

Design and Implementation of Encryption Algorithm on FPGA

Dr. Hanady Hussien

The need of security to protect the data has become of vital importance and critical for many applications. There are several security schemes implemented using hardware or software trying to solve the problem of security. The majority of them are symmetric key encryption schemes and some others are asymmetric encryption schemes. The hardware implementation could improve time efficiency and decrease the power consumption, so the strong cryptography can be implemented in different applications such as wireless sensor network. One of the commonly used public key cryptosystem is Rivest, Shamir and Adleman (RSA) algorithm.

The aim of this project is to study the different encryption algorithms and focus on RSA algorithm and its applications. Then introduces a design for RSA algorithm and implements such design on a Field Programmable Gate Arrays (FPGAs).

Requirement

- ◆ Good knowledge in Very High Speed Integrated Circuit Hardware Description language (VHDL).
- ◆ Familiar with one software languages C or Matlab

Hint

We can build up our knowledge of VHDL during the project