Galois Field based Montgomery Multiplier for RSA Cryptosystem using Area Efficient Adder

Volume 127 - Number 3

Year of Publication: 2015

Authors:

Ritu Gupta, Kavita Khare

10.5120/ijca2015906353

Abstract

Data security is the major point of concern in today’s internet communication system for which cryptography plays a vital role. Modular multiplier plays a key role in modern cryptography system. Galois field arithmetic is being popularly used in such applications. Montgomery multiplication is the method for boosting up the speed of modular multiplication. Montgomery modular multiplier is implemented for larger operand size to design encryption and decryption algorithm for RSA security system. This paper contributes to the implementation of modular multiplier using Montgomery algorithm for RSA encryption and decryption, where existing architecture is implemented using carry select adder and modified carry select adder and it is concluded that later uses 23% less area and approximate 4.5% less output delay as compared to former, in VHDL using Xilinx ISE 9.2i and has been simulated on FPGA device spartan3, xc3s200-5ft256.

References


**Index Terms**

Computer Science

Security

**Keywords**

Carry select adder, Montgomery algorithm, RSA cryptography, modular arithmetic.