Indian J.Sci.Res. 17(2): 332-334, 2018 ISSN: 0976-2876 (Print)
ISSN: 2250-0138(Online)

FPGA IMPLEMENTATION OF SUBSTITUTION-PERMUTATION NETWORK BASED BLOCK CIPHER

[1]S. Soujanya,[2]K. Archana ,[3]Syeda Musharraf Taskeen
[1,2,3] Department of Electronics and Communication Engineering, Mahaveer Institute of Science & Technology, Hyderabad.

Abstract- Network Security & Cryptography is a concept to protect network and data transmission over wireless network. Data Security is the main aspect of secure data transmission over unreliable network. The rapid development in information technology, the secure transmission of confidential data herewith gets a great deal of attention. The conventional methods of encryption can only maintain the data security. The unauthorized user could access the information for malicious purpose. Therefore, it is necessary to apply effective encryption/decryption methods to enhance data security. Sensitive information sent over an open network may be scrambled into a form that cannot be understood by a hacker or eavesdropper. This is done using a mathematical formula, known as an encryption algorithm, which transforms the bits of the message into an unintelligible form. The intended recipient has a decryption algorithm for extracting the original message. There are many examples of information on open networks, which need to be protected in this way, for instance, bank account details, credit card transactions, or confidential health records. This paper presents FPGA implementations of the Substitution-permutation based block cipher with improved security.

Keywords- Security, Cryptography, substitution method

I. Introduction

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.The modern design of block ciphers is based on the concept of an iterated product cipher. Product ciphers were suggested and analyzed by Claude Shannon in his seminal 1949 publication Communication Theory of Secrecy Systems as a means to effectively improve security by combining simple operations such as substitutions and permutations . Iterated product ciphers carry out encryption in multiple rounds, each which uses a different subkey derived from the original key. A widespread implementation of such ciphers is called a Feistel network, named after Horst Feistel, and notably implemented in the DES cipher. Many other realizations of block ciphers, such as the AES, are classified as substitution-permutation networks. In cryptography, an SP-network, or substitution-permutation network (SPN), is a series of linked mathematical operations used in block cipher algorithms such as AES (Rijndael), DES, Tripple DES.

II. Existing Systems

Encryption algorithms can be divided into two different types: symmetric and asymmetric. Symmetric algorithms are those that use the same key for both encryption and decryption, and can be separated into block ciphers and stream ciphers. In a stream cipher each plaintext digit is encrypted one at a time with the corresponding digit of the keystream, to give a digit of the cyphertext stream. Block ciphers operate on large blocks of digits with a fixed, unvarying transformation. Block ciphers are generally well suited to implementation in software. They have the advantage that if an error occurs in the ciphertext, it will only affect the block in which it is located. The most common block ciphers are AES, DES, BLOWFISH, TPRIPLE DES and many others. Although the main objective of all these ciphers is to provide secure information, the way of approach is different. the proposed implementation of substitution-permutation based block cipher is developing new algorithm using the fundamental blocks of some block ciphers.

III. Existing Algorithms

A. Advanced Encryption Standard:

In a standard AES algorithm, there are four steps i.e. SubByte, ShiftRows, MixColumns and AddRoundKey in normal rounds for both the Cipher and its Inverse.

(a) SubBytes - The bytes substitution transformation is a non-linear substitution ofbytes that operates independently on each byte of the State using a substitution table (Sbox). This S-box is also invertible.

[1]Corresponding Author

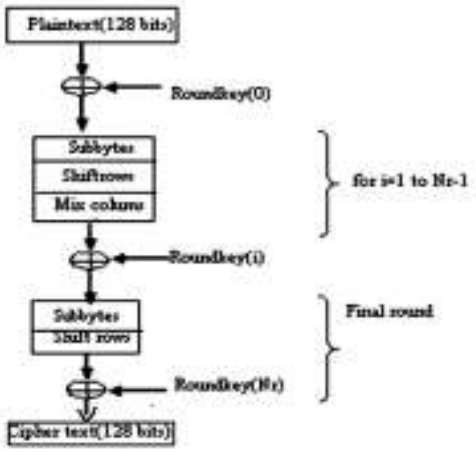

Figure 1: AES Algorithm for Encryption**.**

(b)ShiftRows – In the Shift Rows transformation ShiftRows, the bytes in the last three rows of the State are cyclically shifted over different numbers of bytes (offsets). The first row is not shifted.

(c) MixColumns - a mixing operation which operates on the columns of the state, combining the four bytes in each column using a linear transformation.

(d) AddRoundKey - each byte of the state is combined with the round key; each round key is derived from the cipher key using a key schedule.

