Constructing Elliptic Curve Cryptosystems in Characteristic 2

Neal Koblitz

Dept. of Mathematics, Univ. of Washington, Seattle WA 98195

1. Introduction

Since the group of an elliptic curve defined over a finite field $\mathbf{F}_q$ was proposed for Diffie–Hellman type cryptosystems in [7] and [15], some work on implementation has been done using special types of elliptic curves for which the order of the group is trivial to compute ([2], [13]). A consideration which discourages the use of an arbitrary elliptic curve is that one needs Schoof's algorithm [16] to count the order of the corresponding group, and this algorithm, in addition to being rather complicated, has running time $O(\log^9 q)$ for an elliptic curve defined over $\mathbf{F}_q$. Thus, in applications of elliptic curves where one needs extremely large q — for example, the original version of the elliptic curve primality test ([4], [11]) — this algorithm is too time-consuming.

However, elliptic curve cryptosystems seem to be secure at present provided only that the order of the group has a prime factor of about 40 digits, and in this range Schoof's algorithm is feasible. The purpose of this paper is to describe how one can search for suitable elliptic curves with random coefficients using Schoof's algorithm. We treat the important special case of characteristic 2, where one has certain simplifications in some of the algorithms.

Acknowledgments. I wish to thank Scott Vanstone, Gordon Agnew, Alfred Menezes, and Joe Buhler for valuable discussions.

2. Motivation for constructing elliptic curve cryptosystems with variable coefficients

At present no subexponential algorithm is known for the discrete logarithm

A.J. Menezes and S.A. Vanstone (Eds.): Advances in Cryptology - CRYPTO '90, LNCS 537, pp. 156-167, 1991.

problem on a general elliptic curve: the "baby step – giant step" algorithm (which applies in any group) requires time fully exponential in the length of the largest prime factor of the order of the group. In other words, suppose that we have a nonsupersingular elliptic curve E defined over a finite field whose order $|E|$ is divisible, say, by a 40-digit prime l; you give me a point P on E (whose order is divisible by l); and I multiply P by a secret integer k and give you the result $Q = kP$. Then, with our present level of theoretical knowledge and technology, you will be unable to find k from Q. This is because no algorithm faster than the baby step – giant step algorithm is known for such an elliptic curve.

This situation is in stark contrast with that of the classical discrete logarithm problem in the multiplicative group of a finite field. There, "index calculus" type subexponential probabilistic algorithms have been known for some time, and work by D. Coppersmith (in small characteristic) and D. Gordon (over a prime field, using the number field sieve) make it reasonable to expect that the time to solve the discrete log in $\mathbf{F}_q^\times$ is bounded by $L_q[1/3, c] = \exp\Big((c+o(1))\big((\log q)^{1/3}(\log\log q)^{2/3}\big)\Big)$ for a fairly small constant c.

For this reason, it seems that discrete log cryptosystems based on the group of an elliptic curve are secure over much smaller fields than those based on the multiplicative group of the field, We also note that there is much more choice available when working with elliptic curves: for fixed q one has only one group $\mathbf{F}_q^\times$, but one obtains many groups E by varying the coefficients of the defining equation of the elliptic curve.

Recently, S. A. Vanstone's group at the University of Waterloo implemented a cryptosystem using the elliptic curve $y^2 + y = x^3$ over $\mathbf{F}_q$ with $q = 2^{593}$ [13]. This elliptic curve has very special properties — complex multiplication by cube roots of unity, and supersingularity — and this means that for $q \equiv 2 \pmod 3$ one has the simple formula $|E| = q + 1$. In the present paper we discuss using a variable elliptic curve, i.e., taking advantage of the availability of many different E over a fixed field $\mathbf{F}_q$, $q = 2^n$.

From a practical point of view, there are both pros and cons in using random elliptic curves over $\mathbf{F}_{2^n}$ rather than the special one in [13]. On the positive side, we obtain the added security of being able to change the curve periodically. Moreover, in order to break the cipher one would need an algorithm for solving the discrete log problem on an arbitrary elliptic curve, rather than just on a particular elliptic curve with special structure (complex multiplication by cube roots of unity and supersingularity). Very recently, this advantage has become especially significant because of [14], in which Menezes, Okamoto and Vanstone obtained a reduction of the discrete logarithm on an elliptic curve to the discrete logarithm in a finite field, a reduction which leads to a subexponential algorithm for the discrete log on a supersingular elliptic curve but not on a nonsupersingular curve (which is the general case).

