Journal of Information Technology & Software Engineering ISSN: 2165-7866

Information Technology & Software Engineering

OPEN ACCESS Freely available online

Short Communication

Extended SREXPES8–2 Network Using Symmetrically Interchangeable XOR Operations

Gulomjon Tuychiyev[1], **Abdumannon Jumakulov**[2*]

[1]*Department of Physical and Mathematical Sciences, National University of Uzbekistan, Tashkent, Uzbekistan;* [2]*Department of Physical and Mathematical Sciences, Kokand University, Kokand, Uzbekistan*

ABSTRACT

The article presents a network of SREXPES8–2 with two round functions, which uses a single algorithm for encryption and decryption of sequential blocks of parts. Cryptography, or cryptology (from Antiquated Greek: κρυπτός, romanized: kryptós "covered up, secret"; and γράφειν graphein "to compose" or λογία-logia, "study", respectively), is the training and investigation of strategies for secure correspondence within the sight of ill-disposed behavior. All the more by and large, cryptography is tied in with developing and examining conventions that keep outsiders or the general population from perusing private messages. Present day cryptography exists at the convergence of the disciplines of math, software engineering, data security, electrical designing, advanced signal handling, physical science and others. Center ideas connected with data security (information classification, information trustworthiness, validation, and non-disavowal) are additionally fundamental to cryptography. Commonsense uses of cryptography incorporate electronic business, chip based installment cards, computerized monetary standards, PC passwords, and military correspondences. Cryptography preceding the advanced age was really inseparable from encryption, changing over decipherable data (plaintext) to muddled garbage text (ciphertext), which must be perused by turning around the interaction (decoding). The shipper of a scrambled (coded) message shares the unscrambling (unraveling) strategy just with planned beneficiaries to block access from enemies. The cryptography writing frequently utilizes the names "Alice" (or "A") for the source, "Sway" (or "B") for the planned beneficiary, and "Eve" (or "E") for the listening in adversary. Since the advancement of rotor figure machines in The Second Great War and the approach of PCs in The Second Great War, cryptography techniques have become progressively complicated and their applications more shifted.

Keywords: Feystel network; Lai-Massey scheme; Encryption; Decryption; Round keys; Round functions

INTRODUCTION

The article presents a network of SREXPES8-2 with two round functions, which uses a single algorithm for encryption and decryption of sequential blocks of parts. Cryptography, or cryptology (from Antiquated Greek: Κρυπτός, romanized: Kryptós "covered up, secret"; and γράφειν graphein, "to compose", or-λογία-logia, "study", respectively), is the training and investigation of strategies for secure correspondence within the sight of ill-disposed behavior. All the more by and large, cryptography is tied in with developing and examining conventions that keep outsiders or the General population from perusing private messages. Present day cryptography exists at the convergence of the disciplines of math, software engineering, data security, electrical designing, advanced signal handling, physical science, and others. Center ideas connected with data security (information classification, information trustworthiness, validation, and non-disavowal) are additionally fundamental to cryptography. Commonsense uses of cryptography incorporate electronic business, chip-based installment cards, computerized monetary standards, PC passwords, and military correspondences.

DESCRIPTION

Cryptography preceding the advanced age was really inseparable from encryption, changing over decipherable data (plaintext) to muddled garbage text (ciphertext), which must be perused by turning around the interaction (decoding). The shipper of a scrambled (coded) message shares the unscrambling (unraveling) strategy just with planned beneficiaries to block access from enemies. The cryptography writing frequently utilizes the names "Alice" (or "A") for the source, "Sway" (or "B") for the planned beneficiary, and "Eve" (or "E") for the listening in adversary [6]. Since the advancement of rotor figure machines in the second great war and the approach of PCs in the second great war, cryptography techniques have become progressively complicated and their applications more shifted.

