MATHEMATICS OF COMPUTATION
VOLUME 48, NUMBER 177
JANUARY 1987, PAGES 203–209

Elliptic Curve Cryptosystems

By Neal Koblitz

This paper is dedicated to Daniel Shanks on the occasion of his seventieth birthday

Abstract. We discuss analogs based on elliptic curves over finite fields of public key cryptosystems which use the multiplicative group of a finite field. These elliptic curve cryptosystems may be more secure, because the analog of the discrete logarithm problem on elliptic curves is likely to be harder than the classical discrete logarithm problem, especially over GF(2^n). We discuss the question of primitive points on an elliptic curve modulo p, and give a theorem on nonsmoothness of the order of the cyclic subgroup generated by a global point.

1. Introduction. The earliest public key cryptosystems using number theory were based on the structure either of the multiplicative group $(\mathbf{Z}/N\mathbf{Z})^*$ or the multiplicative group of a finite field GF(q), $q = p^n$. The subsequent construction of analogous systems based on other finite Abelian groups, together with H. W. Lenstra's success in using elliptic curves for integer factorization, make it natural to study the possibility of public key cryptography based on the structure of the group of points of an elliptic curve over a large finite field. We first briefly recall the facts we need about such elliptic curves (for more details, see [4] or [5]). We then describe elliptic curve analogs of the Massey-Omura and ElGamal systems. We give some concrete examples, discuss the question of primitive points, and conclude with a theorem concerning the probability that the order of a cyclic subgroup is nonsmooth.

I would like to thank A. Odlyzko for valuable discussions and correspondence, and for sending me a preprint by V. S. Miller, who independently arrived at some similar ideas about elliptic curves and cryptography.

2. Elliptic Curves. An elliptic curve E_K defined over a field K of characteristic $\neq 2$ or 3 is the set of solutions $(x, y) \in K^2$ to the equation

$$y^2 = x^3 + ax + b, \qquad a, b \in K \tag{1}$$

(where the cubic on the right has no multiple roots). More precisely, it is the set of such solutions together with a "point at infinity" (with homogeneous coordinates $(0, 1, 0)$; if K is the real numbers, this corresponds to the vertical direction which the tangent line to E_K approaches as $x \to \infty$). One can start out with a more complicated general formula for E_K which can easily be reduced to (1) by a linear change of variables whenever $\operatorname{char} K \neq 2, 3$. If $\operatorname{char} K = 2$—an important case in

Received October 29, 1985; revised June 5, 1986.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11T71, 94A60; Secondary 68P25, 11Y11, 11Y40.

0025-5718/87 $1.00 + $.25 per page

possible applications—this general formula can be reduced by a linear change of variables to the form

$$y^2 + cxy + dy = x^3 + ax + b, \qquad a, b, c, d \in K. \tag{2}$$

The points on E_K form a group with identity element the point at infinity. The negative of a point $P \in E_K$ is the second point on E_K having the same x-coordinate as P. Now suppose that $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ are two points not the point at infinity and not the negatives of one another. If K is the real numbers, there is a simple geometric description of the point $P_3 = (x_3, y_3)$ which is their sum: Draw the line through P_1 and P_2 (the tangent line to the curve at P_1 if $P_1 = P_2$), and let P_3 be the negative of the third point of intersection of $\overline{P_1P_2}$ with the curve. Moreover, there are algebraic formulas which can easily be derived from this geometrical procedure and can then be applied over any field K. Namely, if E_K has the equation (2), then

$$x_3 = -x_1 - x_2 + \alpha^2 + c\alpha, \qquad y_3 = -cx_3 - d - y_1 + \alpha(x_1 - x_3), \tag{3}$$

where

$$\alpha = \begin{cases} (y_2 - y_1)/(x_2 - x_1), & \text{if } P_1 \neq P_2; \\ (3x_1^2 + a - cy_1)/(2y_1 + cx_1 + d), & \text{if } P_1 = P_2. \end{cases} \tag{4}$$

In particular, if E_K is given by the equation (1), one sets $c = d = 0$ in (3)–(4), and the formulas become a little simpler.

