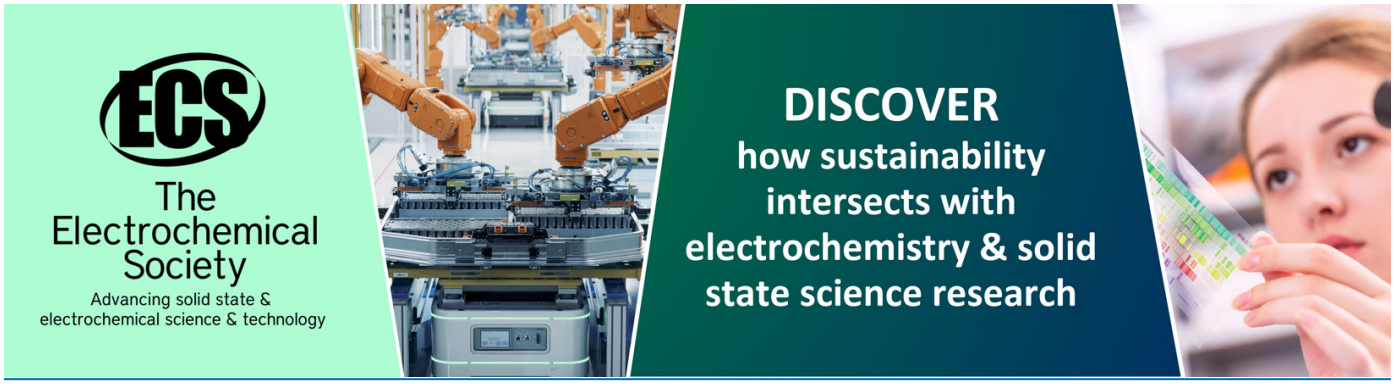
Application three-valued logic in symmetric block encryption algorithms



Journal of Physics: Conference Series **2131** (2021) 022082 doi:10.1088/1742-6596/2131/2/022082

Application three-valued logic in symmetric block encryption algorithms

T R Abdullaev and G U Juraev

National University of Uzbekistan named after Mirzo Ulugbek, City Tashkent. Uzbekistan

E-mail: timurar@yandex.ru

Abstract. The issues of limiting the use of binary logic for the further development of science engineering are discussed. The effectiveness of the use of the ternary number system at this stage in the development of information technologies is substantiated and shown. A method is proposed for increasing the informational entropy of plaintext by adding random data using ternary logic in the process of symmetric encryption. To reliably hide the added random data, the first transforming function is proposed to choose gamming with a key.

1. Introduction

As you know, encryption solves one of the main problems of protecting information - namely, the problem of ensuring the confidentiality of messages. Symmetric ciphers have high encryption speeds and are also much easier implemented both software and hardware. For this reason, symmetric encryption is often used to encrypt messages with a greater length than asymmetric encryption.

Symmetric ciphers are divided into two categories: block and stream ciphers. Block ciphers have a drawback: identical blocks of plaintext correspond to identical blocks of ciphertext and vice versa, the existence of the problem of the last block of an incomplete blocks length of a plaintext. In practice, the most widely used combined methods of encryption (or rather, stream modes using block ciphers), using the principle of generating a stream of keys (gamma cipher) using pseudo-random sequence generators.

Stream ciphers are very productive, often used to encrypt audio and video information. Stream ciphers as gamming ciphers for their implementation require the use of pseudo-random sequence generators to generate gamma (key sequence). With a sufficiently frequent change of key to generate a gamma sequence, stream ciphers provide sufficient durability. However, when using the gamma sequence generator, it is necessary that the recipient of the encrypted message also has exactly the same gamma sequence generator, which generates a sequence of pseudo-random numbers in direct relation to the encryption key.

This article proposes a symmetric encryption method that uses the addition of random data to a message. For this purpose, the ternary number system is used. With this encryption method, there is no need to use pseudo-random number generators on the receiving side.

