

# Second Year Essay: Elliptic Curves in Cryptography

Robert Steele

April 2010

## 1 Introduction

In my essay, I will be looking at one approach to public key cryptography. Public key cryptography is a method of securely transferring information over a public domain. Various forms of public-key cryptography are used to transmit sensitive data, such as banking details, across the internet.

I will be looking at the use of Elliptic Curves for this purpose, and how these geometric objects have links to groups and number theory.

**Definition 1.1.** *Define a rational elliptic curve in Weistrass Normal Form as*

$$E : y^2 = f(x) = x^3 + ax^2 + bx + c$$

*contained within the projective plane. Where the roots of  $f(x)$  are distinct and  $a, b, c \in \mathbb{Q}$ .*

For our purposes, it will suffice to think of the projective plane as  $\mathbb{R}^2$  together with a 'point at infinity' and a curve in Weistrass normal form has a well defined tangent at every point.

Appendix A of Silverman/Tate[ST, p220] discusses the necessary projective geometry in more detail, that I have omit here.

**Definition 1.2.** *Define a rational point as a point  $(x, y)$  s.t.  $x, y \in \mathbb{Q}$ .*

I will denote the set of rational points on the curve  $E$  and the point at infinity as the set  $E(\mathbb{Q})$ .

I claim that if two rational points lie on an elliptic curve  $E$ , then there will be a third rational point on the curve or the point at infinity.

**Proposition 1.3.**  *$P, Q \in E(\mathbb{Q})$  Then the point on  $E$  found by considering the line passing through  $P$  and  $Q$ , denoted  $P * Q$ , is a rational point.*

*Proof.* Let  $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$  be rational points on the elliptic curve  $E : y^2 = x^3 + ax^2 + bx + c$ . Consider the line  $L$  intersecting  $P_1$  and  $P_2$ .

$$L : y = \alpha x + \beta, \text{ where } \alpha = \frac{y_2 - y_1}{x_2 - x_1} \text{ and } \beta = y_1 - \alpha x_1 = y_2 - \alpha x_2$$

If  $(x_2 - x_1) \neq 0$ , then  $\alpha$  is finite and we can then obtain the third point of intersection by the substitution:

$$y^2 = (\alpha x + \beta)^2 = x^3 + ax^2 + bx + c$$

Moving everything to one side gives us

$$x^3 + (a - \alpha^2)x^2 + (b - \alpha\beta)x + (c - \beta^2) = 0$$

The three roots of this cubic are the points at which  $L$  intersects  $E$ . Thus,

$$x^3 + (a - \alpha^2)x^2 + (b - \alpha\beta)x + (c - \beta^2) = (x - x_1)(x - x_2)(x - x_3)$$

Equating the coefficients of the  $x^2$  term on both sides, we see that  $(\alpha^2 - a) = x_1 + x_2 + x_3$ . Hence:

$$x_3 = (\alpha^2 - a) - x_1 - x_2 \text{ and } y_3 = \alpha x_3 + \beta$$

As all the terms on the RHS of the expression for  $x_3$  are rational,  $x_3$  must also be rational. Hence,  $y_3$  is also rational and  $(x_3, y_3)$  is a rational point.

If  $(x_2 - x_1) = 0$ , then  $P_1$  and  $P_2$  lie on a vertical line. We consider the point at infinity as the third intersection of  $L$  and  $E$ , which belongs to the set  $E(\mathbb{Q})$ .  $\square$

**Proposition 1.4.** *For  $P \in E(\mathbb{Q})$ , we can find a rational point on  $E$  found by considering the line tangent to  $E$  at  $P$ .*

*We will denote this rational point  $P * P$ .*

*Proof.* Let  $P = (x, y)$  be a rational point on the elliptic curve  $E : y^2 = x^3 + ax^2 + bx + c$ .

As we are only considering a single point, we cannot use the formula for  $\alpha$  we used above, but want to consider the tangent line to  $E$  at  $P$  in the same way as we consider the line through two rational points above.

