ISSN 2278-3091

Volume 9, No.5, September - October 2020

International Journal of Advanced Trends in Computer Science and Engineering

Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse261952020.pdf

https://doi.org/10.30534/ijatcse/2020/261952020

Modification of the algorithm (OFM) S-box, which provides increasing crypto resistance in the post-quantum period

Serhii Yevseiev [1], Roman Korolyov [2], Andrii Tkachov [3],
Oleksandr Laptiev[4],IvanOpirskyy[5],Olha Soloviova[6]

[1]Doctor of Technical Sciences, Professor, Head of the Department of Cybersecurity and Information Technology, Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine, serhii.yevseiev@hneul.net

[2]Candidateof Technical Sciences,Associate Professorof the Department of Cybersecurity and Information Technology, Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine, korolevrv01@ukr.net

[3]Candidateof Technical Sciences,Senior Researcher, Associate Professorof the Department of Cybersecurity and Information Technology, Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine,snsncps@gmail.com

[4]Doctor of Technical Sciences, Senior Researcher, Head of the Department of Information and Cybersecurity Systems, State University of Telecommunications, Kyiv, Ukraine, alaptev64@ukr.net

[5]Doctor of Technical Sciences,ProfessorDepartment of Information Security, Lviv Polytechnic National University, Lviv, Ukraine,iopirsky@gmail.com

[6]Candidateof Technical Sciences,Head of theDepartment of Information Technology Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine, olga01@ukr.net

ABSTRACT

The entry of mankind into the era of high technology, the rapid growth of computing technology contributes to the expansion of the range of electronic services. To ensure the security of sensitive information, personal data is used cryptographic systems of traditional cryptography (symmetrical cryptosystems) and cryptography with open keys (asymmetric cryptosystems). As a rule, the first provide security services, the second - the distribution of keys. However, in the conditions of totalitarian surveillance in society by the special services of developed countries in cryptographic algorithms "embedded" cryptographic bookmarks, which on the one hand provide "fast" access of special services to confidential information, on the other hand, allow attackers to hack into the cryptosystem and get user data. The article proposes a modification of the well-known algorithm (OFM) S-box, which provides "elimination" of possible cryptographic bookmarks and increasing crypto resistance in the post-quantum period (the appearance of a full-scale quantum computer, that allows you to hack on the basis of The Grover and Shore algorithms modern symmetrical and asymmetrical cryptosystems). In addition, commercial implementation will ensure the "opposition" of possible crypto-deposits by the special services, that will reduce the risk of hacking by identifying "weak" (vulnerable) places based on cryptographic bookmarks.

Key words: Symmetrical crypto-algorithm, cryptographic bookmarks, post quantum period, a quantum computer

1. INTRODUCTION

The computing capabilities of the global community until 2024 are growing under Moore's Law, which allowed in 2015 to develop and implement 1 billion Internet things that have replenished cyberspace. The growth of computing resources has allowed to expand the range of services in almost all areas of life. However, all this contributes to the increase, and sometimes the primacy of cyber attacks on the means to counter them. Attackers are increasingly complexing threats and methods of social engineering, allowing them to obtain synergies and hack into corporate and automated critical object systems, primarily for the banking sector, energy infrastructure systems, telecommunications systems, transport systems, which can lead not only to the hacking of the system as a whole, but also to the blackout and energy collapse of the world

1.1 Literature analysis and problem statement

Recently, in a number of leading countries, public authorities have been trying to weaken encryption algorithms and security standards to facilitate the work of intelligence and law enforcement agencies as part of the measures taken by the state in response to the growing terrorist threat. Among other things, there is a statement about the mandatory introduction of a loophole in the crypto-algorithm, which are state standards. Users often get only the illusion of protection. Using an algorithm, all the details of which are known only to its developer, the user has a single guarantee of durability - a statement of the developer on the reliability of the algorithm.

Thus, almost all developers of cryptographic information security "leave" bookmarks (hatches / loopholes) at the request of intelligence services and / or the state government to provide quick access to confidential information, both for users and for the media. IT giants.

To date, there is no generally accepted terminology for cryptographic bookmarks. However, most English-speaking authors suggest that the term "Backdoors" be fixed by cryptographic loopholes, leaving the term "trapdoors" to refer to information that facilitates the inverse one-way function. In the Russian-language literature to denote [1-5] these concepts use "bookmarks", "loopholes" and "back door" and even "secret passages".

Methods of embedding bookmarks in cryptographic algorithms can be divided into three main groups: weak bookmarks, transmission of information through hidden channels, the SETUP mechanism [6-7].

