Enumeration of Boolean Mapping with Given Cryptographic Properties for Personal Data Protection in Blockchain Data Storage

Konstantin Pankov
Moscow Technical University of Communications and Informatics
Moscow, Russia
pankov_kn@mtuci.ru

***Abstract*—Currently, blockchain data storage systems are considered promising for storing important information, including personal data. However, the requirements of modern legislation in various countries pose challenges to such systems, including the need to delete data at the request of users, which contradicts the very concept of the blockchain. One way to solve this problem is to use encryption. The paper presents the most powerful asymptotic estimates of the cardinality of sets of correlation-immune and (n,m,k)-resilient Boolean mappings that are used in the construction of stream encryption systems. Also, a recurrence relation is proved, allowing to calculate the number of (n,m,k)-resilient mappings for small values n, m and k.**

I. Introduction

The program "Digital Economy of the Russian Federation"[1], prepared by the Ministry of Communications and Mass Media of Russia in 2017 for the implementation of the President Putin annual address to Federal Assembly [2], contains a number of end-to-end digital technologies, which include distributed ledger technology based on blockchain technology. It is worth paying attention to the fact that the blockchain technology was not mentioned in the President's address. In recent years, scholars and developers have made many efforts to study various aspects of these technologies for practical application. Along with these studies, Russian and world organizations are actively working on developing standards for these technologies. In particular, by the order of the Federal Agency for Technical Regulation and Metrology (Rosstandart) No. 2831 dated January 15, 2018, a technical committee on standardization TC 159 "Software and hardware of distributed ledger technologies and blockchain" was established.

Moscow Technical University of Communications and Informatics (MTUCI) has been an active participant in TC 159 since its inception, and since November 2018, in the person of the author of this paper, has headed the working group "Security, Identification and Confidentiality". The immediate plans of the working group include studying the problems of compliance of blockchain-systems with domestic and foreign regulatory and legal framework in the field of information security, as well as problems of personal data protection in these systems [3].

A blockchain is a growing list of records, called blocks, which are linked using cryptographic tool, or rather, a hash function. Each block contains a cryptographic hash of the previous block and some transaction data. Term "blockchain" first appeared in 2008 as the name of a distributed database implemented in the Bitcoin cryptocurrency system [4]. However, the first papers [5], [6] along similar chains appeared in the early 1990s, and conceptual prototypes were described in [7] and [8]. Modern scholars [9] define the blockchain as "new digital ledger". which "can be programmed to record virtually anything of value and important for humankind…" Each user has his own copy of this ledger, and any new entries can be made to it only according to a specific procedure. Once recorded, information can never be changed or erased.

All users of the distributed ledger system form a network of computers, each of which stores a copy of the blockchain. As long as at least one data storage device or user is functioning, the blockchain exists. Adding a new user to the network leads to net's expanding and strengthening.

Due to these features, a distributed ledger system is considered as one of the most promising technologies for storing and protecting data [10], for example, to provide secure workflow and electronic interaction between citizens, state and municipal authorities [11].

The work [12] describes the practical application of the blockchain-system as a distributed data storage, the confidentiality of which is guaranteed by using symmetric encryption systems. In the comments to [12], the author wrote that the described system was implemented. This is an example of the blockchain-system with encryption. Consequently, blockchain systems containing personal data and being part of Russian personal information protection systems should be subject to organizational and technical security measures described in detail in the order of the Federal Security Service (FSS) of Russia No. 378 dated July 10, 2014 [13]. In particular, in order to fulfill obligations to protect personal data in Russia, it is necessary to use cryptographic information protection tools (CIPT) that are officially registered in the certification system of the FSS of Russia. The main criterion for certification is that all encryption algorithms must satisfy the GOST (Russian

standarts) [14]. The standards in the Russian Federation on the CIPT [15] describe block ciphers and their modes of operation, hash functions, as well as the processes of generating and verifying an electronic digital signature. However, for example, stream cipher algorithms are not standardized currently (beginning of 2019). Therefore, it remains relevant to study the characteristics of modern stream ciphers in terms of their security. Also, the blockchain-systems must comply with the requirements of the Russian Federal Law on Personal Data (No. 152-FZ), which was entered into force on July 27, 2006 [16].

