J. Cryptology (1999) 12: 193–196

Journal of
CRYPTOLOGY

The Discrete Logarithm Problem on Elliptic Curves of Trace One

N. P. Smart
Hewlett-Packard Laboratories,
Filton Road, Stoke Gifford,
Bristol BS12 6QZ, England
nsma@hplb.hpl.hp.com

Communicated by Johannes Buchmann

Received 9 December 1997 and revised 11 March 1998

Abstract. In this short note we describe an elementary technique which leads to a linear algorithm for solving the discrete logarithm problem on elliptic curves of trace one. In practice the method described means that when choosing elliptic curves to use in cryptography one has to eliminate all curves whose group orders are equal to the order of the finite field.

Key words. Elliptic curve discrete logarithm problem.

Recently attention in cryptography has focused on the use of elliptic curves in public key cryptography, starting with the work of Koblitz [1] and Miller [3]. This is because there is no known sub-exponential type algorithm to solve the discrete logarithm problem on a general elliptic curve. The standard protocols in cryptography which make use of the discrete logarithm problem in finite fields, such as Diffie–Hellman key exchange, El Gamal and Massey–Omura, can all be made to work in the elliptic curve case.

Due to work of Menezes et al. [2], it is already known that one must avoid elliptic curves which are supersingular, these are the curves which have trace of frobenius equal to zero. Menezes et al. reduce the discrete logarithm problem on supersingular elliptic curves to the discrete logarithm problem in a finite field. They hence reduce the problem to one which is known to have sub-exponential complexity. In this paper we show that one must also avoid the use of curves for which the group order is equal to the order of the finite field, in other words curves for which the trace of Frobenius is equal to one. Hence these are curves for which

$$\#E(\mathbb{F}_p) = p.$$

In addition our method for solving the discrete logarithm problem on this curve runs in

linear time when time is measured in terms of the number of basic group operations that one must perform.

The method of attack has more than just academic interest as elliptic curves of trace one have been proposed as curves to be used in practical systems [4]. At first sight this seems a good idea as if a curve is defined over a prime base field of p elements and the curve has order p, then clearly the standard square root attacks on the discrete logarithm problem will not be effective, at least if p is large enough. However, such curves have an addition structure which renders the systems very weak, as we now show.

After announcing this attack on the Internet it came to my attention that two other groups have also independently come up with roughly the same method at roughly the same time, see [5] and [6].

We assume that our elliptic curve, $\overline{E}$, is defined over a prime finite field, $\mathbb{F}_p$, and that the number of points on $\overline{E}$ is equal to p. Hence the trace of Frobenius is equal to one. Suppose we have two points on the curve, $\overline{P}$ and $\overline{Q}$, and we want to solve the following discrete logarithm problem on $\overline{E}(\mathbb{F}_p)$,

$$\overline{Q} = [m]\overline{P},$$

for some integer m. It would be nice to be able to apply a "logarithm" map to the above equation and hence solve the discrete logarithm problem. Such a "logarithm" would be a homomorphism from the group $\overline{E}(\mathbb{F}_p)$, into a group for which solving the logarithm problem is easy, such as $\mathbb{F}_p^+$. However, no such logarithm map is known which is defined on curves over $\mathbb{F}_p$, however, such a map is known for curves over $\mathbb{Q}_p$.

We first compute an arbitrary lift of $\overline{P}$ and $\overline{Q}$ to points, P and Q, on an elliptic curve, E, defined over $\mathbb{Q}_p$ whose reduction modulo p gives $\overline{E}$. This is trivial in practice as, because neither $\overline{P}$ nor $\overline{Q}$ are points of order two, we can write $P = (x, y)$ where x is the x-coordinate of $\overline{P}$ and y is computed via Hensel's lemma.

We then have

$$Q - [m]P = R \in E_1(\mathbb{Q}_p),$$

where the groups $E_n(\mathbb{Q}_p)$ are as defined in Chapter VII of [7]. We note

$$E_0(\mathbb{Q}_p)/E_1(\mathbb{Q}_p) \cong E(\mathbb{F}_p) \quad \text{and} \quad E_1(\mathbb{Q}_p)/E_2(\mathbb{Q}_p) \cong \mathbb{F}_p^+.$$

