On the Implementation of Elliptic Curve Cryptosystems

Andreas Bender and Guy Castagnoli
Institute for Signal and Information Processing
Swiss Federal Institute of Technology
ETH Zentrum
CH-8092 Zurich, Switzerland

Abstract

A family of elliptic curves for cryptographic use is proposed for which the determination of the order of the corresponding algebraic group is much easier than in the general case. This makes it easier to meet the cryptographic requirement that this order have a large prime factor. Another advantage of this familiy is that the group operation simplifies slightly. Explicit numerical examples are given that are suitable for practical use.

Introduction

An exponential function and a corresponding discrete logarithm function can be defined in every finite cyclic group [Massey 1983]. There appears to be no reason why the exponential function in the multiplicative group of a finite field should be the hardest one to invert and therefore the best candidate for a one-way function. An attractive alternative is to use a cyclic subgroup of the group of points on an elliptic curve defined over a finite field. There is evidence [Miller 1986] that the discrete logarithm defined for a cyclic subgroup of this group is much more difficult to compute than that in the multiplicative group of a finite field.

G. Brassard (Ed.): Advances in Cryptology - CRYPTO '89, LNCS 435, pp. 186-192, 1990.

Some basic definitions

We describe here briefly how to calculate in a group of points on an elliptic curve. For a more complete treatment of the theory of elliptic curves, see [Koblitz 1987],[Hartshorne 1983].

The group of points on an elliptic curve over an arbitrary field can be defined as the set of solutions (x,y) of a certain third-order algebraic equation, including the "point" at infinity (∞,∞) which is the neutral element of the group, together with an operation on these "points". In a field with characteristic $p > 3$, the general Weierstrass equation can be reduced by means of coordinate transformations to the form $y^2=x^3+ax+b$, whereas for characteristic $p = 3$ it can only be reduced to $y^2=x^3+ax^2+bx+c$, and in the case of characteristic $p = 2$ it can be reduced to $y^2+y=x^3+ax+b$. The condition for nonsingularity is $4a^3+27b^2\neq 0$; the group of points of a singular elliptic curve is isomorphic to the multiplicative or additive group of the field over which the curve is defined [Husemoeller 1987, p.78].

We will only deal with the two cases characteristic $p = 2$ and characteristic $p > 3$ because these are the cases of greatest practical interest. The group operation for these cases is defined as follows. To an arbitrary pair of points P and Q specified by their coordinates (x_1,y_1) and (x_2,y_2), respectively, the group operation assigns a third point $P*Q$ with the coordinates (x_3,y_3). These coordinates are computed in the following way for characteristic $p>3$.

$(x_3,y_3) = (\infty,\infty)$ when $P\neq Q$ and $x_1=x_2.$

$x_3=((y_2-y_1)/(x_2-x_1))^2-x_1-x_2$

$y_3=(x_1-x_3)(y_2-y_1)/(x_2-x_1)-y_1$ when $P\neq Q$ and $x_1\neq x_2$

$(x_3,y_3) = (\infty,\infty)$ when $P=Q$, $P=(0,0)$ and P is an element of the group;

$x_3=((3\, x_1{}^2+a)/(2y_1))^2-2\, x_1$

$y_3=(x_1-x_3)(3x_1{}^2+a)/(2y_1)-y_1$ if $P=Q$.

In the case of characteristic p=2, the equations become

$(x_3,y_3) = (\infty,\infty)$ when $P \neq Q$ and $x_1+x_2 = 0$.
$x_3 = ((y_1+y_2)/(x_1+x_2))^2+x_1+x_2$
$y_3=(x_1+x_3)(y_1+y_2)/(x_1+x_2)+y_1+1$ when $P \neq Q$ and $x_1+x_2 \neq 0$.

$(x_3,y_3) = (\infty,\infty)$ when P=Q, P=(0,0) and P is an element of the group;
$x_3=(x_1{}^2+a)^2$
$y_3=(x_1{}^2+a)(x_1+x_3)+y_1+1$ if P=Q.

The geometric interpretation of the operation * becomes clear if one sketches an elliptic curve in the affine plane over the real numbers. To compute P*Q, one first joins these two points by a straight line. Algebraic considerations show that this line must intersect the curve at a third point. The point P*Q is the point whose x-coordinate is the same as for this third point and whose y-coordinate is the negative of the y-coordinate of this third point.