The PES block encryption algorithm was developed in 1990 and is based on the Lay-Messi scheme. In 1991, the authors

Correspondence to: Abdumannon Jumakulov, Department of Physical and Mathematical Sciences, Kokand University, Kokand, Uzbekistan, Tel: 998972108120; E-mail: jumakulov19862106@gmail.com

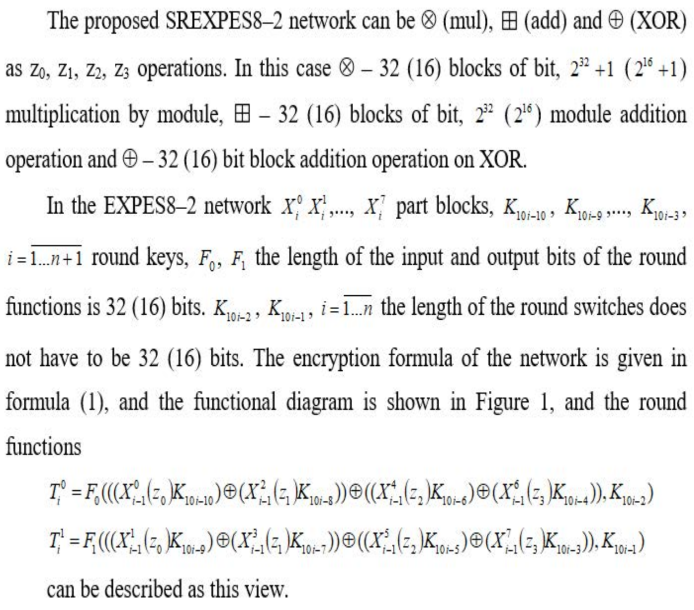
Received: 19-Sep-2022, Manuscript No. JITSE-22-19258; **Editor assigned:** 10-Sep-2022, PreQC No. JITSE-22-19258 (PQ); **Reviewed:** 23-Oct-2022, QC No. JITSE-22-19258; **Revised:** 10-May-2023, Manuscript No. JITSE-22-19258 (R); **Published:**17-May-2023, DOI: 10.35248/2165-7866.23.13.332

Citation: Tuychiyev G, Jumakulov A. Extended srexpes8-2 Network Using Symmetrically Interchangeable XOR Operations. J Inform Tech Softw Eng. 13:332.

Copyright: © 2023 Jumakulov A, et al. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution and reproduction in any medium, provided the original author and source are credited.

redesigned this block encryption algorithm and named it IDEA [1,2]. In these block encryption algorithms, round keys are multiplied by the module on the part blocks $2^{16}+1$, added by the module 2^{16} and in the MA reflection, the module 2^{16}, XOR add operations are used that is the number of operations is limited. However, a single algorithm is used for encryption and decryption. The IDEA NXT block encryption algorithm is based on the extended lay-Messi scheme developed by P. Junod, et al. Later, the IDEA NXT algorithm came to be known as FOX [3].

Currently, block encryption algorithms using a single algorithm for encryption and decryption are widely used. Examples of such block encryption algorithms are block encryption algorithms based on the Feystel network. In the Feystel network, the substitution actions are reflected in the round function, and the round functions do not depend on the network structure. It is also possible to take one sided, that is non-reverse, functions as round functions. Even with the structure of the PES block encryption algorithm and the extended Lay-Messi scheme, the creation of a network using a single algorithm for encryption and decryption using a round function instead of the MA reflection in the algorithm is a topical issue. Based on the above, in this paper, the structure of the PES block encryption algorithm and the extended Lay-Messi scheme, the eight-part block, extended by XOR using the XOR operation, consists of two round functions, the block length is 32 bits, the block length is 256 bits, the block length is 128 bits. The SREXPES8-2 (successfully replaced extended by operation XOR PES) network in the form of a series of algebraic operations (z_0, z_0, z_1, z_1, z_2, z_2, z_3, z_3) in which the block blocks are used to create block encryption algorithms with bits (Figure 1) [4-6].



The proposed SREXPES8–2 network can be $\otimes$ (mul), $\boxplus$ (add) and $\oplus$ (XOR) as z_0, z_1, z_2, z_3 operations. In this case $\otimes$ – 32 (16) blocks of bit, $2^{32}+1$ $(2^{16}+1)$ multiplication by module, $\boxplus$ – 32 (16) blocks of bit, 2^{32} (2^{16}) module addition operation and $\oplus$ – 32 (16) bit block addition operation on XOR.

