Elliptic Curve Cryptosystems

Santiago Paiva

Presentation Overview

- Basics (2 min)
- Part 1: Introduction to Elliptic Curves (5 min)
- Part 2: The Discrete Logarithm Problem (5 min)
- Part 3: Discrete Logarithm Cryptosystems (5 min)
- Conclusion (1 min)
- Q & A (2 min)

Slides: http://www.github.com/spaiva/cumc-2017

Motivation

https://www.microsoft.com/en-us/research/research-area/security-privacy-cryptography/

Basics

Modular Arithmetic

Concept of Modulo Arithmetic

$$d = n \cdot q + r, \qquad 0 \leq r < n$$

We say this as “d is equal to r modulo n”

Examples:

$$r \equiv d \ (mod\ n)$$
$$5 \equiv 26 \ (mod\ 7)$$

Group

- Basic algebraic structure
- A pair $< G,* >$ where G is a set and $*$ is a binary operation such that the following hold: Closure, Associativity, Identity Element, Inverse
- A group in which the group operation is not commutative is called a "non-abelian group" or "non-commutative group".

Examples:

- The group $\mathbb{Z}_n$ uses only integers from 0 to $n - 1$
- $\mathbb{Z}_{15}$ uses integers from 0 to 14

Ring

A triplet $< R, +, * >$ where $+$ and $*$ are binary operations and R is a set satisfying the following properties:

- $< R, + >$ is a commutative group

For all $x, y, z \in R$

- $x * y$ is also in R
- $x * (y * z) = (x * y) * z$
- $x * (y + z) = (x * y) + (x * z)$

Example: The most familiar example of a ring is the set of all integers $\mathbb{Z}$

Fields

$< R, +, * >$ is a commutative ring with:

- R has a multiplicative identity
- Each element, x, in R (except for 0) has an inverse element in R, denoted by x^{-1}

Examples:

- Rational numbers
- Real and complex numbers

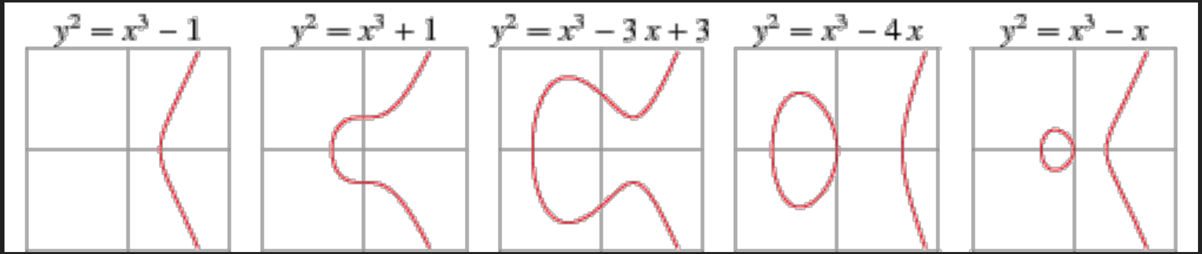
Part I: Introduction to Elliptic Curves

Basics of Elliptic Curves

Definition. Let K be a field of characteristic $\neq 2, 3$ and let $x^3 + ax + b$, where $a, b \in K$, be a cubic polynomial with no multiple roots. Then, an Elliptic Curve over K, noted as $E(K)$, is defined to be the set of points (x, y) with $x, y \in K$, satisfying the equation:

$$\boldsymbol{y^2 = x^3 + ax + b}$$

together with a single element denoted $\mathcal{O}$ called the “point at infinity”.



Basics of Elliptic Curves

If K is a field of characteristic 2, then an Elliptic Curve over K is the set of points satisfying an equation of the following type:

