ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫ
әл-Фараби атындағы Қазақ ұлттық университетінің

ХАБАРЛАРЫ

ИЗВЕСТИЯ

НАЦИОНАЛЬНОЙ АКАДЕМИИ НАУК
РЕСПУБЛИКИ КАЗАХСТАН
Казахский национальный университет
имени аль-Фараби

N E W S

OF THE ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN
al-Farabi Kazakh National University

SERIES
PHYSICO-MATHEMATICAL

6 (340)

NOVEMBER – DECEMBER 2021

PUBLISHED SINCE JANUARY 1963

PUBLISHED 6 TIMES A YEAR

ALMATY, NAS RK

NAS RK is pleased to announce that News of NAS RK. Series physico-mathematical journal has been accepted for indexing in the Emerging Sources Citation Index, a new edition of Web of Science. Content in this index is under consideration by Clarivate Analytics to be accepted in the Science Citation Index Expanded, the Social Sciences Citation Index, and the Arts & Humanities Citation Index. The quality and depth of content Web of Science offers to researchers, authors, publishers, and institutions sets it apart from other research databases. The inclusion of News of NAS RK. Series of chemistry and technologies in the Emerging Sources Citation Index demonstrates our dedication to providing the most relevant and influential content of chemical sciences to our community.

Қазақстан Республикасы Ұлттық ғылым академиясы «ҚР ҰҒА Хабарлары. Физикалық-математикалық сериясы» ғылыми журналының Web of Science-тің жаңаланған нұсқасы Emerging Sources Citation Index-те индекстелуге қабылданғанын хабарлайды. Бұл индекстелу барысында Clarivate Analytics компаниясы журналды одан әрі the Science Citation Index Expanded, the Social Sciences Citation Index және the Arts & Humanities Citation Index-ке қабылдау мәселесін қарастыруда. Webof Science зерттеушілер, авторлар, баспашылар мен мекемелерге контент тереңдігі мен сапасын усынады. ҚР ҰҒА Хабарлары. Химия және технология сериясы Emerging Sources Citation Index-ке енуі біздің қоғамдастық үшін ең өзекті және беделді химиялық ғылымдар бойынша контентке адалдығымызды білдіреді.

НАН РК сообщает, что научный журнал «Известия НАН РК. Серия физико-математическая» был принят для индексирования в Emerging Sources Citation Index, обновленной версии Web of Science. Содержание в этом индексировании находится в стадии рассмотрения компанией Clarivate Analytics для дальнейшего принятия журнала в the Science Citation Index Expanded, the Social Sciences Citation Index и the Arts & Humanities Citation Index. Web of Science предлагает качество и глубину контента для исследователей, авторов, издателей и учреждений. Включение Известия НАН РК в Emerging Sources Citation Index демонстрирует нашу приверженность к наиболее актуальному и влиятельному контенту по химическим наукам для нашего сообщества.

«ҚР ҰҒА Хабарлары.
Физика-математикалық сериясы».
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

Меншіктеуші: «Қазақстан Республикасының Ұлттық ғылым академиясы» РҚБ (Алматы қ.). Қазақстан Республикасының Ақпарат және қоғамдық даму министрлігінің Ақпарат комитетінде 14.02.2018 ж. берілген **No 16906-Ж** мерзімдік басылым тіркеуіне қойылу туралы куәлік.
Тақырыптық бағыты: *математика, информатика, механика, физика, ғарыштық зерттеулер, астрономия, ионосфера.*
Мерзімділігі: жылына 6 рет.
Тиражы: 300 дана.
Редакцияның мекен-жайы: *050010, Алматы қ., Шевченко көш., 28, 219 бөл., тел.: 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

Типографияның мекен-жайы: «Аруна» ЖК, Алматы қ., Мұратбаев көш., 75.

«Известия НАН РК.
Серия физика-математическая».
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

Собственник: Республиканское общественное объединение «Национальная академия наук Республики Казахстан» (г. Алматы).
Свидетельство о постановке на учет периодического печатного издания в Комитете информации Министерства информации и общественного развития Республики Казахстан **No 16906-Ж** выданное 14.02.2018 г.
Тематическая направленность: *математика, информатика, механика, физика, космические исследования, астрономия, ионосфера.*
Периодичность: 6 раз в год.
Тираж: 300 экземпляров.
Адрес редакции: *050010, г. Алматы, ул. Шевченко, 28, оф. 219, тел.: 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

Адрес типографии: ИП «Аруна», г. Алматы, ул. Муратбаева, 75.

News of the National Academy of Sciences of the Republic of Kazakhstan. Physical-mathematical series.
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

Owner: RPA «National Academy of Sciences of the Republic of Kazakhstan» (Almaty). The certificate of registration of a periodical printed publication in the Committee of information of the Ministry of Information and Social Development of the Republic of Kazakhstan **No. 16906-Ж,** issued 14.02.2018
Thematic scope: *mathematics, computer science, mechanics, physics, space research, astronomy, ionosphere.*
Periodicity: 6 times a year.
Circulation: 300 copies.
Editorial address: *28, Shevchenko str., of. 219, Almaty, 050010, tel. 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

Address of printing house: ST «Aruna», 75, Muratbayev str, Almaty.

