RANDOMIZATION-BASED BLOCK CIPHER WITH KEY-MAPPED S-BOX SELECTION

Krishna Prasad Nandeti ¹, Dr. Anshuman Singh ² and Dr. Mahmoud Yousef ³

¹Graduate Assistant, University of Central Missouri, Warrensburg, USA

²Asst. Professor of Computer Science, University of Central Missouri, Warrensburg,
USA

³Professor of Computer Science, University of Central Missouri, Warrensburg, USA

ABSTRACT

This paper proposes a new system of Substitution-Permutation network along with Randomization Expansion of 240 bits of input data. System uses 16 S-Boxes which are selected randomly based on the sub-key values throughout 64 rounds of substitution steps. 64 sub-keys are generated during the Substitution-Permutation process. The middletext is transposed based on decimal value of the sub-key generated during the each round. A CBC mode is the best associated with this system.

KEYWORDS

Middletext, Randomization, SP-network, S-Box, CBC

1. INTRODUCTION

In this internet world every transaction of data is confidential. Day by day the importance of the information security is exponentially increasing. Any organization that relies on transmitting the data is prone to an attacker on the network. Under these critical circumstances we need to protect our data using Cryptographic algorithms [2,4,5] which morph the data before transmitting over networks or store it in a physical location. Cryptography [2,4,5] is a field of study where the data is secured by changing it to non-readable format using different types of algorithms. Every algorithm has its own merits and demerits. In this paper we proposed a new approach to randomize the substitution and permutation which will remove any linearity of the system.

2. CIPHER DESIGN

A random encryption system [1] can be defined as a quadruple (M, K, R, C) where M denotes the message space, K denotes the key space, R denotes the set of random bits, C is the ciphertext space. for $x \in M, k \in K, r \in R$ the deterministic function ψ can be denoted as $\psi: M \times R \times K \rightarrow C$ and Π is a relation expressed as $\Pi = \cup_{r \in R, k \in K, x \in M} (x, k, \psi(x, r, k))$. The relation Π is the set of all possible ciphertexts for a message key pair.

Figure 2.1 Encryption Process

The encryption system is a combination of two important divisions.

1. Randomization expansion
2. Substitution-Permutation network

In this paper we take messages (Plaintext) of length 240 bits and random sequence of bits of length 16. After encryption the ciphertext length will be 256 bits. we use 16 S-Boxes [7] to substitute middletext which are selected based on the key bits throughout 64 rounds of the substitution-permutation network [7]. Randomization expansion [1] is purely based on the 16 random bits generated. The S-Boxes and the key has no role in the randomization expansion.

Figure 2.2 Encryption System

a. Randomization expansion

Randomization [1] provides a set of ciphertexts corresponding to message and key pair. A 16-bit string is generated randomly which is used] to XOR the 240-bit plaintext. Later this 16-bit random generated string is appended to the XOR-ed output of 240-bit plaintext keeping the bandwidth expansion factor [1] to 1.066 and possible ciphertexts to 65,536 for a message and key pair. This is achieved by dividing 16-bit random generated string into 4 equal halves i.e., 4 halves of 4 bits each and XOR 240 bits of plaintext. The output obtained after XOR is concatenated [1] with 16-bit random generated string.

Figure 2.3 Randomization Expansion

b. Key generation

The key is expressed as 512 bits block K, where parts of the key are pulled to make subkeys [7] for each round. There are 5 subkeys for each round which allows substituting and permuting the data. The subkeys are not always pulled from same positions but are pulled from different positions in the key block. At the start of the each round the key block is left circularly shifted using the decimal value of the subkey K0 which is derived using

$$K0 = K(128 + (i \times 4), 131 + (i \times 4))$$

where i is the number of the round. The idea behind left circular shift is to generate a different key block for every round. The possible shift is between 0 to 16 bits. The subkey K0 is always pulled at the start of each round, whereas the other subkeys are taken after the left circular shift [7] of the key block K in that particular round. The decimal value of the subkey

$$K1 = K(i \times 4, (i \times 4) + 3)$$

chooses the S-Box for that particular round and the decimal value of the subkey

$K2 = K((i \times 4) + 256, (i \times 4) + 259)$ chooses the specific row of the selected S-Box from where the middletext should be substituted in that round. The subkey K3 is given by

$$K3 = K(256 - ((i \times 4) + 3), 256 - (i \times 4) \oplus K(512 - ((i \times 4) + 3), 512 - (i \times 4)))$$

