Abstract

In cryptography, a block cipher is a deterministic algorithm operating on fixed-length groups of bits, called blocks, with an unvarying transformation that is specified by a symmetric key. Block ciphers are important elementary components in the design of many cryptographic protocols, and are widely used to implement encryption of bulk data. A block cipher is a method of encrypting text (to produce cipher text) in which a cryptographic key and algorithm are applied to a block of data (for example, 64 contiguous bits) at once as a group rather than applying it to one bit at a time. The primary purpose of encryption is to protect the confidentiality of digital data stored on computer systems or transmitted via the Internet or other computer networks. A recent promising low-cost alternative of advanced encryption standard (AES) on reconfigurable
Optimization of Block Cipher with SIMON

platforms called the SIMON. It has been implemented as the construction of the round function and the key generation of SIMON, that enables bit-serial hardware architectures which can significantly reduce the cost. Encryption and decryption can be done using the same hardware and also propose the hardware architecture of the smallest block cipher ever published on field-programmable gate arrays (FPGAs) at 128-bit level of security.

References


Index Terms

Computer Science

Information Sciences
Keywords
Aes    Simon    Block Cipher    Feistel    Fpga.