Abstract

In this paper the implementation of arithmetic operations in ECC is described. Elliptic curve cryptography is very useful in the field of the network security because of its small key size and its high strength of security. In this paper briefly describing general arithmetic operations we focus on scalar multiplication. We present two techniques: (i) reducing Hamming weight of scalars in binary representation and (ii) using sliding window, for obtaining scalar multiplication in a faster manner. Use of both the techniques is explained by suitable examples.

Reference

Efficient Implementation of Arithmetic Operations in ECC over Binary Fields


Index Terms

Computer Science
Network Security
Key words

Elliptic Curve Discrete Logarithm

Scalar multiplication

Diffie-Hellman Algorithm

Sliding window

hamming weight