Apr 12th, 2:00 PM - 3:00 PM

Elliptic Curves and Cryptography

Linh Nguyen
Illinois Wesleyan University

Andrew Shallue, Faculty Advisor
Illinois Wesleyan University

Cryptography and Elliptic Curves

Linh Nguyen   *Illinois Wesleyan University*

Summary

Cryptography plays an important role in todays world since security is one of the main concerns for the safety of everyone. In our current research project, we are considering using the Icart function to map the corresponding elements from the set of remainders mod p(p is a prime congruent to 2 mod 3) to the points(x,y) on the elliptic curve in order to encode the data. A survey is presented on these topics, including information about the elliptic curves, Icart function and their application to the Diffie Hellman system.

Elliptic curve

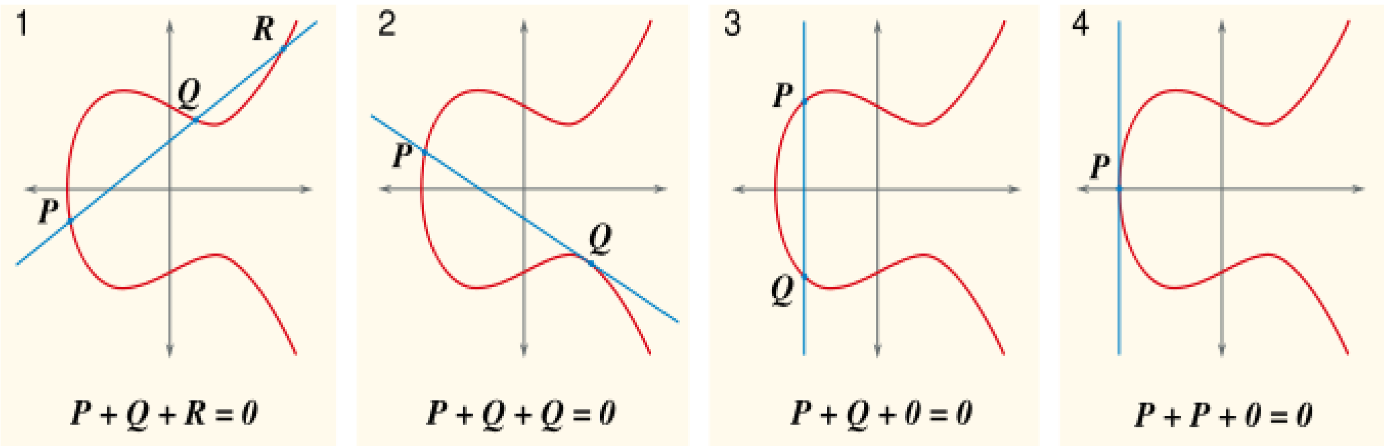
Definition: An elliptic curve (E) over field K is the graph of an equation: $(E): y^2 = x^3 + ax + b$ $(field \neq 2, 3)$ (discriminant $\Delta = 4A^3 + 27B^2$) where K is: complex numbers $\mathbb{C}$, real numbers $\mathbb{R}$, rational numbers $\mathbb{Q}$, finite field(integers mod p ($\mathbb{F}_p$)) , etc. ; a and b are elements of K.
Any elliptic curve of characteristic 2, 3 can be written in Legendre normal form:
y_2=x(x - 1)(x - λ) (a,b,c,d and e are elements of K)

Note: When we have the elliptic curve over complex numbers, we will get the torus.

Properties of the elliptic curve:
Addition:

Let $(E): y^2 = x^3 + ax + b$ (where characteristic of field is not 2 or 3) be an elliptic curve over a field K and $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be points of $(E)(P_1, P_2 \neq \infty)$. We define $P_1 + P_2 = P_3$ where $P_3 = (x_3, y_3)$. We have the following cases [6]:

- If $x_1 \neq x_2(P_1 \neq P_2)$ then $x_3 = m^2 - x_1 - x_2, y_3 = m(x_1 - x_3) - y_1$ and $m = (y_2 - y_1)/(x_2 - x_1)$
- If $x_1 = x_2$ and $y_1 \neq y_2(P_1 \neq P_2)$ then: $P_1 + P_2 = \infty$
- If $P_1 = P_2$ and $y_1 \neq 0$ then: $x_3 = m^2 - x_1 - x_2, y_3 = m(x_1 - x_3) - y_1$ where $m = (3x_1^2 + a)/(2y_1)$
- If $P_1 = P_2$ and $y_1 = 0$ then $P_1 + P_2 = 2P_1 = \infty$