Weak bookmarks are a deliberate weakening of the algorithm, which allows you to know the secret information of the user based on open information [8-9].

Weak bookmarks are always detected by reverse engineering. In some cases, weak bookmarks can be detected only on the basis of the original (open) data of the algorithm, using simple algebraic checks or statistical analysis.

According to the definition [10], a hidden channel is an unspoken information technology and an automated communication channel that can be used to violate security policies.

Thus, a channel is called hidden if it was not specifically designed and was not originally designed to transmit information in an electronic data processing system, such channels include digital steganography algorithms in spatial and frequency domains based on the impossibility ("weakness" of perception of information as visual system and the human auditory system). Such a container can be images (images, videos), audio and text files[11-14]..

Crypto-infrastructure with a loophole (Backdoor, Trapdoor) is an algorithm that contains some hidden structure (loophole) that ensures the existence of a hidden channel of information transmission; knowledge of this structure allows you to get secret information (for example, about the secret key). Without knowledge of the loophole, the algorithm seems reliable. Thus, SETUP mechanisms can be symmetrical and asymmetrical. Like symmetric encryption in symmetric loopholes, the key embedded in the implementation matches the author's key of the loophole required to access the hidden channel (or these keys are easily computed from each other). For example, with reverse engineering, both users and attackers (all but the asymmetric loophole key holder) cannot determine how user secret keys and future secret keys are already being used[15-17].

We use encryption algorithms to view cryptographic bookmarks. This algorithm is an exact copy of the block encryption algorithm, with one exception. The new one defines and establishes a permutation table for nonlinear transformation, which is absent in the old algorithm, and the task of its elements was entirely in the hands of the people implementing the algorithm[18-21]. Theoretically, if you self-identify the elements of the permutation table and keep the table secret, it will increase the longevity of the encryption algorithm (this actually increases the length of the key)

1.2 Aim of the article

The aim of the study is to develop a flowing encryption algorithm based on the blockchain algorithm through the use of dynamically changing nonlinear bijective conversion (S blocks).

To achieve the goal, the following objectives were set:

- to analyze the block encryption algorithm;
- to develop a method of forming a pseudo-key sequence based on new encryption.

2. THE MAIN SECTION

In the algorithm, the block to be encrypted (length of 64 bits) is divided into two equal parts (32 bits) - right and left. Next, thirty-two iterations are performed using iterative keys derived from the original 256-bit encryption key. During each iteration, one conversion based on the Feistel network is made with the right and left half of the encrypted block. First, the right part is folded into module 2^{32} with the current iterative key, then the resulting 32-bit number is divided into eight 4-bits and each of them, using the rearrangement table, is converted into another 4-bit number. After this conversion, the resulting number cycles to the left by eleven discharges. Next, XOR is transformed with the left half of the block. The resulting 32-bit number is recorded in the right half of the block, and the old contents of the right half are transferred to the left half of the block. The diagram of the main step of the algorithm's crypto-transformation is shown in Figure 1.

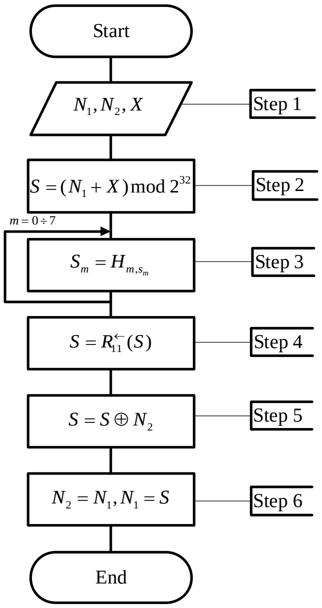

Figure 1: The scheme of the main step of crypto-transformation of the old algorithm

The main step of the algorithm's crypto-transformation consists of the following steps:

Step 1. Entering the original data for the main step of crypto-transformation N - 64-bit block of input is converted into two 32-bit whole numbers (the younger(N_1) and the eldest (N_2) parts);

Step 2. Adding to the key. The younger part of the converted block is folded into a module with the key element used on the step.

Step 3. A block replace. The 32-bit value obtained in the previous step is interpreted as an array of four 4-bit blocks of code: $S_m =(S_0,S_1,S_2,...S_{15})$.

Step 4. A cyclical shift of 11 bits to the left.

Step 5. Beaten addition: the value received on step 3 is broken by module 2 with the older half of the converted block.

Step 6. Shift along the chain: The younger part of the converted block shifts to the place of the senior, and on the its place is placed the result of the previous step.

Then the structure of the algorithm can describe the multi-round diagram, represented in Figure 2.

