ELSEVIER

Information Processing Letters 80 (2001) 261–263

Information Processing Letters

www.elsevier.com/locate/ipl

A note on the x-coordinate of points on an elliptic curve in characteristic two

N.P. Smart

Computer Science Department, Woodland Road, University of Bristol, BS8 1UB, UK

Received 5 December 2000; received in revised form 5 January 2001
Communicated by R. Backhouse

Abstract

We consider how a linear condition on the bits representing an x-coordinate of a point on an elliptic curve over a field of characteristic two can lead to problems both in elliptic curve based Diffie–Hellman key agreement and the method of distinguished points for solving the elliptic curve discrete logarithm problem. Easy solutions are proposed which solve the problems in all cases. © 2001 Elsevier Science B.V. All rights reserved.

Keywords: Cryptography; Elliptic curve cryptography; Distinguished points; Finite field

1. Introduction

In this short note we consider elliptic curve key agreement based on the elliptic curve Diffie–Hellman protocol over fields of even characteristic. Elliptic curves were first proposed for use in cryptography by Koblitz [3] and Miller [4]. They are used since they offer a number of advantages over other systems such as smaller code and key size, less bandwidth and more efficient processing.

We shall start by briefly recapping on the basic definitions that we shall require: Let E denote an elliptic curve over a finite field of even characteristic, $k = \mathbb{F}_{2^q}$, where $\#E(k) = hp$, where p is a large prime, and h is a small integer (usually equal to two or four) called the cofactor. We shall assume throughout that E is given by the equation

$$Y^2 + XY = X^3 + \alpha X + \beta,$$

where $\alpha, \beta \in k$. The basic elliptic curve Diffie–Hellman key (EC-DH) agreement protocol goes as follows: First Alice and Bob publicly choose a point $P \in E(k)$ of order p, this is done at system set up time. The reason for the choice of P to have order p is to avoid small subgroup attacks. On a run of the protocol Alice chooses a random number a and sends $Q_a = [a]P$ to Bob. Bob also chooses a random number b and sends $Q_b = [b]P$ to Alice. Now Alice and Bob can compute the shared secret point

$$Q = [a]Q_b = [b]Q_a = [ab]P.$$

The shared secret is then the x-coordinate of the point Q. In this paper we show that one bit of information on $x(Q)$ is leaked and so one should always use a cryptographic hash of $x(Q)$ as the secret key.

That $x(Q)$ has one bit of redundancy is not a knew result, what is new is the realization that the exact bit leaked is very easy to determine. We also describe how this can effect the standard method of solving the elliptic curve discrete logarithm problem (ECDLP),

E-mail address: nigel@cs.bris.ac.uk, nigel@compsci.bristol.ac.uk (N.P. Smart).

0020-0190/01/$ – see front matter
PII: S0020-0190(01)00169-7

namely the method of distinguished points. It is in this context that we first noticed the phenomena explained in this note, since our code stopped working on one particular example.

We end this introduction by stating that all EC-DH protocols we are aware of make use of a cryptographic hash of $x(Q)$ and so the problem outlined in this note is purely of theoretical interest.

2. Linear conditions on $x(Q)$

The result is based on the following result of Seroussi, see [6] or [1, Chapter IV].

Theorem 1. *Let Q denote an arbitrary point of odd order on the elliptic curve above, then*

$$\mathrm{Tr}_{k/\mathbb{F}_2}\big(x(Q)\big) = \mathrm{Tr}_{k/\mathbb{F}_2}(\alpha).$$

Proof. If $P \in E(\mathbb{F}_{2^q})$ has odd order, then $P = [2]Q$ for some point $Q = (x_1, y_1) \in E(\mathbb{F}_{2^q})$. From the point doubling formula, we have $x = \lambda^2 + \lambda + \alpha$, where $\lambda = x_1 + y_1/x_1$. Thus, $\mathrm{Tr}_{k/\mathbb{F}_2}(x) = \mathrm{Tr}_{k/\mathbb{F}_2}(\alpha)$. □