(It should be noted, however, that to avoid the Menezes–Okamoto–Vanstone reduction one does not have to use random curves and Schoof's algorithm. There are families of nonsupersingular curves whose orders are easy to compute, for example: (1) the curve $y^2+xy = x^3+x^2+1$ over $\mathbf{F}_{2^n}$ for variable n has $|E| = \left|\left(\frac{1+\sqrt{-7}}{2}\right)^n - 1\right|^2$; (2) the curve $y^2+y = x^3$ over $\mathbf{F}_p$ for variable $p \equiv 1 \pmod 3$ has $|E| = p+1+a$, where a is given by $a^2+3b^2 = 4p$ with integers $a \equiv 1 \pmod 3$ and $b \equiv 0 \pmod 3$).)

On the negative side, when using a random curve, in addition to the burden of having to apply Schoof's algorithm to find a case when the number of points is divisible by a ≥ 40-digit prime, the actual computations on a random curve are somewhat slower than on the special curve $y^2+y = x^3$ used in [13]. Suppose we want to compute the multiple of a point by an integer that contains $n+1$ bits, of which $m+1$ bits are 1. In the case of the curve $y^2+y = x^3$, this computation takes only $9m$ multiplications in the field. But in the case of the curve $y^2+xy = x^3+a_2x^2+a_6$ (see §3 below for details on the notation), we need $16m+4n$ multiplications. A second annoyance is that in the general case one always has to carry along both the x- and y-coordinates of points, whereas in the case of the special curve one can simply keep track of one bit of y, and at any time reconstruct y from that bit and the corresponding x, without performing any multiplications (see [13]).

An implementation of a random–curve cryptosystem might work as follows. A special–purpose chip is set up which does arithmetic in a fixed large extension of $\mathbf{F}_2$ and which can compute on an elliptic curve over the field once the coefficients are given to it. Once a week, a computer generates a new random coefficient a_6 such that the order of either the curve $y^2+xy = x^3+a_6$ or the "twisted" curve $y^2+xy = x^3+a_2x^2+a_6$, where a_2 is any element of the field having trace 1 ($a_2 = 1$ will do if the field has odd degree over $\mathbf{F}_2$), is divisible by a large prime. This involves finding the t from Schoof's algorithm (see §4 below) for the first curve — then the first curve has 2^n+1-t points and the twisted curve has 2^n+1+t points — and verifying (perhaps by the elliptic curve factorization algorithm) that one of these two numbers does not factor completely into primes of fewer than 40 digits. Then for the week that follows the coefficient pair (a_2, a_6) becomes part of everyone's public key, i.e., it is read into each of the special–purpose chips that are programmed to perform key exchanges, signatures, message transmission, etc., using computations on a given elliptic curve.

3. Elliptic curves in characteristic 2

An elliptic curve E over an arbitrary field K can be defined as the set of solutions of an equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1}$$

(where $a_i \in K$ and the curve has no singularities), together with the "point at infinity O," which is the identity element of the abelian group E. Here the subscripts of the coefficients indicate their "weights" when they are regarded as indeterminates; the weights are chosen so that the equation (1) is homogeneous if x and y are given weights 2 and 3, respectively.

If char $K \neq 2$, one can use a linear change of variables to reduce the equation to a form in which $a_1 = a_3 = 0$. However, we shall be interested in the case char $K = 2$. In that case it is easy to see that E has a nontrivial point of order 2 (i.e., $|E|$ is even) if and only if $a_1 \neq 0$: in fact, the point with x-coordinate $x = a_3/a_1$ is the point of order 2. Such a curve is called "nonsupersingular" (equivalently, its j-invariant is nonzero). In that case, using a linear change of variables, without loss of generality we may assume that the equation of E is in the form

$$y^2 + xy = x^3 + a_2x^2 + a_6. \tag{2a}$$

The other possibility is that E is "supersingular," i.e., any of the following equivalent conditions holds: (i) $a_1 = 0$, (ii) $|E|$ is odd, (iii) the j-invariant of E is zero. In this case, using a linear change of variables, without loss of generality we may suppose that the equation of E is in the form