NEWS
OF THE NATIONAL ACADEMY OF SCIENCES OF THE REPUBLIC OF KAZAKHSTAN
PHYSICO-MATHEMATICAL SERIES
ISSN 1991-346X
Volume 6, Number 340 (2021), 73–80 https://doi.org/10.32014/2021.2518-1726.104

UDC004.056

Seilova N.A.[1*], Ibrayev R.B.[1], Gorlov L.V.[2], Turdalyuly M.[1]

[1]Satbayev University, Almaty, Kazakhstan;
[2]Al-Farabi Kazakh National University, Almaty, Kazakhstan.
E-mail: seilova_na@mail.ru

CRYPTOGRAPHIC PROPERTIES OF A NONLINEAR NODE OF A BLOCK SYMMETRIC ENCRYPTION ALGORITHM QALQAN

Abstract. Ensuring the confidentiality and integrity of information with limited access to be transmitted through communication channels, as well as circulating in information systems, is achieved by using cryptographic transformation algorithms. In particular, encryption algorithms that ensure the confidentiality of information are the core of cryptographic information protection tools.

The security of such funds is determined primarily by the quality and reliability of the encryption algorithms implemented in them. The system of cryptographic protection of information is self-sufficient to provide cryptographic protection of critical information circulating in the information systems of organizations.

In this paper, the main cryptographic properties of the nonlinear node of the Qalqan block symmetric encryption algorithm, which affect its cryptographic strength, are considered. Algorithms for calculating the cryptographic characteristics are given.

The cryptographic information protection system implements the developed block symmetric encryption algorithm Qalqan and the key generation, generation, distribution and management protocol. When developing a system of cryptographic protection of information, the requirements of the current regulatory legal acts regulating the requirements for the use of cryptographic protection of information in information systems with critical information are taken into account.

The Qalqan algorithm has been developed taking into account the trends in the development of science and technology, and is able to withstand cryptographic attacks due to the “safety margin” laid down at the development stage.

The developed algorithm of block symmetric encryption is recommended to be approved in the prescribed manner as a national standard to ensure the protection of the information space of the state from potential threats arising from undeclared capabilities in the structures of foreign encryption algorithms.

Key words: encryption algorithm, vector boolean functions, nonlinear node.

Introduction. In modern block symmetric encryption algorithms, the scattering principle, which makes it possible to ensure the propagation of the influence of one plaintext character on more than one ciphertext character, as well as the propagation of the influence of one key element on more than one ciphertext characterare implemented in the form of vector boolean functions (replacement table, substitution block).

The correct choice of the characteristics of vector Boolean functions is the main factor in ensuring security, since they are, as a rule, the only nonlinear node of symmetric block encryption algorithms.

In this paper, the main cryptographic properties of the nonlinear node of the Qalqan symmetric block encryption algorithm, implemented as a vector boolean function of 8 variables, are investigated.

In view of the presence of serious claims to the secret internal structure of the nonlinear node of the block symmetric encryption algorithm Grasshopper and the hash function ofStribog [1], the nonlinear node of the block symmetric encryption algorithm Qalqan was designedaccording to the principle of maximum transparency.

For this, a similar to that used in the AES block symmetric encryption algorithm, the generation of a replacement table according to proposed by K. Nyberg in 1991 [2] method was chosen. The constants used in the generation have been changed in order to achieve closer to the optimal values [3] of such cryptographically

important parameters like lowering the maximum of the differential profile in addition and XOR (counteraction to differential analysis), lowering the maximum of the table of linear approximations (counteraction to linear analysis), high algebraic degree, maximum to the class of affine transformations distance (high nonlinearity), absence of linear structures.

Materials and methods. Vector Boolean function.

Definition 1.A Boolean function of *n* variables is a function $f: F_2^n \to F_2$.We denote the set of all Boolean functions of *n* variables by$P_2(n)$, wherein $|P_2(n)| = 2^{2^n}$.

Definition 2.A vector Boolean function of *n* variables is a function $f: F_2^n \to F_2^m$. We consider a vector Boolean function as a set of coordinate Boolean functions.

Definition 3.Hamming Weight $wt(a)$of a binary vector *a* of length *n* is the number of ones, contained in a: $wt(a) = \sum_{i=1}^{n} a_i$.

Definition 4.Hamming distance $d(x, y)$between two binary vectors is the number of positions in which they differ, or, equivalently$d(x, y) = wt(x \oplus y)$.

Definition 5.Scalar product $\langle x, y \rangle$of binary vectors *x* and *y* are defined as $\langle x, y \rangle = x_1 y_1 \oplus x_2 y_2 \oplus \ldots \oplus x_n y_n$.

Definition 6.The weight of a Boolean function *f* is a quantity equal to the power of its support$supp(f) = \{x \in F_2^n : f(x) = 1\}$.

Definition 7.Hamming distance $d(f, g)$between two Boolean functions of *n* variables is the number of positions at which their vectors of values differ from each other.$d(x, y) = |\{x \in F_2^n : f(x) \neq g(x)\}|$.

Definition 8.LetM_n – be some set of Boolean functions in *n* variables. The distance from the function *g* to the set of functions$M_n$is defined as$d(g, M_n) = min\{d(f, g) : f \in M_n\}$.

Definition 9.Any function$f: F_2^n \to F_2^m$can be uniquely written as a Zhegalkin polynomial or an algebraic normal form (ANF): $F(x_1, x_2, \ldots, x_n) = \bigoplus_{k=0}^{n} \bigoplus_{i_1, i_2, \ldots, i_k} a_{i_1, i_2, \ldots, i_k} x_{i_1, i_2, \ldots, i_k} \oplus a_0$,where$\{i_1, i_2, \ldots, i_k\} \subseteq \{1, 2, \ldots, n\}anda_{i_1, i_2, \ldots, i_k} \in F_2^m$.

