International Journal of Computer Science and Software Engineering (IJCSSE), Volume 5, Issue 1, January 2016
ISSN (Online): 2409-4285 www.IJCSSE.org Page: 11-13

New Paradigm Design by Merging the Techniques of Stream Cipher with Block Cipher

Maki Mahdi

Al-Nisour University College/Department of Computer Technical Engineering/Baghdad, Iraq

dr.makimahdi@yahoo.com

ABSTRACT

Symmetric primitives are important units in any cryptographic system, they are the tools for encryption of a data stream. Symmetric primitives are usually divided into block ciphers and stream ciphers, both classes are important to keep the security of data and also both have their advantages and disadvantages, for block cipher is harder in cryptanalysis but its slower in work in other word it works offline always. Stream cipher is faster than block cipher and works online. In this research we attempt to merge some of block cipher techniques that make the block ciphers harder in cryptanalysis (such as S-Box (Confusion) and P-Box (Diffusion)), for design stream cipher also this search presents new paradigm of using. Linear feedback shift register with variable length to avoid the known cryptanalytic attacks(auto correlation attack and linear complexity), and presents a novel stream cipher based on word-oriented not based on bit-oriented to make the stream cipher faster to encrypt the data in some applications that have huge data, like image processing, video, audio, and database management.

Keywords: *Novel Stream Cipher, Block Cipher, Linear Feedback Shift Register (LFSR).*

1. MOTIVATION

Cryptography is used in information security to protect information from unauthorized or accident disclosure while the information is transmitted (either electronically or physically) and while information is in storage.

A cipher is a pair of algorithms which creates the encrypttion and the reversing decryption, the detailed operation of a cipher is controlled both by the algorithm and, in each instance by a key as shown in figure(1).

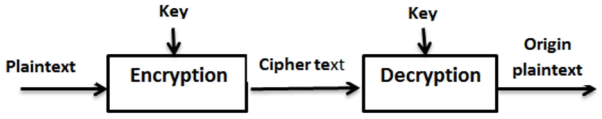

Fig. 1. (Encryption and Decryption process)

There are two general types of key-based algorithms, the first type is the asymmetric (public-key) algorithms which are designed so that the key used for encryption is different from the key used for decryption, and the second type is the symmetric algorithms where the encryption key can be calculated from the decryption key and vice versa.

In most symmetric algorithms, the encryption key and decryption key are the same; these algorithms are also called secret-key algorithms or one-key algorithms. Symmetric algorithms can be divided into two categories, some operate on the plaintext of a single bit at time, these are called stream cipher or stream algorithms, others operate on the plaintext in groups of bits are called block and the algorithms are called block cipher or block algorithms.

2. BLOCK CIPHER

In cryptography, a block cipher is a symmetric key cipher which operates on fixed-length groups of bits, termed blocks. A block cipher consists of two paired algorithms one for encryption (E), and another for decryption (E-1). Both algorithms accept two inputs: an input block of size n-bit and a key of size k-bit, yielding an n-bit output block (as shown in figure 2).for any one fixed key, decryption is the inverse function of encryption, so that

$$E^{-1}_k (E_k (M)) = M$$

For any block M and key K.

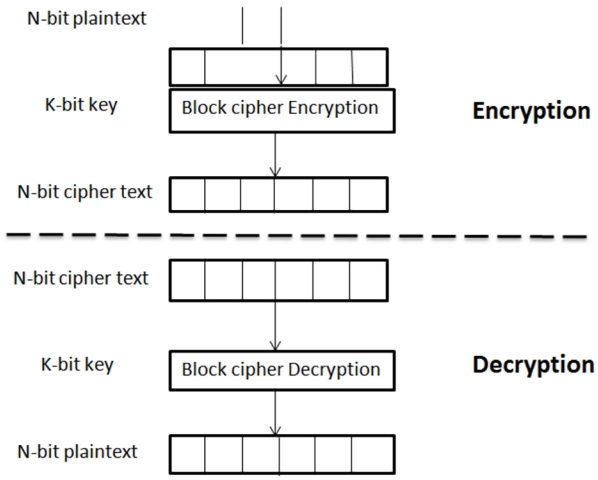

Fig. 2. (Block cipher process)

