# ELLIPTIC CURVE CRYPTOSYSTEMS PROJECT
# FIRST MEETING
# FRIDAY JANUARY 24TH 1997

STEVEN GALBRAITH

This talk is a very basic introduction to elliptic curves. I will try not to assume any prior knowledge of algebra, though I don't explain what a finite field is. There is some mention of the cryptographic applications.

For a more complete introduction to both the mathematical background and the subject of elliptic curves I recommend the book "A Course in Number Theory and Cryptography" by Neal Koblitz (published by Springer-Verlag it can be found in most academic bookshops).

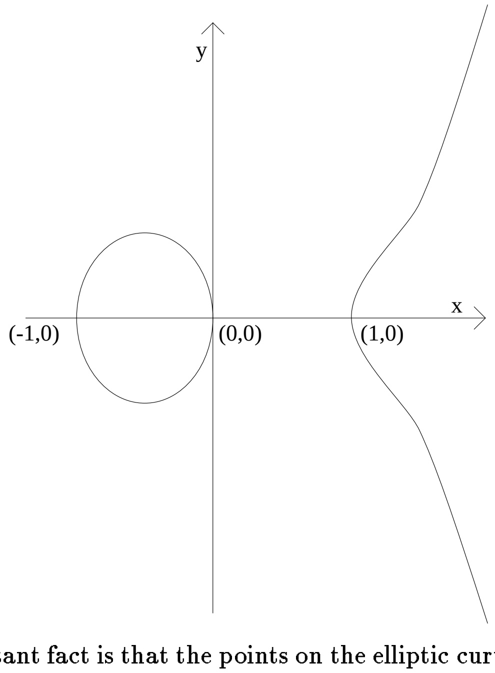
## 1. What is an elliptic curve?

An elliptic curve is an equation of the form

$$y^2 = x^3 + ax + b.$$

By this we mean that we choose fixed values for the numbers $a$ and $b$ and then consider the curve as the set of all the points $(x, y)$ which satisfy the equation.

For example, with $a = -1$ and $b = 0$, the set of points on the elliptic curve has the following graph.

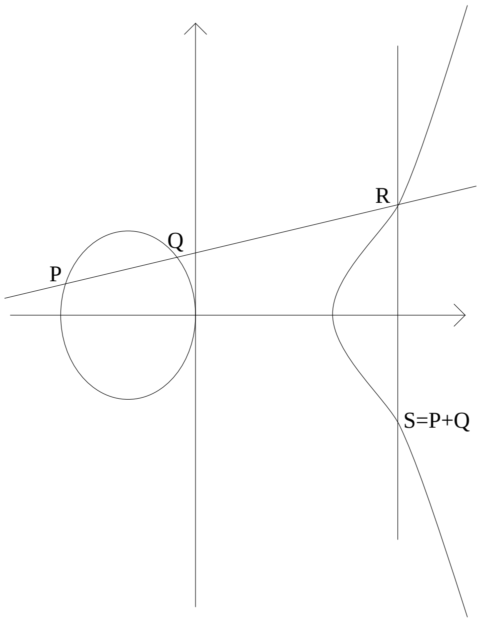



The really important fact is that the points on the elliptic curve have an "addition rule". By this it is meant that for any two points $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$

on the curve, there is a third point $P_3 = (x_3, y_3)$ which we call $P_1 + P_2$, and this addition rule satisfies the properties one would expect. Such an addition structure is called a "group" or "group law".

To construct this addition rule it is necessary to introduce the "point at infinity". This point cannot be written in coordinates as some $(x, y)$. We think of the point at infinity as having infinite $y$ value, and so it is thought of as sitting above the top of the page.

The geometric construction of the group law is the following. To add points $P$ and $Q$ first draw the line between them (if $P = Q$ then take the tangent line to the curve at $P$). This line will hit the curve at some other point $R$. Now draw the line from the point at infinity through $R$ (this line will be a vertical line, as we are considering the point at infinity to lie beyond the top of the page). This line now hits the curve at a third point $S$. The point $S$ is defined to be $P + Q$. For example we have the following picture.




The addition rule has the following properties.

- We write $O_E$ for the point at infinity. Then for all the points $P$ on the curve the addition law satisfies the condition $P + O_E = P$ (i.e., the point $O_E$ really is just like zero).
- For every point $P$ there is a special point $Q$ such that $P + Q = O_E$. We name this special point $-P$. We can then define "subtraction" by $R - S = R + (-S)$.
- For all points $P$ and $Q$ we have $P + Q = Q + P$.
- For all points $P, Q$ and $R$ we have $P + (Q + R) = (P + Q) + R$. This is the "associative" property which means we don't have to worry about which order we perform the additions in.