Definition 10. Algebraic degree *deg*(F) of a function F means the number of variables in the longest term of an algebraic normal form (ANF), at which the coefficient is not equal to the zero vector. A function which degree at most 1 is called affine.Funclion is called linear when ANF's $a_0$is equal to 0.

Definition 11.For each$y \in F_2^n$Walsh-Hadamard coefficient $W_f(y)$of a booleanfunction *f*in*n* variables is the quantity defined by the equality$W_f(y) = \sum_{x \in F_2^n} (-1)^{f(x) \oplus \langle x, y \rangle}$. The set of coefficients $W_f(y)$for all $y \in F_2^n$is called the Walsh-Hadamard spectrum of the booleanfunction*f*.

Definition 12. A component function is any nonzero linear combination of coordinate functions, meansbooleanfunction $\langle b, F \rangle$, where$b \in F_2^m, b \neq 0$ [4].

The properties of vector Boolean function. 1. Algebraic degree. In symmetric block encryption algorithms, booleanfunctions with a sufficiently high degree should be chosen. The parameter deg(*F*) of a booleanfunction must be large. For symmetric block encryption algorithms, this condition is usually imposed so that the system of equations for the key bits constructed by analyzing the structure of the algorithm, including the booleanfunction *F* used as its component would have a high degree. The higher the degree of the system, the more difficult it is to solve, and therefore, to determine the key.

In other words, the value of the algebraic degree primarily determines the resistance of the symmetric block encryption algorithm to analytical attacks.

deg(f)parameter calculation algorithm:

Input: Function $f: F_2^n \to F_2^m$, consisting of the coordinate booleanfunctionsf_i, where$i = 1..m$.

Step 1.Calculate a vector of values $T_{f_i}$of functionf_i: for each $a \in F_2^n$find value of $f(a)$.

Step 2.Using the fast Walsh-Hadamard transform, calculate the vector of coefficients of the ZhegalkinpolynomialP_{f_i}.

Step 3. Count the number of variables in the longest term of the Zhegalkin polynomial for which the coefficient is not equal to the zero vector.

Output: the calculated number of variables in the longest term of the Zhegalkin polynomialis the deg(f) parameter.

2. Poise. Definition13. Boolean function f of n variables is called balanced if its weight is 2^{n-1}.

If the Boolean function is balanced, then the probability that it will take the value 0 or 1 is the same and is equal to 1/2. This allows to weaken the statistical relationship between the input of the function and its output. Otherwise, the cryptanalyst has the opportunity, using the probability ratio, to cryptanalize the cipher.

This statement is generalized to the vector case.

Determining the balance of a booleanfunction algorithm:

Input: function$f: F_2^n \to F_2$.

Step 1.Calculate a vector of values $T_f$of function$f$: for each$a \in F_2^n$count value$f(a)$.

Step 2.Calculate Hamming Weight $wt(T_f)$.

Step 3.Evaluate poise: $wt(T_f) = 2^{n-1}$?

Output:f −is balanced, if$wt(T_f) = 2^{n-1}$.

Definition 14. Vector boolean function $f: F_2^n \to F_2^m$is called balanced, if $|F^{-1}(y)| = |\{x \in F_2^n : F(x) = y\}| = 2^{n-m}$for any$y \in F_2^m$.

Moreover, the following statement is true.

Statement 1. Vector boolean function $f: F_2^n \to F_2^m$is balanced if and only if all its component functions are balanced$\langle v, \rangle$, $v \in F_2^m$, $v \neq 0$.

Note, that for $n = m$ the class of balanced vector functions coincides with the class of one-to-one functions. As a rule, they are the ones of greatest interest for use in symmetric block encryption algorithms as nonlinear nodes (S-box) to ensure unambiguous decryption [4, 5].

Determining the poise of a vector Boolean function algorithm:

Input: function$f: F_2^n \to F_2^m$, consisting of the coordinate Boolean functionsf_i, where$i = 1..m$.

Step 1.Calculate a vector of values$T_{f_i}$of functionf_i: for each$a \in F_2^n$findvalue$f(a)$.

Step 2.Calculate Hamming Weight$wt(T_{f_i})$.

Step 3.Evaluate poise: $wt(T_{f_i}) = 2^{n-1}$?

Step 4: Check the balance of each coordinate function, $f_i -$ is balanced, if$wt(T_{f_i}) = 2^{n-1}$.

Output: f −is balanced, if$wt(T_{f_i}) = 2^{n-1}$for$i = 1..m$.

3.Perfect poise. The property of perfect poise of a Boolean function is a generalization of the usual poise, when this function acts, for example, as a filtering function of a generator.

Definition 15.Vector boolean function $f: F_2^n \to F_2^m$is called perfectly balanced if its any coordinate function is balanced.

Algorithm for Determining the Perfect Equilibrium of a Vector Boolean Function$f: F_2^n \to F_2^m$is similar to the previous algorithm.

4.Avalanche characteristics. The concept of avalanche characteristics of a booleanfunction reflects one of Shannon's principles of constructing encryption transformations, namely, the scattering principle.

Definition 16. Boolean function f of n variables satisfies strict avalanche criterion (SAC), if for any direction $a \in F_2^n$, where$wt(a) = 1$, the derivative$D_a(f)$ is balanced.

If all coordinate functions of a vector booleanfunction$f: F_2^n \to F_2^m$satisfy SAC, then when one input bit changes, each of the output bits will change with a probability of 1/2.Hence, it is expected about half of the output bits to be changed [4, 5].