Using these formulas, one can compute a multiple mP of a given point P in the same order of time as it takes to exponentiate a^m, using the analogous procedure, i.e., by means of $O(\log m)$ doublings and additions, e.g., $11P = P + 2(P + 2(2P))$. Alternatively, one can use recursive formulas which express the coordinates of $2mP$ and $(2m + 1)P$ in terms of those of mP (see [5, pp. 37–38]).

If $K = \mathrm{GF}(q)$, $q = p^n$, is a finite field, then the points of E_K form a finite Abelian group. In some ways this group is similar to the multiplicative group $\mathrm{GF}(q)^*$ of the field K. For example, Hasse proved that the order of the group $|E_K|$ is equal to $q + 1 - a_{E_K}$, where $|a_{E_K}| \leqslant 2\sqrt{q}$, and so it has the same asymptotic size as $|\mathrm{GF}(q)^*| = q - 1$. Actually, one can obtain $\mathrm{GF}(q)^*$ from the above construction of an addition law on E_K if one lets E_K "degenerate" by letting the cubic on the right in (1) acquire a double root; then, if the two slopes at the singular point of E_K are in $\mathrm{GF}(q)$, it turns out that the set of nonsingular points of E_K (i.e., those whose x-coordinate is not the double root) form a group isomorphic to $\mathrm{GF}(q)^*$.

But unlike $\mathrm{GF}(q)^*$, which is a cyclic group, the Abelian group E_K for $K = \mathrm{GF}(q)$ can either be cyclic or else a product of two cyclic groups. In practice, for a "random" elliptic curve, usually either this group is cyclic or else it can be written as a product with one of the cyclic factors much smaller than the other, i.e., it is "almost" cyclic. We shall return to this question when we discuss the examples.

3. Imbedding plaintext. Let $E = E_K$ be an elliptic curve defined over $K = \mathrm{GF}(q)$, where $q = p^n$ is large. We shall suppose that we have a method of imbedding plaintexts in E which is easy to implement and easy to decode. Here are some examples of such methods.

(1) Suppose that p is arbitrary (e.g., 2) and $n = 2n'$ is even. Suppose that our plaintexts are integers m, $0 \leqslant m < p^{n'}$ written in the form $m = m_0 + m_1 p + \cdots + m_{n'-1}p^{n'-1}$, $0 \leqslant m_j < p$; and let $b_0, \ldots, b_{n'-1}$ be a convenient vector space basis of $\mathrm{GF}(p^{n'})$ over $\mathrm{GF}(p)$. Set $x(m) = m_0 b_0 + m_1 b_1 + \cdots + m_{n'-1}b_{n'-1}$, and let $y(m) \in \mathrm{GF}(p^n)$ be either solution of the quadratic equation (1) or (2) defining points on E. Set $P_m = (x(m), y(m)) \in E$. Here such a solution $y(m)$ is guaranteed to exist, but the most efficient algorithms for solving quadratic equations over finite fields are probabilistic (except for R. Schoof's recently discovered method [12] for finding square roots mod p using elliptic curves).

(2) Suppose that $n = 1$, $q = p \equiv 3 \pmod 4$, and E is given by Eq. (1). Suppose that our plaintexts are integers m, $0 \leqslant m < p/1000 - 1$. We try appending three digits to m until we obtain an x, $1000m \leqslant x < 1000(m+1) < p$, such that $f(x) = x^3 + ax + b$ is a square in $\mathrm{GF}(p)$. Then $P_m \overset{\text{def}}{=} (x, f(x)^{(p+1)/4})$ is a point on E; and obviously m can be decoded from P_m simply by dropping the last three digits from the x-coordinate. This is a probabilistic imbedding of $\{m\}$ in E, since there is a miniscule probability that $f(x)$ will be a nonsquare for all $1000m \leqslant x < 1000(m+1)$.

