Design of a Practical Substitution Permutation Network Cryptosystem

Khulood H. Eltartor *
Ibtehaj B. M. Algharbawi *
Raed M. I. Murad **

الملخص

تصميم مقترح لنظام تشفير تطبيقي باستخدام شبكة التبديل و التقليب

دراسة تطبيقية

يعتبر نظام التشفير من الخوارزميات التي تقوم بعمليتي التشفير وفك التشفير، من خلال هذه الدراسة قمنا بتصميم نظام تشفير متكامل بناء على نظام التبديل و التقليب Substitution Permutation Network (SPN) الذي صممه Festiel عام 1973 والذي يتكون من خمس مراحل متكررة ومتتالية من التبديل والتقليب.

أجرينا العديد من التعديلات والتطويرات على نظام Festiel وذلك للحصول على نظام تشفير أكثر سريةً وأمناً ضد طرق الإختراق المختلفة، وذلك بالإضافة إلى توسعة نظام Festiel لاستخدامة في العديد من التطبيقات المختلفة كمواقع المحادثة والبريد الإلكتروني و بطاقات الائتمان وغيرها.

نظام التشفير المقترح يتكون من خمس منظومات تبديل و تقليب متوازية كل منها تتكون من خمس مراحل بحيث تحتوي كل مرحلة على أربعة صناديق تبديل من النوع (4x4 S-Boxes) متطابقة مختلفة في التصميم عن صناديق التبديل للمرحلة التي تليها، تتعامل كل منظومة تبديل وتقليب مع معلومة ذات طول رقمي 16 منزلة رقمية ثنائية (16 binary bits) ، يتم دمج هذه المعلومة مع خمسة مفاتيح تشفير مختلفة لا تعتمد على بعضها البعض يتم توليدها بطريقة عشوائية بحيث تكون موزعة على مراحل المنظومة الخمس. كما يعتبر استخدام خمس منظومات متوازية مؤهلاً للنظام لكي يقوم بتشفير نص طوله الرقمي 80 منزلة رقمية ثنائية أي بطول 10 أحرف أبجدية تبعاً لنظام أسكي كود بحيث يقوم بتشفير هذه الأحرف في نفس اللحظة

*Department of Computer, The Islamic University, Gaza, Palestine, engkhulood@yahoo.com , eng_ibtj@yahoo.com
**Palestine Technical College, Deir El-Balah, Palestine (Supervisor).
raedmrm_2000@yahoo.com

الزمنية، كما أنه يمكن مضاعفة عدد أحرف النص إلى الضعف عن طريق اسـتخدام مـسجلات الترميز من نوع Convolutional Decoders/Encoders ليصبح عدد الأحرف المشفرة فـي نفس اللحظة الزمنية 20 حرف أي بطول رقمي مقداره 160 منزلة رقمية ثنائية يتم دمجها مـع 25 مفتاح تشفير مختلفة مما يؤهل النظام للدخول ظمن أنظمة التشفير المعيارية التطبيقية الحديثة التي تقوم بتشفير نص رقمي يتراوح طوله ما بين 128 إلى 512 منزلة رقمية ثنائية فـي نفـس اللحظة الزمنية.

يوفر النظام المقترح إمكانية تشفير الرسائل بغض النظر عن أطوالهـا الرقميـة و ذلـك بتجزئة الرسالة إلى نصوص كل منها بطول 20 حرف (160 منزلة رقمية ثنائية) ومن ثم تشفير هذه التصوصعلى التوالي.

ABSTRACT

The cryptosystem is an algorithm that executes encryption and decryption processes. In this work, we introduce a cryptosystem based on Festiel's Substitution Permutation Network (SPN) cryptosystem designed in 1973 which consists of five rounds. A number of modifications were added to Festiel's SPN in order to increase its security and expand its capacity to be considered as standard block ciphers. The modified SPN consists of five parallel SPN's, each one employs four different mappings (4x4 S-boxes) distributed to its first four rounds. In addition, five random independent keys are generated for each SPN to encrypt its 16-bit input (2-character input). The overall plaintext of the designed cryptosystem is 80-bit length (10-character plaintext). Since the typical plaintext of a block cipher ranges between 128-512 bits, a convolutional decoding/encoding process is applied to the 80-bit plaintext to expand capacity of the designed cryptosystem to 160-bit length plaintext to be sufficient to encrypt/decrypt 20-character plaintext using 20 different S-boxes and 25 different 16-bit sub-keys. Regardless the length of the plaintext, the proposed cryptosystem applies the encryption process by dividing the plaintext into 20-character blocks to encrypt them sequentially.

