CM–CURVES WITH GOOD CRYPTOGRAPHIC PROPERTIES

Neal Koblitz
Dept. of Mathematics GN-50
University of Washington
Seattle, WA 98195, U.S.A.
koblitz@math.washington.edu

Abstract

Our purpose is to describe elliptic curves with complex multiplication which in characteristic 2 have the following useful properties for constructing Diffie–Hellman type cryptosystems: (1) they are nonsupersingular (so that one cannot use the Menezes–Okamoto–Vanstone reduction of discrete log from elliptic curves to finite fields); (2) the order of the group has a large prime factor (so that discrete logs cannot be computed by giant-step/baby-step or the Pollard rho method); (3) doubling of points can be carried out almost as efficiently as in the case of the supersingular curves used by Vanstone; (4) the curves are easy to find.

1 Introduction

In Atkin's version of the Goldwasser–Kilian primality test ([1], [9]) one starts with a quadratic imaginary field $K = \mathbf{Q}(\sqrt{-D})$ and then constructs an elliptic curve over a finite field which is the reduction of an elliptic curve with complex multiplication by K. This idea can also be applied to the search for elliptic curves which are suitable for the type of cryptosystem described in [3], [8]. As in the primality test, we are looking for elliptic curves whose number of points is equal to a large prime number times a small factor. However, unlike in the primality test, where the curves are defined over very large prime fields, our curves will be defined over small fields. Moreover, we shall be interested in an additional property of the curves, the property of having a small trace of Frobenius. In particular, we shall study curves over small fields of characteristic 2 for which the trace of the Frobenius map is ± 1, i.e., for which the complex multiplication field is $\mathbf{Q}(\sqrt{-D})$ for $D = 2^{k+2} - 1$ a Mersenne number. Such curves lend themselves to particularly efficient computation, since the doubling of points (more precisely, multiplying points by 2^k) can be speeded up when this condition holds.

J. Feigenbaum (Ed.): Advances in Cryptology - CRYPTO '91, LNCS 576, pp. 279-287, 1992.

2 Anomalous curves

An elliptic curve E defined over the field $\mathbf{F}_q$ of q elements will be called "anomalous" if the trace of the Frobenius map (the map $(x, y) \mapsto (x^q, y^q)$) is equal to 1. Equivalently, an "anomalous" curve over $\mathbf{F}_q$ is one for which the number of $\mathbf{F}_q$-points is equal to q.[1] On an anomalous elliptic curve E over $\mathbf{F}_q$, the Frobenius map φ satisfies the characteristic equation $T^2 - T + q = 0$.

We shall also be interested in the "twist" $\widetilde{E}$ of E, whose Frobenius satisfies $T^2+T+q = 0$ (the number of $\mathbf{F}_q$-points on $\widetilde{E}$ is $q+2$). By the "n-twist" $\widetilde{E}_n$ of E we mean the twist of the curve E regarded as a curve over the extension field $\mathbf{F}_{q^n}$ (thus, $\widetilde{E}_1 = \widetilde{E}$). If q is odd and E has equation $y^2 = x^3 + bx + c$, then $\widetilde{E}_n$ has equation $\beta y^2 = x^3 + bx + c$, where $\beta \in \mathbf{F}_{q^n}$ is a nonsquare; if q is even, then the equations are a little different, as we shall see in the examples below. If $n = 2^r n_0$ with n_0 odd, then $\widetilde{E}_n$ can be defined over the smaller field extension $\mathbf{F}_{q^{2^r}}$, and its Frobenius map $(x, y) \mapsto (x^{q^{2^r}}, y^{q^{2^r}})$ satisfies the equation $T^2 + aT + q^{2^r} = 0$, where a is the trace of the complex number $\left((1 + \sqrt{1-4q})/2\right)^{2^r}$.