2. Some disadvantages and limitations of binary logic for the further development of science and technology

As the rapid development of computing systems and information technologies shows, the use of binary logic is accompanied with some limitations.

First, the limitation of the development of microprocessors, in general, of the microelectronic industry based on binary logic is associated with the limit of miniaturization of logic elements and memory cells. Today, data storage capacities that exist in the form of physical media generally comply with Moore's law. In accordance with Moore's law, the number of transistors on a chip chip doubles over a period of one to two years. At the beginning, G.Moore believed that the doubling time is about one year, but over time this estimate has changed noticeably, and now they are talking about doubling in two years [1,2,3].

The second disadvantage of binary logic can be considered the paradoxes of classical logic. One of the paradoxes of classical logic is associated with the following statement: "If A, then B", where A and B are true or false statements. This statement is false if statement A is true and B is false. In all other cases, this statement is true. This form of approval is called "material implication" [4]. These paradoxes of material implication are a direct consequence of two main tenets of classical logic:

1. Every statement is either true or false, and the third is not given;
2. The truth value of a complex statement depends only on the truth values of the simple statements contained in it, as well as on the nature of the relationship between them, and does not depend on their content.

Within these two postulates, an adequate construction of conditional statements is impossible. It is clear that the material implication does not fulfill its function of justification [4].

Third, it should be noted that mathematics cannot apply binary logic with a strict relation to the truth and falsity of statements. In particular, for example, consider the following postulates studied in secondary school:

– «It is impossible to divide by 0». At the same time, when studying ways to simplify fractions in school, the expression for $x = 0,\ 2x/x = 2$ is consistent, and when studying higher mathematics, the expression $\lim_{x\to 0} 1/x = \infty$.

– «It is impossible to find the root of a negative number», which does not cancel «complex numbers», where $\sqrt{-4} = 2i$, at $i = \sqrt{-1}$.

– In Euclidean geometry there is an axiom «through a point not lying on this line one can draw only one and only one straight line parallel to this one», but in the geometry of Lobachevsky the axiom is formulated as «at least two straight lines pass through a point not lying on this line in one plane and not intersecting it» [5].

And the fourth, the number series itself is not binary, but triple, there are negative numbers, positive numbers and «0».

The latter definition, concerning the trinity of a numerical series, did not allow to adequately expressing numbers in bit form. As a result, to distinguish negative numbers from positive numbers in computer science, either the most significant bit, equal to "1", is used, or an additional code is used. Naturally, when transforming one format of a number into another, without control by the user, paradoxes arise. For example, if the variable is "a = –1" in the "byte" format (that is, the range of integers is from –127 to 127) and "b= 255" in the format of "ubyte" (that is, the range of integers from 0 to 255), then "a=b". This paradox can be checked in the "calculator" program of the "Windows XP" operating system. To do this, you need to run the "calculator" program, convert the calculator to "engineering" type, dial "1" and "+/-" to get "–1" click on the "Bin" switch for binary translation, select the "1 byte" switch, and click on the "Dec" switch. At the exit get the number "255".

All the above facts confirm the achievement of the limit of miniaturization of computer elements and for further development requires a transition to fundamentally new technologies.

3. The ternary number system as an alternative number system

How can we overcome the above limitations associated with the use of binary logic? Most likely to use a different number system.

Issues related to the use of the ternary number system for the further development of science and technology have long been discussed. Interest in the ternary logic and its further application arose long before the appearance of the first computers. This circumstance is explained by the remarkable properties of the symmetric code of numbers. For example, under the guidance of Professor N.P. Brusentsov at Moscow State University Lomonosov in 1961 implemented the ternary number system. As a result, the first ternary computer "Setun" was created. At the same time, Professor N.P. Brusentsov as an advantage of the ternary representation of numbers, before the binary, noted the cost effectiveness of the ternary code [6]. Similar work was carried out, and carried out abroad. Since 2008, the University of California Polytechnic State University of San Luis Obispo uses the TCA2 computer system based on the ternary number system for scientific needs.