It is important to note that the addition rule can be described by some fairly simple formulae. Hence the addition of points may be performed purely algebraically; there is no need to draw lines on paper. Further, to compute $nP = P + P + \cdots + P$

($n$ times), we employ the usual "powering" method (in this case it is "doubling") which uses the binary expansion of $n$.

The addition rule works over the complex numbers $\mathbb{C}$, the real numbers $\mathbb{R}$, the rational numbers $\mathbb{Q}$ and also over finite fields $\mathbb{F}_q$ (where $q = p^n$ for some prime number $p$).

We are most interested in the case of elliptic curves over finite fields (i.e., we choose the numbers $a, b \in \mathbb{F}_q$). Since the field is finite there can only be a finite number of points $(x, y)$ on the curve.

For a point $P$ on the curve we define $\langle P \rangle$ to be the set $\{O_E, P, 2P = P + P, 3P = P + P + P, \ldots\}$. Sometimes the set $\langle P \rangle$ will actually contain every point on the curve, but it many cases it is not true that all the points lie in $\langle P \rangle$ for some point $P$.

For the purposes of cryptography we will choose a field $\mathbb{F}_q$, an elliptic curve (i.e., a choice of $a, b \in \mathbb{F}_q$) and also some point $P$ on the curve so that $\langle P \rangle$ is a reasonably large set. This initial data may be considered public knowledge.

## 2. The Elliptic Curve Discrete Logarithm Problem

Suppose we have some point $Q$ which lies in the set $\langle P \rangle$. Then $Q$ must be some multiple $tP$ of the point $P$. The discrete logarithm problem is to find the number $t$ from just $P$ and $Q$.

The first method which springs to mind to solve the discrete logarithm problem is to compute the points $O_E, P, 2P = P + P, 3P, \ldots$ until you come upon $Q$. When the size of the set $\langle P \rangle$ is large enough then this approach will not be efficient.

There are algorithms which are more effective than this naive approach, but the best known algorithms are still not very efficient.

The assumption on which elliptic curve cryptosystems are based is that there are no really good (by which we mean "sub-exponential") algorithms to solve this problem.

## 3. Elliptic Curve Cryptography

The way in which information is transmitted is through the number $t$ by sending the point $tP$. Here is an outline of the Diffie-Hellman key exchange protocol using elliptic curves.

**Diffie-Hellman key exchange.** Users A and B want to share a common key. Using a publicly known curve $E$ and point $P$ they do the following. User A chooses a number $t_A$ and sends the point $Q = t_A P$ to user B. User B chooses a number $t_B$ and sends $R = t_B P$ to user A. User A then computes the key $K = t_A R = t_A(t_B P) = (t_A t_B)P$. User B can also compute the key $K$ from $t_B Q = t_B(t_A P) = (t_A t_B)P$.

Hence the users A and B share a common key $K$. The point is that an eavesdropper would know $Q$ and $R$, but would not be able to construct $K$ without solving the discrete logarithm of either $Q$ or $R$.

There are several other cryptographic systems which may be adapted for use with elliptic curves. For instance the Massey-Omura and ElGamal systems may both be used (simply by rewriting multiplication as addition). Similarly, signature schemes using the above systems may also be implemented for elliptic curves.

## 4. Advantages and Disadvantages of Elliptic Curve Cryptosystems

It is anticipated that, because the fast discrete logarithm algorithms (index calculus techniques) don't seem to be applicable to elliptic curves, good levels of security should be attained using key sizes which are smaller then those needed for similar public key systems (like RSA, finite field methods etc). This is an important consideration now that key sizes for other public key systems are getting quite large. For example, it is hoped that 150 bits will be sufficient for the size of the finite field.

A point $P = (x, y)$ is determined by two field elements, so in general it is necessary to send two field elements in order to transmit a message (twice the amount of information for usual systems in finite fields). However $P = (x, y)$ is almost uniquely defined by just the value of $x$ and in some fields (for instance, characteristic 2 or modulo $p$ when $p \equiv 3 \pmod 4$) calculating square roots is easy. Therefore, for many applications, only the $x$-coordinate (and perhaps one other bit) need be sent.

Also, since the numbers involved are smaller, it is hoped that the process of encryption may be made to work faster then with existing systems. This gain in speed is offset by the fact that the formulae for addition on an elliptic curve are quite complicated.

Finally, for the advantages, there are a wide variety of different curves to choose from. Unfortunately many of these curves are not strong enough for cryptographic applications. In practice it may be better not to use many different curves.

The main concern about elliptic curve cryptosystems is that they are a fairly recent invention and so they have not had as thorough an analysis as other systems (for instance RSA). Only by further investigations into these systems can the cryptographic community develop trust that there are no efficient methods to solve the discrete logarithm problem.