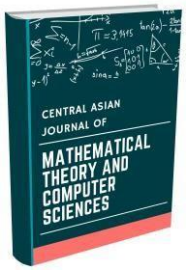


CENTRAL ASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES
https://cajmtcs.centralasianstudies.org/index.php/CAJMTCS
Volume: 05 Issue: 03 | July 2024 ISSN: 2660-5309

Article

Development of an Algorithm for Symmetrical Block Ciphering over the Feistel Network Based on Cryptocurrency Basic Table Transformations

D.E. Akbarov[1*], U.Y. Akbarov[2]

1. Physical and Mathematical Sciences, Professor, Kokand State Pedagogical Institute
2. Physical and Mathematical Sciences, Associate Professor, Kokand State Pedagogical Institute

* Correspondence: akbarov.ummatali1961@gmail.com

Abstract:. This article focuses on the development of a symmetric block encryption algorithm using the Feistel network, enhanced by cryptographically stable table-based transformations. The proposed algorithm integrates fundamental transformations of logical operation tables and bit union operations to ensure cryptographic security. It addresses the issue of improving cryptographic stability in block encryption by incorporating innovative table-based transformations, bit concatenation, and cyclic bit shifts. These advancements contribute to both the theoretical foundation and practical implementation of secure encryption algorithms, which can be applied effectively in information communication networks. The results highlight the feasibility and robustness of the algorithm, particularly in hardware and software encryption systems, ensuring efficient cryptographic security for various applications.

Keywords: encryption, cryptographic strength, Feistel networks, bits, concatenation, algorithm, mathematical model, discovery text, encrypted text.

Citation: Akbarov. Development of an Algorithm for Symmetrical Block Ciphering over the Feistel Network Based on Cryptocurrency Basic Table Transformations. Central Asian Journal of Mathematical Theory and Computer Sciences 2024, 5(3), 339-346

Received: 10th June 2024
Revised: 11th July 2024
Accepted: 24th July 2024
Published: 27th Sept 2024

1. Introduction

The proposed article examines the issues of research and creation of a symmetric block encryption algorithm based on the Feistel network with cryptographically stable table basic transformations. The list of sources devoted to the topic of the Feistel network, their cryptographic features, properties, developments with various new basic transformations, applications and other purposes in the information communication network is widely [1-9, et al.].

Relevance of the task. Hardware implementations of basic table transformation algorithms are convenient and rational, since they do not require calculations, they require only comparisons and transitions in mixing and distributing bits or combining them, while ensuring cryptographic stability of mappings (Rahman, 2024).

2. Materials and Methods

This work [10] is devoted to the study of the issues of cryptographic stability of tables of logical operations and other table transformations with bit unions. Necessary and sufficient conditions for the stability of table transformations are established (Wang, 2024).