$$y^2 + a_3y = x^3 + a_4x + a_6. \tag{2b}$$

In characteristic 2, the addition law $P_{x_3,y_3} = P_{x_1,y_1} \oplus P_{x_2,y_2}$ is given by the following rules in the nonsupersingular case (equation (2a)) and the supersingular case (equation (2b)), respectively: (1) the additive inverse of $P_{x,y}$ is $-P_{x,y} = P_{x,y+x}$ (respectively, $-P_{x,y} = P_{x,y+a_3}$); (2) if $P_{x_1,y_1} \neq \pm P_{x_2,y_2}$, then

$$\begin{aligned} x_3 &= x_1 + x_2 + a_2 + (y_1 + y_2)/(x_1 + x_2) + (y_1^2 + y_2^2)/(x_1^2 + x_2^2), \\ y_3 &= y_1 + x_3 + (x_1 + x_3)(y_1 + y_2)/(x_1 + x_2); \end{aligned} \tag{3a}$$

(respectively,

$$x_3 = x_1 + x_2 + (y_1^2 + y_2^2)/(x_1^2 + x_2^2),$$
$$y_3 = y_1 + a_3 + (x_1 + x_3)(y_1 + y_2)/(x_1 + x_2);\,) \tag{3b}$$

and (3) if $P_{x_1,y_1} = P_{x_2,y_2}$, then

$$x_3 = (x_1^4 + a_6)/x_1^2, \qquad y_3 = y_1 + x_3 + (x_1^2 + y)(x_1 + x_3)/x_1; \tag{4a}$$

(respectively,

$$x_3 = (x_1^4 + a_4^2)/a_3^2, \qquad y_3 = y_1 + a_3 + (x_1^2 + a_4)(x_1 + x_3)/a_3.) \tag{4b}$$

4. Schoof's algorithm

A detailed description of the algorithm is in [16]. Here we shall give only an outline. By Hasse's theorem, the number of points on an elliptic curve E over the field of $q = 2^n$ elements is of the form $N = q + 1 - t$, where $|t| \leq 2\sqrt{q}$. Schoof's algorithm determines N modulo l for a bunch of small primes l. If we run through enough l so that $\prod l > 4\sqrt{q}$, then N can be uniquely determined by the Chinese Remainder Theorem.

For $l > 2$ one determines N modulo l by looking at the points of order l with coordinates in field extensions of $\mathbf{F}_q$. It turns out that N modulo l is determined by the action of the map $(x, y) \mapsto (x^q, y^q)$ on the set of points of order l. For example, suppose that the map $(x, y) \mapsto (x^q, y^q)$ leaves some such point fixed. Then this means that there is a point of order l whose coordinates are in $\mathbf{F}_q$, i.e., our original group of points with $\mathbf{F}_q$ coordinates has a nontrivial element of order l. In that case $N \equiv 0 \pmod{l}$. More generally, the value of N modulo l is determined by how the q-th power map permutes the points of order l.

Thus, a basic role in Schoof's algorithm is played by the so-called "division polynomials," which characterize the points P (with coordinates in extensions of $\mathbf{F}_q$) for which lP is the identity.

5. Division polynomials in characteristic 2

Before specializing to characteristic 2, we recall that in the general case of an elliptic curve given by (1), the division polynomial $f_n \in \mathbf{Z}[x, y, a_1, a_2, a_3, a_4, a_6]$ is a nonzero homogeneous polynomial of total weight $n^2 - 1$ (recall that x has weight 2, y has weight 3, a_i has weight i) such that for a nonzero point $P_{x,y}$ on the elliptic curve one has $nP_{x,y} = O$ ("$P_{x,y}$ is a point of order n") if and only if $f_n(x,y) = 0$ (where for fixed $a_i \in K$ we consider f_n as a polynomial in $K[x,y]$). These polynomials satisfy the following fundamental relations:

Proposition 1. *For $m > n \geq 2$*

$$f_{m+1}f_{m-1}f_n^2 - f_{n+1}f_{n-1}f_m^2 = f_{m+n}f_{m-n}. \tag{5$_{m,n}$}$$

For the proof, see [10].

Proposition 2. *For $n \geq 1$,*

$$f_{2n} = (f_2 \circ n)f_n^4, \tag{6}$$

where $f_2 \circ n$ denotes the function f_2 applied to the x- and y-coordinates of $nP_{x,y}$.

