Abstract

Elliptic curve based cryptosystem is an efficient public key cryptosystem, which is more suitable for limited environments. The performance of elliptic curve cryptosystem heavily depends on an operation called point multiplication. It is the multiplication of a scalar with the given point on the curve. Scalar multiplication is faster by using signed binary representation as
Design and Implementation of Block Method for Computing NAF

compared to binary representation. In this paper “Block Method” for computing NAF is proposed. The Proposed method is more efficient as compared to standard method for computing NAF.

The paper presents the comparative study of both standard and block methods for computing NAF. In this paper we have examined that Overall computation for Point Multiplication operation with NAF method can be made more effective by improving speed of calculating the NAF Part.

Reference

- Qizhi Qiu and Qianxing Xiong, “Research on Elliptic Curve Cryptography”, the 8th international conference on computer supported cooperative work in design proceedings”, IEEE 2003, pp 698-701.
Index Terms

Computer Science  Information Security

Key words
Elliptic curve cryptography  Point multiplication
Binary method
NAF

Block method