By using the relation  $y^2 = f(x)$  and implicit differentiation we find:

$$\alpha = \frac{dy}{dx} = \frac{f'(x)}{2y}$$

If  $\alpha$  is finite, we can use  $\alpha$  as in the expression above and replacing  $y^2$  by  $f(x)$  as well as putting everything over a common denominator gives:

$$\text{x coordinate of } (x, y) * (x, y) = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c}$$

We can then conclude:

$$\text{y coordinate of } (x, y) * (x, y) = \frac{3x^2 + 2ax + b - 3x^4 - 4ax^3 - 6bx^2 - 12cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c} + y$$

If  $\alpha$  is not finite, then the tangent line to  $E$  at  $P$  is vertical. In this case, we designate the point at infinity as the third point on the line. Hence,  $(x, y) * (x, y) = \infty$ .

As the operation  $*$  has been defined, we must consider the cases where one, or both, of the points is the point at infinity.

To be consistent,  $P * \infty$  is the point on the vertical line drawn through  $P$ , the point directly above or below it on the curve  $E$ . If  $P$  is a point at which this vertical line is tangent to  $E$ , then  $P * \infty = P$ .

We define  $\infty * \infty = \infty$ . □

We now define the operation  $'+'$ , which I will also refer to as addition.

**Definition 1.5.**  $P, Q, O \in E(\mathbb{Q})$ . Define  $P + Q$  as  $(P * Q) * \mathbb{O}$  for a fixed  $O$ . We will also denote  $P + P$  as  $2P$ , where  $P + P = (P * P) * \mathbb{O}$

It is convenient to assign the point at infinity as the element  $\mathbb{O}$ . Then if  $P * Q = (x, y)$ ,  $P + Q = (x, -y)$ , removing the need to use the line intersection formulae above more than necessary.

However, note that this is merely convention and not necessary to the definition of the operation  $'+'$  on  $E$ . We will discuss this in more detail in the next section.

The set  $E(\mathbb{Q})$ , together with the operation  $P + Q$  forms a group, which I will formalise in the next section.

## 2 The Group of Rational Points on an Elliptic Curve

In order to form a group,  $E(\mathbb{Q})$  and the operation  $P + Q$  for rational points  $P$  and  $Q$ , must fulfill the axioms of Closure, Identity, Inverses and Associativity.

It was shown in the first section that the operation  $P * Q$  will always result in a third point in  $E(\mathbb{Q})$ . Hence,  $E(\mathbb{Q})$  will be closed under the operation  $P + Q$ .

The fixed rational point  $\mathbb{O}$  used in Defn 1.4 will be the identity element for the group. Take an arbitrary rational point,  $P$ , then:

$$(P + \mathbb{O}) = (P * \mathbb{O}) * \mathbb{O} = P$$

as the three points on  $L_P$  joining  $P$  and  $\mathbb{O}$  will be  $P, \mathbb{O}, (P * \mathbb{O})$ .

Inverses for arbitrary points can also be found.

**Definition 2.1.** Let  $S \in E(\mathbb{Q})$  be such that  $S = \mathbb{O} * \mathbb{O}$ . Then, for an arbitrary  $P \in E(\mathbb{Q})$ , define the inverse of  $P$ ,  $-P$  as  $P * S$ .

This is easily identified as the inverse of a point, using definitions 1.3 and 1.4:

$$(P) + (-P) = P + (P * S) = (P * (P * S)) * \mathbb{O} = S * \mathbb{O} = \mathbb{O}$$

It remains to show that Associativity holds in order to establish a group.

Let  $P, Q, R$  be three points on the curve. We want to prove that  $(P+Q)+R = P+(Q+R)$ . To get  $P+Q$ , we find  $P * Q$  and take the third intersection of the line through this point and  $\mathbb{O}$ . To add  $P+Q$  to  $R$ , we repeat this process, finding  $(P+Q) * R$  then considering the third intersection of the line through this point and  $\mathbb{O}$ .

It is sufficient to show that  $(P+Q) * R = P * (Q+R)$ , as this implies  $(P+Q)+R = P+(Q+R)$ .

In the proof of associativity, it is necessary to use a theorem that I will state, but not prove here. A proof may be found in Milne[JM, p27].

