Elliptic curve Cryptography

Muralidhara V N

Assistant Professor

IIIT Bangalore

Elliptic Curve

Curve over a field defined by

$$y^2 = x^3 + ax + b$$

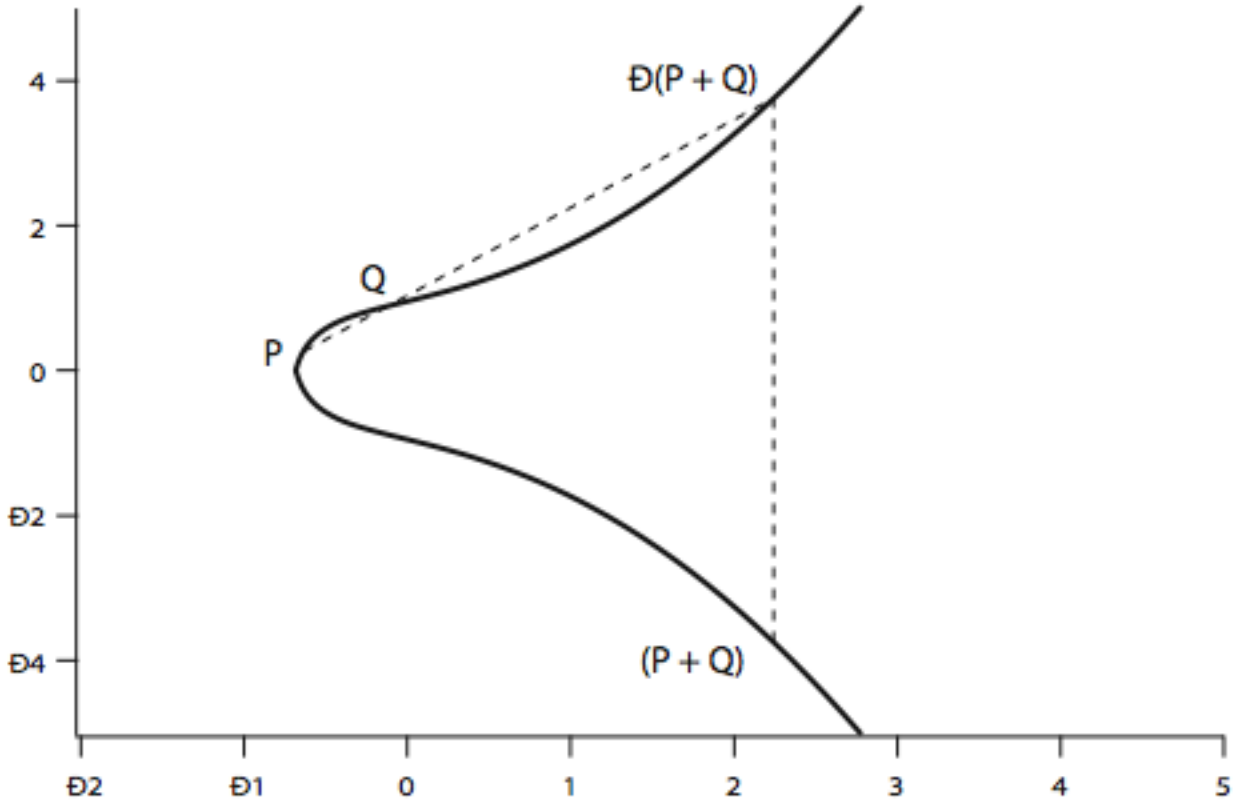
Elliptic Curves in Cryptography

Curve over a finite field (integer mod p) defined by

$$y^2 = x^3 + ax + b$$

$$\mathbf{4}a^3 + \mathbf{27}b^2 \neq \mathbf{0}$$

Example



(b) $y^2 = x^3 + x + 1$

Operation for elliptic curve

Geometrically Q+R is reflection of intersection of Q and R

Discrete Logarithm Problem on EC

- Given an Integer k and a point P, on the computing kP is easy .

- Can be done using repeated addition, takes only O(log k).

Discrete Logarithm Problem on EC

- Given an Integer k and a point P, on the computing kP is easy .
- But given kP and P, computing P is Hard.
- In general only exponential time algorithms are known .

How is it used in Cryptography

Public key crypto systems

Alice and Bob has a pair of keys.

When Alice wants to send a message

Encryption (message, public key of Bob)

Decryption (message, private key of Bob)

How is it used in Cryptography

Users select an elliptic curve and a point G of large order, say n.

Alice chooses a large integer A (<n) which is her secret key and public key is AG.

How is it used in Cryptography

Alice chooses a large integer A (<n) which is her secret key and public key is AG.

To send a message, M to Alice

Send (KG, M+ KAG)

How is it used in Cryptography

Alice chooses a large integer A (<n) which is her secret key and public key is AG.

To send a message, M to Alice

Send (KG, M+ KAG)

Alice Computes M+KAG-A(KG)=M

ECC Security

- Sub-exponential algorithms are known for factorizing Integers and solving discrete logarithmic problems over finite fields.

- In general, only exponential algorithms are known for ECDLP

ECC Security

- In general, only exponential algorithms are known for ECDLP
- Compared to RSA, can use much smaller keys.
- hence for similar security ECC offers significant computational

Comparable Key Sizes for Equivalent Security

Symmetric scheme (key size in bits)	**ECC-based scheme (size of *n* in bits)**	**RSA/DSA (modulus size in bits)**
56	112	512
80	160	1024
112	224	2048
128	256	3072
192	384	7680
256	512	15360