Keywords: cryptosystem, substitution permutation network (SPN), substitution box (S_Box), key, cryptographic testing criteria, LAT, EMOSAC, DDT, NC, MOBIC.

INTRODUCTION:

Cryptosystem is an algorithm that executes encryption and decryption processes. The proposed cryptosystem is classified as a symmetric key block cipher based on the SPN introduced by Festiel [7, 8] and tested by different cryptographic security criteria measures related and illustrated by Murad and Yucel [16]. The main objective of this paper is to introduce a design of a practical and strong expanded SPN cryptosystem. The strength of this cryptosystem depends on the strength of its elements which are the 4×4 bijective S-Boxes. The overall employed S-boxes (20 different mappings) are chosen from a set of 300 randomly generated S-boxes. The strength of each chosen S-box is confirmed using different cryptographic testing criteria such as, Linear Approximation Tables (LAT), Expanded Maximum Order Strict Avalanche Criterion (EMOSAC), Difference Distribution Tables (DDT), Nonlinearity Criterion (NC) and Maximum Order Bit Independence Criterion (MOBIC). In the next section of this work, the cryptographic testing criteria are summarized and followed by the results of testing the S-Boxes of the SPN cryptosystem using these criteria. The third section of the paper explains the structure of a single SPN cryptosystem. Finally, we introduce the designed cryptosystem in section 4 using the tested S-Boxes according to the results provided in section 2. The proposed cryptosystem complicates the job of cryptanalysts to attack SPN block ciphers because it increases the randomness of the cryptosystem by means of the randomly generated S-boxes and independent sub-keys. Moreover, it modifies the SPN cryptosystem to be a practical block cipher and one of typical block-length ciphers. The designed cryptosystem is exploited to provide the security needed in many applications such that, email servers, chatting servers, smart cards, and so on. The designed cryptosystem has been applied to a chatting program which provides a secure way to exchange secure data among many clients.

In the next section of this work, the cryptographic testing criteria are summarized and followed by the results of testing the S-Boxes of the SPN cryptosystem using these criteria. The third section of the paper explains the structure of a single SPN cryptosystem. Finally, we introduce the designed cryptosystem in section 4 using the tested S-Boxes according to the results provided in section 2.

Cryptographic Testing Criteria:

Cryptographic testing criteria are statistical methods used to test the cryptographic strength and the security measures of an S-Box. A number of testing criteria appearing in literature [16, 10, 21] such as LAT, NC, EMOSAC, DDT, and MOBIC are used to test the security of randomly generated S-Boxes. Depending on the results obtained from these testing criteria, the best 20 S-Boxes are chosen to be employed in the proposed design of the SPN cryptosystem. A summary of these criteria are presented in Table (1).

Table1. Summary of Testing Criteria

Testing Criteria	Definitions and Security Conditions
LAT	•Is employed to determine all possible linear relationships between the input and the output bits of the S-Box. •Each element of the normalized LAT represents a bias of a linear expression. The less high-bias linear expressions are found, the more secure the S-Box is.
NC	•Gives the nonlinearity measures between the input and the output bits of the S-Box. •The less low-nonlinearity measures are found, the more secure the S-Box is.
EMOSAC	•Gives the probability of the change in any single output bit (or any linear combination of the output bits) when any single input bit (or any combination of input bits) are flipped. •The more probabilities of 1/2 are found, the more secure the S-Box is.
DDT	•The normalized DDT gives the probability of occurrences of $\mathbf{\Delta Y}$ (an output difference) given $\mathbf{\Delta X}$ (an input difference). •The less low-probability measures are found, the more secure the S-Box is (the worst case is 8/16).
MOBIC	•Gives the correlation coefficient between each pair of the avalanche variables of the output bits whenever any single input bit (or a combination of input bits) is inverted. •The smaller the correlation coefficients (i.e., zero coefficients are the best), the more secure the S-Box is.

