MATHEMATICS OF COMPUTATION
Volume 67, Number 221, January 1998, Pages 353–356
S 0025-5718(98)00887-4

EVALUATION OF DISCRETE LOGARITHMS IN A GROUP OF p-TORSION POINTS OF AN ELLIPTIC CURVE IN CHARACTERISTIC p

I. A. SEMAEV

Abstract. We show that to solve the discrete log problem in a subgroup of order p of an elliptic curve over the finite field of characteristic p one needs $O(\ln p)$ operations in this field.

Let F_q be the finite field of $q = p^l$ elements. We define an elliptic curve E over F_q to be an equation of the form

$$y^2 = x^3 + Ax + B.$$

We suppose $p \neq 2, 3$. Let $E(F_q)$ be the set of points E rational over F_q. It is known that $|N_q - q - 1| \leq 2q^{1/2}$ with $N_q = |E(F_q)|$. The set $E(F_q)$ is a finite abelian group with the "infinite point" P_∞ as the identity element.

The discrete logarithm problem is to compute an integer n such that $Q = nP$, where $Q, P \in E(F_q)$, if such an n exists. This problem is of great significance in cryptology [1], [2]. Suppose that the point P generates a subgroup $\langle P\rangle$ of order m. If $(m, p) = 1$, then the subgroup $\langle P\rangle$ is isomorphic to some multiplicative subgroup of an extension F_{q^k} where $q^k \equiv 1 \pmod{m}$. The values of the isomorphism from $\langle P\rangle$ to F_q^* can be evaluated in a very simple manner. The complexity of the algorithm is no more than $O(\ln m)$ operations in F_{q^k} [3], [4], [5]. Thus when k is small we have an algorithm for the discrete log problem in $\langle P\rangle$ more effective than the algorithms of the kind shown in [6], [7]. However if $(m, p) \neq 1$ the reduction above is impossible. We have $m = p^s m_1$ where $s > 0$ and $(m_1, p) = 1$. Consequently, the discrete log problem in $\langle P\rangle$ is reduced to a discrete log problem in subgroups of order m_1 and p. For the subgroup of order m_1 one can apply the reduction to a multiplicative subgroup of the extension F_{q^k} with minimal k such that $q^k \equiv 1 \pmod{m_1}$.

In this paper we construct an isomorphism from the subgroup of order p to the additive group of F_q. One can evaluate the values of this isomorphism with $O(\ln p)$ operations in F_q. Thus the discrete log problem in a subgroup of order p of an elliptic curve over the field of characteristic p is polynomial.

Assume that a point $P \in E(F_q)$ generates a subgroup of order p. We let t_R denote a local parameter at a point R the coordinates of which are (x_R, y_R) if $R \neq P_\infty$. If R is not of order 2 or P_∞, then $t_R = x - x_R$. If $R \neq P_\infty$ is a point of order 2, then $t_R = y$. Finally $t_{P_\infty} = x/y$. It must be noted that a point R of order

Received by the editor August 30, 1995 and, in revised form, September 11, 1996.
1991 *Mathematics Subject Classification.* Primary 94A60.
Key words and phrases. Cryptography, elliptic curves, discrete logarithms.

2 on E has the coordinates $(x_R, 0)$. Let us take up to the end of this article a point $R \in \langle P\rangle - P_\infty$.

It is known that E is isomorphic to the quotient of the group of divisors of degree 0 by the subgroup of principal divisors, a point Q corresponding to a divisor $D_q = \sum n_T T$ where Q is a sum on E of the points T taken with multiplicities n_T. For example, $D_Q = (Q) - (P_\infty)$. If $Q \in \langle P\rangle$, then pD_Q is a principal divisor that is denoted $(f_Q) = pD_Q$ for some function f_Q on E.

Lemma 1. *Let f be a function on E such that $(f) = pD$ for some nonprincipal divisor D. Let $f' = df/dx$ be the derivative of f with respect to x. Then $(f') = (f) - (y)$.*

Proof. Let v_Q be the valuation at the point Q. Let $D = \sum n_Q Q$. Set $f = t_Q^{pl_Q} f_1$ where f_1 is regular at Q and $f_1(Q) \neq 0$. First we assume that Q is not in the divisor of the function y; that is, Q is neither of order 2 nor P_∞. Hence $df/dx = df/d(x - x_Q) = t_Q^{pl_Q} df_1/dt_Q$. The function df_1/dt_Q is regular at Q [8]. Then $v_Q(f') = pl_Q + m_Q$ where $m_Q = v_Q(df_1/dt_Q) \geq 0$. Let Q be a point of order 2. Then

