Abstract

Curve based cryptography are preferred for embedded hardware since they require shorter operand size than RSA to attain the same security level. So ECC and HECC are more suitable in constrained environment such as smart cards if we can select suitable curves and efficient scalar multiplication technique to speed up arithmetic on the curve. With this in view, this paper explores in details the main operations like scalar multiplication, group operations on Jacobian,
finite field operations etc which are the prime steps for efficient implementation of ECC / HECC. We also have compared the timings of main operations like scalar multiplication, encryption and decryption of Elliptic and Hyperelliptic curve cryptosystems to study the relative performance of these cryptosystems.

**Reference**


Index Terms

Computer Science

Security

Key words

Elliptic Curve Cryptography (ECC) Hyperelliptic Curve
Hyperelliptic Curve Cryptography (HECC)
Scalar Multiplication