A Note on Cyclic Groups, Finite Fields, and the Discrete Logarithm Problem

Alfred J. Menezes & Scott A. Vanstone
Dept. of Combinatorics and Optimization, University of Waterloo
Waterloo, Ontario, N2L 3G1, Canada

Abstract

We show how the discrete logarithm problem in some finite cyclic groups can easily be reduced to the discrete logarithm problem in a finite field. The cyclic groups that we consider are the set of points on a singular elliptic curve over a finite field, the set of points on a genus 0 curve over a finite field given by the Pell equation, and certain subgroups of the general linear group.

Keywords: discrete logarithms, genus 0 curves, general linear group, elliptic curves.

1 Introduction

The Diffie-Hellman key exchange method [5] is a scheme by which two individuals A and B can, by a sequence of transmissions over a public channel, decide upon a secret cryptographic key. The method is as follows. A and B first choose a (multiplicatively written) finite abelian group G and some element $\alpha \in G$. A then selects a random integer a and transmits α^a to B. B in turn selects a random integer b and transmits α^b to A. Both A and B can then determine α^{ab}, which is their secret key.

An intruder C monitoring the transmission between A and B would know G, α, α^a, and α^b. The parameters G and α should be chosen so that it is computationally infeasible for C to then determine α^{ab}. Certainly, if C could compute either a or b, then C could determine α^{ab}. The problem of determining a given α and $\beta = \alpha^a$ is called the *discrete logarithm problem* in G. The integer a, which is unique if restricted to the range $[0, \text{order}(\alpha) - 1]$, is called the discrete logarithm of β to the base α. It is an open problem to decide whether or not determining α^{ab} is equivalent to computing discrete logarithms in G.

Even though any two cyclic groups of order n are isomorphic, an efficient algorithm to compute logarithms in one does not necessarily imply an efficient algorithm for the others. This statement is obvious when one considers that any cyclic group of order n is isomorphic to the additive group of $\mathbb{Z}_n$ and computing logarithms in $\mathbb{Z}_n$ is a triviality. In fact, the discrete logarithm problem can be restated as follows: Determine a computationally efficient

algorithm for computing an isomorphism between a cyclic group of order n and the additive cyclic group $\mathbb{Z}_n$.

The best algorithms that are known for solving the discrete logarithm problem in an arbitrary group G are the exponential square root attacks (see [12]) that have a running time that is roughly proportional to the square root of the largest prime factor of n, where n is the order of α. Consequently, if G and α are chosen such that n has a large prime factor, then these attacks can be avoided.

Let F_q denote the finite field of cardinality q, and let $q = p^m$, where p is the characteristic of F_q. In [5], $G = F_q^*$, the multiplicative group of F_q, was proposed as a candidate for implementing the Diffie-Hellman key exchange system. There are probabilistic subexponential algorithms known for computing logarithms in F_q when either q is a prime [4], or p is fixed [3], or m is fixed [7]. A subexponential algorithm is an algorithm whose running time is

$$O\left(e^{(c+o(1))\ (\log\ z)^d (\log\ \log\ z)^{1-d}} \right),$$

where $\log\ z$ is the size of the input, c is a constant, and $0 < d < 1$. These algorithms are an asymptotic improvement on the general algorithms mentioned in the previous paragraph. For cryptographic purposes we are interested in groups for which subexponential algorithms for the corresponding discrete logarithm are not known. Additionally, for efficient and practical implementation, the group operation should be relatively easy to apply. It was for these reasons that the group of non-singular matrices over a finite field [16], the group of points on an elliptic curve ([10] and [14]), the jacobian of a hyperelliptic curve defined over a finite field [11], and the class group of an imaginary quadratic field [2] have been suggested.

In [13], the logarithm problem in an elliptic curve E over F_q, denoted $E(F_q)$, was reduced to the logarithm problem in the field F_{q^k} in the case that $\gcd(\#E(F_q), q) = 1$. This was achieved by establishing a group isomorphism between the cyclic subgroup of $E(F_q)$ generated by α, and a suitable subgroup of $F_{q^k}^*$. If E is a supersingular elliptic curve, then $k \leq 6$, and the reduction takes probabilistic polynomial time, thus providing a probabilistic subexponential algorithm for the logarithm problem in supersingular curves.

