by p. Second, any other residue class $c + d\sqrt{m}$ is congruent to an element in M. Hence the set $I(\sqrt{m})/(p)$ contains p^2 elements ($= p^2 - 1$ residue classes relatively prime to (p) and the zero residue class which corresponds to elements in (p)).

Now we show that $I(\sqrt{m})/(p)$ is a field, defining addition and multiplication mod p for each coefficient. That is equivalent to taking elements modulo (p) since we subtract multiples of p from $a + b\sqrt{m}$. The proof is immediate since if $\alpha, \beta \in I(\sqrt{m})/(p)$, then $\alpha \pm \beta$, and $\alpha\beta \in I(\sqrt{m})/(p)$. Also, we can define the inverse of $\alpha = a + b\sqrt{m}$ to be $\alpha^{-1} = N(\alpha)^{-1}a - N(\alpha)^{-1}b\sqrt{m}$, where $N(\alpha) =$ the norm of α, and its inverse is taken mod p.

Hence the set $I(\sqrt{m})/(p)$ is a field containing p^2 elements if (p) is a prime ideal in $I(\sqrt{m})$. We note that (p) is a prime ideal in $I(\sqrt{m})$ if and only if the discriminant d (or equivalently m) is a quadratic nonresidue mod p. Hence this field is another copy of GF(p^2) in the representation defined by the irreducible polynomial $D^2 - m$. The last polynomial is irreducible because m is a quadratic nonresidue (mod p). Hence $I(\sqrt{m})/(p)$ is isomorphic to GF(p^2) since all representations of GF(p^2) are isomorphic. This concludes the proof of Theorem 1.

Algorithm: The basic steps of the algorithm are analogous to those of the Merkle–Adleman algorithm for computing logarithms over GF(p). The algorithm splits into precomputation and postcomputation.

Definition 1: Let P be a set of quadratic primes in $I(\sqrt{m})$. We shall denote by the absolute norm of an element in $I(\sqrt{m})$ the absolute value of its norm. P contains the fundamental unit in $I(\sqrt{m})$ as well as one quadratic prime with prime norm form each associate class in $I(\sqrt{m})$ with absolute norm up to N. The quadratic primes with prime norm correspond to the principal prime ideals (π) in $I(\sqrt{m})$, where $\pi \notin Z$. We will prove in Theorem 2 that $N = \exp(\sqrt{(4/3)\log p \log\log p})$ minimizes the running time of the precomputation.

Let $P(N)$ be the cardinality of P. Associates of quadratic primes are not included in P since the fundamental unit of $I(\sqrt{m})$ is included in P.

A. The Precomputation

Given $\alpha, y \in$ GF(p^2) and given p, the precomputation proceeds as follows.

1) Find a suitable quadratic field $Q(\sqrt{m})$ such that its discriminant d (or equivalently m) is a quadratic nonresidue mod p. This is done by adding multiples of p to the coefficients of $k(D)$ such that the discriminant of the new polynomial equals the required value. Refer to the example at the end of this section for details.

2) Fix a set P of quadratic primes in $I(\sqrt{m})$ with small prime norm absolute value. For an algorithm to find P, see Lemma 4.

We only use the quadratic primes with prime norms because any smooth element (i.e., one which factors over P) is representable as a unique product of these primes.

3) Let $b_2 = 8 \times P(N)/\epsilon$ be a prescribed number of trials, where ϵ is the probability that any z in the image of GF(p^2) is smooth. Let $b_1 = 4P(N)$ be the number of smooth elements to be obtained in this step. Do this step at most b_2 times.

Choose random exponents u_i uniformly between 0 and $p^2 - 2$. Find the corresponding $y_i = \alpha^{u_i}$ in GF(p^2). Then find $z_i = f(y_i)$ according to Theorem 1. Try factoring z_i over P. If z_i is smooth, then find its vector of exponents V_i. That is, if

$$P = \{\pi_1, \pi_2, \cdots, \pi_{P(N)}\}, \tag{2}$$

then

$$z_i = \prod_{j=1}^{P(N)} \pi_j^{v_{ij}}, \tag{3}$$

and

$$V_i = \{v_{i1}, v_{i2}, \cdots, v_{i,\,P(N)}\}. \tag{4}$$

If the number of smooth elements obtained in step 3) after b_2 trials is less than b_1, then the algorithm halts and is said to fail.

4) Find a set of independent vectors $\{V_j, 1 \le j \le I\}$ that span the space spanned by $\{V_i, 1 \le i \le b_1\}$. If the resulting set is not a virtual spanning set, then the algorithm halts and is said to fail. A set $\{V_j\}$ is said to be a virtual spanning set if any new V_i has at least a 50 percent chance of being dependent on $\{V_i\}$ (see [11]). Lemma 6 bounds the probability that the algorithm fails.

Once the precomputation is done, we have with high probability a virtual spanning set $\{V_i, 1 \le i \le I\}$.

B. The Postcomputation

Given α and y in GF(p^2), and given a virtual spanning set $\{V_i, 1 \le i \le I\}$, logarithms are calculated as follows.

1) Find the image of y; i.e., the number that corresponds to y in $I(\sqrt{m})/(p)$ under the isomorphism f: GF(p^2) $\rightarrow$ $I(\sqrt{m})/(p)$. Let this operation be denoted by $z = f(y)$.

2) Check if z is smooth; if so, then go to step 4).

3) Choose an exponent s at random uniformly between 0 and $p^2 - 2$. Find $y' = y\alpha^s$ in GF(p^2). Find $z = f(y')$ and go to step 2).

4) Find the vector V_z of exponents of z.

5) Check if V_z is in the span of $\{V_i\}$; if not, then go to step 3).

