عنوان مقاله:

Implementation of an Efficient Processor Scalar Multiplication Elliptic Curve

محل انتشار:

پنجمین کنفرانس بین المللی تحقیقات نوین پژوهشی در مهندسی و تکنولوژی (سال: 1396)

تعداد صفحات اصل مقاله: 15

نویسندگان:

Yaser Ghahramani - *Department of Computer, Ashtian Branch, Islamic Azad university, Ashtian, Iran*

Manouchehr Kazemi - *Department of Computer, Faculty of Computer Ashtian Branch, Islamic Azad university, Ashtian, Iran*

Abbas Zamani Shoorabi - *Department of Computer, Faculty of Computer Ashtian Branch, Islamic Azad university, Ashtian, Iran*

خلاصه مقاله:

The higher computational complexity of an elliptic curve scalar point multiplication operation limits its implementation on general purpose processors. Dedicated hardware architectures are essential to reduce the computational time, which results in a substantial increase in the performance of associated cryptographic protocols. This paper presents a unified architecture to compute modular addition, subtraction, and multiplication operations over a finite field of large prime characteristic GF. Subsequently, dual instances of the unified architecture are utilized in the design of high speed elliptic curve scalar multiplier architecture. The proposed architecture is synthesized and implemented on several different Xilinx FPGA platforms for different field sizes. The proposed design computes a 192-bit elliptic curve scalar multiplication in 2.3 ms on Virtex-4 FPGA platform. It is 13% faster and requires 18% fewer clock cycles for elliptic curve scalar multiplication and consumes considerable fewer FPGA slices as compared to the other existing designs. The proposed design is also resistant to the timing and simple power analysis (SPA) attacks; therefore it is a .good choice in the construction of fast and secure elliptic curve based cryptographic protocols

کلمات کلیدی:

FPGA, ECC, Elliptic Curve, High Speed Cryptosystem, Cryptography Algorithm

لینک ثابت مقاله در پایگاه سیویلیکا:

https://civilica.com/doc/749772