II Personal data protection in blockchain data storage

A. Personal Data Laws and Blockchain

Russia is not the only country where personal data restrictions apply. In 2016, a law was passed in the European Union that regulates the security of personal data and the privacy for all individuals. It's The General Data Protection Regulation 2016/679 or GDPR [17]. By GDPR all people must have sway on their personal data. For example, they have the right to demand that their personal data is deleted from data storage.

However, any information recorded in the blockchain can be deleted or modified with great difficulty. It's almost impossible.

Thus, the blockchain, on the one hand, and, the European and the Russian legislation on the other hand, emanated from incompatible hypotheses about data integrity.

Some scholars argue [18] that personal data laws and the blockchain are totally irreconcilable. At the same time, there are currently papers that show how to create blockchain-systems that provide the ability to delete personal data, for example article [19].

B. How to remove data from public and private blockchain

In order to understand how to fulfill the requirements of the laws on personal data, let's consider the main difference between public and private blockchain.

Any user can participate in the public blockchain, carry out the consensus protocol and support the shared ledger. It's completely open for everyone [20].

In the private blockchain network, user rights are subject to restrictions, which consist, in particular, that not every user can add blocks to the chain. Moreover, different users may have different rights to add information of a certain type.

Usually the number of users or nodes that have the right to add information to the private blockchain is small. These nodes are able to delete data stored in a chain by switching to a new version called “forking”. This is described in detail in [19].

Unfortunately, to achieve a similar effect in the public blockchain is much more difficult. Creating a blockchain fork will require the agreement of too many network nodes and considerable computational effort.

According to [19], there are two methods to solve the problem of deletion of personal data in the public blockchain network.

For treasuring personal data, first method uses stand-alone storage. On the blockchain, only hash of personal data is stored. For example, this method is described in detail in [21].

A second method uses encryption. Each transaction is encrypted on its key, and encrypted cipher text is recorded in the chain.

Instead of deleting information, network nodes that have added a transaction to the chain, upon receiving a request for deletion, delete the corresponding key, which is treasured outside the blockchain. Although the information remains in the chain, it cannot be decrypted.

In [19], concerns have been expressed that the second method may be insecure due to the fact that the encryption algorithm may be broken.

To minimize the risk that the encryption mechanism may eventually be broken, it is required that the encryption algorithm to be used is as close as possible to perfect ciphers.

An perfect cipher is usually understood as one in which the use of a ciphertext by an adversary does not increase the probability of decrypting information. For example, it is described in [22].

One way to create a perfect cipher is a symmetric key cipher where plaintext digits are combined with a true random sequence digit stream (keystream).

Unfortunately, generating and using true random sequences is a difficult task, so pseudo-random sequences generated in stream ciphers can be used instead.

C. Stream cipher as perfect cipher model

The definition of a stream cipher is well known. One of the main ways to design stream ciphers is to use linear feedback shift registers (LFSR), which are also widely known. The example of LFSR is presented in fig. 1.

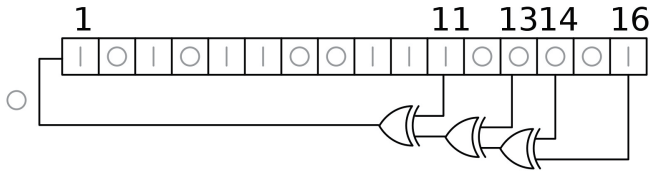

Fig. 1. A 16-bit Fibonacci LFSR from Wikipedia

To increase the security of a stream cipher with LFSR, various schemes have been offered: combination generators (Fig. 2), filter generators, clock-controlled generators, etc. In all these systems, the secret key usually consists of the initial states of component LFSRs.

For example, it is the use of the combining function that brings the properties of the stream cipher on the LFSR to the perfect cipher to some extent. Different properties of a combining function are important to avoid known adversarial attacks. For example, one of the most famous adversarial

attacks against the combination generator is the correlation attack, presented by Siegenthaler [23].

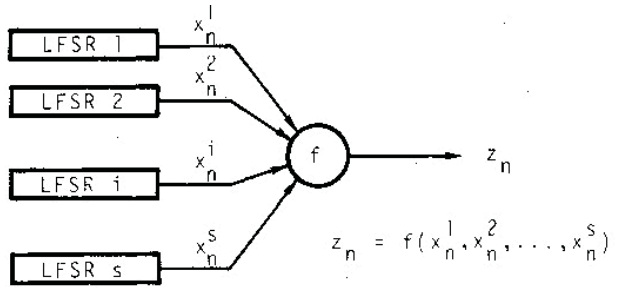

Fig. 2. Combination generator [23]

For the scheme presented in Fig. 2 this attack can be prevented by using a correlation immune [24] and resilient [25] combining function.