$$df/dx = (df/dy)dy/dx = y^{pl_Q}((3x^2 + A)/2y)df_1/dy,$$

where $dy/dx = (3x^2 + A)/2y$. Since $v_Q((3x^2 + A)/2y) = -1$, in this case $v_Q(f') = pl_Q + m_Q - 1$, with $m_Q = v_Q(df_1/dt_Q) \geq 0$. Set $Q = P_\infty$. Then

$$df/dx = (df/d(x/y))d(x/y)/dx = (x/y)^{pl_Q}((-x^3 + Ax + B)/2y^3)df_1/d(x/y),$$

where $d(x/y)/dx = (-x^3 + Ax + B)/2y^3$. Hence we have $v_Q(f') = pl_Q + m_Q + 3$ because $v_{P_\infty}((-x^3 + Ax + B)/2y^3) = 3$ and $m_Q = v_Q(df_1/dt_Q) \geq 0$. Let $D_1 = \sum m_Q Q$. As we have seen D_1 is a positive divisor. On the other hand, since $(f') = (f) - (y) + D_1$, the divisor D_1 is principal. So $D_1 = 0$ and the lemma is proved.

Consider the following map ϕ of points of the group $\langle P\rangle$ to F_q:

$$\phi(Q) = (f'_Q/f_Q)(R), \qquad \phi(P_\infty) = 0.$$

Lemma 2. *The value $\phi(Q)$ is well defined. The map ϕ is an isomorphic embedding of $\langle P\rangle$ into the additive group of F_q.*

Proof. Let D'_Q, D_Q be linearly equivalent divisors. Hence there is the function g such that $(g) = D_Q - D'_Q$. So if $(f) = pD'_Q$, then $g^p f = f_Q$. It is easy to see that $f'_Q/f_Q = f'/f$ so that $\phi(Q)$ is well defined. One can always take D_Q rational over F_q. So $f'_Q/f_Q(R) \in F_q$, since R is rational over F_q. Let us show that ϕ is a homomorphism. Let $Q_i \in \langle P\rangle$ and $(f_{Q_i}) = pD_{Q_i}$, $i = 1, 2$. Define $D_{Q_1+Q_2} = D_{Q_1} + D_{Q_2}$. Then

$$(f_{Q_1+Q_2}) = pD_{Q_1+Q_2} = (f_{Q_1} f_{Q_2}).$$

So the functions $f_{Q_1+Q_2}$ and $f_{Q_1} f_{Q_2}$ are equal up to a multiplicative constant. Hence

$$f'_{Q_1+Q_2}/f_{Q_1+Q_2} = f'_{Q_1}/f_{Q_1} + f'_{Q_2}/f_{Q_2}.$$

We have proved that ϕ is a homomorphism. Since ϕ is non-vanishing on $\langle P\rangle$, then ϕ is an isomorphism and the lemma is proved.

The construction of this isomorphism can also be derived from a general result of Serre [9, pp. 40–41].

Lemma 3. *Let $Q \in \langle P\rangle$. Then the value of the function f'_Q/f_Q at R can be evaluated with $O(\ln p)$ operations in F_q.*

Proof. Let us take $D_Q = (Q+S) - (S)$ where S is of order 2 exactly. Denote by ψ_k the function such that

$$(\psi_k) = k(Q+S) - (kQ+S) - (k-1)(S).$$

Clearly $\psi_p = f_Q$ up to a multiplicative constant. Let $k = k_1 + k_2$, $k_i \geq 0$. Then the following identity is valid [4]:

$$\psi_k \lambda_{k_1,k_2} = \psi_{k_1}\psi_{k_2}, \tag{1}$$

where λ_{k_1,k_2} is a function such that

$$(\lambda_{k_1,k_2}) = (kQ+S) - (k_1Q+S) - (k_2Q+S) + (S).$$

The identity (1) gives us a method for evaluation of the value $f'_Q/f_Q(R)$. Indeed, from (1) we have

$$\psi'_k/\psi_k = \psi'_{k_1}/\psi_{k_1} + \psi'_{k_2}/\psi_{k_2} - \lambda'_{k_1,k_2}/\lambda_{k_1,k_2}.$$