The **proof** follows the same method as the proof of $(5)_{m,n}$ in [10]. That is, (6) will hold as a formal identity in $\mathbf{Z}[x,y,a_1,a_2,a_3,a_4,a_6]$ — and hence will hold over any field and with any stipulated values of the a_i — provided that it holds over the complex numbers. To prove (6) as an identity over $\mathbf{C}$, one observes that f_{2n} has a simple zero at all non-lattice points of order $2n$ and a pole of order $4n^2 - 1$ at the lattice points; f_n^4 has a zero of order 4 at all non-lattice points of order n and a pole of order $4n^2 - 4$ at the lattice points; and $f_2 \circ n$ has a simple zero at all points of order $2n$ which are not of order n and a triple pole at all points of order n. Thus, both sides of (6) have the same zeros and poles, and so are equal up to a constant factor, which is easily checked to be 1. This completes the proof.

In the case when $\operatorname{char} K = 2$ and E has the equation (2a), the first few f_n are:

$$f_1 = 1, \qquad f_2 = x, \qquad f_3 = x^4 + x^3 + a_6, \qquad f_4 = x^6 + x^2 a_6. \tag{7a}$$

In the supersingular case (2b), the first few f_n are:

$$f_1 = 1, \qquad f_2 = a_3, \qquad f_3 = x^4 + a_3^2 x + a_4^2, \qquad f_4 = a_3^5. \tag{7b}$$

Remark. Using the expression for f_4 in (7a), we see that the number of points on the elliptic curve (2a) is divisible by 4 if and only if the trace of a_2 from $K = \mathbf{F}_{2^n}$ to $\mathbf{F}_2$ is zero. Namely, since $f_4 = x^2(x^4 + a_6)$, the two nontrivial points of order 4 are those with x-coordinate $x = a_6^{2^{n-2}}$. Their y-coordinates are in K if and only if (2a) can be solved for y with this value of x. Using the change of variables $y \mapsto xy$, we see that the y-coordinates are in K if and only if $x + a_2 + a_6 x^{-2}$ with $x = a_6^{2^{n-2}}$

has zero trace. But $a_6x^{-2} = a_6^{2^{n-1}}$ is a conjugate of x, and so the first and third terms in the trinomial have the same trace. Thus, we have a nontrivial point of order 4 if and only if the trace of a_2 is zero.

Returning to the general case of arbitrary characteristic, we see that for $n \geq 5$ the following special cases of Proposition 1 can be used to compute f_n recursively:

$$f_{2n+1} = f_{n+2}f_n^3 - f_{n-1}f_{n+1}^3; \qquad (5)_{n+1,n}$$

$$f_2f_{2n} = f_{n+2}f_nf_{n-1}^2 - f_{n-2}f_nf_{n+1}^2. \qquad (5)_{n+1,n-1}$$

From this it is easy to see that f_n can be expressed as a homogeneous polynomial in f_2, f_3 and f_4 of total weight $n^2 - 1$, where f_2, f_3 and f_4 are assigned weights 3, 8 and 15, respectively.

Remark. In the case of a nonsupersingular curve in characteristic 2 with equation (2a), it is not hard to show by induction that the f_n are monic as polynomials in x.

In the case of a supersingular elliptic curve in characteristic 2 with equation (2b), the division polynomials have a particularly simple form. For simplicity, we take $a_3 = 1$.

Proposition 3. *If $a_3 = 1$ in (2a), then*

(i) *for n even, $f_n = f_{n/2}^4$;*

(ii) *for n odd, if one sets $z = f_3 = x^4 + x + a_4^2$, then there exists a polynomial $P_n \in \mathbf{F}_2[u]$ of degree $[(n^2 - 1)/24]$ such that $f_n = P_n(z^3)$ if $3 \not| n$ and $f_n = zP_n(z^3)$ if $3|n$.*

6. Multiples of a point in characteristic 2

Because the formulas in the literature (e.g., [10]) do not apply in characteristic 2, we shall give a proof of modified formulas that apply over $\mathbf{F}_{2^n}$.

Let h_4 denote the partial derivative with respect to x of the defining equation of E, i.e.,

$$h_4 = \begin{cases} x^2 + y, & \text{in the nonsupersingular case (2a);} \\ x^2 + a_4, & \text{in the supersingular case (2b).} \end{cases} \qquad (8)$$

(h is assigned the subscript 4 to indicate its weight).