Clearly if we then let $\psi_1, \ldots, \psi_q$ denote a basis of k over $\mathbb{F}_2$ and write

$$x(Q) = \sum_{i=1}^{q} x_i \psi_i, \quad x_i \in \mathbb{F}_2$$

then we obtain the linear condition,

$$\sum_{i=1}^{q} x_i \,\mathrm{Tr}_{k/\mathbb{F}_2}(\psi_i) = \mathrm{Tr}_{k/\mathbb{F}_2}\big(x(Q)\big) = \mathrm{Tr}_{k/\mathbb{F}_2}(\alpha).$$

Hence one bit of $x(Q)$ is clearly leaked. This is particularly pronounced when there is only one element $\psi_j \in \{\psi_1, \ldots, \psi_n\}$ with $\mathrm{Tr}_{k/\mathbb{F}_2}(\psi_j) = 1$, for then we obtain

$$x_j = \mathrm{Tr}_{k/\mathbb{F}_2}(\alpha).$$

A basis with only one element of trace one can always be constructed since any basis must contain at least one element of trace one, then on adding this element to all other basis elements one obtains a new basis with only one element having trace equal to one.

Many algorithms for elliptic curves over finite fields make use of the heuristic assumption that the bits of $x(Q)$ behave like a random function. One such algorithm is that for solving the ECDLP using distinguished points, see [5,7] for the general method and [2,8] for specific details with respect to certain elliptic curves. In this algorithm one aims to find λ such that

$$Q = [\lambda]P$$

by constructing elements of the form

$$T_i = [a_i]P + [b_i]Q$$

and then storing the triple (T_i, a_i, b_i) if the point T_i is "distinguished" in some sense.

The definition of distinguished is often chosen to be that the low order bits of T_i, with respect to some basis of k over $\mathbb{F}_2$ as above, are set to zero. However, we can now see that this will not in general work since one could be using a basis with $\mathrm{Tr}_{k/\mathbb{F}_2}(\psi_1) = 1$ and $\mathrm{Tr}_{k/\mathbb{F}_2}(\psi_i) = 0$ for all $i \geqslant 2$. In which case one would never obtain a distinguished point in the case that $\mathrm{Tr}_{k/\mathbb{F}_2}(\alpha) = 1$, since T_i would always have odd order. The case where $\mathrm{Tr}_{k/\mathbb{F}_2}(\alpha) = 1$ is common in real systems, since then we can always choose our curve so that the cofactor, h, is equal to two.

A simple solution to the above problem is to define a point, T_i, as distinguished only if the low order bits of

$$x(T_i) + \alpha$$

are zero. The above element will always have trace zero on any curve, which helps to nullify any linear condition on the bits in the representation of $x(T_i)$. The above mentioned problem would at worst only increase the size of the set of distinguished points by two, rather than decreasing the size of the set of distinguished points to zero. Such a performance penalty is easy to accommodate in practice.

3. Conclusion

We have explained how a linear condition on the bits in the x-coordinates of points of odd order on an elliptic curve over a field of even characteristic can cause problems in naive implementations of EC-DH and the method of distinguished points for the ECDLP. We have also explained simple solutions to the above problems which can be implemented at almost no extra cost.

References

[1] I.F. Blake, G. Seroussi, N.P. Smart, Elliptic Curves in Cryptography, Cambridge University Press, Cambridge, 1999.
[2] R. Gallant, R. Lambert, S. Vanstone, Improving the parallelised Pollard lambda search on binary anomalous curves, Math. Comp., to appear.
[3] N. Koblitz, Elliptic curve cryptosystems, Math. Comp. 48 (1987) 203–209.
[4] V. Miller, Use of elliptic curves in cryptography, in: Advances in Cryptology, CRYPTO'85, Lecture Notes in Comput. Sci., Vol. 218, Springer, Berlin, 1986, pp. 47–426.
[5] J.M. Pollard, Monte Carlo methods for index computation (mod p), Math. Comp. 32 (1978) 918–924.
[6] G. Seroussi, Compact representation of elliptic curve points over $\mathbb{F}_{2^n}$, Hewlett-Packard Laboratories Technical Report No. HPL-98-94R1, September 1998.
[7] P.C. van Oorschot, M.J. Wiener, Parallel collision search with cryptanalytic applications, J. Cryptology 12 (1999) 1–28.
[8] M.J. Wiener, R. Zuccherato, Faster attacks on elliptic curve cryptosystems, in: Selected Areas in Cryptography, Lecture Notes in Comput. Sci., Vol. 1556, Springer, Berlin, 1999, pp. 190–200.