6) If V_z is in the span of $\{V_i\}$, then compute the logarithm of y as

$$\log_\alpha y = -s + \sum_{i=1}^{I} a_i u_i \bmod (p^2 - 1). \tag{5}$$

where

$$V_z = \sum_{i=1}^{I} a_i V_i.$$

Example: If GF(17^2), find x such that $(2D + 3)^x = 4D + 2 \bmod (D^2 + D + 6)$.

The idea behind this method is that if we add multiples of p to the coefficients of $k(D)$, then we change the discriminant of the irreducible polynomial but keep the representation of GF(p^2) unchanged.

Finding the mapping f,

$$D = \frac{-1 \pm \sqrt{-23}}{2}.$$

It will be shown in Lemma 1 that smaller values of $|m|$ give, in general, smaller running time for the algorithm. So subtract 17 from the coefficient of D and add an arbitrary number of 17's to the coefficient of D^0. So first looking at $D^2 - 16D + 6 = 0$, we see that

$$D = 8 \pm \sqrt{64 - 6}$$
$$= 8 \pm \sqrt{58}.$$

Next try to modify 58 to -3 (since 3 is the smallest quadratic nonresidue mod 17) by adding some multiple of 17 to 58. For example,

$$58 + np = (A^2)(-3).$$

Hence,

$$A^2 = (-3)^{-1}(58) \pmod{17}$$
$$= (-6)(7) = -42 = 9 \pmod{17},$$
$$A = 3 \text{ or } 14 \pmod{17}. \tag{6}$$

Therefore $D = 8 \pm 3\sqrt{-3}$ satisfies

$$D^2 + (1 - 17)D + (6 + 17n) = 0, \qquad \text{with } n = 5.$$

Hence our mapping f is determined by

$$f(D) = 8 + 3\sqrt{-3}.$$

Next, we fix a set $\boldsymbol{P}$ of small primes, for example,

$$\boldsymbol{P} = \left\{ p_1 = \frac{1 + \sqrt{-3}}{2}, p_2 = 2, p_s = \sqrt{-3} \right\}.$$

Note that p_1 is a fundamental unit in $\boldsymbol{I}(\sqrt{-3})$ and has to be included in $\boldsymbol{P}$. Note also that $\boldsymbol{I}(\sqrt{-3})$ is a unique factorization domain; hence all quadratic primes that are not primes in $\boldsymbol{Z}$ have prime norm. Next we choose

$$u_1 = 111 \qquad y_1 = 6D + 6$$
$$u_2 = 42 \qquad y_2 = D + 12.$$

Then

$$f(y_1) = z_1 = 3 + \sqrt{-3},$$
$$f(y_2) = z_2 = 3 + 3\sqrt{-3}.$$

For the required $y = 4D + 2$,

$$f(y) = z = 12\sqrt{-3}.$$

Factoring z_1, z_2, and z,

$$z_1 = p_1^5 p_2 p_3, \qquad \text{hence } V_{z_1} = (5\,1\,1),$$
$$z_2 = p_1^4 p_2 p_3^2, \qquad \text{hence } V_{z_2} = (4\,1\,2),$$
$$z = p_1^3 p_2^2 p_3^3, \qquad \text{hence } V_z = (3\,2\,3).$$

Addition in the first component is taken mod 6, since we have six units in $\boldsymbol{I}(\sqrt{-3})$.

From the factoring of z_1, z_2, and z

$$V_z = V_{z_1} + V_{z_2},$$

which implies that

$$z = z_1 z_2, \qquad \text{in } \boldsymbol{I}(\sqrt{-3}),$$

which in turn implies that

$$y = y_1 y_2, \qquad \text{in GF}(17^2).$$

Hence

$$\log_\alpha y = \log_\alpha y_1 + \log_\alpha y_2 \bmod (17^2 - 1) = 153.$$

III. Complexity Analysis

As explained in Section II, the algorithm splits into two parts. The precomputation time dominates the postcomputation time and the precomputation can be reused for any fixed GF(p^2). In the next theorem we estimate the complexity of the algorithm.

Theorem 2: The complexity of the algorithm is

$$O\left(\exp\left((1 + \delta)\sqrt{48 \log p \log\log p}\right)\right), \qquad \text{for all } \delta > 0. \tag{7}$$

Before proving Theorem 2, we will first find the required bounds on the number of smooth elements in the image of GF(p^2) under f (i.e., in $\boldsymbol{I}(\sqrt{m})/(p)$).

In the next lemma we obtain an estimate for the number of primes with prime norm (with absolute value of norm up to N) in $\boldsymbol{I}(\sqrt{m})$.

Lemma 1: Let $P(N)$ be the cardinality of $\boldsymbol{P}$. Then

$$\frac{2N}{\log N} > P(N) > \frac{(\log 2)N}{4\sqrt{2} \log p \log\log p \log N},$$

assuming that the extended Riemann hypothesis is valid and that prime ideals are evenly distributed among ideal classes.

Proof: Let $T(N)$ be the total number of prime ideals in $\boldsymbol{I}(\sqrt{m})$ with norm up to N. Then the upper bound is easily proved since $P(N) \le T(N)$. This bound is not tight, but it is sufficient for proving Theorem 2. We note that the norms of ideals are always ≥ 0, hence we do not have to

deal with absolute values in this case. The total number of prime ideals in $I(\sqrt{m})$ with norm up to N, other than those principal ideals generated by primes in Z, is asymptotically equal to the number of primes (in Z) $\leq N$. The reason is that asymptotically half the prime ideals in Z split into two prime ideals in $I(\sqrt{m})$ (refer to [14] for details and see the Appendix).

The other half of prime ideals remain prime in $I(\sqrt{m})$ and hence correspond to principal prime ideals in $I(\sqrt{m})$. The number of these ideals is equal to $O[\sqrt{N}/\log N]$ and does not change the asymptotic number of prime ideals.