D. Correlation-immune and resilient mappings

Let V_n stand for the set of the binary vectors of dimensionality *n* (the vector space of n-tuples of elements from set $F_2 = \{0,1\}$).

Let *n* and *m* be two positive integers. Denote by B_n^m set of all functions from V_n to V_m:

$$B_n^m = \left\{ f(x) = (f_1(x), f_2(x), ..., f_m(x)) : V_n \to V_m, \right\},$$

where $f(x)$ - vectorial Boolean function (Boolean mapping, multi-output Boolean function), $f_i(x) : V_n \to F_2$ for all $i \in \{1,...,m\} = \overline{1,m}$ -- coordinate functions of $f(x)$.

In the pseudo-random generators of stream ciphers, Boolean mappings can be used to combine the outputs to n LFSR, or to filter the content of a single one, generating then m bits at each clock cycle instead of only one, which increases the speed of the cipher. Also Boolean mappings (S-boxes) are parts of iterative block ciphers and they play a central role in their robustness.

The Boolean mapping $f(x) = f(x_1,...,x_n) \in B_n^m$ is said to be correlation-immune with respect to set $I = \{i_1,...,i_t\} \subset \overline{1,n}$ (or equivalently independent of I) if the probability distribution of the random variable $f(X_1,...,X_n)$ is unaltered when $\{X_i, i \notin I\}$ is a set of independent equiprobable random variables and $\{X_i, i \in I\}$ is a set of constants, f is said to be correlation-immune of order k if for every $I \subset \overline{1,n}$ of cardinality at most *k*, the function $f(x)$ is correlation-immune with respect to I. The Boolean mapping $f(x)$ is said to have balanced output if every possible output m-tuple occurs with equal probability $\frac{1}{2^m}$. $f(x) \in B_n^m$ is said to be (n,m,k)-resilient if it is correlation-immune of order k and has balanced output [26].

The correlation-immune and resilient Boolean mappings are investigated in many works (see the survey [27]), mainly when *m=1*.

Enumeration of such mappings is a difficult task. To date, only asymptotic estimates of their number have been obtained ([28], [29], [30], [31]).

Denote by $K[n,m,k]$ the set of the correlation-immune of order k Boolean mappings from B_n^m. Let $R[n,m,k]$ the set of the (n,m,k)-resilient Boolean mappings. Denote by $|A|$ the cardinality of the set *A*.

The author of the paper obtained [32] the best in terms of *n* and *k* estimates for *m = 1* for today:

Theorem 1. Suppose $n \to \infty$ and $k < \frac{n}{\ln n}\left(\frac{\ln 2}{4} - a\right)$ for any $a \in \left(0, \frac{\ln 2}{4}\right)$; then

$$\log_2 |K[n,1,k]| \sim 2^n - \frac{1}{2}\left((n-k)\binom{n}{k} - n\right) - \\ -k - \sum_{i=1}^{k}\binom{n}{i}\log_2\sqrt{\pi/2}.$$

Theorem 2. Suppose $n \to \infty$ and $k < \frac{n}{\ln n}\left(\frac{\ln 2}{4} - a\right)$ for any $a \in \left(0, \frac{\ln 2}{4}\right)$; then

$$\log_2 |R[n,1,k]| \sim 2^n - \frac{n-k}{2}\binom{n}{k} - \sum_{i=0}^{k}\binom{n}{i}\log_2\sqrt{\pi/2}.$$

Also the author of the paper obtained [32] the best estimates for *m > 1*.

Denote by $S(m)$ the set

$$\left\{ r = (r_J, J \subset \overline{1,m}, J \neq \varnothing) \in \{0,1,...,2^{m-1}-1\}^{2^m-1}, \right. \\ \left. \forall s \in \overline{1,m}, \forall \delta \in V_m : \sum_{J \subset 1,m, s \in J} (-1)^{\langle \delta, ch_m(J) \rangle} r_J \in 2^{m-1}\mathbb{Z} \right\},$$

where $ch_m\left(J\right)$ - characteristic (indicator, incidence) vector of a subset J of a set $\overline{1,m}$, $\left\langle x,y\right\rangle$ - the scalar product of vectors *x* and *y*, $\mathbb{Z}$ - the set of integers.