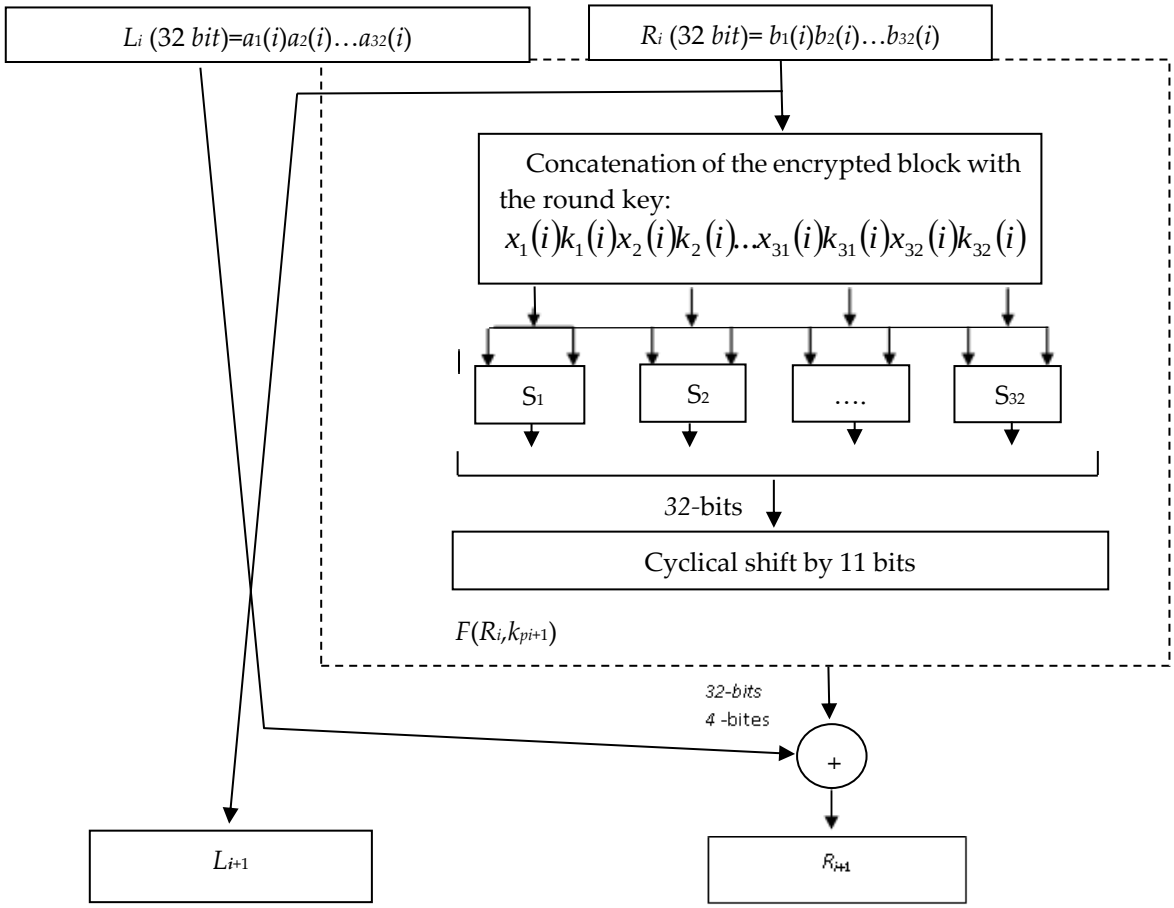
Statement of the problem. The proposed article examines the issues of a strong block encryption algorithm over a Feistel network with basic transformations of logical operation tables and bit union tables (Mogos, 2023).

3. Results

Solution of the problem. It is noted that Feistel networks encrypt data under blocks of bits of the encrypted text with round keys (Zhang, 2022). Round keys have 32 bits, they are formed from the original key, the length of which is not less than 256 bits. Before encrypting the plaintext, it is divided into blocks of 32 bits. In this case, if the length of the encrypted text is not a multiple of 32 bits, then it is added to the multiple with spaces (Dey, 2024). Below there is provided a block diagram of the *i*-round for the bit encryption algorithm, where the basic transformations are: *concatenation of the encrypted 32-bit block with the round key, 32-bit block, bitwise table substitution transformation with the truth table of logical operations, cyclic shift by 11 bits*.

1. The concatenation (connection) of the blocks of the corresponding encrypted part at the i-th round of the plaintext $x_1(i)x_2(i)..x_{31}(i)x_{32}(i)k_{32}(i)$ with the round key $k_1(i)k_2(i)...k_{31}(i)k_{32}(i)$ is carried out as follows: $x_1(i)k_1(i)x_2(i)k_2(i)..x_{31}(i)k_{31}(i)x_{32}(i)k_{32}(i)$
2. The bitwise table substitution of the cipher value of the encrypted open message is transformed into the cipher designation with a truth table of logical operations: at the intersection of column $x_j(i),\ j=1,2,...,32;$; and row $k_t(i),\ t=1,2,...,32.$; the cipher designation is found. That is, according to the inputs $x_j(i)k_t(i).$ and $k_t(i).$, specified in the algorithm of the S_λ λ =1,..,32; blocks, the designation code is determined.
3. A cyclic shift of 11 (or 7, 17, 19) bits is performed by connecting contacts in the following order: 12-bits with the first bit $a_1(i)$ of the left 32-bit block Li (32 bit)=a1(i)a2(i)…a32(i), 13-bits with $a_2(i)$ and so on, 32-bits with $a_{11}(i)$.