Let the number of primes less than or equal to n be denoted by $\pi(n)$. Then it can be shown that $c_1 n/\log n \leq \pi(n) \leq c_2 n/\log n$ for some real constants $(\log 2)/4 \leq c_1 \leq c_2 \leq 2$ (see [9], [19], [22]). Hence

$$T(N) \leq 2\frac{N}{\log N}. \tag{8}$$

This proves the upper bound since $P(N) \leq T(N)$.

To prove the lower bound, we need to bound the number of elements in P (except the unit). First, note that the elements of P correspond to the principal prime ideals in $I(\sqrt{m})$ that are not generated by primes in Z. Let $h(m)$ be the class number of $I(\sqrt{m})$. Then the prime ideals $T(N)$ split into $h(m)$ classes. It can be proved that, asymptotically, each class contains the same number of prime ideals (see [18] for proof), i.e., we have

$$P(N) > (\log 2)/4\frac{N}{h(m)\log N}.$$

The above bound is true for fixed m and $N \to \infty$. We need a similar result that applies for any large N. For example, if the value of N is expected to be larger than any polynomial in p, then a similar result on the distribution of prime ideals up to norm N is needed. Such a result does not appear to be available in the literature. Thus we assume the hypothesis that the prime ideals in a quadratic integral domain $I(\sqrt{m})$ to be equally distributed among the ideal classes.

Once the above hypothesis is assumed, it remains to give a bound on the class number $h(m)$ in terms of p. It can be shown that $h(m) < \sqrt{|m|}\log(|m|)$ (see [18]). We will choose $|m|$ to be the quadratic nonresidue mod p with the smallest absolute value. This choice of $|m|$ is due to the fact that the known bound for $h(m)$ is an increasing function in $|m|$. A bound on this choice of $|m|$ that depends on the validity of the extended Riemann hypothesis was obtained in [2], [17], and an explicit form of the bound was obtained in [3], which is given by

$$|m| < 2\log^2 p.$$

Although the above bound for the class number suggests that $h(m)$ is increasing in $|m|$, the behavior of $h(m)$ is much more complicated. For example, $h(-163) = 1$, while $h(-5) = 2$. A better bound could be obtained if we could find the quadratic field with the smallest class number rather than the quadratic field with the smallest discriminant. However, finding such a field does not appear to be easy in general.

Hence, we obtain the following estimate for the number of elements in P:

$$P(N) > \frac{(\log 2)N}{4\sqrt{2}\log p \log\log p \log N} \tag{9}$$

The use of real quadratic fields makes the estimate for the running time better since there are many more real quadratic fields with class number 1 than imaginary quadratic fields. On the other hand, the bound that we will obtain for the number of smooth elements in real quadratic fields in Lemma 2 below is worse than that for imaginary fields. So we conclude that it is more efficient to map GF(p^2) into a quadratic field that has small class number, preferably 1, provided that the number of smooth elements is not very small.

We do not count the associates of quadratic primes since we include the fundamental unit in $I(\sqrt{m})$, which increases $P(N)$ by 1 and does not change our asymptotic bounds. For an algorithm to find the fundamental unit in a real quadratic field, refer to [6]. This proves Lemma 1.

The next two lemmas bound the number of smooth elements in the image of GF(p^2).

Lemma 2: The number of smooth elements in the image of GF(p^2) (or $I(\sqrt{m})/(p)$) is at least equal to the number of smooth elements in $I(\sqrt{m})$ with norm less than $p^2/4$, for imaginary fields. For real fields, the number of smooth elements in $I(\sqrt{m})/(p)$ is at least equal to the number of smooth elements with absolute value of the norm up to $p^2/(4\max(a^2, b^2, m))$ where the fundamental unit in $I(\sqrt{m})$ is $\eta = (a + b\sqrt{m})/2$.

Proof: Recall that the images of the elements of GF(p^2) are all the elements $a + b\sqrt{m}$, where $a, b \in \{1, 2, \cdots, p-1\}$. First, we shall discuss the case of imaginary fields. Apart from the elements with 2 in the denominator, the element $p + 0\sqrt{m}$ is the smallest element in $I(\sqrt{m})$ that is not in the image of GF(p^2); its norm is p^2. So if no smooth element has 2 in the denominator (in the case $m = 2, 3 \bmod 4$, where all the integers are of the form $a + b\sqrt{m}$ and $a, b \in Z$), then all smooth elements with norm $< p^2$ will be in the image of GF(p^2).

If some smooth element β has 2 in the denominator, then 2β is also smooth (since we always include 2 or its factors in P) if 2β has norm $< p^2$ (i.e., $N(\beta) < p^2/4$ since norm (2) = 4). Then 2β is in the image of GF(p^2).

In the case of real fields, the bound is worse than that obtained for imaginary fields. Recall that the fundamental unit in $I(\sqrt{m})$ is $\eta = (a + b\sqrt{m})/2$. Then, the number of smooth elements in $I(\sqrt{m})/(p)$ is at least equal to the number of smooth primary elements with absolute norm up to $p^2/(4\max(a^2, b^2 m))$. The derivation of this bound will not be included here since a better bound is available for imaginary quadratic fields, and each field GF(p) can be mapped into some imaginary quadratic field. (For the derivation, see [10].) We should note that the value of $\max(a^2, b^2 m)$ can be large compared to m. There is no obvious way to relate these values, and if it happens that the value of a is large, then the bound is not very good. Hence, either we should avoid such quadratic fields, or a

better bound should be obtained. (A subexponential running time will be obtained in Theorem 2 using imaginary fields only, since any GF(p^2) could be mapped into $I(\sqrt{m})/(p)$ for some $m < 0$. The use of real fields may result in a better estimate for the running time.) This proves Lemma 2.