Relations among theses criteria were proved and developed by Murad and Yucel [16] in 2002 in order to simplify the testing process of an S-Box. In other words, instead of using all the criteria to test an S-Box, they developed a number of relations among them in terms of the autocorrelation functions (ACF) and the Walsh-Hadamard Transforms (WHT) [16] of the S-Box. So, it is easier for us to use the ACF and the WHT to evaluate the measures of testing criteria associated with each S-Box directly. Table (2) illustrates the critical security measures of 20 S-Boxes chosen among 300 randomly generated S-Boxes. These measures are evaluated by the employment of the ACF and the WHT in the testing criteria of Table 1.

Table 2. The results of the 20 chosen S-Boxes.

T.C. S-Box	$\overline{\text{LAT}}$	NC	EMOSAC	$\overline{\text{DDT}}$	MOBIC
S_{11}	One high bias = 3/8	One low measure=1/8	One high probability=1	No 8/16 One 6/16	One high correlation=-1
S_{12}	One high bias = 3/8	One low measure=1/8	One high probability=1	No 8/16 Two 6/16	One high correlation=-1
S_{13}	One high bias = -3/8	One low measure=1/8	One high probability=1	No 8/16 Two 6/16	No high correlation
S_{14}	One high bias = 3/8	One low measure=1/8	One high probability=1	No 8/16 One 6/16	One high correlation=-1
S_{21}	One high bias=3/8	One low measure=1/8	One high probability=1	No 8/16 Two 6/16	Three high correlation=1
S_{22}	No high bias	No low measure	No high probability	No 8/16 No 6/16	No high correlation
S_{23}	One high bias=-3/8	One low measure=1/8	One high probability=1	No 8/16 One 6/16	No high correlation
S_{24}	No high bias	No low measure	One high probability=1	No 8/16 Two 6/16	One high correlation=-1
S_{31}	One high bias=-3/8	One low measure=1/8	One high probability=1	No 8/16 One 6/16	No high correlation
S_{32}	No high bias	No low measure	No high probability	No 8/16 One 6/16	No high correlation
S_{33}	One high bias=3/8	One low measure=1/8	One high probability=1	No 8/16 No 6/16	No high correlation
S_{34}	One high bias=-3/8	One low measure=1/8	One high probability=1	No 8/16 Two 6/16	No high correlation
S_{41}	One high bias=-3/8	One low measure=1/8	One high probability=1	No 8/16 No 6/16	No high correlation
S_{42}	No high bias	No low measure	No high probability	No 8/16 No 6/16	No high correlation
S_{43}	One high bias=3/8	One low measure=1/8	One high probability=1	No 8/16 No 6/16	One high correlation=-1
S_{44}	One high bias=3/8	One low measure=1/8	One high probability=1	No 8/16 One 6/16	One high correlation=-1
S_{51}	One high bias=3/8	One low measure=1/8	One high probability=1	No 8/16 One 6/16	No high correlation
S_{52}	No high bias	No low measure	No high probability	No 8/16 No 6/16	No high correlation
S_{53}	One high bias=3/8	One low measure=1/8	One high probability=1	No 8/16 One 6/16	Three high correlation=1
S_{54}	One high bias=3/8	One low measure=1/8	One high probability=1	No 8/16 One 6/16	One high correlation=-1

One can say that the 20 chosen S-Boxes of Table (2) are the most secure S-Boxes among the 300 randomly generated S-Boxes. The security of theses S-Boxes is confirmed by the following points:

1- With respect to LAT test.

•The worst S-Box has only one high-bias close to ±1/2 which is ±3/8. Moreover, some S-Boxes do not have high bias. This confirms the strength of the S-Boxes against linear cryptanalysis [8].

•The biases of each column are randomly distributed through the elements of the normalized LAT matrices.

2- With respect to NC test:

•The worst S-Box includes one low-nonlinearity measure of 1/8. Moreover, some S-Boxes do not have low-nonlinearity measures, which support the security of the S-Boxes against linear cryptanalysis [8].

3- With respect to EMOSAC test:

•Most of EMOSAC measures are equal to 4/8, which is the maximum order SAC is highly satisfied for all input combinations, which means that the S-Boxes show strength against differential cryptanalysis [8]. Moreover, each S-Box has no more that one entry of P=1.

4- With respect to DDT test:

•Most measures are low-probability measures (less than 8/16). The highest probability found was 6/16 with a very limited numbers (The worst chosen S-Box has two measures of 6/16) which increases the security of the S-Boxes against differential cryptanalysis [8].

