Elliptic-curve cryptography (**ECC**) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. ECC requires smaller keys compared to non-EC cryptography (based on plain Galois fields) to provide equivalent security.[1]

Elliptic curves are applicable for key agreement, digital signatures, pseudo-random generators and other tasks. Indirectly, they can be used for encryption by combining the key agreement with a symmetric encryption scheme. They are also used in several integer factorization algorithms based on elliptic curves that have applications in cryptography, such as Lenstra elliptic-curve factorization.

Theory[edit]

For current cryptographic purposes, an *elliptic curve* is a plane curve over a finite field (rather than the real numbers) which consists of the points satisfying the equation

{\displaystyle y^{2}=x^{3}+ax+b,\,}

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

along with a distinguished point at infinity, denoted ∞. (The coordinates here are to be chosen from a fixed finite field of characteristic not equal to 2 or 3, or the curve equation will be somewhat more complicated.)

This set together with the group operation of elliptic curves is an abelian group, with the point at infinity as an identity element. The structure of the group is inherited from the divisor group of the underlying algebraic variety.

{\displaystyle \mathrm {Div} ^{0}(E)\to \mathrm {Pic} ^{0}(E)\simeq E,\,}

$$\mathrm{Div}^0(E) \to \mathrm{Pic}^0(E) \simeq E,$$

Cryptographic schemes[edit]

Several discrete logarithm-based protocols have been adapted to elliptic curves, replacing the group

{\displaystyle (\mathbb {Z} _{p})^{\times }}

with an elliptic curve:

- The Elliptic Curve Diffie–Hellman (ECDH) key agreement scheme is based on the Diffie–Hellman scheme,

- The Elliptic Curve Integrated Encryption Scheme (ECIES), also known as Elliptic Curve Augmented Encryption Scheme or simply the Elliptic Curve Encryption Scheme,
- The Elliptic Curve Digital Signature Algorithm (ECDSA) is based on the Digital Signature Algorithm,
- The deformation scheme using Harrison's p-adic Manhattan metric,
- The Edwards-curve Digital Signature Algorithm (EdDSA) is based on Schnorr signature and uses twisted Edwards curves,
- The ECMQV key agreement scheme is based on the MQV key agreement scheme,
- The ECQV implicit certificate scheme.

At the RSA Conference 2005, the National Security Agency (NSA) announced Suite B which exclusively uses ECC for digital signature generation and key exchange. The suite is intended to protect both classified and unclassified national security systems and information.[8]

Recently, a large number of cryptographic primitives based on bilinear mappings on various elliptic curve groups, such as the Weil and Tate pairings, have been introduced. Schemes based on these primitives provide efficient identity-based encryption as well as pairing-based signatures, signcryption, key agreement, and proxy re-encryption.

Reference :
https://en.wikipedia.org/wiki/Elliptic-curve_cryptography

Reading :

An Introduction to the Theory of Elliptic Curves Joseph H. Silverman
Brown University and NTRU Cryptosystems, Inc.
https://www.math.brown.edu/~jhs/Presentations/WyomingEllipticCurve.pdf

Craig Costello A gentle introduction to elliptic curve cryptography
Summer School on Real-World Crypto and Privacy
https://summerschool-croatia.cs.ru.nl/2017/slides/A%20gentle%20introduction%20to%20elliptic%20curve%20cryptography.pdf

bitcoinbook/ch04.asciidoc
https://github.com/bitcoinbook/bitcoinbook/blob/develop/ch04.asciidoc

Guide to Elliptic Curve Cryptography BOOK
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.394.3037&rep=rep1&type=pdf

You tube Reference :

https://www.youtube.com/results?search_query=Elliptic+Curve+Cryptography

Elliptic Curve Cryptography Overview
https://www.youtube.com/watch?v=dCvB-mhkT0w

Elliptic Curve Diffie Hellman
https://www.youtube.com/watch?v=F3zzNa42-tQ

Elliptic Curve Point Addition
https://www.youtube.com/watch?v=XmygBPb7DPM

Elliptic curves
Explore the history of counting points on elliptic curves, from ancient Greece to present day. Inaugural lecture of Professor Toby Gee.
https://www.youtube.com/watch?v=6eZQu120A80

Martijn Grooten - Elliptic Curve Cryptography for those who are afraid of maths
https://www.youtube.com/watch?v=yBr3Q6xiTw4&t=119s

Elliptic Curve Cryptography, A very brief and superficial introduction
https://www.youtube.com/watch?v=oPJrWYmqGRs