Definition 17. We call the canonical basis of the vector space $F_2^n$the set of vectors$e_j = (0,0,0,\dots,1,\dots 0,0,0)$, in which the only 1 is at position j, $j = 1 \dots n$.

The avalanche characteristic calculating Algorithm:

Input: Vector boolean function$f: F_2^n \to F_2^m$.

Step 1. Initialize the *n* x *m* results matrix to zero.

Step 2. For all binary vectors *a* of length *n*:

Find the value of a vector booleanfunction$f(a)$.

Step 3.For each$j = 1 \dots n$:

Find the value of a vector booleanfunction$f(a + e_j)$.

Step 4.Find the value of $wt(f(a) + f(a + e_j))$.

Step 5. Fill the results into the results matrix for each coordinate Boolean function and its each coordinate.

Step 6.Calculate the deviations of the values in the results matrix from 2^{n-1}.

Output: Maximum deviation in the results matrix.

5. Correlation immunity, stability. Lets denote the number of variables of the booleanfunction - n and the degree of its correlation immunity - m. In other words, it is a booleanfunction whose output does not correlate with the collection of any m inputs.

Definition 18.A booleanfunction *f*is called correlation immune of order k if the weight of

subfunctions$f_{i_1,i_2,\dots,i_k}^{a,a_2,\dots,a_k}$satisfies the relation$wt(f_{i_1,i_2,\dots,i_k}^{a,a_2,\dots,a_k}) = wt(f)/2^k$for any set of indices$1 \le i_1 < \dots < i_k \le n$and any values $a, a_2, \dots, a_k \in F_2$.

In other words, a booleanfunction *f*is called correlation immune of order k if$Pr|f = 1| = Pr\left|f_{i_1,i_2,\dots,i_k}^{a,a_2,\dots,a_k} = 1\right|$, where *Pr* – probability function, means that knowledge of some input bits does not provide statistical information about the value of the function [5].

In other words, the value of correlation immunity primarily determines the resistance of the symmetric block encryption algorithm to statistical attacks.

Definition 19. Boolean function*f*is called*k-resistant*, if any subfunction obtained by fixing at most k variables is balanced.

Statement 2. For a k-ordered correlation-immune boolean function *f* of n variables, having algebraic degree*deg(f)*, the inequality *deg(f)≤n-k*-1 is true [10].

The correlation immunity of a vector Boolean function $F: F_2^n \to F_2^m$**calculating algorithm**

Input: Function$F: F_2^n \to F_2^m$.

Step 1.Create an array of integers D of size 2^n, reset all its elements.

Step 2.Loop over components vF.

Step3.For each component: *w = W*$_{vF}$; *D = D∨w (element by element).*

Step4.For each *i* = 1,...,*n*:

For each vectors $u \in F_2^n$of weight*i:*

if $D_u \neq 0$*, then return, answer: i - 1.*

Output: answer *n.*

6.High nonlinearity. Definition20.The nonlinearity of a Boolean function *f* in *n* variables is the quantity N_f, equal to the Hamming distance from *f* to the set A_n of all affine functions in *n* variables.

This characteristic of a Boolean function can be calculated using the following formula:

$$N_f = d(f, A_n) = 2^{n-1} - max_{c \in F_2^n}\left|W_f(c)\right|/2.$$

From Parseval's equality the following upper bound for the nonlinearity value of a booleanfunction can be obtained:

$$N_f \le 2^{n-1} - 2^{n/2-1}.$$

In practice, the higher the value of the nonlinearity of a booleanfunction, the more preferable it is to use it in symmetric block encryption algorithms.

The nonlinearity degree of a vector booleanfunction calculating algorithm:

Input: vector booleanfunction$f: F_2^n \to F_2^m$.

Step 1. Initialize the results matrix *n*x*m* with zero values.

Step 2.For each$y \in F_2^n$find the Walsh-Hadamardcoefficients $W_f(y) = \sum_{x \in F_2^n}(-1)^{f(x) \oplus \langle x,y \rangle}$.

Step 3.Find the degree of nonlinearity$N_f = d(f, A_n) = 2^{n-1} - max_{c \in F_2^n}\left|W_f(y)\right|/2$.

Output: N_f.

7.Algebraic immunity. Definition21.Algebraic immunity *AI(f)*of a booleanfunction *f* is called the minimum value of *d* such that there exists a booleanfunction *g* of degree *d*, not identically equal to 0, annihilating the function *g* or its negation, that is the relation *fg = 0*or ratio *(f + 1)g = 0* [7].

Obviously, the higher the algebraic immunity of a function, the more difficult it is to apply the algebraic attack.

In [7], it was shown that for any function *f* the estimate $AI(f) \le \left\lceil \frac{n}{2} \right\rceil$,wheren – number of variables of a booleanfunction *f is fair.*

The calculating of the algebraic immunity by enumerating booleanfunctions algorithm:

Input: vector boolean function$f: F_2^n \to F_2^m$.

Step 1.For each$y \in F_2^n$find value$f(a)$.

Step 2.Find a vector of values for the assumed annihilator *g* so that *fg = 0* or *(f + 1)g = 0.* Enumeration should start with linear and affine functions.

Step3.If at step 2 a first-degree annihilator is found, then$AI(f) = 1$.

Step 4. If at step 2 there is no first-degree annihilator, then iterate over second-degree annihilators, etc..

Output: $AI(f)$.

