Abstract

The high performance of an elliptic curve (EC) crypto system depends efficiently on the arithmetic in the underlying finite field. We have to propose and compare two levels of Galois Field GF(2163) and GF(2193). The proposed architecture is based on Lopez-Dehab elliptic curve point multiplication algorithm, which uses Gaussian normal basis for GF(2163) field arithmetic. In which derived parallelized elliptic curve point doubling and addition algorithms with uniform addressing are based on Lopez-Dehab method. The proposed GF(2193) is based on an efficient Montgomery add and double algorithm, also the karatsuba-offman multiplier and Itoh-Tsujii algorithm are used as the inverse component. The hardware design is based on optimized Finite State Machine (FSM), with a single cycle 193 bits multiplier, field adder and field squarer. The different optimization at the hardware level improves the acceleration of the ECC scalar multiplication; increases frequency and the speed of operation such as key generation, encryption and decryption. Finally we have to implement our design using Xilinx XC4VLX200 FPGA device.

References

- Mohamed Abdelkader Bencherif, Hamid Bessalah and Abderrezak Guessoum. Reconfigurable Elliptic curve crypto-Hardware over the Galois Field GF
Reconfigurable Architecture for Network processing


- Yong-ping DAN, Xue-cheng ZOU, Zheng-lin LIU, YUHAN, Li-hua YI, High-performance hardware architecture of elliptic curve cryptography processor over GF (2163)* Journal of Zhejiang University Science ISSN 1862-1775 (Online)

- Gang Quan, James P. Davis, Siddhaveerasharan Devarkal,
Reconfigurable Architecture for Network processing

Duncan A. Buell. High-Level Synthesis for Large Bit-Width Multipliers on FPGAs: A Case Study. Department of Computer Science and Engineering, University of South Carolina, Columbia, SC 29208 USA. pp 213:218.


Index Terms

Computer Science Security

Keywords

Elliptic Curves Cryptography Ecc Fpga Montgomery Karatsuba-offman Galois Field Operations