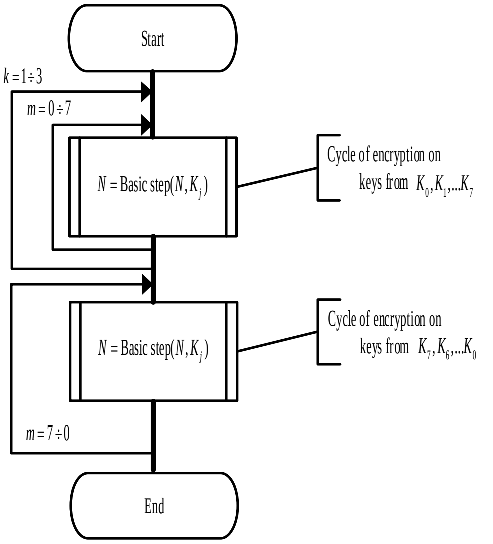
Start
$k=1\div3$
$m=0\div7$
$N=\text{Basic step}(N,K_j)$
Cycle of encryption on keys from $K_0,K_1,...K_7$
$N=\text{Basic step}(N,K_j)$
Cycle of encryption on keys from $K_7,K_6,...K_0$
$m=7\div0$
End

Figure 2: Tncryption cycle

To create an improvement algorithm, we will change the main step of the algorithm's crypto-transformation (Figure 3) in OFM mode

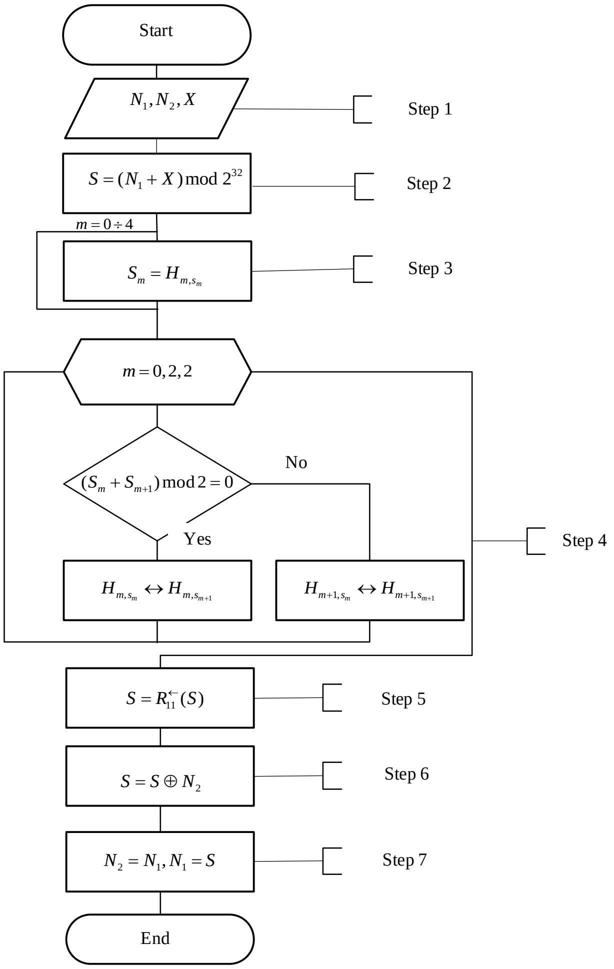

Figure 3: The scheme of improving the main step of crypto-transformation

Take the basis of the order of changes in values in the S block of the RC 4 streaming encryption algorithm. RC4, a streaming encryption algorithm, was proposed in 1987 by Ronald Lynn Rivest, a well-known American cryptography specialist. Since 1994, it has been widely used in a number of cryptographic applications, including known-known ones such as SSL and TLS, to encrypt data transmitted through data networks that do not provide user data protection, WPA, and WEP to protect wireless connections. In the streaming encryption algorithm, two S-block meanings change places when a pseudo-key sequence is formed.

The main step of the algorithm's crypto-transformation consists of the following steps:

Step 1. Entering the original data for the main step of crypto-transformation N - 64-bit block of input is converted into two 32-bit whole numbers (the younger(N_1) and the eldest (N_2) parts);

Step 2. Adding to the key. The younger part of the converted block is folded into a module with the key element used on the step.

Step 3. A block replace. The 32-bit value obtained in the previous step is interpreted as an array of four 8-bit blocks of code: $S_m =(S_0,S_1,S_2,...S_{255})$.