Block diagram of *i*-round for bit encryption algorithm



Here, he notes the following properties of Feistel's network.
The mathematical model of round encryption is expressed as follows:

$$\begin{cases} L_i = R_{i-1}, \\ R_i = L_{i-1} \oplus F(R_{i-1}, K_i). \end{cases}$$

From this, according to the nature of the operation ⊕, the mathematical model of *i*-round decoding is expressed as follows:

$$\begin{cases} R_{i-1} = L_i, \\ L_{i-1} = R_i \oplus F(L_i, K_i). \end{cases}$$

Further, we are going to discuss when encryption is performed with pairs of bits, the basic transformations of pairs of bits:
– concatenation (connection) of the encrypted 32-bit block with the round key, allocated to 16 pairs of bits of the form "00", "01", "10", "11";
– perform a transformation of 32-bit blocks allocated to 16 pairs of bits by table replacement with a given truth table of size 4×4;
– cyclical shift by 11.

1. Concatenation (connection) with pairs of bits of blocks of the corresponding encrypted part at the i-th round of plaintext $x_1(i)x_2(i)..x_{31}(i)x_{32}(i)k_{32}(i)$ with the key of round $k_1(i)k_2(i)...k_{31}(i)k_{32}(i)$ is carried out as follows: $x_1(i)k_1(i)x_2(i)k_2(i)..x_{31}(i)k_{31}(i)x_{32}(i)k_{32}(i)$.
2. The transformation is carried out with pairs of bits of the table replacement cipher value of the encrypted open message to the cipher designation with a truth table of size 4×4: at the intersection of column $x_j(i), x_{j+1}(i)$ $j = 1,2,...,31;$; and row $k_t(i)k_{t+1}(i)$, $t = 1,2,...,31.$; the cipher designation is found. That is, at the inputs $x_j(i)x_{j+1}(i).$ and $k_t(i)k_{t+1}(i).$, specified in the algorithm S_λ λ =1,..,16; blocks, the cipher designation is determined.
   Here, for example, is given one form of the truth table of size 4×4:

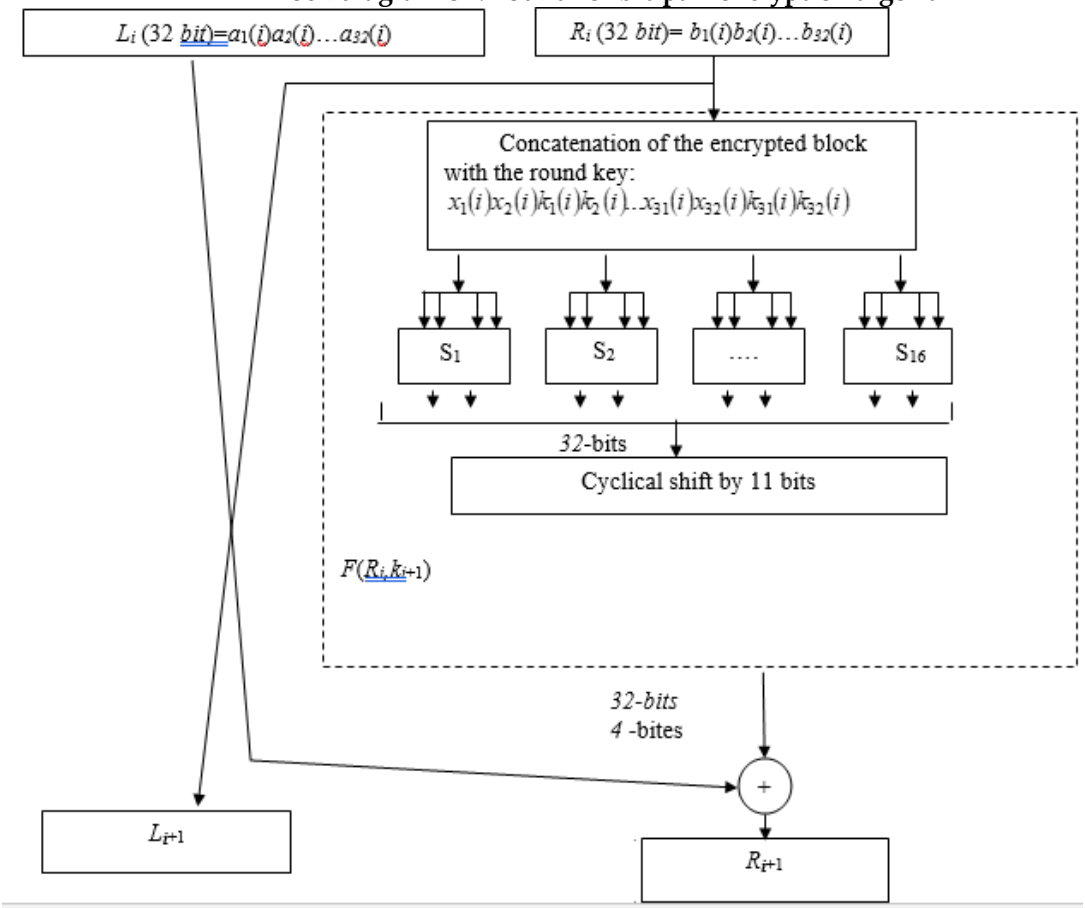
k/x	00	01	10	11
00	10	11	00	01
01	11	00	01	10
10	00	01	10	11
11	01	10	11	00

