World Academy of Science, Engineering and Technology
International Journal of Electrical and Information Engineering
Vol:8, No:12, 2014

Modified Montgomery for RSA Cryptosystem

Authors : Rupali Verma, Maitreyee Dutta, Renu Vig

Abstract : Encryption and decryption in RSA are done by modular exponentiation which is achieved by repeated modular multiplication. Hence, efficiency of modular multiplication directly determines the efficiency of RSA cryptosystem. This paper designs a Modified Montgomery Modular multiplication in which addition of operands is computed by 4:2 compressor. The basic logic operations in addition are partitioned over two iterations such that parallel computations are performed. This reduces the critical path delay of proposed Montgomery design. The proposed design and RSA are implemented on Virtex 2 and Virtex 5 FPGAs. The two factors partitioning and parallelism have improved the frequency and throughput of proposed design.

Keywords : RSA, montgomery modular multiplication, 4:2 compressor, FPGA
Conference Title : ICISS 2014 : International Conference on Information Systems Security
Conference Location : Paris, France
Conference Dates : December 30-31, 2014