An analysis for chosen plaintext attack in Elliptic Curve Cryptosystem based on second order Lucas sequence

ABSTRACT

Elliptic Curve Cryptography is a cryptography based on the algebraic structure of elliptic curves over finite fields. The security of Elliptic Curve Cryptography depends on discrete logarithms that is much more difficult to challenge at equivalent key lengths. Lucas sequence is a sequence that satisfies the recurrence relation and is very useful for fast and reliable primality testing. Therefore, a cryptosystem had been developed which is analogous to Elliptic Curve Cryptosystem, and is based on second order Lucas sequence. This cryptosystem will be tested by using chosen plaintext attack. The chosen plaintext attack is one of the homomorphic attacks. It is a consequence of the multiplication structure and based on homomorphic nature. Thus, this paper reports a way the chosen plaintext attack succeed in Elliptic Curve Cryptosystem based on second order Lucas sequence.

Keyword: Ciphertext; Decryption; Elliptic curve; Encryption; Keys; Lucas sequence; Plaintext