However, we still have no "logarithm" map, as the standard logarithm map for curves defined over $\mathbb{Q}_p$ is only defined on the points of $E(\mathbb{Q}_p)$ which belong to $E_1(\mathbb{Q}_p)$. The groups $E(\mathbb{F}_p) = \overline{E}(\mathbb{F}_p)$ and $\mathbb{F}_p^+$ have the same order by assumption, namely p, which means that we have the equation

$$[p]Q - [m]([p]P) = [p]R \in E_2(\mathbb{Q}_p).$$

We can then apply the p-adic elliptic logarithm, $_p$, to the terms $[p]Q$, $[p]P$ and $[p]R$ which are all points in $E_1(\mathbb{Q}_p)$. We obtain, as $R \in E_1(\mathbb{Q}_p)$ and $[p]R \in E_2(\mathbb{Q}_p)$,

$$_p([p]Q) - m \ _p([p]P) = \ _p([p]R) \equiv 0 \pmod{p^2}.$$

Computing the p-adic elliptic logarithm is an easy matter, see for instance Chapter IV of [7] or [8]. We only need that

$$_p((x, y)) \equiv \frac{-x}{y} \pmod{p^2},$$

if $(x, y) \in E_1(\mathbb{Q}_p)$. So hence

$$m \equiv \frac{{}_p([p]Q)}{{}_p([p]P)} \pmod{p}.$$

Clearly, on the assumption that one knows the group order, the above observation will solve the discrete logarithm problem in linear time. To see this, notice that the only non-trivial computation which needs to be performed is to compute $[p]P$ and $[p]Q$, both of which take $\log p$ group operations on E. However, we notice that in the above method we need only compute the numbers to an accuracy of p^2, so we need only work on the elliptic curve $E(\mathbb{Z}/p^2\mathbb{Z})$.

There is a case when the method will not work and that happens when the curve over $\mathbb{Q}_p$ that one lifts to is the canonical lift. This will happen with probability $1/p$, which in any real life application will be tiny. In such a situation we can easily detect that the method does not work, and all we need then do is perform the method again with another lift of the original curve $\overline{E}$.

Example. To explain the method we use a curve over a small field, namely $\mathbb{F}_{43}$. We take the curve

$$E : Y^2 = X^3 + 39X^2 + X + 41.$$

The group $E(\mathbb{F}_{43})$ can be readily verified to have 43 elements. On this curve we would like to solve the discrete logarithm problem given by

$$\overline{Q} = [m]\overline{P},$$

where $\overline{P} = (0, 16)$ and $\overline{Q} = (10, 36)$. We find the following "lifts" of these points to elements of $E(\mathbb{Q}_p)$ using Hensel's lemma:

$$\begin{aligned} P &= (0, 16 + 20.43 + O(43^2)), \\ Q &= (10, 36 + 40.43 + O(43^2)). \end{aligned}$$

We then need to compute $[43]P$ and $[43]Q$, which we find to be equal to

$$\begin{aligned} [43]P &= (38.43^{-2} + O(43^{-1}), 41.43^{-3} + O(43^{-2})), \\ [43]Q &= (24.43^{-2} + O(43^{-1}), 35.43^{-3} + O(43^{-2})). \end{aligned}$$

We then find that

$$\begin{aligned} {}_{43}([43]P) &= 19.43 + O(43^2), \\ {}_{43}([43]Q) &= 3.43 + O(43^2). \end{aligned}$$

Hence

$$m = \frac{{}_{43}([43]Q)}{{}_{43}([43]P)} = 16 + O(43),$$

and we conclude that m is equal to 16, which can be easily verified to be the correct solution.

References

[1] N. Koblitz. Elliptic curve cryptosystems. *Math. Comp*., 48:203–209, 1987.
[2] A. Menezes, T. Okamoto, and S. Vanstone. Reducing elliptic curve logarithms to a finite field. *IEEE Trans. Inform. Theory*, 39:1639–1646, 1993.
[3] V. Miller. Use of elliptic curves in cryptography. In *Advances in Cryptology, CRYPTO* 85, pages 417–426. LNCS 218, Springer-Verlag, Berlin, 1986.
[4] A. Miyaji. Elliptic curves over $\mathbb{F}_p$ suitable for cryptosystems. In *Advances in Cryptology, AUSCRYPT* 92, pages 479–491. LNCS 718, Springer-Verlag, Berlin, 1993.
[5] T. Satoh and K. Araki. Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves. *Comm. Math. Univ. Sancti. Pauli*, 47:81–92, 1998.
[6] I.A. Semaev. Evaluation of discrete logarithms on some elliptic curves. *Math. Comp*., 67:353–356, 1998.
[7] J.H. Silverman. *The Arithmetic of Elliptic Curves*. GTM 106, Springer-Verlag, New York, 1986.
[8] N.P. Smart. *S*-integral points on elliptic curves. *Proc. Cambridge Philos. Soc*., 116:391–399, 1994.