In the EXPES8–2 network $X_i^0\ X_i^1,\dots,\ X_i^7$ part blocks, K_{10i-10}, $K_{10i-9},\dots,\ K_{10i-3}$, $i=\overline{1\dots n+1}$ round keys, F_0, F_1 the length of the input and output bits of the round functions is 32 (16) bits. K_{10i-2}, K_{10i-1}, $i=\overline{1\dots n}$ the length of the round switches does not have to be 32 (16) bits. The encryption formula of the network is given in formula (1), and the functional diagram is shown in Figure 1, and the round functions

$$T_i^0=F_0(((X_{i-1}^0(z_0)K_{10i-10})\oplus(X_{i-1}^2(z_1)K_{10i-8}))\oplus((X_{i-1}^4(z_2)K_{10i-6})\oplus(X_{i-1}^6(z_3)K_{10i-4})),K_{10i-2})$$

$$T_i^1=F_1(((X_{i-1}^1(z_0)K_{10i-9})\oplus(X_{i-1}^3(z_1)K_{10i-7}))\oplus((X_{i-1}^5(z_2)K_{10i-5})\oplus(X_{i-1}^7(z_3)K_{10i-3})),K_{10i-1})$$

can be described as this view.

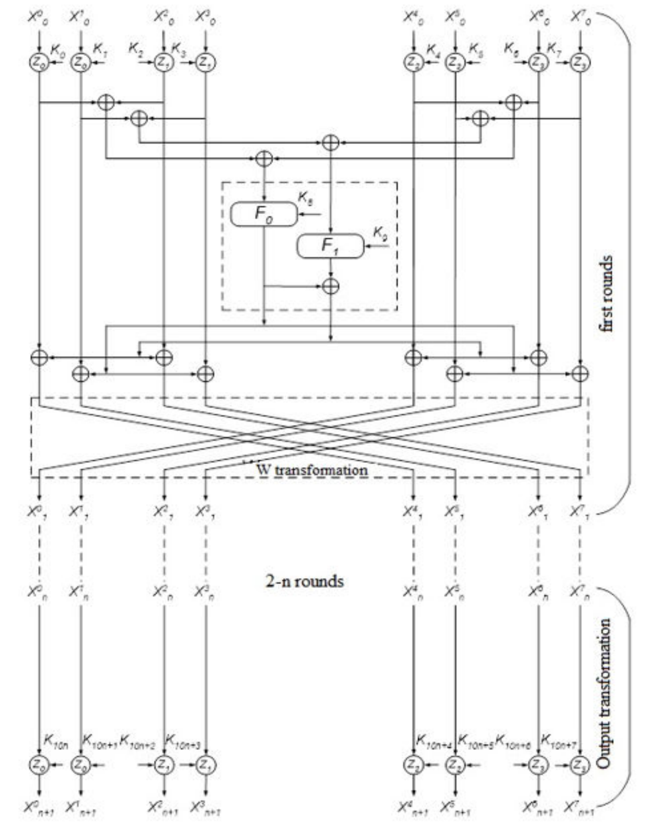
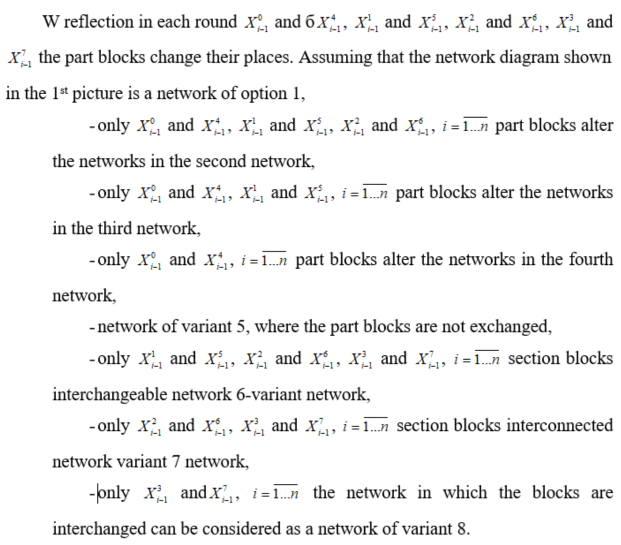


Figure 1: Functional scheme of SREXPES8-2 network.