5- With respect to MOBIC test:

•Most MOBIC measures present low correlation between the avalanche variables. Moreover, each of the S-Boxes with ±1 correlation has a single measure of %100 correlation between the avalanche variables of the output bits.

According to the results of the above security criteria of the chosen S-Boxes, one can observe that these S-Boxes can be safely employed to be the elements of the SPN cryptosystem.

3. SPN Cryptosystem:

In 1945, Claude Shannon developed a cipher that alternates confusion and diffusion functions [22,9]. The confusion component is a nonlinear substitution on a small sub-block, and the diffusion component is a linear mixing of the sub-block connections in order to diffuse the statistics of the system. The Feistel cipher structure [7,8], which dates back to over a quarter century, was the first introduction to a practical architecture based on Shannon's concept (1945), this cipher structure consist of a sequence of rounds of small substitution (referred to as S-Box) easily implemented by table lookup and connected by bit position permutations or transpositions. Such ciphers are generally referred to as Substitution Permutation Network (SPN) [5,9].

Substitution and Permutation

Substitution (confusion) process is the idea of mixing linear and nonlinear operation in order to observe the relationship among the plaintext, ciphertext and key. S-Box acts as the substitution, so the most fundamental property of an S-Box is that the output bits can not be represented as linear operations on the input bits [6,9].

An equally important principle of block cipher is that of Permutation (diffusion operation), the idea that every bit of the ciphertext should depend on every bit of the plaintext and every bit of the key. In other words, the permutation portion of a round is simply the transposition of the bits or the permutation of the bit position, and can be simply described as : the output i of S-Box j is connected to input j of S-Box i [6].This ensures that the statistics of the plaintext are dissipated within the ciphertext, so that an attacker can not predict the plaintext that corresponds to a particular ciphertext, even after observing a number of (similar) plaintexts and their corresponding ciphertexts.

The round function is responsible for satisfying the basic substitution and permutation requirements. Hence, we want each bit of plaintext and each bit of the key to influence each bit of the ciphertext in a nonlinear but invertible manner.

By iterating the round function fixed number of times, we automatically obtain some security as a consequence of the fact that, after each iteration (or round) the output bits become more and more dependent on the input bits [18,9].

Structure of SPN:

An R-round SPN requires (R+1) N-bit keys, K1 ,K2 ,….,KR, KR+1. Each round consists of three stages to the encryption process: the key mixing stage, the substitution stage and the linear transformation stage. In the key mixing stage, the N-bit round input $p = [p_1 p_2 p_3 \cdot\cdot p_N]$ is bitwise XORed with the key $K = [k_1 k_2 k_3 \cdot\cdot k_N]$ for that round. In the substitution stage, the result from key mixing stage is partitioned into M sub-blocks of size n (N=Mn), and each sub-block becomes the input to a bijective $n \times n$ S-Box (a bijective mapping from {0,1}n to {0,1}n). M can also be defined as the number of S-Boxes per round. In the linear transformation stage, the output from the substitution stage is processed through an invertible (bijective) N-bit linear transformation. Classically, the linear transformation was a bitwise permutation, hence the origin of the name substitution permutation network.[16,14,13,9]. The linear transformation is usually omitted from the last round, since it is easily shown that its inclusion adds no cryptographic strength to the SPN. Figure (1) illustrates an example of SPN with N =16, M = n = 4, and R= 4.