In Section 2, we state some results from the literature on the group structure of singular elliptic curves. In Section 3, we show how the logarithm problem in the group of points $C \subset F_q \times F_q$ satisfying the Pell equation $x^2 - Dy^2 = 1$ can be easily reduced to the logarithm problem in either F_q or F_{q^2}, where q is odd. Let $GL(n, q)$ denote the group of $n \times n$ non-singular matrices whose entries lie in F_q. In Section 4, we reduce the logarithm problem in certain cyclic subgroups of $GL(n, q)$ to the logarithm problem in some extension of F_q. These results demonstrate that in designing a cryptosystem, the group G must be judiciously chosen.

2 Singular Elliptic Curves

For more details on elliptic curves, the reader is referred to [9] or [19].

Let E be a singular elliptic curve defined over a field K with rational singular point $P = (x_0, y_0)$. We note here that E is a curve of genus 0, and that in some of the literature such a curve is not called an elliptic curve. After the change of variables $x \to x' + x_0$, $y \to y' + y_0$, we can assume that the Weierstrass equation for E is

$$E \ : \ y^2 + a_1xy - a_2x^2 - x^3 = 0, \quad a_1, a_2 \in K, \tag{1}$$

with singular point $P = (0, 0)$.

Let $y^2 + a_1xy - a_2x^2 = (y - \alpha x)(y - \beta x)$, where α, β are in K or in K_1 (K_1 is the quadratic extension of K). Then P is called a *node* if $\alpha \neq \beta$, and a *cusp* if $\alpha = \beta$. Let $E_{ns}(K)$ denote the set of solutions $(x, y) \in K \times K$ to (1), excluding the point P, and including the point at infinity $\mathcal{O}$. $E_{ns}(K)$ is called the non-singular part of $E(K)$. One can define an addition on $E_{ns}(K)$ given by the usual chord-and-tangent law. The next result states that $E_{ns}(K)$ is a group, and determines the structure of this group. K^* denotes the multiplicative group of non-zero elements of K, while K^+ denotes the additive group of K.

Theorem 1 ([9], 7.2) *(i) If P is a node, and α, $\beta \in K$, then the map $\phi : E_{ns}(K) \longrightarrow K^*$ defined by*

$$\phi : \mathcal{O} \mapsto 1 \qquad \phi : (x, y) \mapsto (y - \beta x)/(y - \alpha x)$$

is a group isomorphism.
(ii) If P is a node, and α, $\beta \notin K$, α, $\beta \in K_1$, then let L be the subgroup of K_1^* consisting of the elements of norm 1. The map $\psi : E_{ns}(K) \longrightarrow L$ defined by

$$\psi : \mathcal{O} \mapsto 1 \qquad \psi : (x, y) \mapsto (y - \beta x)/(y - \alpha x)$$

is a group isomorphism.
(iii) If P is a cusp, then the map $\omega : E_{ns}(K) \longrightarrow K^+$ defined by

$$\omega : \mathcal{O} \mapsto 0 \qquad \omega : (x, y) \mapsto x/(y - \alpha x)$$

is a group isomorphism. ■

Using the result above, we immediately derive the following.

Theorem 2 *Let E be a singular elliptic curve defined over the finite field F_q with singular point P.*
(i) If P is a node, then the logarithm problem in $E_{ns}(F_q)$ is reducible in polynomial time to the logarithm problem in F_q or F_{q^2}, depending on whether $\alpha \in F_q$ or $\alpha \notin F_q$, respectively.
(ii) If P is a cusp, then the logarithm problem in $E_{ns}(F_q)$ is reducible in polynomial time to the logarithm problem in F_q^+. ■

Let $q = p^m$, where p is the characteristic of F_q. Then

$$F_q^+ \cong \underbrace{F_p^+ \oplus \cdots \oplus F_p^+}_{m}.$$

Note that the logarithm problem in F_p^+ can be efficiently solved in polynomial time by the extended Euclidean algorithm. Thus if we are given a basis of F_q over F_p, then we can also compute logarithms in F_q^+ in polynomial time. We thus obtain the following.

Corollary 3 *If E is a singular elliptic curve defined over a field F_q with a cusp, then logarithms in $E_{ns}(F_q)$ can be computed in polynomial time.* ■

3 Another Class of Genus 0 Curves

The curves described in this section were pointed out to us by Jeff Shallit [18].

