Scalar and Multi-Scalar Addition Chain in Elliptic Curve Cryptography

W.V.A. Nisansala, G.S. Wijesiri

[2]*Department of Mathematics, University of Kelaniya, Kelaniya, Sri Lanka*

Cryptography is a mathematical based technology that ensure the security of communications in the presence of malicious adversaries. Nowadays, cryptography deals with designing of algorithms, protocols and systems to secure transfer of information. The Elliptic Curve Cryptography (ECC) is a main branch of the public key cryptography (asymmetric cryptosystem) which was introduced by Neal Koblitz and Victor Miller in 1985. Higher speed, the efficiency of using power, bandwidth and less storage are some advantages of ECC. The strength of ECC is based on the inability of determining the scalar k of the scalar multiplication kP, where P is a point of an elliptic curve in finite field and it is known as the Elliptic Curve Discrete Logarithm Problem (ECDLP). Hence, the scalar multiplication is the central operation of ECC. Since most of the efficient and secure exponentiation methods (i.e. double-and-add, triple-and-add methods) depend on the secret scalar or exponent, an attacker may reveal the secret information through the side channel analysis (side channel attack). Simple Power Analysis (SPA) is a type of side channel attack that an attacker retrieves secret key by observing the power consumption traces. One way to overcome this problem is the use of doubling free addition chain since it results a fixed sequence of operations, and an attacker cannot detect any information through SPA. Therefore, we have implemented a new methodology that is more secure and reasonably efficient, a doubling free simultaneous addition chain involving Lucas pattern to compute the scalar and multi-scalar multiplication.

Keywords: Elliptic Curve Cryptography, Simple Power Analysis, Doubling-free Addition Chain

[1]Corresponding author. Tel.: +94-71-531-1220
E-mail address: ashani.vbv@gmail.com