# 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

$$
y^{2}=x^{3}+A x+B
$$

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

The discrete logarithm problem is to compute an integer $n$ such that $Q=n P$, where $Q, P \in E\left(F_{q}\right)$, 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 $q^{k} \equiv 1(\bmod m)$. 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 $\left(m_{1}, p\right)=1$. 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 $q^{k} \equiv 1\left(\bmod m_{1}\right)$.

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 $P \in E\left(F_{q}\right)$ generates a subgroup of order $p$. We let $t_{R}$ denote a local parameter at a point $R$ the coordinates of which are $\left(x_{R}, y_{R}\right)$ if $R \neq P_{\infty}$. If $R$ is not of order 2 or $P_{\infty}$, 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

[^0]2 on $E$ has the coordinates $\left(x_{R}, 0\right)$. 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, $D_{Q}=(Q)-\left(P_{\infty}\right)$. If $Q \in\langle P\rangle$, then $p D_{Q}$ is a principal divisor that is denoted $\left(f_{Q}\right)=p D_{Q}$ for some function $f_{Q}$ on $E$.

Lemma 1. Let $f$ be a function on $E$ such that $(f)=p D$ for some nonprincipal divisor $D$. Let $f^{\prime}=d f / d x$ be the derivative of $f$ with respect to $x$. Then $\left(f^{\prime}\right)=$ $(f)-(y)$.
Proof. Let $v_{Q}$ be the valuation at the point $Q$. Let $D=\sum n_{Q} Q$. Set $f=t_{Q}^{p l_{Q}} f_{1}$ 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 $P_{\infty}$. Hence $d f / d x=$ $d f / d\left(x-x_{Q}\right)=t_{Q}^{p l_{Q}} d f_{1} / d t_{Q}$. The function $d f_{1} / d t_{Q}$ is regular at $Q$ [8]. Then $v_{Q}\left(f^{\prime}\right)=p l_{Q}+m_{Q}$ where $m_{Q}=v_{Q}\left(d f_{1} / d t_{Q}\right) \geq 0$. Let $Q$ be a point of order 2 . Then

$$
d f / d x=(d f / d y) d y / d x=y^{p l_{Q}}\left(\left(3 x^{2}+A\right) / 2 y\right) d f_{1} / d y
$$

where $d y / d x=\left(3 x^{2}+A\right) / 2 y$. Since $v_{Q}\left(\left(3 x^{2}+A\right) / 2 y\right)=-1$, in this case $v_{Q}\left(f^{\prime}\right)=$ $p l_{Q}+m_{Q}-1$, with $m_{Q}=v_{Q}\left(d f_{1} / d t_{Q}\right) \geq 0$. Set $Q=P_{\infty}$. Then

$$
d f / d x=(d f / d(x / y)) d(x / y) / d x=(x / y)^{p l_{Q}}\left(\left(-x^{3}+A x+B\right) / 2 y^{3}\right) d f_{1} / d(x / y)
$$

where $d(x / y) / d x=\left(-x^{3}+A x+B\right) / 2 y^{3}$. Hence we have $v_{Q}\left(f^{\prime}\right)=p l_{Q}+m_{Q}+3$ because $v_{P_{\infty}}\left(\left(-x^{3}+A x+B\right) / 2 y^{3}\right)=3$ and $m_{Q}=v_{Q}\left(d f_{1} / d t_{Q}\right) \geq 0$. Let $D_{1}=$ $\sum m_{Q} Q$. As we have seen $D_{1}$ is a positive divisor. On the other hand, since $\left(f^{\prime}\right)=(f)-(y)+D_{1}$, the divisor $D_{1}$ is principal. So $D_{1}=0$ and the lemma is proved.

Consider the following map $\phi$ of points of the group $\langle P\rangle$ to $F_{q}$ :

$$
\phi(Q)=\left(f_{Q}^{\prime} / f_{Q}\right)(R), \quad \phi\left(P_{\infty}\right)=0
$$

Lemma 2. The value $\phi(Q)$ is well defined. The map $\phi$ is an isomorphic embedding of $\langle P\rangle$ into the additive group of $F_{q}$.

Proof. Let $D_{Q}^{\prime}, D_{Q}$ be linearly equivalent divisors. Hence there is the function $g$ such that $(g)=D_{Q}-D_{Q}^{\prime}$. So if $(f)=p D_{Q}^{\prime}$, then $g^{p} f=f_{Q}$. It is easy to see that $f_{Q}^{\prime} / f_{Q}=f^{\prime} / f$ so that $\phi(Q)$ is well defined. One can always take $D_{Q}$ rational over $F_{q}$. So $f_{Q}^{\prime} / f_{Q}(R) \in F_{q}$, since $R$ is rational over $F_{q}$. Let us show that $\phi$ is a homomorphism. Let $Q_{i} \in\langle P\rangle$ and $\left(f_{Q_{i}}\right)=p D_{Q_{i}}, i=1,2$. Define $D_{Q_{1}+Q_{2}}=D_{Q_{1}}+D_{Q_{2}}$. Then

$$
\left(f_{Q_{1}+Q_{2}}\right)=p D_{Q_{1}+Q_{2}}=\left(f_{Q_{1}} f_{Q_{2}}\right)
$$