Proposition 4. *Let $P = (x,y)$ be a point on an elliptic curve E over a field K of characteristic 2 having equation (2a) (resp. (2b)). For $n \geq 1$ let $f_n \in$*

$\mathbf{F}_2[x,y,a_2,a_6]$ (resp. $f_n \in \mathbf{F}_2[x,y,a_3,a_4]$) be the division polynomials, and set $f_0 = 0$. Then for $n \geq 2$ the coordinates of nP are

$$\left(x + \frac{f_{n+1}f_{n-1}}{f_n^2},\ y + (f_2 \circ n) + \frac{f_{n+1}^2 f_{n-2}}{f_2 f_n^3} + h_4 \frac{f_{n+1}f_{n-1}}{f_2 f_n^2}\right), \tag{9}$$

where h_4 is as in (8) and $f_2 \circ n$ has the same meaning as in Proposition 2, i.e.,

$$f_2 \circ n = \begin{cases} x + f_{n-1}f_{n+1}/f_n^2, & \textit{in the nonsupersingular case (2a);} \\ a_3, & \textit{in the supersingular case (2b).} \end{cases}$$

Proof. The formula for the x-coordinate of nP is the same as in [10] and [16], and the proof in the general case is valid in characteristic 2. However, the formula for the y-coordinate is quite different (because in [10] and [16] one has to divide by 2). We prove the formula for the y-coordinate in (9) by induction on n. For $n = 2$ it follows immediately from (4a) and (4b). Now for $n \geq 2$ we suppose that nP is given by (9), and we prove the formula for the y-coordinate of $(n+1)P$.

For the duration of this proof we introduce the notation x_n and y_n for the x- and y-coordinates of $nP_{x,y}$, and we set

$$\tilde{x}_n = x_n + x = f_{n+1}f_{n-1}/f_n^2; \qquad \tilde{y}_n = y_n + y + (f_2 \circ n).$$

Thus, our induction assumption is that $\tilde{y}_n = f_{n+1}^2 f_{n-2}/(f_2 f_n^3) + (h_4/f_2)\tilde{x}_n$, and we must prove the analogous formula with n replaced by $n+1$. Applying the addition formulas (3a) and (3b) to compute the y-coordinate of $P_{x,y} \oplus nP_{x,y}$, in both the supersingular and nonsupersingular cases we have

$$\begin{aligned} \tilde{y}_{n+1} &= \frac{\tilde{x}_{n+1}}{\tilde{x}_n}(\tilde{y}_n + (f_2 \circ n)) \\ &= \frac{f_{n+2}f_n^3}{f_{n-1}f_{n+1}^3}\left(\frac{f_{n+1}^2 f_{n-2}}{f_2 f_n^3} + \frac{f_{2n}}{f_n^4}\right) + \frac{h_4}{f_2}\tilde{x}_{n+1}, \end{aligned}$$

by the induction assumption and Proposition 2. After clearing denominators, we find that the desired formula for $\tilde{y}_{n+1}$ reduces to $(5)_{n+1,n-1}$. This completes the proof.

7. Curves of almost-prime order

For applications to discrete log cryptosystems ([7], [15]), one needs elliptic curves over $\mathbf{F}_{2^n}$ whose order N is either prime or "almost prime." If B is some constant, we shall use the term "B-almost prime" to mean that N is divisible by a prime factor $\geq N/B$.

In practice, apparently such elliptic curves occur with reasonable frequency, even when n is fairly large. However, from a theoretical point of view, the situation is not satisfactory. In fact, at present one cannot prove (for any fixed B) that there are infinitely many elliptic curves over $\mathbf{F}_{2^n}$ (as n and the coefficients a_i vary) of B-almost prime order. Because of results of Deuring [3], Waterhouse [19] and Schoof [17] on the distribution of this order (see also Lenstra's Proposition 1.7 in [11]), we know that for large n the orders of the elliptic curves over $\mathbf{F}_{2^n}$ are close to being uniformly distributed among the even numbers N which satisfy $|N - 2^n - 1| \leq 2\sqrt{2^n} = 2^{n/2+1}$ (more precisely, to be sure there is an E with a given N, one must take N closer to 2^n+1, i.e., $|N-2^n-1| \leq 2^{n/2}$). Thus, the conjecture that there are infinitely many elliptic curves of 2-almost prime order over $\mathbf{F}_{2^n}$ as n varies would follow from the following conjecture: There are infinitely many primes in the set $S = \cup_n \left(2^n - 2^{(n-1)/2}, 2^n + 2^{(n-1)/2}\right)$. More generally, one would expect that the probability of an integer in S being B-almost prime is similar to the probability that an arbitrary integer of the same order of magnitude is B-almost prime. But such a conjecture has not been proved.