Theorem 3. Suppose $n\to\infty$ and $k\left(5+2\log_2 n\right)+6m\le n\left(\frac{5}{18}-a\right)$ for any $a\in\left(0;\frac{5}{18}\right)$; then

$$\log_2\left|K\left[n,m,k\right]\right|\sim m2^n+\left(\frac{n+1+\log_2\pi}{2}-k\right)\left(2^m-1\right)-$$

$$-m2^{m-1}-\left(2^m-1\right)\left(\frac{n-k}{2}\binom{n}{k}+\sum_{i=0}^{k}\binom{n}{i}\log_2\sqrt{\frac{\pi}{2}}\right)+$$

$$+\sum_{i=0}^{k}\binom{n}{i}\log_2\left|S\left(m\right)\right|.$$

Theorem 4. Suppose $n\to\infty$ and $k\left(5+2\log_2 n\right)+6m\le n\left(\frac{1}{3}-a\right)$ for any $a\in\left(0,\frac{1}{3}\right)$; then

$$\log_2\left|R\left[n,m,k\right]\right|\sim m2^n-$$

$$-\left(2^m-1\right)\left(\frac{n-k}{2}\binom{n}{k}+\sum_{i=0}^{k}\binom{n}{i}\log_2\sqrt{\frac{\pi}{2}}\right)+$$

$$+\sum_{i=0}^{k}\binom{n}{i}\log_2\left|S\left(m\right)\right|.$$

Calculating $\left|S\left(m\right)\right|$ for small m is easy. For example, for $t\in\left\{2,3,4\right\}$

$$\log_2\left|S\left(t\right)\right|=2\cdot3^{t-2}-1.$$

For large m, you can use the estimate from [33]:

$$m-1\le\log_2\left|S\left(m\right)\right|\le1+\left(m-2\right)\left(2^{m-1}-1\right).$$

If $m=2$, this estimate is equivalent $1\le\log_2\left|S\left(m\right)\right|\le1$.

The proofs of Theorems 1-4 will be published in the near future in the journal "Discrete Mathematics and Applications".

F. Recurrence relation for the number of resilient mappings

Let J be non-empty subset of $\overline{1,m}$. The component function [34] f^J is the linear combination of coordinate functions of the Boolean mapping $f\left(x\right)$ with non all-zero coefficients:

$$f^J=f_{j_1}\oplus\ldots\oplus f_{j_s},J=\left\{j_1,\ldots,j_s\right\}\subset\overline{1,m}$$

From [27] it follows that properties of a mapping from B_n^m can be expressed via properties of its component functions in some cases. These properties include correlation immunity. Correlation immunity is an example of reducible and secondary property for B_n^m [27].

Denote by $\left\|g\right\|$ the weight of a Boolean function $g\in B_n^1$. Weight of a Boolean function $g\left(x\right)$ is the number of vectors $x\in V_n$ such that $g\left(x\right)=1$.

For any subset $I=\left\{i_1,\ldots,i_t\right\}\subset\overline{1,n}$ and any non-empty subset $J\subset\overline{1,m}$, let $w_I^J\left(f\right)$ denote the weight $\left\|\left(f^J\right)_{i_1,\ldots,i_{|I|}}^{1,\ldots,1}\right\|$ of the subfunction $\left(f^J\right)_{i_1,\ldots,i_{|I|}}^{1,\ldots,1}$ of the component function f^J of the Boolean mapping $f\left(x\right)\in B_n^m$, which is obtained by setting the variables $x_{i_1},\ldots,x_{i_t}$ equal to the constant 1.

Also for any subset $I=\left\{i_1,\ldots,i_t\right\}\subset\overline{1,n}$ and any non-empty subset $J\subset\overline{1,m}$, let $F_I^J\left(f\right)$ denote the spectral Fourier-Walsh-Hadamard coefficient [29]:

$$F_I^J\left(f\right)=2^{n-1}-\left\|f^J\left(x\right)\oplus\left(ch_n\left(I\right),x\right)\right\|.$$

The spectral Fourier-Walsh-Hadamard coefficient $F_I^J\left(f\right)$ is called the coefficient of statistical structure according to [35].