Lemma 3: Let S be the set of smooth elements in the image of GF(p^2) under f, and N the maximum absolute norm of the elements of P. Then

$$\Pr\{\text{an element in the image is smooth}\} = \epsilon \geq \frac{\binom{P(N)+u}{u}}{p^2},$$

where

$$u = \left\lfloor \frac{\log\left(\frac{p^2}{4k}\right)}{\log N} \right\rfloor,$$

and k, a constant depending on which quadratic field is used, is given by

$$k = \begin{cases} 1, & \text{if } m < 0 \\ \max(a^2, b^2 m), & \text{if } m > 1 \end{cases}$$

Proof: Following [9], we only need to show that the number of elements in S is at least

$$\binom{P(N)+u}{u}.$$

If we multiply any u elements from P, the maximum absolute norm we can produce is

$$N^u \leq N^{\log(p^2/4k)/\log N} = N^{\log_N(p^2/4k)} = \frac{p^2}{4k}.$$

The above bound for the cardinality of S is the number of ways to choose u or less elements from $P(N)$ (with replacement since repetition is allowed). The last quantity is a lower bound on the number of smooth elements in the image of GF(p^2).

Recall that we only consider primes with prime norm in P. Hence different combinations of products of elements of P yield different elements in $I(\sqrt{m})$. This is essential to our proof, otherwise different combinations could yield the same element.

Hence the cardinality of $S \geq \binom{P(N)+u}{u}$, completing the proof of Lemma 3.

Now we estimate the complexity of the algorithm. First, we will find the complexity of steps a and b in the precomputation.

Lemma 4: The set of quadratic primes with prime absolute norm less than N in $I(\sqrt{m})$ can be found in $O(N \log N)$ steps.

Proof: Any element $\beta \in I(\sqrt{m})$ can be represented as

$$\beta = \begin{cases} a + b\sqrt{m} & m = 2, 3 \bmod 4, \quad \text{where } a, b \in Z \\ \frac{a + b\sqrt{m}}{2} & m = 1 \bmod 4, \quad \text{where } a = b \bmod 2,\ a, b \in Z \end{cases} \tag{10}$$

The algorithm to find the small quadratic primes in $I(\sqrt{m})$ (up to norm = N) in analogous to the "Sieve of Eratosthenes" [19] for finding all small primes in Z. First, we need to list all elements in $I(\sqrt{m})$ with $|\text{norm}| \leq N$. Considering the case of imaginary fields first, this can be easily done because for negative values of m, elements with small norm are exactly the elements with small $|a|, |b|$ in (10).

For $m = 2, 3 \bmod 4$, we list all the elements $a + b\sqrt{m}$ for $a = 0$, and b ranging from 0 up to $b_{\max}$ where $N(b_{\max}\sqrt{m}) \leq N$, and repeat for different values of a until we get all the elements with norm $\leq N$. In the case $m = 1 \bmod 4$ we consider even values for b if a is even, and similarly for odd a.

Next we sort all these elements (with respect to their norms), which takes time = $O(N \log N)$, since the number of elements of norm $\leq N$ is $\leq KN$, where K is a constant depending on m. (The total number of elements considered is less than $(1/m)N$.) Then we go through the sorted list, canceling multiples of every element we encounter. The remaining elements are the small quadratic primes. Next, we go through the list of primes and cancel all primes that have a nonprime norm. Finally, we choose one representative from each associate class of small quadratic primes. This process takes time (see [12, sec. 1.2.7, eq. (3)]), less than $K\sum_{i=2}^{N} N/i = O(N \log N)$ since if $N(\alpha) = i$, we need to cancel at most $K(N/i)$ multiples of α from the list of small elements.

For the case of real fields, we need to count the primary integers with prime absolute norm up to N. Refer to the appendix for definition and properties of primary integers. Let the fundamental unit in $I(\sqrt{m})$ be $\eta = (a + b\sqrt{m})/2$. Then the definition of primary numbers can be translated into relations between the coefficients as follows (see [6] and the Appendix).

A number $\alpha = (x + y\sqrt{m})/2$ is primary if and only if both x and $y \geq 0$, and

$$\begin{aligned} &\frac{x}{y} > \frac{a}{b}, && \text{if } N(\alpha) > 0,\ N(\eta) > 0 \\ &\frac{x}{y} < \frac{bm}{a}, && \text{if } N(\alpha) < 0,\ N(\eta) > 0 \\ &\frac{x}{y} > \frac{bm}{a}, && \text{if } N(\alpha) > 0,\ N(\eta) < 0 \\ &\frac{x}{y} < \frac{a}{b}, && \text{if } N(\alpha) < 0,\ N(\eta) < 0. \end{aligned}$$

These relations imply that we search two regions of the $x - y$ plane bounded by two lines. Consider the case where $N(\eta) > 0$. The first region is bounded by the x axis, a line with slope b/a, and the hyperbola given by $(x^2 + my^2)/4 = N$, for positive norm elements. The second region is bounded by the y axis, the line with slope a/bm, and the hyperbola $x^2 - my^2 = -4N$ for negative norm elements. Similar regions are obtained for the case $N(\eta) < 0$. The area of these regions is still $< KN$ for some K depending on m. Hence, the complexity of finding the primes with small prime norm in real quadratic fields is $O(N \log N)$. This concludes the proof of Lemma 4.

Lemma 5: The mapping f can be found in $O(\log^3 p)$ operations in GF(p).

Proof: First, we find the smallest quadratic nonresidue mod p. This operation takes time $= O(\log^3 p)$ since checking for a quadratic nonresidue mod p is just raising m to the $((p-1)/2)$th power (which takes $O(\log p)$ operations in GF(p)), and we need $O(\log^2 p)$ such checks (see Lemma 1).

Using the method described in the example, the remaining part is to find A from $A^2 = m^{-1}m_1 \bmod p$ (see (6)), which is equivalent to finding square roots mod p.

A probabilistic algorithm for computing square roots mod p runs in time (see [13, sec. 4.6.2, Exercise 15])

$$O(\log^2 p). \tag{12}$$

If we use the method described in the proof of Theorem 1, then we need to find roots of the polynomials over finite fields, which also takes polynomial time (see [13, sec. 4.6.2]). Hence, the time needed for the first two operations is polynomial in $\log p$. This proves Lemma 5.