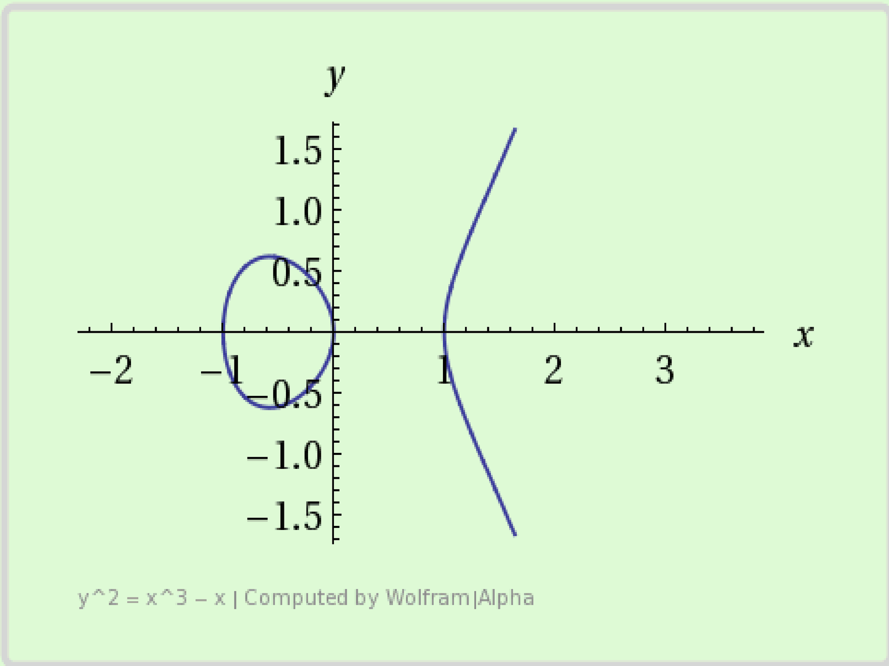
[4]

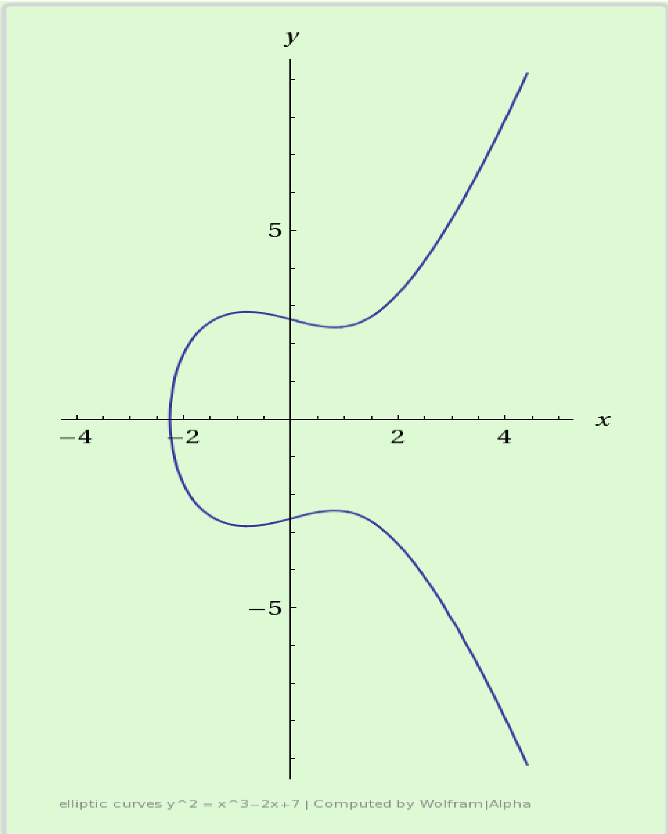
Note:

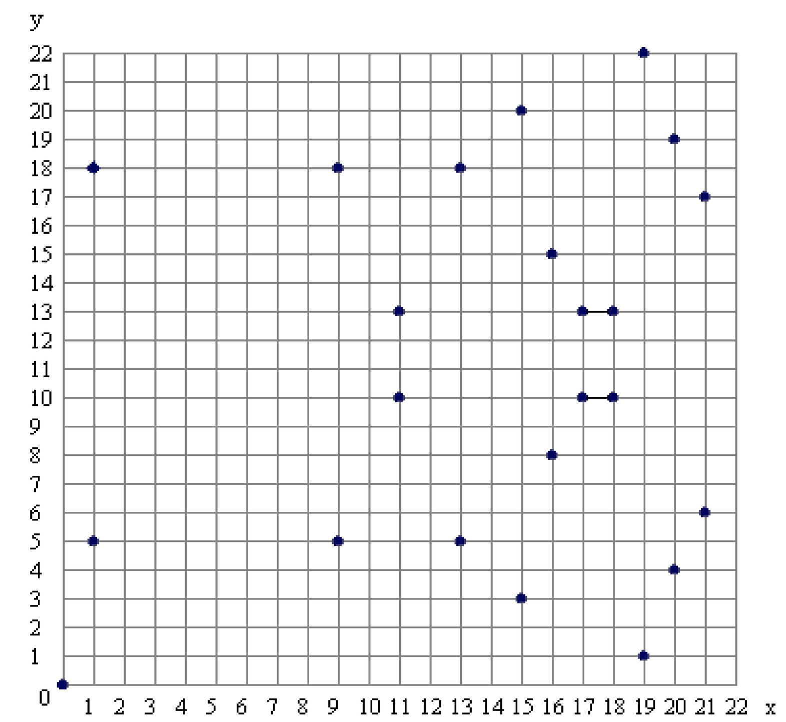
1. $P + \infty = \infty + P = P$
2. $P + (-P) = \infty$
3. $P + (Q + R) = (P + Q) + R$
4. $P + Q = Q + P$