The most important case for practical implementation is $q = 2^k$. In that case, the computation of $\varphi : (x, y) \mapsto (x^{2^k}, y^{2^k})$ on an $\mathbf{F}_{2^{kn}}$-point is accomplished by a shift operation of negligible time. Thus, if we want to multiply a point P by 2^k on an anomalous curve, the fastest way to do this is to use the identity $\varphi^2 - \varphi + 2^k = 0$, i.e., $2^k P = \varphi(P) - \varphi^2(P)$, since instead of k additions of points we need only perform one. (On the twisted curve $\widetilde{E}$, one analogously has $2^k P = -\varphi(P) - \varphi^2(P)$.)

The greater efficiency obtained if one can double points by taking squares in $\mathbf{F}_{2^n}$ was first realized by Menezes and Vanstone [6], who were working with curves defined over $\mathbf{F}_2$ whose Frobenius map has trace 0, i.e., satisfies the relation $T^2 + 2 = 0$. In that case, since $2P = -\varphi^2(P)$, no addition of points is required, i.e., doubling of points is "free." However, curves with 0 trace of Frobenius are supersingular. In [7] it was shown that the discrete log problem on a supersingular elliptic curve reduces to the discrete log problem in the multiplicative group of a finite field of about the same size. That is, supersingular elliptic curve cryptosystems are now known to be no more secure than the original Diffie–Hellman cryptosystem in a small extension of the underlying finite field. For this reason we shall keep away from curves whose Frobenius map φ has trace 0. The anomalous curves — those for which φ has trace 1 — are the "next best thing."

In general, for given q the equation of an anomalous elliptic curve over $\mathbf{F}_q$ can be found

[1] The term "anomalous" was introduced by Barry Mazur in a different context: given an elliptic curve E over a number field, he calls a prime "anomalous" for E if the Frobenius of E at that prime has trace 1.

by finding $\mathbf{F}_q$-roots of the modular equation corresponding to the complex multiplication field $\mathbf{Q}(\sqrt{1-4q})$, as explained in [4]. However, in our examples we shall be concerned only with small q, for which an equation for E can be found quickly by trial and error.

Theorem. *Let E be an anomalous elliptic curve defined over $\mathbf{F}_q$, and let $\widetilde{E}$ be its twist.*

(a) *If P is an $\mathbf{F}_{q^n}$-point on E (or $\widetilde{E}$), then the multiple qP can be computed with a single addition of points (together with shift operations for the computation of $x \mapsto x^q$ in a normal basis of $\mathbf{F}_{q^n}$).*

(b) *In the special case $q = 2$, any of the multiples $2^l P$ for $l \leq 4$ can be computed with a single addition of points.*

Proof. Part (a) follows from the above discussion.

(b) In the case $q = 2$, at first it might seem that an anomalous curve has no advantage, because computing $2P = P + P$ takes only one addition of points anyway. However, if we use the relation $T - T^2 = 2$ satisfied by φ, iterate and simplify, we obtain the following polynomial identities satisfied by the map φ (which is defined on the $\mathbf{F}_{2^n}$-points of E by $P_{(x,y)} \mapsto P_{(x^2,y^2)}$):

$$4 = 2T - 2T^2 = (T - T^2)T - 2T^2 = -T^3 - T^2$$

$$8 = 4 \cdot 2 = (-T^3 - T^2)(T - T^2) = -T^3 + T^5$$

$$16 = 4^2 = T^6 + 2T^5 + T^4 = T^6 + (T - T^2)T^5 + T^4 = -T^7 + 2T^6 + T^4 =$$

$$= -T^7 + (T - T^2)T^6 + T^4 = T^4 - T^8.$$

(The analogous formulas on the twist $\widetilde{E}$ are obtained from these by replacing T by $-T$.) Thus, in computing kP, any string of $l \leq 4$ zeros can be handled with a single addition of points, as claimed.

Roughly speaking, if one uses k's of small Hamming size, one gets doubling of points "almost 3/4 for free." If E has equation $y^2 + xy = f_3(x)$ for $f_3(x) \in \mathbf{F}_2[x]$ of degree 3 (an explicit equation will be given below), and if $P = P_{(x,y)}$ is an $\mathbf{F}_{2^n}$-point, then the above binomials in T lead to simple formulas for $2^l P$, $l \leq 4$, for example: $8\,P_{(x,y)} = P_{(x^8, x^8+y^8)} + P_{(x^{32},y^{32})}$.

