Elliptic Curve Cryptography

Daniel Eisenberg

1 Elliptic curves as abelian groups

Given a field F, an elliptic curve E over F is defined as

$$E = \{(x, y) \in F^2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_5\}.$$

If F has any characteristic other than 2 or 3, the defining equation can be reduced to

$$y^2 = x^3 + bx + c. \tag{1}$$

For characteristic 3, the defining equation can be reduced to $y^2 = x^3 + ax^2 + bx + c$.

In the interest of inducing a group structure on E, we will also include a point O, called the *point at infinity*, which can be thought of as sitting at the extremes of the y-axis. We define O to have the property that all vertical lines in F^2 intersect O. For convenience, we will henceforth also refer to $E \cup \{O\}$ as simply E.

Suppose $F \cong \mathbb{R}$. Define a binary operation $+$ on E as follows, given points A and B on E,

1. If $A = O$, define $A + B = B$; if $B = O$, define $A + B = A$.
2. If $A \neq B$, define L as the line connecting A to B; if $A = B$, define L as the tangent line to the curve at A. Counted with multiplicity, L will intersect the curve at 3 points, A, B, and C. Define $A + B = -C$ where $-C$ is obtained by reflecting the point C about the x-axis.

It is clear from the above that $A + (-A) = O$. It can be shown that this operation is commutative and associative. Therefore we have an abelian group $(E, +)$ with identity element O. It can further be shown that this group exists regardless of our choice of F; though the geometric interpretations may not remain valid, algebraic interpretations of the $F \cong \mathbb{R}$ case extend to other fields. This in particular is the reason the simplified form of the defining equation for the curve does not apply to fields of characteristic 2 or 3: The slope of the tangent line to the curve at a point (x, y) can be found by implicit differentiation. In the case of equation (1), this is

$$\frac{3x^2 + b}{2y}$$

which for a field of characteristic 2 ensures all tangent lines are vertical, and for a field of characteristic 3 ensures all tangent lines are horizontal. These considerations require that the operation on fields of characteristic 2 or 3 include additional constraints; although the property that $A + B + C = O$ iff A, B, and C are colinear is preserved in these cases.

For cryptographic purposes, we will only consider finite fields $F \cong \mathbb{F}_{2^m}$ for large integers m and $F \cong \mathbb{F}_p$ for large primes p.

2 Cryptographic properties of elliptic curves over $\mathbb{F}_p$

Let p be a large prime and let E be an elliptic curve over $\mathbb{F}_p$.

Given an arbitrary $k \in \mathbb{F}_p$, there is approximately a 50% chance that k is a quadratic residue mod p. This means that approximately half of the elements in $\mathbb{F}_p$ correspond to x-coordinates of points on E, since the defining equation requires that the x-coordinates of points on the curve be perfect squares mod p.

Given two points A and B on E, we can compute $A + B$ in an acceptable amount of time, which is to say neither quickly nor unacceptably slowly, provided we have already mapped all points of E (by identifying the set of quadratic residues mod p). We define a multiplication $* : \mathbb{N} \times E \to E$ by repeated addition: given a point P on E and a positive integer k, $kP = P + \ldots + P$ for k copies of P.

We can now state the *elliptic curve discrete logarithm problem* (ECDLP) as follows, given points A and B on E, we want to find a positive integer k such that $B = kA$.

The ECDLP is believed to be intractable. This allows us to transform many algorithms which make use of the assumed intractability of the standard discrete logarithm problem (DLP) into algorithms making use of elliptic curves. The general formula for so doing involves rewriting steps which involve multiplication in $\mathbb{Z}_q$ for a prime q into addition on an elliptic curve E over $\mathbb{F}_p$, and, by extension, replacing exponentiaion mod q by multiplication on E. This technique has produced analogues of the Pohlig-Hellman attack on discrete logarithms, the baby step, giant step attack on discrete logarithms, the Diffie-Hellman key exchange algorithm, the ElGamal cryptosystem, and the ElGamal digital signature algorithm. These analogues are all correct, but the attacks are not computationally feasible provided E and p are well chosen.

Importantly, there is no known analogue for elliptic curves of the index calculus attack on discrete logarithms. This is because there is no known meaningful analogue of a small prime. This allows much smaller primes to be used to generate a computationally infeasible ECDLP than are required for a standard discrete logarithm problem.

One exception to this is the case of a *singular* elliptic curve, or an elliptic curve whose equation has repeated roots. On such curves the ECDLP can be reduced to the DLP. Thus we avoid singular curves for cryptographic applications of the ECDLP.