The correlation-immune order can be determined by the vector

$$F_k\left(f\right)=\left(F_I^J\left(f\right):J\subset\overline{1,m},J\ne\varnothing,I\subset\overline{1,n},\left|I\right|\le k\right)$$

which consists of the first (i.e., corresponding to the vectors of the weights *0, ... , k*) coefficients of statistical structure for each component function of Boolean mapping $f\left(x\right)\in B_n^m$.

For example [33],

$$f\left(x\right)\in R\left[n,m,k\right]\Leftrightarrow F_k\left(f\right)=\vec{0},$$

where $\vec{0}$ - vector $\left(0,\ldots,0\right)$ of dimensionality $\left(2^m-1\right)\sum_{i=0}^{k}\binom{n}{i}$.

Theorem 5. If *n*, *m* and *k* be three positive integers and $k<n$, then

$$\left|R\left[n,m,k\right]\right|=$$

$$=\sum_{\substack{z(I,J)\in\mathbb{Z},J\subset\overline{1,m},J\ne\varnothing,\\ I\subset\overline{1,n-1},|I|=k}}\left|\left\{h\in B_{n-1}^m:F_I^J\left(h\right)=0\;\forall I\subset\overline{1,n-1},\left|I\right|<k;\right.$$

$$\left.F_I^J\left(h\right)=2^{|I|}z\left(I,J\right)\forall I\subset\overline{1,n-1},\left|I\right|=k;\right\}$$

$$\forall J \subset \overline{1,m}, J \neq \varnothing\Big\}\Big| \times$$

$$\times\Big|\Big\{g \in B_{n-1}^m : F_I^J\left(g\right) = 0\,\forall I \subset \overline{1,n-1}, \left|I\right| < k; \forall J \subset \overline{1,m},$$

$$J \neq \varnothing, F_I^J\left(g\right) = -2^{|I|} z\left(I,J\right) \forall I \subset \overline{1,n-1}, \left|I\right| = k\Big\}\Big|.$$

Proof.

$$\left|R\left[n,m,k\right]\right| = \left|\left\{f\left(x\right) \in B_n^m : F_k\left(f\right) = \vec{0}\right\}\right| .$$

Consider the following formulas connecting the weights of subfunctions of a function and its spectrum coefficients [29]:

$$F_I^J = \sum_{L \subset I} \left(-1\right)^{|L|} \left(2^{n-1} - 2^{|L|} w_L^J\right), \tag{1}$$

$$w_I^J - 2^{n-|I|-1} = 2^{-|I|} \cdot \sum_{L \subset I} \left(-1\right)^{|L|+1} F_L^J, \tag{2}$$

Using (1) and (2), we get:

$$f\left(x\right) \in B_n^m \Leftrightarrow w_I^J\left(f\right) = 2^{n-|I|-1} :$$

$$\forall J \subset \overline{1,m}, J \neq \varnothing, \forall I \subset \overline{1,n}, 1 \le \left|I\right| \le k .$$

There is a one-to-one correspondence between $f^J \in B_n^1$ and the pair of its subfunctions $\left\{\left(f^J\right)_n^1, \left(f^J\right)_n^0\right\}$:

$$h\left(x_1,...,x_{n-1}\right) = \left(f^J\right)_n^1 = x_n f^J$$

$$g\left(x_1,...,x_{n-1}\right) = \left(f^J\right)_n^0 = \left(x_n \oplus 1\right) f^J = f^J - x_n f^J$$

Therefore, we have for any subset $K = \left\{i_1,...,i_t\right\} \subset \overline{1,n-1}$

$$w_K^J\left(h\right) = \left\|\left(f^J\right)_{i_1,...,i_{|I|}}^{1,...,1,1}\right\| = w_{K \cup \{n\}}^J\left(f\right)$$

$$w_K^J\left(g\right) = \left\|\left(f^J\right)_{i_1,...,i_{|I|}}^{1,...,1,0}\right\| = w_K^J\left(f\right) - w_{K \cup \{n\}}^J\left(f\right).$$