Alternately, as Victor Miller pointed out to me, for k arbitrary it is efficient to write

k to the base 16 and precompute $k_0 P$ for $1 \leq k_0 < 16$. Then if one uses the last formula above to compute $16^j P$, it is easy to see that on the average the number of additions of points is less than $1/3$ of the expected number of additions of points required with the repeated doubling method based on the binary expansion of k.

3 Number of points

Let E be an anomalous curve over $\mathbf{F}_q$, and let $\widetilde{E}_n$ be its n-twist. Then there is a simple relationship between the number N_n (resp. $\widetilde{N}_n$) of $\mathbf{F}_{q^n}$-points on E (resp. on $\widetilde{E}_n$) and the root $\alpha = (1 + \sqrt{1-4q})/2$ of the characteristic polynomial $T^2 - T + q$. Namely, $N_n = |\alpha^n - 1|^2$, $\widetilde{N}_n = |\alpha^n + 1|^2$. This leads to a very simple algorithm for computing N_n and $\widetilde{N}_n$: first compute the Fibonacci-type sequence a_n given by $a_0 = 2$, $a_1 = 1$, $a_{n+1} = a_n - q\,a_{n-1}$ for $n \geq 1$; then $N_n = q^n + 1 - a_n$ and $\widetilde{N}_n = q^n + 1 + a_n$.

Once we have an anomalous curve E defined over $\mathbf{F}_q$, we want to find an extension field $\mathbf{F}_{q^n}$ such that the number N_n of $\mathbf{F}_{q^n}$-points on E or the number $\widetilde{N}_n$ of $\mathbf{F}_{q^n}$-points on $\widetilde{E}_n$ is divisible by a large prime (say, of at least 30 digits). Because $N_n = |\alpha^n - 1|^2$ and $\widetilde{N}_n = |\alpha^n + 1|^2$, it follows that $N_{n_1} | N_n$ whenever $n_1 | n$ and $\widetilde{N}_{n_1} | \widetilde{N}_n$ whenever n/n_1 is an odd integer. So if N_n (resp. $\widetilde{N}_n$) is to be a product of a small factor and a large prime, we must take n equal to a prime (resp. equal either to a prime or else to a prime times a very small power of 2).

4 Examples defined over $\mathbf{F}_2$

Here we consider the anomalous curve $E:\ y^2 + xy = x^3 + x^2 + 1$ over $\mathbf{F}_2$ and its twist $\widetilde{E}:\ y^2 + xy = x^3 + 1$, which have complex multiplication by $\mathbf{Q}(\sqrt{-7})$. For certain prime n one has $N_n = 2\cdot$prime (or $\widetilde{N}_n = 4\cdot$prime). Here is a table of all values of $N_n/2$ and $\widetilde{N}_n/4$ for $n < 200$ which are prime (actually, probable prime, since I verified primality using *Mathematica*) and which are of at least 30 digits:

$N_{101}/2 = 1\ 26765\ 06002\ 28230\ 88614\ 28085\ 08011$

$N_{107}/2 = 81\ 12963\ 84146\ 06692\ 18285\ 10322\ 12511$

$N_{109}/2 = 324\ 51855\ 36584\ 26701\ 48744\ 86564\ 61467$

$N_{113}/2 = 5192\ 29685\ 85348\ 27627\ 89670\ 38334\ 67507$

$N_{163}/2 = 5846\ 00654\ 93236\ 11672\ 81474\ 17535\ 98448\ 34832\ 91185\ 74063$

$\widetilde{N}_{103}/4 = 2\ 53530\ 12004\ 56459\ 53586\ 25300\ 67069$

$\widetilde{N}_{107}/4 = 40\ 56481\ 92073\ 03335\ 60436\ 34890\ 37809$

$\widetilde{N}_{131}/4 = 6805\ 64733\ 84187\ 69269\ 32320\ 12949\ 34099\ 85129$

Thus, for example, the number of points on the curve $y^2 + xy = x^3 + 1$ over $\mathbf{F}_{2^{131}}$ (a field which according to the table in [11] has an optimal normal basis) is divisible by a 39-digit probable prime. (The field $\mathbf{F}_{2^{113}}$ also has an optimal normal basis.)