This subkey K_3 is concatenated with K_0 and the decimal value of those concatenated 8 bits are used to make a left circular shift of the middletext, which can make a shift of 0 to 256 bits every round. The key block K is divided into 4 equal halves which make 128 bits each and all the halves are XOR together to generate subkey K_4 . This subkey K_4 serves as a XOR factor at the end of the each round.

$$K_4 = K(0,127) \oplus K(128,255) \oplus K(256,383) \oplus K(384,512)$$

Fig 2.4 Key generation process

c. Round design

There are 64 rounds in the substitution-permutation network. Each round consists of a substitution from the S-Box and a permutation which is a left circular shift. Later after permutation the middletext is XOR with a subkey.

We have 16 S-Boxes numbered from 0 to 15. The S-Box for that specific round is selected by the subkey $K1$. As the subkey $K1$ is 4 bit the decimal value of it lies always between 0 and 15. Using a S-Box which is selected based on the key will make analysis difficult because each time key changes the order of selection of S-Boxes changes. To substitute bits from the S-Box the subkey $K2$ is used. the subkey $K2$ chooses the row of values to be substituted from the selected S-Box. The corresponding middletext values are substituted from the S-Box.

Now a permutation, a left circular shift is applied. The value of how many bits needs to be shifted is derived from the subkey $K3$ and $K0$. The subkeys $K3$ and $K0$ are concatenated [1] to form 8 bit string. Now the decimal value of this 8 bit string is used to perform the left circular shift on the middletext.

$$Middletext = Middletext \lll DecimalValue(K3 || K0)$$

Where $||$ is taken as concatenation of bit strings. The algorithm does not follow a specific permutation table [7,8] and only depends on the key. As the key changes the permutation values also changes. The middletext is divided into two halves and each half is XOR with the subkey $K4$. After XOR both the resultants are combined together and supplied as input to the next round.

Figure 2.5 Round Description

3. MODE OF OPERATION FOR EXPANSION CIPHERS

Among the modes of operation for block ciphers, CBC [3] mode can be used with a tweak for this algorithm. We cannot directly use the standard modes of operations as 240 bits of plaintext expands to 256 bits of ciphertext. To make this happen we will inject the Initialization vector [3] of 256 bits after the expansion of plaintext during encryption process. In the later stages the ciphertext of previous stage is used as input. All the properties of CBC mode remain unchanged.

Figure 3.1 CBC mode

4. EVALUATION

a. Plaintext - Ciphertext correlation

Plaintext - Ciphertext correlation [2,5,6] gives us a statistical weakness of the algorithm. This is taken greater care while developing the algorithm. By any means for the same set of Plaintext and the Key, Ciphertext will not be the same for different executions because of the Randomization expansion. And flipping a bit in the Plaintext or Key will never have the same Ciphertext bit positions changed. An analysis is done on large set of input Plaintexts at different levels in the encryption algorithm to observe how many bits are changed from the input to output.

First level of observation is on the Randomization expansion. This gives a clear idea of how many bits are changed in the level of Randomization expansion. We are 95% confident that 128.1117 bits are changed during this level. The summary of the analysis is as followed.

Minimum	1st Quartile	Median	Mean	3rd Quartile	Maximum
1.0	70.0	129.0	128.5	186.0	251.0

Table 4.1 T-test results for Randomization expansion

Second level of observation is on the 64 rounds of SP-network [2,4,5,6,8]. In this level the output of the Randomization expansion is taken as the input for evaluation and the final Ciphertext is taken as the output. Here we are 95% confidence that 127.9226 bits are changed between the rounds. The summary of the analysis is as followed.