When choosing an alternative number system, it should be evaluated on the so-called "economy" or "density." Under the "economy" or "density" refers to the supply of numbers that can be written using a certain number of characters. For example, to express all 1000 numbers in the range from “0” to “999” in decimal notation, you need “30” characters, by “10” characters to “3” digits [7], that is:

$$z = sr, \tag{1}$$

where *z* is the total number of characters required,
s is the base of the number system,
r is the number of discharge.
From here the number of required discharge will be equal to:

$$r = \frac{z}{s}. \tag{2}$$

The number of numbers that can be expressed in this number system with a given number of discharges is:

$$n = s^r. \tag{3}$$

Or expressed through the total number of signs and bases of the number system:

$$n = s^{z/s}. \tag{4}$$

Taking into account the practical use, consider the value of the number system equal, for example, "s = 2,3,4,5,6", for the number of characters equal to "z = 60" in (4):

$$\text{at } s = 2, n = 2^{60/2} = 1073741824;$$
$$\text{at } s = 3, n = 2^{60/3} = 3486784401;$$
$$\text{at } s = 4, n = 2^{60/4} = 1073741824;$$
$$\text{at } s = 5, n = 2^{60/5} = 244140625;$$
$$\text{at } s = 6, n = 2^{60/6} = 60466176.$$

It is obvious that the most "economical" number system and having the maximum "density" is the "ternary number systems" [7].

Currently, there is an active search for alternative ways to increase processor performance. For this purpose, in the world there are several research groups.

Now let us dwell on the problem of solving the problem of the element base. For the transition to the ternary number system it is impossible to use old constructive solutions for processing, transmitting and storing information. But scientific laboratories, looking for opportunities to increase speed and increase the density of stored information, for the order of several decades, no longer operate with a binary number system.

A group of scientists from the University of Kiel (Germany) was able in 2017 to successfully synthesize a new class of spin-cross molecules on the surface of the material, with a huge data storage potential. As a result, the storage density of conventional hard drives can be increased by two orders of magnitude, that is, 100 times, while the size of the media can be much smaller than today. It was also found that the synthesized molecules for information storage are not two possible states, but three. The technology proposed by this group of scientists uses as a storage unit for information one molecule the size of one nanometer, respectively, its area is one hundred times smaller than that used in current technologies [8].

Chemists under the guidance of Professor Felix Tuczek synthesized a magnetic molecule of the spin crossover Fe (III). And the physicists Jasper-Tönnies, Gruber, Sujoy Karan were able to precipitate these molecules onto the surface of nitrogenous copper. Using the influence of an electromagnetic field, three different spin states can be communicated to molecules. In experiments, this system showed its performance [8].

Also, to save resources, when creating a quantum computer, it was found that it is advisable to operate not qubits, but qurits, since the economic costs are the same and the amount of information processed is three times larger [9].

4. The use of the ternary number system in information technology and cryptography

As applied to computer science, the ternary number system can be symmetric and asymmetric. In the symmetric ternary notation, the elementary units of information are trit equal to “–1, 0, 1”, and in the asymmetrical - “0, 1, 2”. For ease of writing "-1", in the ternary notation, you can use the symbol "$\bar{1}$". Then, in the symmetric ternary notation, it is not necessary to use special signs to determine the region of negative numbers. Then, in the symmetric ternary notation, it is not necessary to use special signs to determine the region of negative numbers. For example, «$-1_{10} = \bar{1}_3$», «$-255_{10} = \bar{1}00\bar{1}\bar{1}0_3$», a «$255_{10} = 100110_3$». To change the sign of a number, it is enough to invert all the tritas equal to "1" and "$\bar{1}$" to inverse, and to determine the sign of a number, it is enough to determine the sign of the most significant trit. Hence, all the mathematical operations in the ternary number system are performed faster and easier.

