Abstract

The implementation of encryption/decryption algorithm is the most essential part of the secure communication. In currently existing encryption algorithms there is a tradeoff between implementation cost and resulting performances. Scalable encryption algorithm is targeted for small-embedded application with limited resources (such as memory size, processor capacity). SEA n, b is parametric in the text, key and processor word size and uses a limited instruction
set (i.e. NOT, AND, OR, XOR gates, word rotation and modular addition). And it has a provable security against linear and differential cryptanalysis. This paper includes the conversion of loop architecture of SEA into flowchart, in such a way that encryption and decryption process are separated, loop is split into two parts and controlling inputs are removed. By this method it is easy to design in VHDL language, for implementation in FPGA.

Reference

- Data Encryption Standard, FIPS PUB 46-3, Oct. 1999

Index Terms

Computer Science

Wireless

Key words

Scalable Encryption Algorithm

VHDL

FPGA