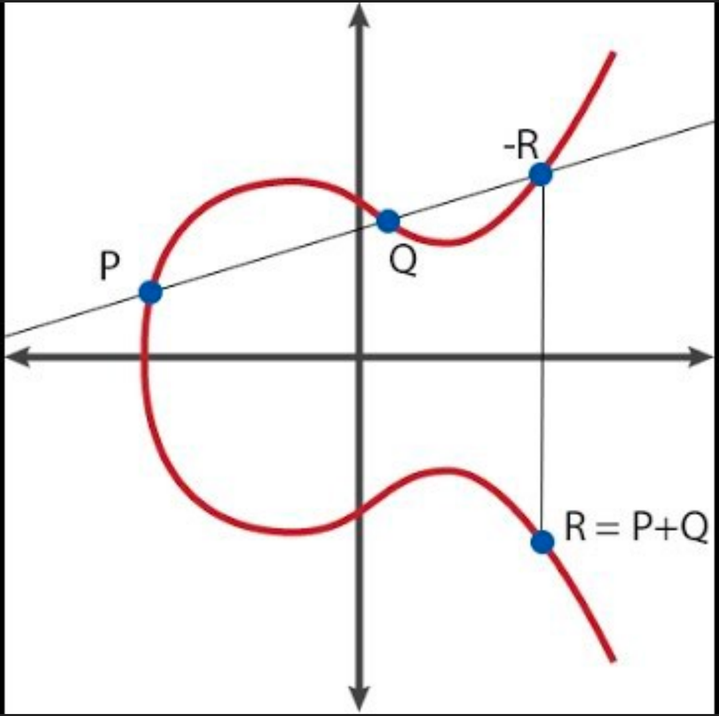
$$y^2 + cy = x^3 + ax + b \qquad y^2 + xy = x^3 + ax^2 + b$$

(where the cubic on the right has no multiple roots) together with $\mathcal{O}$

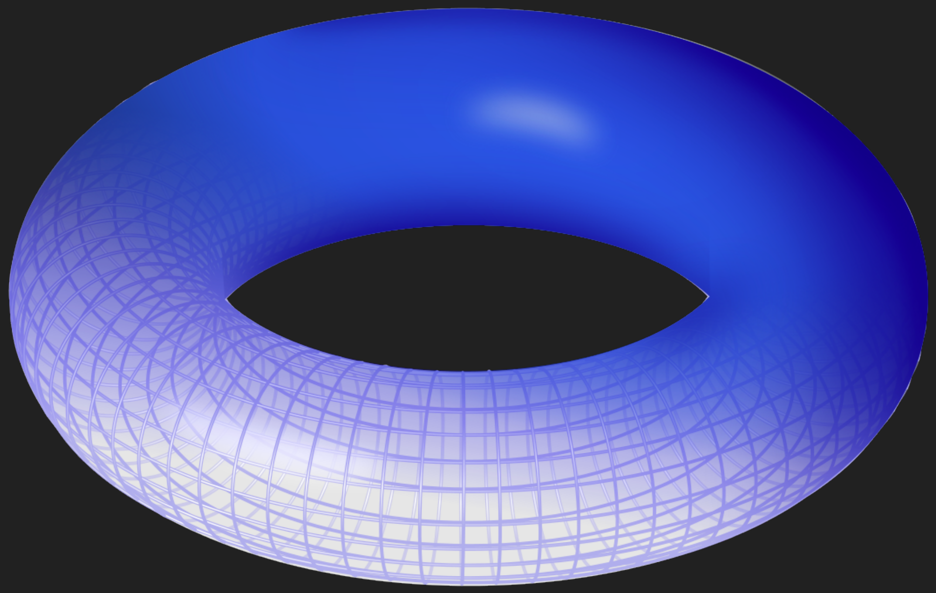
If K is a field of characteristic 3, then an Elliptic Curve over K is the set of points satisfying the equation:

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

Elliptic Curves over $\mathbb{R}$



Elliptic Curves over $\mathbb{C}$



Part II: The Discrete Logarithm Problem

The Discrete Logarithm Problem

A major computationally hard problem in Number Theory

$$y = g^k \, mod \, p$$

Given y, g, and p (g and p very large) it is not easy to calculate k

- We need fewer bits for the integer k in order to achieve the same level of security as with other cryptosystems (like RSA)
- The discrete logarithm problem is considered to be computationally intractable. That is, no efficient classical algorithm is known for computing discrete logarithms in general
- This problem is known to be infeasible in Elliptic Curves groups beyond 2^{120}elements

The Discrete Logarithm Problem

Definition. Let G be a finite cyclic group with n elements, let g be a generator of G, and let $\mathbb{Z}_n$ denote the ring of integers modulo n. The discrete logarithm function of base g is defined as

$$log_g \colon G \longrightarrow \mathbb{Z}_n$$

This function is a group isomorphism, with the following property:

If c is another generator of G, then it follows that $log_c\,(b) = log_c(g) \cdot log_g(b)$

The Discrete Logarithm Problem for Elliptic Curves

Problem. Given that there is some integer k such that $kP = Q$, where P and Q are points on the curve $E(\mathbb{F}_q)$ with $q = p^n$ for some prime p, find k (given that k exists).