Hence the function ψ'_k/ψ_k is expressed by a linear combination of $O(\ln k)$ functions of the form $\lambda'_{k_1,k_2}/\lambda_{k_1,k_2}$. Let η_{k_1,k_2} be

$$(\eta_{k_1,k_2}) = ((k_1+k_2)Q+S) + (-k_1Q+S) + (-k_2Q+S) - 3(S),$$

κ_k be

$$(\kappa_k) = (kQ+S) + (-kQ+S) - 2(S).$$

Let us note that $\eta_{k_1,k_2}(X-S), \kappa_{k_1}(X-S)$ are linear functions in x, y. The coefficients of these functions are determined by the coordinates of the points $(k_1+k_2)Q, k_1Q, k_2Q$. We have the equality

$$\lambda_{k_1,k_2} = \eta_{k_1,k_2}\kappa_{k_1}^{-1}\kappa_{k_2}^{-1}.$$

Then it is easy to see that

$$\lambda'_{k_1,k_2}/\lambda_{k_1,k_2} = \eta'_{k_1,k_2}/\eta_{k_1,k_2} - \kappa'_{k_1}/\kappa_{k_1} - \kappa'_{k_2}/\kappa_{k_2}.$$

The functions on the right-hand side of this equality can be determined from the following considerations. Let $\delta = ax + by + c$ be any linear function in x, y. Let $\delta_1 = \delta(X+S)$. We have to find the value of the function δ'_1/δ_1 at some point R. Express this function by the functions δ, δ', where $\delta' = d\delta/dx = a + b(3x^2+A)/2y$. We have $d\delta = (2y\delta')dx/2y$. It is known [8] that $dx/2y$ is an invariant differential on E. In other words $(dx/2y)(X+S) = (dx/2y)(X)$ for any point $S \in E$. So denoting $\delta_2 = 2y\delta'$ we have $d\delta(X+S) = \delta_2(X+S)dx/2y$. Hence $\delta'_1 = \delta_2(X+S)/2y$. Finally,

$$\delta'_1/\delta_1 = \delta_2(X+S)/2y\delta(X+S). \tag{2}$$

Thus we have to evaluate the values of $O(\ln k)$ functions of type δ'/δ where the coefficients are determined by the coordinates of the points $(k_1+k_2)Q, k_1Q, k_2Q$. Altogether we have to evaluate $O(\ln k)$ such points. Since the points of this set are expressed by the same set, the complexity of this calculation is no more than $O(\ln k)$ operations in F_q.

From (2) it follows that the functions $\eta'_{k_1,k_2}/\eta_{k_1,k_2}, \kappa'_{k_i}/\kappa_{k_i}$ are regular at R. Thus the total complexity of evaluation of the values of the functions ψ'_k/ψ_k at R

takes no more than $O(\ln k)$ operations in F_q. Note that the calculations above are performed in the extension of F_q obtained by adjoining the point of order 2. Since this extension has degree at most 3, the complexity of the operations in this field is proportional to those in F_q. This proves the lemma.

From Lemma 3 it follows that the complexity of the discrete log problem in the group $\langle P\rangle$ is no more than $O(\ln p)$ operations in F_q. Actually, to get an integer n such that $Q = nP$ in $E(F_q)$ one must evaluate the values $\phi(Q), \psi(P) \in F_q$, then $n = \phi(Q)(\phi(P))^{-1}$.

In [10] H.-G. Ruck generalizes the results of the present paper to curves of arbitrary genus.

References

1. V. Miller, *Use of elliptic curves in cryptography*, Advances in Cryptology—Crypto '85, Springer-Verlag, New York, 1986, 417–426. MR **88b:**68040
2. N. Koblitz, *Elliptic curve cryptosystems*, Math. Comp. **48** (1987), 203–209. MR **88b:**94017
3. A. Menezes, S. Vanstone, and O. Tatsuaki, *Reducing elliptic curve logarithms to logarithms in a finite field*, Proc. 23rd ACM Sympos. Theory of Computing, 1991, pp. 80–89.
4. И. А. Семаев, *Быстрый алгоритм вычисления спаривания А. Вейля на эллиптической кривой*, International Conference "Modern Problems in Number Theory", Russia, Tula, Sept. 20–25, 1993, Abstracts of papers.
5. G. Frey and H.-G. Ruck, *A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves*, Math. Comp. **62** (1994), 865–874. MR **94h:**11056
6. S. Pohlig and M. Hellman, *An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic significance*, IEEE Trans. Inform. Theory, IT-24 (1978), 106–110. MR **58:**4617
7. J. M. Pollard, *Monte-Carlo methods for index computation* $(\bmod p)$, Math. Comp. **32** (1978), 918–924. MR **58:**10684
8. J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, 1986. MR **87g:**11070
9. J. P. Serre, *Sur la topologie des variétés algébriques en caractéristique p*, Sympos. Internac. Topologia Algebraica, Mexico City, 1956, 24–53. MR **20:**4559
10. H.-G. Ruck, *A remark on the paper "Evaluation of discrete logarithms on some elliptic curves, by I. A. Semaev"*, communication to "Mathematics of Computation".

43-2 Profsoyusnaya ul., Apt. 723, 117420 Moscow, Russia