It should be noted that when searching for a second-degree annihilator, the complexity of this algorithm exceeds 2^{56}operations for F_2^8.

8. Linear structures

Definition22.Function$f: F_2^n \to F_2^m$has a linear structure if there are a nonzero binary vector of length *n* such that $D_a(f(x)) \equiv const$, where$x \epsilon F_2^n$ exists.

It should be noted that by now the presence of linear structures in the vector boolean function$f: F_2^n \to F_2^m$has not been used in attacks on symmetric block encryption algorithms.

At the same time, the presence of a linear structure indicates its similarity to a linear function, therefore, the use of such functions in algorithms of block symmetric encryption is undesirable.

Linear structure search algorithm:

Input: vector boolean function$f: F_2^n \to F_2^m$.

Step 1. Loop over all input nonzero binary vectors *a* of length *n*.

Step 2.Calculate the directional derivative $D_a(f(x)) = f(x) \oplus f(x \oplus a)$, where$x \epsilon F_2^n$.

Step 3.Verify$D_a(f(x)) \equiv const$?

Output:Function$f: F_2^n \to F_2^m$has a linear structure, if$D_a(f)) \equiv const$.

Results. The analysis of the properties of the Qalqan symmetric block algorithm replacement node. In the Qalqan symmetric block encryption algorithm, a nonlinear node that allows resisting analytical attacks is implemented in the form of replacement nodes - vector booleanfunctions of length 8.

The replacement node is fixed as follows (in C-like format):

uint8 sb[256] = {0xeb, 0x89, 0xdb, 0xcb, 0xf3, 0xf5, 0xfb, 0x90, 0xe6, 0x3d, 0xe5, 0x2e, 0xe3, 0x0b, 0x56, 0xe1,0x6c, 0x12, 0x80, 0x28, 0xed, 0x22, 0x09, 0x4a, 0xee, 0x27, 0x9b, 0x58, 0x35, 0x57, 0xef, 0x94,0x29, 0xc0, 0x16, 0x7c, 0x5e, 0x87, 0x0a, 0x7e, 0xe8, 0x11, 0x0e, 0xaf, 0x9a, 0x84, 0x3a, 0x1a,0x69, 0x71, 0x8c, 0xbc, 0xd2, 0x55, 0x33, 0xd1, 0x85, 0x75, 0xb5, 0x83, 0xe9, 0x50, 0x54, 0xac,0x8a, 0xd6, 0x7f, 0x1f, 0x14, 0x4e, 0x21, 0x82, 0x30, 0x24, 0xdd, 0x9f, 0x1b, 0x32, 0x20, 0xa8,0x6a, 0xb0, 0x97, 0x62, 0x19, 0xd8, 0xc8, 0x0c, 0x52, 0x02, 0x5c, 0x43, 0x03, 0x95, 0x13, 0x81,0xab, 0x77, 0xa6, 0xf2, 0x59, 0x67, 0x41, 0xec, 0x76, 0x98, 0xb4, 0x73, 0x86, 0x9c, 0xf7, 0xcf,0xdc, 0xba, 0xa4, 0xfd, 0xc4, 0x99, 0xdf, 0xce, 0xea, 0x1c, 0x36, 0xbd, 0x34, 0xd7, 0x49, 0x64,0x5a, 0x6f, 0x74, 0x01, 0xa0, 0x39, 0x91, 0x00, 0x15, 0x3f, 0x38, 0xb8, 0x8f, 0x26, 0x5f, 0xf8,0x07, 0xa3, 0x0d, 0xda, 0xf0, 0xe7, 0xd0, 0xd9, 0x93, 0xf6, 0x06, 0x47, 0x0f, 0xa1, 0x4b, 0xc5,0x2a, 0xff, 0x46, 0x60, 0xd5, 0x1d, 0x2f, 0xa9, 0x92, 0x17, 0x72, 0x8e, 0x7a, 0xaa, 0x18, 0x6e,0x37, 0x08, 0x1e, 0x63, 0x31, 0xc2, 0xbf, 0xc6, 0x9e, 0x65, 0xd4, 0x3b, 0x96, 0x9d, 0xde, 0x45,0xca, 0x2d, 0xa5, 0xfe, 0x4d, 0xb9, 0x66, 0xc3, 0xb3, 0xcc, 0xad, 0x61, 0xbe, 0x7b, 0x68, 0x88,0x25, 0x2b, 0x53, 0x5b, 0x44, 0x40, 0xa7, 0xa2, 0x5d, 0xc9, 0x51, 0xae, 0xe4, 0xc7, 0xf9, 0x78,0x70, 0xcd, 0x42, 0x4f, 0x4c, 0x3c, 0xe0, 0x3e, 0x7d, 0xb7, 0xd3, 0xb2, 0xf1, 0x8d, 0x79, 0x8b,0x6b, 0xe2, 0x10, 0x23, 0x04, 0x6d, 0xc1, 0xfc, 0x05, 0xb6, 0xf4, 0x48, 0xbb, 0xb1, 0x2c, 0xfa};