We now suspect we should be able to create a presumably secure public key cryptosystem using elliptic curves, since we have a problem which we believe to be intractable. However, we can only send points on a curve. In order to encode a message, we can use Koblitz's method:

First we represent the plaintext as a number m. We want to encode m in the x-coordinate of a point, but in order to do so, m must be a quadratic residue mod p. As previously noted, the probability that $m^3 + bm + c$ is a quadratic residue mod p is approximately $1/2$. In order to make several attempts at embedding m in a point $P_m \in E$, we choose an integer K such that $1/2^K$ is an acceptable probability of failing to encode the message. We assume that $(m + 1)K < p$ (otherwise we can chunk the message). If successful, we will encode m as $x = mK + j$ where $0 \leq j < K$. We accomplish this by adding each value of j to mK until $x^3 + bx + c$ is a quadratic residue mod p. The message is embedded as $P_m = (x, y)$ and we can recover the message by calculating $m = \lfloor x/K \rfloor$.

3 An ElGamal cryptosystem for elliptic curves

Suppose Alice wants to send a message to Bob. Bob chooses an elliptic curve E over a field $\mathbb{F}_p$ for a large prime p. Bob then chooses a point α on E and a secret integer a, and computes $\beta = a\alpha$. Bob then makes E, p, α, β public. Alice embeds the message m as $P_m \in E$, chooses a random integer k, and calculates

$$y_1 = k\alpha; y_2 = x + k\beta.$$

Alice then sends (y_1, y_2) (along with any necessary message recovery information, for example K from Koblitz's method) to Bob. Bob now decrypts the message by calculating

$$y_2 - ay_1 = x + k\beta - k\beta = x.$$

Basic elliptic curve analogues for ElGamal digital signatures and for the Diffie-Hellman key exchange algorithm involve similarly simple substitutions.

4 Brute force attacks on elliptic curve cryptosystems

Elliptic curve cryptosystems have been broken by brute force attacks. At present, no elliptic curve cryptosystem considered to be contemporarily cryptographically secure is known to have been broken. Cases of successful brute force attacks on such cryptosystems involve immense computational time and resources, and a brute force attack on a cryptosystem which meets minimum cryptographic standards requires several orders of magnitude more computational resources than the systems which have been broken.

5 Factoring composite numbers using elliptic curves

Elliptic curves can be used to factor composite numbers. This method is primarily useful when the composite n to be factored has roughly 40-50 digits; when n is smaller or larger there are faster alternatives. It is also useful for larger n which have relatively small prime factors (10-20 digits). The basic idea is to assume that n is prime, choose points on several elliptic curves over $\mathbb{Z}_n$, and multiply these points by large numbers. In the course of evaluating these multiplications, we will be forced to invert random elements of $\mathbb{Z}_n$, which of course is not always possible. When this fails, the point will fall outside the curve and we can investigate the value which was not invertible as a possible factor of n (it may be a composite of large primes, in which case little information will be gained).

This method is essentially the $p-1$ factoring method, but it is often feasible when, for a prime factor p of n, $p-1$ has large prime factors, while the $p-1$ method will generally fail in this case.

6 Identity-Based Encryption

One application of elliptic curve cryptography is a cryptosystem in which users have a public key which is a unique public identifier, such as their email address. In this way, someone sending a message can be assured they are encrypting it using the correct recipient's public key. This cryptosystem uses an elliptic curve with the defining equation $y^2 = x^3 + 1$ over $\mathbb{F}_p$ for a large prime p of the form $6q - 1$ for prime q. Such a curve is referred to as supersingular, and is not cryptographically secure for the ECDLP. However, there is a bilinear function $\tilde{e}$ which maps pairs of points (aP_0, bP_0) to q^{th} roots of unity $\forall a, b \in \mathbb{Z}$. Properties of this curve and function can be used to create a cryptosystem which relies on the difficulty of finding q^{th} roots of unity mod p (where q is secret). Meanwhile decryption is achieved by the bilinearity properties of $\tilde{e}$.

This system requires a trusted authority who computes users' private keys from their public keys by a secret integer s. This means that the security of the entire system relies exclusively on s remaining secret.

References

J. Bos and M. Kaihara, “PlayStation 3 computing breaks 2^{60} barrier. 112-bit ECDLP solved.”
From Labratory for Cryptographic Algorithms,
École Polytechnique Fédérale de Lausanne. http://lacal.epfl.ch/112bit_prime

[No author credit] “Certicom Announces Elliptic Curve Cryptography Challenge Winner.” From Certicom.
http://www.certicom.com/index.php/2004-press-releases/36-2004-press-releases/
300-solution-required-team-of-mathematicians-2600-computers-and-17-months-

B. Lynn “On the Implementation of Pairing-Based Cryptosystems.”
http://crypto.stanford.edu/pbc/thesis.pdf

W. Trappe and L. Washington, *Introduction to Cryptography with Coding Theory. Second Edition*, Pearson, 2006

E. Weisstein, “Elliptic Curve.” From MathWorld–A Wolfram Web Resource.
http://mathworld.wolfram.com/EllipticCurve.html