World Academy of Science, Engineering and Technology
International Journal of Computer and Systems Engineering
Vol:10, No:10, 2016

Efficient Semi-Systolic Finite Field Multiplier Using Redundant Basis

Authors : Hyun-Ho Lee, Kee-Won Kim

Abstract : The arithmetic operations over GF(2m) have been extensively used in error correcting codes and public-key cryptography schemes. Finite field arithmetic includes addition, multiplication, division and inversion operations. Addition is very simple and can be implemented with an extremely simple circuit. The other operations are much more complex. The multiplication is the most important for cryptosystems, such as the elliptic curve cryptosystem, since computing exponentiation, division, and computing multiplicative inverse can be performed by computing multiplication iteratively. In this paper, we present a parallel computation algorithm that operates Montgomery multiplication over finite field using redundant basis. Also, based on the multiplication algorithm, we present an efficient semi-systolic multiplier over finite field. The multiplier has less space and time complexities compared to related multipliers. As compared to the corresponding existing structures, the multiplier saves at least 5% area, 50% time, and 53% area-time (AT) complexity. Accordingly, it is well suited for VLSI implementation and can be easily applied as a basic component for computing complex operations over finite field, such as inversion and division operation.

Keywords : finite field, Montgomery multiplication, systolic array, cryptography
Conference Title : ICCCIS 2016 : International Conference on Cryptography, Coding and Information Security
Conference Location : Osaka, Japan
Conference Dates : October 10-11, 2016