One could resolve this theoretical difficulty by constructing cryptosystems from the jacobians of genus 2 curves, as described in [9]. Then from a result of Iwaniec and Juttila on the number of primes between $2^{2n} - 2^{1.5n}$ and 2^{2n} (see Theorem 5 in [1]) and a result of Adleman and Huang [1] on the distribution of the orders of such jacobians it follows that for any n one can find a genus 2 curve over $\mathbf{F}_{2^n}$ of prime order in probabilistic polynomial time in n. However, the analog of Schoof's algorithm for genus 2 curves seems to be prohibitively complicated; in any case, no one has yet implemented a polynomial time algorithm to determine the number of points on a random genus 2 curve.

In what follows, let us assume that as the coefficients vary in (2a) the probability of B-almost primality of $N = |E|$ is the same as that of a random even integer of the same order of magnitude. Since $N \approx q = 2^n$, for fixed B and large q the latter probability is asymptotic to $\sum_{j=1}^{B/2} \frac{1}{j\log(q/2j)} \approx \frac{1}{n}\log_2(B/2)$. Thus, if we want a $\geq$40-digit (i.e., $\geq$134-bit) prime factor of N, so that we can take $B = 2^{n-134}$, then we expect to have to try $n/(n-135)$ curves before finding E with $|E|$ divisible by a $\geq$40-digit prime. For example, if we choose $n = 148$, then we expect to have to apply Schoof's algorithm about 6 times (since each time we are actually determining the order of a curve and its twist simultaneously).

Alternatively, we could set $B = 2$, i.e., insist that $|E|$ be twice a prime. Recall that $|E|/2$ is odd if and only if a_2 has trace 1 in (2a). Although we must apply Schoof's algorithm more times (≈ 46 if $n = 135$), we can shorten the process in the following way. In Schoof's algorithm, when we compute $t \pmod{l}$ for the first few values of $l = 3, 5, 7, \ldots$, we first determine whether $t \equiv q+1 \pmod{l}$; in that case our curve has order $q+1-t$ divisible by l, and so we immediately move on to another random choice of a_6. For instance, with $q = 2^{135}$, after quickly ruling out E for which 3, 5 or 7 divides $|E|$, the expected number of curves we must go through before finding E with $|E|/2$ prime is $\frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} \cdot \frac{6}{7} \cdot \log 2^{134} \approx 21$.

8. Running time of the search for a suitable curve

To fix ideas, suppose that we want to find a curve $E: \ y^2 + xy = x^3 + x^2 + a_6$ over $\mathbf{F}_q$ with $q = 2^{135}$, such that $|E| = q + 1 - t$ is twice a prime. We shall give a rough estimate of the number of field multiplications required to determine t. In comparison, testing $(q+1-t)/2$ for primality is extremely fast. As explained at the end of the last section, we expect to have to go through this procedure about 21 times with different random $a_6 \in \mathbf{F}_q$ before we find the desired E.

As explained in §4, Schoof's algorithm proceeds by computing t modulo l for all odd primes $l \leq L$, where L is the smallest prime such that $\prod_{l \leq L} l > \sqrt{q} = 2^{67.5}$, i.e., $L = 59$. (Here we have $\sqrt{q}$ rather than $4\sqrt{q}$ because we already know that $|E| \pmod{4}$ is 2.) For each l, one runs through the possible τ, $0 \leq \tau < l$, testing whether or not $t \equiv \tau \pmod{l}$. On the average one expects to find the value of τ which is $t \pmod{l}$ after testing about $l/2$ values of τ. Given l and τ, the testing procedure (except for one or two exceptional values of τ, which we shall neglect in our time estimate) consists in determining whether a certain polynomial is zero modulo $f_l(x)$. Part of that polynomial does not depend on τ, and so can be computed once and for all modulo $f_l(x)$. It turns out that the most time-consuming part of the algorithm is computing f_τ^{2q}, $f_{\tau-1}^q$, and $f_{\tau+1}^q$ modulo f_l. For $\tau \geq 2$ the first two of these will be available from the computations for $\tau - 2$ and $\tau - 1$, and so the heart of the computation is to find $f_{\tau+1}^q$ modulo f_l. Note that $f_l \in \mathbf{F}_q[x]$ is monic of degree $(l^2-1)/2$. Thus, 135 times we must successively square a polynomial of degree $< l^2/2$ and divide the result by f_l. The division requires about $(l^2/2)^2 = l^4/4$

