Oral presentation: 152

Scalar and multi-scalar multiplication in Elliptic Curve Cryptography using Fibonacci numbers

N. P. A. A. Sandamali* and G. S. Wijesiri

Department of Mathematics, Faculty of Science, University of Kelaniya, Sri Lanka
*anuththarasandamali5@gmail.com

Cryptography is a science, which enables secure communications from various malicious adversaries using mathematical techniques. As a branch of cryptography, Neal Koblitz and Victor Miller introduced the Elliptic Curve Cryptography (ECC), in 1985. ECC provides us several advantages such as higher speed, efficient use of power and less storage. Security of ECC is based on the hardness of Elliptic Curve Discrete Logarithm Problem (ECDLP), which is defined as the problem of determining scalar d of the scalar multiplication $Q = dP$, when P and Q are given, where P and Q are two points on the elliptic curve. Lot of research are carried out to speed up and improve ECC implementations. Such researches mainly focus on the scalar multiplication, since it is the most important and time-consuming ECC operation. In this work we also focus on scalar as well as multi-scalar multiplication. Although Elliptic Curve Cryptosystems have enormous advantages, side channel attacks can break their common implementations. Finding methods against side channel attacks on elliptic curves is also a very active research. Simple Power Analysis (SPA) is a one type of side channel attack. In SPA, the attackers use the power consumption to monitor each operation and it helps attackers to retrieve secret scalar. Scalar multiplication is considered as a basic operation for elliptic curve cryptosystems. There are various methods to compute scalar multiplication in ECC. Generally, the most popular method is binary method. Unfortunately, although the binary method has excellent features, SPA attackers are able to fully reveal the secret scalar d, by observing the power trace of the binary method. One way to overcome this problem is finding a doubling free addition chain. Our main objective in this research is finding a doubling-free addition chain to compute scalar and multi-scalar multiples. As a solution for this problem, we proposed a new methodology to compute scalar and multi-scalar multiplication using Fibonacci numbers. We propose three algorithms. The first algorithm is for pre-computations in which we get a sequence of Fibonacci numbers to compute multiples. Using the resulting sequence, the second algorithm compute the relevant scalar multiplication. Using the same sequence, the third algorithm can compute the relevant multi-scalar multiplication. The proposed method shows higher performance when we compare new algorithms with traditional binary method.

Keywords: Doubling-free addition chain, Elliptic Curve Cryptography, multi-scalar multiplication, scalar multiplication, simple power analysis