World Academy of Science, Engineering and Technology
International Journal of Cognitive and Language Sciences
Vol:17, No:07, 2023

A Design of Elliptic Curve Cryptography Processor based on SM2 over GF(p)

Authors : Shiji Hu, Lei Li, Wanting Zhou, DaoHong Yang

Abstract : The data encryption, is the foundation of today's communication. On this basis, how to improve the speed of data encryption and decryption is always a problem that scholars work for. In this paper, we proposed an elliptic curve crypto processor architecture based on SM2 prime field. In terms of hardware implementation, we optimized the algorithms in different stages of the structure. In finite field modulo operation, we proposed an optimized improvement of Karatsuba-Ofman multiplication algorithm, and shorten the critical path through pipeline structure in the algorithm implementation. Based on SM2 recommended prime field, a fast modular reduction algorithm is used to reduce 512-bit wide data obtained from the multiplication unit. The radix-4 extended Euclidean algorithm was used to realize the conversion between affine coordinate system and Jacobi projective coordinate system. In the parallel scheduling of point operations on elliptic curves, we proposed a three-level parallel structure of point addition and point double based on the Jacobian projective coordinate system. Combined with the scalar multiplication algorithm, we added mutual pre-operation to the point addition and double point operation to improve the efficiency of the scalar point multiplication. The proposed ECC hardware architecture was verified and implemented on Xilinx Virtex-7 and ZYNQ-7 platforms, and each 256-bit scalar multiplication operation took 0.275ms. The performance for handling scalar multiplication is 32 times that of CPU(dual-core ARM Cortex-A9).

Keywords : Elliptic curve cryptosystems, SM2, modular multiplication, point multiplication.
Conference Title : ICSLP 2023 : International Conference on Speech and Language Processing
Conference Location : Stockholm, Sweden
Conference Dates : July 06-07, 2023