Minimum	1st Quartile	Median	Mean	3rd Quartile	Maximum
97.0	123.0	128.0	128.0	133.0	158.0

Table 4.2 T-test results for SP-network

Third level of observation is on the whole encryption process. The input for evaluation is the Plaintext and the output is the Ciphertext. We are 95% confident that 127.9452 bits are changed throughout the encryption process. The summary of the analysis is as followed.

Minimum	1st Quartile	Median	Mean	3rd Quartile	Maximum
97.0	123.0	128.0	128.0	133.0	167.0

Table 4.3 T-test results for the Encryption process

Summarizing the three levels of analysis it is evident that on an average 128 bits are changed at random places of the Ciphertext for every execution.

b. S-Box security

The most non-linear part of the algorithm is the Substitution-Permutation network [4,5,6]. The design criteria of each S-Box are as follows.

- 1) Each S-Box takes 4 input bits and gives 4 output bits.
- 2) The output bits are not related with any of the input bits. The values of the S-Box are random generated fixed values.
- 3) Each S-Box has 256 substitution values which is a 16x16 matrix. The values follow the rules

$$\bigcap_{j=0}^{15} S_{i,j} = \phi \quad \bigcap_{i=0}^{15} S_{i,j} = \phi$$

Where S represents the S-Box, i is the row and j is the column.

- 4) The column indexes are the input values and the values for that particular round to be substituted are based on the sub key and represent the row indexes.

Addition to this, the design of the algorithm itself eradicates the linearity in it. For every round a S-Box is selected based on the sub key value, and which row of values should be substituted is decided by another sub key. For instance, let us take each output of S-Box are linear functions, but these linear functions are chosen randomly based on the sub key values not in the linear

fashion. The randomization expansion provides more complexity to this step by changing the input Plaintext bits to a great extent.

Another part of the non linearity [6] is the permutation. Unlike in DES, we do not use a fixed P-Box to permute the bits. The value of permutation is decided by the sub key for each round making analysis nearly impossible.

5. CONCLUSION

In this paper we illustrated new approach of encrypting and decrypting the data using a symmetric key. This approach can be applied on any file formats which can be read as binary data. In this paper we used 240 bit plaintext as our block size, further enhancements can be done on increasing the block size. The ciphertext is of length 256 bits which 16 bits of it is a data head because of randomization expansion. A possible future enhancement can be the removal of 16 bits data head but still should be able to do randomization expansion.

REFERENCES

- [1] Rivest, Ronald L., and Alan T. Sherman. "Randomized encryption techniques." In *Advances in Cryptology*, pp. 145-163. Springer US, 1983.
- [2] Schneier, B. *Applied Cryptography*, Second Edition: protocols, algorithms, and source code in C. New York: Wiley, 1996.
- [3] Dworkin, M., NIST Special Publication 800-38A, 2001 Edition: Recommendation for Block Cipher Modes of Operation, Methods and Techniques, December 2001, Natl. Inst. Stand. Technol. [Web page], <http://www.csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf>
- [4] I. Tanenbaum, AS.: "Computer Networks" 2nd edition, Prentice Hall, London. 1989
- [5] *Cryptography and Network security*, 2nd Edition by Atul Kahate. Tata Mc- Graw-Hill Publications, New Delhi.
- [6] Biham, Eli and Shamir, Adi (1991). "Differential Cryptanalysis of DES-like Cryptosystems" *Journal of Cryptology*. 4 (1): 3–72
- [7] National Institute of Standards and Technology. *Data Encryption Standard*. FIPS PUB 46-2. December 30, 1993..
- [8] "Announcing the ADVANCED ENCRYPTION STANDARD (AES)" Federal Information Processing Standards Publication 197. United States National Institute of Standards and Technology (NIST). November 26, 2001