Then the value of each of the four blocks is replaced by a new one, which is selected by the replacement table as follows: the value of the block S_i changes to S_i order element (numbering from zero) i node of substitutions (i.e. i line of the replacement table, numbering also from zero). In other words, as a replacement for the block value, an item is selected from a replacement table with a number equal to the number of the block being replaced, and a column number equal to the 8-bit value of a whole non-negative number.

Step 4. Dynamic change in the replacement table is as follows: if the amount S_0 +S_1even number, then change places of value $S_0 \leftrightarrow S_1$of the tables H_0, otherwise $S_0 \leftrightarrow S_1$of the tables H_1. If the amount S_2 +S_3even number, then change places of value $S_2 \leftrightarrow S_3$of the tables H_2, otherwise $S_0 \leftrightarrow S_1$of the tables H_3.

Step 5. A cyclical shift of 11 bits to the left.

Step 6. Beaten addition: the value received on step 3 is broken by module 2 with the older half of the converted block.

Step 7. Shift along the chain: The younger part of the converted block shifts to the place of the senior, and on the its place is placed the result of the previous step.

Step 6. The resulting value of the converted block is returned as a result of execution the algorithm of the main step of crypto-transformation.

Using this transformation allows dynamically (based on a simple pseudo-key sequence generator) to form of OFM mode and provide the required level of crypto resistance.

3. CONCLUSIONS

Analysis of cryptographic tools for basic security services has shown that symmetrical and asymmetrical cryptosystems and specialized hash functions are used to ensure confidentiality (security during transmission), integrity (security in storage and modification only to authorized users), and authenticity (authenticity of the source of the message). And humanity "blindly believes" the resilience of the algorithms provided. However, to ensure the "solution of issues" control of the individual, and total surveillance of society as a whole by the intelligence services and/or the state/community of states used various cryptographic bookmarks, allowing "quickly" to find key data, and to gain access to personal/confidential user data.

Analysis of the capabilities of cyber criminals demonstrates virtually unlimited computational capabilities in the emergence of a full-scale quantum computer and the entry of mankind into the era of post-quantum cryptography, which practically calls into question the possibilities of ensuring durability as symmetrical. as well as asymmetric cryptosystems (and based on elliptical curves). This is evidenced by the research of the scientific community, as well as specialists of the NIST USA. In February 2019, the U.S. National Institute of Standards and Technology continued to select candidates for post-quantum cryptography algorithms. In the post-quota period, the use of cryptographic bookmarks in order to "strengthen" the durability of algorithms of symmetrical and asymmetrical cryptography, almost "any" interference in the algorithm in its practical implementation can lead to the "destruction" of its integrity of the structure and reduce its durability.

Developed encryption algorithm on the base a flowing encryption algorithm based on the blockchain algorithm through the use of dynamically changing nonlinear bijective conversion (S blocks) avoids significant information security issues.

REFERENCES

1. Maslov A.A., Sotnikova M.V. **Determination of radiotechnical parameters of phasomanipulated signals**.*Journal of Modern Information Technologies and IT Education.* 2019.Vol.15, No. 1. pp.107-114
2. Gromov D. V., Suyakov S. A., **Methods for measuring and converting time-frequency parameters of signals**, *“Journal“ Informatization and Control Systems in Industry* ” 2013.No. 3 (45).
3. Grigoryan D.S. **Cogerent data processing in tasks of spectral analysis of super resolution radar signals**. *Journal of Radio Electronics" Electronic Journal.* 2012. № 3 http://jre.cplire.ru/jre/mar12/1/text.html.
4. Ara Jullion A. Abello, Gabriele Francesca Y., Domingo, Maria Jamelina T. Joven, Samanta Alexis S. Malubay. **Power Measurement Model Optimizationusing using MATLAB.***International Journal of Advanced Trends in Computer Science and Engineering. (IJATCSE).* 2019. Vol. 8, № 3, May – June. pp. 538 – 542.
5. Bakiko V.M., Popovich P.V.,. Shvaichenko V.B. **Determination of noise immunity of a communication channel in case of accidental interference**. *Bulletin of the National tech. University "KhPI"*: Coll. Science. Kharkiv: NTU "KhPI", 2018. № 14 (1290). P. 7 - 10.
6. Milov O., Yevseiev S. Milevskyi S. Ivanchenko Y., Nesterov O., Puchkov O., Yarovyi A., Salii A., , Tiurin V., Timochko O.**Development the model of the antagonistic agent’s behavior under a cyber-conflict.***Eastern European Journal of Advanced Technologies*. Kharkiv.2019. 4/9 (100). pp. 6–19.
7. Lubov Berkman, Oleg Barabash, Olga Tkachenko , Andri Musienko, Oleksand Laptiev, Ivanna Salanda.**The Intelligent Control System for infocommunication networks.***International Journal of Emerging Trends in Engineering Research (IJETER)* Volume 8. No. 5, May 2020. pp.1920 – 1925.