[6]

Pictures of the Elliptic Curves







Elliptic curve equation: $y^2 = x^3 + x$ over F_{23}

[3, 7]

Icart's Function

Icart's Function is one way to match the messages that are used to transfer among organizations or people to the points on the elliptic curve.

Elliptic curve with $p = 2 \mod 3$
$E_{a,b}: y^2 = x^3 + ax + b \mod \text{p}$

Icart's Function[5, 1]:
$f_{a,b}: \mathbb{F}_p \longmapsto E_{a,b}$
$u \longmapsto (x, y)$

$x = (v^2 - b - u^6/27)^{(2p-1)/3} + \frac{u^2}{3}$
$y = ux + v$
$v = \frac{(3a-u^4)}{6u}$

The research goal is to increase the number of collisions so that the more points on the elliptic curve got hit by the values of u mapped to them.

Diffie-Hellman key exchange

Diffie Hellman Protocol

Alice and Bob side

Alice and Bob want to establish a key for communicating. The Diffie-Hellman scheme for accomplishing this is as follows [2]:

1. Either Alice or Bob selects a large, secure prime number p and a primitive root α (mod p). Both p and α can be made public.
2. Alice chooses a secret random x with $1 \leq x \leq p - 2$ and Bob selects a secret random y with $1 \leq y \leq p - 2$
3. Alice sends a^x (mod p) to Bob, and Bob sends a^y(mod p) to Alice.
4. Using the messages that they each have received, they can each calculate the session key K. Alice calculates K by K $\equiv (a^y)^x$ (mod p) and Bob calculates K by K$\equiv (a^x)^y$ (mod p)

Alice		Bob
compute aP	$\rightarrow$	$b(aP)$
$a(bP)$	$\leftarrow$	compute bP

Attacker side

Here is how the intruder in the middle attack works [2]:

1. Eve chooses an exponent z.
2. Eve interpretes a^x and a^y.
3. Eve sends a^z to Alice and Bob (Alice belives she is receiving a^y and Bob believes he receives a^x).
4. Eve computes $K_{AE} \equiv (a^x)^z$ (mod p) and $K_{EB} \equiv (a^y)^z$ (mod p). Alice, not realizing that Eve is in the middle, also computes K_{AE} and Bob computes K_{EB}.
5. When Alice sends a message to Bob, encrypted with K_{AE}, Eve interpretes it, deciphers it, encrypts it with K_{EB} and sends it to Bob. Bob decrypts with K_{EB} and obtains the message. Bob has no reason to belive communication was insecure. Meanwhile , Eve is reading the juicy gossip that she has obtained.

Alice		Bob	Eve
compute aP	$\rightarrow$	$b(aP)$	$c(aP)$
$a(bP)$	$\leftarrow$	compute bP	$c(bP)$

References

[1] Pierre-Alain Fouque and Mehdi Tibouchi, *Estimating the size of the image of deterministic hash functions to elliptic curves*, Cryptology ePrint Archive, Report 037, 2010.

[2] Wade Trappe and Lawrence Washington, **Introduction to cryptography with coding theory**, second edition, Pearson Prentice Hall, New Jersey, 2006.

[3] Wolfram Alpha, `http://www.wolframalpha.com/`

[4] Wikipedia, `http://en.wikipedia.org/wiki/Elliptic_curve`

[5] Jean Sebastien Coron, `http://www.jscoron.fr/cours/mics3crypto/shash.pdf`

[6] Joseph H. Silverman, `http://www.math.brown.edu/~jhs/Presentations/WyomingEllipticCurve.pdf`

[7] certicom, `https://www.certicom.com/index.php/31-example-of-an-elliptic-curve-group-over-fp`