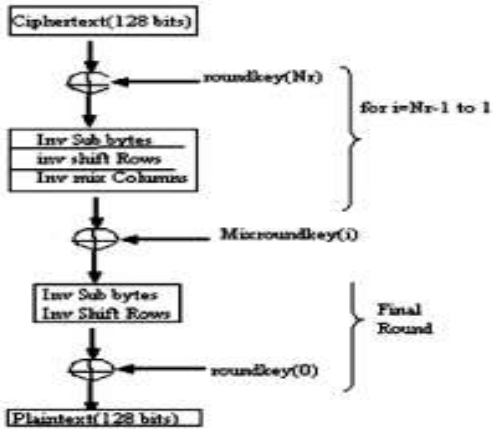

Figure 2: AES Algorithm For Decryption.

B. Data encryption standard:

DES performs an initial permutation on the entire 64 bit block of data. It is then split into 2, 32 bit sub-blocks, Li and Ri which are then passed into what is known as a round , of which there are 16 (the subscript i in Li and Ri indicates the current round).

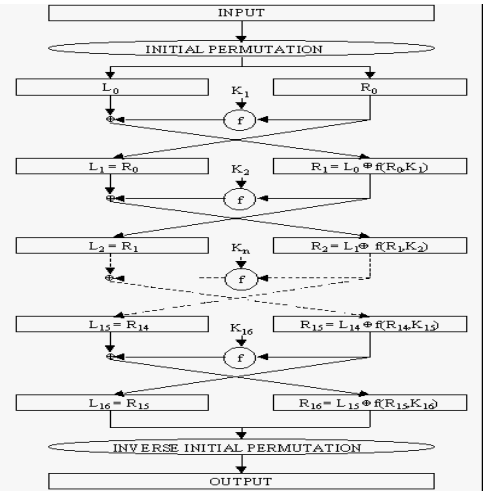

Figure 3: DES Algorithm

Each of the rounds are identical and the effects of increasing their number is twofold - the algorithms security is increased and its temporal efficiency decreased. Clearly, these are two conflicting outcomes and a compromise must be made. For DES the number chosen was 16, probably to either guarantee the elimination of any correlation between the ciphertext and the plaintext or key 6. At the end of the 16th round, the 32-bit Li and Ri output quantities are swapped to create what is known as the pre-output. This [R16, L16] concatenation is permuted using a function which is the exact inverse of the initial permutation. The output of this final permutation is the 64 bit ciphertext.

Iv. Proposed Approach

In cryptography, an SP-network, or substitution-permutation network (SPN), is a series of linked mathematical operations used in block cipher algorithms such as AES (Rijndael), DES. Such a network takes a block of the plaintext and the key as inputs, and applies several alternating "rounds" or "layers" of substitution boxes (S-boxes) and permutation boxes (P-boxes) to produce the ciphertext block.

The S-boxes and P-boxes transform (sub) blocks of input bits into output bits. It is common for these transformations to be operations that are efficient to perform in hardware, such as exclusive or (XOR) and bitwise rotation. The key is introduced in each round, usually in the form of "round keys" derived from it. (In some designs, the S-boxes themselves depend on the key.).Decryption is done by simply reversing the process (using the inverses of the S-boxes and P-boxes and applying the round keys in reversed order).

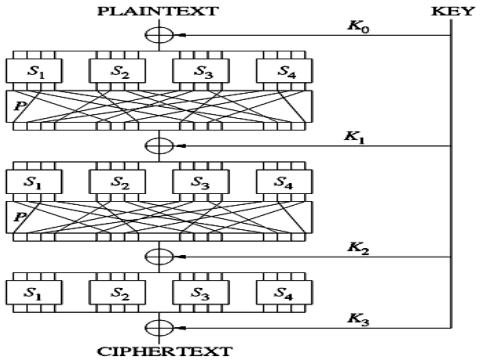

Figure 4: General Block Diagram Of SPN Based Block Cipher.

V. Hardware And Software Requirements

XILINX ISE 9.1i, SPARTAN3E FPGA.

VI.Results

In our paper we are giving data in the form of block of the plaintext and the key , and applying several alternating "rounds" or "layers" of substitution boxes (S-boxes) and permutation boxes (P-boxes) to get the ciphertext block and is the Resultant of Encryption method. Decryption is done by simply reversing the process that is ciphertext and reversed keys as input, applying alternating to get original plaintext.

References

[1] High Throughput-less area efficient FPGA implementation of block cipher aes algorithm, International journal of Computer Science and its Applications, [ISSN 2250 – 3765].

[2] Block Ciphers - Analysis, Design andApplications, Lars Ramkilde Knudsen July 1, 1994.

[3] Joan Daemen and Vincent Rijmen, AES submission document on Rijndael, Version 2, September1999. http://csrc.nist.gov/CryptoToolkit/aes/rijndael/Rijndael.pdf

[4] Applied cryptography: protocols, algorithms, and source code in C, second edition, Bruce scheneir.

[5] AES Proposal: Rijndael, Joan Daemen, Vincent Rijmen, Document version 2.

[6] A primer on electronic document security, Technical Whitepaper.

[7] wikepedia.com/cryptography