(3) Let $p = 2$, $n \equiv 4 \pmod 6$, let $b_0, \ldots, b_{n-1}$ be a convenient vector space basis of $\mathrm{GF}(2^n)$ over $\mathrm{GF}(2)$, and let E be given by the equation

$$E\colon\ y^2 + y = x^3. \tag{5}$$

Suppose that our plaintexts are in the range $m < 2^{n-10}$, $m = m_0 + m_1 2 + \cdots + m_{n-11}2^{n-11}$, $m_j \in \{0,1\}$, and try setting $y = m_0 b_0 + \cdots + m_{n-11}b_{n-11} + m_{n-10}b_{n-10} + \cdots + m_{n-1}b_{n-1} \in \mathrm{GF}(2^n)$ with various $m_{n-10}, \ldots, m_{n-1} \in \{0,1\}$; if $y^2 + y$ is a cube in $\mathrm{GF}(2^n)$, then the point $P_m = (x, y)$ is on E for $x = (y^2 + y)^{(2^n+2)/9}$. This gives a probabilistic imbedding of the set $\{m\}$ of plaintexts in E.

4. Cryptosystems. Cryptosystems based on $\mathrm{GF}(q)^*$ can be translated to systems using the group E, where E is an elliptic curve defined over $\mathrm{GF}(q)$. We shall illustrate this by describing two elliptic curve public key cryptosystems for transmitting information. A discussion of an elliptic curve analog for the Diffie-Hellman key exchange system can be found in [9].

(1) *Elliptic curve analog of the Massey-Omura system.* Let $q = p^n$ be large, let E be an elliptic curve defined over $\mathrm{GF}(q)$, and let $N = |E|$. Here q and E are fixed and publicly known, as is N. We also have a publicly known imbedding $m \mapsto P_m$ of plaintexts as points of E. Suppose that user A wants to send user B a message m. She chooses a random integer c satisfying $0 < c < N$ and g.c.d.$(c, N) = 1$, and transmits cP_m. Next, B chooses a random integer d with the same properties, and transmits $d(cP_m)$ to A. Then A transmits $c'(dcP_m) = dP_m$ back to B, where $c'c \equiv 1 \pmod N$. Finally, B computes $d'dP_m = P_m$, where $d'd \equiv 1 \pmod N$.

(2) *Elliptic curve analog of the ElGamal system.* We assume the same setup as in (1), except that now no one needs to know N. (This is no major theoretical saving, since R. Schoof [12] has found an algorithm to compute N in $O(\log^9 q)$ bit operations; but it might be a great practical convenience to be able to avoid this.) We further let $G \in E$ be a fixed and publicly known point. The receiver B chooses a

randomly and publishes the key aG, while keeping a itself secret. To transmit a message m to B, user A chooses a random integer k and sends the pair of points $(kG, P_m + k(aG))$. To read the message, B multiplies the first point in the pair by his secret a, and then subtracts the result from the second point in the pair.

Remark. Both Massey and Omura's and ElGamal's constructions are essentially variants of Diffie and Hellman's original key exchange system. In the elliptic curve context, the latter consists in each user A choosing an integer c and making cP public; two users A and B take as their key $d(cP) = c(dP)$, where d is B's secret key. Massey-Omura works the same way, except that user B waits until A publishes cP and then makes dcP (rather than dP) known to A. The ElGamal system uses the same type of construction, with the additional element that the map $P \mapsto P + Q$ is used as a "generalized Vernam cipher." (The author thanks the referee for this remark.)

Breaking either the elliptic curve Massey-Omura or the ElGamal system requires the solution of the elliptic curve analog of the discrete logarithm problem:

Elliptic Curve Discrete Logarithm Problem. Given an elliptic curve E defined over $\mathrm{GF}(q)$ *and two points $P, Q \in E$, find an integer x such that $Q = xP$ if such x exists.*

It is likely that this problem will prove to be more intractible than the classical discrete logarithm problem. The strongest techniques known for the latter do not seem to be applicable to the elliptic curve analog (see [9] for a discussion of this). In particular, elliptic curves might be especially suitable for use over $\mathrm{GF}(2^n)$, because, as Odlyzko explains [11], discrete logarithms in $\mathrm{GF}(2^n)$ are relatively easy to compute unless n is chosen to be quite large. It is likely that the analogous systems using elliptic curves over $\mathrm{GF}(2^n)$ will be secure with significantly smaller values of n.

However, in order to avoid an easy solution to the discrete logarithm problem using the techniques that apply to any finite Abelian group (which take approximately $\sqrt{r}$ operations, where r is the largest prime dividing the order of the group), it is important to choose E and q so that $N = |E|$ is divisible by a large prime (see the examples below). Notice that this is the exact opposite of the (more difficult) requirement in Lenstra's factoring algorithm, where one must look for elliptic curves with N a "smooth" number.