**Theorem 2.2.** *If two cubic curves in the projective plane intersect in exactly nine points, then every cubic curve passing through eight of the points also passes through the ninth.*

To form  $P * (Q+R)$ , we first have to find  $Q * R$ , join that to  $\mathbb{O}$ , and take the third intersection,  $Q+R$ . Then we must join  $Q+R$  to  $P$ , giving the point  $P * (Q+R)$ .

In figure 2.3[ST, p21], each of the points  $\mathbb{O}, P, Q, R, P * Q, P+Q, Q * R, Q+R$  lies on one of the dotted lines and one of the solid lines. If the intersection of the dotted line through  $P+Q$  and  $R$  and the solid line through  $P$  and  $Q+R$  lies on the cubic, then we have proven  $P * (Q+R) = (P+Q) * R$ .

We have nine points:  $\mathbb{O}, P, Q, R, P * Q, P+Q, Q * R, Q+R$  and the intersection of the two lines. As a line has a linear equation, and if you have three linear equations and multiply them together, we obtain two cubics through the nine points. The set of solutions to each cubic equation is just the union of the three lines.

Now applying theorem 2.2, taking for  $C_1$  the union of the three dotted lines and for  $C_2$  the union of the three solid lines. By construction, these two cubics go through the nine points. But the original cubic curve  $C$  goes through eight of the points, and therefore it goes through the ninth. Thus, the intersection of the two lines lies on  $C$ , which proves that  $(P+Q) * R = P * (Q+R)$ .

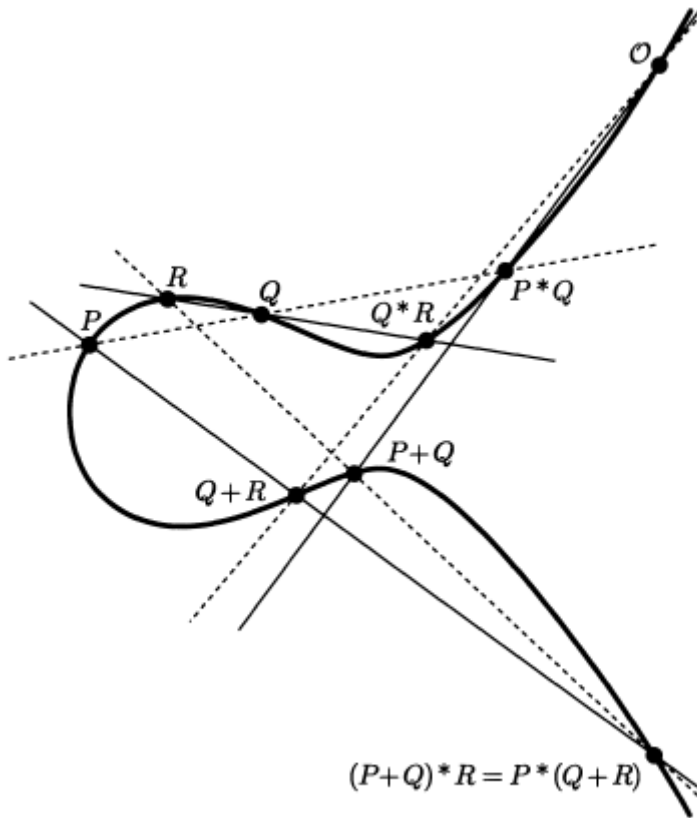


Diagram 2.3: Verifying the Associative Law

## 2.1 Choice of Zero Element

As mentioned at the end of the previous section, it is conventional to choose the point at infinity as the identity element of the group,  $\mathcal{O}$ .

This is only for computational ease, we can choose a different rational point on  $E$ , say  $\mathcal{O}'$  as the identity element and we get a group with the same structure. In fact [ST, p21], the map

$$P \mapsto P + (\mathcal{O}' - \mathcal{O})$$

is an isomorphism between the groups with the different identity elements.

## 3 Cryptography

We will now look at some applications of the group properties of elliptic curves to public-key cryptography.

Public-key cryptography is the secure transfer of information between two parties through a public domain, without establishment of key beforehand.

Today, public-key encryption is used to transfer sensitive information, such as

bank details, over the internet.