Where the values: "00", "01", "10", "11", corresponding to the cipher designations, are distributed uniformly, i.e. each of them is repeated 4 times. In this case, will ensure cryptographic stability of the transformation of the table substitution [10].

A cyclical shift of 11 (or 7, 17, 19) bits is accomplished by attaching contacts in the following order: 12-bits with the first bit $a_1(i)$ of the left 32-bit block L_i (32 *bit*)=$a_1(i)a_2(i)…a_{32}(i)$, 13-bits with $a_2(i)$; then, the 32-bit with $a_{11}(i)$. Encryption with pairs (even number) of bits, and a shift by a prime number greater than 2, has a positive effect on security (Dong, 2024).

Below there is provided the block diagram of the *i*-round for the bit-pair encryption algorithm.

Block diagram of *i*-round for bit-pair encryption algorithm



Now, a general block diagram with a set of basic transformations $F(R_i k_{i+1})$ or $F(R_i K_{i+1})$ is given: *concatenation (connection) of bits or with pairs of bits, transformation of a bitwise table substitution of the cipher of the value of the encrypted plaintext into a cipher designation with a truth table of logical operations or with pairs of bits, and a shift by a prime number has a positive effect on the resistance.*

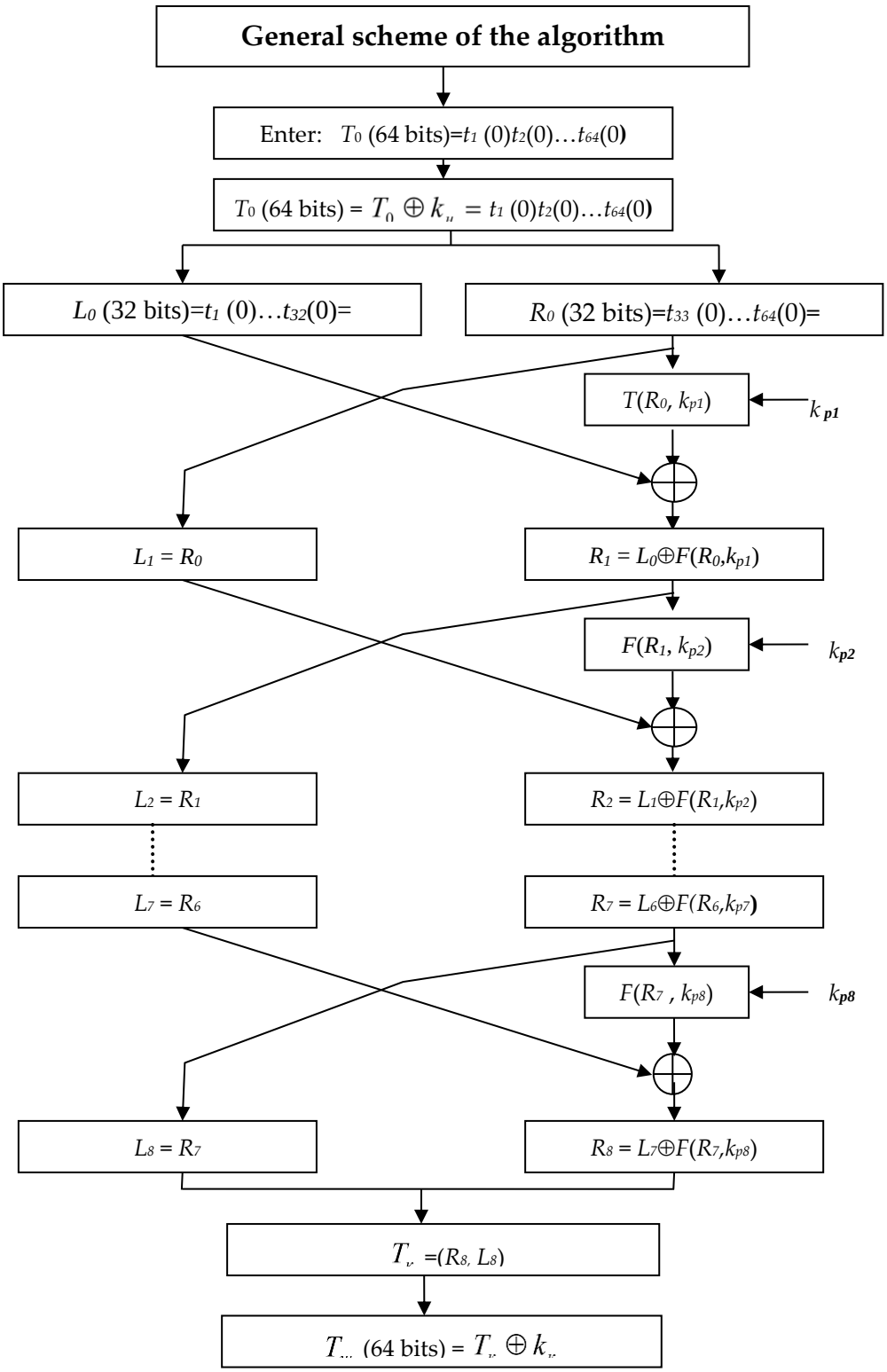
4. Discussion