Let q be an odd prime or odd prime power, and let D be a non-zero element of F_q. Let C denote the set of solutions $(x, y) \in F_q \times F_q$ to the equation

$$x^2 - Dy^2 = 1. \tag{2}$$

The elements of C are the affine points of an algebraic curve of genus 0, defined by equation (2). We definition an operation $\oplus$ on the elements of C as follows. If (x_1, y_1), $(x_2, y_2) \in C$, then

$$(x_1, y_1) \oplus (x_2, y_2) = (x_1x_2 + Dy_1y_2,\ x_1y_2 + x_2y_1).$$

Lemma 4 *$(C, \oplus)$ is an abelian group.*

Proof. It can easily be verified that the addition operation is closed, associative and commutative. The identity element is $(1, 0)$, while the inverse of (x, y) is $(x, -y)$. ■

Let $\chi(a)$ denote the quadratic character of $a \in F_q$, i.e.

$$\chi(a) = \begin{cases} 0 & \text{if } a = 0 \\ 1 & \text{if } a \text{ is a quadratic residue in } F_q \\ -1 & \text{if } a \text{ is a quadratic non-residue in } F_q. \end{cases}$$

We now determine the group structure of C.

Theorem 5 *$(C, \oplus)$ is a cyclic group of order $q - \chi(D)$.*

Proof.
Case (i) ($\chi(D) = -1$): Let $f(W) = W^2 - D \in F_q[W]$. Then $f(W)$ is irreducible over F_q, and so $F_{q^2} \cong F_q[W]/(f(W))$, where $(f(W))$ denotes the ideal generated by $f(W)$. Let

H denote the unique multiplicative subgroup of F_{q^2} of order $q+1$, and let $\alpha = x + yW$ be an arbitrary element of F_{q^2}. Then $\alpha \in H$ if and only if $\alpha^{q+1} = 1$. Now,

$$\begin{aligned} \alpha^{q+1} &= (x+yW)^q\,(x+yW) \\ &= (x+yW^q)\,(x+yW). \end{aligned}$$

Since

$$W^q \;=\; W(W^2)^{(q-1)/2} \;=\; WD^{(q-1)/2} \;=-W,$$

we have

$$\begin{aligned} \alpha^{q+1} &= (x-yW)\,(x+yW) \\ &= x^2 - y^2W^2 \\ &= x^2 - Dy^2. \end{aligned}$$

Consequently, $\alpha \in H$ if and only if $(x,y) \in C$. Thus the map $\phi \;:\; C \longrightarrow H$ defined by

$$\phi \;:\; (x,y) \;\mapsto\; x+yW$$

is a bijective map. It is also easy to verify that ϕ is a group homomorphism. Hence C is a cyclic group of order $q+1$.

Case (ii) ($\chi(D) = 1$): Let $a \in F_q$ be a square root of D. We can rewrite equation (2) as $(x-ay)(x+ay) = 1$. Let

$$u = x - ay \qquad \text{and} \qquad v = x + ay.$$

We then have

$$x = \frac{u+v}{2} \qquad \text{and} \qquad y = \frac{v-u}{2a}.$$

This gives a $1-1$ correspondence between solutions (x,y) of (2), and solutions (u,v) of $uv = 1$. The equation $uv = 1$ has exactly $q-1$ solutions (u,v) in $F_q \times F_q$, namely a unique solution for each $u \in F_q^*$. Thus the map $\psi \;:\; C \longrightarrow F_q^*$ defined by

$$\psi \;:\; (x,y) \;\mapsto\; x - ay$$

is a bijective map. It is also easy to verify that ϕ is a group homomorphism. Hence C is a cyclic group of order $q-1$. ■

Note that if $\chi(D) = -1$, then the isomorphism ϕ is trivial to compute, while if $\chi(D) = 1$, then the isomorphism ψ is easy to compute, given a square root a of D in F_q. Since square roots in F_q can be computed in probabilistic polynomial time (see [1]) we can state the next result.

Theorem 6 *If $\chi(D) = -1$ then the logarithm problem in C is reducible in constant time to the logarithm problem in F_{q^2}. If $\chi(D) = 1$, then the logarithm problem in C is reducible in probabilistic polynomial time to the logarithm problem in F_q.* ■

4 A Class of Matrix Groups

We first review some basic notions from linear algebra (see [8]). Let $f(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n$ be a monic polynomial in $F_q[x]$. The companion matrix of f is the $n \times n$ matrix

$$C_f = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}$$

We have $C_f \in GL(n, q)$ if and only if $f(0) = a_0 \neq 0$. The characteristic polynomial equation of C_f is just $f(x) = 0$, and the minimal polynomial and characteristic polynomial of C_f are identical. If f is irreducible over F_q, then the order of C_f is equal to the order of any root of f in F_{q^n}. Consequently, if f is a primitive polynomial, then $ord(C_f) = q^n - 1$.