5. Examples. (1) In the ElGamal elliptic curve system, given $q = p^n$, choose both E and G randomly. For example, let $g(y) = y^2$ if $p > 2$ and $g(y) = y^2 + y$ if $p = 2$. Then choose random elements $x, y, a \in \mathrm{GF}(p^n)$, and set $b = g(y) - x^3 - ax$. Then $G = (x, y)$ is a point on the elliptic curve with equation (1) or (2) (with $c = 0$, $d = 1$). (The discriminant of the equation must be nonzero, but this is virtually certain if a and b are random elements of a large finite field.)

Before using the chosen E and G, one should check that the order of G in E is not a smooth integer; if a product of fairly small primes takes G to the identity (the point at infinity), then another random choice should be made.

(2) Let E be given by the equation $y^2 + y = x^3$ over $\mathrm{GF}(2^n)$, $n \equiv 4 \pmod 6$, as above. As described above, we have a simple (probabilistic) imbedding $m \mapsto P_m$ of plaintexts into E. This E is also convenient for other reasons. The formulas for doubling a point are particularly simple:

$$2P = \left(x^4, y^4 + 1\right) \quad \text{for } P = (x, y),$$

as we see by substituting $x_1 = x_2 = x$, $a = b = c = 0$, $d = 1$ in (3)–(4) and using the equation (5) of the curve to simplify $y_3 = -1 - y + x^2(x - x^4)$.

In addition, there is an easy formula for N in this case:

$$N = |E| = 2^n + 1 - 2(-2)^{n/2} = \left((-2)^{n/2} - 1\right)^2.$$

Thus, in order to ensure that N is divisible by a large prime, we could, for example, choose n so that $n/4 \equiv 1 \pmod 3$ gives a Mersenne number with a large factor, e.g., a Mersenne prime (for example, $n = 508$).

This curve could be used for the Massey-Omura system or, after choosing a random point G (using the technique described above for imbedding plaintexts in E), for the ElGamal system.

(3) Let E be given by the equation

$$y^2 + y = x^3 - x \tag{6}$$

over GF(p), p a large prime, and set $G = (0, 0)$. It is known that, if the equation of E is considered over the field of rational numbers, then $G = (0, 0)$ is a point of infinite order whose multiples exhaust all rational points of E. It does *not* follow that, after reduction modulo p, G generates all points of E over GF(p); in fact, the latter group is not necessarily cyclic. However, it is likely that G almost always generates a large part of $E_{\mathrm{GF}(p)}$. We now discuss this in more detail.

6. Primitive Points. In elliptic curve cryptosystems of the sort discussed above, one does not work with the entire group E, but rather with cyclic subgroups: the groups $\langle P_m \rangle$ in the Massey-Omura system and the group $\langle G \rangle$ in the ElGamal system. It is desirable for the groups $\langle P_m \rangle$ and $\langle G \rangle$ to be large, i.e., for their index in E to be small. More precisely, the order of these cyclic subgroups should be nonsmooth, i.e., divisible by a large prime, in order to preclude easy solution of the discrete logarithm problem in them.

In our examples, G is either a "random" point chosen after we have specified q (in Examples (1)–(2) above) or else a global point (Example (3)), i.e., a fixed point of infinite order on an elliptic curve E_Q defined over the rational numbers which is then reduced mod p after we choose some large p and decide to work with $E_{\mathrm{GF}(p)} = E \bmod p$. In either case, it is natural to ask: What is the probability (as p varies with G fixed, or as p and "random" G both vary) that G generates $E \bmod p$? Or, if we cannot rely on that happening often enough, we might ask: What is the probability, if $|E \bmod p|$ is divisible by a large prime l, that $|\langle G \bmod p \rangle|$ will also be divisible by l?