Denote by $z_I^J\left(f\right)$ any difference $2^{n-|I|-1} - w_I^J\left(f\right)$ for $f\left(x\right) \in B_n^m$. Now we get

$$F_I^J = \sum_{L \subset I} \left(-2\right)^{|L|} z_L^J\left(f\right), \tag{3}$$

$$z_I^J\left(f\right) = 2^{-|I|} \cdot \sum_{L \subset I} \left(-1\right)^{|L|+1} F_L^J, \tag{4}$$

Also

$$f\left(x\right) \in B_n^m \Leftrightarrow$$

$$\Leftrightarrow z_I^J\left(f\right) = 0 : \forall J \subset \overline{1,m}, J \neq \varnothing, \forall I \subset \overline{1,n}, \left|I\right| \le k .$$

Therefore, we have for any subset $I \subset \overline{1,n-1}$

$$z_I^J\left(h\right) = 2^{(n-1)-|I|-1} - w_I^J\left(h\right) =$$

$$= 2^{n-(|I|+1)-1} - w_{I \cup \{n\}}^J\left(f\right) = z_{I \cup \{n\}}^J\left(f\right),$$

$$z_I^J\left(g\right) = 2^{(n-1)-|I|-1} - w_I^J\left(g\right) = \left(2^{n-|I|-1} - w_I^J\left(f\right)\right) -$$

$$-\left(2^{n-(|I|+1)-1} - w_{I \cup \{n\}}^J\left(f\right)\right) = z_I^J\left(f\right) - z_{I \cup \{n\}}^J\left(f\right).$$

Thus, for each fixed vector of integers

$$\left(z\left(I,J\right) \in \mathbb{Z} : \forall J \subset \overline{1,m}, J \neq \varnothing, \forall I \subset \overline{1,n-1}, \left|I\right| = k\right)$$

of dimensionality $\left(2^m - 1\right)\binom{n-1}{k}$, there is a one-to-one correspondence between the set of functions $f\left(x\right) \in B_n^m$ satisfying condition

$$w_{I \cup \{n\}}^J\left(f\right) = 2^{n-(|I|+1)-1} - z\left(I,J\right) \forall I \subset \overline{1,n-1} : \left|I\right| = k \tag{5}$$

and the Cartesian product for sets

$$\Big\{h\left(x\right) \in B_{n-1}^m : z_I^J\left(h\right) = 0\,\forall I \subset \overline{1,n-1}, \left|I\right| < k, \forall J \subset \overline{1,m},$$

$$J \neq \varnothing, z_I^J\left(h\right) = z\left(I,J\right) \forall I \subset \overline{1,n-1}, \left|I\right| = k\Big\}$$

and

$$\Big\{g\left(x\right) \in B_{n-1}^m : z_I^J\left(g\right) = 0\,\forall I \subset \overline{1,n-1}, \left|I\right| < k\,\forall J \subset \overline{1,m},$$

$$J \neq \varnothing, z_I^J\left(g\right) = -z\left(I,J\right) \forall I \subset \overline{1,n-1}, \left|I\right| = k\Big\}$$

Since (3) and (4), it follows that condition (5) is equivalent to

$$F_{I \cup \{1\}}^J\left(f\right) = \sum_{L \subset I \cup \{1\}} \left(-2\right)^{|L|} z_L^J\left(f\right), I \subset \overline{1,n-1}; \left|I\right| = k$$

$$J \subset \overline{1,m}; J \neq \varnothing .$$

Using (3) and (4), we get $\forall J \subset \overline{1,m}$, $J \neq \varnothing$, $\forall I \subset \overline{1,n-1}$, $\left|I\right| < k$:

$$F_I^J\left(h\right) = \sum_{L \subset I} \left(-2\right)^{|L|} z_L^J\left(h\right) = 0 .$$

Also $\forall J \subset \overline{1,m}$, $J \neq \varnothing$, $\forall I \subset \overline{1,n-1}$, $\left|I\right| = k$:

$$F_I^J\left(h\right)=\sum_{L\subset I}\left(-2\right)^{|L|}z_L^J\left(h\right)=\left(-2\right)^{|I|}z\left(I,J\right)$$

As above $\forall J\subset\overline{1,m}$, $J\neq\varnothing$, $\forall I\subset\overline{1,n-1}$, $\left|I\right|<k$:

$$F_I^J\left(g\right)=0$$

and $\forall J\subset\overline{1,m}$, $J\neq\varnothing$, $\forall I\subset\overline{1,n-1}$, $\left|I\right|=k$:

$$F_I^J\left(g\right)=-\left(-2\right)^{|I|}z\left(I,J\right)$$

End of proof.

