Abstract

This paper presents the architecture and modeling of RSA public key encryption/decryption systems. It supports multiple key sizes like 128 bits, 256 bits, 512 bits. Therefore it can easily be fit into the different systems requiring different levels of security. In this paper simple shift and add algorithm is used to implement the blocks. It makes the processing time faster and used
comparatively smaller amount of space in the FPGA due to its reusability. Each block is coded with Very High Speed Integrated Circuit Hardware Description Language. The VHDL code is synthesized and simulated using Xilinx-ISE 10.1. It is verified that this architecture support multiple key of 128bits, 256bits, and 512 bits.

Reference

- Hwang E. Digital Logic and Microprocessor Design with VHDL.

Index Terms

Computer Science       Security

Key words

RSA       VHDL       FPGA
modular multiplication.