In the general block diagram of the encryption algorithm given below, the transformations are defined: $T_к = (R_8, L_8)$ - the final block of the encrypted message and the bitwise addition of this block with the final key k_k, that is $T_ш = T_к \oplus k_k = (R_8, L_8) \oplus k_k$

Such definitions of transformation of the design of algorithms on the one hand increase the stability, on the other hand provide convenience in the development of effective designs of software and hardware based on the proposed algorithms based on the Feistel network. Indeed, taking the block $T_ш$ as an input block, as the initial key k_k, applying the keys of the rounds in the reverse order: $k_н$, k_{p8}, …, k_{p1}, $k_н$, the process of decryption of the encrypted message blocks [1-3] as encryption is carried out.

With the development of computational methods and technology, independent cryptographic stability of the transformation, the encryption algorithms of guaranteed stability used as a standard are lost due to the small length of the key (Umarovich, 2024).

According to another expression, the stability of the algorithm is naturally weakened. Therefore, the problem arises: preserving the basic transformations of the algorithm, lengthen their original keys and round keys [3,7-10].



A block diagram for solving such a problem for algorithms based on the Feistel network may look like this:

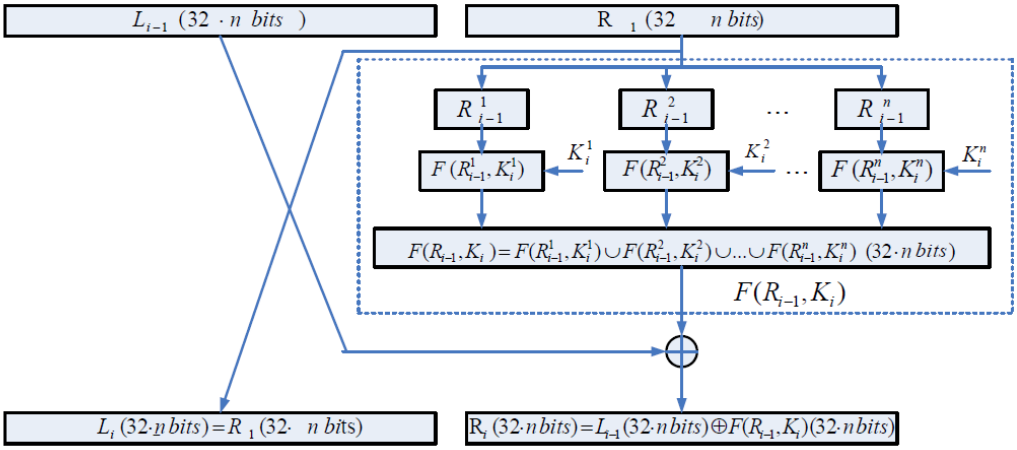


Figure 4.3. *I-round of modified Feistel network.*

Where:

