A Realistic Approach of Implementing Closed Network Data Security on FPGA

Senthil Kumar.M1, S. Rajalakshmi2, V. Naga Sree Ram3, R. Vishnu Kant4

1, 3, 4 Department of Electronics and Communication Engineering
2 Department of Computer Science Engineering
Sri Chandrasekharendra Saraswathi Viswa Maha Vidyalaya University, Enathur,
Kancheepuram- 631561, Tamil Nadu, India.
1senthilkumar.murugesan@ymail.com, 2raji.scsvmv@gmail.com, 3ramkumar.venneti@gmail.com,
4ramanvishnukant@ymail.com

Abstract—This paper approaches a simple technique to develop the RSA algorithm using FPGA that can be used as a standard device in the secured communication system. This RSA algorithm is implemented in the FPGA using VHDL. A simple nested loop addition and subtraction has been used for implementation. This results in very low frequency requirement with consideration of high speed by reducing the gate counts with low power consumption. Also, it supports multiple key size requirements and is of low cost compared to earlier methods. The information to RSA encryption side is in the form of statement and the same will appear in the decryption side and its real time input/output also achieved effectively. This technique is applicable only when users own the system module i.e. closed network. The hardware design is targeted on Xilinx Spartan 3E device and it supports lower versions as well. This RSA algorithm design has made use of 1000 total equivalent gate count approximately and achieved a clock frequency of 23 MHz.

Index Terms- Cryptography, FPGA, VHDL, Security.