THE DISCRETE LOGARITHM PROBLEM ON ELLIPTIC CURVES OF TRACE ONE

N.P. SMART

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.

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, Okamoto and Vanstone, [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, Okamoto and Vanstone 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 shall 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. In addition our method runs 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 the 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 addition structure which renders the systems very weak as we shall now show.

We shall assume that our elliptic curve, E, is defined over a prime finite field, $\mathbb{F}_p$, and that the number of points on 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 $E(\mathbb{F}_p)$,

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

for some integer m. We first compute an arbitrary lift of $\overline{P}$ and $\overline{Q}$ to points, P and Q, on the same elliptic curve but considered as a curve over $\mathbb{Q}_p$. 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

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

where the groups $E_n(\mathbb{Q}_p)$ are as defined in [5][Chapter VII]. We note

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

But the groups $E(\mathbb{F}_p)$ and $\mathbb{F}_p^+$ have the same order by assumption, namely p. So we have

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

If we then take the p-adic elliptic logarithm, ψ_p, of every term in the previous equation we obtain

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

This is possible as for any point $P \in E(\mathbb{Q}_p)$ we have $[p]P \in E_1(\mathbb{Q}_p)$, as $p = |E(\mathbb{F}_p)|$, and the p-adic elliptic logarithm is defined on all points in $E_1(\mathbb{Q}_p)$. Computing the p-adic elliptic logarithm is an easy matter, see for instance [5][Chapter IV] or [6]. So hence

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

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.

1. Example

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

$$E : Y^2 = X^3 - 4X^2 - 128X - 432.$$

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 $P = (0, 16)$ and $Q = (12, 1)$. We find the following "lifts" of these points to elements of $E(\mathbb{Q}_p)$ using Hensel's Lemma,

$$\begin{aligned} P &= (0, 16 + 21.43 + 22.43^2 + 20.43^3 + 26.43^4 + 8.43^5 + 35.43^6 + 36.43^7 + O(43^8)), \\ Q &= (12, 1 + 12.43 + 35.43^2 + 29.43^3 + 18.43^4 + 36.43^5 + 14.43^6 + 14.43^7 + O(43^8)). \end{aligned}$$

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

$$\begin{aligned} [43]P &= (10.43^{-2} + 10.43^{-1} + 16 + 31.43 + 34.43^2 + O(43^3), \\ &\qquad 21.43^{-3} + 40.43^{-2} + 17.43^{-1} + 29 + 22.43 + 37.43^2 + O(43^3)), \\ [43]Q &= (13.43^{-2} + 41.43^{-1} + 9 + 9.43 + 24.43^2 + O(43^3), \\ &\qquad 41.43^{-3} + 14.43^{-2} + 42.43^{-1} + 15 + 30.43 + 28.43^2 + O(43^3)). \end{aligned}$$

We then find that

$$\begin{aligned} \psi_{43}([43]P) &= 20.43 + 6.43^2 + 32.43^3 + O(43^4), \\ \psi_{43}([43]Q) &= 28.43 + 15.43^2 + 22.43^3 + O(43^4). \end{aligned}$$

Hence

$$m = \frac{\psi_{43}([43]Q)}{\psi_{43}([43]P)} = 10 + O(43).$$

And we conclude that m is equal to 10, 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 Transactions on Information Theory*, 39:1639–1646, 1993.

[3] V. Miller. Use of elliptic curves in cryptography. In *Advances in Cryptology, CRYPTO 85*, pages 417–426. Springer Verlag, LNCS 218, 1986.

[4] A. Miyaji. Elliptic curves over $\mathbb{F}_p$ suitable for cryptosystems. In *Advances in Cryptology, AUSCRYPT 92*, pages 479–491. Springer Verlag, LNCS 718, 1993.

[5] J.H. Silverman. *The Arithmetic Of Elliptic Curves.* Springer-Verlag, GTM 106, 1986.

[6] N.P. Smart. S-integral points on elliptic curves. *Proc. Camb. Phil. Soc.*, 116:391–399, 1994.

Hewlett-Packard Laboratories,Filton Road, Stoke Gifford, Bristol BS12 6QZ, U.K.

E-mail address: `nsma@hplb.hpl.hp.com`