Elliptic Curve Cryptography System Based On Indexing Dictionary Technique

Hsu Myat Nandar
"University of Computer Studies, Yangon, Myanmar"
phwethayalphi@gmail.com

Abstract

Cryptography is one of the most important sciences in the current area. Elliptic Curve Cryptography (ECC) has attracted the attention of researchers and product developers due to its robust mathematical structure and highest security compared to other existing algorithms. ECC provides greater security more efficient performance than the first generation public key technique.In this paper, application for elliptic curve cryptosystem work as symmetric cryptographic system by investigates fromindexing dictionary technique. This system is implemented to transfer secret messages between the sender and receiver using indexing dictionary technique for English text. The dictionary technique is just a list ofwords orsecure sentences. This dictionary is constructed to 841 secure messages stores in database. These messages are encoded to ECC indexing points and ECC points are used as indexes of dictionary in this system. These indexes of points are encrypted and decrypted instead of encrypting the text messages. In this system, linear feedback shift register (LFSR) is used to generate the secret key. Secret permutation and inverse permutation key is used to increase randomized for points sequence of data. This system test it by execute encryption and decryption process with more flexible and efficient.