III. Conclusion

Thus, we can conclude that one of the ways to solve the problem of storing personal data in blockchain data storage is to use stream encryption systems, the characteristics of which should be as close as possible to perfect ciphers and resistant to attacks on cryptosystems. Correlation-immune and (n,m,k)-resilient Boolean mappings are important building blocks for such cryptographic systems. One of the significant tasks in the study of these sets of mappings is the problem of finding their cardinality, for the solution of which the asymptotic formulas (Theorem 1-4) and recurrence relation (Theorem 5) are proposed in the paper.

From Theorem 5 we can conclude that, it is necessary to study sets of mappings with different vectors $F_k\left(f\right)$ to find the cardinality of the set of the (n,m,k)-resilient Boolean mappings. For fixed values of n, m and k, the cardinality of sets of mappings from B_n^m with different vectors $F_k\left(f\right)$ can now be found only experimentally. The study of sets of functions with vectors $F_k\left(f\right)$ may be a further extension of this work.

Note that it is easy to formulate and prove a recurrence relation similar to that obtained in Theorem 5 for the cardinality of the set of the correlation-immune of order k Boolean mappings from B_n^m.

Further study of such sets of mappings will help to create more robust cryptographic systems for personal data protection in blockchain data storage. This task is particularly relevant in the case of a public blockchain.

Acknowledgment

I would like to thank professor O.V. Denisov for encouraging my research of Boolean mapping with given cryptographic properties and for many ideas I used.

References

[1] The Russian Government official website, On approval of the program "Digital Economy of the Russian Federation". 31.07.2017, (In Russian), Web: http://government.ru/docs/28653/.

[2] Official Internet Resources of the President of Russia, Presidential annual address to Federal Assembly. December 1, 2016, Web: http://www.kremlin.ru/events/president/news/53379/.

[3] Federal Agency of Communications (Rossvyaz) official website, Scientific research of MTUCI contributes to the formation of the work agenda for the blockchain standardization trademark, (In Russian), Web: https://www.rossvyaz.ru/press/news/news6369.htm.

[4] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, Web: https://bitcoin.org/bitcoin.pdf.

[5] S. Haber; and W. Stornetta, "How to time-stamp a digital document", Journal of Cryptology, Vol. 3, Issue 2, 1991, pp. 99–111.

[6] D. Bayer, S. Haber; and W. Stornetta, "Improving the Efficiency and Reliability of Digital Time-Stamping", *Sequences II. Methods in Communication, Security, and Computer Science*, 1993, pp 99–111.

[7] D. Mazieres; and D. Shasha, "Building secure file systems out of Byzantine storage" *Proceedings of the Twenty-First ACM Symposium on Principles of Distributed Computing*, 2002, pp. 108–117.

[8] N. Szabo, Bit Gold, Web: http://unenumerated.blogspot.ru/2005/12/bit-gold.html.

[9] D. Tapscott and A. Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin Is Money, Business, and the World,* New York: Penguin Random House, 2016.

[10] A. I. Vlasov, A. A. Karpunin, and I. O. Novikov, "System analysis of the blockchain data exchange and storage technology" *Modern technologies. System analysis. Modelin*g, (In Russian), Vol. 3 (55); 2017, pp .75-83.

[11] K.N. Pankov, "The introduction of distributed ledger technology to ensure secure workflow and electronic interaction of citizens, state and municipal authorities". *Report at the Grand National Information Security Forum "Infoforum-2018"*, (In Russian), Web: https://yadi.sk/d/vgZtBfnj3SAzJa.

[12] Napitok, Practical use of the blockchain as distributed data storage, (In Russian), Web: https://habr.com/post/337082/.

[13] GARANT system, Order of the Federal Security Service of Russia dated July 10, 2014 No. 378 "On approval of the Composition and content of organizational and technical measures to ensure the security of personal data when they are processed in personal data information systems using cryptographic information protection tools necessary for the implementation of the Russian Government's Federation of requirements for the protection of personal data for each of the levels of security", (In Russian), Web: http://base.garant.ru/70727118/#ixzz5cIa53VXp.