1. Block length 64m bits, $m = 1,2,... \prec \infty$; of the plaintext. Original key length $|K| \cdot n$ *bits*, $n = 2,... \prec \infty$.
2. Combining the i-round key parts $K_i = K_i^1 K_i^2 .. K_i^n - i$.
3. Lengths of R_i – the left and L_i – right parts of the Feistel network: $|L| = |R| = 32 \cdot n$ *bits*.
4. $L_{i-1}(32 \cdot n\ bits)$ – the right part of i-round.
5. $R_{i-1}(32 \cdot n\ bits)$ – the left part of i-round.
6. $L_{i-1}^1(32\ bits)$, $L_{i-1}^2(32\ bits)$,..., $L_{i-1}^n(32\ bits)$ – 32-*bit* parts of the i -round key.
7. $R_{i-1}^1(32\ bits)$, $R_{i-1}^2(32\ bits)$,..., $R_{i-1}^n(32\ bits) - i$ -round of the left part.
8. $F(R_{i-1}^1, K_i^1)$, $F(R_{i-1}^2, K_i^2)$,..., $F(R_{i-1}^n, K_i^n) - i$ -round, corresponding transformations of the Feistel function.

The mathematical model of the modified Feistel network of i – round is as follows:

$$\begin{cases} L_i(32 \cdot n\ bits) = R_{i-1}(32 \cdot n\ bits) \\ R_i(32 \cdot n\ bits) = L_{i-1}(32 \cdot n\ bits) \oplus F(R_{i-1}, K_i)(32 \cdot n\ bits) \end{cases}$$

From the above modified Feistel network, it is clear that depending on the value of n, there are Feistel functions $F(R_{i-1}^1, K_i^1)$, $F(R_{i-1}^2, K_i^2)$,..., $F(R_{i-1}^n, K_i^n)$. This allows using several existing algorithms with proven effective transformations and S-blocks with increasing key length. It is noted that with $n = 1$ the key length is 256, with $n = 2$ the key length is 512, and so on. In the general form of the given modification, there is $l_1 = l \cdot n$, where l – is the key length of the main modified algorithm based on the Feistel network. In the general form of the given modification, there is $l_1 = l \cdot n$, where l – is the length of the key of the main modified algorithm based on the Feistel network (Kumar, 2019).

The encryption/decryption speed of the basic and modified algorithms is the same, since the number of transformations performed is the same [3,4,6-8].

5. Conclusion

Thus, the proposed modified Feistel networks have the following advantages:

1. Preserving the cryptographic design and properties of the basic transformations, it will increase the stability of the algorithm by increasing the value of some parameters of the algorithm.
2. Maintaining the properties and stability of transformations, increase the length of the algorithm key. This ensures the stability of the algorithm with respect to a cryptographic attack of exhaustive search of the initial key of the algorithm and the keys of rounds with basic transformations.
3. The speeds of the original algorithm and the modified one are the same. This circumstance ensures the effectiveness of the modification in relation to the development of software and hardware of the algorithm in applications.
4. The proposed algorithms with basic transformations: *concatenation (connection)* of the encrypted block of the open message with the round key, *tabular replacement* of the cipher value with the cipher designation, cyclic shift by a prime number greater than 7, are simple procedures that do not require calculations.

This case allows the desired possibilities of software and hardware implementation of such algorithms (Sorokin, 2020). Considering the importance and relevance of the solution of the problem, it would be inappropriate for scientific specialists to pay due attention to the results obtained and published by the authors.

