A survey on elliptic curve cryptography

ABSTRACT

Cryptography is an evolving field that research into discreet mathematical equation that is representable by computer algorithm for providing message condentiality. The scheme has been widely used by nation-states, corporates and individual who seeks privacy for data in storage and during transmission. This paper provides a ground up survey on elliptic curve cryptography. It tailors the mathematics behind elliptic curve to the applicability within a cryptosystem. In brief, elliptic curve is a study of points on two-variable polynomials of degree 3. With curve dened over a finite field, this set of points acted by an addition operation forms a finite group structure. Also known as torsion points, they are used to represent the coded messages. Encryption and decryption transform a point into another point in the same set. Besides providing conceptual understanding, discussions are targeting the issues of security and efficiency of elliptic curve cryptosystem. This paper serve as a basis in guiding anyone interested to understand the fundamental concept behind this cryptosystem. Moreover, we also highlight subareas of research within the scope of elliptic curve cryptosystem.

Keyword: Elliptic curve; Endomorphism; Finite field; Group structure; Scalar multiplication