[14] P. Umnikov, and M. Nikishov, Problems of blockchain implementation in Russia, (In Russian), Web: https://corpshark.ru/p/problemy-vnedreniya-blockchain-v-rossii/.

[15] Technical committee on standardization TC 26 "Cryptographic Information Security" official website, National standards, (In Russian), Web: https://tc26.ru/standarts/natsionalnye-standarty/.

[16] The International Association of Privacy Professionals official website, Russian Federal Law on Personal Data (No. 152-FZ), Web: https://iapp.org/media/pdf/knowledge_center/Russian_Federal_Law_on_Personal_Data.pdf.

[17] Access to European Union law, Regulation (eu) 2016/679 of the european parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Web: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[18] D. Gerard, David Gerard Personal Site, the GDPR and "blockchain" — whatever that word specifically means (28.06.2018), Web: https://davidgerard.co.uk/blockchain/2018/06/28/ibm-the-gdpr-and-blockchain-whatever-that-word-specifically-means/.

[19] TNW, D. Michels, "Here's how GDPR and the blockchain can coexist", Web: https://thenextweb.com/syndication/2018/07/26/gdpr-blockchain-cryptocurrency/.

[20] J. Praveen, IBM official website, The difference between public and private blockchain, Web: https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/.

[21] G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing privacy: Using blockchain to protect personal data", *Security and Privacy Workshops (SPW), 2015 IEEE*, May 2015, pp. 180–184.

[22] R.Talbert, QUORA, Cryptography: What is a perfect cipher and why is the one time pad a perfect cipher?, Web: https://www.quora.com/Cryptography-What-is-a-perfect-cipher-and-why-is-the-one-time-pad-a-perfect-cipher.

[23] T. Siegenthaler, "Decrypting a Class of Stream Ciphers Using Ciphertext Only" *IEEE Trans. Comput.,* 34, 1, Jan. 1985, pp. 81-85.

[24] T. Siegenthaler, “Correlation-immunity of nonlinear combining functions for cryptographic applications”, *IEEE Transactions on Information theory*, V. IT-30, No 5, 1984, pp. 776–780.

[25] B. Chor, O. Goldreich, J. Hastad, J. Freidmann, S. Rudich and R. Smolensky, “The bit extraction problem or t-resilient functions”, *Proc. 26th IEEE Symposium on Foundations of Computer Science, Portland, Oregon,* 1985, pp. 396-407.

[26] K. Gopalakrishnan and D. R. Stinson, “Three characterizations of non-binary correlation-immune and resilient functions”, *Designs, Codes and Cryptography*, Volume 5, Issue 3, May 1995, pp. 241–251.

[27] O. A. Logachev, A. A. Salnikov, and V. V. Yashchenko, *Boolean Functions in Coding Theory and Cryptography*. Rhode Island: American Mathematical Society Providence, 2011.

[28] O.V. Denisov, “An asymptotic formula for the number of correlation-immune of order *q* boolean functions”, *Discrete Math. Appl*., 2, 1992, pp. 279–288.

[29] O.V. Denisov, “A local limit theorem for the distribution of a part of the spectrum of a random binary function”. *Discrete Math. Appl.* **10**, 2000, pp. 87–101.

[30] E. Bach, “Improved asymptotic formulas for counting correlation immune Boolean functions”, *SIAM Journal on Discrete Mathematics*, vol. 23, No. 3, 2009, pp. 1525—1538.

[31] E. R. Canfield, Z. Gao, C. S. Greenhill, B. D. McKay and R. W. Robinson, “Asymptotic enumeration of correlation-immune boolean functions”, *Cryptography and Communications*, No. 2, 2010, pp. 111-126.

[32] K. N. Pankov, “Improved asymptotic estimates for numbers of correlation-immune and (n,m,k)-resilient vectorial boolean functions” *Diskr. Mat.* (In Russian), 2018, Volume 30, Issue 2, pp. 73–98.

[33] K. N. Pankov, “Asymptotic estimates for numbers of Boolean mappings with given cryptographic properties” *Mat. Vopr. Kriptogr.* (In Russian), 2014, Volume 5, Issue 4, pp. 73–97.

[34] C. Carlet, “Vectorial Boolean Functions”, In *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*. Cambridge: Cambridge University Press, 2010, pp. 398-472.

[35] *Cryptographic vocabulary* (In Russian), Moscow: MCCME, 2006.