Abstract

Initially SEA is designed for software implementations in controllers, smart cards, or processors. In this Paper we proposed a system that investigates its performances in recent field-programmable gate array (FPGA) devices. The present symmetric encryption algorithms result from a tradeoff between implementation cost and resulting performances. The proposed system is applicable where there are limited processing resources with high throughput requirements.

For this purpose, we propose a SEA loop Architecture with Behavior model (VHDL) coding. So the number of logic gates required is very less when compared with Gate level model. Because of less number of logic gates, time taken to execute the loop architecture is less. So we are achieving a faster execution time (Frequency in MHZ). The proposed design is parametric in the key and word size, provably secure against linear or differential cryptanalysis. Beyond its low cost performances, a significant advantage of the proposed
architecture is its full flexibility for any parameter of the scalable encryption algorithm, taking advantage of generic VHDL coding.

Reference

- F. Mace, F. -X. Standaert, and J.-J Quisquater “FPGA implementation(s) of a Scalable Encryption Algorithm,” in IEEE Transaction on very large scale integration (VLSI) systems, VOL.16, NO. 2, FEBRUARY 2008

Index Terms

Computer Science

Security
Key words

FPGA – Field Programmable Gate Array
Computer security
DES - Data Encryption Standard
VHDL – Hardware Description Language