Some of block cipher techniques:

There are two principles which can be used in block cipher to make it secure and resistant to statistical attacks, Confusion (Substitution) serves to hide any relationship between the plaintext, the ciphertext, and the key. A good confusion makes the relationship statistics so complicated that even these powerful cryptanalytic tools won't work. Diffusion (permutation) spreads the influence of individual plaintext or key bits over as much of the ciphertext as possible, this also hides statistical relationships and makes cryptanalysis more difficult, sometimes a block cipher that incorporates layers of substitution (always called S-Box) and permutation (is called P-Box).

S-Box:

The S-Box is simply a substitution: mapping of m-bit inputs to n-bit outputs this S-Box is called "mn S-Box ". S-Boxes are generally the only nonlinear step in an algorithm they are what give a block cipher its security and its powerful against cryptanalytic attacks. The bigger they are the better.

P-Box:

The permutation is required to provide the necessary diffusion of the outputs from the S-Boxes over as many of the S-Boxes inputs in the next layer as possible,[3].
This permutation (P-Box) maps each input bit to an output position, no bits are used twice and no bits are ignored.

3. STREAM CIPHER

A stream cipher is a symmetric key cipher where plaintext bits are combined with a pseudorandom cipher bit stream (key stream), an Exclusive-OR (XOR) operation. In stream cipher the plaintext bits are encrypted one bit at time.
Pseudorandom key generator (RKG):
Usually RKG is based on shift register to generate stream of bits as key stream there are many types of shift register the more known is linear feedback shift register LFSR.
An n-stage LFSR consists of shift register R= (r_n , r_{n-1} ,…,r_1) and tap sequence T = (t_n , t_{n-1}, … , t_1),
Where each r_i and t_i is one bit, at each step bit r_1 is appended to the key stream, bit r_n , … , r_2 are shifted right and a new bit derived from T and R is inserted into the left of the register (see figure 3).

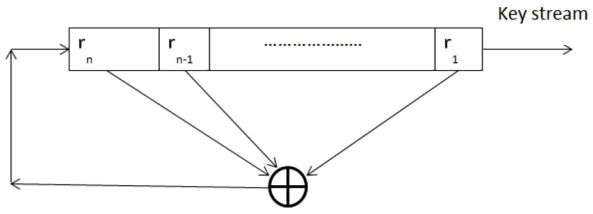

Fig. 3. (Linear feedback shift register)

An n-stage LFSR can generate pseudorandom bit strings with a period (2^n – 1). To achieve this tap sequence *T* must cause *R* cycle through (2^n – 1) nonzero bit sequence before repeating.

4. PROPOSED GENERATOR CONSTRUCTION

In stream cipher cryptography, a well-known construction for generating key streams is using clock-controlled linear feedback shift registers (LFSRs) based on pseudorandom binary sequences (PRBs) their output comes out from right most stage and input feedback bit comes in to left most stage and output bit usually combined with output of other LFSR through combination function mostly be nonlinear function. In most cases the output of LFSR consists of one bit to form the key stream. The stream cipher construction proposed in this research is based on the LFSR with different manner and using two main Block cipher techniques that considered as block cipher's advantages (S-Box and P=Box), in other words the proposed generator is hybrid the advantages of the stream cipher and block cipher, the proposed key stream generator structure consists of two parts, the first part contains four LFSRs denoted by SR_1 , SR_2 , SR_3 , and SR_4 , as depicted in figure 4. The shift

registers SR_1,SR_2,SR_3, and SR_4 have length 128 equally, the LFSR lengths were chosen to ensure relatively prime periods *with* (P_{SR1} , P_{SR2} , P_{SR3} , P_{SR4})= 1 , where P_{SRn} is the PRBs period of LFSR SR_n , the second part contains four S-Boxes with different contents , each S-Box is consisting of 256×256 matrix, the content of each matrix is random numbers (0 through 255), the output of S-Box is 8-bit, finally there is one P-Box contains random numbers (o through 8).