Now we prove the result on the running time of the algorithm.

Proof of Theorem 2: Steps 3) and 4) in the precomputation dominate the running time of the algorithm since we have shown that steps 1) and 2) take polynomial time. First, we shall find the value of N that minimizes the running time of the precomputation. The bounds obtained below are for imaginary fields. If, for a real field, the constant k (see Lemma 2) is small, then we obtain the same bound. If k is large, then the bound given below for the running time of the algorithm is not very accurate. In this case, a better bound than that obtained in Lemma 2 for the fraction of smooth elements should be obtained, or these fields should be avoided.

We will upper bound each of the two remaining operations separately. First the complexity of b_2 trials to find b_1 smooth elements is (see [11])

$$O\left(b_2\left\{P(N) + 2\log(p-1) + \log\frac{m+1}{2}\right\}\right) \tag{13}$$

operations comparable to arithmetic operations in GF(p), because division in the factoring process does not require more than the inversion of a 2×2 matrix over the rationals.

The last two terms in the above expression are due to the fact that repetition is allowed in dividing z by small quadratic primes and the maximum number of repetitions is $\log(m+1)(p-1)^2/2)$, since the maximum absolute norm of any element in the image of GF(p^2) under f is $(p-1)^2(m+1)$. The only case that is not considered here is for real fields, where we deal with a unit that has large coefficients. Since the fundamental unit η of the field is included in $\boldsymbol{P}$, we have to keep repeating dividing by η. This operation also takes polynomial time and can be neglected. Also, we can neglect $2\log(p-1) + \log(m+1)/2$ with respect to the term $P(N)$ in (13), since $P(N) \gg \log p$, and m is $O(\log^2 p)$.

Substituting for the value of b_2, the quantity in (13) is bounded by

$$O\left(\{P(N)\}^2/\epsilon\right) = O\left[(P(N))^2 p^2 \frac{u!P(N)!}{(P(N)+u)1}\right].$$

Using Stirling's formula, this is bounded by

$$O\left[(P(N))^2 p^2 \frac{u^u}{(P(N))^u}\right]. \tag{14}$$

Using the bounds on $P(N)$ from Lemma 1, and using the bounds for u, namely

$$\frac{\log\frac{p^2}{4}}{\log N} - 1 < u \le \frac{\log\frac{p^2}{4}}{\log N},$$

we obtain the following bound for the quantity in (14), neglecting constants and logarithmic factors,

$$O\left[\frac{N^3}{\log^3 p \log^3 N} p^2 \left[\frac{\log^2\frac{p^2}{4}\log\log p}{N}\right]^{\log(p^2/4)/\log N}\right]$$

$$\le O\left(\exp\left\{3\log N + 2\log p + \frac{\log p^2}{\log N} \cdot \left(2\log\log\frac{p^2}{4} + \log\log\log p - \log N\right)\right\}\right)$$

$$= O\left(\exp\left\{3\log N + \frac{4\log p}{\log N}(\log\log p + \log\log\log p)\right\}\right). \tag{15}$$

Ignoring the $\log\log\log p$ factor in the above expression, this expression is minimized at

$$\log N = \sqrt{\frac{4}{3}\log p \log\log p}\,. \tag{16}$$

Since N has to be an integer and we ignored a logarithmic factor in the estimate for the running time, we have for any $\delta > 0$ the following bounds if N is sufficiently large:

$$\frac{1}{1+2\delta}\sqrt{(4/3)\log p\log\log p} < \log N \le \sqrt{(4/3)\log p\log\log p}\,,$$

and we can bound (15) by

$$O\left(\exp\left\{3\sqrt{(4/3)\log p\log\log p} + \frac{4\log p\log\log p(1+2\delta)}{\sqrt{(4/3)\log p\log\log p}}\right\}\right)$$

$$= O\left(\exp\left\{(1+\delta)\sqrt{48\log p\log\log p}\right\}\right). \tag{17}$$

The last part of the precomputation is to check for independence of the vectors $\{V_i, 1 \le i \le b_1\}$, which takes time $= O((P(N))^3 b_1)$ and can be bounded by (see

[11], [21])

$$O(N^4) = O\left(\exp 4\sqrt{(4/3)\log p \log\log p}\right). \quad (18)$$

It can be seen that (17) dominates (18), as well as (11) and (12).

The complexity of the postcomputation is easily shown to be less than the precomputation. The complexity of finding a smooth element is $1/\epsilon$, which is much less than (13). We need only two trials on the average to get a vector of exponents in the span of the virtual spanning set $\{V_i, 1 \le i \le I\}$. Hence we conclude that (17) is an upper bound for the running time of the algorithm.

All that remains is to prove that the algorithm will fail with probability $\to 0$ as $p \to \infty$.

Lemma 6: The set $V_i, 1 \le i \le I$, produced by the precomputation fails to be a virtual spanning set with probability $\to 0$ as $p \to \infty$.

Proof: The proof is the same as in [11]. The algorithm will fail if either the number of smooth elements obtained in the precomputation is less than $4P(N)$, or if no virtual spanning set is obtained. We use the union bound to bound the total probability of failure. So we quote the bound on the probability of failure from [11]

$$\Pr\{\text{failure}\} \le \frac{3}{2P(N)}.$$

Using the bounds for $P(N)$ from Lemma 1 and bounding N from (16), we see that the probability of failure is bounded by

$$O\left(\exp -\frac{1}{2}\sqrt{\frac{4}{3}\log p \log\log p}\right).$$

IV. Conclusions and Remarks

We have described a probabilistic algorithm for computing logarithms over GF(p^2). The complexity of our algorithm is proved to be of subexponential time by assuming the extended Riemann hypothesis and assuming that prime ideals are equally distributed among ideal classes (refer to Lemma 1). Also, the algorithm will fail with probability $\to 0$ as $p \to \infty$.