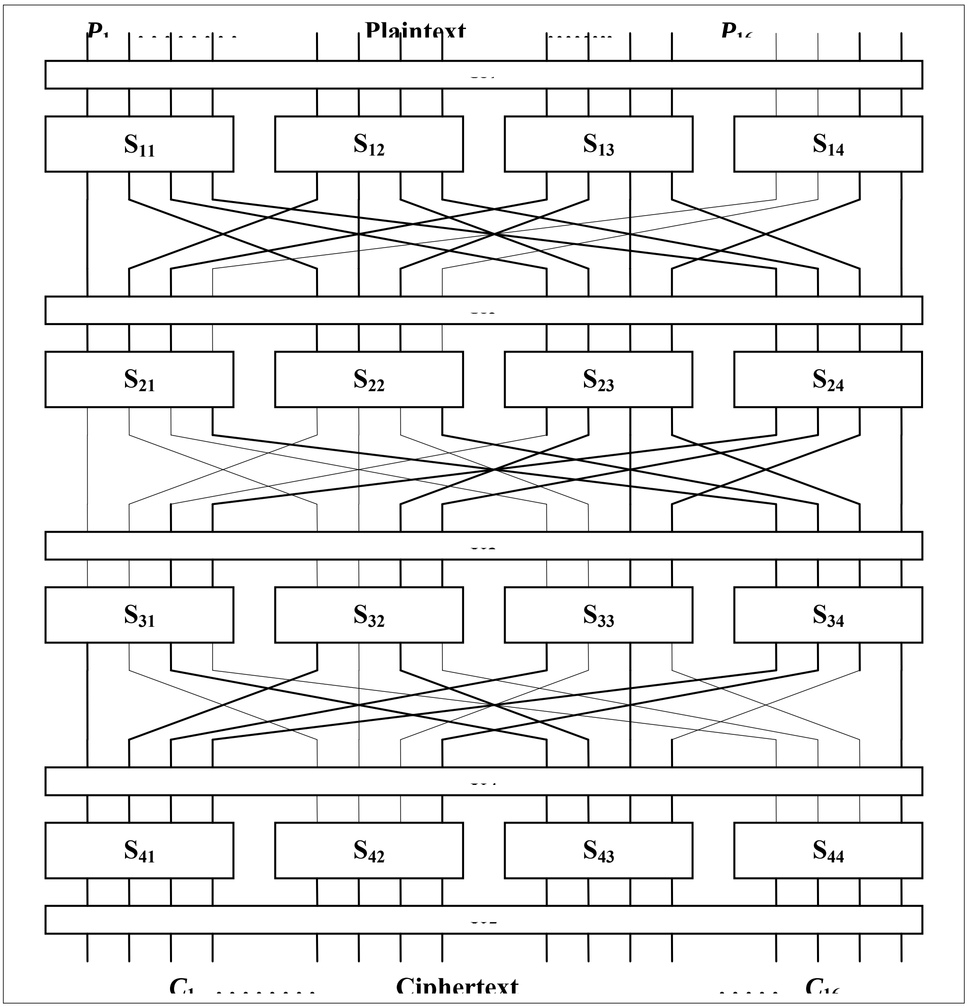


Figure 1. Basic Substitution Permutation Network Cipher

Decryption is accomplished by running the SPN "backwards", reversing the order of the rounds. The key KR+1 is first XORed with the ciphertext, followed by applying an inverse mapping for each S-Box in the round R, then resulting sub-blocks XORed with KR. For the other rounds (from R-1 to 1), the inverse permutation is applied, followed by an inverse mapping for each S-Box, then the resulting sub-blocks XORed with the corresponding K of that round [16,14,13,9].

A number of modifications are added to the SPN cipher to be stronger against cryptanalysis and attacking techniques; these modifications can be **summarized as follows:**

1. Using four different mappings through the SPN cipher. In other words, S-Boxes (1), S-Box (2), S-Box (3) and S-Box (4) represent the mapping process in the first, second, third and fourth round respectively.

2. Five random 16-bit keys for each are used to encrypt/decrypt two-character (16-bit) plaintext resulting in the corresponding ciphertext. Moreover, these five keys are randomly generated and independent of each other.

One can observe that this SPN can not be considered as a practical cryptosystem, because it encrypts/decrypts a small number of plaintext/ciphertext bits (i.e. 16 bits). The practical block cipher cryptosystems encrypts/decrypts a 128-512-bit block length plaintext/ciphertext. Regardless the block length of the input plaintext, the designed cryptosystem deals with plaintexts/ciphertexts has more than 20 characters by dividing them into 20-character blocks to encrypt/decrypt them sequentially. If the time factor is considered, the large cryptosystems dealing with large number of input bits are more secure against different methods of cryptanalysis. In other words, attacking such cryptosystems exhausts long time and hard effort. There are many ways to expand the SPN cryptosystem cipher such as; expanding the size of S-Boxes which leads to an expansion of the SPN. In the following section, we present another way of SPN expansion by using a number of parallel SPNs and applying decoding/encoding processes to compress/expand a plaintext/ciphertext of a typical block length. So, there will be no need for expanding the size of the previously tested 4×4 S-Boxes. This method will prevent us from testing larger size S-Boxes because they need a long time to be tested by the previously discussed security criteria.