In [16], the authors propose the following group for use in the Diffie-Hellman key passing scheme. Let $f_1, f_2, \ldots, f_s$ be distinct primitive polynomials over F_q of degrees $m_1, m_2, \ldots, m_s$ respectively (in [16], the authors erroneously use irreducible polynomials instead of primitive polynomials). Let C_i be the companion matrix of f_i, and define the block matrix

$$C = \begin{pmatrix} C_1 & 0 & \cdots & 0 \\ 0 & C_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & C_s \end{pmatrix}$$

Then $C \in GL(n, q)$, where $n = \sum_{i=1}^{s} m_i$. Let P be an arbitrary matrix in $GL(n, q)$, and set $A = P^{-1}CP$. The order of A is

$$\begin{aligned} ord(A) &= ord(C) \\ &= lcm(\, ord(C_1),\, ord(C_2),\, \ldots,\, ord(C_s)\,) \\ &= lcm(\, q^{m_1} - 1,\, q^{m_2} - 1,\, \ldots,\, q^{m_s} - 1\,), \end{aligned}$$

and the group used is $< A >$, the subgroup of $GL(n, q)$ generated by A. The discrete logarithm problem in $< A >$ is to find l, given A and $B = A^l$. In [15, p. 230], Odlyzko comments that this problem is reducible to the problem of computing logarithms in the fields $F_{q^{m_i}}$. We now show how this can be accomplished.

Note that the characteristic polynomial equation of C, and thus also that of A, is $f = f_1 f_2 \cdots f_s = 0$. For each i, $1 \leq i \leq s$, the polynomial f_i splits in $F_{q^{m_i}}$. Thus the splitting field of f over F_q is F_{q^k}, where $k = lcm(m_1, m_2, \ldots, m_s)$. Since the f_i are distinct, the roots of f (the eigenvalues of A) are also distinct, and hence A is diagonalizable over F_{q^k}. Hence we can write $D = Q^{-1}AQ$, where D is the diagonal matrix with diagonal entries being the roots of f. Let α_{ij}, $1 \leq j \leq m_i$, be the roots of f_i in F_{q^k}. Then

$D^l = Q^{-1}A^lQ = Q^{-1}BQ$, and so we can determine D^l. For each i, let β_i be the entry in D^l which is in the same position as α_{i1} in D. Then we have that $\beta_i = \alpha_{i1}^l$, and so we can determine l modulo $(q^{m_i} - 1)$ by solving a discrete logarithm problem in F_{q^k}. Using the generalized Chinese Remainder Theorem, we can put these results together to obtain l modulo $ord(A)$, as desired.

In order for the reduction to be polynomial time, k should be bounded by a polynomial in the size of the input A, namely $n^2 \log_2 q$. This is not true in general, as the following argument shows. Let s be the number of primes less than d, and let m_i be the i^{th} prime. Then by [17, Corollary 1], we have

$$s \ < \ (1.3d)/(\log d),$$

and hence

$$n \ = \ \sum_{i=1}^{s} m_i \ < \ (1.3d^2)/(\log d) \ < \ 1.3d^2,$$

and so $d > 0.87\sqrt{n}$. Now, by [17, Theorem 10], we have that for $d \geq 101$,

$$k \ = \ \prod_{i=1}^{s} m_i \ > \ e^{0.84d} \ > \ e^{0.7\sqrt{n}}.$$

To overcome the problem of k being too big, we do the computations in the fields $F_{q^{m_1}}$, $F_{q^{m_2}}$, ..., $F_{q^{m_s}}$ in turn.

Theorem 7 *The logarithm problem in $<A>$ is reducible in probabilistic polynomial time to the logarithm problems in the fields $F_{q^{m_1}}$, $F_{q^{m_2}}$, ..., $F_{q^{m_s}}$.*

Proof After determining f, the factorization $f = f_1 f_2 \cdots f_s$ over F_q can be obtained in probabilistic polynomial time using the algorithm in [1]. This determines the numbers $m_1, m_2, \ldots, m_s$. To do arithmetic in $F_{q^{m_i}}$, we need to find an irreducible polynomial $g_i(x)$ of degree m_i over F_q. We can simply choose $g_i(x)$ to be $f_i(x)$. We then have $F_{q^{m_i}} \cong F_q[x]/(g_i(x))$, and that $\alpha_{i1} = x$ is an eigenvalue of A in $F_{q^{m_i}}$. Note that the constant polynomials in $F_q[x]$ form a subfield isomorphic to F_q.
For each i, $1 \leq i \leq s$, we can find α_{i1}^l as follows. Let μ_i be an eigenvector of A corresponding to the eigenvalue α_{i1}. This can, of course, be obtained by finding a non-zero solution y to $(A - \alpha_{i1}I)y = 0$; note that the components of μ_i can be chosen to be in $F_{q^{m_i}}$. Let $Q_i \in GL(n, q^{m_i})$ be such that the first column of Q_i is μ_i. Then the first column of the matrix $D_i = Q_i^{-1}AQ_i$ is $(\alpha_{i1}, 0, \ldots, 0)^t$. Hence the first column of $D_i^l = Q_i^{-1}BQ_i$ is $(\alpha_{i1}^l, 0, \ldots, 0)^t$. Now, μ_i, Q_i^{-1} and D_i^l can be computed in time that is bounded by a polynomial in n and $m_i \log q$. Since $m_i \leq n$, and $s \leq n$, we conclude that the expected time of the reduction is bounded by a polynomial in n and $\log q$. ■