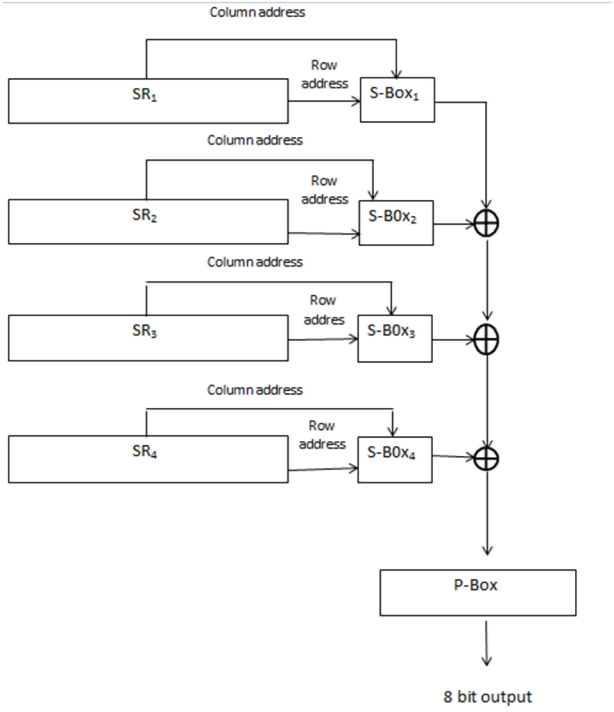

Fig. 4. The proposed generator

From each SR_n extracted two set of bits from fixed stages , each set consists of 8-bit these two sets represent the row and the column addresses in S-Box matrix respectively their crossing produce 8-bit are output of S-Box, the output of the four S-Boxes then Xored together to produce 8-bit, the P-Box receives this 8-bit to modify their positions based on the eight random numbers to form the 8-bit output of key stream generator , after each using of S-Boxes, their contents shifted vertically and horizontally and the content of P-Box also shifted horizontally.

The proposed generator initialization is as follows:

- The key initialization of LFSR is simply done by loading the LFSRs with 512 bits.
- The contents of four S-Boxes and P-Box are filled in the first application of generator by random numbers.

The security analysis of proposed generator is:

- The complexity of four LFSRs is 2^{512} and the four S-Boxes are 10^{262144} ((256×256×4) mod 40) in addition to P-Box is 10^8.
- The complexity of S0Boxes and P-Box are derived from its nonlinearity because shifting its contents at each use and the output of S-Boxes and P-Box are different until the same two inputs is used.

5. CONCLUSIONS

Novel stream cipher design with Block cipher characteristics merge the advantages of Block cipher with stream cipher and make the stream cipher is harder to cryptanalysis, as well as this paradigm enable to use LFSR with short length where the complexity can be increased by using confusion and diffusion, also the novel stream cipher make good choice to encrypt the huge data applications. The output of this generator are block of 8-bit can encrypt block of 8-bit of plaintext.
The complexity of this paradigm can be increased by using more than four LFSRs and large S-Boxes that is make the output of key stream generator mare than 8-bits (as 16-bits or more).

REFERENCES

[1] S. Bono, M. Green, "Security analysis of a cryptographically", In proceedings of the USENIX security symposium, August 2005.
[2] R. Oppliger, "Contemporary Cryptography", Artech House, Inc.,2005.
[3] Wikipededia the free encyclopedia: Federal Standard 1037c.Institute for telecommunications Science. Retrieved on 18/9/2012 from Http://en.wikipedia.org/wiki/security.