A Practical Design of SPN Cryptosystem:

In this section, we introduce a new design of a practical algorithm represented by :

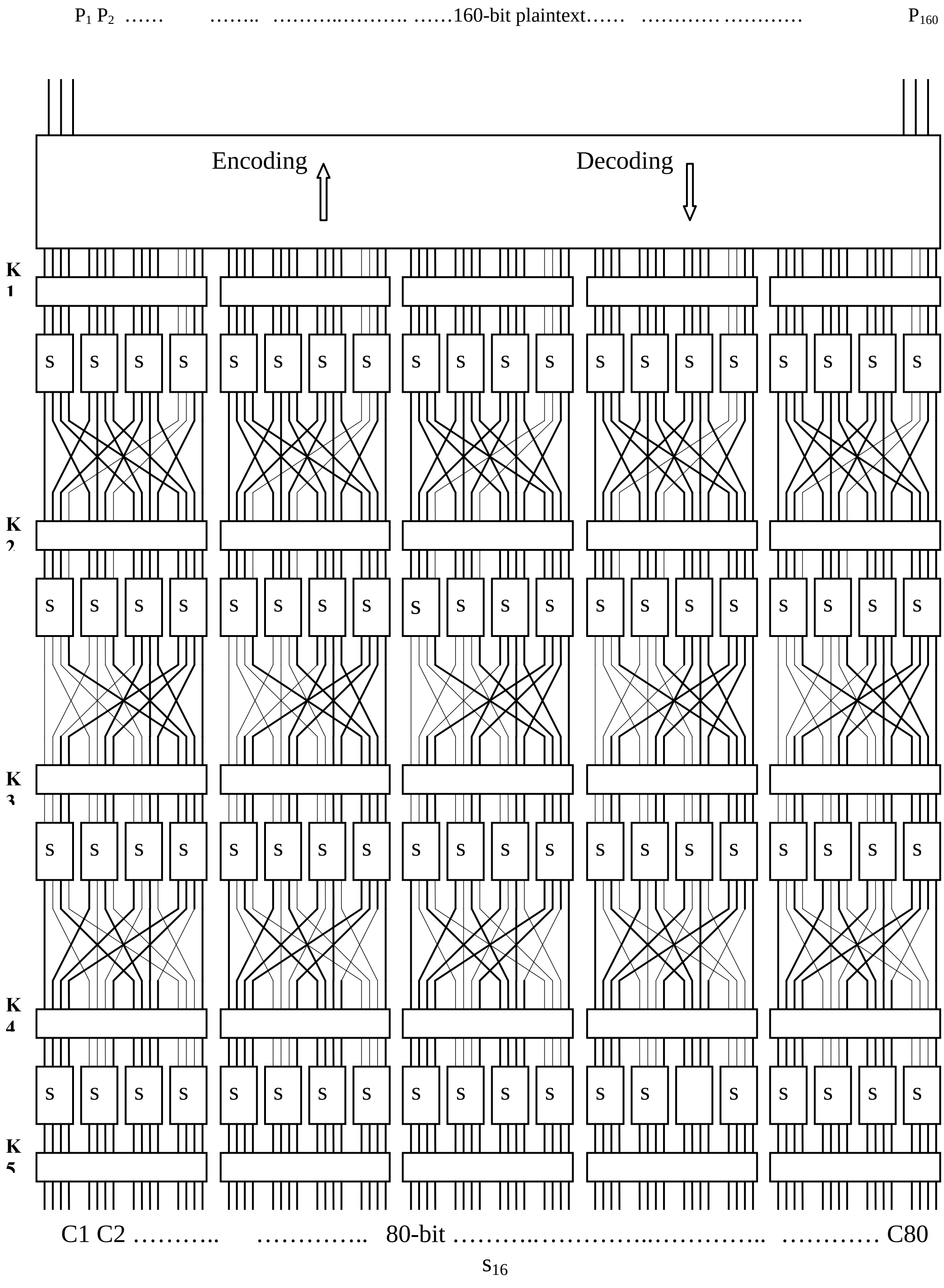
1- **Five Parallel SPNs:** In order to increase the block length of the plaintext/ciphertext, five parallel SPNs are used to construct the proposed cryptosystem.Since each SPN deals with 16 bits (2 characters) so, the designed SPN deals with $16\times5=80$ bits (10 characters).