field multiplications. Putting this all together, we find the following estimate for the number of field multiplications in the most time-consuming part of Schoof's algorithm for a given elliptic curve:

$$135 \cdot \sum_{3 \leq l \leq 59,\ l \text{ prime}} l^5/8 \approx 3 \cdot 10^{10}.$$

In [13] the authors describe a special–purpose chip that performs about 15000 multiplications per second in $\mathbf{F}_{2^{593}}$, using an optimal normal basis. Since the time is roughly linear in the extension degree, a similar chip for $\mathbf{F}_{2^{135}}$ would perform about 66000 multiplications per second; hence, the length of time to find $|E|$ is about

$$3 \cdot 10^{10}/66000 = 4.5 \cdot 10^5 \text{ sec} \approx 5 \text{ days}.$$

Thus, if we have more than 21 computers working in parallel, each with a different a_6, then within a week we are likely to find a new elliptic curve E such that $|E|/2$ is a 40-digit prime.

Remark. The above time estimate is too big, perhaps, for complete practicality. However, the improved versions of Schoof's algorithm that are being developed (by A. O. L. Atkin, N. Elkies, V. Miller, and others) should soon decrease this time estimate, thereby making the random–curve method a practical choice of public key cryptosystem.

References

1. Adleman L. M. and Huang M. A., "Recognizing primes in random polynomial time," *Proc. 19th Annual ACM Symp. on Theory of Computing*, 1987, 462-469.

2. Bender A. and Guy Castagloni, "On the implementation of elliptic curve cryptosystems," *Advances in Cryptology - Crypto '89*, Springer-Verlag, 1990, 186-192.

3. Deuring M., "Die Typen der Multiplikatorenringe elliptischer Funktionenkörper," *Abh. Math. Sem. Hansischen Univ.* 14 (1941), 197-272.

4. Goldwasser S. and Kilian J., "Almost all primes can be quickly certified," *Proc. 18th Annual ACM Symp. on Theory of Computing*, 1986, 316-329.

5. Koblitz N., *Introduction to Elliptic Curves and Modular Forms*, Springer-Verlag, 1984.

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

7. Koblitz N., "Elliptic curve cryptosystems," *Math. Comp.* **48** (1987), 203-209.

8. Koblitz N., "Primality of the number of points on an elliptic curve over a finite field," *Pacific J. Math.* **131** (1988), 157-165.

9. Koblitz N., "Hyperelliptic cryptosystems," *J. Cryptology* **1** (1989), 139-150.

10. Lang S., *Elliptic Curves Diophantine Analysis*, Springer-Verlag, 1978.

11. Lenstra A. K. and Lenstra H. W., Jr., "Algorithms in number theory," Technical Report 87-008, Univ. Chicago, 1987.

12. Menezes A. and S. A. Vanstone, "Isomorphism classes of elliptic curves over finite fields," *Research Report 90-01*, University of Waterloo, 1990.

13. Menezes A. and S. A. Vanstone, "The implementation of elliptic curve cryptosystems," preprint.

14. Menezes A., T. Okamoto, and S. A. Vanstone, "Reducing elliptic curve logarithms to logarithms in a finite field," preprint.

15. Miller V., "Use of elliptic curves in cryptography," *Advances in Cryptology - Crypto '85*, Springer-Verlag, 1986, 417-426.

16. Schoof R. J., "Elliptic curves over finite fields and the computation of square roots mod p," *Math. Comp.* **44** (1985), 483-494.

17. Schoof R. J., "Nonsingular plane cubic curves over finite fields," *J. Combinatorial Theory* **46** (1987), 183-211.

18. Silverman J., *The Arithmetic of Elliptic Curves*, Springer-Verlag, 1986.

19. Waterhouse W. C., "Abelian varieties over finite fields," *Ann. Sci. École Norm. Sup.*, 4^{e} sér. **2** (1969), 521-560.