Elliptic Curve Cryptosystem Based Secure Communication System

Naing Linn, May Aye Khine

Linn3368@gmail.com

Abstract

Security aspects come into play when it is necessary or describe to protect the information transmission. The goal of cryptography is to make it possible for two people to exchange a message in such a way that other people cannot understand the message. This thesis is intended to implement a secure information system for critical applications. The key Derivation Function is to calculate Keying data which is divided into two keys, ENCkey and MACkey. ENCkey is used for encryption and decryption the message and MACkey is used for message authentication code(MAC) scheme to check the receiving message is valid or not. The XOR Encryption scheme is used for encryption operation. We compare the performance of Elliptic Curve Cryptosystem(ECC) with other cryptosystem in terms of key sizes; ECC has the same level of security with smaller key sizes. So, ECC is used the smart and other critical applications such as military departments, banking systems and etc.