Abstract

In this paper, design and FPGA (Field Programmable Gate Array) implementation of embedded system for time based IDEA encryption is presented. Presently available encryption systems, suffer from Brute Force attack in which all key combinations are tried out to find the correct key. In such a case, the time taken for breaking the code depends on the system used for cryptanalysis. In the proposed system, time is used as a second dimension of the key. That is, the correct key entered at the correct time is needed for proper decryption. The proposed scheme uses a dynamically varying number of shifts for both encryption and decryption thereby the system needs to wait till that time and this forms the time based key input. Hence, the possibility of brute force attack is minimized and is free from the system capability. IDEA encryption algorithm is taken as the base and time factor is implemented as a second dimension of the key. The proposed system adds complexity to the IDEA encryption algorithm by including the time as a second dimension besides increasing the time required for cryptanalysis. As the proposed system needs concurrent execution and real time processing, the system is implemented using Altera Stratix III FPGA and the results are presented.
Reference

- RC5-The Wikipedia free encyclopedia.
- John Kelsey, Bruce Schneier, David Wagner, “Key – Schedule of IDEA, G-DES, GOST, SAFER and Triple DES”.
- Joan Daemen, Rene Govaerts and Joos Vandewalle, “Weak Keys for IDEA”
Index Terms

Computer Science

Information Security

Key words

Encryption

Decryption

Real Time Systems

Time Based Key

Brute Force attack

Cryptanalysis

FPGA