2- **Decoding/Encoding Process:** Since 80-bit (result from 5 SPNs) block length of the plaintext/ciphertext is still less than the minimum length of the typical modern block ciphers cryptosystems, so we apply a decoding/encoding process. A convolutional decoder/encoder of two shift registers is employed to double the treated bits of the plaintext. In other words, the proposed design becomes able to deal with 20 characters (160-bit) instead of 10 characters (80-bit). At the transmitter, the 160-bit plaintext is decoded into 80-bit and then encrypted by the designed SPN cryptosystem that gives an 80-bit ciphertext. While at the receiver, the 80-bit ciphertext is decrypted using a designed cryptosystem with inverse mappings, so the decryption process produces 80 decoded bits which must be encoded to recover the original 160-bit plaintext.

3- **Random Keys:** To increase security and randomness of the designed cryptosystem, five different independent keys are generated randomly for each 20 characters. As a result many ciphertext may be produced for the same plaintext. Referring to Figure (2), one can observe that, each key (80-bit) is partitioned to five subkeys. These subkeys (16-bit) are distributed through the five SPNs.

One can observe that by using decoders/encoders of more than 2 shift registers the cryptosystem can be expanded to deal with plaintexts/ciphertexts of *r* times 80-bit block length, where *r* is the number of decoders/encoders shift registers.

The designed cryptosystem is cryptographically strong against different methods of cryptanalysis. The Strength of each SPN in the proposed system has been tested against linear and differential cryptanalysis [6,16] giving very low probability keys. This proves the strength of the proposed system against linear and differential cryptanalysis because the strength of the overall designed cryptosystem depends on the strength of its individual SPNs.


P1 P2 …… …….. ………..………. ……160-bit plaintext…… ……….. …………
P160
Encoding
Decoding
K 1
K 2
K 3
K 4
K 5
S
C1 C2 ……….. ………….. 80-bit ………..…………..………….. ………… C80
S16

CONCLUSION:

The designed SPN cryptosystem has different features make it practical and strong cryptosystem. First of all, expanding the cryptosystem using parallel SPNs reduces the time required to execute the encryption/decryption process of the overall plaintext/ciphertext.

Secondly, each SPN includes four different S-Boxes; one per round. So, the designed cryptosystem has 4×5=20 different S-Boxes of different mappings which increases the randomness of the overall cipher.

Then, using 20 different S-Boxes through the designed SPN cryptosystem increases the strength of the overall cryptosystem. So, if the cryptosystem is to be attacked by linear or differential cryptanalysis, five different models are going to be used in the attacking process. This means that the success in breaking one SPN dose not lead to a success in breaking the overall SPN cryptosystem. Furthermore, breaking one part of the system will not give the attackers any information about the other parts of it.

Another important source of the strength is the generation of five random keys (five 80-bit keys or 25 16-bit subkeys) for each 20 characters (160 bits) of the plaintext. Moreover, these five keys are independent of each others and randomly generated and changed randomly to another 25 subkeys whenever an new plaintext/ciphertext is to be encrypted/decrypted, so that, the produced ciphertext are different of each others with respect to the same plaintext.

The use of five random 80-bit keys complicates the attacking process. In other words, the attacking process must be applied partially to each single SPN of the designed cryptosystem. This means that the success of discovering one 16-bit subkey of a single SPN does not lead to the discovery of the other subkeys of the same SPN. Moreover, the discovery of this subkey does not lead to the discovery of the overall 80-bit key.

Finally, the designed cryptosystem is exploited to provide the security needed for many applications such as, email servers, chatting servers, smart cards, and so on. The designed cryptosystem was applied to chatting software designed by a computer programmer in Visual Basic Language and installed in the network of IUG Electrical and Computer Engineering Dapartment. The designed cryptosystem has proved a good security to exchange secure data among many clients.