If we consider the possibility of using ternary logic as an encryption function, we have one more positive point. In the binary system of calculus there are only “16” logical two operand transforming functions, such as conjunction, disjunction, modulo two, multiplication modulo two, etc. As a gamma, you can use at least “216” reversible logic functions or a combination of them. In this case, in the binary number system, only “6” reversible logical functions are possible, of which only “2” are suitable for use.

It should be noted that the ternary data representation is widely used in information transfer systems in various physical environments. The need to use more than two signal states is associated with the smoothing of the pulse front and, as a consequence, the reduction of noise in the channel. In particular, the 4B3T protocol is one of the methods of linear coding of information for its subsequent transmission over an optical cable, twisted pair, coaxial cable, or infrared radiation [10,11]. The essence of the method is to represent 4 bits of information in 3 signal levels: plus, zero and minus, according to the MMS43 coding table. This method of data presentation is used in ISDN data transmission networks via the BRI interface [12,13,14].

Based on the foregoing, to overcome the shortcomings of binary logic and the number system, the further development of information technologies will most likely be based on the threefold logic and number system. Based on this hypothesis, it is proposed to use a method based on the addition of random data to the message and homophonic ciphers using the ternary number system.

Consider the symbols that are used in the message when processing in digital form. As a rule, this is an ASCII (American Standard Code for Information Interchange - American Standard Code for Information Exchange) code that has 256 characters-bytes in a set. But the bytes themselves consist of a set of simpler characters - bits, there are only two “0” and “1”. It is this set of characters that is proposed to be supplemented with the third character “2”, that is, this character should be added to the message as random data. Due to the fact that the symbol “2” differs from the signs of the message, it can be added to any place in the message and by any amount. At the same time, mixing random data into information performs two functions:

– Translates data into a ternary view;

– Introduces data to the entropy, that is, accident.

We define the required length of the data block and the key encryption sequence. Proceeding from the position that, at present, to ensure the strength of a cipher with a huge margin, an encryption key for block ciphers of 256 bits is often used in practice, then the system being developed must operate with a key sequence of no less length. As a result, we have:

$$2^{256} = 1{,}158 \times 10^{77},$$
$$3^{161} = 6{,}554 \times 10^{76},$$
$$3^{162} = 1{,}966 \times 10^{77},$$
$$\mathbf{3^{161} < 2^{256} < 3^{162}}.$$

It follows that the encryption key of block ciphers with a length of 162 trits of the ternary number system ensures the strength of the cipher, not less than the encryption key with a length of 256 bits of the binary number system. When choosing one treyt (byte analogy) equal to "6" tritium, the length of the key sequence must be a multiple of "6".

Considering the need to present encrypted ternary data in binary form, for the reverse transmission via communication channels, we will analyze the matching density when translating trites to bits:

$3^1 \le 2^2$ – the completeness of the matching is equal $100 \times 3^1 \le 2^2 = 75\%$;
$3^2 \le 2^4$ – the completeness of the matching is equal $100 \times 3^2 \le 2^4 = 56\%$;
$3^3 \le 2^5$ – the completeness of the matching is equal $100 \times 3^3 \le 2^5 = 84\%$;
$3^4 \le 2^7$ – the completeness of the matching is equal $100 \times 3^4 \le 2^7 = 63\%$;
$3^5 \le 2^8$ – *the completeness of the matching is equal* $100 \times 3^5 \le 2^8 = \mathbf{95}\%$;
$3^6 \le 2^{10}$ – the completeness of the matching is equal $100 \times 3^6 \le 2^{10} = 71\%$.

This shows that it is optimal to compare the "5" trites with the "8" bits. With this method, of the possible "256" codes of the binary number system, "243" codes used by the ternary number system will be involved. It follows that the additional requirement to key sequence, it must be a multiple of "5". In this case, the least common multiple of "5" and "6" following the "162" is equal to "180". Hence, the length of the key sequence that meets the following conditions:

not worse than $2^{256} = 1{,}158 \times 10^{77}$;
multiple “6” for dividing by treyt;
multiple “5” for reverse conversion to the binary view should be “180” trit.