The order of the group

It is possible to implement the Diffie-Hellman public key-distribution system without knowing the order of the underlying cyclic group. However, the Pohlig-Silver-Hellman algorithm for computing discrete logarithms can be used in an arbitrary cyclic group and runs in time $O(\sqrt{p})$ where p is the largest prime factor of the order of the group. Therefore it is vital to know that the order of the cyclic group is large enough to provide cryptographic security. If we use the multiplicative group of a finite field this problem is trivial: the group order is just equal to p^n-1. However, the computation of the order of the group of points on an elliptic curve over a finite field is difficult in general. Schoof's algorithm to determine this order runs in polynomial time but is not very practical[Schoof 1985].

A Cryptographically Useful Subclass of Elliptic Curves

To avoid cumbersome computation of the group order, we suggest the use of the subclass of elliptic curves having the coefficient a = 0 in their defining equation. These equations then read

$y^2=x^3+b$ for characteristic $p > 3$ and
$y^2+y =x^3+b$ for characteristic $p = 2$.

This specialization has been considered previously in cryptology for random bit generators [Kaliski 1987]. We observe that every nonzero coefficient b satisfies the nonsingularity condition. The following special properties for this specialization are well known.

Property 1:Let p be a prime $\neq 2,3$. If $p \equiv -1 \pmod 3$ the equation $y^2=x^3+b$ has exactly p solutions (x,y) in $GF(p)^2$ (excluding the neutral element) for every b in GF(p)[Kaliski 1987].

Property 2: The integer 3 does not divide p^f-1 if and only if the integer f is odd and $p \equiv -1 \pmod 3$[Grosswald 1984].

Property 3: Let m be an odd positive integer greater than 1. Then $y^2+y=x^3+b$ has exactly 2^m solutions (x,y) (excluding the neutral element) in $GF(2^m)^2$[Lidl Niederreiter 1983].

These properties combine to give the following recipe for group orders.

Proposition: The order of the group of the elliptic curve defined by $y^2=x^3+b$ over GF(p) with $p \equiv -1 \pmod 3$ is p+1. The order of the group of the elliptic curve defined by $y^2+y=x^3+b$ over $GF(2^m)$, where m is odd, is 2^m+1.

Choice of the Elliptic Curve and Cyclic Subgroup

1. The case GF(p)

If $p \equiv -1 (\mathrm{mod}\ 3)$, it follows that p+1 must be divisible by 3 and, since p is an odd prime, p+1 is also divisible by 2. This means that the largest prime factor of the group order p+1 will be achived if p+1 is of the form p+1=2.3.p* where p* is another prime. If p+1=2.3.p* it is also very easy to find a generating element for the cyclic subgroup of order p* or greater to use as a base of the discrete logarithm. Since we have the free parameter b in the defining equations of the curves it is no problem to choose an arbitrary element and to compute its sixth power; if the result is not the neutral element, the order of this particular element is a multiple of p* and so cryptographically useful.

2. The case GF(2^m)

Because 2^m+1 is not divisible by 2, the next smallest possible factor of the order 2^m+1 is 3. Cryptographically, we want $2^m+1=3p^*$ where p* is a prime. Our computations have shown that this is indeed possible for some interesting m.

Numerical Results

The prime number theorem states that the probability that an integer selected arbitrarily in the interval [1,x] is a prime is 1/ln(x). For p+1=6p*, we are interested in the probability that q and 6q-1 are both prime when q is randomly selected in the interval [1,x]. For a rough estimate we may assume the two occurrences to be independent, so we have

$$P(x \text{ and } 6x\text{-}1 \text{ prime}) \sim 1/(\ln(x)\ln(6x-1))$$

If we want to have an x with hundred decimal digits we get

$$P \sim 1/\ln(10^{100})^2 \sim 10^{-4}.$$

This means that with an efficient prime number test (and a reasonably fast computer) it is feasible to search. As numerical results we get

GF(p):
$p^*=\{10^{10}+19, 10^{20}+1267, 10^{21}+367, 10^{50}+4209, 10^{100}+42337\}$ and furthermore $p^*=28'356'863'910'078'205'288'614'550'619'314'021'777$ for which $p=6p^*-1=2^{127}+24933$ is prime. This is the smallest prime greater than 2^{127} for which $(p+1)/6$ is also prime. For this curve which is convenient in computer arithmetic we also give the element (3,5) which lies on the curve defined over GF(p) through $y^2=x^3-2$ and has order p.