REFERENCES

1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. –М.: издательство ТРИУМФ, 2003 – p. 816.
2. Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В. Основы криптографии: Study guide, 2nd edition. – М.: Гелиос АРВ, 2002.- p. 480.
3. Акбаров Д. Е. Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг қўлланилиши – Тошкент, «Ўзбекистон маркаси», 2009 – p. 434.
4. Акбаров Д. Е. , Сиддиқов А. А , Тураев Б.Т. Фейстел тармоғи ва унга асосланган симметрик блоклаб шифрлаш алгоритмларини такомиллаштиришнинг фундаментал усуллари. Materials of scientific and technical conference: «Амалий математика ва ахборот хавфсизлиги». 2014 y. April, 28-30. pp. 274-281.
5. Зензин О. С., Иванов М. А.. Стандарт криптографической защиты – AES. Конечные поля /Под ред. М. А. Иванова – М.: КУДИЦ-ОБРАЗ, 2002. - p. 176.
6. Акбаров Д. Е. Об одном алгоритме шифрования данных с симметричным ключом. // Инфокоммуникации: Сети-Технологии-Решения. -4(8)/2008. - pp. 25-36.
7. АкбаровД.Е., Умаров Ш. А. Working out the new algorithm enciphered the data with a symmetric key. // Siberian Federal University. Engineering&Technologies. 2016, 9(2). – pp. 214-224.
8. Акбаров Д.Е., Мухтаров Ф.М.,Умаров Ш. А .Фундаментальные методы модификации сети Фейстеля алгоритмов шифрования // Information letter of the Karakalpak Branch of the Academy of Sciences of the Republic of Uzbekistan. Nukus. 2016. №4. pp. 13-16.
9. Акбаров Д.Е., Умаров Ш.А. Новый алгоритм блочного шифрования данных с симметричным ключом. // Вісник НТТУ «КПІ». Серія Приладабудування. -2016.-Vol.: 52(2). pp. 82-91.
10. Умаров Ш.А. Разработка криптостойких логических и табличных отображений для алгоритмов шифрования. // Dissertation for Doctor of Philosophy in Mathematics (Ph.d). Cypher–05.01.05. –Ташкент. Нац. Университет. Докторский Ученый совет DSc 03/30. 12.2019 FM 01.02 – Defense succeeded 13.06. 2023.
11. Акбаров Д.Е., Умаров Ш.А. Электротехнические схемы криптографических табличных преобразований. // Ферганский политехнический институт. Научно-технический журнал. Vol.: 27, №5. 2023. pp. 9–17.
12. Dey, C. (2024). Enhancing the Key Recovery Attack on Round Reduced Salsa. *IEEE Access*, *12*, 31736–31744. https://doi.org/10.1109/ACCESS.2024.3367797
13. Dong, D. (2024). Hardware Implementation of Next Generation Reservoir Computing with RRAM-Based Hybrid Digital-Analog System. *Advanced Intelligent Systems*. https://doi.org/10.1002/aisy.202400098
14. Kumar, T. (2019). The cryptographic properties of feistel network-based quasigroups. *Advances in Intelligent Systems and Computing*, *814*, 539–549. https://doi.org/10.1007/978-981-13-1501-5_47

15. Mogos, G. (2023). Quantum Biometric Fingerprint Encryption Based on Confusion and Feistel Algorithm. *2023 International Conference on Platform Technology and Service, PlatCon 2023 - Proceedings*, 53–57. https://doi.org/10.1109/PlatCon60102.2023.10255158
16. Rahman, M. M. (2024). Practical Implementation of Robust State-Space Obfuscation for Hardware IP Protection. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, *32*(2), 333–346. https://doi.org/10.1109/TVLSI.2023.3307027
17. Sorokin, M. (2020). On Integral Distinguishers for Ciphers Based on the Feistel Network Generalizations. *Mechanisms and Machine Science*, *80*, 189–197. https://doi.org/10.1007/978-3-030-33491-8_23
18. Umarovich, J. G. (2024). Round key formation algorithm for symmetric block encryption algorithms. *E3S Web of Conferences*, *501*. https://doi.org/10.1051/e3sconf/202450102007
19. Wang, Y. (2024). An image encryption algorithm based on circular rotation and generalized Feistel structure. *Soft Computing*, *28*(5), 4335–4358. https://doi.org/10.1007/s00500-023-08747-z
20. Zhang, Y. (2022). Cryptanalysis against Type-III Generalized Feistel Networks and Its Variants with SP Type Round Functions. *2022 IEEE 10th International Conference on Information, Communication and Networks, ICICN 2022*, 71–76. https://doi.org/10.1109/ICICN56848.2022.10006631