The steps of the algorithm are similar to the steps of the Merkle–Adleman algorithm. The differences between the two algorithms are due to the difference in the structure between Z and $I(\sqrt{m})$.

We should note that the constant 48 in the exponent above is an upper bound. In practice, the constant is 24 for most values of p, i.e., for those values of p that remain prime in any quadratic field with the unique factorization property (or even fields with small class number that is not equal to one).

It is still an open problem whether there is a subexponential time algorithm for computing logarithms over GF(p^m), for $p^m \to \infty$ in an arbitrary manner. This result is a step forward towards obtaining a subexponential time algorithm for the general problem.

Acknowledgment

The author would like to thank Dr. A. Odlyzko for very helpful comments regarding the inclusion of nonunique factorization domains, and the simplification of Theorem 1. Also, the author would like to thank Prof. P. Sarnak regarding the inclusion of real fields. The author would also like to thank a referee for many comments regarding the organization of the paper.

Appendix
An Overview of Quadratic Fields

A. Introduction

This Appendix presents an overview of the theory of number fields (mainly quadratic fields). The notation is as follows.

Greek letters denote algebraic numbers (that are not rationals). Boldface italic capital letters denote algebraic number fields, rings of integers in the fields, and ideals in the rings of integers. Lowercase italic letters denote rationals (or integers) in Q (or Z). Uppercase italic letters denote polynomials over fields or rings. A polynomial over a field (or a ring) means that the coefficients of the polynomial are taken from the field (or the ring).

An element in Z will be referred to as an integer, while an element in the ring of integers of an extension of Q will be referred to as an algebraic integer. For example, an integer in a quadratic extension of Q will be referred to as a quadratic integer.

The results will only be stated without proofs; for proofs and more details, the reader is referred to [6], [14], [19].

B. Definitions

1) Algebraic and Transcendental Numbers: An algebraic number is a number ζ that satisfies an equation

$$A(x) = a_0\zeta^n + a_1\zeta^{n-1} \cdots + a_n = 0, \quad (19)$$

where $a_0, a_1, \cdots,$ and $a_n \in Z$, not all zero. The degree of ζ is the lowest degree of any polynomial that ζ satisfies (called the minimal polynomial).

A number which is not algebraic is called transcendental, e.g., e, π.

2) Algebraic Integers: If the minimal polynomial of ζ is monic (i.e. has its leading coefficient $a_0 = 1$) then ζ is an algebraic integer.

3) Algebraic Fields: An algebraic number field $Q(\zeta)$ is the set of all the "numbers" $R(\zeta) = P(\zeta)/Q(\zeta)$, where ζ is a given algebraic number of degree n, $P(\zeta)$ and $Q(\zeta)$ are polynomials over Q of degree at most $n-1$, and $Q(\zeta) \ne 0$.

Example: If $n = 1$, then $\zeta \in Q$.

Example: If $n = 2$, then we say that ζ is quadratic, i.e. ζ satisfies a second degree equation

$$a_0x^2 + a_1x + a_2 = 0,$$

hence $\zeta = (a + b\sqrt{m})/c$, or $\sqrt{m} = (c\zeta - a)/b$, for some a, b, $c \in Z$, and m a square free integer. We note that m will always denote a (positive or negative) square free integer, since $Q(\sqrt{m}) = Q(\sqrt{mk^2})$ for any $k \in Z$. We should note that the discriminant d of the quadratic field is not necessarily square free. The relation between m and d is mentioned later in this section (subsection C-6), "Ideals in $I(\sqrt{m})$," (23)).

C. Quadratic Fields

1) Quadratic Integer: A quadratic number is said to be a quadratic integer if its minimal polynomial is monic.

Lemma 7: The quadratic integers in $Q(\sqrt{m})$ are given by

$$\alpha = \begin{cases} a + b\sqrt{m}, & \text{for } m = 2, 3 \bmod 4 \\ a + b\dfrac{1+\sqrt{m}}{2}, & \text{for } m = 1 \bmod 4, \end{cases} \tag{20}$$

where $a, b \in Z$.

Theorem 3: The set $Q(\sqrt{m})$ is a field. The set integers in $Q(\sqrt{m})$, denoted by $I(\sqrt{m})$, form an integral domain, i.e., a ring containing Z.

2) Divisibility in $I(\sqrt{m})$: Let $\alpha, \beta \in I(\sqrt{m})$. Then α is said to divide β if and only if there exists $\gamma \in I(\sqrt{m})$ such that $\alpha\gamma = \beta$ in $I(\sqrt{m})$.

3) The Norm of an Element in $Q(\sqrt{m})$: Let $\alpha = (a + b\sqrt{m})/c \in Q(\sqrt{m})$, where $a, b, c \in Z$. Then the norm of α is defined as (denoting the conjugate of a number α by $\bar{\alpha}$)

$$N(\alpha) = \alpha\bar{\alpha} = \left(\frac{a + b\sqrt{m}}{c}\right)\left(\frac{a + b\sqrt{m}}{c}\right) = \frac{a^2 - b^2 m}{c^2}. \tag{21}$$

Lemma 8: The norm is multiplicative, i.e., if $\alpha, \beta \in Q(\sqrt{m})$, then $N(\alpha\beta) = N(\alpha)N(\beta)$.

Lemma 9: The norm of a quadratic integer α is an integer (in Z).

4) Units in $I(\sqrt{m})$: A quadratic integer α is called a unit if and only if α has an inverse in $I(\sqrt{m})$.

Lemma 10: If $\alpha \in I(\sqrt{m})$, then α is a unit if and only if $N(\alpha) = \pm 1$.

Associates of Elements: Two elements α, and β in $I(\sqrt{m})$ are said to be associates if and only if $\alpha v = \beta$ for some unit $v \in I(\sqrt{m})$.