The first question is the elliptic curve analog of the primitive root problem for GF(p) that was considered by E. Artin (see the Preface to [6] and also [14] and [10] for more details). Let $a \neq 0, \pm 1$ be a fixed integer which is not of the form $\pm b^n$ for any $n > 1$. Artin first observed that one can use the Chebotarev density theorem to show that, for any prime l, the probability that l divides the index of a in GF(p)*, i.e., that $l \mid p - 1$ and $a^{(p-1)/l} \equiv 1 \pmod p$, is equal to $1/(l(l-1))$. He then conjectured that these events are independent for different l, in which case the probability that a is a generator, i.e., that no prime l divides the index of a in GF(p)*, is equal to

$$\prod_{\text{primes } l} \left(1 - \frac{1}{l(l-1)}\right) = 0.3729\ldots. \tag{7}$$

It was later noticed that the events are not necessarily independent, and for certain a one must modify a few of the factors in (7). For example, the number that has the highest probability of being a generator is $a = -3$, where this probability is obtained by deleting the $l = 3$ term in (7). In particular, since -3 is a square and hence not a generator whenever $p \equiv 1 \bmod 3$, it follows that -3 is a generator of GF(p)* for 89.7% of all $p \equiv 2 \bmod 3$. The modified Artin conjecture was shown by C. Hooley to hold if one assumes the generalized Riemann hypothesis (GRH).

In the elliptic curve case, an analog of Artin's conjecture was proposed by Lang and Trotter [7] (see also [3]). Let E be a fixed elliptic curve defined over $\mathbf{Z}$ with discriminant Δ, and let $p_1, p_2, \ldots$ be the increasing sequence of primes with the primes dividing Δ omitted. Let G be a fixed point of infinite order on E which is not of the form nG' for any $n > 1$. One says that G is "primitive for p" if $G \bmod p$ generates $E \bmod p$. Let $f(n)$ be the proportion of the first n primes for which G is primitive:

$$f(n) = f_{E,G}(n) = \frac{1}{n}\left|\{\, j \leqslant n \mid G \text{ is primitive for } p_j \}\right|.$$

Then Lang and Trotter conjectured that $f(n)$ approaches a nonzero limit and described how to determine this limit. In the case of the three elliptic curves

(8) $A\colon y^2 + y = x^3 - x, \quad B\colon y^2 + y = x^3 + x^2, \quad C\colon y^2 + xy + y = x^3 - x^2$

and the point $G = (0,0)$, they conjectured the following value:

$$\lim_{n\to\infty} f(n) = \prod_l \left(1 - \frac{l^3 - l - 1}{l^2(l-1)(l^2-1)}\right) \approx 0.440.$$

This conjecture supposes that the events $l \mid [E \bmod p\colon \langle G \bmod p\rangle]$ are independent for different l. (Actually, at the "bad" prime 37, 43, 53, respectively, one must introduce a correction term which does not, however, affect the above value in the first three decimal places [15].)

In the case of elliptic curves with complex multiplication, a weaker version of the Lang-Trotter conjecture (where one must ignore primes p that do not split in the complex multiplication field) was proved by Gupta and Murty [3] assuming the GRH. Serre ([13], see also [10]), also assuming the GRH, proved an analogous result about the question of cyclicity of $E \bmod p$: The proportion of p for which $E \bmod p$ is a cyclic group approaches a nonzero constant.

Lang and Trotter tested their conjecture in the cases (8) (and $G = (0,0)$) for the first 200 primes. The results were not very close to the predicted value of 88 primes for which G is primitive (the numbers were 91, 96 and 91, respectively; my computations show that these numbers should be corrected to 92, 96, 92), so they then discarded the first twenty p_j, and counted the proportion of the remaining 180. In the interval p_j, $20 < j \leqslant 200$, the agreement with the predicted proportion was fairly good. Recently, Trotter [15] has extended these computations to the first 2000 primes, obtaining more convincing statistical evidence supporting the conjecture for the curves (8).

7. Nonsmooth Cyclic Subgroups. The second question about the index of $\langle G \bmod p\rangle$ in $E \bmod p$ is weaker: If we have ensured that $|E \bmod p|$ is nonsmooth and know that it is divisible by a large prime l, then what is the probability that $|\langle G \bmod p\rangle|$ is also divisible by l? Unless $l^2 \mid |E \bmod p|$, which is not likely for large

l, this is equivalent to asking about the probability that l divides the index of $\langle G \bmod p\rangle$ in $E \bmod p$. In other words, for fixed E, G, and l, what is the conditional probability that $l \mid [E \bmod p\colon \langle G \bmod p\rangle]$ given that $l \mid |E \bmod p|$? Following the argument in [7] and using the Chebotarev density theorem and results of Serre and Bashmakov for non-CM curves, one has the following answer.