5 Examples defined over $\mathbf{F}_4$, $\mathbf{F}_8$ and $\mathbf{F}_{16}$

I. We consider the curve $E: y^2 + xy = x^3 + \gamma$, where $\gamma \in \mathbf{F}_4$ satisfies $\gamma^2 = \gamma + 1$, and its twist $\widetilde{E}: y^2 + xy = x^3 + \gamma x^2 + \gamma$. The curves E and $\widetilde{E}$ have complex multiplication by $\mathbf{Q}(\sqrt{-15})$. For certain prime n one has $N_n = 4$·prime or $\widetilde{N}_n = 6$·prime. Here is a table of all probable prime values of at least 30 digits of $N_n/4$ and $\widetilde{N}_n/6$ for $n < 100$:

$N_{67}/4 = 54445\ 17870\ 73501\ 54153\ 44659\ 58609\ 44105\ 99059$

$N_{79}/4 = 91\ 34385\ 23331\ 81432\ 38773\ 05730\ 45979\ 44745\ 23653\ 03319$

$\widetilde{N}_{59}/6 = 55384\ 49982\ 43714\ 94566\ 50574\ 99908\ 87769$

Note that the fields $\mathbf{F}_{4^{67}}$ and $\mathbf{F}_{4^{79}}$ have optimal normal bases [11].

II. We consider the curve $E: y^2 + xy = x^3 + \gamma$, where $\gamma \in \mathbf{F}_8$ satisfies $\gamma^3 = \gamma + 1$, and its twist $\widetilde{E}: y^2 + xy = x^3 + x^2 + \gamma$. The curves E and $\widetilde{E}$ have complex multiplication by $\mathbf{Q}(\sqrt{-31})$. For certain prime n one has $N_n = 8$·prime or $\widetilde{N}_n = 10$·prime. Here is a table of all probable prime values of at least 30 digits of $N_n/8$ and $\widetilde{N}/10$ for $n < 66$:

$N_{37}/8 = 324\ 51855\ 36584\ 26723\ 11495\ 75723\ 35741$

$\widetilde{N}_{47}/10 = 27\ 87593\ 14981\ 63278\ 92689\ 03181\ 39617\ 36218\ 74561$

$\widetilde{N}_{59}/10 = 191\ 56194\ 26082\ 36107\ 29479\ 33791\ 57473\ 18375\ 04813\ 70807\ 01777$

III. Finally, we return to the curve $E: y^2 + xy = x^3 + x^2 + 1$ in §4, and consider its 4-twist $\widetilde{E}_4: y^2 + xy = x^3 + \gamma x^2 + 1$, where $\gamma \in \mathbf{F}_{16}$ is an element with absolute trace 1. Since the 4-th power of $\alpha = (1+\sqrt{-7})/2$ is $(1-3\sqrt{-7})/2$, it follows that E regarded over $\mathbf{F}_{16}$ is also anomalous. (The fact that the same curve is anomalous over both $\mathbf{F}_2$ and $\mathbf{F}_{16}$ is to be expected, because the complex multiplication fields $\mathbf{Q}(\sqrt{1-2^{k+2}})$ are the same when $k=1$ and $k=4$, since $\sqrt{-63} = 3\sqrt{-7}$.) For certain n equal to 4 times a prime, one has $\widetilde{N}_n = \widetilde{N}_4 \cdot \text{prime} = 18 \cdot \text{prime}$. There is one case for $n < 200$ when $\widetilde{N}_n/18$ is a prime of more than 30 digits:

$$\widetilde{N}_{148}/18 = 1982\ 28846\ 20916\ 10945\ 91407\ 67798\ 27981\ 11637\ 92081$$

The field $F_{2^{148}}$ happens to have an optimal normal basis [11].

In summary, the above elliptic curves all give rise to Diffie–Hellman type cryptosystems which are secure at our present level of knowledge and technology. The examples in §4 have the additional feature that, when computing a multiple kP, any string of ≤ 4 zeros in the binary representation of k can be handled with only a single addition of points. In the case of the examples in §5.I (respectively, §5.II, §5.III) a string of 2 (resp. 3, 4) zeros in k can be handled with a single addition of points.