Inverse replacement node used in decryption:

uint8 isb[256] = {0x87, 0x83, 0x59, 0x5c, 0xf4, 0xf8, 0x9a, 0x90, 0xb1, 0x16, 0x26, 0x0d, 0x57, 0x92, 0x2a, 0x9c,0xf2, 0x29, 0x11, 0x5e, 0x44, 0x88, 0x22, 0xa9, 0xae, 0x54, 0x2f, 0x4c, 0x79, 0xa5, 0xb2, 0x43,0x4e, 0x46, 0x15, 0xf3, 0x49, 0xd0, 0x8d, 0x19, 0x13, 0x20, 0xa0, 0xd1, 0xfe, 0xc1, 0x0b, 0xa6,0x48, 0xb4, 0x4d, 0x36, 0x7c, 0x1c, 0x7a, 0xb0, 0x8a, 0x85, 0x2e, 0xbb, 0xe5, 0x09, 0xe7, 0x89,0xd5, 0x66, 0xe2, 0x5b, 0xd4, 0xbf, 0xa2, 0x9b, 0xfb, 0x7e, 0x17, 0x9e, 0xe4, 0xc4, 0x45, 0xe3,0x3d, 0xda, 0x58, 0xd2, 0x3e, 0x35, 0x0e, 0x1d, 0x1b, 0x64, 0x80, 0xd3, 0x5a, 0xd8, 0x24, 0x8e,0xa3, 0xcb, 0x53, 0xb3, 0x7f, 0xb9, 0xc6, 0x65, 0xce, 0x30, 0x50, 0xf0, 0x10, 0xf5, 0xaf, 0x81,0xe0, 0x31, 0xaa, 0x6b, 0x82, 0x39, 0x68, 0x61, 0xdf, 0xee, 0xac, 0xcd, 0x23, 0xe8, 0x27, 0x42,0x12, 0x5f, 0x47, 0x3b, 0x2d, 0x38, 0x6c, 0x25, 0xcf, 0x01, 0x40, 0xef, 0x32, 0xed, 0xab, 0x8c,0x07, 0x86, 0xa8, 0x98, 0x1f, 0x5d, 0xbc, 0x52, 0x69, 0x75, 0x2c, 0x1a, 0x6d, 0xbd, 0xb8, 0x4b,0x84, 0x9d, 0xd7, 0x91, 0x72, 0xc2, 0x62, 0xd6, 0x4f, 0xa7, 0xad, 0x60, 0x3f, 0xca, 0xdb, 0x2b,0x51, 0xfd, 0xeb, 0xc8, 0x6a, 0x3a, 0xf9, 0xe9, 0x8b, 0xc5, 0x71, 0xfc, 0x33, 0x7b, 0xcc, 0xb6,0x21, 0xf6, 0xb5, 0xc7, 0x74, 0x9f, 0xb7, 0xdd, 0x56, 0xd9, 0xc0, 0x03, 0xc9, 0xe1, 0x77, 0x6f,0x96, 0x37, 0x34, 0xea, 0xba, 0xa4, 0x41, 0x7d, 0x55, 0x97, 0x93, 0x02, 0x70, 0x4a, 0xbe, 0x76,0xe6, 0x0f, 0xf1, 0x0c, 0xdc, 0x0a, 0x08, 0x95, 0x28, 0x3c, 0x78, 0x00, 0x67, 0x14, 0x18, 0x1e,0x94, 0xec, 0x63, 0x04, 0xfa, 0x05, 0x99, 0x6e, 0x8f, 0xde, 0xff, 0x06, 0xf7, 0x73, 0xc3, 0xa1};

Properties in the Table 1 have been established during the research of the above basic cryptographic properties.

Table 1. Research results of the main cryptographic properties of substitution nodes affecting cryptographic strength.

№	Vectorbooleanfunctionproperty	Qalqan symmetric block encryption algorithm
1	High algebraic degree of coordinate functions	7
2	Balanceofcoordinatefunctions	$wt(T_{fi}) = 2^{n-1} = 128$
3	Perfectpoise	$wt(T_{fi}) = 2^{n-1} = 128$
4	Avalanche criterion	128±
5	Correlation immunity	0
6	Nonlinearity, distance to a class of affine functions	112
7	Algebraicimmunity	$4 \geq AI(f) > 1$
8	Linearstructures	Absent

Conclusion. It is necessary to choose "good in all respects" vector Boolean functions as a reliable replacing node of a cryptographically strong algorithm of block symmetric encryption. Since the relationship between various cryptographic properties of vector boolean functions is not obvious it becomes a very nontrivial mathematical problem.

Сейлова Н.А.[1*], Ибраев Р.Б.[1], Горлов Л.В.[2], Тұрдалыұлы М.[1]

[1]Satbayev University, Алматы, Қазақстан;
[2] Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан.
E-mail: *seilova_na@mail.ru*

QALQAN БЛОКТЫҚ СИММЕТРИЯЛЫҚ ШИФРЛАУ АЛГОРИТМІНІҢ СЫЗЫҚТЫ ЕМЕС ТҮЙІНІНІҢ КРИПТОГРАФИЯЛЫҚ ҚАСИЕТТЕРІ

Аннотация. Байланыс арналары арқылы берілуге тиіс, сондай-ақ ақпараттық жүйелерде айналымда болатын қол жеткізу шектелген ақпараттың құпиялылығы мен тұтастығын қамтамасыз етуге криптографиялық қайта құру алгоритмдерін қолдану арқылы қол жеткізіледі. Атап айтқанда, ақпараттың құпиялылығын қамтамасыз ететін шифрлау алгоритмдері ақпаратты криптографиялық қорғау құралдарының өзегі болып табылады. Мұндай құралдардың қауіпсіздігі ең алдымен олардағы шифрлау алгоритмдерінің сапасы мен сенімділігімен анықталады.

Ақпаратты криптографиялық қорғау жүйесі ұйымдардың ақпараттық жүйелерінде айналымға түсетін сыни ақпаратты криптографиялық қорғауды қамтамасыз ету үшін жеткілікті болып табылады.