THEOREM. *Let G be a fixed point of infinite order on an elliptic curve E of discriminant Δ which is defined over $\mathbf{Z}$ and does not have complex multiplication. Then, for all but finitely many primes l,*

$$\lim_{x\to\infty} \frac{|\{\text{primes } p \leqslant x,\ p \nmid \Delta \mid l \text{ divides } [E \bmod p\colon \langle G \bmod p\rangle]\}|}{|\{\text{primes } p \leqslant x,\ p \nmid \Delta \mid l \text{ divides } |E \bmod p|\}|} = \frac{l^3 - l - 1}{l^2(l^2-2)} = \frac{1}{l} + O\left(\frac{1}{l^3}\right).$$

COROLLARY. *Under the conditions of the theorem, for all but finitely many primes l,*

$$\lim_{x\to\infty} \frac{|\{\text{primes } p \leqslant x,\ p \nmid \Delta \mid l \text{ divides } |\langle G \bmod p\rangle|\}|}{|\{\text{primes } p \leqslant x, p \nmid \Delta \mid l \text{ divides } |E \bmod p|\}|} = 1 - \frac{1}{l} + \frac{1}{l^2} + O\left(\frac{1}{l^3}\right).$$

In the corollary, the extra l^{-2} term arises from the possibility that $l^2 \mid |E \bmod p|$.

Finally, we note that the gist of these conjectures and partial results is that, even though $|E \bmod p|$ increases with p, the index $[E \bmod p\colon \langle G \bmod p\rangle]$ on the average does not. Thus, for extremely large p, the subgroup generated by G can be expected to be almost as "good" (i.e., nonsmooth) as E itself.

Department of Mathematics GN-50
University of Washington
Seattle, Washington 98195

1. W. DIFFIE & M. HELLMAN, "New directions in cryptography," *IEEE Trans. Inform. Theory*, v. 22, 1976, pp. 644–654.

2. T. ELGAMAL, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Trans. Inform. Theory*, v. 31, 1985, pp. 469–472.

3. R. GUPTA & M. R. P. MURTY, "Primitive points on elliptic curves," *Compositio Math.*, v. 58, 1986, pp. 13–44.

4. N. KOBLITZ, *Introduction to Elliptic Curves and Modular Forms*, Springer-Verlag, New York, 1984.

5. S. LANG, *Elliptic Curves: Diophantine Analysis*, Springer-Verlag, New York, 1978.

6. S. LANG & J. TATE, eds., *The Collected Papers of Emil Artin*, Addison-Wesley, Reading, Mass., 1965.

7. S. LANG & H. TROTTER, "Primitive points on elliptic curves," *Bull. Amer. Math. Soc.*, v. 83, 1977, pp. 289–292.

8. H. W. LENSTRA, JR., "Factoring integers with elliptic curves." (Preprint.)

9. V. S. MILLER, "Use of elliptic curves in cryptography," *Abstracts for Crypto* '85.

10. M. R. P. MURTY, "On Artin's conjecture," *J. Number Theory*, v. 16, 1983, pp. 147–168.

11. A. M. ODLYZKO, "Discrete logarithms and their cryptographic significance," *Advances in Cryptology: Proceedings of Eurocrypt* 84, Springer-Verlag, New York, 1985, pp. 224–314.

12. R. SCHOOF, "Elliptic curves over finite fields and the computation of square roots mod p," *Math. Comp.*, v. 44, 1985, pp. 483–494.

13. J.-P. SERRE, *Resumé des Cours de l'Année Scolaire*, Collège de France, 1977–1978.

14. D. SHANKS, *Solved and Unsolved Problems in Number Theory*, 3rd ed., Chelsea, New York, 1985.

15. H. TROTTER, personal correspondence and unpublished tables, October 29, 1985.

16. P. K. S. WAH & M. Z. WANG, *Realization and Application of the Massey-Omura Lock*, Proc. Internat. Zurich Seminar, March 6–8, 1984, pp. 175–182.