Part III: Discrete Logarithm Cryptosystems

Elliptic Curves Cryptography

It is a public-key cryptosystem like RSA, Rabin, ElGamal

Every user has a public and a private key.
- Public key is used for encryption/signature verification
- Private key is used for decryption/signature generation

All public-key cryptosystems have some underlying mathematical operation
- RSA has exponentiation (raising the message or ciphertext to the public or private values)
- Elliptic Curves have point multiplication (repeated addition of two points)

Elliptic Curve Cryptosystems

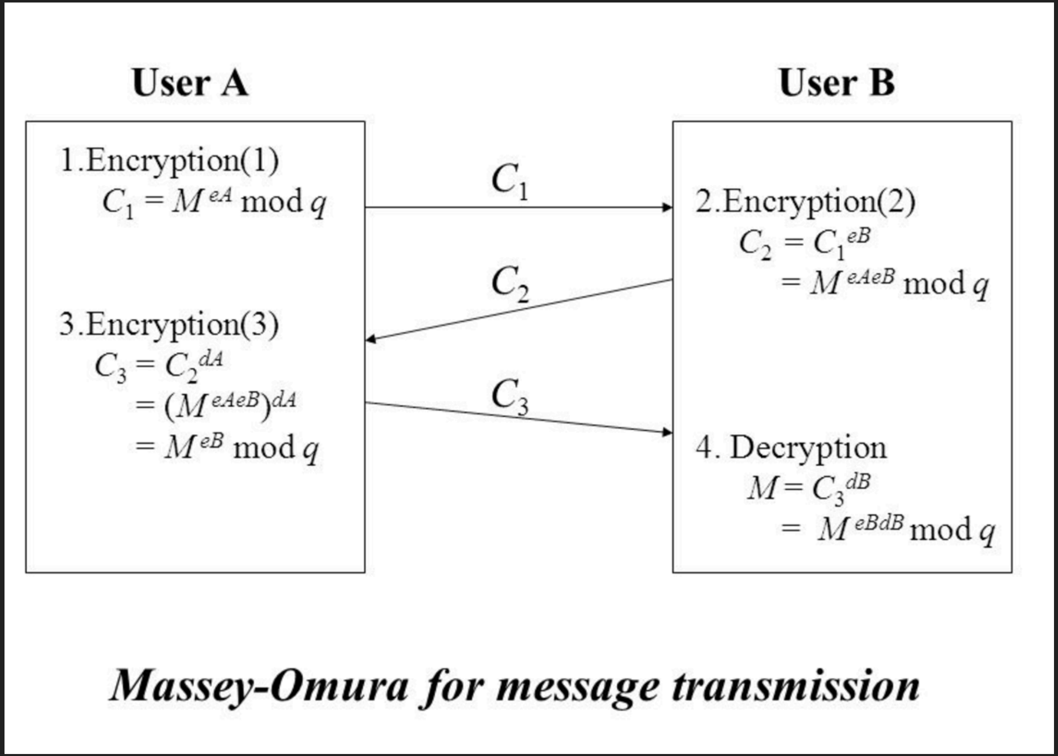
1) **Diffie-Hellman Key Exchange Protocol**
2) **Massey-Omura Encryption**
3) Analogue of ElGamal
4) Shank’s Algorithm
5) Pohlog-Hellman Algorithm

Diffie-Hellman Key Exchange Protocol

Diffie-Hellman Key Exchange

Step	Alice	Bob
1	Parameters: p, g	
2	$A = \text{random}()$ $a = g^A \pmod p$	$\text{random}() = B$ $g^B \pmod p = b$
3	$a \longrightarrow$ $\longleftarrow b$	
4	$K = g^{BA} \pmod p = b^A \pmod p$	$a^B \pmod p = g^{AB} \pmod p = K$
5	$\longleftarrow E_K(data) \longrightarrow$	

Massey-Omura Encryption



Applications

- To encrypt, ECC takes nearly 10 times of that of RSA up to a key size of 384 (ECC) and 7680 (RSA)
- To decrypt, RSA takes more time for a key size higher than 1024 (RSA) compared to 163 (ECC)
- Encryption on small devices that have limited storage and computational power
- Areas: wireless communication devices, smart cards, web servers, networks, wearable devices

Conclusion

- Short introduction to Elliptic Curves
- Introduction to the Discrete Logarithm Problem and the Discrete Logarithm Problem for Elliptic Curves
- 2 Cryptosystems: Diffie-Hellman Key Exchange and Massey-Omura Encryption

Q & A

Elliptic Curve Cryptosystems

Santiago Paiva

paiva.santiago@gmail.com
@stronnics
github.com/spaiva/cumc-2017