Бұл жұмыста Qalqan блоктық симметриялы шифрлау алгоритмінің сызықты емес түйінінің негізгі криптографиялық қасиеттері қарастырылады, оның криптографиялық тұрақтылығына әсер етеді, криптографиялық сипаттамаларды есептеу алгоритмдері келтірілген.

Ақпаратты криптографиялық қорғау жүйесі Qalqan блоктық симметриялық шифрлау алгоритмін және кілттерді құру, қалыптастыру, тарату және басқару хаттамасын жүзеге асырады. Ақпаратты криптографиялық қорғау жүйесін әзірлеу кезінде сыни ақпараты бар ақпараттық жүйелерде ақпаратты криптографиялық қорғау құралдарын пайдалануға қойылатын талаптарды регламенттейтін қолданыстағы нормативтік құқықтық актілердің талаптары ескерілген.

Qalqan алгоритмі ғылым мен техниканың даму үрдістерін ескере отырып әзірленген, әзірлеу кезеңінде салынған "беріктік қоры"есебінен криптографиялық шабуылдарға қарсы тұруға қабілетті.

Блоктық симметриялық шифрлаудың әзірленген алгоритмін мемлекеттің ақпараттық кеңістігін шетелдік шифрлау алгоритмдерінің құрылымдарында декларацияланбаған мүмкіндіктер есебінен туындайтын ықтимал қауіп-қатерлерден қорғауды қамтамасыз ету үшін белгіленген тәртіппен ұлттық стандарт ретінде бекіту ұсынылады.

Түйінді сөздер: шифрлау алгоритмі, векторлық логикалық функциялар, сызықты емес түйін

Қаржыландыру көзі. *Жұмыс № AP06851287 ЖТН "блоктық симметриялық шифрлау алгоритмін әзірлеу" гранттық жобасы аясында орындалды.*

Сейлова Н.А.[1*], Ибраев Р.Б.[1], Горлов Л.В.[2], Турдалыулы М.[1]

[1]Satbayev University, Алматы, Казахстан;
[2] Казахский национальный университет им. Аль-Фараби, Алматы, Казахстан.
E-mail: seilova_na@mail.ru

КРИПТОГРАФИЧЕСКИЕ СВОЙСТВА НЕЛИНЕЙНОГО УЗЛА АЛГОРИТМА БЛОЧНОГО СИММЕТРИЧНОГО ШИФРОВАНИЯ QALQAN

Аннотация. Обеспечение конфиденциальности и целостности информации с ограниченным доступом, подлежащей передаче по каналам связи, а также циркулирующей в информационных системах, достигается применением алгоритмов криптографического преобразования.

В частности, алгоритмы шифрования, обеспечивающие конфиденциальность информации, являются ядром средств криптографической защиты информации. Безопасность таких средств определяется в первую очередь качеством и надежностью реализованных в них алгоритмов шифрования.

Система криптографической защиты информации является самодостаточной для обеспечения криптографической защиты критической информации, циркулирующей в информационных системах организаций.

В данной работе рассмотрены основные криптографические свойства нелинейного узла алгоритма блочного симметричного шифрования Qalqan, влияющие на его криптографическую стойкость, приведены алгоритмы вычисления криптографических характеристик.

Система криптографической защиты информации реализует разработанныйалгоритма блочного симметричного шифрования Qalqan и протокол генерации, формирования, распределения и управления ключами.

При разработке системы криптографической защиты информации учтены требования действующих нормативных правовых актов, регламентирующих требования к использованию средств криптографической защиты информации в информационных системах с критической информацией.

Алгоритм Qalqan разработан с учетом тенденций развития науки и техники, способен противостоять криптографическим атакам за счет заложенного на этапе разработки «запаса прочности».

Разработанный алгоритм блочного симметричного шифрования рекомендуется утвердить в установленном порядке в качестве национального стандарта для обеспечения защиты информационного пространства государства от потенциальных угроз, возникающих за счет не декларированных возможностей в структурах иностранных алгоритмов шифрования.

Ключевые слова: алгоритм шифрования, векторные булевы функции, нелинейный узел.

Источник финансирования. *Работа выполнена в рамках грантового проекта «Разработка алгоритма блочного симметричного шифрования», ИРН № AP06851287.*

Information about authors:

Seilova Nurgul Abadullaevna – Assistant professor, Ph.D. Sciences, project manager № AP06851287, Almaty, Kazakhstan; seilova_na@mail.ru; https://orcid.org/0000-0003-3827-179X;

Ibrayev Renat Bulatovich – Master in Military Affairs a nd Security, h ead o f l aboratories, Satbayev University, renafm@mail.ru, *https://orcid.org/0000-0002-7800-9035*;

Gorlov Lev Vladimirovich – Master in Military Affairs and Security, PhD student,Al-Farabi Kazakh National University, Almaty, Republic of Kazakhstan, lev.gorlov@gmail.com, https://orcid.org/0000-0002-8208-4716;

Turdalyuly Mussa – PhD, Associate Professor, Satbayev University, Almaty, Kazakhstan, m.turdalyuly@gmail.com, *https://orcid.org/0000-0002-1470-3706*.

REFERENCES

[1] Léo Perrin, Aleksei Udovenko. Exponential S-Boxes: a Link Between the S-Boxes of BelT and Kuznyechik/Streebog // IACR Transactions on Symmetric Cryptology. — 2016. — P. 99–124. — ISSN 2519-173X. — doi:10.13154/tosc.v2016.i2.99-124.

