Abstract

In asymmetric cryptography, Elliptic Curve Cryptography (ECC) is the fastest in term of computation and the strongest in term of security. It can be used in message encryption/decryption, digital signature or key exchange. ECC can be implemented in hard over binary field $GF(2^n)$ or in soft over prime field $GF(p)$. This paper presents an efficient software implementation of ECC scalar multiplication over prime field using GNU Multiple Precision (GMP) Library. The differential fault attacks (DFA) on the RSA cryptosystem can be extended to ECC one by inserting bit errors during computation. In this paper, a "No Correctness Check for Input Points" (NCCIP) attacks was applied and a countermeasures was given to protect ECC cryptosystem against it. Software implementation in C language, using GMP library, was simulated on Intel(R) Core(TM) i3 CPU M380 @ 2.87GHz(3 GB RAM, 32-bit architecture).

References

1. D. R. Stinson, Cryptography Theory And Practice. 3th edition, Chapman and Hall/CRC,
2006.


https://gmplib.org/gmp-man-6.0.0a.pdf


Index Terms

Computer Science Security
Keywords

ECC, scalar multiplication, DFA, GMP Library, El-gamal Scheme