

Project 1:

VLSI Design and Implementation of a Modified Stream Cipher Algorithm

Instructor: Prof. Hazem H. Ali

Abstract

A5/1 is a GSM encryption algorithm that protects user data transmission over air. However, the A5/1 was cryptanalyzed by using different attack techniques. In this project a VLSI circuit realizing an new algorithm for a modified version of the A5/1 that offers security improvement to the vulnerabilities will be developed with 512 bits key length target.