Keeping your data safe using Number Theory and Abstract Algebra

Supragyapal Singh, joined with Khoa Bui

Concordia University of Edmonton
Department of Mathematical and Physical Sciences

Abstract

Elliptic curve cryptography (ECC) is one of the most popular modern cryptosystems being used in secure data transmission because of its efficiency, yet providing the equivalent security to cryptosystems not based on elliptic curves. In this presentation, we will discuss the mathematical background behind cryptosystems that are based on the algebraic structure of elliptic curves over finite fields. Furthermore, we will present real-life applications of ECC by introducing the Diffie-Hellman key exchange and El Gamal asymmetric cryptosystem.

Fig. 1: Source: Hartnett [1].

Cryptographic Background

- Cryptography helps to safely transfer our data and confidential information.
- Crytography even helped the Allied win World War 2.

Modern Cryptography has the following components:

- **Plaintext data**: is the unencrypted data.
- **Ciphered data**: is the encrypted data.
- **Encryption**: is the process of encoding information in a way that only authorized parties can access via decryption.
- **Decryption**: is the process of decoding information.

Fig. 2: The Machine the Allied Used to Break the Enigma Code [3].

Mathematical Background

- A **finite field** $\mathbb{F}$ is a finite set of numbers which is closed under addition and multiplication, and every element in $\mathbb{F}$ has its negation in $\mathbb{F}$, every non-zero element in $\mathbb{F}$ has its inverse in $\mathbb{F}$. For each prime number p, there is a unique finite field of p elements, denoted by $\mathbb{F}_p$.
- Consider the finite field $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$ of 5 elements which is obtained by taking integers modulo 5.

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

×	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Fig. 3: Arithmetic in the finite field $\mathbb{F}_5$.

Elliptic Curve

An **elliptic curve** E over a field $\mathbb{F}_p$ is the set of solutions of a cubic equation of the type:

$$y^2 = x^3 + ax^2 + bx + c.$$

where the coefficients a, b and c in $\mathbb{F}$.

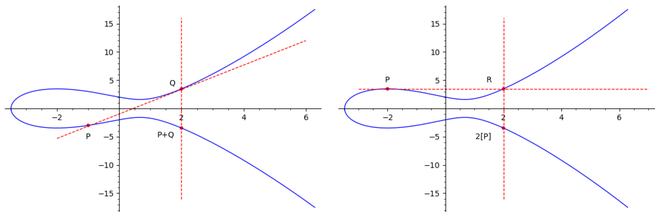

Fig. 4: Elliptic Curve $E : y^2 = x^3 + 2x^2 - 4x + 4$.
Left: Point Addition. Right: Point Doubling

- **Point doubling**: is the method of computing $nP = P + P + \cdots + P$ (n times) by computing doubling points $2P, 4P, 8P, \cdots$ where P is a point on an elliptic curve.

Then the fundamental problem of ECC is given the points P, and Q on an elliptic curve where $Q = nP$, compute the integer n.

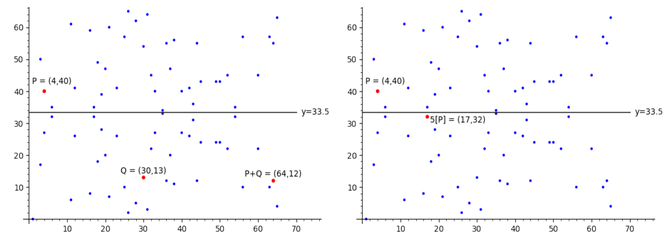

Fig. 5: Left: Point Addition. Right: Point Doubling on Elliptic curve $y^2 = x^3 + 4x + 5$ over $\mathbb{F}_{67}$.

The Elliptic curve Diffie-Hellman Key Exchange

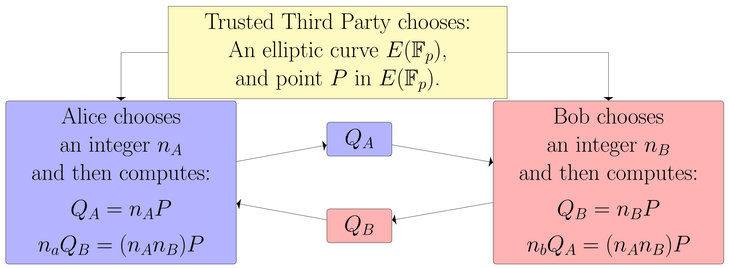

Fig. 6: Diffie-Hellman Key Exchange is use to verify identities and establish secure communication between two parties.

The Elliptic Curve El-Gamal Cryptosystem

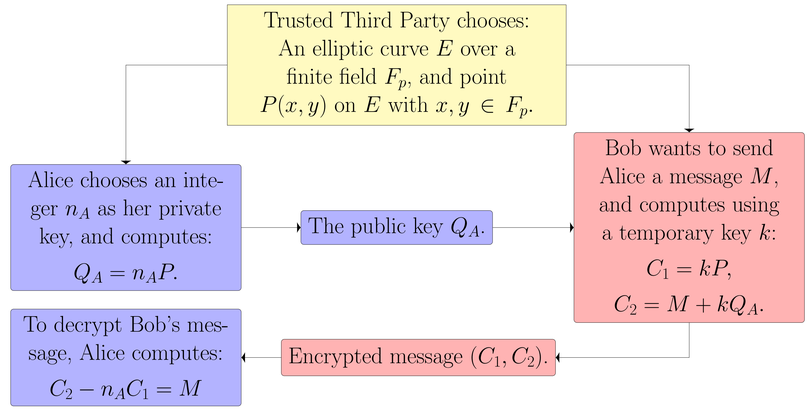

Fig. 7: El-Gamal Cryptosystem is an Asymmetric Cryptosystem that uses the same information as Elliptic Diffie-Hellman.

Conclusion and Future Research

- Elliptic curve cryptography is popular due to its smaller key size compare to other cryptosystems.
- ECC can be used to construct key exchange, encryption and signature schemes.
- For future research, we will focus on cryptosystems that are still safe under attacks of quantum algorithms.
- Moreover, we can work on why elliptic curves on certain finite field are less secure than others.

Acknowledgement

My acknowledgement goes out to Dr. Tran, Dr. Huntemann, Dr. Marinova, Dr. Guelzow, as well as my partner Khoa Bui and I acknowledged the support from the Natural Sciences and Engineering Research Council of Canada (NSERC) (funding RGPIN-2019-04209 and DGECR-2019-00428) and from the Department of Mathematical and Physical Sciences, Concordia University of Edmonton during our project in summer 2021.

References

[1] Kevin Hartnett. *Mathematicians Seal Back Door to Breaking RSA Encryption*. Dec. 2018. URL: https://www.quantamagazine.org/mathematicians-seal-back-door-to-breaking-rsa-encryption-20181217.

[2] Nigel Smart. *Cryptography: An Introduction (3rd Edition)*. New York: McGraw-Hill, 2003.

[3] Jennifer Wilcox. *Solving the enigma: History of the cryptanalytic bombe*. 2006. URL: https://www.nsa.gov/portals/75/documents/about/cryptologic-heritage/historical-figures-publications/publications/wwii/solving_enigma.pdf.