Lemma 11: The units in a quadratic field form a multiplicative group. Moreover, there exists a special unit η (called the fundamental unit) such that for any unit $v \in I(\sqrt{m})$ we have $v = \pm\eta^n$ for some (positive or negative) $n \in Z$.

Units in Imaginary Quadratic Fields: A quadratic field $Q(\sqrt{m})$ is said to be imaginary if $m < 0$. For $m = -1$, $I(\sqrt{-1})$ has four units: $\pm 1, \pm\sqrt{-1}$. For $m = -3$, $I(\sqrt{-3})$ has six units: ± 1, $(\pm 1 \pm \sqrt{-3})/2$. For all other imaginary quadratic fields $I(\sqrt{m})$ has two units: ± 1.

Units in Real Quadratic Fields: If $m > 1$, then $Q(\sqrt{m})$ is called a real quadratic field. Any real quadratic field contains an infinite number of units. The smallest unit less than 1 is the fundamental unit.

Primary Numbers: A quadratic integer α in a real quadratic field $Q(\sqrt{m})$ is said to be a primary number if

$$1 \le |\alpha/\bar{\alpha}| < \eta^2 = |\eta/\bar{\eta}|, \alpha > 0,$$

where η is the fundamental unit in $I(\sqrt{m})$.

Theorem 4: Every real quadratic integer (except 0) has precisely one associate that is primary (see [6]).

5) Primes and Factorization in $I(\sqrt{m})$: An integer in $I(\sqrt{m})$ that is not zero or a unit is said to be a prime if it is only divisible by units and its associates.

Every element $\alpha \in I(\sqrt{m})$ not zero or a unit can be expressed as a product of prime powers, i.e.,

$$\alpha = \prod_i \pi_i^{e_i}, \tag{22}$$

where π_i is a quadratic prime for all i, and e_i is a positive integer for all i.

Unique Factorization (UF): If (22) can be written uniquely for all $\alpha \in I(\sqrt{m})$, except for the order of primes and multiplication by units, then the integral domain $I(\sqrt{m})$ is said to be a unique factorization domain (UFD). We note that the ring of integers Z is a UFD (the fundamental theorem of arithmetic [19]).

Unique Factorization in Quadratic Fields: In general, unique factorization does not hold in a quadratic field. In this section we shall state the known facts about quadratic fields with the UF property. For proofs, the reader is referred to [6], [14].

Quadratic Fields with Unique Factorization: There exist nine imaginary quadratic fields with the UF property, namely the quadratic fields corresponding to

$$m = -1, -2, -3, -7, -11, -19, -43, -67, -163.$$

As for real quadratic fields, there are many more with the UF property. It is an open problem whether there exists an infinite number of real quadratic fields with the unique factorization property.

By studying the factorization of "ideals" in $I(\sqrt{m})$, we can regain UF in quadratic fields.

6) Ideals in $I(\sqrt{m})$: A set A of elements in $I(\sqrt{m})$ is defined as *idea* if 1) $\alpha, \beta \in A$ implies $\alpha + \beta \in A$, and 2) $\alpha \in A, \gamma \in I(\sqrt{m})$ implies $\alpha\gamma \in A$.

Basis of an Ideal: There exists a set of elements $\{\beta_i\}$ in A, such that for any $\alpha \in A$,

$$\alpha = \sum_i \gamma_i \beta_i, \qquad \text{for some } \gamma_i \in I(\sqrt{m}).$$

We say that $\{\beta_i\}$ generates A, and (if $\{\beta_i\}$ is minimal) that $\{\beta_i\}$ is a basis for A.

Theorem 5: Any ideal in $I(\sqrt{m})$ can be generated by at most two generators.

Notation: If an ideal A is generated by α, β, then we denote A by (α, β).

Principal Ideals: If an ideal A is generated by one element α, then $A = (\alpha)$ is said to be a principal ideal (i.e., all the elements in A are multiples of α). If all the ideals in a domain are principal, then the domain is said to be a principal ideal domain.

The Norm of Principal Ideals: Let $A = (a + b\sqrt{m})$ be a principal ideal in $I(\sqrt{m})$. Then the norm of A is defined to be equal to the absolute value of the norm of its generator, i.e., if $A = (\alpha)$, then $N(A) = |N(\alpha)|$. For norms of nonprincipal ideals, refer to [6].

Theorem 6: The domain $I(\sqrt{m})$ is a principal ideal domain if and only if it is a unique factorization domain.

Multiplication of Ideals: Let A and B be ideals in $I(\sqrt{m})$. Then the product of A and B is defined as

$$C = AB = \{\alpha\beta | \alpha \in A, \beta \in B\}.$$

An ideal A is said to divide B if and only if there exists an ideal C such that $AC = B$. The previous condition is satisfied if and only if A contains B.

An ideal A is said to be a prime ideal if it is divisible only by itself and the unit ideal. The unit ideal, denoted by (1), is generated by any unit in $I(\sqrt{m})$, and is equal to $I(\sqrt{m})$ itself. We note that two associates generate the same ideal.

We shall denote by $I(\sqrt{m})/A$ the result of taking all elements of $I(\sqrt{m})$ modulo the ideal A. Two elements $\alpha, \beta \in I(\sqrt{m})$ are said to be congruent mod A if $\alpha - \beta \in A$.

Unique Factorization of Ideals into Prime Ideals: Any ideal in $I(\sqrt{m})$ can be written as a product of prime ideals in a unique

way (apart from order of prime ideals), i.e.,

$$A = \prod_i \Pi_i^{e_i},$$

where Π_i's are prime ideals in $I(\sqrt{m})$, and e_i's are positive integers.

Before studying the structure of ideals in $I(\sqrt{m})$, we note that in Z every prime ideal is generated by a prime integer. This is because Z is a unique factorization domain and hence a principal ideal domain.

