Abstract

The finite field modular multiplier is the most critical component in the elliptic curve crypto processor (ECCP) consuming the maximum chip area and contributing the most to the device latency. Modular multiplication, point multiplication, point doubling are few of the critical activities to be carried out by multiplier in ECC algorithm, and should be managed without compromising on security and without burdening space and time complexities. Since the area complexity of the Crypto processor is mainly based on the Modular Multiplier incorporated within the ECC processor, the major contribution of this work includes the replacement of traditional Karatsuba multiplier with the proposed space optimized multiplier inside the processor. The complete modular multiplier and the cryptoprocessor module is synthesized and simulated using Xilinx ISE Design suite 14.4 software. Experimental investigation show an improvement in area efficiency of cryptoprocessor, since proposed scheme occupies relatively reduced percentage area of FPGA as compared to the one using traditional Karatsuba multiplier.

References

- M. Morales-Sandoval, C. Feregrino-Urife, and P. Kitsos. Bit-serial and digit-serial GF (2^m) Montgomery multipliers using linear feedback shift registers.
Index Terms

Computer Science

Security

Keywords

ECC: Double point multiplication: Karatsuba Multiplier: Systolic Multipliers: Area Complexity.