5 Conclusions

By Theorem 2, we see that the logarithm problem in $E_{ns}(F_q)$ is no harder than the logarithm problem in F_{q^k}, where $k = 1$ or $k = 2$, in the case that E has a node. If E has a cusp, then logarithms in $E_{ns}(F_q)$ can be efficiently computed. Theorem 6 states that the logarithm problem in C is no harder than the logarithm problem in F_{q^k}, where $k = 1$ or $k = 2$. This is perhaps a little surprising since the group operation in C seems more complicated that the multiplication operation in F_q. Similarly, Theorem 7 says that the logarithm problem in $<A>$ is no more difficult than the logarithm problem in a suitable extension F_{q^m}, where $m = max\{m_1, m_2, \ldots, m_s\}$, and $m \leq n$. Since the group operation in C or in $<A>$ is more expensive that the group operation in the fields F_{q^k} or F_{q^m} respectively, the former groups offer no advantage over finite fields for the implementation of cryptographic protocols whose security is based on the difficulty of computing discrete logarithms in a group.

References

[1] M. Ben-Or, "Probabilistic algorithms in finite fields", *22nd Annual Symposium on Foundations of Computer Science*, 394-398, 1981.

[2] J. Buchmann and H. Williams, "A key-exchange system based on imaginary quadratic fields" *Journal of Cryptology*, **1** (1988), 107-118.

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

[4] D. Coppersmith, A. Odlyzko and R. Schroeppel, "Discrete logarithms in $GF(p)$", *Algorithmica*, **1** (1986), 1-15.

[5] W. Diffie and M. Hellman, "New directions in cryptography", *IEEE Transactions on Information Theory*, **22** (1976), 644-654.

[6] ElG85a T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms", *IEEE Transactions on Information Theory*, **31** (1985), 469-472.

[7] T. ElGamal, "A subexponential-time algorithm for computing discrete logarithms over $GF(p^2)$", *IEEE Transactions on Information Theory*, **31** (1985), 473-481.

[8] K. Hoffman and R. Kunze, *Linear Algebra*, Prentice-Hall, N. J., 1971.

[9] D. Husemöller, *Elliptic Curves*, Springer-Verlag, New York, 1987.

[10] N. Koblitz, "Elliptic curve cryptosystems", *Mathematics of Computation*, **48** (1987), 203-209.

[11] N. Koblitz, "Hyperelliptic cryptosystems", *Journal of Cryptology*, **1** (1989), 139-150.

[12] K. McCurley, "The discrete logarithm problem", *Cryptology and Computational Number Theory*, Proceedings of Symposia in Applied Mathematics, **42** (1990), 49-74.

[13] A. Menezes, T. Okamoto and S. Vanstone, "Reducing elliptic curve logarithms to logarithms in a finite field", *Proceedings of the 23rd Annual ACM Symposium on the Theory of Computing*, 80-89, 1991.

[14] V. Miller, "Uses of elliptic curves in cryptography", *Advances in Cryptology – Proceedings of Crypto '85*, Lecture Notes in Computer Science, **218** (1986), Springer-Verlag, 417-426.

[15] A. Odlyzko, "Discrete logarithms in finite fields and their cryptographic significance", *Advances in Cryptology – Proceedings of Eurocrypt '84*, Lecture Notes in Computer Science, **209** (1985), Springer-Verlag, 224-314.

[16] R. Odoni, V. Varadharajan and R. Sanders, "Public key distribution in matrix rings", *Electronic Letters*, **20** (1984), 386-387.

[17] J. Rosser and L. Schoenfield, "Approximate formulas for some functions of prime numbers", *Illinois Journal of Mathematics*, **6** (1962), 64-94.

[18] J. Shallit, personal communication, 1991.

[19] J. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986.