Math Final Project: An Introduction to Elliptic Curves and their Cryptographic Applications

Kaitlyn Hernon

December 2024

1 Introduction

For my final project, I will outline the basics of elliptic curves and explain the importance of elliptic curves in cryptography. This paper will begin with an overview of elliptic curves and how they are defined, before moving into their applications in cryptography. Elliptic Curve Cryptography (ECC) is a form of public-key cryptography that is more efficient and secure than its alternatives.

The idea of using elliptic curves in cryptography was proposed by Victor Miller and Neal Koblitz in 1985, becoming popular and widely used by the early 2000s.

2 Defining Elliptic Curves

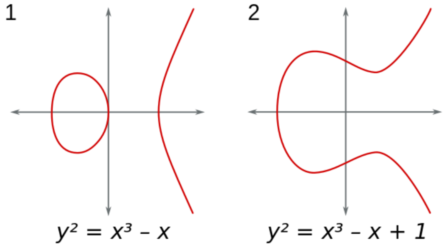


Figure 1: Elliptic Curves

A cubic F defined over k is an elliptic curve defined over k if and only if $F(k) \neq \phi$ and it is non-singular.

Consider two curves F and G defined over k, and let $\varphi : F \to G$ be a rational map defined over k. We say that φ is **birational** if there exists a rational map $\psi : G \to F$, defined over k, such that for "almost all" the points of F(k) and G(k), the maps $\psi \circ \varphi$ and $\varphi \circ \psi$ defined and equal to the identity. We say that

F and G are **birationally equivalent** over k, if there exists a birational map φ from F to G defined over k.

Two elliptic curves defined over k are said to be **equivalent** over k if there exists a birational map, defined over k, from one to the other

2.1 Definition

An elliptic curve is of the form $y^2 = x^3 + Ax + B$ and is also naturally a group. [1] An elliptic curve must be **non-singular**, or, the curve cannot have any cusps or overlaps. This means the discriminant must be non-zero, or:

$$4a^3 + 27B^2 \neq 0$$

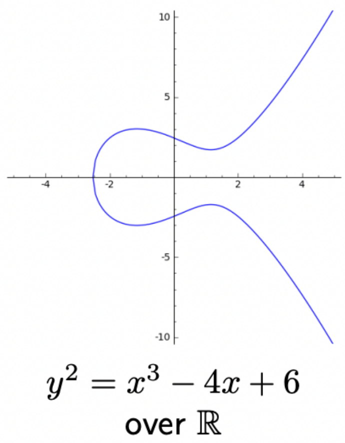


Figure 2:

2.2 Addition on Elliptic Curves (mod p)

What makes elliptic curve cryptography so effective is the simplicity of computing scalar multiplication of a point P times constant a on an elliptic curve E, in hand with the difficulty of calculating a given just the point P and the product point.

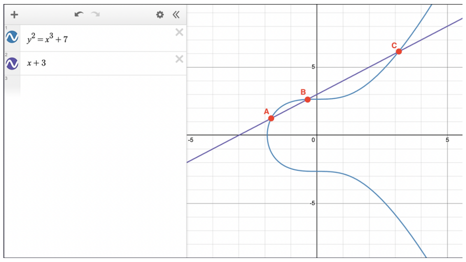
Let p be a prime. An elliptic curve E (mod p) is the set of all the points (x,y) with $0 \leq x, y < p$ satisfying the equations $y^2 \equiv x^3 + bx + c \pmod{p}$, $0 \leq b, c < p$

Let $(x_1, y_1) \oplus (x_2, y_2) = (x_3, y_3)$ where $x_3 = m^2 - x_1 - x_2$ and $y_3 = m(x_1 - x_3) - y_1$.

[1] https://math.mit.edu/classes/18.783/2017/Lecture1.pdf

Where $m \equiv$

$$\begin{cases} (y_2 - y_1)(x_2 - x_1)^-1(\text{mod p}) & (x_1, y_1) \neq (x_1, y_1) \\ (3x_1^2 + b)(2y_1)^-1(\text{mod p}) & (x_1, y_1) = (x_1, y_1) \end{cases}$$



$A \oplus B = C$
$B \oplus C = A$
$A \oplus C = B$

3 Cryptography

3.1 What is RSA?

RSA is a common and widely used type of public-key encryption that encodes messsages using public and private keys. It serves as a base model for most public-key encryption algorithms.