The probability of the appearance of "0" or "1" when using the binary number system in random messages is approximately 50%. Similarly, the number of occurrences of "0", "1" and "2" in the ternary representation should be uniform: 33.3% - "0", 33.3% - "1" and 33.3% - "2". Hence, the number of added “2” symbols should be approximately no more than 33% of the total amount of data, which is 180/3 = 60 tritas. It is necessary to take into account the balance between increasing the length of the message and the necessary degree of entropy of random information. It is necessary

to take into account the balance between increasing the length of the message and the necessary degree of entropy of random information.

To reliably hide the added random data, the first transforming function is proposed to choose the operation gamming with the encryption key.

The function for mixing the key and the plaintext block is proposed to be used in the ternary logic in the following form (table 1) [16,17]:

$$r = (s + k + 2) mod\ 3. \tag{5}$$

where r is the trit of new block,
s is the trit of block,
k is the trit of key.

Table 1. The Truths of the Transforming Function $r = (s + k + 2) mod\ 3$.

s	k	$r = (s + k + 2) mod\ 3$
0	0	2
0	1	0
0	2	1
1	0	0
1	1	1
1	2	2
2	0	1
2	1	2
2	2	0

The corresponding inverse gamming function is equal (table 2):

$$s = (r - k + 1) mod\ 3. \tag{6}$$

Table 2. The Truths of the Transforming Function $s = (r - k + 1) mod\ 3$.

r	k	$s = (r - k + 1) mod\ 3$
0	0	1
0	1	0
0	2	2
1	0	2
1	1	1
1	2	0
2	0	0
2	1	2
2	2	1

These functions are selected from the consideration that when you next XOR with a key was not obtained the source code.

Figure 1 shows the mechanism for complementing messages from 128 to 160 bits with a third symbol in the amount of 52 to 20 (that is, as a result, we will have 180 characters):

1) the input is a message size of from 128 to 160 bits (16 to 20 bytes);

2) “2” is mixed in randomly to the message, complementing the message up to 180 characters.

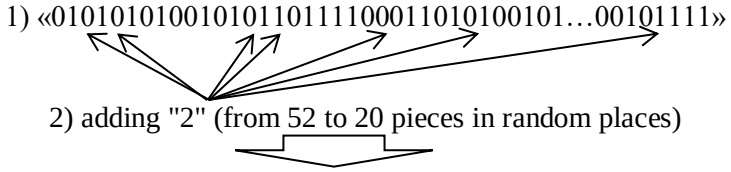


Figure 1. The scheme of mixing the third character in random places of the message.

The summation with a three-character key can be calculated by the specified formula (5):

Message: «0102102101001010211201111002011010210010 1…0010211 11»
Key: «0120120001201001200120120200220012001101 2…212122021»
Result: «2111111021121200000210120121120211100000 2…102002021».

After gamming operation in the output block, it is impossible to determine where the random data was added. Moreover, if encrypt the same message block with the same key, then the output will result in different encrypted blocks, which will make it difficult for the cryptanalyst to open the cipher.

If gamming ciphers are used, then plaintext can be recovered from the cipher text using the inverse formulas. To do this, it is enough to sum up the three-character key with the cipher text using the formula (6) intended for decryption, and exclude the symbol "2" from the received message:

Cipher text: «2111111021121200000210120121120211100000 2…102002021»
Key: «0120120001201001200120120200220012001101 2…212122021»
Message: «0102102101001010211201111002011010210010 1…0010211 11».

The received original message, after excluding the symbol “2”, has the form:

«0101010100101011011110001101010010 1…00101111».

Another use of random data is steganography. In steganography is not added to the message random data, and the message in a special way is mixed randomly.

The next encryption method using random data is the so-called "homophonic ciphers". The essence of such ciphers is to hide the frequency of using the characters of an open message.