W reflection in each round X_{i-1}^0 and бX_{i-1}^4, X_{i-1}^1 and X_{i-1}^5, X_{i-1}^2 and X_{i-1}^6, X_{i-1}^3 and X_{i-1}^7 the part blocks change their places. Assuming that the network diagram shown in the 1st picture is a network of option 1,

- only X_{i-1}^0 and X_{i-1}^4, X_{i-1}^1 and X_{i-1}^5, X_{i-1}^2 and X_{i-1}^6, $i=\overline{1\dots n}$ part blocks alter the networks in the second network,
- only X_{i-1}^0 and X_{i-1}^4, X_{i-1}^1 and X_{i-1}^5, $i=\overline{1\dots n}$ part blocks alter the networks in the third network,
- only X_{i-1}^0 and X_{i-1}^4, $i=\overline{1\dots n}$ part blocks alter the networks in the fourth network,
- network of variant 5, where the part blocks are not exchanged,
- only X_{i-1}^1 and X_{i-1}^5, X_{i-1}^2 and X_{i-1}^6, X_{i-1}^3 and X_{i-1}^7, $i=\overline{1\dots n}$ section blocks interchangeable network 6-variant network,
- only X_{i-1}^2 and X_{i-1}^6, X_{i-1}^3 and X_{i-1}^7, $i=\overline{1\dots n}$ section blocks interconnected network variant 7 network,
- only X_{i-1}^3 andX_{i-1}^7, $i=\overline{1\dots n}$ the network in which the blocks are interchanged can be considered as a network of variant 8.

$$\begin{cases} X_i^0 = (X_{i-1}^4(z_2)K_{10i-6}) \oplus T_i^0 \oplus T_i^1 \\ X_i^1 = (X_{i-1}^5(z_2)K_{10i-5}) \oplus T_i^0 \\ X_i^2 = (X_{i-1}^6(z_3)K_{10i-4}) \oplus T_i^0 \oplus T_i^1 \\ X_i^3 = (X_{i-1}^7(z_3)K_{10i-3}) \oplus T_i^0 \\ X_i^4 = (X_{i-1}^0(z_0)K_{10i-10}) \oplus T_i^0 \oplus T_i^1 \\ X_i^5 = (X_{i-1}^1(z_0)K_{10i-9}) \oplus T_i^0 \\ X_i^6 = (X_{i-1}^2(z_1)K_{10i-8}) \oplus T_i^0 \oplus T_i^1 \\ X_i^7 = (X_{i-1}^3(z_1)K_{10i-7}) \oplus T_i^0 \end{cases}, \; i = \overline{1...n} \qquad (1)$$

$$\begin{cases} X_{n+1}^0 = (X_n^0(z_0)K_{10n}) \\ X_{n+1}^1 = (X_n^1(z_0)K_{10n+1}) \\ X_{n+1}^2 = (X_n^2(z_1)K_{10n+2}) \\ X_{n+1}^3 = (X_n^3(z_1)K_{10n+3}) \\ X_{n+1}^4 = (X_n^4(z_2)K_{10n+4}) \\ X_{n+1}^5 = (X_n^5(z_2)K_{10n+5}) \\ X_{n+1}^6 = (X_n^6(z_3)K_{10n+6}) \\ X_{n+1}^7 = (X_n^7(z_3)K_{10n+7}) \end{cases}, \text{ the last contradiction}$$

The networks in options 2 to 8 are similar to the encryption formulas (1), only

- in the 2nd network option, X_i^3 and X_i^7 calculations,
- in the 3rd network option, X_i^2 and X_i^6, X_i^3 and X_i^7 calculations,
- in the 4th network option, X_i^1 and X_i^5, X_i^2 and X_i^6, X_i^3 and X_i^7 calculations,
- in the 5th network option, X_i^0 and X_i^4, X_i^1 and X_i^5, X_i^2 and X_i^6, X_i^3 and X_i^7 calculations,
- in the 6th network option, X_i^0 and X_i^4 calculations
- in the 7th network option, X_i^0 and X_i^4, X_i^1 and X_i^5 calculations,
- in the 8th network option, X_i^0 and X_i^4, X_i^1 and X_i^5, X_i^2 and X_i^6

Calculations exchange their places:

In the round n´, SREXPES8-2 network, there are 10 round switches in each round and 8 round switches in the final reflection that is the total number of round switches 10n+8. In encryption, the encryption round keys are generated from the algorithm key K_i^c according to one rule 10^n+8.

