

## FPGA Implementation of RSA Encryption Algorithm for E-Passport Application

**Authors :** Khaled Shehata, Hanady Hussien, Sara Yehia

**Abstract :** Securing the data stored on E-passport is a very important issue. RSA encryption algorithm is suitable for such application with low data size. In this paper the design and implementation of 1024 bit-key RSA encryption and decryption module on an FPGA is presented. The module is verified through comparing the result with that obtained from MATLAB tools. The design runs at a frequency of 36.3 MHz on Virtex-5 Xilinx FPGA. The key size is designed to be 1024-bit to achieve high security for the passport information. The whole design is achieved through VHDL design entry which makes it a portable design and can be directed to any hardware platform.

**Keywords :** RSA, VHDL, FPGA, modular multiplication, modular exponential

**Conference Title :** ICSRD 2020 : International Conference on Scientific Research and Development

**Conference Location :** Chicago, United States

**Conference Dates :** December 12-13, 2020