In the following examples I will consider the transfer of data from 'Alice' to 'Bob' over the internet. As there is a chance of interception of data during transfer, anything sent between Alice and Bob will be considered 'public information'.

A successful public-key encryption algorithm would allow Alice and Bob to transfer information easily between themselves without a third party, who has access to all the public information, being able to deduce the information.

### 3.1 Elliptic Curves Over Finite Fields

In cryptography, instead of considering elliptic curves over  $\mathbb{Q}$  as before, we consider elliptic curves over a finite field  $\mathbb{F}_q$ , where  $q$  is often a large prime.

We can use the algebraic formulae for point addition derived in Proposition 1.3 to calculate the addition of points in  $\mathbb{F}_q$ , using the standard operations for addition, subtraction, multiplication modulo  $q$  and using multiplication by inverses in the field to replace division.

The necessary inverses can be calculated using an adaptation of the euclidean algorithm [HMV, p40].

For example, let us consider  $E(\mathbb{F}_{29})$ [HMV, p80] where:

$$E : y^2 = x^3 + 4x + 20$$

Then the points in  $E(\mathbb{F}_{29})$  are:

$\infty$  (2, 6) (4, 19) (8, 10) (13, 23) (16, 2) (19, 16) (27, 2)  
(0, 7) (2, 23) (5, 7) (8, 19) (14, 6) (16, 27) (20, 3) (27, 27)  
(0, 22) (3, 1) (5, 22) (10, 4) (14, 23) (17, 10) (20, 26)  
(1, 5) (3, 28) (6, 12) (10, 25) (15, 2) (17, 19) (24, 7)  
(1, 24) (4, 10) (6, 17) (13, 6) (15, 27) (19, 13) (24, 22)

Examples of addition of points are:

$$(5, 22) + (16, 27) = (13, 6)$$

$$2(5, 22) = (14, 6)$$

### 3.2 The Discrete Logarithm Problem

The Discrete Logarithm problem states:

For  $a, b \in \mathbb{F}_p$ , where  $p$  is a large prime, find  $k$  such that:

$$a^k = b \pmod{p}$$

This problem is computationally difficult with current technology (non-quantum computers) if  $p$  is chosen sufficiently well. The problem is the basis for public key cryptography and discussed in many cryptography texts. [DS, §5.1][KN, p97]

By using elliptic curves over finite fields, we can construct a similar problem, retaining the computational difficulty:

The Elliptic Curve Discrete Logarithm Problem (ECDLP) states [HMV, p153]: Given an elliptic curve  $E$  over a finite field  $\mathbb{F}_q$ , a point  $P \in E(\mathbb{F}_q)$  of order  $n$ , and a point  $Q \in \langle P \rangle$ , find the integer  $l \in [0, n - 1]$  such that  $Q = lP$ .

Using this problem, we can establish cryptographic methods, based on its difficulty.

### 3.3 Diffie-Hellman Key Exchange [W, p170]

Alice and Bob first agree on an Elliptic Curve  $E$  over a finite field  $\mathbb{F}_q$  such that the ECDLP is hard in  $E(\mathbb{F}_q)$ . They also decide on a point  $P \in E(\mathbb{F}_q)$  such that the subgroup generated by  $P$  has large order.

All the above is considered public information.

1. Alice chooses  $a \in \mathbb{Z}$ , computes  $P_a = aP$ , and sends  $P_a$  to Bob.
2. Bob chooses  $b \in \mathbb{Z}$ , computes  $P_b = bP$ , and sends  $P_b$  to Alice.
3. Alice computes  $aP_b$ .
4. Bob computes  $bP_a$ .
5. As  $aP_b = bP_a$ , Alice and Bob can use a public method to extract a key from this point in  $E(\mathbb{F}_q)$ . For example, the last 50 digits of the x coordinate.

The eavesdropper in this method needs to solve the following problem:

#### Diffie-Hellman Problem:

Given  $P$ ,  $P_a$  and  $P_b$  in  $E(\mathbb{F}_q)$ , compute  $aP_b = bP_a$ .