So the functions $f_{Q_{1}+Q_{2}}$ and $f_{Q_{1}} f_{Q_{2}}$ are equal up to a multiplicative constant. Hence

$$
f_{Q_{1}+Q_{2}}^{\prime} / f_{Q_{1}+Q_{2}}=f_{Q_{1}}^{\prime} / f_{Q_{1}}+f_{Q_{2}}^{\prime} / f_{Q_{2}}
$$

We have proved that $\phi$ is a homomorphism. Since $\phi$ is non-vanishing on $\langle P\rangle$, then $\phi$ 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 $f_{Q}^{\prime} / f_{Q}$ 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 $\psi_{k}$ the function such that

$$
\left(\psi_{k}\right)=k(Q+S)-(k Q+S)-(k-1)(S)
$$

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]:

$$
\begin{equation*}
\psi_{k} \lambda_{k_{1}, k_{2}}=\psi_{k_{1}} \psi_{k_{2}} \tag{1}
\end{equation*}
$$

where $\lambda_{k_{1}, k_{2}}$ is a function such that

$$
\left(\lambda_{k_{1}, k_{2}}\right)=(k Q+S)-\left(k_{1} Q+S\right)-\left(k_{2} Q+S\right)+(S)
$$

The identity (1) gives us a method for evaluation of the value $f_{Q}^{\prime} / f_{Q}(R)$. Indeed, from (1) we have

$$
\psi_{k}^{\prime} / \psi_{k}=\psi_{k_{1}}^{\prime} / \psi_{k_{1}}+\psi_{k_{2}}^{\prime} / \psi_{k_{2}}-\lambda_{k_{1}, k_{2}}^{\prime} / \lambda_{k_{1}, k_{2}}
$$

Hence the function $\psi_{k}^{\prime} / \psi_{k}$ is expressed by a linear combination of $O(\ln k)$ functions of the form $\lambda_{k_{1}, k_{2}}^{\prime} / \lambda_{k_{1}, k_{2}}$. Let $\eta_{k_{1}, k_{2}}$ be

$$
\left(\eta_{k_{1}, k_{2}}\right)=\left(\left(k_{1}+k_{2}\right) Q+S\right)+\left(-k_{1} Q+S\right)+\left(-k_{2} Q+S\right)-3(S)
$$

$\kappa_{k}$ be

$$
\left(\kappa_{k}\right)=(k Q+S)+(-k Q+S)-2(S)
$$

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 $\left(k_{1}+k_{2}\right) Q, k_{1} Q, k_{2} Q$. 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

$$
\lambda_{k_{1}, k_{2}}^{\prime} / \lambda_{k_{1}, k_{2}}=\eta_{k_{1}, k_{2}}^{\prime} / \eta_{k_{1}, k_{2}}-\kappa_{k_{1}}^{\prime} / \kappa_{k_{1}}-\kappa_{k_{2}}^{\prime} / \kappa_{k_{2}}
$$

The functions on the right-hand side of this equality can be determined from the following considerations. Let $\delta=a x+b y+c$ be any linear function in $x, y$. Let $\delta_{1}=\delta(X+S)$. We have to find the value of the function $\delta_{1}^{\prime} / \delta_{1}$ at some point $R$. Express this function by the functions $\delta, \delta^{\prime}$, where $\delta^{\prime}=d \delta / d x=a+b\left(3 x^{2}+A\right) / 2 y$. We have $d \delta=\left(2 y \delta^{\prime}\right) d x / 2 y$. It is known [8] that $d x / 2 y$ is an invariant differential on $E$. In other words $(d x / 2 y)(X+S)=(d x / 2 y)(X)$ for any point $S \in E$. So denoting $\delta_{2}=2 y \delta^{\prime}$ we have $d \delta(X+S)=\delta_{2}(X+S) d x / 2 y$. Hence $\delta_{1}^{\prime}=\delta_{2}(X+S) / 2 y$. Finally,

$$
\begin{equation*}
\delta_{1}^{\prime} / \delta_{1}=\delta_{2}(X+S) / 2 y \delta(X+S) \tag{2}
\end{equation*}
$$

Thus we have to evaluate the values of $O(\ln k)$ functions of type $\delta^{\prime} / \delta$ where the coefficients are determined by the coordinates of the points $\left(k_{1}+k_{2}\right) Q, k_{1} Q, k_{2} Q$. 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 $\eta_{k_{1}, k_{2}}^{\prime} / \eta_{k_{1}, k_{2}}, \kappa_{k_{i}}^{\prime} / \kappa_{k_{i}}$ are regular at $R$. Thus the total complexity of evaluation of the values of the functions $\psi_{k}^{\prime} / \psi_{k}$ 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 $Q=n P$ in $E\left(F_{q}\right)$ 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 $G F(p)$ 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 (mod p), Math. Comp. 32 (1978), 918-924. MR 58:10684
8. J. H. Silverman, The arithmetic of elliptic curves, Springer-Verlag, 1986. MR $\mathbf{8 7 g} \mathbf{1 1 0 7 0}$
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


[^0]:    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.

