Abstract

Nowadays world is seen through mobile internet in a fraction of seconds, which invaded the need for many mobile applications. Financial transactions through mobile phones has become primitive mode of transactions. All these mobile applications including financial transactions demands for better security due to pervasive environment. In our work, we propose light weight Elliptical Curve Cryptographic method suitable for mobile applications. Elliptic curve point multiplication or scalar multiplication is the operation of adding a point \( P \) on the elliptic curve to itself successively scalar number of times. This paper describes an algorithm for light weight computation of scalar multiplication for elliptic curves defined over binary fields using projective coordinate system eliminating the need to perform inversions as needed with computations involving affine coordinates. It effectively incorporates fast computation method for binary elliptic curves by making use of Exclusive-OR gates. The effectiveness of the algorithm is measured both by Matlab simulation and Field-Programmable Gate Array (FPGA) implementation. Hardware implementation using Verilog proves that the proposed algorithm consumes less resources in terms of delay and power.
References


Index Terms

Computer Science Security
Keywords

Vedic multiplier, Urdhva Tirgyagbyham sutra, ECC, conventional array multiplier, FPGA implementation, delay, low power, low area consumption.