The second example of this kind is $p^*=1'537'228'672'809'132'109$ for which $p=6p^*-1=2^{63}+16845$ is prime. This is the smallest prime greater than 2^{63} for which $(p+1)/6$ is prime. The element (3,5) again lies on the curve $y^2=x^3-2$ and has order p.

$GF(2^m)$:
If we take m=127 there exists the extremely simple irreducible polynomial $g(x)=x^{127}+x+1$ and $p^*=(2^{127}+1)/3$ is prime. The element (x,x) has maximal order $2^{127}+1$ on the elliptic curve it generates.

Taking m=61 and generating $GF(2^{61})$ with the irreducible polynomial $G(x)=x^{61}+x^5+x^2+x+1$, we obtain elliptic curves of order $2^{61}+1=3p^*$ whereby $p^*=(2^{61}+1)/3$ is prime. The element (x,x) - the components being expressed in GF(2)[x]/(g(x)) - has order $2^{61}+1$ which is maximal on the elliptic curve it generates.

What follows is a list of exponents m for which $(2^m+1)/3$ is prime.

2 - 100: [3,5,7,11,13,17,19,23,31,41,43,47,53,59,61,71,79,83,89]
100 - 200: [101,107,113,127,131,137,149,167,173,179,191,197,199]
200 - 300: [227,233,239,251,257,263,269,281,293]
300 - 400: [311,313,317,341,347,353,359,383,389]
400 - 500: [401,419,431,443,449,461,467,479,491]
500 - 600: [503,509,521,557,563,569,587,593,599]
600 - 700: [617,641,647,653,659,677,683]
700 - 800: [701,719,743,761,773,797]
800 - 900: [809,821,827,839,857,863,881,887]

1500 - 1600: [1511,1523,1553,1559,1571,1583]
>1600 : [1601,1607,1613,1619,1637,...]

Acknowledgement

We thank Ueli Maurer for arising our interest in elliptic curves and Karl Aberer for his help with the computer programming. The first author also expresses his gratitude to Professor James L. Massey for being allowed to do this work as undergraduate research at his institute, for the support concerning the presentation at CRYPTO '89 and for showing him how to formulate a scientific text.

Bibliography

[Grosswald 1984]................Grosswald, Emil. Topics from the Theory of Numbers. Birkhaeuser Boston 1984.

[Hartshorne 1983]..............Hartshorne, Robin. Algebraic Geometry. Springer New York 1983.

[Husemoeller 1987].............Husemoeller, Dale. Elliptic Curves. Springer New York 1987.

[Kaliski 1987]......................Kaliski, Burton S. Jr.. "A Pseudo-Random Bit Generator Based on Elliptic Logarithms". Advances in Cryptography: Proceedings of CRYPTO '86. Andrew M. Odlyzko, Ed.. Springer 1987. pp. 84 - 100.

[Koblitz 1987].....................Koblitz, Neal. A Course in Number Theory and Cryptography. Springer New York 1987.

[Lidl Niederreiter 1983].....Lidl, Rudolf; Niederreiter, Harald. Finite Fields. Addison-Wesley Massachusetts 1983.

[Massey 1983]....................Massey, James L.."Logarithms in Finite Cyclic Groups - Cryptographic Issues". Proc. 4th Benelux Symposion on Information Theory, Leuven, Belgium. May 1983, pp.17 - 25.

[Miller 1986]......................Miller, Victor. "Use of Elliptic Curves in Cryptography". Advances in Cryptography: Proceedings of CRYPTO '85. H.C. Williams, Ed.. Springer 1986. pp. 417 - 426.

[Schoof 1985]....................Schoof, Rene. "Elliptic Curves over Finite Fields and the Computation of Square Roots mod p". Mathematics of Computation, vol.44 (1985), pp. 483-494.