If the eavesdropper can solve the ECDLP in  $E(\mathbb{F}_q)$ , then they can use  $P$  and  $P_a$  to find  $a$ . Then they can compute  $aP_b$ . However, it is not known if  $aP_b$  can be computed without solving the computationally difficult ECDLP.

### 3.4 Massey-Omura Encryption [W, p173]

One method for Alice to send a message to Bob without pre-establishing a key is the following:

- Alice puts her message in a box and puts her lock on it.
- She sends the box to Bob.
- Bob puts his lock on it and sends it back to Alice.
- Alice takes her lock off the box and sends the box back to Bob.

- Bob removes his lock and reads the message.

We can use the properties of  $E(\mathbb{F}_q)$  to implement this method mathematically:

1. Alice and Bob agree on an elliptic curve  $E$  over a finite field  $\mathbb{F}_q$  such that the ECDLP is hard in  $E(\mathbb{F}_q)$ . Let  $N = \#E(\mathbb{F}_q)$ , the number of elements in  $E(\mathbb{F}_q)$ .
2. Alice represents her message as a point  $M$  in  $E(\mathbb{F}_q)$ . We will not discuss how to represent the message as a point here, but Washington[W, p174] describes a method proposed by Koblitz.
3. Alice chooses a secret integer  $m_A$  with  $\gcd(m_A, N) = 1$ , computes  $M_1 = m_A M$  and sends  $M_1$  to Bob.
4. Bob chooses a secret integer  $m_B$  with  $\gcd(m_B, N) = 1$ . Computes  $M_2 = m_B M_1$  and sends it to Alice.
5. Alice computes  $m_A^{-1}$  in  $E(\mathbb{F}_q)$ . She computes  $M_3 = m_A^{-1} M_2$  and sends  $M_3$  to Bob.
6. Bob computes  $m_B^{-1}$  in  $E(\mathbb{F}_q)$ . He computes  $M_4 = m_B^{-1} M_3$ . Then  $M_4 = M$  is the message as:

$$M_4 = m_B^{-1} m_A^{-1} m_B m_A M = M$$

The eavesdropper in this method knows  $E(\mathbb{F}_q)$  and the points  $m_A M$ ,  $m_B m_A M$  and  $m_B M$ .

Let  $a = m_A^{-1}$ ,  $b = m_B^{-1}$ ,  $P = m_A m_B M$ .

Then the eavesdropper knows  $P$ ,  $bP$ ,  $aP$  and wants to find  $abP$ . This is the Diffie-Hellman problem as in the previous method.

This procedure works with any finite group but is rarely used in practice.

### 3.5 Comparison to RSA

Elliptic Curve Cryptography(ECC) is one of the most widely used public-key cryptographic methods, together with RSA encryption.

RSA encryption uses the computational difficulty of factorisation of the product of two large prime numbers as the basis for encryption.

It is thought ECC provides the same level of security as an RSA based system, but requires less data. Washington[W, p169] claims that 4096 bits of RSA encryption give the same level of security as 313 bits in an ECC system.

This reduction in space required reduces storage and transmission requirements for the encryption system.

Washington[W, p169] also describes ECC systems as being faster to generate, quoting a trial where a 512 bit RSA key took 3.4 minutes to generate, whereas

an equivalent ECC system, a 163 bit ECC-DSA key, took 0.597 seconds under the same conditions.

Despite verification taking slightly longer than in an RSA system, ECC systems provide benefits over the more widely used RSA system in many circumstances.

## 4 Bibliography

[ST] *Rational Points on Elliptic Curves*. Joseph H. Silverman, John Tate  
*Springer-Verlag*

[K] *Elliptic Curves*. Anthony W. Knap *Princeton University Press*

[MM] *Elliptic Curves*. Henry McKean, Victor Moll *Cambridge Univeristy Press*

[HMV] *Guide to Elliptic Curve Cryptography*. Hankerson D., Menezes A., Vanstone S.

[DS] *Cryptography: Theory and Practice*. Douglas Stinson

[KN] *A Course in Number Thoery and Cryptography*. Koblitz N.

[W] *Elliptic Curves: Number Theory and Cryptography*. Lawrence C. Washington

[JM] *Elliptic Curves*. J.S.Milne