10n+8 times decryption round keys are created based on encryption round keys. Encryption uses the encryption round key instead of 1st figure and formulas K_i and the decryption round key K_i^c is used in encryption, that is one network is used for encryption and decryption K_i^d, only the order of the keys changes. The n⁻round SREXPES8-2 network connects the first, second, and n-round decryption keys to the encryption round keys as follows:

$$(K_{10(i-1)}^d, K_{10(i-1)+1}^d, K_{10(i-1)+2}^d, K_{10(i-1)+3}^d, K_{10(i-1)+4}^d, K_{10(i-1)+5}^d, K_{10(i-1)+6}^d, K_{10(i-1)+7}^d, K_{10(i-1)+8}^d, K_{10(i-1)+9}^d) =$$
$$((K_{10(n-i+1)}^c)^{z_0}, (K_{10(n-i+1)+1}^c)^{z_0}, (K_{10(n-i+1)+2}^c)^{z_1}, (K_{10(n-i+1)+3}^c)^{z_1}, (K_{10(n-i+1)+4}^c)^{z_2}, (K_{10(n-i+1)+5}^c)^{z_2},$$
$$(K_{10(n-i+1)+6}^c)^{z_3}, (K_{10(n-i+1)+7}^c)^{z_3}, K_{10(n-i)+8}^c, K_{10(n-i)+9}^c), i = \overline{1...n}.$$

If as calculations z_0, z_1, z_2, z_3 are used $\otimes$ $K = K^{-1}$, $\boxplus$ is used, $K = -K$ and $\oplus$ is used, $K = K$ here K^{-1} in the number K^{-1}, $2^{32}+1$ ($2^{16}+1$) modulus inverse value, – K – K to the number 2^{32} (2^{16}) opposite value per module. For 32-bit numbers, for 16-bit numbers $K \otimes K^{-1} = 1 \bmod (2^{16}+1)$ and $-K \boxplus K = 0$.

The final reflection round keys are linked to the encryption round keys as follows:

$$(K_{10n}^d, K_{10n+1}^d, K_{10n+2}^d, K_{10n+3}^d, K_{10n+4}^d, K_{10n+5}^d, K_{10n+6}^d, K_{10n+7}^d) = ((K_0^c)^{z_0}, (K_1^c)^{z_0}, (K_2^c)^{z_1}, (K_3^c)^{z_1}, (K_4^c)^{z_2},$$
$$(K_5^c)^{z_2}, (K_6^c)^{z_3}, (K_7^c)^{z_3}). \qquad (3)$$

CONCLUSION

The main advantage of the proposed SREXPES8-2 network is that it involves a round function, uses a single algorithm for encryption and decryption, and algebraic operations are variable. As a network round function, it is possible to obtain reflections that are widely used in block encryption algorithms, as well as one-way, that is, non-existent reflections. As actions z_0, z_1, z_2, z_3 add, mul, chorus actions, in the vision of (z_0, z_0, z_1, z_1, z_2, z_2, z_3, z_3) in the way of 3^4=81 can be choosen that is, all possible options are equal to 81, and the network has four options.

By selecting operations F_0, F_1 in 81 ways and options in eight ways, it is possible to build 648 block encryption algorithms based on the SREXPES8-2 network, whose round functions do not change. Block encryption algorithms based on the SREXPES8-2 network facilitate the development of hardware and software by using a single algorithm for encryption and decryption in the network.

REFERENCES

1. Lai X, Massey JL. A proposal for a new block encryption standard. In workshop on the theory and application of cryptographic techniques. Springer. 1991;389-404.
2. Lai X, Massey JL. On the design and security of block cipher. ETH series in information processing, v.1, Konstanz: Hartung Gorre Verlag. 1992.
3. Junod P, Vaudenay S. FOX: A new family of block ciphers. In International Workshop on Selected Areas in Cryptography. 2004;114-129.
4. Li C, Liu Y, Zhang LY, Chen MZ. Breaking a chaotic image encryption algorithm based on modulo addition and XOR operation. Int J Bifurcat Chaos. 2013;23(04):1350075.
5. Davis R. The data encryption standard in perspective. IEEE Communications Society Magazine. 1978;16(6):5-9.
6. Han J, Park CS, Ryu DH, Kim ES. Optical image encryption based on XOR operations. Opt Eng. 1999;38(1):47-54.