8. Olexandr Laptiev, German Shuklin, Spartak Hohonianc, Amina Zidan, Ivanna Salanda.**Dynamic model of Ceber Defence Diagnostics of information Systems with the Use of Fozzy Technologies***IEEE ATIT 2019 Conference Proceedings Kyiv, Ukraine, December 18-20*, pp.116-120.
9. Sweta Srivastav, Sangeeta Gupta.**Results with Matlab coding of Middle Graph of Cycle and its relatedgraphs in context of Sum Divisor Cordial***International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, Volume-8 Issue-2, February 2020. pp.398-401.
10. Mashkov O.A., Sobchuk V.V., Barabash O.V., Dakhno N.B., Shevchenko H.V., Maisak T.V. **Improvement of variational-gradient method in dynamical systems of automated control for integro-differential models**. *Mathematical Modeling and Computing*, 2019, Vol. 6, No. 2, pp. 344 – 357.
11. Barabash O., Dakhno N., Shevchenko H., Sobchuk V. **Integro-Differential Models of Decision Support Systems for Controlling Unmanned Aerial Vehicles on the Basis of Modified Gradient Method.***IEEE 5th International Conference on Methods and Systems of Navigation and Motion Control (MSNMC)*. 16-18 October, National Aviation University, 2018. Kyiv, Ukraine. pp. 94 – 97.
12. Ihor Ruban, Nataliia Bolohova, Vitalii Martovytskyi, Nataliia Lukova-Chuiko , Valentyn Lebediev. **Method of sustainable detection of augmented reality markers by changing deconvolution.***International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE).*Volume 9, No.2, March-April 2020,pp.1113-1120.
13. Barabash O., Kopiika O., Zamrii I., Sobchuk V., Musienko A. **Fraktal and Differential Properties of the Inversor of Digits of Qs-Representation of Real Number**. *Modern Mathematics and Mechanics. Fundamentals, Problems and Challenges* (ISSN 1860-0832). Springer International Publishing AG, 2019. pp. 79 – 95.
14. Barabash O., Sobchuk V., Lukova-Chuiko N. and Musienko A. **Application of Petri Networks for Support of Functional Stability of Information Systems.***2018 IEEE First International Conference on System Analysis & Intelligent Computing (SAIC). 08-12 October*, *Igor Sikorsky Kyiv Polytechnic Institute*, 2018. Kyiv, Ukraine. pp. 36 – 39.
15. Oleg Barabash, OleksandrLaptiev, Oksana Kovtun, Olga Leshchenko, Kseniia Dukhnovska, Anatoliy Biehun. **The Method dynavic TF-IDF**. *International Journal of Emerging Trends in Engineering Research (IJETER)*, Volume 8. No. 9, September 2020.pp 5713-5718
16. Barabash Oleg, Laptiev Oleksand, Tkachev Volodymyr, Maystrov Oleksii, Krasikov Oleksandr, Polovinkin Igor. **The Indirect method of obtaining Estimates of the Parameters of Radio Signals of covert means of obtaining Information.** *International Journal of Emerging Trends in Engineering Research (IJETER)*, Volume 8. No. 8, August 2020. Indexed- ISSN: 2278 – 3075. pp4133 – 4139
17. Vitalii Savchenko, Oleh Ilin, Nikolay Hnidenko, Olga Tkachenko, Oleksander Laptiev, Svitlana Lehominova.**Detection of Slow DDoS Attacks based on User's Behavior Forecasting**. *International Journal of Emerging Trends in Engineering Research (IJETER)* Volume 8. No. 5, May 2020. Scopus Indexed - ISSN 2347 – 3983. pp.2019 – 2025.
18. Laptiev Oleksandr, Shuklin German, Savchenko Vitalii, Barabash Oleg, Musienko Andrii and Haidur Halyna. **The Method of Hidden Transmitters Detection based on the Differential Transformation Model**. *International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE).* Vol. 8, No 6, November – December 2019, pp. 2840 – 2846.
19. Monica Thomas , Dr. Varghese S Chooralil.**Security and Privacy via Optimised Blockchain.** *International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE).* Vol. 8, No 3, May – June 2019, pp. 415 – 418.
20. Norliza Katuk.**The application of blockchain for halal product assurance: A systematic review of the current developments and future directions.***International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE).* Vol. 8, No 5, September – October 2019, pp. 1893 – 1902.