Elliptic Curves Cryptographic Techniques

Ali Makki Sagheer
Department of Information System
College of Computer
University of Anbar, Ramadi, Iraq
ali_makki@ieee.org

Abstract— The security issues are very important for information technology applications now a day such as ATM and Smart cards. One of the recent public key cryptosystems is Elliptic Curves Cryptography. The group of the elliptic curve points forms an Abelian group, that is a suitable choice for constructing the Elliptic Curve Discrete Logarithm Problem (ECDLP). This led to create cipher system based on the difficulty of its solution. That is open a new windows for treatment with special groups and new operations.

This paper provides three proposed techniques as a modification of ElGamal cryptosystem based on the elliptic curves, as well as, implement these techniques, compute the computational complexity of these methods compared to the original methods, compare these methods with the original methods in running time of several messages have different sizes. A great reduction in calculation time is resulted, also these techniques makes the cipher text more confused than cipher text which resulted from original techniques.

Keywords-component; Elliptic Curves Cryptography; Discrete Logarithm Problem; Elliptic Curve Discrete Logarithm Problem; ElGamal; Menezes-Vanstone

both cryptosystems for encryption/decryption and digital signatures.

As we have seen, the bit length of key for secure RSA is increased over the development of technology, and this has put a heavier processing based on applications using RSA. This burden has implications, especially for e-commerce applications that conduct large number of secure transmission. Recently, computing system has been challenge RSA. This led to the attraction to the elliptic curve cryptography (ECC).

ECC has some advantages like less computing, small storage capacity and narrow bandwidth comparing with other public-key cryptosystems [3].

The ECC is unlike earlier cryptosystem, an elliptic curve works with a finite *Abelian group* formed by the points on an elliptic curve defined over a finite field. ECC can be used for encryption and decryption schemes, Digital Signature Algorithm (DSA) and key distribution [4].

ECC represent the higher strength per bit for all known public key cryptosystem because of the difficulty of the hard problem upon which it is based. This greater difficulty of the