Elliptic Curves and Cryptography

Linh Nguyen
Illinois Wesleyan University

Andrew Shallue, Faculty Advisor
Illinois Wesleyan University

Follow this and additional works at: https://digitalcommons.iwu.edu/jwprc

Part of the Applied Mathematics Commons

Nguyen, Linh and Shallue, Faculty Advisor, Andrew, "Elliptic Curves and Cryptography" (2014). John Wesley Powell Student Research Conference. 17.
https://digitalcommons.iwu.edu/jwprc/2014/posters2/17

This Event is protected by copyright and/or related rights. It has been brought to you by Digital Commons @ IWU with permission from the rights-holder(s). You are free to use this material in any way that is permitted by the copyright and related rights legislation that applies to your use. For other uses you need to obtain permission from the rights-holder(s) directly, unless additional rights are indicated by a Creative Commons license in the record and/ or on the work itself. This material has been accepted for inclusion by faculty at Illinois Wesleyan University. For more information, please contact digitalcommons@iwu.edu.
©Copyright is owned by the author of this document.
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 to a prime congruent to 2 mod 3 to the points 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:

\[ y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \]

(field \( \neq 2,3 \)) (discriminant \( \Delta = -4a_4^3 - 27a_6^2 \)) where K is in complex numbers C, real numbers R, rational numbers 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:

\[ y^2 = x^3 + a_1 x^2 + a_2 x + a_3 \]

where characteristic of field is not 2, 3 (Discriminant \( \Delta = 4a_1^3 + 27a_2^2 \) = 0, finite field( integers mod p (\( \mathbb{F}_p \)) = 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31). If \( \Delta = 0 \), then we have a singular curve, i.e., a curve with a singular point at (0,0).

Properties of the elliptic curve:

Addition:

- If \( P \neq Q \), then \( P + Q \) is defined as the inverse of \( P - Q \) on the elliptic curve.
- If \( P = Q \), then \( P + Q \) is defined as the inverse of \( 2P \) on the elliptic curve.

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.

\[ \begin{align*}
\text{Icart Function} : & f_{\mathbb{F}_p} : E_{\mathbb{F}_p} \\
& u \mapsto (x, y) \\
& x = (s^2 - 8 - u^2/627)^{2p-1/3} + \frac{u}{6} \\
& y = u^2 + 1 - 3a - 5x \\
& v = \frac{1}{6}x
\end{align*} \]

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.

Pictures of the Elliptic Curves

[Image]

Diffie-Hellman key exchange

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 a (mod p).
2. Both p and a can be made public.
3. Alice chooses a secret random x with \( 1 \leq x \leq p - 2 \) and Bob selects a secret random y with \( 1 \leq y \leq p - 2 \).
4. Alice sends \( a^x \) (mod p) to Bob, and Bob sends \( a^y \) (mod p) to Alice.

Attacker side

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

1. Eve chooses an exponent z.
2. Eve interprets \( a^z \) and \( a^z \).
3. Eve sends \( a^z \) to Alice and Bob (Alice believes she is receiving \( a^z \) and Bob believes he receives \( a^z \)).
4. Eve computes \( K_{AE} \equiv (a^z)^x \) (mod p) and \( K_{EB} \equiv (a^z)^y \) (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 interprets it, deciphers it, and encrypts it with \( K_{EB} \) and sends it to Bob. Bob decrypts with \( K_{EB} \) and obtains the message. Bob has no reason to believe communication was insecure. Meanwhile, Eve is reading the juicy gossip that she has obtained.

References