5. Conclusion

The efficiency of using the ternary number system for the further development of information technologies and science in general is substantiated. It is noted that the use of ternary logic in microelectronics significantly improves the performance of processors, and also allows several times to increase the storage density of conventional hard drives and significantly reduce the size of storage media.

Proposed by the use of the ternary number system in symmetric cryptography for mixing random data in plaintext. Adding random data to the encrypted message will allow to the probabilistic nature of information conversion operations, which makes it difficult to use the general principle of cryptanalysis of ciphers based on attempts to identify the statistical properties of the encryption algorithm, for example, by selecting special source texts or cryptograms.

The proposed method of adding random data in the plaintext block allows you to:

– add the character “2” to any place of the processed text block;
– increase the entropy of open information;
– use different block sizes of open information;
– use a more complex formula for operation gamming than in binary logic;

– receive at the output of encryption each time different encrypted blocks.

Using gamming with the key as the first conversion function ensures that the random data added is hidden. In this case, with the proposed method of encryption using ternary logic in stream ciphers and gamming ciphers, there is no need to use pseudo-random number generators on the receiving side, as well as changing the key to generate a gamma sequence.

If we take into account that public-key cryptographic systems use multivalued prime and natural numbers, as well as more numbers in the ternary number system than in any other system, we can hope that the use of the ternary number system for public-key encryption also gives positive results.

References

[1] Moore's law // Free encyclopedia *Wikipedia*. URL: https://en.wikipedia.org/wiki.
[2] Skorobov A. Moore's Law // Site of the Faculty of Mathematics and Mechanics of Ural State University.2005. URL: http://cs.usu.edu.ru/study/moore/.
[3] Shashlov S. Zakon Moore - 40 years! // *IXBT* website. URL: http://www.ixbt.com/editorial/moorelaw40th.shtml.
[4] Zinoviev A. A. Logic science. - M: *Thought*,1971.
[5] Hyperbolic geometry (Lobachevskian geometry) // Free encyclopedia *Wikipedia*. URL: https://en.wikipedia.org/wiki/Hyperbolic_geometry.
[6] Brusentsov N. P. "The use of the ternary code and three-digit logic in digital machines". *Scientific report* №24BT (378), Moscow State University, Moscow 1969. –27 p.
[7] Fomin S. V. Number systems - M: *Science*, 1987.
[8] Nilova M. Molecular Winchesters and Trites Instead of Bits - This is the Future of Data Storage // https://golos.io.2017, URL: http://www.uni-kiel.de.
[9] Grokhotov M. The Future of Quantum Computers - in Ternary Computations. https://infuture.ru/article/475.
[10] 4B3T // Free encyclopedia *Wikipedia*. URL: https://en.wikipedia.org/wiki/4B3T.
[11] Bobrysheva G. V. Evaluation of the corrective properties of channel codes of type (n, k). // *Computational systems and information processing technologies: Interuniversity collection of scientific papers*. Issue 2 (28). - Penza: Information and Publishing Center of PSU, 2003. –164 p.
[12] James Irvine, David Harle. Data Communications Networks: An Engineering Approach. – Wiley, 2001. – Page Count: 268.
[13] William Stallings. Data and Computer Communications, Sixth Edition. – Publisher: *Prentice Hall*, 1999. – Page Count: 800.
[14] Brusentsov N. P. The paradoxes of logic, common sense and the dialectical postulate of Heraclitus-Aristotle, Software systems and tools: Thematic collection No. 4. / Ed. L. N. Korolev. - M: *Publishing Department of VMIK MSU*, 2003. p. 35-38.
[15] Pronkin Yu. S., Lesnichevskaya I. A. Elements of probability theory and mathematical statistics: Tutorial. - Tver: TSTU, 2005. - 104 p.
[16] Three-state logic // Free encyclopedia *Wikipedia*. URL: https://en.wikipedia.org/wiki/Three-state_logic.
[17] Ternary logic // Site *Synopses Wiki!*, University ITMO. URL: https://neerc.ifmo.ru/wiki/index.php.