Splitting of Prime Ideals in Z into Prime Ideals in $I(\sqrt{m})$: For each prime ideal Π in $I(\sqrt{m})$ there exists one and only one prime ideal P in Z such that $\Pi | P$ in $I(\sqrt{m})$. On the other hand, each prime ideal in Z either remains prime in $I(\sqrt{m})$ or splits into (not necessarily distinct) prime ideals in $I(\sqrt{m})$.

Let d be the discriminant of $Q(\sqrt{m})$. Then

$$d = \begin{cases} m, & \text{if } m = 1 \bmod 4 \\ 4m, & \text{if } m \neq 1 \bmod 4 \end{cases} \tag{23}$$

The prime ideals in Z split in $I(\sqrt{m})$ according to the following rules.

1) For the ideal (2),

$$(2) = \begin{cases} (2), & \text{if } d = m = 5 \bmod 8, \\ \left(2, \dfrac{1+\sqrt{m}}{2}\right)\left(2, \dfrac{1-\sqrt{m}}{2}\right), & \text{if } d = m = 1 \bmod 8, \\ (2, 1+\sqrt{m})^2, & \text{if } \dfrac{d}{4} = m = -1 \bmod 4, \\ (2, \sqrt{m})^2, & \text{if } \dfrac{d}{4} = m = 2 \bmod 4. \end{cases}$$

2) For $p > 2$,

$$(p) = \begin{cases} (p), & \text{if } (p, m) = 1, \\ & \text{and } m \text{ is a quadratic nonresidue mod } p, \\ (p, x+\sqrt{m})(p, x-\sqrt{m}), & \text{if } (p, m) = 1, \\ & \text{and } x^2 = m \bmod p, \\ (p, \sqrt{m})^2, & \text{if } p | m. \end{cases}$$

We should note that, although the above prime ideals in $I(\sqrt{m})$ appear to have two generators, we know that for certain quadratic fields all ideals are principal. Hence each of these prime ideals can be represented as (π) for some quadratic prime $\pi \in I(\sqrt{m})$.

Equivalence of Ideals: Two ideals A, B are said to be equivalent if there exist $\alpha, \beta \in I(\sqrt{m})$ such that $\alpha A = \beta B$, where αA is the ideal $(\alpha\alpha_1, \alpha\alpha_2)$ and $A = (\alpha_1, \alpha_2)$. If the ring $I(\sqrt{m})$ is a unique factorization domain (or equivalently principal ideal domain), then all ideals are equivalent. In the general case, where unique factorization is absent, the ideals are divided into equivalence classes.

The equivalence classes of ideals in an algebraic number field form a group. The order of the ideal class group is called the class number of the field. The class number $h(m)$ of the field $Q(\sqrt{m})$ is equal to 1 if and only if the ring $I(\sqrt{m})$ is a unique factorization domain.

References

[1] L. Adleman, "A subexponential algorithm for the discrete logarithm problem with applications to cryptography," in *Proc. 20th Ann. FOCS Conf.*, Oct. 1979.

[2] N. Ankeny, "The least quadratic non residue," *Ann. Math.*, vol. 55, pp. 65–72, 1952.

[3] E. Bach, "What to do until the witness comes: Explicit bounds for primality testing and related problems," to be published.

[4] E. Berlekamp, *Algebraic Coding Theory*. New York: McGraw-Hill, 1978.

[5] I. Blake, R. Fuji-Hara, R. Mullin, and S. Vanstone, "Computing logarithms in finite fields of characteristic two," *SIAM J. Alg. Discr. Methods*, vol. 5, pp. 276–285, 1984.

[6] H. Cohn, *Advanced Number Theory*. New York: Dover, 1980.

[7] D. Coppersmith, "Fast evaluation of logarithms in fields of characteristic two," *IEEE Trans. Inform. Theory*, vol. IT-30, pp. 587–594, July 1984.

[8] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. Inform. Theory*, vol. IT-22, pp. 644–654, Nov. 1976.

[9] J. Dixon, "Asymptotically fast factorization of integers," *Math. Comput.*, vol. 36, no. 153, Jan. 1981.

[10] T. ElGamal, "Cryptography and logarithms over finite fields," Ph.D. dissertation, Elec. Eng. Dept., Stanford Univ., Stanford, CA, 1984.

[11] M. Hellman and J. Reyneri, "Fast computation of discrete logarithms in GF(p^m)," presented at Crypto '82 Conf., Santa Barbara, CA, Aug. 1982.

[12] D. Knuth, *The Art of Computer Programming*, vol. 1. Reading, MA: Addison-Wesley, 1973.

[13] D. Knuth, *The Art of Computer Programming*, vol. 2. Reading, MA: Addison-Wesley, 1981.

[14] D. Marcus, *Number Fields*. New York: Springer-Verlag, 1975.

[15] R. Merkle, "Secrecy, authentication, and public key systems," Ph.D. dissertation, Elect. Eng. Dept., Stanford Univ., Stanford, CA, June 1979.

[16] J. Miller, "On factorization with a suggested new approach," *Math. Comput.*, vol. 29, pp. 155–172, 1975.

[17] H. Montgomery, *Topics in Multiplicative Number Theory*, Lecture Notes in Mathematics, no. 227. New York: Springer-Verlag 1971.

[18] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*. Warsaw: Polish Scientific, 1974.

[19] I. Niven and H. Zuckerman, *The Theory of Numbers*. New York: Wiley, 1980.

[20] A. Odlyzko, "Discrete logarithms in finite fields and their cryptographic significance," *Proc. Eurocrypt '84*, to appear.

[21] S. Pohlig, "Algebraic and combinatoric aspects of cryptography," Ph.D. dissertation, Elec. Eng. Dept., Stanford Univ., Stanford, CA, June 1977.

[22] H. Walum, "Discrepancies in the distribution of prime numbers," *J. Number Theory*, vol. 15, no. 2, Oct. 1982.

[23] A. Western and J. Miller, *Tables of Indices and Primitive Roots*, Royal Society Mathematical Tables, vol. 9. London: Cambridge Univ., 1968.