6 Some aspects of efficient implementation

Balanced binary expansion. As noted in [10], one can take advantage of the fact that subtracting points on an elliptic curve is as easy as adding. For example, instead of computing $15P$ as $P+2(P+2(P+2P))$, it is more efficient to compute $2(2(2(2P)))-P$. This is different from exponentiation in a finite field, where it would take longer to compute $\left(\left(\left(a^2\right)^2\right)^2\right)^2/a$ than $a\left(a\left(a\cdot a^2\right)^2\right)^2$, because division takes much longer than multiplication.

Suppose you want to compute kP. The following algorithm, which is equivalent to the second algorithm in [10], will give k as a sum of a minimal number of powers of 2 with coefficients ± 1: move from right to left in the binary expansion of k, replacing each sequence of two or more 1-bits $11\cdots11$ by $100\cdots0\text{-}1$. We shall call the result the "balanced binary expansion" of k. For example, for $k = 3895$ we move from the binary

to the balanced binary expansion as follows:

$$\begin{array}{cccccccccccc} 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & -1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & -1 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 & -1 & 0 & 1 & 0 & 0 & -1 & 0 & 0 & -1 \end{array}$$

The balanced binary expansion of an arbitrary k is likely to have more sequences of several 0's than its binary expansion. In fact, it is simple to show that on the average $2/3$ of a number's balanced binary digits are 0. Thus, when we are computing on the anomalous curves in §4, the easy step of converting k to balanced binary will generally enable us to compute kP faster, because of the circumstance that any string of ≤ 4 zeros can be handled with a single addition of points. For example, to compute $15P = 16P - P$ requires only 2 additions of points.

In a Diffie–Hellman type key exchange, where one multiplies points by randomly generated r-bit integers k, one could limit oneself to k of Hamming size $\leq s$, where $s \ll r$. If the binary expansion is used, there are $\sum_{j \leq s} \binom{r}{j}$ such k; whereas if we use the balanced binary expansion, then there are almost $\sum_{j \leq s} 2^j \binom{r}{j}$ different k of Hamming size $\leq s$. (We say "almost" because not all sequences of digits can occur; but most do occur when $s \ll r$.)

The following is an even more efficient key exchange procedure. It is based on a suggestion of Hendrik Lenstra.

Base-φ expansion. Again suppose that we are working in the group of $\mathbf{F}_{2^n}$-points of the anomalous $\mathbf{F}_2$-curve $E: y^2 + xy = x^3 + x + 1$ or its twist $\widetilde{E}: y^2 + xy = x^3 + 1$. Then on E the Frobenius map $\varphi: (x, y) \mapsto (x^2, y^2)$ is the element $\pi = (1 + \sqrt{-7})/2$ of the endomorphism ring $\mathbf{Z}\left[(-1 + \sqrt{-7})/2\right]$ (on $\widetilde{E}$ it is $\pi = (-1 + \sqrt{-7})/2$). In the key exchange protocol, instead of choosing a random r-bit positive integer n whose balanced binary expansion has Hamming size $\leq s$, each player now chooses a linear combination n of the φ^j, $0 \leq j < r$, with coefficients $c_j = 0$ or ± 1, such that $\leq s$ of the coefficients are nonzero. Then computing $nP = \sum c_j \varphi^j(P)$ requires only $\leq s - 1$ additions of points, and we have recaptured the efficiency of working with supersingular curves.

One could also compute arbitrary multiples nP, where now $n \in \mathbf{Z}$, by representing n "to the base φ." Namely, since $\varphi = (\pm 1 + \sqrt{-7})/2$ is an element of norm 2 in the Euclidean domain $\mathbf{Z}\left[(1 + \sqrt{-7})/2\right]$, any element of the ring — in particular, n — has a unique representation in the form $\sum \epsilon_j \varphi^j$, where $\epsilon_j \in \{0, 1\}$.