[2] Kaisa Nyberg, Perfect non-linear S-boxes // EUROCRYPT 1991: Advances in Cryptology — EUROCRYPT ’91. – P. 378-386.

[3] Jie Cui, Liusheng Huang, Hong Zhong, Chinchen Chang, Wei Yang, An improved AES S- box and

its performance analysis // International Journal of Innovative Computing, Information and Control, 2011, volume 7, № 5(A), - P. 2291-2302.

[4] A.A.Gorodilova, From cryptanalysis of a cipher to a cryptographic property of a boolean function, Applied discrete math, 2016, number 3(33), 16–44.

[5] Shushuev G.I. «Vector Boolean functions at a distance of one from APN-function», Applied discrete mathematics, 2016.

[6] Buryakov M.L. Algebraic, combinatorial and cryptographic properties of parameters of affine constraints of Boolean functions, MSU, Moscow, 2009.

[7] *E.K. Alekseyev*, *E.K. Karelina*, Classification of correlation-immune and minimal correlation-immune Boolean functions of 4 and 5 variables, MSU, Moscow, 2015.

[8] Tuzhilin M.E. Algebraic immunity of boolean functions, Russian State University for the Humanities, Applied discrete mathematics, 2008.

[9] Courtois N., Meier W. Algebraic Attacks on Stream Ciphers with Linear Feedback // Proceedings of Eurocrypt 2003, Lecture Notes in Computer Sciences. 2003. V. 2656. P. 345 – 359.

[10] Chulkin T.A., Voloshyuk K.M. «Development of an algorithm for constructing replacing nodes of the encryption algorithms», Bulletin of the Siberian State Aerospace University named after academician M.F. Reshetiev, 2009.

[11] Logachev O.V., Salnikov A.A., Yaschenko V.V. «Cryptographic properties of discrete functions», Conference materials « Moscow University and the development of cryptography in Russia ». Moscow: Moscow Center for Continuous Mathematical Education.2003. –p. 174-199.

[12] N.M. Kiseleva, E.S. Lipatova, I.A. Pankratova, E.E. Trifonova, Algorithms for calculating the cryptographic characteristics of vector Boolean functions, «Computational methods in discrete mathematics», №46, 2019.

МАХМҰНЫ

ФИЗИКА

ИНФОРМАТИКА

МАТЕМАТИКА

СОДЕРЖАНИЕ

ФИЗИКА

ИНФОРМАТИКА

МАТЕМАТИКА

CONTENTS

PHYSICS

COMPUTER SCIENCE

MATHEMATICS

Publication Ethics and Publication Malpracticein
the journals of the National Academy of Sciences of the Republic of Kazakhstan

For information on Ethics in publishing and Ethicalguidelines for journal publication see http://www.elsevier.com/publishingethics and http://www.elsevier.com/journal-authors/ethics.

Submission of an article to the National Academy of Sciences of the Republic of Kazakhstan implies that the described work has not been published previously (except in the form of an abstract or as part of a published lecture or academic thesis or as an electronic preprint, see http://www.elsevier.com/postingpolicy), that it is not under consideration for publication elsewhere, that its publication is approved by all authors and tacitly or explicitly by the responsible authorities where the work was carried out, and that, if accepted, it will not be published elsewhere in the same form, in English or in any otherlanguage, including electronically without the written consent of the copyright-holder. In particular, translations into English of papers already published in another language are not accepted.

No other forms of scientific misconduct are allowed, such as plagiarism, falsification, fraudulent data, incorrect interpretation of other works, incorrect citations, etc. The National Academy of Sciences of the Republic of Kazakhstan follows the Code of Conduct of the Committee on Publication Ethics (COPE), and follows the COPE Flowcharts for Resolving Cases of Suspected Misconduct (http://publicationethics.org/files/u2/New_Code.pdf). To verify originality, your article may be checked by the Cross Check originality detection service http://www.elsevier.com/editors/plagdetect.

The authors are obliged to participate in peer review process and be ready to provide corrections, clarifications, retractions and apologies when needed. All authors of a paper should have significantly contributed to the research.

The reviewers should provide objective judgments and should point out relevant published works which are not yet cited. Reviewed articles should be treated confidentially. The reviewers will be chosen in such a way that there is no conflict of interests with respect to the research, the authors and/or the research funders.

The editors have complete responsibility and authority to reject or accept a paper, and they will only accept a paper when reasonably certain. They will preserve anonymity of reviewers and promote publication of corrections, clarifications, retractions and apologies when needed. The acceptance of a paper automatically implies the copyright transfer to the National Academy of Sciences of the Republic of Kazakhstan.

The Editorial Board of the National Academy of Sciences of the Republic of Kazakhstan will monitor and safeguard publishing ethics.

Правила оформления статьи для публикации в журнале смотреть на сайтах:

www:nauka-nanrk.kz

http://physics-mathematics.kz/index.php/en/archive

ISSN2518-1726 (Online),
ISSN 1991-346X (Print)

Редакторы: *М.С. Ахметова, А. Ботанқызы, Д.С. Аленов, Р.Ж. Мрзабаева*
Верстка на компьютере *Г.Д.Жадыранова*

Подписано в печать 10.12.2021.
Формат 60x881/8. Бумага офсетная. Печать –ризограф.
9,5 п.л. Тираж 300. Заказ 6.

Национальная академия наук РК
050010, Алматы, ул. Шевченко, 28, т. 272-13-19