Public key: Positive integers n and e $n = pq$ where p and q are primes, and $gcd(e, \phi(n)) = 1$ $(\phi(n) = (p-1)(q-1))$

Private key: $d \equiv e^-1(\text{mod } \phi(n))$

To encrypt: $\varepsilon(m) \equiv m^e(\text{mod } n)$

To decrypt: $D(m) \equiv m^d(\text{mod } n)$

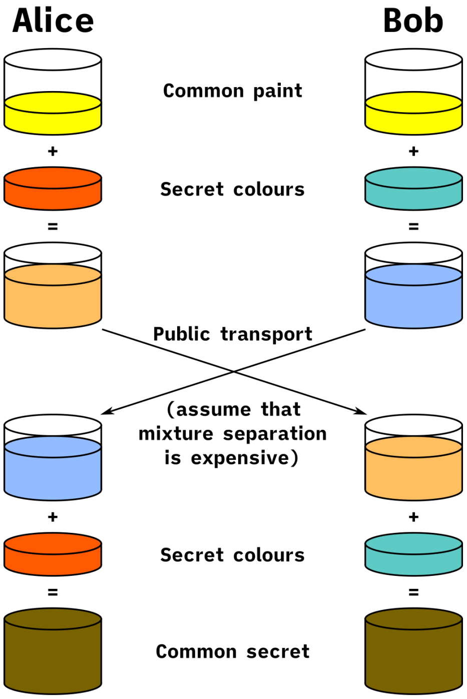
3.2 Why use Elliptic Curve Cryptography?

Elliptic Curve Cryptography offers many benefits for security. It achieves the same level of security as RSA and other strong encryption algorithms, but with significantly smaller key sizes. A 256-bit elliptic curve cryptography key is equivalent to a 3072-bit RSA key in terms of security strength. [2]

3.3 How does Elliptic Curve Cryptography Wok?

In elliptic curve cryptography, each user has a public key, that is used to send an encrypted message, and a private key, that is used to decrypt encrypted messages.

[2] `https://nordvpn.com/blog/elliptic-curve-cryptography/`



3.3.1 Diffie-Hellman Key Exchange

The Diffie-Hellman key exchange was published in the 1970s, and was the first example of a public-key cryptography algorithm that used a public and private key. How it works:

1. Alice and Bob choose an elliptic curve E over a finite field $\mathbf{F}_n$ such that the discrete log problem on $E(F_n)$ is nontrivial. Alice and Bob also choose a point $P \in E(F_n)$ where the subgroup generated by P is large.

2. Alice selects an integer a and Bob chooses an integer b.

3. Alice computes and sends aP to Bob, and Bob computes and sends bP to Alice. Alice's key $aP := P \oplus P \oplus ... \oplus P$, adding P a times.

4. Alice uses a to compute $a(bP)$ and Bob uses b to compute $b(aP)$.

5. Alice and Bob will extract a key from the value abP.

[3]

3.3.2 Tripartite Diffie-Hellman Key Exchange

Published in 2000, Antoine Joux proposed a version of Diffie-Hellman with three participants using the Tate pairing.

[3] https://dc.ewu.edu/cgi/viewcontent.cgi?article=1159&context=theses

3.3.3 The Tate Pairing

The Tate Pairing is a symmetric bilinear function that maps two points on an elliptic curve to an element of a field. It is defined as the following

$E(F_q)_N \times \frac{E(F_q)}{NE(F_q)} \to \frac{F_q^*}{(F_q^*)^N}, (P, Q) \to \langle P, Q \rangle_{Tate}$

1. Choose a prime $p > 2^{1000}$, an elliptic curve E/F_p and a point $S \in E(F_p)$ of order N with $p \equiv 1 \pmod{N}$.

2. Alice, Bob, and Carl choose secret keys *a, b,* and c, respectively.

3. Alice publishes $A = aS$, Bob publishes $B = bS$, and Carl publishes $C = cS$

4. Alice computes $\langle B, C \rangle^a_{Tate}$, Bob computes $\langle A, C \rangle^a_{Tate}$, and Carl computes $\langle A, B \rangle^a_{Tate}$ [4]

5. They all end up with the shared secret $\langle S, S \rangle^{abc}_{Tate}$

3.4 Real World Applications

Where is this kind of cryptography used In our world, elliptic curve cryptography is one of the most secure and commonly used cryptographic algorithms. It is used in all kinds of technological systems that we use in our daily life.

- Online banking and payments
- Email encryption
- Cryptocurrency & blockchain (Bitcoin)

4 Conclusion

Elliptic Curve Cryptography is a strong, secure, and efficient system. Its smaller key sizes make it advantageous over other alternative systems. We can apply content for our class to real world applications.

References

[1] https://dc.ewu.edu/cgi/viewcontent.cgi?article=1159\&context=theses

[2] https://nordvpn.com/blog/elliptic-curve-cryptography/

[3] http://honors.cs.umd.edu/reports/ECCpaper.pdf

[4] https://enge.math.u-bordeaux.fr/publications/buch.pdf

[5] https://math.uchicago.edu/~may/REU2020/REUPapers/Perez-Stark.pdf

[4] https://www.math.brown.edu/johsilve/Presentations/WyomingEllipticCurve.pdf

[6] https://www.umsl.edu/~siegelj/information_theory/projects/elliptic_curves_group_law.pdf

[7] https://www.math.brown.edu/johsilve/Presentations/WyomingEllipticCurve.pdf

[8] https://www.math.purdue.edu/~arapura/preprints/shimura1.pdf

[9] https://math.mit.edu/classes/18.783/2017/Lecture1.pdf

[10] https://www.math.columbia.edu/~avizeff/Fermat/Hellegouarch-Schneps.pdf