We can also obtain a "balanced φ-expansion" of n as follows. Recall that φ satisfies $\varphi(1 - \varphi) = 2$ on E (it satisfies $-\varphi(1 + \varphi) = 2$ on $\widetilde{E}$). We shall work on E (the argument for

$\widetilde{E}$ is analogous with the φ-expansion replaced by the $(-\varphi)$-expansion). Write $n = n_0 + 2n_1 + 2n_2$, where $n_0 \in \{0, 1\}$ and n_2 is the part of the φ-expansion of $(n - n_0)/2$ consisting of all runs of ≥ 2 consecutive 1-bits. Note that $2(1 + \varphi + \varphi^2 + \cdots + \varphi^{j-1}) = \varphi - \varphi^{j+1}$. Hence we replace each sequence of $j \geq 2$ consecutive 1-bits $11 \cdots 11$ in the expansion of n_2 by $-1\,000 \cdots 10$ in the expansion of $2n_2$.

But unfortunately, expressing an arbitrary n as a balanced φ-expansion will not necessarily be more efficient than using its balanced binary expansion. This is because the φ-expansion of n has approximately twice as many bits as the binary expansion. The following example illustrates why the base φ does not generally have an advantage over the base 2.

Example. Consider the group of $\mathbf{F}_8$-points of $E: y^2 + xy = x^3 + x^2 + 1$, which has order 14. Suppose we want to compute $10P$. Using the binary expansion, we take $2(P + 4P)$, which requires 3 additions. Since the base-φ expansion of 5 is 100101, computing $10P = (\varphi^5 + \varphi^2 + 1)2P$ also requires 3 additions. Note that if we happen to know that φ acts as -3 on the $\mathbf{F}_8$-points of E, and so $10 = \varphi^2 + 1$, then we can compute $10P$ with a single addition of points. However, in the general case of $\mathbf{F}_{2^n}$-points it is not clear how to obtain a φ-expansion of n that is much shorter than the one that comes from the Euclidean algorithm in the ring $\mathbf{Z}[(1 + \sqrt{-7})/2]$.

Acknowledgments. I would like to thank Hendrik Lenstra, Andrew Odlyzko, and Scott Vanstone for helpful conversations.

References

[1] S. Goldwasser, J. Kilian, Almost all primes can be quickly certified, *Proceedings of the 18th ACM Symp. Theory of Computing* (1986), 316-329.

[2] N. Koblitz, *A Course in Number Theory and Cryptography*, Springer-Verlag, 1987.

[3] N. Koblitz, Elliptic curve cryptosystems, *Math. of Computation*, **48** (1987), 203-209.

[4] A. K. Lenstra and H. W. Lenstra, Jr., Algorithms in number theory, in: *Handbook of Theoretical Computer Science*, Vol. A, *Algorithms and Complexity*, ed. by j. van Leeuwen, Amsterdam: Elsevier (1990), 673-715.

[5] A. Menezes and S. A. Vanstone, Isomorphism classes of elliptic curves over finite fields of characteristic 2, *Utilitas Mathematica*, **38** (1990), 135-154.

[6] A. Menezes and S. A. Vanstone, Elliptic curve cryptosystems and their implementation, to appear in *J. Cryptology*.

[7] A. Menezes, T. Okamoto, and S. A. Vanstone, Reducing elliptic curve logarithms to logarithms in a finite field, *Proceedings of the 23rd ACM Symp. Theory of Computing*, 1991.

[8] V. Miller, Use of elliptic curves in cryptography, *Advanced in Cryptology - Crypto '85*, Springer-Verlag, 1986, 417-426.

[9] F. Morain, Implementation of the Goldwasser–Kilian–Atkin primality testing algorithm, preprint.

[10] F. Morain and J. Olivos, Speeding up the computations on an elliptic curve using addition-subtraction chains, *R.A.I.R.O. Technical Informatics and Applications*, **24** (1990), 531-543.

[11] R. C. Mullin, I. M. Onyszchuk, S. A. Vanstone, and R. M. Wilson, Optimal normal bases in GF(p^n), *Discrete Appl. Math.*, **22** (1988/89), 149-161.