REFERENCES:

1. A Menezes., P Van., O Orshot., and S Vanstone., October 1996: Handbook of Applied Cryptography, Fifth eddition, pp. 15-32.
2. Biham and Shamir., 1990 : Differential Cryptanalysis of DES-like Cryptosystem, Spring-Verlag, Advances in Cryptology-CRYPTO'90.
3. Chan Yeob Yeum., 2000 : Design, Analysis and applications of Cryptographic Techniques, phD. Thesis, Department of Mathematics, Royal Holloway, University of London, pp. 11-33.
4. Ed Schaefer., 1998: An Introduction to Cryptography, Santa Clara University.
5. Howard M. Heys and Stafford E. Tavares., September 1994: Substitution-Permutation Network Resistant to Differential and Linear Cryptanalysis, Department of Electrical and Computer Engineering, Queen's University, Kingston, Ontario, Canada, pp. 1-8.
6. Howard M. Heys., March 2001: A Tutorial on Linear and Differential Cryptanalysis, Technical Report CORR 2001-17, Center of Applied Cryptographic Research, Department of Combinatronics and Optimization, University of Waterloo.
7. H. Feistel., May 1973: Cryptography and Computer Privacy, Scientific American, Vol.228, no.5, pp. 15-23.
8. H. Feistel, November, 1975 : Some Cryptographic Techniques for Machine-to-Machine Data Communications, Proceedings of IEEE, Vol. 63, no.11, pp. 1545-1554,.
9. Ibtehaj Al-Gharbawi, Khulood El-Tartori And Raed Murad., July 2005: A SECURED SUBSTITUTION PERMUTATION NETWORK CRYPTOSYSTEM, P.S., Senior Project Report, Department Of Control And Communication Engineering, The Islamic University.
10. Isil Vergili and Melek D. Yücel., August 2001: Avalanche and Bit Independence Properties for the Ensembles of Randomly Chosen $n \times n$ S-Boxes, Turkish Journal of Electrical Engineering and Computer Sciences, Vol.9, No.2, pp. 137-145.
11. Jorge Auñón and V. Chandrasekar., 1997: Introduction to Probability and Random Processes, First eddition, McGraw-Hill, New York, London.
12. Kaliski, B.s. and Yin, Y.L. 1995: On Differential and Linear Cryptanalysis of the Rc-5 Encryption Algorithm, CRYPTO'95.
13. Keliher L., Meijer H and S. Tavares., 1997: A New Substitusion-Permutation Network Cipher Using Key-Dependent S-Boxes, Proceedings of Fourth International Workshop on Selected Areas in Cryptography

(SAC'97), Department of Computing and Information Science, Carleton University, Ottawa, Canada, pp. 13-26.

14. Keliher L., October 2003: Linear Cryptanalysis of Substitution Permutation Network, phD. Thesis, The School of Computing, Queen’s University, Kingston, Ontario, Canada, pp. 11-14.
15. Lai X. and Massey J., 1991: Markov Ciphers and Differential Cryptanalysis, advances in cryptology-EUROCRYPT'91.
16. Murad R. and Yucel M., July 2002: Relations among Cryptographic Security Criteria and Linear Cryptanalysis, M.s., Thesis, Department of Electrical and Electronics Engineering, Middle East Technical University.
17. Melek D. Yücel., 2003: Introduction to Cryptography, Lecture Notes, Middle East Technical University, pp. 1-20.
18. Mirza F., 1996: Block Ciphers and Cryptanalysis, Department of Mathematics, Royal Holloway University of London, Journal of Cryptography, pp. 2-12.
19. Papoulis A., 2002: Probability, Random Variables, and Stochastic Processes, Second eddition, Polytechnic Institute of New York.
20. Roddy D., 2001: Satellite Communications, Third eddition, McGraw-Hill, New York, London, Singapore, pp. 181,
21. Réjane Forré., 1998: The Strict Avalanche Criterion-Properites of Boolean Functions and Extended Definition, Springer-Verlag.
22. Stalling W., 2006: Cryptography and Network Security – Principles and Practices, Fourth edition, Prentice Hall, USA.
23. Silvester A., December 2004: Differential Cryptanalysis and Data Encryption Standard, Course Notes, Department of Mathematics and Statistics, University of Calgary, Alberta, Canada.
24. Johan Wallén., December 2003: On the differential and linear properties of addition. Research Report A84, Laboratory for Theoretical Computer Science, Helsinki University of Technology, Espoo, Finland.
25. Bernard Sklar, 2001: Digital Communications: Fundamentals and Applications, Second Edition, Prentice Hall, University of California, Los Angeles, USA.